De openbare registers digitaal

Een studie naar de invloed van het elektronisch aanleveren van de notariële akte bij het Kadaster op de aansprakelijkheidsverdeling tussen Kadaster en notaris

Bastiaan van Loenen
Apeldoorn, april 1998
De Dienst voor het kadaster en de openbare registers
afdeling Openbare Registers en Kadaster
afdeling Beleid en Marketing
&
Technische Universiteit Delft
Subfaculteit Geodesie
Sectie Geo-informatie en Grondbeleid

De wereld wordt niet beter, slechts efficiënter....

Voorwoord

In veel logistieke branches wordt veelvuldig gebruik gemaakt van de uitwisseling van digitale gegevens. Het Kadaster is voornemens om gebruik te maken van digitale technieken voor de gegevensuitwisseling tussen met name de notaris en Kadaster. Het Kadaster wil de elektronische aanlevering van het afschrift van de notariële akte mogelijk maken. Dit rapport is een studie naar de aansprakelijkheid tussen Kadaster en de partijen waar het Kadaster mee communiceert. Het rapport is als afstudeerscriptie geschreven in een samenwerkingsverband tussen de subfaculteit Geodesie en de Dienst voor het kadaster en de openbare registers.

Lezers die geïnteresseerd zijn in de kenmerken van de digitale vorm van communiceren verwijs ik naar hoofdstuk 2. Lezers die geïnteresseerd zijn in de huidige gang van zaken bij het Kadaster kunnen in hoofdstuk 3 terecht. Hoofdstuk 4 handelt over de problemen van de nieuwe media voor het Kadaster en hoofdstuk 5 geeft een aantal oplossingsrichtingen. De nieuwe situatie die het Kadaster voor ogen heeft voor de aanlevering wordt in hoofdstuk 6 beschreven. Voor lezers die geïnteresseerd zijn in de elektronische aangifte bij de Douane of de gang van zaken op de Amsterdamse Effectenbeurs is hoofdstuk 7 aanbevelenswaardig.

Tijdens mijn verblijf in Apeldoorn van augustus 1997 tot april 1998 heb ik in een zeer prettige sfeer kunnen werken aan mijn scriptie. Hiervoor wil ik de hele afdeling Beleid en Marketing van het Kadaster heel erg bedanken.
Speciale dank is er voor veel mensen. Allereerst veel dank voor mijn directe begeleiders: Wim Louwman van het Kadaster en Jaap Zevenbergen van de subfaculteit. Daarnaast dank ik mevrouw De Jong voor haar begeleiding van mijn onderzoek als mijn afstudeerhoogleraar en voor haar inhoudelijke kritiek en adviezen. Voor de indirecte begeleiding wat zich onder andere uitte in adviezen over de vormgeving en inhoud van mijn scriptie ben ik de volgende personen dankbaar: Peter Laarakker, Alexander Maljaars en Gerrie Fenten.
Van onschatbare waarde voor mijn onderzoek is de levende kadasterencyclopedie, de heer Klaasse, geweest. Kamergenoten die mijn frustraties over het verloop van het onderzoek moesten aanhoren, mij gerust konden stellen en zelf ook hun ervaringen met mij deelden, wil ik ook bedanken: Henny, Carolina, Herman en Jacques bedankt!
Tenslotte is er één persoon die ik nog meer dank ben verschuldigd dan bovengenoemde personen: (ex-) kamergenoot Jan Stufken. Hij heeft me begeleid als een begeleider, aangehoord als een goed psycholoog, mijn scriptie gelezen als een Neerlandicus en kritiek gegeven als een manager.
Een ieder die ik vergeten ben, wil ik hier bedanken voor zijn of haar bijdrage die mede heeft geleid tot de totstandkoming van mijn scriptie.

Apeldoorn, april 1998
Bastiaan van Loenen

Inhoudsopgave

Samenvatting

In het IT-programma 2000 heeft het Kadaster aangegeven de bestaande werkwijzen zoveel mogelijk te willen vervangen door de inzet van informatietechnologie. Onderdeel van het IT-programma is de realisatie van het Kadastraal Vastgoedinformatiesysteem (KVS). Eén van de stappen om tot KVS te komen is de realisatie van de mogelijkheid afschriften van notariële akten elektronisch bij het Kadaster aan te leveren. Het elektronisch aanleveren kan met Electronic Data Interchange (EDI) gerealiseerd worden. EDI is de geautomatiseerde, gestandaardiseerde en genormeerde gegevensuitwisseling tussen organisaties. Bij het Kadaster wordt de mogelijke realisatie van het elektronisch aanleveren onderzocht in het project Elan.
In de vastgoedinformatiebranche is in tegenstelling tot andere branches weinig tot geen ervaring met EDI. De ervaring die men elders heeft opgedaan met EDI kan waardevol zijn voor het Kadaster. Voor het Kadaster en notariaat (KANO) is het tevens belangrijk dat de huidige aansprakelijkheidsverdeling ook in de nieuwe situatie gehandhaafd blijft.
De probleemstelling die in dit rapport centraal staat is:

Welke invloed heeft het door EDI aanleveren en verwerken van de notariële akte bij het Kadaster op de aansprakelijkheidsverdeling tussen partijen en hoe kan deze verdeling, mede op basis van ervaringen met EDI elders, juridisch worden vormgegeven?

Huidige situatie: analoog aanleveren van het kadasterformulier

Het analoge kadasterformulier met de verklaring van eensluidendheid wordt in de openbare registers bij het Kadaster ingeschreven. Het formulier moet naast de inhoudelijke eisen voortvloeiend uit de Wet op het Notarisambt en de Kadasterwet, integer en authentiek zijn. Na inschrijving moet het Kadaster er voor zorgen dat het formulier beschikbaar en leesbaar blijft met behoud van integriteit en authenticiteit.
De aansprakelijkheidsverdeling in de analoge situatie vloeit voort uit de Kadasterwet, de Wet op het Notarisambt uit 1842 en het Burgerlijk Wetboek. De notaris is aansprakelijk voor vervulling van de (inhoudelijke) eisen aan het kadasterformulier. Voor het transport van het afschrift van de notariële akte en het kadasterformulier is, buiten aangetekende post, de aanbieder (meestal de notaris), aansprakelijk. Het Kadaster is aansprakelijk voor de toetsing van de inschrijvingsvereisten. Voor de opslag van het kadasterformulier in de openbare registers en de gegevensverstrekking uit de registers en de kadastrale registratie is het Kadaster eveneens aansprakelijk.
Het grootste risico dat het Kadaster loopt binnen de verwerking van de aangeboden schriftelijke documenten is het ongeautoriseerd wijzigen van het kadasterformulier of het wijzigen van de kadastrale registratie door zijn medewerkers. Het feit dat het waarborgen van de rechtszekerheid van registergoederen vooral afhangt van het (dis)functioneren van kadastermedewerkers vormt een zwakke schakel in het verwerkingsproces van de notariële akte. Computertechnieken als EDI zijn een ideale oplossing om deze taak te vervullen.

Problemen van EDI voor KANO

De invoering van EDI brengt een aantal problemen met zich mee. Deels worden deze veroorzaakt door de eisen die door EDI aan de stukken gesteld worden (gestandaardiseerde stukken) en deels doordat de eisen in de Kadasterwet en Wet op het Notarisambt specifiek op een analoog stuk zijn gericht.
Verder moet ten gevolge van o.a. de bepalingen verzameld in de Wet computercriminaliteit de communicatie tussen Kadaster en notariaat op een adequaat beveiligde wijze geschieden.
Tenslotte is de onzekerheid omtrent de duurzaamheid van de opslag van digitale stukken een bron van problemen. De centrale vraag is hierbij tweeledig: waar moet het digitale stuk op worden bewaard en wat moet worden opgeslagen?

Oplossingen voor EDI bij KANO

De problemen kunnen worden opgelost. De standaardisatie van de stukken zal voor 99 van de 100 stukken mogelijk zijn. Voor een gering aantal inschrijvingen zal een bewaarder van vlees en bloed noodzakelijk blijven.
De inschrijving van een akte op een nieuw medium moet in de Kadasterwet mogelijk worden gemaakt. De nieuwe vormvereisten moeten in de uitvoeringsregeling van de Kadasterwet worden geregeld. Aanpassing van de Wet op het Notarisambt is niet nodig.
Door de aanbieding van elektronische stukken te koppelen aan voorwaarden gesteld in een vergunning of in een Interchange Agreement kan de beveiliging van de communicatie, de conflicthantering en de mogelijkheid om meerdere stukken tegelijk bij het Kadaster aan te bieden worden geregeld. De vergunning heeft als voordeel ten opzichte van het Interchange Agreement dat het Kadaster eenzijdig de voorwaarden kan aanpassen. Een vergunning moet echter wel worden verankerd in de Kadasterwet.
De huidige gang van zaken voor wat betreft het aanbieden van een stuk bij het Kadaster rechtvaardigt de beperking van het aantal aanbieders door de aanbieding afhankelijk te stellen van een Interchange Agreement of vergunning verleend door het Kadaster.

Voor de aansprakelijkheidsverdeling is met name de technische invulling van de juridische eisen aan het digitale equivalent van de notariële akte van belang. De technische invulling van de juridische eisen aan het digitale equivalent van de notariële akte kan op de volgende wijze:

- gebruik van een gesloten systeem Kadaster - aanbieder
- gebruik van de hashwaarde voor de integriteitsbepaling
- gebruik van asymmetrische encryptie voor de herkomst van het stuk en de onleesbaarheid tijdens verzending
- gebruik van biometrische kenmerken voor de toegang tot de systemen
- gebruik van procedurele beveiliging voor de constatering van een verloren of afgedwaald stuk

Voor de opslag van het digitale document is het Kadaster aansprakelijk. Het Kadaster moet zorg dragen voor de beschikbaarheid, de leesbaarheid en het behoud van integriteit en authenticiteit van het document. De Write Once Read Many-plaat met waarborgen voor integriteit en authenticiteit heeft zich (nog) niet bewezen en kan door zijn kwetsbare fysieke gesteldheid voor rechtsonzekerheid op lange termijn (~100 jaar) zorgen.
Het behoud van de controles op integriteit en authenticiteit leidt ertoe dat de gegevens en de soft- en hardware die nu deze controles mogelijk maken moeten worden bewaard.
Het bestaande analoge schaduwarchief moet ter waarborg van de betrouwbaarheid van de digitale openbare registers worden aangevuld met een digitaal schaduwarchief.

De rol van een Trusted Third Party (TTP)
Een TTP is een derde partij die door communicerende partijen wordt vertrouwd. Een TTP kan diverse functies vervullen; een TTP kan de rol van Certificerende Instantie spelen en de sleutelgeneratie en verificatie bekrachtigen. Ook kan het oordeel of de registratie van een TTP bij een conflict tussen partijen van doorslaggevende betekenis zijn.
Een Trusted Third Party is voor het Kadaster alleen van belang als deze de rol van Certification Authority (CA) vervult.

Elektronisch aanleveren bij het Kadaster

De problemen die het elektronisch aanleveren van het digitale equivalent met zich meebrengt heeft het Kadaster in samenwerking met het notariaat grotendeels onderkend en met de voorgenomen wijziging van de Kadasterwet is een juridische oplossing gevonden om het elektronisch aanleveren mogelijk te maken. De (vorm)vereisten aan het digitale equivalent van de notariële akte zullen in de nog te wijzigen

Uitvoeringsregeling Kadasterwet worden opgenomen. De aanbieding van de digitale stukken zal anders dan in de analoge situatie worden gekoppeld aan een vergunningsstelsel.

De toepassing van hashwaarden en semi-asymmetrische encryptie geeft technisch invulling aan de juridische eisen van integriteit en authenticiteit van het stuk. Het stuk zal over een gesloten netwerk worden aangeboden aan het Kadaster. De autorisatie tot de systemen is nog niet geregeld.
De encryptie die zal worden toegepast is slechts bedoeld voor de identificatie van afzenders en notaris en niet voor de beveiliging van de documenten. Naast digitale openbare registers willen het Kadaster en het notariaat openbare registers van geanalogiseerde digitale equivalenten van notariële akten.

De aansprakelijkheid van het Kadaster heeft vanaf het moment van inschrijven betrekking op de juistheid en volledigheid van de gegevens als blijkt dat de digitale openbare registers niet overeenstemmen met de analoge openbare registers. Is dit niet het geval dan is de notaris aansprakelijk voor de overeenstemming van het digitale equivalent van de akte met de minuutakte en de inhoudelijke juistheid en volledigheid van het digitale equivalent van de akte.

Over de mogelijke rol van een TTP neemt het Kadaster in afwachting van de (juridische) ontwikkelingen op dit moment omtrent TTP's een afwachtende houding aan. Vooralsnog zal het Kadaster zelf de sleutelgeneratie verzorgen.

EDI elders

In het onderzoek is het systeem dat de invoeraangifte bij de Douane regelt nader bekeken en de wijze waarop op de Amsterdamse Effectenbeurs aandelen worden verhandeld. Beide branches zijn voor wat betreft de waarde van het document vergelijkbaar met het document dat wordt ingeschreven in de openbare registers. De eisen die het Kadaster echter stelt aan de opslag van het document worden niet aan de opslag van de documenten van de Douane en de Amsterdamse Effectenbeurs gesteld. De waarde van het ingeschreven stuk in de openbare registers kan na zelfs 100 jaar nog grote waarde hebben. Bij de Douane is de waarde van de aangifte na een aantal jaar niet meer aanwezig en op de Effectenbeurs heeft de transactie na een aantal dagen zijn waarde verloren. Gezien de eisen die het Kadaster dus moet stellen aan de duurzaamheid van de opslagmedia en de gegevens op deze media in de openbare registers, zijn beide geselecteerde branches niet vergelijkbaar gebleken.

Conclusies

De invloed van het elektronisch aanleveren op de aansprakelijkheidsverdeling tussen partijen wordt vooral bepaald door de waarborgen van de techniek. De juridische eisen aan het analoge formulier en het digitale equivalent van de notariële akte zijn gelijk. Slechts de technische invulling van de juridische eisen verschilt.
Voor het aanbieden van het afschrift van de notariële akte en het kadasterformulier is en blijft de aanbieder (de notaris of vergunninghouder) aansprakelijk. Het Kadaster is en blijft aansprakelijk voor de inschrijving van stukken in de openbare registers. Voor de inhoudelijke juistheid van de stukken in de digitale openbare registers zal de notaris aansprakelijk zijn als de technologische waarborgen de integriteit en authenticiteit van het stuk bevestigen. Is dit niet het geval dan zal het Kadaster aansprakelijk zijn voor de inhoudelijke juistheid van stukken die het verstrekt uit de openbare registers. Het Kadaster is en blijft eveneens aansprakelijk voor de leesbaarheid en beschikbaarheid van het ingeschreven stuk.
Als de beschikbaarheid, leesbaarheid en de controle op de integriteit en authenticiteit van het digitale equivalent technisch worden gewaarborgd zal de aansprakelijkheidsverdeling niet verschuiven. Indien één van de vier eisen niet worden gewaarborgd kan de aansprakelijkheidsverdeling verschuiven ten nadele van het Kadaster.

Summary

In its IT-program 2000 the Cadastre stated its intention to replace the existing working methods as much as possible by using information technology. Part of this IT-program is the establishment of the Cadastral Real Estate Information System. One of the steps to complete this system is the introduction of the possibility to deliver copies of notarial documents electronically to the Cadastre. Such an electronic delivery can be effectuated by use of Electronic Data Interchange (EDI). EDI is the automated, standardised and normalised interchange of data between organisations. At the Cadastre the possibility of introducing the digital delivery is investigated in the Elan project.
In contradiction to other branches there is little, if any, experience with EDI in the Real Estate branch. The elsewhere gathered information concerning this experience can be of great value to the Cadastre. For the Cadastre and the profession of notaries (CANO) it is also important to maintain the current situation of the distribution of responsibility in the new situation.
The central question of this report is:

Which are the consequences of the delivery and processing of the notarial documents by using EDI to the Cadastre on the distribution of responsibility between these two parties, and how can this distribution juridical be designed, taking into account the experiences with EDI elsewhere?

Current situation: Analogous delivery of the cadastral form

The analogous cadastral form with the declaration of a true copy is entered in the public registers at the Cadastre. Besides the requirements in contents resulting from the Cadastre Act and the Act on the profession of Notary the form should be authentic and integer. After registration the Cadastre should take care of the form staying available and readable with preservation of its integrity and authenticity.
The division of liability in the analogous situation results from the Cadastre Act, the Act on the Profession of Notary from 1842 and the Civil Code. The notary is liable for the correctness of the contents of the cadastral form. For the transportation of the copy of the notarial document and the cadastral form the presenter (most of the times the notary) is responsible. The Cadastre is liable for the testing of the inscribing requirements as well as for the storage of the cadastral form in the public registers and the data supply from the registers and the cadastral registration.
The severest risk the Cadastre runs at processing the documents is the unauthorised changing of the cadastral form or the cadastral registration by its staff.
The fact that the guarantee of the legal security of register goods mainly depends on the (dis-) functioning of cadastral staff forms a weak link in the processing of the notarial document. Computer technology like EDI are an ideal solution to fulfil this task.

Problems from EDI for CANO

The introduction of EDI brings a few problems. Part of these are caused by the requirements of EDI regarding the documents (standardised documents) and part by the fact that the requirements in the Cadastre Act and the Act on the Profession of Notary are specifically focused on an analogous document.
Furthermore the communication between Cadastre and Notary has to take place in an adequately secured way as a consequence of regulations in the Act on the computer criminality.
Finally the uncertainty concerning the durability of the storage of digital pieces is a source of difficulties. The central question in this subject-matter is twofold: where should the digital document be stored and what should, besides the digital piece, be saved?

Solutions for EDI at CANO

The problems can be solved. The standardisation of the documents will in 99 out of the 100 cases be possible. For a small number of the registrations s a keeper of flesh and blood will remain necessary.
The registration of a document on a new medium should be made possible in the Cadastre Act. The new form requirements have to be arranged in the execution regulation of the Cadastre Act. Adaptation of the Law on the profession of notary is not necessary.
By joining the offering of electronic documents with requirements stated in a licence or Interchange Agreement the protection of the communication, the handling of conflicts and the possibility to offer more documents at the same time at the Cadastre can be arranged. The licence has the advantage with respect to the Interchange Agreement that the Cadastre can partially adapt the conditions. A licence however has to be based in the Cadastre Act.
The current practice of presenting documents to the Cadastre justifies the limitation of the number of presenters by making the right to present documents depended on an Interchange Agreement or licence given by the Cadastre.

For the division of liability especially the technical completion of the juridical requirements is important. The technical completion of the juridical requirements of the digital equivalent of the notarial document can take place in this way:

- the use of a closed system Cadastre-presenter
- the use of the hashvalue for the determination of integrity
- the use of asymmetrical encryption for the origin of the documents and the unreadability during the sending.
- the use of biometric characteristics for entrance into the systems
- the use of procedural protection for the founding of a lost or strayed document

The Cadastre is liable for the storage of the document. The Cadastre should take care of the availability, the readability and the preservation of integrity and authenticity of the document. The Write Once Read Many plate with guarantees for the integrity and authenticity has not (yet) proven itself and can, because of its vulnerable physical state, cause legal uncertainty on the long term (~100 years).
The conservation of the controls on integrity and authenticity leads to the fact that the data and the soft- and hardware, which make these controls possible at this moment, should be stored.
The existing analogous shadow archive should be completed by a digital shadow archive to maintain the reliability.

The role of a Trusted Third Party (TTP)
A TTP is a third party that is trusted by communicating parties. A TTP can fulfil various functions; a TTP can fulfil the roll of Certification Authority and confirm the keygeneration and take care of the verification. The judgement of the registration of a TTP can in case of a conflict also be of decisive meaning.
A Trusted Third Party is to the Cadastre only important when it fulfils the roll of Certification Authority.

Electronic delivery at the Cadastre

The problems the electronic delivery of the digital equivalent takes with it are, in co-operation with the profession of notary, mostly discerned by the Cadastre. A juridical solution to make the electronic delivery possible has been found with the intended change of the Cadastre Act. The (form) requirements of the digital equivalent of the notarial document will be inserted in the Execution arrangement of the Cadastre Act. The offering of the digital pieces will, other than in the analogous situation, be joined to a system of licences.

The application of hashvalues and semi-asymmetrical encryption gives technical implementation to the juridical requirements of integrity and authenticity of the piece. The piece will be presented to the Cadastre through a closed network. The authorisation to the systems has not yet been arranged.

The encryption is only meant for the identification of the senders and notary, but not for the protection of the documents. Besides digital public registers the Cadastre and the profession of notary want a public register of digital equivalents of notarial documents that are made analogous.

The responsibility of the Cadastre has, from the moment of registration, connection to the correctness and completeness of the data when it turns out that the digital public registers do not coincide with the analogous public registers. When this is not the case the notary is liable for the accordance of the digital equivalent of the document with the minute document and the correctness with respect to contents and completeness of the digital equivalent of the notarial document.

At this moment the Cadastre assumes an attitude of expectation about the possible role of a TTP waiting for the (juridical) developments. For the time being the Cadastre will take care of the key-generation.

EDI elsewhere

During the research the system that handles the import declaration at the Customs and the way the Amsterdam Stock Exchange deals in shares has been looked at further. Both branches are, concerning the value of the document, comparable with the document that is entered in the public registers. The demands the Cadastre makes to the storage of the document are not made to the documents of the Customs and the Amsterdam Stock Exchange.
The entered piece in the public registers can even be valuable after 100 years. At the Customs the value of the declaration is already gone after a year and at the stock exchange it already lost its value after a couple of days. Respected the requirements the Cadastre has to require from the durability of the storage media, the selected branches are not comparable.

Conclusions

The consequences of the electronic delivery on the distribution of responsibility between parties are mainly determined by the guarantees of the technology. The juridical requirements to the analogous form and the digital equivalent of the notarial documents are the same. Only the technical completion of the juridical requirements is different.
The presenter is and remains responsible for the offering of the copy of the notarial document and the cadastral form. For the entering of the pieces in the public registers the Cadastre is and remains liable. For the correctness in contents of the pieces in the digital public registers the notary will be responsible when the technical guarantees confirm the integrity and authenticity of the piece. When this is not the case the Cadastre will be liable for the correctness in contents of the pieces it provides from the public registers. The Cadastre is and remains also responsible for the readability and availability of the entered piece.
When the availability, readability and control of integrity and authenticity of the digital equivalent are technical guaranteed the division of responsibility will not change. If one of these four requirements is not guaranteed the division of responsibility can shift at the cost of the Cadastre.

1. Inleiding

De laatste jaren zijn EDI-technieken sterk in opkomst. EDI staat voor Electronic Data Interchange. Letterlijk vertaald betekent EDI: elektronische gegevensuitwisseling. Een gangbare definitie van EDI luidt[1]:

EDI is de geautomatiseerde, elektronische uitwisseling van gestructureerde en genormeerde gegevens tussen computers van verschillende organisaties.

Met name de logistieke sector kent vele toepassingen. Complete papierstromen worden hierbij vervangen door elektronische berichtenuitwisseling met behulp van EDI-technieken. Ook bij het Kadaster kunnen omvangrijke gegevensstromen met papier worden onderscheiden. Bij de aanlevering van het afschrift van de notariële akte door de notaris aan het Kadaster speelt papier een grote rol.
Om tot een efficiëntere bedrijfsvoering te komen en aan de behoefte aan digitale gegevens van de klanten van het Kadaster te kunnen voldoen, heeft het Kadaster in het IT-programma 2000 aangegeven dat men de bestaande werkwijzen zoveel mogelijk wil vervangen door de inzet van informatietechnologie (onder andere met EDI). Onderdeel van het IT-programma is de realisatie van het Kadastraal Vastgoedinformatiesysteem (KVS). Dit systeem zal stapsgewijs dé informatiedatabank van het Kadaster worden waar gegevens uit de kadastrale registratie, de hypotheekregistratie en het landmeetkundig cartografisch gegevenssysteem worden gecombineerd. Eén van de te nemen stappen om tot KVS te komen is de realisatie van de mogelijkheid afschriften van notariële akten elektronisch bij het Kadaster aan te leveren. Deze mogelijkheid wordt in het project Elan samen met de Koninklijke Notariële Beroepsorganisatie onderzocht.

Alvorens de elektronische aanlevering van de notariële akte technisch te realiseren, is het van belang inzicht te krijgen in de juridische gevolgen van de invoering van het elektronisch aanleveren. De nieuwe vorm van aanleveren zorgt namelijk voor een aantal juridische problemen. Deze juridische problemen hangen samen met het ontbreken van zekerheid omtrent de wijze waarop bestaande rechtsnormen zullen worden toegepast bij gebruik van EDI. Een deel van deze problemen vloeit voort uit de Kadasterwet en de Wet op het Notarisambt uit 1842, die er expliciet of impliciet van uit gaan dat gegevens door middel van een geschrift worden uitgewisseld. Tevens is het onzeker of het recht dat de notariële akte nu belichaamt ook zonder papier kan worden vertegenwoordigd. Het grootste discussiepunt hierbij is de vervanging van de analoge handtekening door een digitale handtekening.

Bij het op papier aanleveren van de akte worden soms fouten gemaakt die leiden tot schade bij partijen. In het huidige analoge aanleverproces van de notariële akte bij het Kadaster is bij wet (Burgerlijk Wetboek en Kadasterwet) vastgelegd wie op welk moment aansprakelijk is voor welke activiteit; de aansprakelijkheidsverdeling vloeit voort uit de wet.
Ook bij het elektronisch aanleveren van de akte bij het Kadaster kunnen fouten optreden die tot schade kunnen leiden bij partijen. Welke partij bij het elektronisch aanleveren van de notariële akte aansprakelijk is voor welke fouten is thans om bovengenoemde redenen onduidelijk. De onzekerheid van het toepassen van bestaande rechtsnormen kan gevolgen hebben voor de aansprakelijkheidsverdeling van de betrokken partijen. Is het Kadaster in de analoge situatie bijvoorbeeld niet aansprakelijk voor de berichten van de afzender in de elektronische situatie hoeft dit niet meer het geval zijn[2].

In de vastgoedwereld wordt (nog) niet op grote schaal gebruik gemaakt van EDI-technieken; EDI bevindt zich hier in een beginstadium. Dit in tegenstelling tot sommige andere branches waar reeds enige jaren

[1] Vlist, P. van der, e.a., 1992.
[2] De ontvanger is aansprakelijk voor schade ten gevolge van een fout in de berichtgeving als de ontvanger het communicatiemiddel heeft voorgeschreven aan de afzender; art. 3:37 vierde lid BW

gebruik wordt gemaakt van EDI. De ervaringen die men daar heeft opgedaan met EDI geven inzicht in hoe men met het aanleverproces van de akte met EDI om moet gaan. Met name de juridische invulling van de onzekerheden levert een bijdrage aan de nieuwe en onbekende vorm van communiceren tussen Kadaster en notaris.

Probleemstelling

Welke invloed heeft het door EDI aanleveren en verwerken van de notariële akte bij het Kadaster op de aansprakelijkheidsverdeling tussen partijen en hoe kan deze verdeling, mede gezien ervaringen met EDI elders, juridisch worden vormgegeven?

De probleemstelling beslaat het gehele proces van aanlevering door de notaris bij en verwerking van de notariële akte door het Kadaster. Ook de wettelijke eisen aan de inhoudelijke juistheid van de notariële akte worden in het onderzoek meegenomen.
De probleemstelling zal met inachtneming van de uitgangspunten en randvoorwaarden die het Kadaster hanteert in zijn onderhandelingen met de Koninklijke Notariële Beroepsorganisatie over het aanleverproces bekeken worden. Deze uitgangspunten en randvoorwaarden zijn:

- het aanbieden van het analoge kadasterformulier met de verklaring van eensluidendheid moet mogelijk blijven
- iedereen moet het digitaal equivalent van de akte elektronisch kunnen aanleveren
- de bestaande wettelijke procedures en wettelijke eisen aan de akte moeten zoveel mogelijk gehandhaafd blijven
- de digitaal equivalenten van akten moeten voldoende beveiligd via het netwerk worden aangeleverd
- de digitaal equivalenten van akten worden landelijk centraal opgeslagen
- de huidige aansprakelijkheidsverdeling moet gehandhaafd blijven

Met de notariële akte zoals deze in de probleemstelling wordt genoemd wordt voor de analoge situatie het kadasterformulier met een verklaring van eensluidendheid bedoeld[3]. Voor de elektronische aanlevering wordt met de notariële akte bedoeld: het digitale equivalent van de notariële akte. Onder aansprakelijkheid wordt verstaan: de aansprakelijkheid voor schade ontstaan door gebreken in het aanleverproces en fouten bij de verwerking van de akte. De aansprakelijkheid zoals die in het Burgerlijk Wetboek, de huidige Kadasterwet en de huidige Wet op het Notarisambt behandeld wordt, vormt hier het uitgangspunt.
Omdat de techniek bij EDI de waarborg vormt voor een betrouwbare communicatie tussen organisaties en de registratie bij organisaties, en veel juridische problemen samenhangen met de mate waarin gebruik wordt gemaakt van de mogelijkheden die de techniek biedt, zullen de technische mogelijkheden voor wat betreft een betrouwbare communicatie en registratie van documenten worden onderzocht.
Bij de in het onderzoek betrokken ervaringen van andere organisaties met EDI is de nadruk gelegd op de technische vormgeving van het document en de aansprakelijkheidsverdeling in de digitale situatie. De andere branche moet vergelijkbaar zijn met de Kadaster - notarisbranche (KANO) en op basis van: de waarde van het document, de eisen omtrent de betrouwbaarheid van de uitwisseling van het document, het aantal deelnemers dat met elkaar communiceert en het vertrouwen dat de communicerende partijen in elkaar hebben.

De organisatorische veranderingen die EDI met zich mee brengt worden niet onderzocht. Ook technische aspecten als de werking van herkenningstechieken en apparatuurkeuzes bij het gebruik van EDI vallen buiten de reikwijdte van het onderzoek. Partijen die niet direct betrokken zijn bij het aanleverproces bij het Kadaster, zoals softwareleveranciers, service-providers, netwerk- en computerinfrastructuurleveranciers worden niet of slechts summier in het onderzoek meegenomen.

Het belang van het onderzoek is drieledig:

[3] Zie art. 11 eerste lid Kw

1. inzicht verkrijgen in de risico's en aansprakelijkheden van de huidige situatie en de toekomstige (digitale) situatie van het aanleveren en verwerken van de notariële akte bij het Kadaster.
2. overzicht verkrijgen van ervaringen met EDI buiten de Kadasterbranche, met de bijbehorende aansprakelijkheidsanalyse, en daardoor
3. uitzicht op het elektronisch aanleveren en verwerken van de notariële akte met een juridisch gefundeerde en duidelijke aansprakelijkheidsverdeling.

Uitwerking van de probleemstelling

De onderstaande onderzoeksvragen geven gezamenlijk het antwoord op de hoofdvraag. De vragen 1, 2, 3, 4 en 5 corresponderen respectievelijk met de hoofdstukken 2, 3, 4 en 5, 6 en 7.

1. *Wat is EDI in het algemeen, welke (technische) elementen kunnen in het algemeen een rol spelen bij de betrouwbaarheid van de uitwisseling en opslag van gegevens en welke voor- en nadelen kan EDI opleveren voor het Kadaster en notariaat in het algemeen?*
   De achtergrond van de probleemstelling wordt hier besproken. In eerste instantie zal in het algemeen ingegaan worden op EDI. Daarbij wordt aandacht besteed aan de algemene voordelen en knelpunten van EDI. De in de EDI-wereld gebruikelijke vorm om de aansprakelijkheid vast te leggen (het Interchange Agreement) wordt behandeld en de technische mogelijkheden, die de betrouwbaarheid van de communicatie en registratie kunnen vergroten, besproken. Tenslotte komen verschillende vormen van Trusted Third Parties (TTP's) aan de orde.

2. *Hoe ziet het analoog aanleveren en verwerken van de notariële akte bij het Kadaster eruit, hoe is de aansprakelijkheid verdeeld en hoe is deze verdeling juridisch vormgegeven?*
   Het analoge aanlever- en verwerkproces wordt besproken en de daarbij betrokken partijen. Aan de hand van het aanleverproces worden de mogelijke fouten bij de aanlevering en verwerking van de notariële akte bij het Kadaster geïnventariseerd en geanalyseerd. Tenslotte zal de aansprakelijkheidsverdeling in de analoge situatie worden gegeven.

3. *Welke (juridische) problemen geeft het aanbieden bij het Kadaster van een digitaal equivalent van de notariële akte en hoe kunnen deze problemen technisch en/ of juridisch worden opgelost?*
   De invoering van EDI bij het Kadaster kan niet zomaar worden gedaan. De problemen die moeten worden opgelost voordat EDI operationeel kan worden, worden beschreven en oplossingen hoe om te gaan met de problemen worden aangedragen. De oplossingen zullen zowel juridisch als technisch van aard zijn. Tevens zal worden ingegaan op de mogelijke rol van een TTP in het aanleverproces.

4. *Hoe ziet het beoogde elektronisch aanleveren en verwerken van de notariële akte bij het Kadaster eruit, welke partijen zijn aansprakelijk voor welke fouten op welk moment van het proces en waaruit blijkt dit?*
   Het project elektronisch aanleveren is een deel van het traject dat moet leiden tot het Kadastraal Vastgoedinformatiesysteem (KVS). Het aanleveren en verwerken van de notariële akte zoals dit de projectgroep Elan voor ogen staat wordt beschreven en geanalyseerd. De (theoretische) foutenbronnen, mogelijke foutendetecties en de toekomstige aansprakelijkheidsverdeling zullen worden weergegeven.

5. *Welke branche waar EDI reeds operationeel is, is vergelijkbaar met KANO en hoe is daar de aansprakelijkheid verdeeld?*
   Er zijn reeds bedrijfssectoren overgegaan op het gebruik van EDI. Daar waar vroeger papieren contracten gebruikelijk waren, is dit vervangen door EDI. Op basis van criteria die kenmerkend zijn voor het elektronisch aanleveren bij het Kadaster zijn twee branches geselecteerd die reeds ervaring met EDI hebben. Van deze branches wordt een beschrijving van de situatie voor wat betreft het digitale proces, de technische eisen aan het stuk en de wijze waarop aansprakelijkheidsverdeling juridisch is geregeld, gegeven. Ook wordt aandacht besteed aan de manier waarop men met conflicten omtrent EDI omgaat.

Werkwijze

De onderzoeksmethode is tweeledig. Deze bestaat ten eerste uit een literatuurstudie over EDI en voor EDI kenmerkende elementen als het Interchange Agreement en Trusted Third Parties. De literatuurstudie is ook verricht voor de beschrijving van het aanleverproces van de notariële akte bij het Kadaster en voor de beschrijving van de processen bij de branches vergelijkbaar met het Kadaster en notariaat. Op basis van de literatuurstudie over EDI en het analoge aanleverproces bij het Kadaster is onderzocht of EDI zonder problemen voor de aanbieding van het digitale equivalent kan worden gebruikt. Als daar aanleiding toe bestaat, zijn oplossingen aangedragen die ervoor moeten zorgen dat de invoering van EDI bij het aanbieden van het digitale equivalent mogelijk wordt. Deze oplossingen zijn zowel technologisch als juridisch van aard.
Verder is door interviews met mensen die direct betrokken zijn bij de ontwikkeling van het elektronisch aanleveren het digitale proces zoals het Kadaster dat voor ogen staat, beschreven en geanalyseerd.
Na een selectie op basis van de literatuur is, door middel van een interview met een medewerker van een vergelijkbare branche, beoordeeld of de branche inderdaad vergelijkbaar is. Op basis van een vervolg-interview is het digitale proces bij de vergelijkbare branche beschreven en geanalyseerd.
Op basis van de analyse van het huidige proces van aanleveren bij het Kadaster, van de geconstateerde problemen, de aangedragen oplossingen en de invulling van het proces zoals het KANO voor ogen staat, is gekomen tot de conclusies en aanbevelingen.

2. Electronic Data Interchange

2.1 Inleiding

De laatste jaren zijn EDI-technieken sterk in opkomst. Met name de logistieke sector kent vele toepassingen. Complete papierstromen worden hierbij vervangen door elektronische gegevensuitwisseling met behulp van EDI-technieken. Ook tussen het Kadaster en notariaat kunnen omvangrijke gegevens- en papierstromen worden onderscheiden. Met name bij de aanlevering van de notariële akte door de notaris aan het Kadaster speelt papier nog steeds een grote rol.

In dit hoofdstuk wordt een deel van de achtergrond van de probleemstelling uit hoofdstuk 1 beschreven. Naast de voor- en nadelen die EDI voor een organisatie in het algemeen kan opleveren wordt aandacht besteed aan de in de EDI-wereld gebruikelijke vorm om de gemaakte afspraken vast te leggen: het Interchange Agreement. Tenslotte zullen de verschillende functies van Trusted Third Parties worden behandeld.

2.2 Electronic Data Interchange in het algemeen

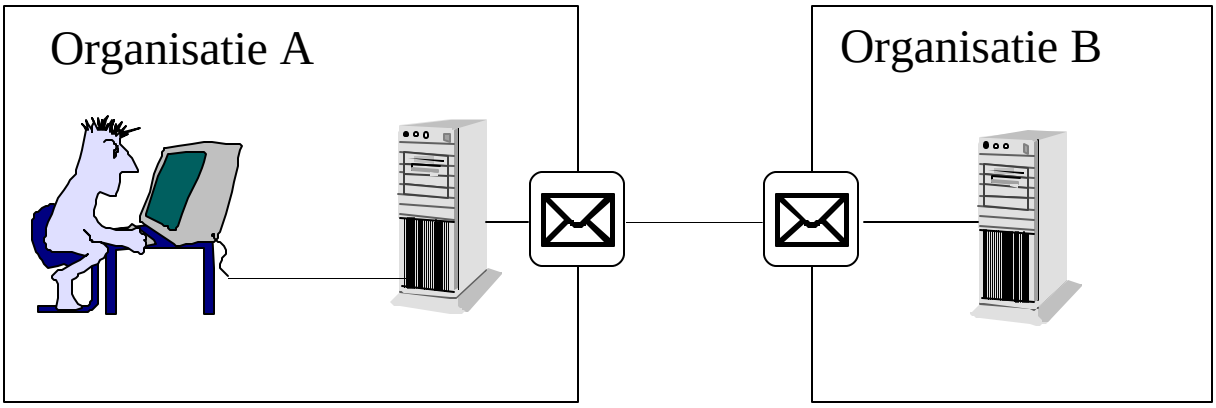
EDI staat voor Electronic Data Interchange. Letterlijk vertaald betekent EDI dus: elektronische gegevensuitwisseling. Een gangbare definitie van EDI luidt[4]:

EDI is de geautomatiseerde, elektronische uitwisseling van gestructureerde en genormeerde berichten tussen computers van verschillende organisaties.

In de praktijk kan EDI als volgt worden omschreven[5]:
EDI is een vorm van berichtenuitwisseling tussen bedrijven, waarbij door een computerprogramma van organisatie A een bericht wordt samengesteld, dat niet wordt afgedrukt, maar door vertaalprogramma wordt omgezet in een standaardvorm en standaardtaal. Zo'n standaardbericht wordt vervolgens door een communicatieprogramma geschikt gemaakt om via de telefoonlijn te worden verzonden naar de computer van organisatie B. Bij organisatie B worden de ontvangen signalen door het communicatieprogramma weer omgebouwd tot het standaardbericht in de standaardvorm en de standaardtaal. Dit bericht wordt vervolgens door het vertaalprogramma weer omgezet in een vorm die door de computers van organisatie B kan worden verwerkt.
De computers (toepassingsprogramma's) van organisaties A en B communiceren dus rechtstreeks. Ze vervangen de werkwijze van afdrukken, versturen en invoeren van gegevens.

Naast de begrippen uit de definitie van EDI, spelen er bij EDI nog een viertal begrippen een centrale rol: integriteit, authenticiteit, authenticatie (=authentificatie) en identificatie. Integriteit van het bericht wil zeggen: de inhoud van een bericht is gelijk en volledig gebleven tijdens verzending, transport en verwerking. De authenticiteit van een bericht is te beschrijven als: de zekerheid ten aanzien van de echtheid van een bericht[6]. Authenticatie is de controle op de authenticiteit en identificatie tenslotte kan worden beschreven als: de verificatie van de herkomst van het bericht[7].

[4] Vlist, P. van der, e.a., 1992.
[5] Zie figuur 2.1
[6] Schut en Wiersema, 1997.
[7] Esch, R.E. van, en C. Prins e.a., 1993.



Figuur 2.1 Electronic Data Interchange

2.2.1 Algemene voordelen van EDI

EDI biedt de gebruikers een groot aantal voordelen. De meeste voordelen hangen samen met de nadelen die papier als gegevensdrager heeft. Het transport van papier is traag[8] en er zijn veel bewerkingen nodig voor de verzending van papieren documenten; printen, in de envelop, postzegel, in de brievenbus stoppen en bij de ontvanger het omgekeerde proces: uit de brievenbus halen, de envelop openen en het document in de computer zetten. EDI vereist veel minder bewerkingen dan papier. Minder bewerkingen kunnen door minder mensen worden gedaan. Minder mensen maken minder fouten. Dit zorgt ervoor dat ook minder tijd aan het herstellen van fouten wordt besteed. Minder fouten zorgen voor een betere kwaliteit van het product.
Daarnaast kunnen EDI-berichten sneller worden verwerkt dan papieren berichten. Dit leidt er onder andere toe dat organisaties kleinere voorraden kunnen aanhouden. De snellere verwerking kan ook andere voordelen opleveren. Gedacht kan worden aan de mogelijkheid om betaalopdrachten op een later tijdstip bij de bank aan te leveren of de snellere informatie-uitwisseling tussen autoriteiten, die belast zijn met de opsporing van strafbare feiten.
Door EDI is het mogelijk om nieuwe service en/ of diensten te verlenen. Het geven van klantkaartgerichte aanbiedingen door supermarkten bijvoorbeeld of het 24 uur per dag openstellen van een digitaal overheidsloket.
Tenslotte is het door de uniforme standaards van EDI mogelijk om databanken van verschillende organisaties te koppelen. Dit kan leiden tot het ontdekken van inconsistente gegevens van (rechts-) personen die mogelijk het gevolg zijn van frauduleus handelen van deze (rechts-)personen.

2.2.2 Algemene problemen van EDI[9]

De problemen die EDI met zich mee kan brengen zijn vierledig:

1. Juridische problemen
2. Beveiligingsproblemen
3. Technische problemen
4. Overige problemen

[8] Internetjargon spreekt van slakkenpost.
[9] Zie ook: Net, D.J. van der, 1994.

Juridische problemen

Het kenmerk van digitale bestanden in het algemeen en EDI in het bijzonder is het niet meer aanwezig zijn van papier. Er is sprake van een nieuwe gegevensdrager. De huidige wetgeving in Nederland maar ook daarbuiten hanteert voor gegevensdragers als uitgangspunt het papier.
De authenticiteit van (de inhoud van) een gegevensdrager wordt bepaald op basis van kenmerken die aan het papier zijn gegeven. Het vereiste van een ondertekend geschrift of bepalingen van gelijke strekking is bijvoorbeeld veelvoorkomend.
Omdat de wetgeving uitgaat van papier als gegevensdrager en daar concrete invulling aan heeft gegeven, is het ten eerste onzeker of er andere dan papieren gegevensdragers geoorloofd zijn en ten tweede of een digitale handtekening eenzelfde waarde kan vertegenwoordigen als een analoge handtekening. De juridische status van zowel andere gegevensdragers dan papier, als van de digitale handtekening is onzeker.
De juridische onzekerheid of aan de digitale handtekening dezelfde authenticiteit kan worden verbonden als aan de analoge hangt af van de vraag waarom de wetgever de vormvereisten heeft geëist, wat de functies en de eigenschappen van de vormvereisten zijn en of de elektronische handtekening deze functies en eigenschappen kan vervullen[10]. Als dit niet zo is dan zal aanpassing van wetten noodzakelijk zijn om de digitale handtekening te kunnen gebruiken.
EDI-berichten kunnen niet als authentieke akten gekwalificeerd worden[11]. Zij zijn (initieel) niet vastgelegd op papier en niet voorzien van handtekeningen in de letterlijke zin van het woord. EDI-berichten, ook die met toevoeging van een integriteitsberekening en met waarborgen van identiteit en authenticiteit door middel van een elektronische handtekening, hebben dan ook (nog) vrije bewijskracht. De rechter bepaalt de waarde. Partijen dienen aan te tonen dat voldoende maatregelen tijdens verzending en bij ontvangst zijn getroffen om identiteit, authenticiteit en integriteit te kunnen waarborgen.

Wetten die het onmogelijk maken een ander medium dan papier te gebruiken moeten worden aangepast om van EDI gebruik te kunnen maken. Een uitspraak van de Hoge Raad (of andere rechterlijke instanties) kan een andere optie zijn om de dwingende rechtskracht van akten ook bij meer moderne werkwijzen (= digitaal bestand en elektronische handtekening zorgt voor authenticiteit) te continueren of definitief niet te accepteren.
In vele wetten is inmiddels het expliciete vereiste van papier vervangen door de terminologie bescheiden en andere gegevensdragers. Voorbeelden zijn het Burgerlijk Wetboek deel 2 (artt. 10.3, 24.1, 394.6), de Algemene wet inzake rijksbelastingen (o.a. artt. 8 en 52), de Archiefwet 1995, het Wetboek van Koophandel (o.a. art.8) en de Douanewet (o.a. art. 8)[12].
In de Algemene wet inzake rijksbelastingen, de Communautaire douanewet en het Handelsregisterbesluit 1996 (Stb. 417) is daarnaast een eerste stap gezet op het gebied van de vervanging van de analoge handtekening. De Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994 (Stcrt. 252) staat een persoonlijke code toe als identificatie van de aangever en bevestiging van de waarheid van de inhoud van het elektronische belastingformulier[13] en de Communautaire douanewet laat de Douane vrij in de keuze van een techniek die de handtekening kan vervangen[14]. Het Handelsregisterbesluit 1996 tenslotte stelt dat bij de persoonlijke kenmerken van een persoon ook de elektronische handtekening kan worden gedeponeerd[15].
Het verdient aanbeveling om ter overtuiging van de rechter voldoende maatregelen te treffen om (voor bepaalde of onbepaalde tijd) identiteit, authenticiteit en integriteit van de berichten te waarborgen. Het Interchange Agreement is één van de middelen waarmee dit kan.

[10] Huydecoper en Van Esch, 1997.
[11] Esch, R.E. van, en C. Prins e.a., 1993.
[12] Zie ook Staatsblad 598
[13] Art. 20 vijfde lid Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994
[14] Artt. 4ter en 4bis toepassingsverordening Communautaire douanewet
[15] Art. 1 derde lid Handelsregisterbesluit 1996

Beveiligingsproblemen

Met EDI komt de communicatie tussen organisaties via een (telefoon-, kabel-, glasvezel-, ISDN-) lijn tot stand. Onbevoegden kunnen via de communicatielijn berichten aftappen en zelfs bij de organisaties elektronisch inbreken. Verminking, verlies of ongewenste inzage van het bericht en/ of ongeautoriseerd gebruik van het systeem van organisaties kunnen tot grote schade leiden. De beveiliging van de berichtgeving is daarom vaak gewenst.
De meeste organisaties die gebruik van EDI (willen) maken, kunnen in eerste instantie zelf beslissen of de (communicatie van de) gegevens beveiligd moeten worden en op welk niveau dit gewenst is. Daarnaast zijn er een aantal wetten die impliciet of expliciet vereisen dat de communicatie beveiligd moet geschieden[16]. De Wet computercriminaliteit (Stb. 1993, 33) stelt dat overtreding van het verbod van computervredebreuk alleen strafbaar is als daarbij een beveiliging wordt doorbroken (art 138a WvS). Artikel 350b Wetboek van strafrecht bepaalt dat strafbaar is degene, aan wiens schuld te wijten is dat gegevensverkeer wordt verstoord c.q. een virus wordt verspreid. Tenslotte bevat de Wet computercriminaliteit een bepaling die is opgenomen in het Burgerlijk Wetboek (art 2:393 vierde lid BW), waarin aan de accountant in het kader van de controle van de jaarrekening van een onderneming de plicht wordt opgelegd melding te maken “van zijn bevindingen met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking”.
De vereiste graad van beveiliging is doorgaans afhankelijk van de omstandigheden van het geval. In het Wetboek van strafrecht (art138a WvS) wordt de eis van minimale beveiliging gesteld. Artikel 8 van de Wet persoonsregistraties (WPR, Stb. 665) spreekt van “de nodige voorzieningen van technische en organisatorische aard” dan wel van “passende maatregelen”. Dit betekent dat “state of the art” bepalend zal zijn, waarbij de kosten van beveiliging en de beschikbaarheid van beveiligingsmiddelen een rol zullen spelen[17]. Professor Franken geeft aan de eisen van de WPR het predikaat adequate beveiliging: er heeft een afweging plaatsgevonden tussen het te beveiligen belang en de genomen maatregelen[18].
Technisch zijn er vele mogelijkheden die kunnen zorgen voor de beveiliging van gegevens. In de paragraaf over het Interchange Agreement zullen verschillende beveiligingsmethoden worden besproken.

Technische problemen

Met EDI levert men zich grotendeels over aan de techniek: programmatuur, apparatuur, opslagmedia en telecommunicatieverbindingen. Dit betekent dat de beheersbaarheid van processen complexer wordt, maar ook dat de kans op technische storingen toeneemt. Het technisch disfunctioneren van het systeem, het standaardiseren van de berichten tussen de organisaties en de keuze van apparatuur, software en communicatienetwerk vormen gezamenlijk de technische problemen van EDI.

Overige problemen

De problemen die zich niet laten indelen in één van de bovengenoemde categorieën zijn de overige problemen. Deze hebben betrekking op de automatiseringskosten en de sociale gevolgen van de invoering van EDI. Als laatste kan overmacht organisaties schade bezorgen.

Automatiseringskosten
Wanneer men gebruik wil maken van EDI moeten ten eerste de uit te wisselen gegevens digitaal aanwezig zijn. Ten tweede moet een EDI-omgeving binnen de organisatie worden gecreëerd. Er moet geschikte hard- en (EDI-) software worden aangeschaft of de bestaande worden aangepast. EDI-deskundigheid (helpdesk) moet worden aangesteld en gebruikers van het nieuwe systeem moeten ervaring met het nieuwe systeem krijgen.
Daarnaast zal de organisatie moeten worden aangepast. Dit kan inhouden dat de helpdesk moet worden uitgebreid en er controlerende organen moeten worden toegevoegd.

[16] Proceedings Digital Security, deuren en sleutels in de informatiewereld, symposium Elektrotechniek TU Delft, 13 mei 1997.
[17] De wet van Moore stelt dat de rekenkracht van een computer, in een gegeven prijsklasse, iedere 18 maanden verdubbelt.
[18] Franken, H., 1993.

Sociale problemen
Alle vormen van automatisering hebben als doel kostenbesparing. En daar wordt meestal mee bedoeld dure mensen vervangen door goedkope computers. Het invoeren van EDI leidt tot een verlies van banen bij de organisaties die met EDI willen communiceren. EDI zal voornamelijk de mensen die het uitvoerende werk van een organisatie doen kunnen vervangen. Omdat er mensen door EDI worden vervangen en dus overbodig zullen worden, kan het besluit tot invoering van EDI leiden tot sociale onrust binnen de organisatie.
De invoering van EDI levert ook banen op. Het beheer van de systemen en de uitbreiding van de helpdesk zijn hier voorbeelden van.

Overmacht
Een probleem van EDI is de grote afhankelijkheid van een snel transport; vertragingen leiden tot problemen. Bijvoorbeeld een staking bij de groothandel die de producten levert aan een supermarkt of een wegblokkade door vrachtwagenchauffeurs kunnen leiden tot een just in time voorraadtekort.
Ook stroomuitval of anderszins vertragingen in de communicatie veroorzaakt door overmacht kunnen leiden tot schade bij bedrijven waar niets aan kan worden gedaan.

2.3 Interchange Agreement[19] [20]

Voor veel juridische regels is nog niet duidelijk hoe deze door de rechter zullen worden geïnterpreteerd; er is sprake van rechtsonzekerheid als het om EDI gaat. Bedrijven die tot elektronische berichtenuitwisseling willen overgaan, kunnen een grotere mate van juridische zekerheid scheppen door met de partijen waarmee gegevens zullen worden uitgewisseld contractuele voorzieningen te treffen voor het gebruik van EDI. Deze contractuele voorziening wordt Interchange Agreement (verder IA) genoemd. In een IA worden drie delen onderscheiden: juridische bepalingen, de technische bijlage en de scenariobeschrijving. De juridische bepalingen en de technische bijlage worden hier behandeld. De scenariobeschrijving is in het kader van het onderzoek niet van belang en zal niet worden besproken.

2.3.1 Juridische bepalingen

In de juridische bepalingen wordt overeengekomen om welke informatie-uitwisseling het gaat, het tijdstip van de totstandkoming van de overeenkomst, hoe vaak er uitgewisseld wordt en wat voor de informatie wordt betaald. Ook de onderstaande aspecten kunnen worden geregeld in de juridische bepalingen van een IA.

Identificatie van de afzender en ontvanger
Hoe bepaal je dat een bericht afkomstig is van degene die zegt dat hij de afzender is. Met andere woorden hoe bewijs je dat men de persoon of organisatie is, voor wie men zich uitgeeft? Technische mogelijkheden zijn voorhanden om de afzender en ontvanger te identificeren. Deze mogelijkheden worden in de technische bijlage toegelicht.

Ontvangstbevestiging en inhoudsbevestiging
Wanneer er een bericht verstuurd is, kan de verzender in een IA een bevestiging verlangen dat het bericht is aangekomen bij de andere organisatie. Deze stuurt dan een ontvangstbevestiging en/ of inhoudsbevestiging. Uit veiligheidsoverwegingen kan er een bepaalde tijdsduur worden vastgesteld waarbinnen een bericht bij A en/ of een bevestiging bij B moet zijn ontvangen.
De inhoud van het bericht moet aan eisen voldoen die in de technische bijlage verder worden geregeld. Een controle voor de integriteit van het bericht kan met het bepalen van de hashwaarde[21]. Het gebruik van

[19] Graaf, F. de, 1990.
[20] Esch, R.E., C. Prins e.a., 1993.

deze techniek zal ook in de technische bijlage worden toegelicht. Het bepalen van de hashwaarde kan leiden tot het constateren van fouten. In de technische bijlage wordt geregeld hoe een verloren, afgedwaald of verminkt bericht wordt geconstateerd. Een niet-integer en/ of niet-authentiek bericht wordt in het algemeen niet door de ontvangende organisatie geaccepteerd en zal de verzender nogmaals moeten sturen.

Verwerken, registreren en opslaan van het EDI-bericht
Het kan voor een organisatie van belang zijn dat het gestuurde bericht direct na ontvangst wordt verwerkt. Een bestelling van een supermarkt bij zijn groothandel bijvoorbeeld moet ervoor zorgen dat na het ontvangen van het bericht de opdracht onmiddellijk wordt uitgevoerd. Organisaties verplichten zich dan het EDI-bericht te verwerken binnen een bepaalde tijdslimiet.
Het registreren van het bericht en het opslaan dient ook door beide organisaties te gebeuren, eventueel door een tussenpartij ondersteund. Ten aanzien van de bewaarplicht legt het Wetboek van Koophandel een ieder die een bedrijf uitoefent een boekhoudingsverplichting op, welke gedurende tien jaar bewaard moet worden. De bewaring van berichten zal moeten geschieden conform de eisen die de wet hieraan stelt om leesbaarheid van de registratie binnen een redelijke termijn te waarborgen.

Beveiliging van EDI-berichten
De diverse wetten dwingt organisaties hun computersystemen en bestanden te beveiligen tegen misbruik (door derden). Organisaties hebben er zelf ook belang bij dat vertrouwelijke informatie niet door onbevoegden kan worden gelezen. Organisaties beslissen zelf over de mate van beveiliging en de wijze waarop beveiligd wordt[22]. De beveiligingsmethoden en de verificatie van de herkomst van een bericht worden in de technische bijlage bij de IA nader gespecificeerd.

Aansprakelijkheid
Gebruikers kunnen in de IA de aansprakelijkheid voor schade ten gevolge van bepaalde gebeurtenissen of voor bepaalde vormen van schade beperken of uitsluiten.
Daarnaast kunnen zij het aansprakelijkheidsdomein inperken door contractueel bepaalde tekortkoming veroorzakende omstandigheden als overmacht aan te duiden, die zonder deze contractuele regeling zouden leiden tot een toerekenbare tekortkoming van de schuldenaar.
Bij fouten in of van berichtgeving die kunnen leiden tot schade kan gedacht worden aan dubbele berichten, verdwaalde berichten, verminkte berichten en/ of verloren berichten.

Bewijs
Als er over de bewijskracht van bepaalde stukken of handelingen een overeenkomst wordt gesloten moet conform art. 6:246, tweede lid BW worden gehandeld. Dit betekent dat de overeenkomst gegeven de omstandigheden niet in strijd met de redelijkheid en billijkheid mag zijn. Bij de beoordeling van de redelijkheid en billijkheid zal de rechter rekening houden met de maatregelen, die partijen hebben getroffen om een juiste registratie te bevorderen en de registratie te beveiligen tegen manipulatie. In de bewijsbepaling van de IA kunnen verschillende bewijsrechtelijke onderwerpen worden opgenomen.
Ten eerste kunnen partijen de bewijslast zo verdelen dat één van de partijen een bepaald feit zal moeten bewijzen, indien dit door de wederpartij wordt betwist.
Ten tweede kunnen zij overeenkomen dat de elektronische registratie van een tussen hen uitgewisseld EDI-bericht toelaatbaar is als bewijsmiddel.
Ten derde kunnen partijen bepalen dat de elektronische registratie van één van hen of van een onafhankelijke derde dwingend bewijs oplevert. De registratie van de TTP wijst dan de ‘schuldige’ partij aan[23].

[21] De hashwaarde is het controlegetal, dat wordt verkregen volgens een bepaald algoritme. De hashwaarde is uniek voor het betreffende gegevensbestand. Welk algoritme gebruikt wordt, kan door de organisaties worden afgesproken.
[22] Medewerkers van de eigen organisatie moeten hierbij niet worden onderschat. Uit onderzoek van Datapro blijkt dat 57% van alle inbraken in het bedrijfssysteem door eigen personeel werd gepleegd; ‘Axtent verklaart hackers de oorlog’, Automatiseringsgids vrijdag 13 februari 1998.
[23] Zie voor vormen van Trusted Third Parties paragraaf 2.4

Conflictenbeslechting
Bij het uitwisselen van gegevens via EDI kunnen op veel momenten fouten ontstaan. In een IA kan worden geregeld hoe te handelen bij de beslechting van geschillen.
Bij de beslechting van geschillen kan onderscheid gemaakt worden tussen informele en formele beslechting. Aan informele geschillenoplossing zullen partijen zelf vorm geven. Voor de formele geschillenoplossing kunnen gebruikers van EDI in de IA een regeling opnemen. In deze regeling kunnen zij bepalen aan welke rechter zij eventuele geschillen voorleggen. Ook kunnen zij bepalen dat geschillen worden voorgelegd aan arbiters. Een instantie die de arbitragerol zou kunnen vervullen is de TTP. Bij het ontbreken van een geschillenoplossingsregeling gelden in principe de wettelijke bewijsregels.
Een geschillenoplossing door de rechter heeft een aantal nadelen. De rechter heeft meestal niet de benodigde kennis van de informatietechnologie en zal daar één of meer deskundigen voor zoeken. Terwijl de organisaties in het ongewisse verkeren over de mogelijke uitkomst, zoekt de rechter een deskundige. Dit kan oplopen tot twee maanden zoektijd. Als dan een deskundige is gevonden zal zijn deskundigheid door specialisten van de betrokken partijen op de proef worden gesteld. Kortom een geschillenoplossing door de rechter kost veel tijd, is duur en kan zorgen voor ongewenste publiciteit.

Wetgeving
Het kan bij EDI-toepassingen gaan om internationale gegevenstransport. De wettelijke beperkingen voor gegevenstransport kunnen per land verschillen. In Nederland is het de wet op de Persoonsregistraties (WPR) die het transport aan beperkingen onderhevig maakt. De beperkingen hebben betrekking op de geheimhouding van persoonsgegevens.
Op korte termijn wordt de WPR vervangen door de Wet bescherming persoonsgegevens (WBP). Dit wetsontwerp heeft een breder toepassingsgebied dan de WPR en is strenger van aard.

2.3.2 Technische bijlage

In de technische bijlage wordt uitvoering gegeven aan de juridische bepalingen. De nadruk ligt op de technische realisering van de juridische bepalingen. Over de volgende onderdelen kan een technische bijlage handelen:

Eisen aan het EDI-systeem
Voor de toepassing van EDI moeten de systemen van de organisaties op elkaar worden afgestemd. De organisaties moeten zorg dragen voor geschikte hardware, randapparatuur en voor (EDI-)software die aan de eisen van de organisaties voldoet. Functionele eisen, beveiligingseisen en eisen met betrekking tot de keuze van het opslagmedium zullen de invulling van de apparatuur en software bepalen.
Daarnaast zal een keuze moeten worden gemaakt voor een telecommunicatieleverancier.

Structuur van de berichtgeving
EDI vereist eenduidigheid: in betekenis van het bericht, in inhoud van het bericht en in interpretatie van het bericht door de computersystemen. In welke structuur wordt het bericht verstuurd? De vorm, inhoud, identificatie en interpretatie van de berichten wordt door de computers vastgelegd. De meeste vormvereisten zijn vastgelegd in de internationale EDI-standaard EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) van de Internationale Organisation for Standaardisation (ISO 9735) en van de Working Party 4 van de Verenigde Naties in Genève. EDIFACT omvat alle internationaal opgestelde en overeengekomen regels, aanbevelingen, normen en gegevensverzamelingen voor het gestructureerde elektronische berichtenverkeer tussen autonome informatiesystemen. Voor de identificatie van zender en ontvanger kan men zich houden aan de UNCID (Uniform Rules of Conduct for Interchange of Trade Data by teletransmission).

Beveiliging
Het bericht kan op verschillende manieren worden beveiligd. In het algemeen geldt hoe meer beveiligingsmaatregelen hoe trager de berichtgeving en dus hoe hoger de kosten. En hoe meer gebruikers toegang tot het systeem krijgen hoe onveiliger het systeem. De beveiliging kan worden

gescheiden in de toelating tot het systeem (autorisatie), het onleesbaar maken van de berichten, het kunnen controleren van de integriteit en authenticiteit van het bericht en het constateren van het verlies van een bericht. Omdat sommige documenten slechts juridische waarde hebben wanneer ze integer en authentiek zijn, worden de integriteit en de authenticiteit van berichten apart behandeld.

Autorisatie voor het systeem
De meest simpele beveiliging is de kantoor-bureau-computer login-code gecombineerd met een wachtwoord. De meeste organisaties stellen deze beveiliging beschikbaar of dwingen medewerkers ertoe van de beveiliging gebruik te maken. Kritiek is het achterlaten van de computer zonder dat uitgelogd wordt of de screensaver met wachtwoord wordt aangeroepen. Op dat moment kunnen onbevoegden gebruik makend van de autorisatie van de ingelogde persoon toegang krijgen tot informatie die vertrouwelijk kan zijn en kunnen er op naam van de ingelogde persoon berichten worden verstuurd naar de wederpartij.
Naast gebruik te maken van de zorgeloze medewerker kan het wachtwoord ook gekraakt worden. Niet zo moeilijk als het wachtwoord op het toetsenbord staat vermeld of anderszins eenvoudig is te kraken (naam van de man/ vrouw/ kinderen/ idool etc.).
Meer geavanceerd is de beveiliging met behulp van biometrische kenmerken. Een geautoriseerde medewerker meldt zich bij de computer met bijvoorbeeld zijn vinger en krijgt toegang tot het systeem. Vingeridentificatie, DNA-herkenning, irisherkenning[24] en stemherkenning zijn methoden waarbij het mogelijk kraken van de code niet zozeer meer een risico vormt als wel de persoon met toegang tot een bepaald systeem. De vinger en de iris van bijvoorbeeld ‘de directeur’ kan veel geld waard zijn. Daarnaast zijn er mensen als Robert Paul die de meest zeldzame stemmen kunnen nadoen en op deze wijze zich toegang tot een systeem kunnen verschaffen. Een combinatie van biometrische kenmerken zorgt voor een (voor een ieder) veilige manier van het autoriseren van personen[25].

Encryptie (versleuteling)
Voor veel toepassingen is alleen de autorisatiebeveiliging niet toereikend. Het kwaad geschiedt als het bericht op het telecommunicatienet is gekomen. Daar wordt het door een hacker[26] afgetapt en misbruikt. Het bericht zal tijdens het transport over telecommunicatienetwerken moeten worden beveiligd. Dit kan door encryptie (versleuteling) op het bericht toe te passen.
De versleuteling van een bericht zorgt ervoor dat een bericht onleesbaar wordt. Dit kan door de oorspronkelijke tekens te vervangen door andere tekens (substitutie) of je laat de oorspronkelijke tekens voor wat ze zijn en verandert ze alleen van plaats (transpositie). Er zijn twee soorten van encryptietechnieken: de symmetrische versleuteling en de asymmetrische.
Symmetrische encryptie wil zeggen dat beide partijen beschikken over de geheime sleutel voor het vercijferen respectievelijk ontcijferen van het bericht[27]. Een bekend symmetrisch systeem is de Data Encryption Standard (DES)[28].

[24] Een Japanse bank heeft de irisherkenning met videocamera’s getest en is tot de conclusie gekomen dat hooguit 1 op de 100.000 keer een verkeerde identificatie wordt gemaakt; ‘Oki beproeft identificatie via oog’, Automatiseringsgids vrijdag 30 januari 1998.
[25] De ontwikkeling van het klonen kan er echter toe leiden dat twee exact dezelfde mensen bestaan ook qua biometrische kenmerken.
[26] Een hacker is een persoon of organisatie die wederrechtelijk toegang tot eens anders computersysteem verkrijgt en daar gegevens inziet, kopieert, wijzigt of laat verdwijnen. Het systeem wordt dan ‘gekraakt’.
[27] zie figuur 2.2
[28] DES is ook bekend onder naam Data Encryption Algorithm kortweg DEA.

Organisatie A

Organisatie B

Figuur 2.2 Symmetrische encryptieF4 9.crypti78tie BEie BEiej rg /FRG BT 2999.5 518tiem 2999.5 4 12.l 265.5 4 12.l

Een combinatie van de sleuteltechnieken is ook mogelijk. Bijvoorbeeld het verzenden van het bericht met een symmetrische sleutel en de publieke sleutel van de (beoogde) ontvanger.

De asymmetrische encryptie heeft ten opzichte van de symmetrische encryptie een aantal voordelen en een nadeel.
Het grote voordeel van asymmetrische encryptie is dat het naast de versleutelfunctie ook een non-repudiation functie vervult[30]. De privésleutel kan immers alleen door de verzender worden gemaakt. Bij de symmetrische encryptie is deze functie niet aanwezig aangezien beide partijen over dezelfde sleutel beschikken. Men kan ten gunste van de eigen organisatie (of ten laste van de ander) misbruik van dit gegeven maken.
Daarnaast heeft asymmetrische encryptie als voordeel dat voor de communicatie met een willekeurige andere organisatie steeds gebruik kan worden gemaakt van hetzelfde sleutelpaar. Dit in tegenstelling tot de symmetrische encryptie waar voor elke communicatiepartner een unieke sleutel moet worden gemaakt.

Nadeel van asymmetrische versleuteling is dat het trager is dan symmetrische versleuteling.

Integriteit van het bericht
De integriteit van een bericht kan worden bepaald met behulp van een berekening van het gegevensbestand waarbij gebruik wordt gemaakt van een afgesproken algoritme[31]. Dit algoritme kan per afzender verschillend zijn.
De verschillende algoritmen zijn gebaseerd op hetzelfde principe: het genereren van een unieke waarde die gebaseerd is op de inhoud van het document[32]. De unieke waarde is zodanig gegenereerd dat het eenvoudig is om deze uit de data van het document te genereren maar dat het niet mogelijk is om uit de waarde de data van het document te genereren. De unieke waarde wordt de hashwaarde genoemd[33].
Het gebruik van de hashwaarde zorgt dus niet voor het onleesbaar maken van het bericht. Toepassing van de hashwaarde is een mogelijkheid om te controleren of de inhoud van een bericht tijdens het versturen hetzelfde is gebleven (integer zijn van het bericht).
De hashwaarde kan met het bericht worden meegestuurd en door de ontvangende partij worden gecontroleerd.

Identificatie van de afzender
De identificatie van de afzender is voor een ontvangende organisatie een doel op zich. Is de afzender bij de ontvanger bekend of is er sprake van een onbekende? Voor het identificeren van de afzender kan gebruik worden gemaakt van beveiligingsmethoden. Voorbeelden zijn asymmetrische encryptie, de hashwaarde en de call-back procedure.
Op welk niveau (organisatieniveau, afdelingsniveau of persoonsniveau) de afzender bekend is of moet zijn is organisatie-afhankelijk en bepalen de organisaties zelf.

Asymmetrische encryptie
De asymmetrische encryptie is onder het kopje beveiliging (encryptie) van subparagraaf 2.3.3 reeds beschreven. Ook de identificatiefunctie is daar beschreven.

Hashwaarde
Het berekenen van de hashwaarde kan op zeer verschillende manieren. Bijvoorbeeld door het optellen van alle numerieke velden. Om te garanderen dat 10009 niet verandert in 90001 zonder dat de hashwaarde verandert, kan de positie van het karakter in de berekening worden meegenomen. Het totaal kan worden vermenigvuldigd met een afgesproken uniek nummer van een partij, enz. enz.

[30] Non repudiation wil zeggen dat de verzending van het bericht niet door de afzender kan worden ontkend.
[31] De meest gebruikte algoritmen zijn naar oplopende betrouwbaarheid: Cyclic Redundancy Check (CRC), Modification Detection Code (MDC) en de Message Authentication Code (MAC).
[32] Http://rs6000.ibm.com/resource/aix_resource/pubs/redbooks/htmlbooks/sg244579.00/4579c27.html ; d.d. 10-02-1998
[33] In het Engels spreekt men van one-way hash.

Met andere woorden iedere partij kan gebruik maken van een unieke bepaling van de hashwaarde en kan als zodanig worden geïdentificeerd. A en B spreken het gebruik van een algoritme af. Partij A berekent de hashwaarde volgens algoritme AA dus deze hashwaarde moet er bij B bij gebruik van algoritme AA uitkomen.

Call-back procedure
Een andere methode om te bepalen wie de afzender van het bericht was, is de call-back procedure. Een bericht van organisatie A meldt zich bij organisatie B. B verbreekt de verbinding en zoekt op basis van zijn eigen adresbestand contact met de computer van A. Bevestigt A het bericht dan kan de verwerking van het bericht bij B beginnen.

2.4 Trusted Third Party

De Trusted Third Party (TTP) is een systeem dat in een netwerkomgeving als onafhankelijke partij tot taak heeft de authenticiteit en integriteit van het elektronische (handels)verkeer te garanderen. TTP diensten kunnen als volgt worden gekwalificeerd[34]:

Primaire diensten, ten behoeve van handelspartners om specifieke al dan niet cryptografische zakelijke transacties mogelijk te maken. Te denken valt aan key-management services, de vaststelling van de identiteit van partijen in het handelsverkeer, certificatie van sleutels, documenten en transacties, 'time stamping' (het certificeren van het tijdstip waarop een berichtenuitwisseling heeft plaatsgevonden), bewaring van berichten en broncodes, het leveren van een branche- of gebruikersgericht informatieregister.
Secundaire diensten, die niet als direct onderdeel van een transactie of het transactieproces, zoals auditing diensten, verschaffing van (al of niet versleuteld) bewijsmateriaal, bemiddeling en arbitrage, het opstellen van algemene voorwaarden met betrekking tot het dragen van risico's in het elektronische handelsverkeer.
Controle diensten, waarbij het dienstenniveau van andere TTP's wordt getoetst of waarbij andere TTP's worden geaccrediteerd (een soort 'super-TTP-service').

Onder een primaire dienst zou het bewaren van de publieke sleutel kunnen behoren. Op het eerste gezicht een merkwaardige taak, de sleutels zijn immers openbaar. Maar de integriteit en authenticiteit van digitaal opgeslagen informatie moet zijn gegarandeerd. Zo zal informatie die elektronisch is ondertekend om de authenticiteit en de integriteit te waarborgen ook na jaren nog verifieerbaar moeten zijn. Het is dan ook noodzakelijk dat de betreffende publieke sleutel even lang beschikbaar blijft als de opgeslagen informatie[35]. Daarnaast kan een TTP de private sleutels uitgeven en deze verifiëren.

De onafhankelijke vastlegging van 'originele' elektronische documenten valt onder de primaire dienst van een TTP. Deze taak van een TTP zorgt voor (meer) rechtszekerheid bij het elektronisch berichtenverkeer. Hoe de wetgever met de (fouten bij) elektronische berichtgeving omgaat is immers door gebrek aan jurisprudentie onduidelijk. Door het hebben van een onafhankelijke TTP die alle berichtgeving zowel van ontvanger als verzender verkrijgt en bewaart, staan de organisaties wettelijk sterker. De rechter heeft in de TTP een objectieve instantie met kennis van (elektronische) zaken (welke de rechter veelal niet heeft) die door de organisaties wordt vertrouwd. Voor beide organisaties is zo het vertrouwen in het systeem gewaarborgd.

[34] EU INFOSEC 93 Task S.01: Report to the commission of the EC for the User Requirements for Trusted Third Party Services, Reference S2101/01, October 1993. Geciteerd in: Franken, H., e.a., 'De notaris en het elektronisch rechtsverkeer', pagina 149 en 150.
[35] Koops, B-J, Computerrecht 1997/4.

Bij een (EDP-) audit van een proces wordt een proces regelmatig of continue getoetst aan de eisen die door de organisaties aan het proces worden gesteld. Voorbeelden van processen waar een audit op kan worden toegepast zijn conversieprocessen van digitale naar analoge media of andersom en verwerkingsprocessen van digitale bestanden.
Door de (EDP-) audit van een proces door een TTP zullen partijen (en ook de rechter) een groter vertrouwen in de betrouwbaarheid van het verloop van een (elektronisch) proces hebben.

Tenslotte kan de secundaire bemiddelings- en arbitragefunctie een imagoverlies van partijen en kostbare processen voorkomen. Voor het bewijs van een bepaald rechtsfeit kan men in een IA bepalen dat er een TTP wordt ingesteld, welke alle berichten verkrijgt. De TTP kan de taak tot bewaring van de berichtgeving krijgen en zal bij onenigheid over fouten als objectieve partij kunnen optreden met een doorslaggevende analyse van de berichtgeving. De registratie van de TTP heeft dan dwingende bewijskracht.

3. Analoog aanleveren en inschrijven van de notariële akte bij het Kadaster

3.1 Inleiding

Sinds de grondlegging van het Kadaster door Napoleon Bonaparte is er veel gebeurd met de inschrijving van de notariële akte in de openbare registers. De ontwikkeling der techniek heeft geleid tot andere werkwijzen. Dit geldt ook voor de aanlevering van de notariële akte. Door een blik in het verleden te werpen wordt duidelijk dat niet alleen de ontwikkeling der techniek verantwoordelijk is geweest voor een veranderende werkwijze van notaris en Kadaster.
Het huidige (analoge) aanleverproces wordt in dit hoofdstuk beschreven en geanalyseerd. Aan bod komen de betrokken partijen voor wat betreft hun aansprakelijkheid in het proces, de juridische vormgeving van de aansprakelijkheid en onvolkomenheden in het systeem. Besloten zal worden met conclusies omtrent het analoge aanleverproces.

3.2 Geschiedenis van de inschrijving van akten

3.2.1 Overschrijven wordt inschrijven

De eerste hypothecaire administratie waarbij enigszins van een uniforme vastlegging op landelijk niveau sprake was, dateert uit 1811. Deze administratie werd onder de Franse overheersing van de Staat der Nederlanden ingevoerd. Het Kadaster werd in 1832 ingevoerd en zorgde voor de standaardisatie van de aanduiding van rechtsobjecten.
Bij de invoering van het Burgerlijk Wetboek op 1 oktober 1838 werd uitsluitend aan gepubliceerde overdrachten en vestigingen van zakelijke rechten op onroerende goederen, inclusief de vestiging van hypotheek, rechtskracht toegekend. Overeenkomstig het bepaalde in artikel 30 van het Besluit Invoering Hypothecair Stelsel van 1 augustus 1828 (Stb. 52) zijn openbare registers ingesteld, waarin publicatie van de rechten plaatsvindt. Sinds 1839 zijn de hypothecaire administratie, het Kadaster (en de Scheepsbewijzen) één organisatie[36]. Onder het vanaf toen geldende recht omvatten de openbare registers voor onroerende goederen[37]:

1. een dagregister
2. een register voor de inschrijving van hypothecaire verbanden en voor de overschrijving van afschriften van processen-verbaal van inbeslagneming (hyp 3), en
3. een register voor de overschrijving van alle overige ter overschrijving ingeleverde stukken (hyp 4)

Het terminologische onderscheid tussen in- en overschrijving betrof enerzijds de vestiging van rechten van hypotheek (de daarop betrekking hebbende stukken werden ingeschreven) en anderzijds de overdracht van onroerende zaken en de vestiging van andere zakelijke rechten dan dat van hypotheek op onroerende zaken (deze werden overgeschreven). De inhoud van de stukken die werden aangeboden ter in- of overschrijving, werd met de pen respectievelijk ingeschreven en overgeschreven door bladschrijvers. Deze werden per regel betaald. De functie van het dagregister was vast te stellen op welke dag het stuk was aangeboden. Dit was nl. nodig omdat het daadwerkelijk in- of overschrijven met de pen eerst enige

[36] Dubbelt, W., 1979.
[37] Brouwer, 1995.

tijd na de dag van aanbieding kon plaatsvinden. Het Kadaster was aansprakelijk wanneer de overgeschreven akte niet overeenstemde met de akte van de notaris.
Door de wet van 28 februari 1947 werd om hoofdzakelijk economische redenen de overschrijving vervangen door de inschrijving van de akten: de notaris diende een afschrift van de akte alsmede een speciaal kadasterformulier aan te bieden met een verklaring van eensluidendheid[38]. De notaris werd vanaf toen verantwoordelijk gehouden voor de inhoudelijke juistheid van zowel afschrift als kadasterformulier[39].

Microfilm
Tot 1964 werden alle akten bewaard op duurzaam kadasterpapier. In de vestigingen van het Kadaster in het land begon zich echter een ruimtecapaciteitsprobleem voor te doen. Als reactie op deze praktische problemen werd in 1964 de wet van 1947 aangepast. De openbare registers mochten nu mechanische reproducties in dubbel zijn. Dit betekende dat men de akten op microfilm (in tweevoud) kon zetten en de oorspronkelijke akte in principe mocht vernietigen.

In de Memorie van Antwoord (ingezonden 16 juni 1964, zitting 1963-1964-**7271**) op het commentaar van de kamercommissie op het wetsontwerp verklaart de Staatssecretaris van Financiën het volgende:

'Het ontwerp is vooral geïnspireerd door de grote behoefte aan ruimtebesparing. Dit neemt niet weg dat door de nieuwe werkwijze noch de dienstverlening aan het publiek noch de rechtszekerheid zal verslechteren.
Het vormen van een schaduwarchief kan in verband met calamiteiten, waarvan de vernietiging van de openbare registers het gevolg zou zijn, de rechtszekerheid slechts bevorderen.'

Het raadplegen van het notariaat omtrent een in wezen interne reorganisatie van de hypotheekkantoren, waarvan het notariaat geen enkel nadeel zal ondervinden, achtte de Staatssecretaris niet nodig.
Wel was de Staatssecretaris van mening dat, zelfs in het geval dat tot vernietiging van de oorspronkelijke registers zou worden overgegaan, de onbeperkte leesbaarheid van de microfoto's en daarmede de rechtszekerheid voldoende was gewaarborgd. Hier werd gewezen op het schaduwarchief. Dit is het archief waar één van de 'microfilms in dubbel' centraal (thans in Lelystad bij het Computer Uitwijk Centrum) worden bewaard en waar alle mogelijke maatregelen worden getroffen om de films in goede staat te houden[40].

3.2.2 Evaluatie van de geschiedenis

De aanlevering van de notariële akte aan de openbare registers bij het Kadaster heeft zich ontwikkeld door hoofdzakelijk economische motieven. Daarbij heeft men gebruik kunnen maken van de ontwikkeling van diverse technieken. Het overschrijven door het Kadaster werd overtypen door de notaris. Het overtypen werd kopiëren en het kopiëren printen. En de openbare registers werden op microfilm gezet ondanks dat men niet exact de gevolgen van deze nieuwe techniek voor de rechtszekerheid kon overzien. Daarbij komt dat de aansprakelijkheid van het Kadaster voor de juistheid voor zover voortvloeiend uit het overschrijven van de inhoud van de akten in de openbare registers met het inschrijven is overgegaan naar het notariaat. Deze besluiten werden eenzijdig door de regering genomen.

Door de verzelfstandiging van het Kadaster is de invloed van de Staat ingeperkt en is de positie van het Kadaster in vergelijking tot 1947 en 1964 ten opzichte van het notariaat veranderd. Kon de Staatssecretaris in 1964 nog zeggen dat het notariaat niets met een mediumverandering van doen had,

[38] In de verklaring van eensluidendheid bij het kadasterformulier verklaart de notaris dat het kadasterformulier woordelijk gelijkluidend met de authentieke akte is.
[39] Zie: De Wet van 28 november 1947, Stb H 66
[40] Memorie van antwoord op de voorgestelde wetswijziging houdende vervanging van de inhoud van ten hypotheekkantore gehouden openbare registers door mechanische reprodukties (ingezonden 16 juni 1964) Nr.5 zitting 1963-1964-**7271**; [Staatssecretaris van Financiën Van den Berge].

heden ten dage is dat wel anders, getuige het vele overleg dat tussen Kadaster en notariaat bijvoorbeeld op het vlak van bewaring van akten plaatsvindt.

3.3 Het papieren aanleverproces

3.3.1 Beschrijving van de partijen bij de aanlevering

De partijen die een grote rol spelen bij het aanleveren van de notariële akte bij het Kadaster zijn de notaris en het Kadaster. PTT post zorgt voor de bezorging van de documenten. Naast het notariaat kunnen ook deurwaarders, vertegenwoordigers van gemeenten en zaakwaarnemers akten in de openbare registers doen inschrijven. Dit gebeurt slechts zelden en daarom voert het te ver om ook deze partijen te beschrijven.

De Dienst voor het kadaster en de openbare registers (het Kadaster)[41]

Algemeen
Het Kadaster ontleent zijn huidige bestaansrecht aan de Organisatiewet Kadaster (Stb. 125): “er is een Dienst voor het kadaster en de openbare registers. Hij bezit rechtspersoonlijkheid en is gevestigd te Apeldoorn” [42].
Naast de hoofdvestiging in Apeldoorn zijn er (nog) vijftien Kadastervestigingen verspreid over Nederland. In totaal werken ongeveer 2000 mensen bij het Kadaster.

Wettelijke taken
De Kadasterwet (Stb. 186) vormt de belangrijkste wettelijke basis voor de taak van het Kadaster. In die wet worden conform het Burgerlijk Wetboek[43] regels gesteld met betrekking tot de openbare registers voor registergoederen, alsmede met betrekking tot het Kadaster, de registratie voor schepen en de registratie voor luchtvaartuigen. De maatschappelijke opdracht aan het Kadaster, het bevorderen van de rechtszekerheid bij het maatschappelijk verkeer in vastgoed inclusief schepen en luchtvaartuigen, is verder neergelegd in de Organisatiewet Kadaster en onder andere de Landinrichtingswet.
Kerntaken van het Kadaster zijn het inwinnen, accepteren, muteren, beheren en verstrekken van informatie over vastgoed; het meewerken aan het landinrichtingsproces en het in stand houden van een net van zogenaamde coördinaatpunten, de Rijksdriehoekmeting. Deze kerntaken worden uitsluitend door de wetgever bepaald.
Het Kadaster beschikt dankzij zijn wettelijke taken over het grootste vastgoedinformatiesysteem van Nederland, de ‘levensbron’ voor de uitvoering van zijn meeste taken. De kadastrale databank bevat gegevens over meer dan zeven miljoen eigendommen van zo’n drie-eneenhalf miljoen zakelijk gerechtigden. Professionele klanten als de makelaars, de gemeenten, de waterschappen en de notarissen raadplegen veelvuldig dit gegevenssysteem. De notarissen zijn naast klant van het Kadaster tevens de voornaamste leverancier van het Kadaster en zorgen zo samen met het Kadaster voor de rechtszekerheid bij het maatschappelijk verkeer in registergoederen.

Nevenactiviteiten
In de keuze van eventuele marktactiviteiten heeft het Kadaster, binnen de gestelde bedrijfseconomische eisen, een zekere vrijheid. Bij de vervulling van zijn wettelijke taken is die vrijheid er niet; het Kadaster voert de wet uit.

[41] Uit: Kadaster jaarverslag 1993, 1994, 1995 en 1996.
[42] Art. 2 Organisatiewet Kadaster
[43] Art. 3:16 BW

Juridische positie
Het van stelsel openbare registers in Nederland wordt met betrekking tot de weergave daarin van de civielrechtelijke toestand van onroerend goed, veelal aangeduid als onvolledig en negatief. Niet alle wijzen van rechtsverkrijging vereisen inschrijving in de openbare registers en een inschrijving garandeert niet altijd dat het recht ook daadwerkelijk verkregen is[44].
Eén van de kenmerken van een negatief stelsel van grondboekhoudingen is de lijdelijkheid van de registrerende instantie. Dit wil zeggen dat de bewaarder der registers een akte moet inschrijven als wordt voldaan aan de inschrijvingsvereisten die in de Kadasterwet staan opgesomd. Wanneer een stuk is ingeschreven in de openbare registers heeft dit rechtskracht tegenover derden. Deze mogen te goeder trouw vertrouwen op de openbare registers.
Daarnaast is er de kadastrale registratie. Dit is de toegangspoort tot de openbare registers. Ten aanzien van de kadastrale registratie is de bewaarder niet lijdelijk[45]. Hij zal bij gerede twijfel over de beschikkingsbevoegdheid, geldigheid van de titel of leveringsgebreken niet overgaan tot zgn. kadastrale toepassing. Hij zal een waarschuwing in de kadastrale registratie opnemen. De waarschuwing heeft tot gevolg dat een koop niet door kan gaan omdat de koper onvoldoende vertrouwen heeft in de kadastrale tenaamstelling.

De organisatie
Het Kadaster is sinds 1 mei 1994 een Zelfstandig Bestuursorgaan (ZBO). Dit is een rechtstreeks gevolg van het regeerakkoord van het kabinet Lubbers (1990-1994). In dit regeerakkoord staat dat Diensten die niet tot de kernactiviteiten van een departement behoren, op afstand van het departement gezet zullen worden. ZBO's verschillen van elkaar in de mate van ministeriële verantwoordelijkheid.
De minister (staatssecretaris) van VROM is (eind) verantwoordelijk voor de continuïteit van het Kadaster, voor de kwaliteit van de dienstverlening en voor de vaststelling van de kadastrale tarieven. Het Kadaster is als bestuursorgaan verantwoordelijk voor de uitvoering van zijn wettelijke taken. Daarnaast mag het Kadaster nevenactiviteiten verrichten of daaraan deelnemen. Het Kadaster is zelf verantwoordelijk voor het financieel en personeel beheer. Hierbij wordt gestreefd naar kostendekkendheid van zijn activiteiten en een zo hoog mogelijke efficiëntie. Als bestuursorgaan kan het Kadaster (nog steeds) besluiten in de zin van de Algemene wet bestuursrecht (AWB) nemen. Het verlenen van bijvoorbeeld een vergunning behoort dus, mits de Kadasterwet dit toestaat, tot de mogelijkheden. Tevens is het Kadaster als ZBO gehouden aan de algemene beginselen van behoorlijk bestuur gesteld in de AWB. Tenslotte is het Kadaster als ZBO een overheidsorgaan als bedoeld in de Archiefwet 1995 (Stb. 276).
Het verzelfstandigde Kadaster wordt geleid door een driehoofdige Raad van Bestuur. Een uit vijf personen bestaande Raad van Toezicht heeft de taak toezicht uit te oefenen op de Raad van Bestuur en deze zo nodig te adviseren. De mate waarin de minister van VROM de taakuitoefening kan controleren wordt beschreven in de Organisatiewet Kadaster. De minister moet de jaarstukken, het meerjarenbeleid en tariefwijzigingen goedkeuren. Verder heeft de minister zeggenschap over de samenstelling van de Raad van Bestuur en de Raad van Toezicht.

De notaris[46]

Algemeen
Nederland telt ongeveer 1200 notarissen en 1500 kandidaat-notarissen gevestigd in circa 800 kantoren. Notariskantoren kennen geen specialisaties; alle kantoren moeten in principe alle diensten even goed kunnen verrichten.

[44] Asser-Mijnssen-de Haan,1992.
[45] Zevenbergen, J.A., WPNR 96/6240.
[46] Http://www.notaris.nl ; d.d. 30-10-1997 en Mourik, M.J.A. van, 1995.

Wettelijke taak[47]
De Wet op het Notarisambt (Stb. 276) omschrijft de taak van de notaris als volgt: notarissen zijn openbare ambtenaren, uitsluitend bevoegd, om authentieke akten te verlijden wegens alle handelingen, overeenkomsten en beschikkingen waarvan de wet gebiedt of de belanghebbenden verlangen, dat bij authentiek geschrift blijken zal; het tijdstip van verlijden te verzekeren; de akten in bewaring te houden en daarvan grossen, afschriften en uittreksels uit te geven; alles voor zoover het verlijden dier akten door de wet niet ook aan andere ambtenaren opgedragen of aan dezelve geheel voorbehouden is[48].

Nevenactiviteiten[49]
De notaris rekent niet alleen het opstellen van de akten zelf tot zijn taak. Hij leidt meestal ook de besprekingen die aan de akte vooraf gaan. Hij geeft juridische adviezen, maakt onderhandse akten op en bemiddelt bij geschillen tussen partijen. De notaris is vertrouwensman en adviseur op een breed terrein van het privaatrecht alsook op specifieke terreinen van het belastingrecht.

Juridische positie
De notaris is een onafhankelijke en onpartijdige partij bij het bevestigen van een overeenkomst tussen twee partijen. Bij de inschrijving van de meeste rechtsfeiten in de openbare registers wordt een notariële akte vereist. Dit ter bevordering van de rechtszekerheid. De Wet op het Notarisambt en de Kadasterwet stellen eisen met betrekking tot de inhoud van de akte. Het vervullen van deze eisen is een taak van de notaris.

Aanstelling
Om in Nederland tot notaris te kunnen worden benoemd moet men aan bepaalde in de Wet op het Notarisambt omschreven eisen voldoen. De drie belangrijkste eisen zijn:
1. dat de betrokkene Nederlander is
2. dat hij/ zij de bij de wet voorgeschreven notariële examens met goed gevolg heeft afgelegd, waardoor de betrokkenen kandidaat-notaris wordt
3. dat de kandidaat-notaris daarna minstens drie jaar praktijk heeft opgedaan op een of meerdere notariskantoren

Na zijn benoeming door de Koning(in) moet de notaris een drieledige eed afleggen, waarvan voor het publiek de beroepseed het belangrijkste onderdeel is. Daarin zweert de notaris dat hij:
1. de door hem aanvaarde taak eerlijk, nauwkeurig en onpartijdig zal vervullen
2. zo stipt mogelijk de wetten die op zijn beroep betrekking hebben, zal naleven
3. de grootst mogelijke geheimhouding over de inhoud van de door hem opgemaakte akte in acht zal nemen

De aflegging van de eed waarborgt de onpartijdige en onafhankelijke vertrouwensfunctie van de notaris. Door het afleggen van de eed is de notaris niet alleen bevoegd maar (behoudens enkele uitzonderingen) ook verplicht zijn diensten aan het publiek te verlenen.

Toezicht
Notarissen, hun plaatsvervangers en kandidaat-notarissen staan onder controle van de Kamer van Toezicht: een college van vijf leden, waarvan de president van een Arrondissementsrechtbank voorzitter is.

[47] Art. 2 van de bij de Tweede Kamer in behandeling zijnde nieuwe Wet op het notarisambt luidt: “Het ambt van de notaris houdt in de bevoegdheid om authentieke akten te verlijden in de gevallen waarin de wet dit aan hem opdraagt of een partij zulks van hem verlangt en andere in de wet aan hem opgedragen werkzaamheden te verrichten.”
[48] Art. 1, Wet op het Notarisambt, Wet van den 9den julij 1842, op het notarisambt, zoals laatstelijk gewijzigd bij de wet van 24 mei 1996, Stb 276
[49] De in de Tweede Kamer in behandeling zijnde Wet op het notarisambt beperkt de mogelijke nevenactiviteiten van de notaris in art. 15 expliciet. In de memorie van toelichting verklaart de Staatssecretaris dat de onpartijdigheid van de notaris alleen voor de wettelijke taken geldt en niet van toepassing is als de notaris bijv. als adviseur optreedt. De notaris mag volgens lid 3 van het artikel niet bemiddelen bij de koop en verkoop van onroerende zaken, financieringen en verzekeringen; Tweede Kamer, vergaderjaar 1995-1996, 23706, nr. 8

Koninklijke Notariële Beroepsorganisatie[50]

De Koninklijke Notariële Beroepsorganisatie (KNB) is de beroepsorganisatie van alle notarissen en kandidaat-notarissen. De belangrijkste taken van de KNB zijn het behartigen van de belangen van haar leden en het bijdragen van een goede beroepsuitoefening. De KNB onderhoudt daardoor nauwe banden met de overheid, de politiek en met tal van maatschappelijke organisaties. Verder besteedt de KNB veel aandacht aan voorlichting aan eigen leden en aan het publiek.
In de voorgestelde nieuwe Wet op het notarisambt zal de KNB een publiekrechtelijke beroepsorganisatie (PBO) worden. Dit betekent dat de KNB verordeningen kan maken waar alle notarissen aan gebonden zijn.

3.3.2 Wettelijke basis van het inschrijven van de akte in de openbare registers

Het inschrijven van de notariële akte in de openbare registers vindt zijn wettelijke basis onder andere in het Burgerlijk Wetboek. De voor de overdracht van registergoederen en voor de vestiging van beperkte rechten vereiste levering geschiedt door een daartoe bestemde, tussen partijen opgemaakte notariële akte, gevolgd door de inschrijving daarvan in de daartoe bestemde openbare registers[51]. Er worden openbare registers gehouden, waarin feiten voor de rechtstoestand van registergoederen van belang, worden ingeschreven[52].
De in de openbare registers in te schrijven feiten staan in het Burgerlijk Wetboek opgesomd. Tevens zijn er procedurele eisen gesteld.
De Wet op het Notarisambt stelt eisen aan de inhoud van de akte en de wijze waarop en door en voor wie deze wordt verleden[53]. In de Kadasterwet staat waar en op welke wijze een inschrijving kan worden verkregen, welke stukken daartoe aan de bewaarder moeten worden aangeboden, wat deze stukken moeten inhouden, hoe de registers worden ingericht, hoe de inschrijvingen daarin geschieden en hoe de registers kunnen worden geraadpleegd.
Het Burgerlijk Wetboek stelt in artikel 3:20 dat de bewaarder van de openbare registers een inschrijving weigert te doen wanneer de nodige stukken niet worden aangeboden of wanneer de aangeboden stukken niet aan de wettelijke eisen voldoen of wanneer een ander wettelijk vereiste niet is vervuld. Wanneer een weigering ten onrechte is geschied beveelt de president van de rechtbank, rechtdoende in kort geding, op vordering van de belanghebbende de bewaarder de inschrijving alsnog te verrichten. Indien de bewaarder vermoedt dat de in de aangeboden stukken vermelde kenmerken niet overeenstemmen met die welke met betrekking tot het registergoed behoren te worden vermeld, of dat de in te schrijven rechtshandeling door een onbevoegde is verricht of onverenigbaar is met een andere rechtshandeling, ter inschrijving waarvan hem de nodige stukken zijn aangeboden, is hij bevoegd de aanbieder en andere belanghebbenden daarop opmerkzaam te maken (art. 3:19 vierde lid BW). Bij een onjuiste feitelijke omschrijving of een onjuiste of onvolledige kadastrale aanduiding van de onroerende zaak wordt volgens artikel 59 Kadasterwet de bijhouding van het Kadaster eerst voltooid, nadat een stuk tot verbetering is ingeschreven in de openbare registers. Tenaamstelling van de verkrijger zal trouwens in de kadastrale registratie ook achterwege blijven, zolang het vermoeden van onbevoegdheid van de vervreemder bij de bewaarder bestaat, bijvoorbeeld omdat deze niet bij het Kadaster als rechthebbende bekend is[54].

[50] Http://www.notaris.nl/knb/home.html ; d.d. 01-12-1997
[51] Art. 3:89 BW
[52] Art. 3:16 BW
[53] Wet op het Notarisambt, Hoofdstuk III Van de akten en derzelve vorm, van de minuten, grossen, afschriften en repertoria.
[54] Asser-Mijnssen- de Haan, 1992.

3.3.3 Inschrijvingsvereisten en autorisatie van personen

Inschrijving van het afschrift van de notariële akte in de openbare registers zorgt voor de vervulling van één van de voorwaarden voor het ontstaan van rechtsfeiten. Het is noodzaak dat de integriteit en de authenticiteit van de akte gewaarborgd zijn[55]. Ook moet de identiteit van de persoon die inschrijft bekend zijn en moet hij/ zij geautoriseerd zijn in te schrijven.

Integriteit
Integriteit van het document wil zeggen: de inhoud van het afschrift van de akte is ongewijzigd gebleven tijdens opmaak, verzending en transport. Ofwel de akte die de notaris heeft verstuurd, is ongewijzigd aangekomen bij het Kadaster.
De integriteit van het kadasterformulier wordt bepaald door de vervulling van de vele vormvereisten die uit de Uitvoeringsregeling Kadasterwet 1994 (Stcrt. 81) voortvloeien[56]. Ook het vereiste standaard kadasterformulier draagt bij aan verzekering van de integriteit[57] [58].
Een voorbeeld van een vormvereiste is dat de notaris iedere pagina parafeert en per pagina aangeeft hoeveel pagina's nog volgen. De specifieke eisen aan het kadasterformulier en eventuele wijzigingen daarop zorgen ervoor dat de bewaarder eenvoudig kan constateren dat het een kadasterformulier betreft en dat er al dan niet wijzigingen en correcties zijn geschied. Als de notaris een regel heeft doorgehaald of iets heeft toegevoegd aan het document dient hij dit in de kantlijn te bevestigen met zijn paraaf.

Authenticiteit van de akte
Art 183 lid 2 Wetboek van Burgerlijke Rechtsvordering (Rv) geeft aan wat een authentieke akte is. Het is een akte in de vereiste vorm en bevoegdelijk opgemaakt door ambtenaren aan wie bij of krachtens de wet is opgedragen op die wijze te doen blijken van door hen gedane waarnemingen of verrichtingen. De bedoelde ambtenaren zijn: de notaris, de deurwaarder en de ambtenaar van de Burgerlijke Stand. De handtekening van de ambtenaar die door deze in de uitoefening van zijn functie is geplaatst, wordt voor echt gehouden tot op het bewijs van het tegendeel. Daarmee is ook de echtheid van de betreffende akte gegeven[59]. De vereiste vorm wordt uitgewerkt in de Wet op het Notarisambt en de Kadasterwet. De authenticiteit wordt ontleend aan de handtekeningen van partijen, de handtekening van de notaris, de ambtszegel der notaris en de plaats, het jaar, de maand of dag en voor inschrijving in de openbare registers de minuut op de akte alsmede aan de voorlezing van de akte aan verschijnende personen voor het verlijden van de akte[60].
De aan het Kadaster aangeboden documenten betreffen niet de authentieke akte maar een afschrift ervan en een apart formulier met een verklaring van eensluidendheid. De verklaring van eensluidendheid heeft betrekking op de authentieke akte. De notaris verklaart conform artikel 11 eerste lid Kw op het kadasterformulier dat hij heeft geconstateerd dat dit formulier eensluidend met de authentieke akte is. De verklaring bevestigt hij door deze te ondertekenen en zijn ambtszegel te plaatsen. De authenticiteit van het kadasterformulier is hiermee vastgesteld.

De handtekening van de bewaarder wordt bij het tijdstip van aanbieding geplaatst. Samen met het deel, nummer en tijdstip van aanbieding maakt dit de inschrijving authentiek.

[55] Een kadasterformulier kan authentiek zijn, terwijl de inhoud door gebeurtenissen bij berichtaanmaak, verzending, transport en ontvangst niet meer integer is.
[56] Zie ook Kadasterwet onder titel 2
[57] Art. 4 Kadasterregeling 14 april 1994
[58] Artt. 3, 5, 6, 7, 8, 11, 12, 13 Uitvoeringsregeling Kadasterwet 1994 (zoals deze luidt per 29 april 1995)
[59] Hidma en Van Velten, 1996.
[60] Artt. 45, 38, 30, 26 Wet op het Notarisambt

Identificatie van de afzender
Identificatie is het bewijzen dat men de persoon is, voor wie men zich uitgeeft. De identificatie van de notaris blijkt uit zijn naam, standplaats, paraaf en handtekening.
De identificatie van de notaris bij het Kadaster gebeurt door herkenning. De medewerkers van de Kadastervestiging kennen de notarissen uit hun district (en hun handtekening/ parafen/ stempel).
De notaris wordt beëdigd voor de arrondissementsrechtbank[61]. Na de eedaflegging wordt zijn handtekening en paraaf gedeponeerd bij de griffier van de rechtbank van het arrondissement waartoe zijn standplaats behoort[62].
De bewaarder wordt bij de notaris aan de stempel van zijn handtekening herkend.

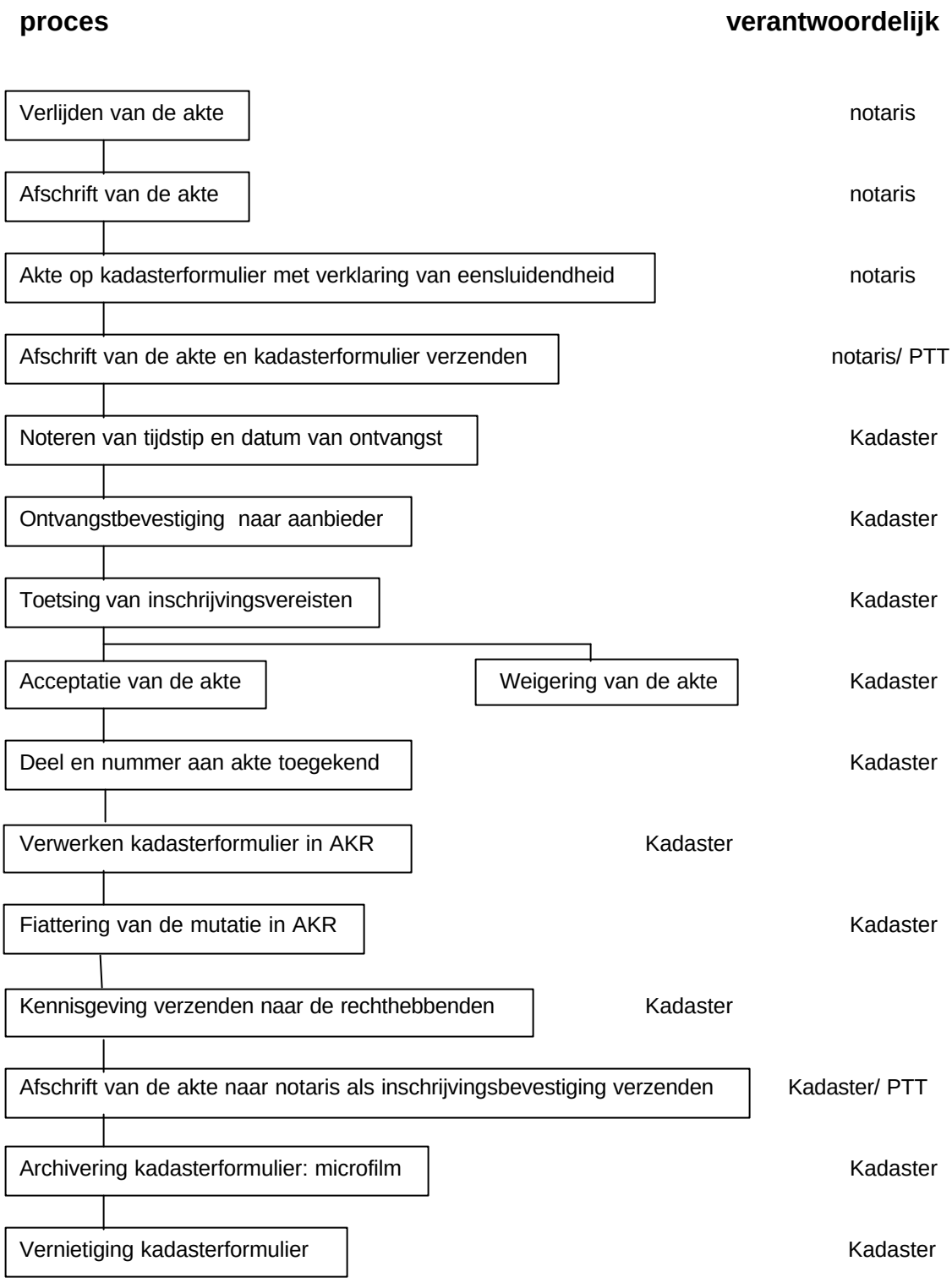
Autorisatie in het aanleverproces
De notaris is bij wet bevoegd de notariële akte op te maken en te verlijden. De notaris kan bij afwezigheid worden vervangen door een door de Kamer van Toezicht aangewezen kandidaat-notaris. Hij legt dan de eed af en zijn handtekening en paraaf dient dan gedeponeerd te zijn bij de arrondissementsrechtbank tot welker ressort het waargenomen kantoor behoort[63].

Bij het Kadaster zijn de bewaarders geautoriseerd de akten in te schrijven of het inschrijven te weigeren. In de praktijk laat de bewaarder dit over aan kadastermedewerkers die hier zijn toestemming voor hebben gekregen. Een stempel van de handtekening van de bewaarder vervangt de handtekening van de bewaarder. Voordat de medewerker een akte weigert in te schrijven neemt hij/ zij contact op met de bewaarder.

3.3.4 De opslag van het stuk

Het kadasterformulier met de verklaring van eensluidendheid wordt na inschrijving geconverteerd naar microfilm. Na de conversie wordt het kadasterformulier met verklaring van eensluidendheid vernietigd.
Van de microfilm wordt een kopie gemaakt. Eén van beide exemplaren gaat naar de kadastervestiging waar het kadasterformulier werd aangeboden. De andere microfilm wordt centraal bij het Computer Uitwijk Centrum (CUC) opgeslagen. De openbare registers op microfilm hebben dezelfde bewijskracht als de oorspronkelijke openbare registers[64].
Karmac Holland BV verzorgt de conversie van papier naar microfilm. De microfilm is van archiefkwaliteit met een gegarandeerde bewaartermijn van tenminste tachtig jaar[65]. Literatuur omtrent dit onderwerp meldt een duurzaamheid variërend van 50 tot 500 jaar afhankelijk van de wijze waarop de microfilm wordt bewaard[66].
Het Kadaster is vrijgesteld om de archieven na twintig jaar aan de Rijksarchiefdienst ter beschikking te stellen[67]. Derhalve dient het Kadaster zelf zorg te dragen voor de duurzaamheid van de openbare registers.

[61] Art. 18 Wet op het Notarisambt
[62] Art. 20 Wet op het Notarisambt
[63] Artt. 5 en 20 Wet op het Notarisambt
[64] Art. 9 tweede lid Kw
[65] Boekwerk Kadaster Algemeen (herdruk september 1997).
[66] Http://www.oclc.org/oclc/presres/micrographic/pres_microfilm.htm ; d.d.18-03-98,
http://esdis.gsfc.nasa.gov/msst/conf1996/B2_3Stutz.html d.d. 20-03-98
[67] Brief van 28 december 1977 betreffende opschorting van overbrenging van archiefbescheiden van het Kadaster.


proces
verantwoordelijk
Verlijden van de akte
notaris
Afschrift van de akte
notaris
Akte op kadasterformulier met verklaring van eensluidendheid
notaris
Afschrift van de akte en kadasterformulier verzenden
notaris/ PTT
Noteren van tijdstip en datum van ontvangst
Kadaster
Ontvangstbevestiging naar aanbieder
Kadaster
Toetsing van inschrijvingsvereisten
Kadaster
Acceptatie van de akte
Weigering van de akte
Kadaster
Deel en nummer aan akte toegekend
Kadaster
Verwerken kadasterformulier in AKR
Kadaster
Fiattering van de mutatie in AKR
Kadaster
Kennisgeving verzenden naar de rechthebbenden
Kadaster
Afschrift van de akte naar notaris als inschrijvingsbevestiging verzenden
Kadaster/ PTT
Archivering kadasterformulier: microfilm
Kadaster
Vernietiging kadasterformulier
Kadaster

3.3.5 Het aanleverproces

De aanlevering van de notariële akte bij het Kadaster is een proces dat grotendeels voortvloeit uit wetten. Het Burgerlijk Wetboek, de Kadasterwet en de Wet op het Notarisambt uit 1842 zijn deze wetten. De onderstaande stappen worden per akte doorlopen.

1. De notaris maakt de minuutakte in zijn vereiste vorm op en ondertekent deze met vermelding van het tijdstip van ondertekening; de notaris verlijdt de akte van levering[68]
2. De notaris maakt een afschrift van de akte en maakt een eensluidend kadasterformulier. Op het kadasterformulier zet de notaris de verklaring van eensluidendheid. De notaris ondertekent deze verklaring[69]
3. De notaris biedt afschrift van de akte en formulier Hyp4A met verklaring van eensluidendheid aan bij het Kadaster[70]
4. Het aangeboden stuk wordt van het tijdstip van aanbieding voorzien[71]
5. Kadaster stuurt een ontvangstbevestiging met tijdstip van ontvangst (per fax) terug[72] [73]
6. Bewaarder toetst de inschrijvingsvereisten en weigert of accepteert de akte[74]
7. Bewaarder schrijft de akte in (geeft een deel en nummer aan de akte[75], het kadasterformulier krijgt tijdstip van ontvangst en deel en nummer met handtekening van de bewaarder) of belt de notaris ter verwittiging van de weigering. Na overleg wordt de akte door de notaris opnieuw gemaakt of komt deze in het register van voorlopige aantekeningen (= weigeringsregister) terecht. Na inschrijving van het kadasterformulier in de openbare registers (niet inbegrepen register van voorlopige aantekeningen) is de voor overdracht van een onroerend zaak vereiste levering geschied
8. Kadaster verwerkt het kadasterformulier (met relaas van de bewaarder) in de kadastrale registratie (AKR) en stuurt een kennisgeving van de bijwerking van de kadastrale registratie naar de rechthebbenden (≠notaris)[76]
9. De mutaties in de kadastrale registratie worden door de bewaarder gefiatteerd. De stukken kunnen op dat moment met de status goedgekeurde mutatie middels AKR uit de openbare registers worden opgevraagd
10. Kadaster stuurt een inschrijvingsbevestiging naar de notaris: het afschrift van de akte met de tijd en de datum van inschrijving, deel en nummer en relaas en handtekening van de bewaarder[77]
11. Het kadasterformulier wordt in dubbel op microfilm gezet (de openbare registers), een aantal jaar bewaard en tenslotte vernietigd[78]

[68] Artt. 30 en 38 Wet op het Notarisambt
[69] Artt. 40 en 45 Wet op het Notarisambt; art. 11 Kw
[70] Art. 3:89 BW
[71] Art. 12 tweede lid Kw
[72] Artt. 3:18 en 3:19 BW, art. 17 Kw, art. 19 Kr
[73] Het tijdstip van ontvangst is gelijk aan het tijdstip van inschrijving.
[74] Artt. 3:19 BW en 3:20 BW, artt. 5 en 6 Kr
[75] deel en nummer: art. 12 derde lid Kw, artt. 12-15 Kr
[76] Art. 14 Kb
[77] Art. 13 Kw
[78] Art. 9 Kw

3.4 Mogelijke fouten in het aanleverproces

In het aanleverproces kunnen op verschillende momenten diverse fouten optreden. Deze zijn in te delen in drie groepen:

1. Fouten door transport van het document
2. Fouten bij de verwerking van de akte bij het Kadaster
3. Fouten met betrekking tot de inhoud van het document

3.4.1 Fouten door transport van een document

Het vervoer van de akten naar het Kadaster gebeurt door PTT post of door koeriers en/ of loopjongens van de notaris. Er worden nauwelijks door anderen dan notarissen akten aangeboden. Als dat gebeurt, is het door deurwaarders, advocaten, zaakwaarnemers of vertegenwoordigers van gemeenten.
Het Kadaster verzendt al zijn (wettelijk verplichte) correspondentie met behulp van PTT post.

Bij de volgende onderdelen van het aanlever- en verwerkingsproces kunnen door het transport van een document fouten optreden:
1. Het versturen van het afschrift van de akte en het kadasterformulier naar het Kadaster
2. Het versturen van de ontvangstbevestiging naar de aanbieder
3. Het versturen van de inschrijvingsbevestiging naar de aanbieder
4. Het versturen van de nota naar de aanbieder
5. Het versturen van de kennisgevingen naar rechthebbenden
6. Het transporteren van het kadasterformulier naar Karmac Holland B.V. voor de microverfilming van het kadasterformulier

De fouten die tijdens het transport van documenten kunnen optreden zijn:
a) Het document gaat verloren
b) Het document wordt door tussenkomst ongeautoriseerde(n) gewijzigd
c) Het document wordt door ongeautoriseerde(n) gelezen
d) Het document wordt dubbel verstuurd
e) Het document dwaalt af: komt in bezit van derden
f) Het document wordt vertraagd
g) Het document wordt fysiek verminkt: het document wordt (gedeeltelijk) onleesbaar

Voorbeeld van een fout door vertraagde akten
Voor hetzelfde perceel wordt een hypotheekakte bij een andere notaris verleden dan de transportakte. Beide notarissen sturen de akten op dezelfde dag weg. De hypotheekakte wordt een dag eerder aangeboden en ingeschreven. Deze kan echter niet kadastraal worden toegepast. Later wordt de transportakte ingeschreven en toegepast. Het hypotheekrecht is niet gevestigd. De hypotheekakte moet worden doorgehaald en opnieuw worden aangeboden en ingeschreven.

3.4.2 Fouten bij de verwerking van de akte bij het Kadaster

Nadat de akte door de notaris is opgestuurd ontvangt het Kadaster het afschrift en het kadasterformulier. Op dat moment begint de verwerking van de akte bij het Kadaster. Bij de verwerking van de akte kunnen fouten optreden, deels te wijten aan het onbewust of bewust handelen van kadasterpersoneel, deels aan de wettelijk bepaalde procedures voor de inschrijving.

Fouten door het Kadaster

Bij het verwerken kunnen fouten ontstaan door menselijk handelen. Gedacht kan worden aan fouten bij:

- het noteren van het tijdstip van aanbieding
- het toekennen van deel en nummer aan de akte: een akte krijgt geen (uniek) deel en nummer van het Kadaster
- het signaleren van akten[79]
- het archiveren van het kadasterformulier: de akte is niet meer leesbaar of beschikbaar; de conversie van papier naar microfilm gaat verkeerd. Of de akte wordt fysiek verminkt: kop koffie valt over de akte
- het bijwerken van de kadastrale registratie

De kadastrale registratie is de toegangspoort tot de openbare registers. Wanneer de openbare registers niet toegankelijk zijn via de kadastrale registratie dan is het Kadaster aansprakelijk. Het komt bijvoorbeeld voor dat het deel en nummer dat aan de akte is toegekend vergeten wordt in AKR bij te werken.

Fouten zonder schuld van het Kadaster

Een andere soort fouten die bij de verwerking van de akte voorkomt is een gevolg van het moment van aanbieden van de akte. De volgorde van het behandelen van de stapel aanbiedingen en de inschrijving van beslagen op zakelijke rechten kunnen leiden tot schade buiten de schuld van het Kadaster en notaris om.

Het behandelen van de stapel aanbiedingen
Akte 1 wordt bij de notaris om 17.00 uur verleden. Dezelfde dag wordt akte 2 om 17.05 verleden. De akten betreffen dezelfde overdracht maar naar een andere verkrijger.
Beide akten worden de volgende dag om 9.00 uur aan het Kadaster aangeboden; ze zitten in dezelfde postzak. Akte 2 ligt bovenop de stapel en akte 1 onderop. Akte 2 wordt ingeschreven om 9:00 uur (tijdstip van aanbieding) en toegepast. Akte 1 wordt ingeschreven om 9:00 uur maar kan niet kadastraal worden toegepast omdat er inmiddels een andere gerechtigde staat geregistreerd.
De bewaarder zal bij de behandeling van akte 1 deze akte vergelijken met de eerder toegepaste akte 2. Mocht blijken dat akte 1 eerder is verleden dan wordt deze akte alsnog toegepast. Deze handelwijze is conform artikel 3:21 Burgerlijk Wetboek.
De notaris heeft geen wanprestatie geleverd, het Kadaster heeft rechtmatig ingeschreven en toch is de ‘verkrijger’ van akte 2 geen verkrijger geworden.

Beslagen op zakelijke rechten
Executoriale (arrest op goederen tot tenuitvoerlegging van een vonnis) en conservatoire (beslaglegging op goederen als middel tot bewaring van recht) beslagen worden door een gerechtelijke uitspraak van kracht. Het moment van aanbieding is bepalend voor de rechtstoestand. Het beslag wordt in de registratie aangetekend.
Voor het beslag is een dag van respijt ingesteld. Is een akte een dag voordat het beslag van kracht wordt ingeschreven, dan gaat de akte voor; het beslag werkt niet tegen de verkrijger.

[79] Signalering wil zeggen de akte is bij het Kadaster in behandeling. Signalering heeft dezelfde status als de ontvangstbevestiging. Wanneer een akte is ontvangen en er geen beslag is gelegd, gaat de notaris over tot uitbetalen. Foute signalering zorgt voor onterechte uitbetaling aan de vervreemder (zie verder onder 3.4.4)

Ongeautoriseerde inschrijvingen en mutaties van inschrijvingen

Tenslotte kunnen bij de verwerking van de akte fouten optreden die bewust worden gemaakt door notarissen, derden en kadastermedewerkers. We spreken dan over ongeautoriseerde inschrijvingen en mutaties van inschrijvingen.

Identificatie van partijen
De identificatie van degene die de akte heeft opgemaakt wordt niet door het Kadaster gedaan voor wat betreft bekende notarissen. Als een derde inschrijft onder de naam van een bij het Kadaster bekende notaris kan er worden ingeschreven.
Als een onbevoegde een notaris simuleert en een akte aanbiedt, kan deze worden ingeschreven. De akte moet dan wel aan de vormvereisten voldoen (zie subparagraaf 3.3.3).

Onrechtmatige daad van kadasterpersoneel
Bij het archiveren van het kadasterformulier kan 'iets' verkeerd gaan zodat kadasterformulier en akte niet meer eensluidend zijn. Het is echter ook heel goed mogelijk dat een kadastermedewerker, die geautoriseerd is de vormvereisten voor inschrijven te toetsen, een wijziging aanbrengt op het kadasterformulier. Hij is hier niet toe geautoriseerd. De wijziging kan betrekking hebben op het corrigeren van de notaris (zoals een vergeten handtekening of paraaf plaatsen). Minder onschuldig is het wijzigen ten voordele van bepaalde (rechts)personen. Het onderstaande voorbeeld maakt dit duidelijk.

Voorbeeld van onrechtmatige daad van kadasterpersoneel: fraude met hypotheekrecht
Een daartoe bevoegd persoon bij het Kadaster kan een hypotheekrecht doorhalen[80]. Op dezelfde onroerende zaak kan dan wederom een hypotheekrecht worden verkregen. Immers een notaris kijkt in de openbare registers en ziet dat de onroerende zaak onbelast is en geeft aan de hypotheekgever, na het passeren van de hypotheekakte, een notariële verklaring af dat een hypotheekrecht is gegeven aan X met het onderpand Y[81]. Het onterecht doorgehaalde hypotheekrecht staat wel in de openbare registers maar is niet meer als een actuele inschrijving opgegeven; de toegangspoort naar de openbare registers is gesloten. De hypothecaire lening staat nog wel in het bestand van de verstrekker van de hypothecaire lening. Deze zal wanneer de aflossing van de lening niet meer betaald wordt aan haar schuldenaar verzoeken de aflossing te betalen. Doet deze dat niet dan zal men stappen ondernemen en er achter komen dat er gefraudeerd is.

3.4.3 Fouten met betrekking tot de inhoud van het document

In het document kunnen fouten staan. Fouten in dit verband slaat op de inhoudelijke juistheid, op de integriteit en de authenticiteit van de documenten. Het Kadaster toetst de akte op de laatste twee punten. De inhoudelijke juistheid van de akte wordt ambtshalve door de notaris gewaarborgd. Desondanks kunnen er fouten ontstaan in de inhoud van het document.

Fouten in de inhoudelijke juistheid van de documenten

Verlijden van de akte
De notaris verlijdt de akte ten onrechte; vereisten die uit de Wet op het Notarisambt voortvloeien heeft hij onvolledig of geheel niet vervuld.

Legitimatie personen bij de notaris/ Notariaat te kwader trouw
Door valse legitimatie te tonen aan de notaris wordt een onroerende zaak van de vermeende vervreemder aan een derde te goeder trouw verkocht. Raadplegen van het verificatie informatiesysteem (VIS) dat

[80] Een doorgehaald hypotheekrecht betekent dat de hypotheekakte in de openbare registers niet meer via de kadastrale registratie (AKR) toegankelijk is en dus onvindbaar zal zijn.
[81] Er wordt wel verwezen naar hypotheekakten die zijn doorgehaald en de notaris moet deze in het kader van zijn rechercheplicht inzien.

gegevens over identiteitsbewijzen, waardepapieren en overige documenten die worden vermist, zijn gestolen of ongeldig zijn verklaard, kan de notaris helpen de identiteit van de cliënten vast te stellen.

Het ontvangstbewijs = inschrijvingsbevestiging?
De ontvangstbevestiging wordt door het notariaat ten onrechte als inschrijvingsbevestiging behandeld.
Het Kadaster stuurt de ontvangstbevestiging naar de notaris. Deze beschouwt de ontvangstbevestiging als inschrijvingsbevestiging en geeft de vervreemder de overdrachtssom. De akte wordt echter niet ingeschreven. De 'verkrijger' is zijn geld kwijt en de vervreemder zit in Chili.
De notaris is aansprakelijk voor de schade van de 'verkrijger'. Deze werkwijze kan de notaris zich permitteren omdat hij/ zij dit met de verzekeringsmaatschappijen heeft afgesproken en zich ervoor heeft laten verzekeren.

Het foutief toetsen van de inschrijvingsvereisten[82]

Het Kadaster schrijft onterecht in of weigert ten onrechte in te schrijven. Wanneer een feit in de registers is ingeschreven, kan daarna de geldigheid van de inschrijving niet meer worden betwist op grond dat de formaliteiten die voor de inschrijving worden vereist, niet in acht zijn genomen (art. 3:22 BW).

Ontbreken van de integriteit van de documenten

Ontbreken van inschrijvingsvereisten
Het ontbreken van de eisen die de Kadasterwet stelt aan de volledigheid van documenten is reden voor de bewaarder een stuk niet in te schrijven. Het ontbreken van een handtekening op de documenten, parafen per bladzijde en bladnummering zijn onzorgvuldigheden van de notaris die leiden tot weigering van inschrijving.

Het versturen van de ontvangstbevestiging
Dikwijls stuurt de notaris een ontvangstbevestiging met de inschrijvingsbescheiden mee. Hierop staan de akten die volgens hem/ haar zijn aangeboden. Een enkele vestiging van het Kadaster (Rotterdam) controleerde deze lijst niet met de werkelijk aangeboden akten. Het kon gebeuren dat op het formulier van de notaris tien akten stonden geboekt als aangeboden terwijl het Kadaster er slechts negen ontvangen had. Het Kadaster stuurde het formulier van de notaris bevestigend terug. Er was dan een akte 'zoekgeraakt' bij het Kadaster.

Het inschrijven van de akte in de openbare registers
De bewaarder schrijft in echter zonder zijn handtekening op het kadasterformulier te zetten. Hij kan eveneens vergeten zijn deel en nummer op het kadasterformulier te zetten.

Ontbreken van authenticiteit van de documenten

De notaris laat zijn vrouw de akte tekenen en biedt de akte aan. De authenticiteit van de handtekening of parafen van de notaris wordt niet door het Kadaster nagegaan. Er moet een handtekening staan en of deze van de notaris, zijn klerk of vrouw is, doet voor inschrijving in de openbare registers niet ter zake.

3.4.4 Foutendetectie in het aanleverproces

Veel van de bovengenoemde fouten blijken in de praktijk fictief. Ze komen niet voor of worden in een vroeg stadium van het aanleverproces gevonden. Het aanleverproces kent (bewust of onbewust) een aantal controles die de meeste fouten boven tafel leggen. De momenten van 'controle' zijn hieronder per foutengroep opgesomd.

[82] De inschrijvingsvereisten staan in de artt. 11-13 en 18-23 Kw en art. 11 Kr

Fouten door transport van de documenten

Nadat een notaris de akte heeft verstuurd, verwacht deze dezelfde dag een ontvangstbevestiging en een inschrijvingsbevestiging zo spoedig mogelijk. In de praktijk varieert dit van enkele dagen tot enkele weken. Wanneer er geen bevestigingen komen, wordt contact opgenomen met het Kadaster. Zoekgeraakte akten worden zo ‘gevonden’.
Een door transport (fysiek of inhoudelijk) gewijzigde akte kan door zijn wijzigingen wellicht niet worden ingeschreven omdat de vormvereisten niet worden vervuld. De notaris krijgt dan telefonisch bericht van het Kadaster. Eventuele inhoudelijke wijzigingen kunnen door de rechthebbenden die een kennisgeving van de mutatie in AKR krijgen thuisgestuurd worden geconstateerd. En de essentialia uit de akte staan in AKR.

Fouten bij de verwerking van de akte bij het Kadaster

Toekennen van deel en nummer
Bij het muteren van de kadastrale registratie zal het computersysteem aangeven dat het in te voeren nummer al bestaat en zal geen mutatie toestaan.

Signaleren van de akte
Een foute signalering zal bij de werkelijke inschrijving van de akte ontdekt worden. Vaak is dit te laat en is het leed al geschied.

Beslaglegging
In AKR kijkt de notaris of er beslag is gelegd. Dit doet hij voordat hij het geld naar de vervreemder overmaakt, na de zogeheten narecherche.

Identificatie van de notaris
De naam en de handtekening van de notaris herkent de bewaarder. Als deze onbekend zijn, zal het dossier met notarissen er op na worden geslagen en eventueel de arrondissementsrechtbank voor verificatie van de handtekening en paraaf van de notaris.
Voor een inschrijving moet de aanbieder betalen. Meestal is de aanbieder de notaris. De rekening van de inschrijving gaat naar het adres van de bij het Kadaster bekende adres van de notaris. Is dit adres niet bekend dan zal uit onderzoek moeten blijken of de notaris gerechtigd was akten op te maken en in te schrijven. Ditzelfde geldt voor de ontvangstbevestiging en inschrijvingsbevestiging.

De simulatie van een bij het Kadaster bekende notaris zal om de bovengenoemde redenen ook niet onbekend blijven. De gesimuleerde notaris krijgt de rekening van de inschrijving, een ontvangstbevestiging en een inschrijvingsbevestiging thuisgestuurd. Als deze niet kloppen zal het Kadaster het waarschijnlijk snel te weten komen.
Echter de tijd die voorbijgaat tussen het moment van aanbieden en het moment van ontdekken van de fout zal voor de ‘vervreemder’ voldoende zijn om een derde te goeder trouw te vinden en de zaak te verkopen.

Autorisatie
De fouten die door misbruik van geautoriseerden van het Kadaster zijn ontstaan kunnen met behulp van andere gegevensverzamelingen dan die van het Kadaster naar voren komen. Te denken valt bijvoorbeeld aan registraties van bankinstellingen.

Fouten in de inhoud van de akte

Inhoudelijke juistheid van de akte
Indien de akte voldoet aan de inschrijvingsvereisten die in de Kadasterwet zijn gesteld dan moet de bewaarder de akte inschrijven. Dit geeft geen garanties over de juistheid van de inhoud van de akte. Deze moeten door de notaris worden onderzocht. De bewaarder controleert de juistheid van de inhoud van de akte wanneer hij de akte toepast in de kadastrale registratie. Bij het niet kunnen toepassen van de akte in AKR omdat bijvoorbeeld de kadastrale aanduiding niet op naam van de vervreemder staat, wordt de notaris door de bewaarder gebeld. De notaris beslist verder wat te doen.

Door raadpleging van AKR kan een ieder zien wat er in hoofdlijnen veranderd is. Hoewel geen rechtsgevolg aan de juistheid van de kadastrale registratie mag worden verbonden, kan constatering van onjuistheid van de gegevens in AKR leiden naar inhoudelijke onjuistheden in de akte. Immers de notaris ontdekt een andere verkrijger dan in de akte, vraagt het kadasterformulier uit de openbare registers op en vergelijkt deze met de authentieke akte.

De rechtsverkrijger en -vervreemder krijgen een kennisgeving van bijwerking van de kadastrale registratie thuisgestuurd. Als deze niet blijkt te kloppen (bijvoorbeeld een naam is verkeerd gespeld) wordt het Kadaster daar meestal van op de hoogte gebracht.

Inschrijvingsvereisten
Bij vermoeden dat aan de inschrijvingsvereisten niet wordt voldaan neemt de bewaarder contact op met de betreffende notaris (artikel 3:19 vierde lid BW). Onderling komt men er meestal wel uit (= de notaris maakt een nieuwe akte).

Integriteit
Als een akte niet integer is dan voldoet hij niet aan de inschrijvingsvereisten. De bewaarder zal de akte weigeren in te schrijven en de aanbieder daarvan op de hoogte stellen.

3.4.5 Momenten in het aanleverproces zonder controle

Eensluidendheid van het kadasterformulier met de akte
Het kadasterformulier met een verklaring van eensluidendheid wordt ingeschreven in de openbare registers. Het afschrift van de akte wordt naar de notaris teruggestuurd en kan door de notaris worden vergeleken met de oorspronkelijke akte. Zijn akte en afschrift niet meer eensluidend, dan maakt de notaris bij het Kadaster bezwaar tegen de inschrijving. De rechter doet uitspraak.
Het kadasterformulier en het afschrift worden door het Kadaster niet vergeleken op eensluidendheid. Het ingeschreven kadasterformulier kan dus niet eensluidend met de akte zijn en toch worden ingeschreven. In het geval dat het gewijzigde kadasterformulier wordt ingeschreven, is de notaris aansprakelijk aangezien hij heeft verklaard dat beide documenten eensluidend zijn. AKR raadpleging na inschrijving door de notaris kan uitkomst bieden, hoewel hij dit niet hoeft te doen.

Authenticiteit
De authenticiteit van het kadasterformulier wordt niet door het Kadaster gecontroleerd.

Tijdstip van aanbieding noteren
Het noteren van het tijdstip van aanbieding wordt niet gecontroleerd.

Archiveren
Op het archiveren van de akten werd in het Centrale Uitwijk Centrum tot voor kort geen acht geslagen. De akten waren niet goed geëtiketteerd en konden dus heel lastig terug worden gevonden. Men is bezig dit proces te verbeteren.

De raadpleging van de archieven van de vestigingen gebeurt dagelijks. Een adequate archivering heeft men daar gerealiseerd.

Bijwerking van de kadastrale registratie
Wanneer een kadastermedewerker zijn autorisatie op het systeem misbruikt voor bijvoorbeeld de doorhaling van een hypotheekrecht op het kadasterformulier en in de kadastrale registratie, kan hij dit ongemerkt doen. De betreffende persoon kan slechts op de dag van inschrijving worden geïdentificeerd aan zijn logincode. Wanneer er bij de fiattering problemen zijn kan de betrokken muteerder snel worden achterhaald. Correcte doorhaling van de hypotheek zal geen problemen opleveren. Na fiattering van de dag gaan de gegevens van wie wat heeft gemuteerd verloren.

3.5 Aansprakelijkheid binnen het papieren aanleverproces

In het voorgaande is duidelijk geworden dat in het huidige proces van inschrijving van de notariële akte zowel bij de notaris, de PTT als bij het Kadaster problemen kunnen ontstaan. Welke partij aansprakelijk is voor welke deel van het aanlevertraject wordt hierna besproken.

De aansprakelijkheidsverdeling zoals die in de analoge situatie bestaat, vloeit voort uit de wet en haar uitvoeringsbepalingen. Onder de wet wordt hier verstaan het Burgerlijk Wetboek, de Kadasterwet, de Wet op het Notarisambt en de Postwet.
De hieronder genoemde partijen zijn bij het proces van aanleveren betrokken en kunnen aansprakelijk zijn voor een deel van het proces.

Kadaster
De aansprakelijkheid van het Kadaster is geregeld in artikel 117 van de Kadasterwet. Het Kadaster is jegens betrokkenen aansprakelijk voor schade die zij lijden, doordat in strijd met de wet een inschrijving is geweigerd of is geschied. Het Kadaster is eveneens aansprakelijk voor alle verdere vergissingen, verzuimen, vertragingen of andere onregelmatigheden van zijn ambtenaren, gepleegd bij het houden van de registers of bij het opmaken of afgeven van afschriften, uittreksels en getuigschriften. Voor de bijwerking en het schriftelijk verstrekken van gegevens uit de kadastrale registratie is het Kadaster ook aansprakelijk.

Het Kadaster is niet aansprakelijk voor de inhoudelijke juistheid van de akte of het kadasterformulier. Het Kadaster accepteert de akte zonder inhoudelijk onderzoek als aan de wettelijke (vorm)vereisten wordt voldaan[83].

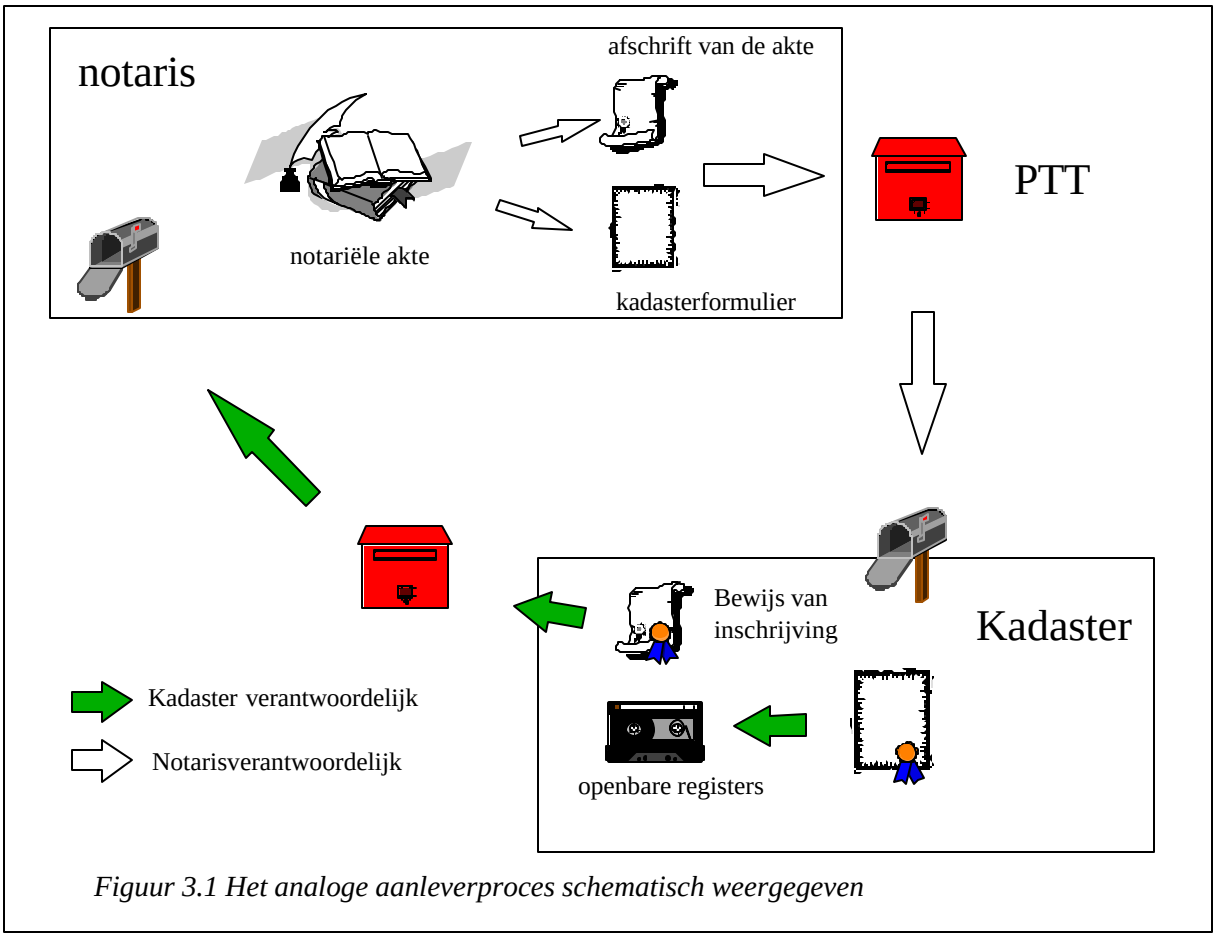
Voor het verzenden van een ontvangstbevestiging en een inschrijvingsbevestiging van het Kadaster naar de notaris is het Kadaster aansprakelijk, tenzij dit aangetekend gebeurt. Ditzelfde geldt voor het versturen van de kennisgeving uit de kadastrale registratie naar de rechthebbenden.

Notaris
De aansprakelijkheid van de notaris is in de Wet op het Notarisambt geregeld in artikel 73: “Behalve in de gevallen, waarin zulks uitdrukkelijk bij deze wet is bepaald, kunnen notarissen, indien daartoe termen bestaan, tot schadevergoeding jegens de belanghebbenden worden veroordeeld, indien de akten, voor hen verleden, uit hoofde van gebrek in den vorm in rechte nietig worden geacht of geoordeeld worden authenticiteit te missen, en verder in alle gevallen, waarin een verpligting bestaat tot schadevergoeding.”. De Wet op het Notarisambt en de Kadasterwet stellen eisen met betrekking tot de inhoud van de akte. Het vervullen van deze eisen is een taak van de notaris. Voor het nalaten of onvolledig vervullen van deze eisen is de notaris aansprakelijk. De notaris is dus aansprakelijk voor de inhoudelijke juistheid, integriteit en authenticiteit van de akte. Evenals voor de inhoudelijke juistheid, integriteit en authenticiteit van

[83] Art. 3:19 BW, art. 11 tweede lid Kw

afschriften van akten en het kadasterformulier. Dit is het rechtsgevolg van de verklaring van eensluidendheid van de notaris die door de Kadasterwet (art. 11) wordt vereist voor inschrijving van de notariële akte in de openbare registers.
Het aanbieden van het afschrift van de notariële akte aan het Kadaster is in artikel 3:89 tweede lid BW geregeld: “Zowel de verkrijger als de vervreemder kan de akte doen inschrijven”. Het aanbieden van de akte laten de rechthebbenden echter vrijwel altijd over aan de notaris. Deze zorgt dan dat de akte bij het Kadaster aankomt. De notaris is dan aansprakelijk voor het verzenden van de akte.

PTT Post
PTT Post heeft de aansprakelijkheid voor haar fouten in haar algemene voorwaarden binnen de wettelijke marges uitgesloten[84]. Alleen bij geregistreerd vervoer, verzending als postpakket, aangetekende verzending of verzending van brieven met aangegeven waarde, kan men aansprakelijk worden gesteld voor schade als gevolg van verlies, beschadiging of vertraagde aflevering. En zelfs dan is de maximale geldelijke aansprakelijkheid vastgesteld op 12.000 gulden. Voor een postzending met waarde-aangifte geldt het bedrag van de waarde-aangifte als maximum uit te keren bedrag.
PTT Post kan zich niet beroepen op een uitsluiting of beperking van zijn aansprakelijkheid voor zover schade is ontstaan uit zijn eigen handelen of nalaten, geschied hetzij roekeloos met de wetenschap dat die schade er waarschijnlijk uit zou voortvloeien (art. 7 vijfde lid Postwet).



Figuur 3.1 Het analoge aanleverproces schematisch weergegeven

[84] Zie: algemene voorwaarden voor het vervoer van postzendingen artt. 8 en 15, PTT Post 1996

3.6 Conclusies

De aansprakelijkheidsverdeling is in de huidige situatie scherp afgebakend en helder. De notaris is aansprakelijk voor de inhoudelijke juistheid van de akte en zorgt ervoor dat het Kadaster de akte volledig en ongewijzigd krijgt. Het Kadaster zorgt voor de toetsing van de akte voor inschrijving in de openbare registers en verstrekt daaruit gegevens aan derden. PTT Post is voor de normale postverzending niet aansprakelijk voor vermiste, verminkte of vertraagde postverzending.

Er zijn diverse momenten te onderscheiden waar het momenteel fout kan gaan, soms met verstrekkende gevolgen. Deze fouten komen met name voor in de verwerking van de akte. Het grootste risico dat het Kadaster loopt binnen de verwerking van de akte is het ongeautoriseerd wijzigen van het kadasterformulier of de kadastrale registratie door zijn medewerkers.
De tijd waarbinnen fouten ontdekt (kunnen) worden is kritiek voor het hele proces. De onder 3.4.4 genoemde foutendetecties kan voor wat betreft het transport van de akte enige weken duren. Ook de gesimuleerde notaris kan op zijn vroegst pas na het versturen van de ontvangstbevestiging worden ontdekt. Als de ontvangstbevestiging wordt gestuurd natuurlijk. Echter de meeste onvolkomenheden worden in de praktijk vrijwel altijd snel ontdekt. In hoofdzaak zijn het het Burgerlijk Wetboek en de Kadasterwet die voor verplichte communicatie en dus foutendetectie tussen de notaris en de bewaarder zorgen. Het kunnen toepassen van de akte in de kadastrale registratie ziet binnen het Kadaster (indirect) toe op een correcte verwerking van de akte en zorgt voor controle op de inhoudelijke juistheid van de akte.

Desondanks is het mogelijk te frauderen; het proces is zeker niet waterdicht. Dat er zo weinig fout gaat, kan enerzijds worden toegeschreven aan het wederzijdse vertrouwen tussen notariaat en Kadaster in elkaars functioneren, anderzijds aan de betrouwbaarheid van PTT Post. De factor toeval kan op deze plaats ook genoemd worden.

Het systeem kan waterdicht functioneren. De notaris moet dan persoonlijk bij het Kadaster het ingeschreven kadasterformulier binnen een tijdseenheid na inschrijving vergelijken met de door hem opgemaakte akte. Constateert de notaris geen verschil en voldoet het kadasterformulier aan de (vorm)vereisten na inschrijving dan is het zeker dat er zowel bij de PTT als bij het Kadaster geen fouten zijn gemaakt en de burger met 100% zekerheid op de openbare registers van het Kadaster kan vertrouwen. De kadastermedewerker mag daarbij natuurlijk niet frauduleus zijn.

Het feit dat het waarborgen van de rechtszekerheid van registergoederen vooral afhangt van het (dis)functioneren van kadastermedewerkers vormt een zwakke schakel in het verwerkingsproces van de notariële akte.
Het gebruik van nieuwe technieken verdient aanbeveling zodat de onzekere factor (de kadastermedewerker) beter te controleren of zelfs te vervangen is. Computertechnieken als EDI lijken een ideale oplossing om deze taak te vervullen. Voor verdere argumentatie voor invoering van EDI kan feilloos worden aangesloten bij de memorie van toelichting op de wetswijziging van 1947:

‘De woordelijke overschrijving is een werkmethode, die ten tijde van haar totstandkoming mogelijk verantwoord, toch bezwaarlijk gezegd kan worden in een meer moderne administratie te passen. Bovendien is het systeem voor den Staat oneconomisch, gezien het aanzienlijk bedrag, dat door den Staat jaarlijks aan loonen aan de zoogenaamde bladschrijvers moet worden uitbetaald’.

4. Problemen van EDI voor het Kadaster en notariaat

4.1 Inleiding

Bij EDI gaat het om het handelingen tussen computers. Er worden digitaal berichten uitgewisseld. Digitale berichten zijn vluchtige berichten: met één druk op de knop zijn ze weer verdwenen of zijn ze gewijzigd. De techniek zorgt voor de constatering van fouten in de berichtgeving en de betrouwbaarheid van de berichten op het moment van verzenden en ontvangen van het bericht.
De huidige wet- en regelgeving geeft voor de invoering van EDI een aantal problemen. Deels zijn deze problemen te wijten aan de (nieuwe) mogelijkheden die EDI biedt, deels door de specifieke eisen die voornamelijk in de Kadasterwet aan het in te schrijven stuk worden gesteld. Daarnaast is het vooral de opslag van data die de nodige juridische aandacht vereist.
In dit hoofdstuk worden de problemen die door de invoering van EDI bij het Kadaster en notariaat kunnen ontstaan besproken. De problemen die zich voordoen voor het nieuwe stuk zijn eveneens van toepassing op het bewijs van inschrijving en het bewijs van ontvangst door het Kadaster aan de aanbieder van het stuk (doorgaans de notaris) verstrekt.

4.2 Standaardisatie van akten

EDI is in paragraaf 2.1 gedefinieerd als de geautomatiseerde elektronische uitwisseling van *gestructureerde* en *genormeerde* berichten tussen *computers* van verschillende organisaties. Deze kenmerken van EDI zorgen ervoor dat er bij KANO (nog) niet van EDI gesproken kan worden.

Het Burgerlijk Wetboek en de Kadasterwet stellen een aantal randvoorwaarden waaraan niet zondermeer door EDI bij KANO voldaan kan worden.
Ten eerste laat het Burgerlijk Wetboek de vorm van overeenkomsten vrij, tenzij partijen deze overeenkomen. Een notaris mag dus een notariële akte opmaken in de door hem wenselijk geachte vorm. In dit kader bezien kan het vereisen van een inhoudelijke standaard van het digitale equivalent van de notariële akte door het Kadaster als een onredelijk vereiste worden beschouwd door de rechter.
Ten tweede stelt het Burgerlijk Wetboek dat het weigeren in te schrijven van de akte alleen door de bewaarder kan gebeuren[85]. De Kadasterwet regelt dat het de bewaarder is die inschrijft[86]. De wetten vereisen dus mensen in het verwerkingsproces bij het Kadaster. EDI vereist een elektronische bewaarder. De eisen die in de Kadasterwet aan een bewaarder worden gesteld kunnen onmogelijk door een computer worden vervuld[87] (o.a. meester in de rechten of een vergelijkbare opleiding). De bewaarder kan zijn bevoegdheden mandateren aan een computer. De computer doet het werk en de bewaarder is verantwoordelijk voor het resultaat. Maar het volledig vervangen van de bewaarder door een computer is bij de huidige wetgeving onmogelijk.

[85] Art. 3:19 BW, art. 3:20 BW
[86] Art. 7 eerste lid Kw
[87] Art. 6 tweede lid Kw

4.3 Beveiliging[88]

Beveiliging van het stuk

Een gevolg van de nieuwe techniek is dat de gegevens aangeboden aan het Kadaster door onbevoegden kunnen worden onderschept en zonder zichtbare sporen achter te laten weer worden doorgezonden. Dit roept de noodzaak tot beveiliging van de communicatie tussen partijen op.
Diverse wetten[89] [90] dwingen partijen ertoe om de communicatie te beveiligen. Beveiliging legt de drempel om de gegevens te wijzigen hoger en maakt het inbreken in het systeem bovendien strafbaar. Beveiliging kan worden gescheiden in vijf delen[91].
Ten eerste kan de beveiliging het onleesbaar maken van de stukken betekenen. Dit is noodzakelijk in situaties waar partijen er belang bij hebben dat een stuk niet bij het Kadaster wordt aangeboden. Dit is bijvoorbeeld het geval als er beslag is gelegd op een onroerende zaak. De mogelijke kennisname van de inhoud van het elektronische beslag, kan ervoor zorgen dat juist dat stuk verloren gaat door onbevoegde tussenkomst.
Ten tweede willen het Kadaster en notariaat er zeker van zijn dat alle berichten die zij versturen (stuk, bewijs van inschrijving, bewijs van ontvangst) ook daadwerkelijk aankomen. Met name de notaris wil zeker weten of het gewenste rechtsgevolg is ingetreden. De constatering van verloren of afgedwaalde berichten is een tweede vorm van beveiliging.

De openbare registers moeten de ingeschreven stukken betrouwbaar weergeven. Betrouwbare registers betekenen dat de wijze van aanbieding ook voldoende waarborgen moet bevatten om de integriteit en de authenticiteit van het in te schrijven stuk te kunnen vaststellen. De controles op de integriteit en authenticiteit zijn de derde en vierde vorm van beveiliging.
Als bijvoorbeeld een equivalent tijdens transport gewijzigd wordt of een virus aan het document toegevoegd wordt door een onbevoegde dan moet het Kadaster kunnen constateren dat het aangeboden equivalent niet eensluidend met de notariële akte wordt aangeboden.

Tenslotte kan de beveiliging van de toegang tot de systemen als beveiligingsvorm worden genoemd. Alleen de notaris mag stukken ondertekenen en moet dus als enige toegang hebben tot de systemen die zijn unieke kenmerken genereren. Het moet onmogelijk zijn dat een medewerker van de notaris zich bij het Kadaster elektronisch voor kan doen als de notaris. Hetzelfde geldt voor het onbevoegd uitgeven voor de bewaarder door bijvoorbeeld een kadastermedewerker.

Voor het bewijs van ontvangst en het bewijs van inschrijving gelden dezelfde eisen om dezelfde redenen van het waarborgen van de integriteit van de documenten en de identiteit van de afzender.

Beveiliging van de opslag

De openbare registers moeten zodanig beveiligd worden dat het onmogelijk is een stuk ongemerkt te wijzigen of te laten verdwijnen. Het wijzigen en/ of verdwijnen van de stukken kan diverse oorzaken hebben. Bijvoorbeeld door direct zichtbare oorzaken als een brand of door minder opvallende oorzaken als een kraak van de openbare registers.

Het kraken van de digitale openbare registers zal altijd mogelijk zijn. De mate en de actualiteit van beveiliging(smethoden) bepaalt op welke termijn een kraak slaagt. Het ontbreken van een afdoende

[88] Beveiliging: het onleesbaar maken van gegevens en met voldoende zekerheid de integriteit en de authenticiteit van de gegevens kunnen waarborgen teneinde misbruik van de gegevens te voorkomen en/ of te constateren.
[89] Zie paragraaf 2.2.2 Het kennis nemen van een stuk is slechts strafbaar als een beveiliging wordt doorbroken.
[90] De openbare registers en de kadastrale registratie zijn van de WPR uitgezonderd. Ook van de Wet bescherming persoonsgegevens (WBP) zullen gegevens zijn uitgezonderd als zij worden verstrekt voor de uitvoering van een publieke of wettelijke taak; Automatiseringsgids 13 februari 1998.
[91] Zie ook subparagraaf 2.3.2

beveiliging van de digitale openbare registers kan leiden tot veelvuldige kraakjes van derderangs krakers en door de kraakjes tot digitale openbare registers waar onzichtbare en (niet-) systematische fouten in zijn gezet.

4.4 Inschrijvingsvereisten

In hoofdstuk drie zijn de huidige eisen die aan het analoge stuk worden gesteld beschreven. Deze eisen zijn opgesteld voor analoge stukken en zijn niet (volledig) toepasbaar op de elektronische stukken. Het herwaarderen van de definities van stuk, verzoekschrift, afschrift, geschrift, formulier en uittreksel, getekende verklaring, getekend uittreksel en getekend afschrift zodat deze ook op digitale stukken van toepassing zijn, zou betekenen dat de Kadasterwet niet hoeft worden gewijzigd. Of dit een reële optie is natuurlijk de vraag. Aan documenten denken we inmiddels niet alleen meer aan papier maar ook, mede dankzij MS Words *.doc, aan digitale bestanden. Echter de eisen in de Uitvoeringsregeling kunnen alleen op papier van toepassing (o.a. het kadasterformulier hyp4, paginanummering). Deze kunnen niet gelden voor digitale formulieren. Dit betekent dat in ieder geval de Uitvoeringsregeling Kadasterwet 1994 aan moeten worden gepast aan het nieuwe medium.
Voor elektronische equivalenten van akten moeten dus andere (nieuwe) vereisten gelden dan voor analoge afschriften van akten[92]. Wel moeten de algemene eisen die voor het analoge stuk gelden, het integer en authentiek[93] zijn van het stuk, ook voor het nieuwe stuk gelden. Alleen de wijze waarop deze eisen technisch worden ingevuld, is anders.
De status van het nieuwe stuk zal dezelfde zijn als die van het kadasterformulier, namelijk een afschrift van de authentieke akte opgesteld op een door het Kadaster verstrekt formulier met de garantie van de notaris voor de eensluidendheid met de authentieke akte[94]. De 'digitale eensluidendheid' zal door de techniek moeten worden geconstateerd en gegarandeerd. Of zoals prof. Hidma suggereert: "De bij het Kadaster gedeponeerde (elektronische) verklaring dat hij -na raadpleging van het netwerk- de gelijkluidendheid aan de minuutakte heeft geconstateerd, kan zonder problemen een soortgelijke garantieverklaringsfunctie vervullen".

De functies die het kadasterformulier vervult, zijn samengevat: het kunnen controleren van de integriteit en authenticiteit van het stuk aangeboden aan het Kadaster ter inschrijving in de openbare registers. Voor het elektronische stuk moeten deze eisen nader worden ingevuld.

De authenticiteit van het nieuwe stuk verdient bijzondere aandacht. De Wet op het Notarisambt (oud en nieuw) stelt dat alleen de notaris afschriften mag verstrekken. De notaris is dus persoonlijk geautoriseerd om een afschrift te verstrekken. Net als een afschrift is ook alleen de notaris bevoegd om een kadasterformulier met een verklaring van eensluidendheid af te geven. Deze bevoegdheid is zichtbaar doordat de notaris het afschrift of formulier ondertekent. De (wijze van het zetten van de) handtekening wordt als uniek beschouwd. Voor het nieuwe digitale stuk betekent dit dat alleen de notaris toegang tot de automatische systemen en de beschikking over unieke codes mag hebben. Omdat de geautoriseerde (notaris, bewaarder) verantwoordelijk is voor het gebruik van zijn unieke sleutel, doet hij/ zij er verstandig aan de toegang tot de unieke sleutel zo goed mogelijk te beveiligen.

Ook de eisen die gesteld worden aan het bewijs van ontvangst en het bewijs van inschrijving kunnen in de digitale situatie niet meer worden voldaan. Deze eisen behoeven in de wet en uitvoeringsregeling eveneens aanpassing.

[92] EDI vereist aanpassing van de artt. 11, 12, 13, 14, 15 Kw en nagenoeg alle artikelen in titel 2 en titel 3 Kw en verdere uitvoeringsregelingen met betrekking tot de inschrijvingsvereisten
[93] Authentiek wil hier zeggen: het stuk is opgemaakt en ondertekend door een daartoe bevoegd persoon.
[94] De nieuwste ontwikkelingen van de wijziging van de Wet op het Notarisambt voor wat betreft het afgeven van digitale notariële afschriften zijn buiten beschouwing gelaten.

4.5 De opslag van het stuk

De openbare registers moeten blijvend reproduceerbaar zijn tot leesbare tekens met behoud van integriteit en authenticiteit. De opslag gebeurt nu op microfilm, dat zich nog maar dertig jaar heeft bewezen, maar met het gebruik van EDI is dit medium niet meer bruikbaar.
De huidige stand van zaken met betrekking tot het opslagmedium geeft echter geen uitsluitsel over de duurzaamheid van het medium. Het roesten van de WORM-plaat[95] na jaren (~100 jaar?) geeft aan dat er wellicht naar andere en/ of nieuwe technieken moet worden gezocht om een oplossing van dit probleem te vinden. Een oplossing kan ook gezocht worden in de randvoorwaarden van de opslag van dit optische medium: gedacht moet worden aan ruimten in vacuüm, waar de temperatuur, luchtdruk etc. constant is.

Naast het duurzaamheidsprobleem van het opslagmedium geven de digitale media andere problemen. Deze problemen hangen samen met de snelle technologische ontwikkelingen. Wat nu bijvoorbeeld als standaard wordt gehanteerd wordt over vijf jaar als oud bestempeld[96].
De oude stukken moeten leesbaar blijven en de controles op integriteit en authenticiteit moeten mogelijk blijven. Dit betekent dat ook de oude hard- en software moet worden bewaard. Als er bijvoorbeeld gebruik wordt gemaakt van elektronische sleutels of coderingen die de toegang verlenen tot de documenten, moeten deze sleutels of coderingen om de leesbaarheid en de authenticiteit en integriteit van het document te garanderen bewaard blijven. De beschikbaarheid en betrouwbaarheid van de randapparatuur is misschien wel de grootste onzekerheid.

Tenslotte zullen door de technologische ontwikkelingen de technieken die ‘unieke’ kenmerken aan ingeschreven stukken geven verouderen. De oude stukken zijn na verloop van tijd makkelijk te kraken. Aanpassing van de techniek voor nieuwe stukken maakt deze state of the art veilig maar zijn de oude stukken nog wel betrouwbaar?

Samengevat kan de bewaarplicht worden gescheiden in twee probleemgroepen: wat moet worden bewaard en op welk medium moet het stuk worden opgeslagen om de beschikbaarheid, leesbaarheid, integriteit en authenticiteit van het stuk blijvend te kunnen garanderen.

Consistentie van de digitale openbare registers
Het houden van digitale openbare registers heeft gevolgen voor de analoge stukken reeds opgeslagen op microfilm. Deze zullen digitaal gemaakt moeten worden door ze te scannen, te digitaliseren of imagen. Gescande kadasterformulieren en digitaal equivalenten van akten komen in één registratie terecht. Het digitaal equivalent is controleerbaar voor wat betreft de integriteit en de authenticiteit, ook bij de kadasterbalie, het gescande formulier niet.
De betrouwbaarheid van het digitale stuk is afhankelijk van de technische waarborgen en zal na verloop van tijd veranderen. Het gebruik van nieuwe technieken voor bijvoorbeeld de digitale handtekening van de notaris betekent dat er per inschrijvingsperiode andere technieken worden gebruikt en daarmee samenhangend de betrouwbaarheid van de verschillende akten per inschrijvingsperiode verschilt.
Verschillende inwinnigstechnieken zorgen ervoor dat de betrouwbaarheid van de digitale openbare registers per 'akte' verschilt.

[95] WORM-plaat staat voor Write Once Read Many-plaat; een beeldplaat die één keer wordt beschreven en daarna slechts kan worden gelezen.
[96] Wie herinnert zich nog de 5 ¼ inch floppy? Over vijf jaar herinneren we ons de 3 ½ inch diskette niet meer en over tien jaar.....

4.6 Conclusies

Het invoeren van EDI voor de elektronische aanlevering van de notariële akte heeft in de Kadasterwet haar grootste knelpunten. De Wet op het Notarisambt en de Kadasterwet stellen respectievelijk aan het afschrift en kadasterformulier de nodige (vorm)vereisten. Deze bepalingen dienen voor wat betreft het kadasterformulier te worden aangepast aan het nieuwe medium.
Verder moet ten gevolge van diverse wetgeving de communicatie tussen Kadaster en notariaat op een adequaat beveiligde wijze geschieden.
Tenslotte is het de opslag van digitale stukken die een bron van problemen is. De centrale vraag is hierbij tweeledig: wat moet worden bewaard en op welk medium moet het stuk worden opgeslagen om de beschikbaarheid, leesbaarheid, integriteit en authenticiteit van het stuk blijvend te kunnen garanderen.

5. Oplossingen voor de problemen van EDI bij het Kadaster en notariaat

5.1 Inleiding

In dit hoofdstuk zijn de eisen die gesteld worden aan de stukken voor inschrijving en de eisen voor de opslag ervan vertaald naar de digitale mogelijkheden. Op welke wijze kunnen de digitale media de analoge vervangen en hoe moet daar juridisch mee worden omgegaan zijn vragen die centraal staan in dit hoofdstuk.
De indeling van hoofdstuk 4 zal zoveel mogelijk worden aangehouden. De beveiliging en de inschrijvingsvereisten van het stuk zijn samen genomen omdat diverse technieken beide problemen tegelijk kunnen oplossen. Naast de technische oplossingen zal in 5.7 de juridische vormgevingsmogelijkheden voor de invoering van EDI worden beschreven. In 5.8 zal de mogelijke rol van een Trusted Third Party in het proces worden besproken. Besloten wordt met conclusies.

5.2 Standaardisatie van het stuk

Door standaardisatie van de berichten is het mogelijk stukken zonder tussenkomst van mensen te beoordelen op hun geschiktheid voor inschrijving. Het invoeren van standaarden kan in theorie volledig worden doorgevoerd. De standaard heeft betrekking op lay-out, de invulling van velden en het formaat van het bestand. De gewenste gegevens moeten eenduidig door de computers te interpreteren zijn. De reeds bestaande kadasterformulieren zouden als uitgangspunt kunnen worden gehanteerd bij de standaardisatie daar het voor 90% dezelfde (koop-, verkoop-) transacties betreffen. Slechts in de overige 10% zullen speciale standaarden oplossingen moeten bieden.
Het Kadaster en notariaat kunnen met elkaar overeenkomen dat het nieuwe stuk volgens een standaard wordt opgemaakt die het mogelijk maakt het nieuwe stuk automatisch te verwerken. Het Kadaster kan ook eenzijdig op uitvoeringsniveau bepalen dat voor elektronische stukken alleen volgens een bepaalde standaard kunnen worden ingeschreven. Dit is ook het geval voor het analoge kadasterformulier[97]. Een andere manier om het notariaat te stimuleren het stuk gestandaardiseerd aan te bieden is het instellen van een speciaal tarief voor het aanbieden van standaarddocumenten.

Een middag bij de bewaarderstelefoon[98] leert dat in de praktijk de inschrijvingsvereisten heel divers zijn. Ze zijn verspreid over vele wetten, per geval verschillend en zeker niet limitatief. Volledige standaardisatie zal niet mogelijk zijn; nieuwe gevallen worden ontdekt als de notaris zijn standaardvelden vult of als een inschrijving wordt geweigerd. De bewaarder zal in geval van weigering door de computer het nieuwe geval moeten beoordelen of de weigering terecht is. Standaardisatie van stukken moet tot 99% mogelijk zijn maar een Kadaster zonder bewaarder van vlees en bloed is onmogelijk.

[97] Artt. 7 eerste lid en art. 8 Uitvoeringsregeling Kadasterwet 1994 (zoals deze luidt per 29 april 1995). Art. 4 Kadasterregeling 1994 geeft invulling aan de artikelen uit de uitvoeringsregeling in bijlage 1 tot en met 3

[98] De bewaarderstelefoon is een soort helpdesk voor de kadastermedewerker in de vestiging die de toetsing van de inschrijving verzorgt. Vragen omtrent het weigeren en inschrijven van een kadasterformulier worden door de bewaarder aan de bewaarderstelefoon beantwoord.

5.3 Beveiliging van het stuk en inschrijvingsvereisten

In paragraaf 4.3 worden een vijftal verschillende eisen aan de beveiliging gesteld. De eis van integer en authentiek stuk voor inschrijving is tevens een eis die de constatering van een niet integer en authentiek stuk in zich heeft; een controle op de inschrijvingsvereisten. De beveiliging van toegang tot de systemen moet worden gezien als een garantie dat het de notaris is die het stuk heeft ondertekend. Van een authentiek stuk kan dus worden gesproken als de herkomst van het stuk bekend is en de toegang tot het systeem dat de herkomst aangeeft alleen voor de notaris mogelijk is (exclusiviteit voor de notaris).
De overige eisen zijn het onleesbaar maken van een stuk en het constateren van een verloren of afgedwaald stuk. Bestaande technieken die de eisen zouden kunnen vervullen worden besproken. Per methode wordt aangegeven aan welke criteria ze voldoen.

Aangezien zowel het aanbieden van het stuk, als het versturen van het bewijs van ontvangst en het bewijs van inschrijving aan vergelijkbare eisen moeten voldoen, wordt hier slechts de beveiliging van het stuk behandeld.

Geen beveiliging

Geen beveiliging betekent dat onbevoegden relatief gemakkelijk kennis kunnen nemen van de gestuurde informatie. Op zich is dit niet erg daar de informatie bestemd is voor de openbare registers en dus na inschrijving openbaar wordt. Echter een onbevoegde kan de informatie onderscheppen en veranderen en weer versturen. Dit is, zonder beveiliging, geen strafbare handeling (Wet computercriminaliteit).
Een onbevoegde kan zich zelfs uitgeven als notaris zonder dat het Kadaster dit weet. Slechts bij de rekeningcontrole van de gesimuleerde notaris zal de 'fout' geconstateerd worden.
De integriteit en authenticiteit zijn met deze methode onvoldoende gewaarborgd en oncontroleerbaar.

Juridisch gevolg
Het Kadaster is aansprakelijk voor het toetsen van de inschrijvingsvereisten voor inschrijving in de openbare registers. Als de mogelijkheid bestaat om onbevoegd akten aan te laten bieden, het Kadaster heeft niet voldoende kunnen vaststellen wie de akte heeft opgemaakt, en het Kadaster schrijft desondanks toch in dan heeft de bewaarder een fout gemaakt in de zin van artikel 117 Kw en is het Kadaster aansprakelijk.

Kenmerk geen beveiliging:	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
	nee	nee	nee	nee	nee

Beveiliging door een gesloten netwerk

Het verzenden van het stuk over een gesloten netwerk is een beveiliging in de zin dat de toegang tot het systeem beperkt is en daardoor de bereikbaarheid/ leesbaarheid eveneens. Dit wil niet zeggen dat er niet op ingebroken kan worden. Onbevoegden kunnen via de vele netwerken waarmee of het KNB-net of het Kadasternetwerk gekoppeld is, binnenkomen en stukken aanmaken, wijzigen en/ of onderscheppen waarvan zij de waarde (h)erkennen.
De integriteit en authenticiteit zijn met deze methode onvoldoende gewaarborgd en oncontroleerbaar.

Juridisch gevolg
Door een kraak op het gesloten netwerk bestaat het risico dat de afzender gesimuleerd wordt en dat van die mogelijkheid misbruik wordt gemaakt. Het Kadaster schrijft bijvoorbeeld een stuk in dat niet bestaat of verminkt is tijdens transport. De aansprakelijkheid ligt ook in dit geval bij het Kadaster die moet vertrouwen op de controlerende functie van het notariaat. Geeft het notariaat geen melding van een onterecht ontvangen bewijs van ontvangst, bewijs van inschrijving en/ of rekening of controleert hij/ zij het

ingeschreven stuk niet met de minuutakte dan heeft het Kadaster een probleem omdat met onvoldoende zekerheid de authenticiteit van het stuk is vastgesteld.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
gesloten net:	nee	nee	nee	nee	gedeeltelijk

Procedurele beveiliging

Tijdslimieten tussen transacties
Bij gebruik van EDI kan de notaris een werkwijze hanteren die ervoor zorgt dat binnen een bepaalde tijd na het versturen van het stuk het bewijs van ontvangst en het bewijs van inschrijving/ weigering moet zijn ontvangen. Is dit niet het geval dan wordt het Kadaster gebeld of anderszins op de hoogte gebracht.

Volgnummers voor transacties
De communicatie van notaris met het Kadaster en van het Kadaster met de notaris kan genummerd worden. Per soort bericht moet deze verschillen. Dus voor een inzage in AKR een aparte bijhouding als ook voor de verzoeken tot inschrijving. Is er een bericht kwijtgeraakt dan blijkt dit uit de niet opeenvolgende nummering die bij het Kadaster is aangeboden. Het Kadaster zal deze constatering kunnen aantekenen op het bewijs van ontvangst en wachten met inschrijving totdat er door de notaris duidelijkheid wordt gegeven.

Verevening van de berichtgeving
Per aangeboden stuk moeten twee berichten van het Kadaster richting notaris gaan: een bewijs van ontvangst van het stuk en een bewijs van inschrijving of van weigering van het stuk. Indien het inkomende bericht bij het Kadaster na verloop van een periode niet gelijk is aan twee uitgaande berichten dan is er één bericht niet verstuurd. Bij de notaris werkt het precies andersom: per uitgaand bericht naar het Kadaster moeten twee binnenkomende berichten zijn geweest. Is dit niet het geval dan is er tijdens het verzenden een bericht kwijtgeraakt.

Kenmerk. pro-	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
cedurele bev.:	nee	ja	nee	nee	nee

Call-back procedure of inbelprocedure

De call-back procedure is een vorm van identificatie van de wederpartij. Dit garandeert geenszins dat het stuk integer is overgekomen. Ook de authenticatie kan onvoldoende zeker worden gedaan. Een onbevoegde kan een notarisadres simuleren en zich als notaris uitgeven. Hetzelfde geldt voor de inbelprocedure. Het bij het Kadaster melden dat notaris X een akte wil inschrijven kan worden gesimuleerd. Authenticatie na inschrijving kan met deze methode ook niet meer plaatsvinden.
De integriteit en authenticiteit zijn met deze methode onvoldoende gewaarborgd en oncontroleerbaar.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
callback:	nee	nee	nee	nee	nee

Symmetrische beveiliging[99]

Symmetrische encryptie maakt het stuk voor onbevoegden onleesbaar en het kan slechts met een sleutel leesbaar worden. Is het stuk leesbaar dan kan met dezelfde sleutel het stuk weer worden versleuteld. De onbevoegde moet dus de sleutel hebben om te kunnen manipuleren.
Er kleven aan deze methode een aantal nadelen. Zowel het Kadaster als de aanbieder dienen te beschikken over dezelfde sleutel (en niet een andere partij zoals een TTP; hoe meer partijen de

[99] Zie voor een beschrijving van symmetrische encryptie paragraaf 2.3.2

beschikking hebben over vertrouwelijke informatie hoe meer kans er is op fraude). Het beschikken over dezelfde sleutel door twee partijen geeft de mogelijkheid om de wederpartij te simuleren.

Een tweede probleem ligt in het elkaar toesturen van de symmetrische sleutel. Tijdens het sturen kan de sleutel onderschept worden en dient er een nieuwe sleutel te worden gegenereerd. Als er een nieuwe sleutel moet worden gemaakt, wegens verbeterde technische mogelijkheden bijvoorbeeld, dan speelt iedere keer weer het probleem: komt de sleutel integer over?
Tenslotte moet het Kadaster bij symmetrisch encryptie voor iedere notaris een aparte sleutel hanteren. Dit is onpraktisch.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
symm. encrypt:	ja	nee	nee	deels	nee

Asymmetrische beveiliging[100]

Toepassing van asymmetrische encryptie op het stuk betekent dat het stuk volledig onleesbaar wordt verzonden. Dit op een zodanige manier dat alleen de ontvanger het bericht kan lezen en dat de afzender alleen de geconstateerde afzender is die het stuk kan hebben verstuurd.

Door het bericht en het digitaal equivalent van de akte met zowel de privésleutel van de aanbieder en/ of notaris en de publieke sleutel van het Kadaster is het minder eenvoudig het bericht en/ of het stuk te wijzigen. Omdat de privésleutel uniek is voor een partij, mag de andere partij bij constatering van deze sleutel er vanuit gaan dat degene die zich meldt, is wie hij zegt te zijn. De aanbieder weet zeker dat alleen het Kadaster de akte kan lezen, terwijl het Kadaster er vanuit mag gaan dat het notaris A was die de akte heeft "ondertekend".

Het onbevoegd gebruik (laten) maken van zijn privésleutel is de verantwoordelijkheid van de notaris. Voor het onbevoegd gebruik (laten) maken van de privésleutel van het Kadaster is het Kadaster aansprakelijk.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
asymm. encrypt.:	ja	nee	nee	ja	nee

Semi-asymmetrische encryptie

Semi-asymmetrische beveiliging is hetzelfde als onvolledige asymmetrische encryptie. Er wordt alleen gebruik gemaakt van identificatiefunctie van de encryptie en niet van de functie die het stuk onleesbaar maakt. De identificatie kan doordat de privésleutel van de notaris met de publieke sleutel van de notaris bij het Kadaster wordt ontsleuteld.
De publieke sleutel van het Kadaster wordt dus niet gebruikt om het bericht alleen voor het Kadaster leesbaar te maken.

Kenmerk semi-	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
asymm. encrypt.:	nee	nee	nee	ja	nee

[100] Zie voor een beschrijving van asymmetrische encryptie paragraaf 2.3.2

Beveiliging met hashwaarden[101]

Er bestaan verschillende manieren om de hashwaarde te gebruiken:

1. als identificatiemiddel
2. als integriteitscontrolegetal

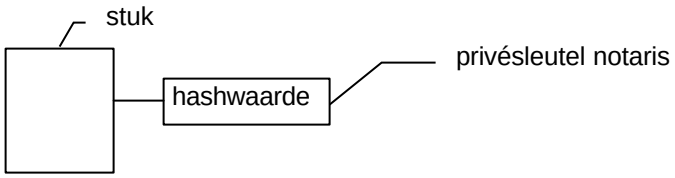
Hashwaarde als identificatiemiddel heeft het manco dat ook de symmetrische encryptie heeft: per notaris moet een hashwaardeberekening worden afgesproken en deze moet gecertificeerd en beheerd worden. Alleen gebruik maken van de hashwaardeberekening geeft nog een probleem: de hashwaardeberekening is gebaseerd op de inhoud van het document en wordt kenbaar gemaakt door een controlegetal. Dit getal zal met het stuk meegestuurd moeten worden. Als het stuk dus onderschept wordt door een onbevoegde heeft hij de beschikking over een stuk en het bijbehorende controlegetal. Enig kunst- en vliegwerk leidt tot het algoritme van de hashwaardeberekening en dus tot de mogelijkheid de notaris en/ of Kadaster te simuleren.

De hashwaarde als integriteitscontrolegetal is goed bruikbaar voor de constatering van een mogelijke wijziging van het stuk (door onbevoegde en/ of technische oorzaak). Een wijziging van het stuk leidt tot een wijziging van de hashwaarde en tot inschrijving in het register van voorlopige aantekeningen. De integriteitswaarde geeft geen garantie voor de authenticiteit van het stuk.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
hashwaarde:	nee	nee	ja	nee	nee

De hashwaarde (semi-)asymmetrisch versleuteld

Versleuteling van de hashwaarde is een mogelijkheid die voorkomt dat het hele stuk versleuteld hoeft te worden en dat er toch controle op de integriteit en authenticiteit kan plaatsvinden. Het stuk wordt verzonden naar het Kadaster met een versleutelde hashwaarde. Als de hashwaarde volledig versleuteld is, is het onmogelijk de hashwaarde te ontcijferen en het hashwaarde-algoritme te reconstrueren.
Wordt de semi-asymmetrische encryptie toegepast dan kan de onbevoegde met de publieke sleutel van de notaris de privésleutel ontcijferen en zo de hashwaarde leesbaar maken. Hij kan dan het hashwaarde-algoritme reconstrueren.



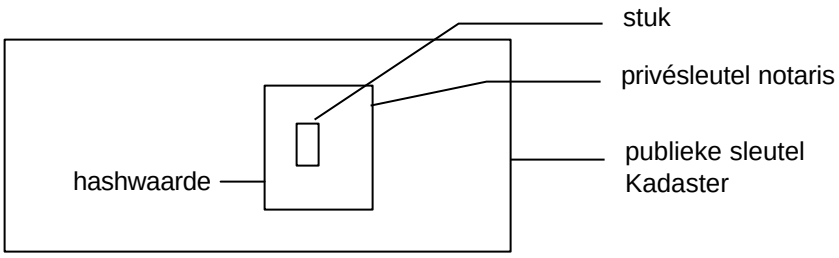
Figuur 5.1 Semi-asymmetrische versleuteling van de hashwaarde

Kenmerk hashwaarde:	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
-asymm. encryptie:	nee	nee	ja	ja	nee
-semi-asymm. encryptie:	nee	nee	ja	ja	nee

[101] Zie voor een beschrijving van hashwaarden paragraaf 2.3.3

Asymmetrische encryptie met hashwaarde gecombineerd

Een combinatie van een integriteitscontrole en asymmetrische encryptie is mogelijk.
Asymmetrische encryptie biedt de mogelijkheid om de hashwaarde 'tussen' de sleutels te versturen. Dus eerst de privésleutel over het stuk dan de hashwaarde bepalen en vervolgens de publieke sleutel van het Kadaster eroverheen. Zie het onderstaande figuur.



Figuur 5.2 Asymmetrische versleuteling van de hashwaarde

Het stuk is onleesbaar verzonden, kan alleen door de beoogde ontvanger worden gelezen en deze ontvanger kan de afzender identificeren. Door de controle van hashwaarde is de integriteit gewaarborgd.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
stuk en hw encryptie:	ja	nee	ja	ja	nee

Biometrische identificatie

De exclusiviteit van de notaris voor het verzenden van het stuk en voor de bewaarder voor de verzending van het bewijs van inschrijving en het bewijs van ontvangst kan door middel van de biometrische kenmerken van de bevoegde persoon.
Toegang tot het systeem op basis van biometrische kenmerken geeft de mogelijkheid tot het identificeren van de verzender van het bericht op persoonsniveau.
Voor de notaris die als enige is bevoegd zijn handtekening te zetten onder afschriften en digitale stukken is de biometrie een goede mogelijkheid om de exclusiviteit en daarmee de authenticiteit van het stuk te waarborgen.
Voor het verstrekken van bewijzen van inschrijving en bewijzen van ontvangst zijn door de bewaarder medewerkers gemandateerd tot het zetten van zijn handtekening(stempel). Indien per bewaarder biometrische methoden worden gebruikt kan de huidige werkwijze niet meer plaatsvinden. Alleen de bewaarder kan dan een bewijs verstrekken. De toetsing van de inschrijvingsvereisten kan de bewaarder net als in de analoge situatie overlaten aan zijn medewerkers die alleen met hun biometrische kenmerken toegang hebben tot het inschrijvingssysteem. De bewaarder blijft dan verantwoordelijk voor de toetsing door zijn medewerkrers.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
biometrie:	nee	nee	nee	nee	ja

'Kaart' als identificatiemiddel

Door speciale bevoegdheden aan een kaart te geven en deze kaart aan de bevoegden te geven kan de autorisatie tot het systeem worden geregeld. Voorbeelden van kaarten zijn de digipass en de pinpas. Het intoetsen van een code in combinatie met de kaart leidt tot de toegang tot het systeem. De kaart geeft geen garantie dat alleen de bevoegde er gebruik van maakt. De kaart als autorisatiemiddel is voor het Kadaster de meest praktische moderne invulling van de wijze waarop in de huidige situatie de bevoegdheden van de bewaarder zijn gemandateerd.

Kenmerken	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
'kaart':	nee	nee	nee	nee	ja

Alle mogelijkheden bij elkaar levert de volgende tabel op:

Methode	Onleesbaar	Verlies	Integriteit	Herkomst	Exclusiviteit
Geen beveiliging	nee	nee	nee	nee	nee
Gesloten netwerk	nee	nee	nee	nee	gedeeltelijk
Procedurele beveiliging	nee	ja	nee	nee	nee
Call back procedure	nee	nee	nee	nee	nee
Symmetrische beveiliging	ja	nee	nee	gedeeltelijk	nee
Asymmetrische beveiliging	ja	nee	nee	ja	nee
Semi-asymm. beveiliging	nee	nee	nee	ja	nee
Beveiliging met hashwaarden	nee	nee	ja	nee	nee
Hashwaarde asymm. versleutelen	nee	nee	ja	ja	nee
Asymm. om akte en hashwaarde	ja	nee	ja	ja	nee
Biometrische identificatie	nee	nee	nee	nee	ja
'Kaart'	nee	nee	nee	nee	ja

Het onleesbaar maken van een bericht kan door symmetrische of asymmetrische encryptie te gebruiken. Het constateren van een verloren of een verdwaald bericht kan met procedurele beveiliging worden geconstateerd. De integriteit van het stuk wordt door toepassing van de hashwaarde gegarandeerd. En de toegang tot de systemen kan door biometrische methoden of een kaart met unieke waarden in combinatie met het gebruik van een gesloten netwerk worden gewaarborgd.

5.4 Beveiliging van de digitale openbare registers

Procedurele beveiliging
De opslag van de bij aanbieding geconstateerde hashwaarde van het stuk is belangrijk voor de bewijspositie van het Kadaster. Als na inschrijving blijkt dat de hashwaarde niet meer overeenkomt met de eerder bij notaris en Kadaster berekende waarde dan is het digitaal equivalent van de akte (en wellicht de inhoudelijke essentialia) bij het Kadaster gewijzigd[102]. Het spreekt voor zich dat de notaris dan niet meer aansprakelijk kan worden gehouden voor inhoudelijke juistheid van het digitaal equivalent van de akte.
Wanneer de bewaarder in plaats van toetsing van het digitaal equivalent van de akte wijzigingen in het digitaal equivalent aanbrengt, dan moet dit worden geconstateerd. Als na verloop van tijd de wijziging wel

[102] Weglopen voor koffie zonder uit te loggen bijvoorbeeld kan leiden tot schade als onbevoegden (collega's) van de geboden mogelijkheid gebruik maken en op naam van de ingelogde ten onrechte digitale equivalente akten inschrijven.

wordt ontdekt dan kan door een inschrijvingsvereisten-volgsysteem[103] de bewaarder die de betreffende akte heeft getoetst worden achterhaald.
Het volgsysteem is overbodig als na de toetsing van de (vorm)vereisten wederom de hashwaarde van het digitale equivalent wordt bepaald[104]. Bij constatering van een ongewijzigde hashwaarde kan dan direct worden ingeschreven in de digitale openbare registers. Dit voorkomt dat een geconstateerd hashwaardeverschil met een technische oorzaak (duurzaamheid opslagmedia, conversies) aan het functioneren van de bewaarder wordt toegerekend.

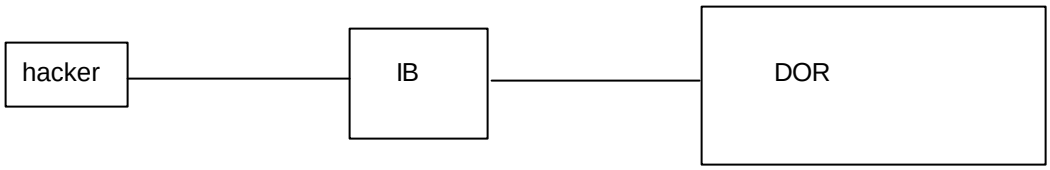
Digitaal schaduwarchief
De waarborg voor blijvende leesbaarheid van de openbare registers kan door de inschakeling van een schaduwarchief bij bijvoorbeeld het Computer Uitwijk Centrum (CUC) met meer zekerheid worden gewaarborgd. In geval van brand of andere schade aan het moedersysteem kan het schaduwarchief worden geraadpleegd.
Een andere functie die het digitale schaduwarchief kan vervullen is het kunnen opsporen van een kraak in de digitale openbare registers. De verschillen tussen de twee registraties betekenen een blootlegging van de kraak.

Ook het uitvallen van het systeem kan opgevangen worden door een instantie als het CUC. Daar zijn reeds alle kopieën van microfilms opgeslagen en zullen de digitale kopieën ook worden bewaard. Het CUC kan complete computerinfrastructuren leveren als daar behoefte aan is.

Integriteitscontrole van de digitale openbare registers
Een mogelijkheid om een wijziging in de openbare registers te kunnen constateren is het dagelijks tweemaal ('s avonds na sluiting en ś ochtends voor opening van het Kadaster) berekenen van een hashwaarde van het hele digitale openbare register. Aan het begin van de dag dezelfde hashwaarde constateren als aan het einde van de vorige dag geeft de zekerheid dat de digitale openbare registers ongewijzigd zijn gebleven.

Testen van de beveiliging
De beveiliging van het systeem kan door een hacker worden getest. Zo worden de zwakke plekken zichtbaar en kunnen dan beter beveiligd worden. Nadeel is dat de hacker inzicht krijgt in het proces en de structuur van de systemen van het Kadaster en daar zijn voordeel mee kan doen.

Geen directe communicatie met de digitale openbare registers
Tenslotte kan een kraak lastiger worden gemaakt als de kraker niet rechtstreeks met DOR kan communiceren. Een interne berichtendienst (IB) die als intermediair fungeert en verzoeken tot inzage in de digitale openbare registers beantwoord aan de klant kan dit mogelijk maken.



Figuur 5.3: een mogelijke beveiliging tegen hackers

[103] Een volgsysteem wil zeggen dat de handelingen die een bepaalde persoon doet worden geregistreerd door een computer. Deze handelingen worden vervolgens bewaard zolang men dit nodig acht. Het inschrijvingsvereisten-volgsysteem is een volgsysteem voor de toetsing door kadastermedewerkers van de inschrijvingsvereisten.
[104] Zie ook paragraaf 5.6

5.5 De opslag van het stuk

In hoofdstuk 4 hebben we gezien dat er bij de opslag twee problemen spelen: wat moet worden opgeslagen en waarop moet worden opgeslagen. De wat vraag heeft betrekking op de mogelijkheid om de integriteit en de authenticiteit te kunnen controleren. De waarop vraag heeft betrekking op de eeuwige leesbaarheid van het stuk.
Omdat de beantwoording van zowel de wat vraag als de waarop vraag afhankelijk is van de wijze waarop een stuk wordt aangeboden zullen ter beantwoording drie verschillende mogelijkheden van elektronische aanlevering en verwerking worden beschreven.

Mogelijkheid 1: het stuk met privésleutel aangeboden opgeslagen op WORM-plaat

Het stuk wordt bij de notaris op een *toepassingsonafhankelijk* formaat opgemaakt en de notaris zet zijn *privésleutel op het stuk*. Van dit geheel wordt de *hashwaarde* berekend. Het stuk met privésleutel en de hashwaarde wordt versleuteld met de *publieke sleutel* van het Kadaster.
Na inschrijving wordt het stuk met privésleutel van de notaris opgeslagen op de *WORM-plaat* van het Kadaster.

Leesbaarheid (beschikbaarheid)
Het gebruik van een toepassingsonafhankelijk formaat van het ingeschreven stuk lijkt de opslag van de hard- en software in principe overbodig te maken. Maar een toepassingsonafhankelijk formaat kan alleen naar de huidige maatstaven worden beoordeeld. De garantie dat een stuk eeuwig toepassingsonafhankelijk is en zal blijven is er niet. Daarom zal de hard- en software toch opgeslagen moeten worden.
De privésleutel van de notaris wordt op het stuk gezet. Dit betekent dat het stuk onleesbaar is, tenzij gebruik wordt gemaakt van de publieke sleutel van de notaris. Deze publieke sleutel moet dus te allen tijde bewaard blijven.
Het is op dit moment onzeker of de opslag van het stuk op de WORM-plaat duurzaam genoeg voor de digitale openbare registers is. Dit kan ertoe leiden dat over een aantal jaar (~100 jaar?) het stuk niet meer leesbaar is. Het overbrengen van de gegevens op een andere gegevensdrager is dan de oplossing. Dit moet zodanig gebeuren dat de juiste en volledige gegevens blijvend beschikbaar zijn en binnen een redelijke termijn leesbaar kunnen worden gemaakt. De gegevens op de nieuwe gegevensdrager moeten dan ook dezelfde rechtskracht krijgen als de gegevens op de oude gegevensdrager.
Het stuk is overigens tijdens verzending niet leesbaar voor onbevoegden.

Integriteit
De integriteit van het stuk wordt bepaald door de hashwaarde. De privésleutel is een onderdeel van het stuk. Een wijziging in privésleutel en/ of stuk leidt tot een gewijzigde hashwaarde.
Om deze wijziging te kunnen constateren moet de hashwaarde die is geconstateerd bij inschrijving van het stuk behouden blijven. Omdat zowel stuk als privésleutel bepalend zijn voor de hashwaarde moet naast het stuk ook de privésleutel bewaard worden.
Tenslotte moet het algoritme dat de hashwaarde berekend opgeslagen worden om eventuele aansprakelijkheden voor niet integere of onvolledige openbare registers te kunnen weerleggen. Als het algoritme niet toepassingsonafhankelijk is dan moet de hardware die de berekening mogelijk maakt ook bewaard worden.

Authenticiteit
De authenticiteit van het stuk wordt bepaald door de privésleutel van de notaris. Omdat de privésleutel alleen met de publieke sleutel gelezen kan worden moet de publieke sleutel opgeslagen worden. De leesbaarheid van de privésleutel hoeft niet door het Kadaster te worden gewaarborgd door de opslag van

de openbare sleutel. Dit kan heel goed door een derde onafhankelijke partij die ook Certification Authority (CA) is. Het Kadaster kan natuurlijk ook de rol van CA spelen en in het openbaar register de openbare sleutels bewaren.
De privésleutel moet state of the art veilig zijn. Wanneer over een aantal jaar de huidige sleutelgeneratie kraakbaar blijkt, moeten er andere sleutels worden gezocht om voldoende zeker te kunnen zijn van de authenticiteit. De oude blijven echter wel in de openbare registers.

Mogelijkheid 2: het stuk met hashwaarde aangeboden en opgeslagen op WORM-plaat

Het stuk wordt bij de notaris op een *toepassingsafhankelijk* formaat opgemaakt. Van het *stuk* wordt de *hashwaarde* berekend en om de *hashwaarde* wordt de *privésleutel* van de notaris gezet.
Het *stuk* wordt opgeslagen op *WORM-plaat* waarbij de privésleutel van de notaris wordt vervangen door de naam van de notaris.

Leesbaarheid
Ondanks het gebruik van een toepassingsafhankelijk formaat voor het stuk moeten de hard- en software die het lezen van het stuk mogelijk maken bewaard blijven.
Tijdens verzending is het stuk leesbaar.

Integriteit
De integriteit wordt bepaald door het stuk zonder privésleutel. Het stuk moet ter waarborg van de integriteit met de geconstateerde hashwaarde bewaard blijven. Wanneer een notaris de integriteit van zijn stuk in de openbare registers in twijfel trekt kan het Kadaster altijd aantonen dat het stuk dat is ingeschreven dezelfde hashwaarde had als de door de notaris meegestuurde hashwaarde.
De privésleutel is niet medebepalend voor de hashwaarde van het stuk en kan, met behoud van integriteit van het stuk, vervangen worden door de naam van de notaris.
Om in de toekomst dezelfde waarde te kunnen berekenen moet ook het hashwaarde-algoritme bewaard blijven en de soft- en hardware waarmee de berekening plaats kan vinden.

Authenticiteit
De authenticiteit van het stuk wordt bepaald door de privésleutel van de notaris. Vervanging van de privésleutel van de notaris door de naam van de notaris zorgt ervoor dat het stuk niet meer authentiek is. Een garantie van een EDP-auditor dat de conversie van privésleutel naar naam van de notaris volgens een betrouwbaar proces verloopt kan het Kadaster vrijwaren van de aansprakelijkheid voor fouten van de notaris.
Het niet opslaan van de privésleutel van de notaris kan ertoe leiden dat de notaris ontkent dat hij de akte heeft aangeboden of zelfs heeft opgemaakt. Raadpleging van de koper en/of verkoper bieden dan uitkomst voor wat betreft de opmaak van de notariële akte. Nog steeds kan de notaris de inschrijving ontkennen tenzij hij akkoord gaat met de handelwijze van het Kadaster.
De authenticiteit is met deze methode onvoldoende gewaarborgd en oncontroleerbaar geworden.

Mogelijkheid 3: analogiseren van het digitale stuk

Een andere mogelijkheid is de digitale stukken te converteren naar analoge media teneinde de duurzaamheid van de gegevens te kunnen garanderen. De betrouwbaarheid van de gegevens wordt daardoor minder dan in het digitale bestand. De controles van integriteit en authenticiteit vallen weg en de conversie op zich is wederom een bron van fouten.
Schrijft een notaris bijvoorbeeld een digitaal equivalent in waarin een hypotheekrecht van 100.000 gulden in plaats van de oorspronkelijke 1.000.000 zoals in de notariële akte wordt vermeld en wordt het oorspronkelijke bestand vernietigd met de mededeling dat notaris A is geregistreerd als notaris die de akte heeft aangeboden/ opgemaakt dan is het voor het Kadaster moeilijk aan te tonen dat de ingeschreven akte slechts 100.000 in plaats van de 1.000.000 die de minuutakte vermeldde.

Verschil digitale akte en geprinte digitale akte

De twee grote verschillen tussen de digitale en de geprinte digitale 'akte' zijn de elektronische handtekening van de notaris en de hashwaarde. De identificatie van de notaris van de geprinte akte kan niet meer. Zijn digitale handtekening is immers niet analoog te herleiden tot zijn gecertificeerde kenmerken. De notaris die de authentieke akte heeft opgemaakt en ondertekend zal daarnaast niet instaan voor fouten door de 'conversie' van digitaal naar analoog. De notaris kan dus niet aansprakelijk zijn voor de juistheid van het analoge geprinte kopie van de akte.
De microfilm met op deze wijze verkregen gegevens is dus van geen waarde zowel voor het Kadaster als voor de notaris *tenzij* de notaris na de conversie kennis neemt van de analoge openbare registers en daar constateert dat zowel zijn naam als de inhoud correct is weergegeven. En deze constatering schriftelijk bevestigt bij het Kadaster. Dit is een onpraktische situatie voor de notaris.
Een bijkomend nadeel voor een geanalogiseerd openbaar register is de verstrekking van de gegevens uit de openbare registers. Een papieren afschrift kan alleen worden gekregen indien de betreffende kadastervestiging dit aanvraagt bij het centrale microfilmarchief. De stukken worden immers centraal opgeslagen (doelstelling Kadaster: één centraal openbaar register). Vanuit dat centrale punt moet het stuk op papier worden gezet en naar de vestiging worden gefaxt. Tenslotte zal met een stempel het stuk worden gecertificeerd. Dit is geen werkbare situatie voor het Kadaster en gaat voorbij aan de mogelijkheden die de nieuwe vorm van aanbieden van het stuk biedt[105].
De meerwaarde van de microfilm zou de directe leesbaarheid van de gegevens op de film kunnen zijn[106]. Als het digitale equivalent niet meer leesbaar is kan, door raadpleging van de geanalogiseerde gegevens, via de leesbare naam van de notaris en zijn cliënten de minuutakte worden achterhaald.
Een andere reden om voor microfilm te kiezen is er als een stuk verstrekt uit de digitale openbare registers, (na een aantal jaar) gekraakt wordt en aan de digitale openbare registers van het Kadaster wordt tegengeworpen. Een houdbaarheidstermijn van de digitale handtekening van het Kadaster is echter een meer praktische oplossing.

De onderstaande tabel geeft voor de opslag aan welke kenmerken moeten worden toegekend aan de verschillende technieken.

Opslag van:	integriteits-waarborg	authenticiteits-waarborg	beschikbaarheid/ leesbaarheid van het stuk
toepassingsonafhankelijk formaat	-	-	X
integriteitsalgoritme (met soft- en hardware)	X	-	X
publieke sleutel (met software)	-	(X)	X
geen privésleutel notaris bewaren	-	-	X
stuk zonder integriteitswaarde	-	-	X
stuk met alleen integriteitswaarde	X	-	X
stuk met alleen privésleutel	-	X	-
stuk met privésleutel en integriteitswaarde	X	X	-
analogiseren stuk daarbij de privésleutel notaris vervangen door letters	-	-	X
Opslag op:			
WORM optische schijf	X	X	(X?)
microfilm	-	-	(X)

[105] Zie ook paragraaf 5.6
[106] Argumenten voor de microfilm als het moment dat een bom op het Kadaster en op het digitaal schaduwarchief de openbare registers vernietigd zijn niet realistisch. Het microfilm archief kan ook door een bom worden getroffen en het notariskantoor evenzeer.

5.6 Verstrekken van informatie uit de openbare registers van het Kadaster

Het Kadaster is aansprakelijk voor alle vergissingen, verzuimen, vertragingen of andere onregelmatigheden van zijn ambtenaren bij het houden van de registers of bij het opmaken of afgeven van afschriften, uittreksels en getuigschriften, art. 117 tweede lid Kw[107].

Het Kadaster is kortom aansprakelijk voor de gegevens die zij uit de openbare registers verstrekt. Om er zeker van te zijn dat de gegevens na de inschrijving niet gewijzigd zijn, kan voor de verstrekking van de gegevens de integriteit nogmaals worden bepaald. Komt deze hashwaarde overeen met de hashwaarde die de notaris in eerste instantie en het Kadaster nogmaals bij de inschrijving heeft geconstateerd dan kunnen de gegevens worden verstrekt. Het moet wel mogelijk zijn om de integriteit van het stuk te bepalen.
Deze handelwijze voorkomt dat frauduleuze medewerkers of hackers ongemerkt een wijziging op de akte kunnen aanbrengen. De kans dat er onjuiste gegevens worden verstrekt is hiermee nihil geworden.
Voor het verstrekken van gecertificeerde afschriften uit de digitale openbare registers moet het Kadaster gebruik maken van de privésleutel. De afgegeven afschriften kunnen, vanwege de snelle technologische ontwikkelingen en de daardoor grotere kraakbaarheid van de sleutel, slechts een beperkte tijd geldig zijn.

Een integriteitscontrole bij het verstrekken van de gegevens aan 'klanten' geeft het Kadaster een controle dat de akte ongewijzigd is gebleven en kan de garantie van de volledigheid van de gegevens met (nog) meer zekerheid worden gegarandeerd. Ook als ‘klanten’ op een analoog medium de gegevens verstrekt willen krijgen kan de bovengenoemde werkwijze worden gehanteerd. Nadat de hashwaardecontrole is doorlopen kan het stuk bij de kadastervestiging worden geprint en worden voorzien van een handtekeningsstempel van de bewaarder.

5.7 Juridische vormgevingsmogelijkheden EDI

De wijze waarop een stuk wordt aangeboden maakt voor het Kadaster in principe niet uit. Pas op het moment dat het stuk in ontvangst wordt genomen door het Kadaster wordt het interessant voor het Kadaster. Voldoet het stuk aan de inschrijvingsvereisten, dan wordt het ingeschreven, voldoet het niet dan wordt inschrijving geweigerd.
De aanbieder heeft belang bij een zo betrouwbaar mogelijke communicatie. Als het stuk bijvoorbeeld niet integer door het Kadaster wordt ontvangen, dan volgt boeking in het register van voorlopige aantekeningen en dat kost de aanbieder geld.
Ook het Kadaster heeft belang bij een betrouwbare communicatie. Het moet het bewijs van ontvangst en het bewijs van inschrijving naar de aanbieder zenden. Als daar door onbevoegden wijzigingen op worden aangebracht dan moet de aanbieder dat kunnen constateren. Ook zal de aanbieder zekerheid willen hebben wie de afzender van zowel het bewijs van ontvangst als inschrijving is geweest: is dit het Kadaster of een onbevoegde?
Verder kan het zijn dat door een technische storing bij één der partijen een fout optreedt in het stuk zodat dit niet kan worden ingeschreven, ofwel wettelijk in het register van voorlopige aantekeningen worden geboekt. Dit is niet wenselijk.
Om dit soort onduidelijkheden juridisch te regelen staan het Kadaster als ZBO drie wegen open: de wet, het Interchange Agreement of een vergunningsstelsel.

[107] Aan de wet moet worden toegevoegd: en andere gegevensdragers.

Wet

Het Kadaster en het notariaat voeren een bij wet opgelegde taak uit. In het Burgerlijk Wetboek, de Kadasterwet en Wet op het Notarisambt worden zaken als het verzenden van een ontvangstbevestiging, de authenticiteit van het aangeboden stuk, de verwerking van het stuk bij het Kadaster en het registreren van het stuk in de openbare registers geregeld. De wettelijke basis van de inschrijving kan niet voor elektronische inschrijving verloren gaan. De eisen die aan het document en aan het proces in de wetten worden gesteld, kunnen niet door een bepaling in bijvoorbeeld een Interchange Agreement worden vervangen.

De inschrijvingsvereisten die de rechtszekerheid moeten waarborgen, moeten dus bij wet en uitvoeringsregeling worden geregeld. In de wet moet het elektronisch aanleveren van een stuk mogelijk worden gemaakt. Bij uitvoeringsregeling moet de nieuwe invulling van de huidige eisen van het stuk (de integriteit en authenticiteit) worden geregeld. Ook zal het formaat van het stuk in de uitvoeringsregeling moeten worden beschreven.

De wijze waarop de aanbieding van een elektronisch stuk plaatsvindt, kan bij uitvoeringsmaatregelen juridisch worden geregeld. Het Kadaster hoeft geen overleg te voeren met individuele aanbieders over de voorwaarden waaraan de aanbieder moet voldoen en er hoeft geen register van bijvoorbeeld vergunninghouders worden bijgehouden. Conflicten kunnen alleen door een rechter worden opgelost, ook conflicten met een technische oorzaak.

Iedereen kan elektronisch aanbieden als voldaan wordt aan de eisen die aan het elektronische stuk worden gesteld.

Eisen aan de beveiliging van de communicatie, aan de applicatie van de aanbieder en aan het netwerk waarlangs aangeboden kan worden, kunnen echter niet aan de aanbieder worden opgelegd. Dit kan ertoe leiden dat zeer veel aanbiedingen technisch afgekeurd worden en/of dat de brievenbus van het Kadaster wordt vervuild met onzinnige aanbiedingen. Daarnaast is er, bij de huidige onzekerheid over de status van TTP's, voor het Kadaster de onzekerheid omtrent de identiteit van de aanbieder en de controlerende rol van de notaris in het geheel.

Interchange Agreement

Het Interchange Agreement is een overeenkomst tussen twee (of meer) partijen. Beide stemmen in met de overeengekomen voorwaarden. Per partij zal het Kadaster moeten onderhandelen over de voorwaarden. Partijen kunnen natuurlijk ook een vertegenwoordigende partij, bijvoorbeeld de KNB, machtigen om namens hen te onderhandelen. De voorwaarden kunnen per individuele aanbieder worden aangepast hoewel men zal moeten handelen naar het gelijkheidsbeginsel. Voor het wijzigen van de voorwaarden zullen de partijen veelvuldig overleg voeren.

Als een partij zich niet houdt aan de voorwaarden van het Interchange Agreement zullen in de voorwaarden eveneens de sancties daarop worden vermeld. Dit kan voor de aanbieder de intrekking van de bevoegdheid tot het aanbieden van elektronische stukken inhouden. Het Kadaster kan in een Interchange Agreement worden verplicht een schadevergoeding te betalen aan aanbieders als bijvoorbeeld de inschrijving vertraagd verloopt.

Indien het Kadaster een bepaalde aanbieder weigert te accepteren kan het besluit van het bestuur van de Dienst altijd worden aangevochten bij de bestuursrechter. Deze zal het besluit van het bestuur toetsen aan de algemene beginselen van behoorlijk bestuur.

Voor het gebruik van het Interchange Agreement is geen wettelijke basis nodig; wilsovereenstemming tussen de partijen is voldoende om gebruik te maken van het Interchange Agreement.

Het Interchange Agreement kan worden gebruikt voor de wijze waarop de aanbieding van de stukken aan het Kadaster moet plaatsvinden. In de voorwaarden kunnen zaken als wijze van en niveau van beveiliging, eisen aan de applicatie van de aanbieder en procedures wat te doen als een inschrijving niet kan plaatsvinden, worden geregeld. Door het aanbieden alleen mogelijk te maken over een gesloten netwerk wordt voorkomen dat de brievenbus van het Kadaster vervuild wordt met onzinnige aanbiedingen.

Ook kunnen voorwaarden worden opgenomen die verbonden zijn met de mogelijkheden van het nieuwe medium. Het 24 uur per dag openstellen van de postbus van het Kadaster bijvoorbeeld voor de aanbieding van de stukken. De voorwaarden bieden tevens mogelijkheden om meerdere akten tegelijk bij het Kadaster aan te bieden.

Het Interchange Agreement biedt de mogelijkheid om een andere wijze van afhandeling van conflicten te kiezen dan gebruikelijk is. Dit wil zeggen dat men af kan spreken een onafhankelijke derde bij conflict in te schakelen of zelfs al in te schakelen voor de registratie van de berichtgeving. Zie verder onder TTP.
Een ander voordeel van een Interchange Agreement is de bekendheid van de identiteit van de aanbieder. Zonder gebruik te hoeven maken van de bekrachtiging van de identiteit van de aanbieder door een TTP wordt de aanbieder herkend en wordt de ontvangstbevestiging en het bewijs van inschrijving 'teruggeëdit'.

Het Interchange Agreement stelt voorwaarden aan het aanbieden van de stukken. Daarom kan het gebruik van een Interchange Agreement voor het aanbieden van stukken aan het Kadaster in strijd zijn met artikel 3:89 BW. Deze stelt dat zowel vervreemder als verkrijger de akte kan doen inschrijven.
De gang van zaken in de praktijk is echter dat niet de in de Wet genoemde vervreemder of verkrijger maar de notaris de stukken namens cliënten aanbiedt. In de Wet staat ook niet vermeld hoe de vervreemder en verkrijger de stukken moeten of kunnen aanbieden.

Een Interchange Agreement biedt voldoende mogelijkheden om de wijze waarop de aanbieding van elektronische stukken aan het Kadaster moet voldoen juridisch te kunnen regelen. De wijze waarop de stukken in de huidige situatie worden aangeboden, rechtvaardigen het gebruik van en Interchange Agreement voor de aanbieding.

Vergunningsstelsel
Het verlenen van een vergunning heeft een wettelijke basis nodig. Een vergunning voor de elektronische aanbieding van stukken kan worden verleend als de Kadasterwet daar een mogelijkheid voor biedt. Dat is (nog) niet het geval. De mogelijke voorwaarden behorend bij de vergunning hebben op dezelfde zaken betrekking als de voorwaarden in een Interchange Agreement. De voorwaarden zijn echter voor alle partijen gelijk.
In vergelijking tot het Interchange Agreement heeft het vergunningsstelsel het voordeel dat de voorwaarden eenzijdig kunnen worden opgelegd en veranderd. Om voldoende draagvlak voor de elektronische aanbieding te krijgen zal het Kadaster desondanks veelvuldig met in ieder geval de KNB overleggen over de voorwaarden.
Verder kan met de vergunning relatief snel de bijbehorende voorwaarden worden veranderd, zonder daarvoor overleg te voeren met gebruikersgroepen etc. van het Kadaster. Voldoen de technische specificaties niet meer dan kunnen deze in de voorwaarden van de vergunning worden bijgesteld.
De nadelen van het Interchange Agreement gelden voor het overige eveneens voor het vergunningsstelsel.

De eisen aan de stukken moeten overeenkomstig de huidige analoge situatie bij wet worden geregeld. Voor de juridische vormgeving van de wijze van aanbieding van elektronische stukken aan het Kadaster is het Interchange Agreement of vergunningsstelsel geschikt.
Hoewel het BW[108] aangeeft dat "zowel verkrijger als vervreemder kan de akte kan doen inschrijven" zal door het benodigde contract of vergunning voor elektronische aanlevering zowel voor verkrijger als vervreemder dit niet mogelijk zijn. De notaris zal worden gemachtigd de inschrijving in de openbare registers te verzorgen. In de praktijk is het zeldzaam dat iemand anders dan de notaris de akte doet inschrijven. Het Kadaster heeft ook nu zijn systemen gebaseerd op het aanbieden van het stuk door de notaris: hij/ zij krijgt immers de rekening van de inschrijving en niet de verkrijger of vervreemder die de akte doet inschrijven. En ook het bewijs van ontvangst en het bewijs van inschrijving worden naar de notaris gestuurd ongeacht de aanbieder.
Hoewel in theorie iedereen kan aanbieden zijn de gevolgen van de aanbieding altijd voor de notaris. Bij gevolgen moet hier gedacht worden aan de aansprakelijkheid doordat stukken niet of te laat worden ingeschreven doordat niet wordt voldaan aan de inschrijvingsvereisten. In principe verandert er voor de verkrijger en vervreemder niets in vergelijking tot de analoge situatie.

[108] Zie art. 3:89 eerste lid BW

Het is gezien de ervaringen in de praktijk niet onredelijk de notaris (of een andere aanbieder) met vergunning of Interchange Agreement het exclusieve recht te geven van elektronische aanbieding.

5.8 Trusted Third Party

Het belang van een Trusted Third Party (TTP) voor de bewijslast is in 2.4 al aangegeven. Een TTP kan bij het Kadaster en notariaat een aantal functies vervullen. De voornaamste functies hebben betrekking op de controle op de berichtgeving en de registraties van de communicerende partijen. De controle kan bestaan uit het constateren dat een bericht is verzonden en ontvangen, maar kan ook een controle van integriteit van het bericht en identiteit van de afzender inhouden. Daarnaast kan de TTP als arbiter fungeren. In het algemeen kunnen de functies van sleuteluitgever en -beheerder en het waarmerken van de elektronische transacties worden genoemd.

TTP voor controle op het transport van het document
Als de notaris een bericht heeft verstuurd en het Kadaster ontkent de ontvangst van dat bericht dan kan de registratie van een TTP aantonen dat de notaris een bericht heeft verstuurd maar dat dit bericht inderdaad nooit in het bezit van het Kadaster is gekomen of dat het Kadaster het bericht wel heeft ontvangen[109]. Vice versa geldt voor de ontvangstbevestiging en andere berichtgeving richting aanbieder hetzelfde. Door de TTP is er zekerheid voor de partijen dat beide partijen voldoen aan verzend- en ontvangstvoorwaarden en dat de constatering dat een bericht is afgedwaald niet afhankelijk is van de constatering van één der partijen.
Het belang dat het Kadaster heeft in het ontkennen van een ontvangen bericht is niet aanwezig. De rol van de TTP is voor de controle op het transport alleen voor de notaris van belang. Met de TTP kan notaris A aantonen dat een bericht is verzonden richting Kadaster maar nooit is aangekomen. Als intussen een andere notaris (B) een digitaal equivalent betreffende de overdracht van hetzelfde perceel aanbiedt, lijdt de cliënt van notaris A schade door een technische fout van de netwerkleverancier of de tussenkomst van een hacker. De TTP kan de notaris vrijwaren van fouten maar er niet voor zorgen dat zijn digitaal equivalent met terugwerkende kracht wordt ingeschreven omdat het Kadaster het digitaal equivalent niet heeft ontvangen en dus het tijdstip van aanbieding niet heeft kunnen vaststellen.

TTP als controle op de integriteit en identiteit van het bericht
Een TTP kan naast het registreren dat een bericht ontvangen cq. verzonden is ook de bevoegdheid krijgen integriteit van het bericht en de identiteit en de afzender van het bericht te controleren. Dit kan tot de constatering leiden dat de soft- of hardware van Kadaster of notaris niet goed functioneert. De TTP bepaalt de hashwaarde van de bericht en de notaris en het Kadaster hebben hetzelfde gedaan. Komen de hashwaarden van Kadaster en notariaat overeen dan kan de verwerking van het digitaal equivalent van de akte verder gaan. Als dit niet zo is dan kan de hashwaarde van de TTP aangeven waar de foute berekening is gemaakt. Als het Kadaster het integriteitsalgoritme verkeerd heeft gebruikt en dus ten onrechte een stuk als niet correct beschouwd, kan de TTP de notaris gelijk geven en verdere fouten van het Kadaster voorkomen. Het Kadaster moet in dit geval het tijdstip van aanbieding handhaven.

Aangezien alle notarissen met hetzelfde algoritme de integriteit verzekeren en het Kadaster daarom ook alleen ditzelfde algoritme ter controle gebruikt, zal bij een verkeerde toepassing van het algoritme door het Kadaster het aantal technische afkeuringen gelijk zijn aan het aantal aangeboden stukken. Als dit het geval is, zal het duidelijk zijn dat het Kadaster 'iets' verkeerd doet en zal men maatregelen nemen. Voor de constatering van een foute berekening bij het Kadaster is een TTP niet noodzakelijk.

TTP als controle op de betrouwbaarheid van de openbare registers

[109] Dit wordt de non-repudiation functie van de TTP genoemd. Non-repudiation houdt in dit geval in het niet kunnen ontkennen van de verzending of de ontvangst van een bericht.

De redenering voor de integriteit van de berichten en identiteit van de afzender gaat ook op voor de registratie van de berichten. Een TTP kan de uitgewisselde berichten voor onbepaalde tijd registreren. Bij een conflict over de aansprakelijkheid van de juistheid van de gegevens in de openbare registers kan de registratie van de TTP een beslissende rol spelen. Is er bijvoorbeeld twijfel of notaris A of notaris B de akte heeft opgemaakt dan kan de registratie van de TTP hierover uitsluitsel geven. In dit geval moet de TTP naast het bericht ook de digitaal equivalenten van akten controleren op identiteit van de notaris en integriteit van het document en de documenten met het resultaat van de controles opslaan. Als na inschrijving van een digitaal equivalent van een akte de TTP de registeridentificatie van het Kadaster krijgt kan het ook fungeren als schaduwarchief van het Kadaster.

De registratie van de digitale equivalenten van akten door een TTP kan van pas komen indien de hashwaarde van een digitale equivalent niet meer overeenkomt met de bij het digitaal equivalent vermelde waarde. Deze controle heeft echter slechts betrekking op de digitale registratie (DOR) van het Kadaster zelf. Het Kadaster is aansprakelijk voor vergissingen, verzuimen, vertragingen of andere onregelmatigheden van zijn ambtenaren gepleegd bij het houden van de registers of bij het opmaken of afgeven van afschriften, uittreksels en getuigschriften (art. 117 tweede lid Kw). Een TTP als controle-orgaan voor de interne controle van de digitale openbare registers is daarom niet noodzakelijk. Het Kadaster kan ook zelf een schaduwarchief creëren en beheren.

TTP als beheerder en certificeerder van sleutels en algoritmen
Een TTP kan de functie van sleuteluitgever, -beheerder en -certificeerder vervullen. Als het Kadaster of notaris een bericht niet (meer) kunnen lezen doordat ze de verkeerde sleutel gebruikt hebben of de sleutel van de wederpartij niet kunnen vinden, kan de TTP er zorg voor dragen dat de vermiste sleutel in het bezit komt van één der partijen. De certificeerfunctie van de TTP geeft partijen de mogelijkheid de identiteit van de partner te controleren.
Bij het elektronisch aanleveren hangt veel zo niet alles af van het functioneren van de integriteitscontrole. Het algoritme waarmee de controle gebeurt mag nooit verloren gaan. De TTP kan het algoritme bewaren en als dat nodig blijkt verstrekken aan partijen.

Deze functie is zowel voor het Kadaster als de notaris van essentieel belang. Het registreren en certificeren van de privé-sleutel en de publieke sleutel en het bewaren van de controle-algoritmen door een onafhankelijke partij bevordert de rechtszekerheid van het elektronisch aanleveren.

5.9 Conclusies

De meeste problemen die in hoofdstuk 4 zijn geschetst kunnen technisch worden opgelost. De standaardisatie van de stukken zal voor 99 van de 100 stukken mogelijk zijn. Voor 1% van de inschrijving van de stukken zal een bewaarder van vlees en bloed noodzakelijk blijven.

Beveiliging en inschrijvingsvereisten van stukken
De invulling van de algemene eisen van de stukken voor inschrijving in de openbare registers kan voor wat betreft de integriteit door de hashwaarde techniek worden gedaan.
De authenticiteit kan door toepassing van asymmetrische encryptie in combinatie met de beveiliging van de toegang tot de systemen die de asymmetrische encryptie mogelijk maken. De beveiliging van de toegang kan met de pinpas zoals die nu gebruikelijk is maar zal wanneer de techniek dit toelaat voor de notaris moeten worden vervangen door de toegang op basis van biometrische kenmerken.
Zowel door symmetrische als asymmetrische encryptie maken de stukken onleesbaar tijdens communicatie. Alleen de procedurele beveiliging, bijvoorbeeld volgnummers op stukken of een beperkte tijdsduur tussen het verzenden en het ontvangen van een stuk, kan een verloren of afgedwaald bericht constateren.

Het gebruik van een gesloten systeem voor de communicatie tussen Kadaster en aanbieder is noodzakelijk omdat dan het systeem beperkt toegankelijk is en eventuele onbevoegden meer moeite moeten doen om met het Kadaster of notaris te kunnen communiceren.

De veiligste en betrouwbaarste technische invulling van de juridische eisen aan het stuk zijn de volgende:

- gebruik van een gesloten systeem Kadaster-aanbieder
- gebruik van de hashwaarde voor de integriteitscontrole
- gebruik van asymmetrische encryptie voor de herkomst van het stuk en de onleesbaarheid tijdens verzending
- gebruik van biometrische kenmerken voor de toegang tot de systemen
- gebruik van procedurele beveiliging voor de constatering van een verloren of afgedwaald stuk

Opslag
De akte moet conform de bewaarplicht duurzaam opgeslagen worden. Microfilm heeft zich ruim dertig jaar bewezen, maar kan niet worden gebruikt. Met de conversie van digitaal naar analoog gaan namelijk ook gegevens verloren die de integriteit en de authenticiteit van het stuk garanderen.
De WORM-plaat met waarborgen voor integriteit en authenticiteit heeft zich echter niet bewezen en kan door zijn kwetsbare fysieke gesteldheid ook voor rechtsonzekerheid op lange termijn zorgen (~100 jaar).

Het behoud van de controles op integriteit en authenticiteit leidt ertoe dat de gegevens en de soft- en hardware die nu deze controles mogelijk maken moeten worden bewaard. Dit zijn de privésleutel van de notaris, de publieke sleutel van de notaris, de hashwaarde geconstateerd bij inschrijving, het hashwaarde-algoritme en het digitale equivalent. Een toepassingsonafhankelijk formaat van het digitale stuk maakt de opslag van hardware en software in principe overbodig, echter de software die de integriteit en authenticiteit van het stuk controleert, moet behouden blijven.
Het bestaande analoge schaduwarchief moet ter waarborg van de betrouwbaarheid van de digitale openbare registers worden aangevuld met een digitaal schaduwarchief.

Juridische vormgeving
De inschrijving van een akte op een nieuw medium moet in de Kadasterwet mogelijk worden gemaakt. De nieuwe vormvereisten moeten in de uitvoeringsregeling van de Kadasterwet worden geregeld. Aanpassing van de Wet op het Notarisambt is niet nodig.
Voor de beveiliging van de communicatie, de conflicthantering en de mogelijkheid om meerdere stukken tegelijk bij het Kadaster aan te bieden kan contractueel of in vergunningsvoorwaarden worden geregeld. De vergunning heeft als voordeel ten opzichte van het contract dat het Kadaster eenzijdig de voorwaarden kan aanpassen.
De huidige gang van zaken voor wat betreft het aanbieden van een stuk bij het Kadaster rechtvaardigt de beperking van het aantal aanbieders door de aanbieding afhankelijk te stellen van een contract of vergunning verleend door het Kadaster.

De mogelijke rol van een TTP

Een TTP bij het elektronisch aanleveren van de notariële akte bij het Kadaster door notaris(kantoor) is van groot belang voor de registratie van openbare sleutels van de notarissen en Kadaster en de algoritmen die gebruikt gaan worden voor de bepaling van de identiteit van de afzender en de integriteit van het digitale equivalent van de akte. De controle van de integriteit van het digitale equivalent en identiteit van de aanbieder, notaris en bewaarder door een TTP is mogelijk maar niet noodzakelijk. Dit geldt eveneens voor het digitale schaduwarchief dat een controle op de digitale openbare registers kan zijn. Het Kadaster kan, gelet op de aansprakelijkheid, ook zelf zorg dragen voor deze ‘interne’ controle.

6. Elektronisch aanleveren en inschrijven van het digitale equivalent van de notariële akte bij het Kadaster

6.1 Inleiding

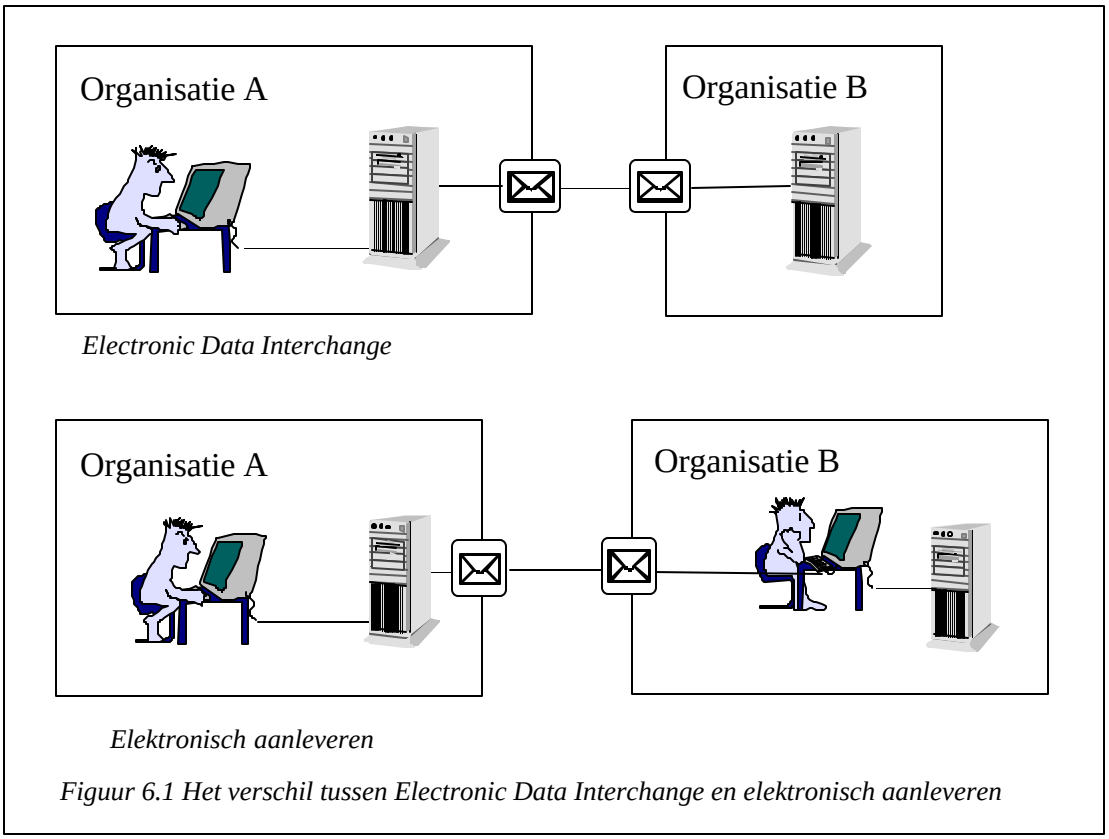
Dit hoofdstuk bespreekt de plannen zoals die op dit moment de werkgroep Elan voor ogen staan. In 6.2 zal het project Elan worden besproken. Het digitale aanleverproces en de daaruit voortvloeiende foutenbronnen en de detectie van de fouten worden behandeld en als daar aanleiding voor is geanalyseerd. De beveiliging,de nieuwe inschrijvingsvereisten en de juridische invulling van de nieuwe techniek komen aan de orde.
In dit hoofdstuk zal verder duidelijk worden dat elektronisch aanleveren in weinig opzichten verschilt van EDI en dat de problemen van EDI ook voor het elektronisch aanleveren van de notariële akte gelden.

6.2 Elan

De elektronische aanlevering van akten bij het Kadaster wordt onderzocht door de projectgroep Elan.
Elan bestaat uit een stuurgroep en een projectgroep. De stuurgroep stuurt het project aan en onderhoudt direct contact met de Koninklijke Notariële Beroepsorganisatie. Dit gebeurt in de landelijke werkgroep elektronisch aanleveren. Zo wordt het nodige draagvlak voor het project bij de vertegenwoordiging van de notarissen gecreëerd.
De projectgroep houdt zich met de inhoudelijke invulling van het project bezig. Het project startte in april 1997 en heeft in september 1997 een eerste tussenpunt bereikt. Op basis van Rapid Application Development en Timeboxing heeft men een processchema, een processimulatie, informatie-analyse, een beveiligingsconcept en een digitaal kaartje gemaakt.

Elektronisch aanleveren van de notariële akte [1] EDI

In het project Elan wordt uitgegaan van elektronisch aanleveren en verwerken van de notariële akte. Dit is niet hetzelfde als het gebruik maken van EDI. Het verschil tussen het elektronisch aanleveren en verwerken bij het Kadaster en EDI zit in de inzet van mensen. Bij EDI gaat het om gestructureerde en genormeerde berichtenuitwisseling en -verwerking tussen computers van verschillende organisaties. Bij elektronisch aanleveren gaat het om zoveel mogelijk gestructureerde communicatie tussen computers van verschillende organisaties. De notaris is vrij de akte en dus ook het digitale equivalent van de akte in een opmaak te maken die hij wenselijk acht. Bij het verwerken van het elektronische bericht bij het Kadaster wordt gebruik gemaakt van mensen. De problematiek die speelt bij EDI (zie hoofdstuk 2) gaat ook op voor het elektronische aanleveren en verwerken bij het Kadaster. Zie ook figuur 6.2 voor het verschil tussen elektronisch aanleveren en EDI.
In het algemeen kan men zeggen dat het elektronisch aanleveren het gehele proces van aanleveren, verwerken en opslaan van het digitale equivalent van de stukken overziet. Daarbij wordt het geheel ondersteund door de herkenningstechnologie voor de kadastrale toepassing, de werkstroombesturing en het portaalsysteem voor het ontvangen van het digitale equivalent van de notariële akte.



Figuur 6.1 Het verschil tussen Electronic Data Interchange en elektronisch aanleveren

De doelstellingen van Elan bestaan uit een kerndoelstelling, een aanpalende doelstelling en een plan van aanpak[110].

De kerndoelstelling is een geheel elektronische verzending en ontvangst te realiseren van akten in digitaal formaat, met inachtneming van afdoende borging voor beveiliging op de vlakken identificatie en integriteit. Daarbij wordt expliciet aandacht besteed aan de procedurele aspecten die daar mee te maken hebben, en de elektronische communicatie tussen de individuele notariskantoren en het Kadaster.
Een aanpalende doelstelling is te onderzoeken wat de mogelijkheden zijn om het Notariaat in staat te stellen op een gebruiksvriendelijke en simpele manier grenzen voor het Kadaster aan te geven en mee te sturen met de digitale akten.
Daarnaast wordt een plan van aanpak opgesteld om een pilot uit te voeren waarin de vastgestelde procesgang en bijbehorende voorgestelde systemen kunnen worden uitgeprobeerd. Dit onderdeel *PvA voor ELAN-pilot* is tevens eindpunt van dit project.

Functionaliteit
In het stappenplan KVS wordt de beoogde functionaliteit van het elektronisch aanleveren beschreven. Uitgangspunten voor de functionaliteit van het elektronisch aanleveren zijn:
- de akten kunnen voldoende beveiligd via het netwerk worden aangeleverd
- het bewijs van ontvangst wordt automatisch teruggezonden
- een bewijs van inschrijving wordt na beoordeling van de akte eveneens geautomatiseerd teruggezonden
- de elektronische akten worden automatisch voorzien van een identificatienummer
- de akten worden opgeslagen in een documentair informatiesysteem. In een eerste fase van een procesdatabase wordt de status van de akten bijgehouden

In de planning wordt 1 oktober 1998 als streefdatum voor elektronisch aanleveren genoemd. Aangezien de Kadasterwet voor het elektronisch aanleveren geschikt moet worden gemaakt, wordt op dit moment uitgegaan van een operationeel elektronisch aanleveren in 1999. In de eerste helft van 1999 moeten de akten digitaal op de werkplek aanwezig zijn. Gerekend vanaf de start van het project (april 1997) tot het einde van de planning leert dat binnen een tijdsbestek van ongeveer twee jaar het elektronisch aanleveren van de notariële akte bij het Kadaster operationeel zal zijn.

6.3 Het elektronisch aanleverproces

6.3.1 Beschrijving van de partijen bij de aanlevering

De bij de elektronische aanlevering betrokken partijen zijn het Kadaster en de notaris. Daarnaast is het de KNB die als gesprekspartner van het Kadaster in de landelijke werkgroep elektronisch aanleveren optreedt namens haar leden. In het digitale aanleverproces heeft men verder te maken met een netwerkleverancier, een softwareleverancier, eventueel een service-provider en een hardware-leverancier.
De juridische positie van de partijen die zorg dragen voor de totstandkoming van de verbinding tussen Kadaster en notaris is afhankelijk van het afgesloten contract of de voorwaarden van de vergunning. Dit hangt mede samen met hoe de aansprakelijkheid van partijen als netwerkleveranciers contractueel is ingeperkt.
De notaris maakt de akte op volgens de eisen die uit de wet voortvloeien[111]. Het Kadaster moet ook in de digitale situatie zorg dragen voor een betrouwbare openbare registers waar derden op kunnen vertrouwen.

6.3.2 Wettelijke basis inschrijven in de openbare registers

[110] De Dienst voor het kadaster en de openbare registers, 1997.
[111] Zie voor een gedetailleerde beschrijving van de juridische positie van partijen hoofdstuk 3.3

De aanlevering van de notariële akte bij het Kadaster is een proces dat in de analoge situatie grotendeels voortvloeit uit wetten. Het Burgerlijk Wetboek, de Kadasterwet en de Wet op het Notarisambt zijn deze wetten. Voor het digitale proces wijkt men niet veel van het analoge proces af. Er zijn openbare registers en voor de voor de overdracht vereiste levering geschiedt door de inschrijving van de notariële akte in de openbare registers. De wijze waarop de inschrijving plaatsvindt en de eisen die aan het in te schrijven stuk worden gesteld wijzigen echter wel.
Het kadasterformulier zal terminologisch worden vervangen door het digitale equivalent van de notariële akte.

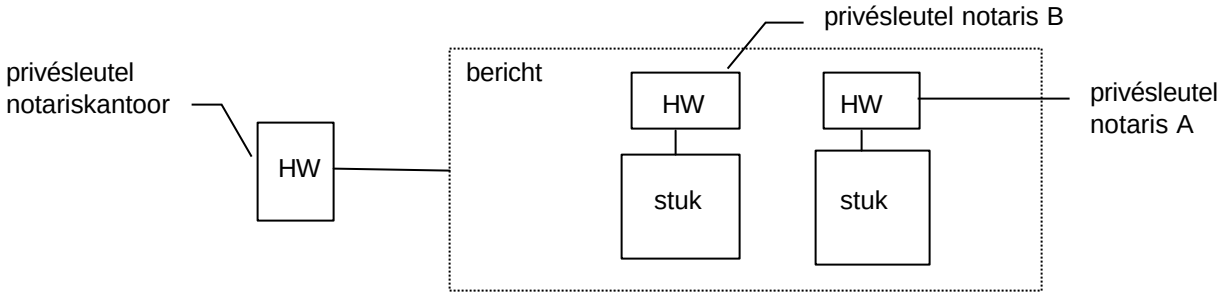
Vergunningsstelsel
De landelijke werkgroep elektronisch aanleveren is van zins de elektronische aanlevering met een vergunningsstelsel in de wet te regelen. Dit zou moeten gebeuren in een nieuw artikel 11A van de Kadasterwet. De vergunningverlening wordt daarin verbonden aan bij uitvoeringsregeling te bepalen voorwaarden[112].
Bij de aanvraag van de vergunning moet de aanvrager aangeven langs welk netwerk hij wil aanleveren. Als het Kadaster meent dat het netwerk niet aan de door hun gestelde eisen voldoet, wordt de vergunning niet verleend. In de vergunning worden tevens eisen gesteld aan de programmatuur, de hardware en het bericht. De eisen voor het bericht bestaan uit het te gebruiken formaat (pdf[113]), de structuur van de berichten en controlemogelijkheden voor integriteit van het bericht en identiteit van de afzender en notaris.
De eisen aan het digitale equivalent van de notariële akte geschieden bij uitvoeringsregeling. De voorwaarden die bij uitvoeringsregeling worden geregeld worden in subparagraaf 6.3.4 besproken.

Het aanbieden van de akten moet behalve via netwerken van bepaalde beroepsgroepen ook via een, in beginsel, voor een ieder toegankelijk (kadaster)netwerk mogelijk zijn.

[112] Zie bijlage 1 voor mogelijke voorwaarden op te nemen in een vergunningsstelsel of IA
[113] PDF staat voor Portable Document Format; http://www.adobe.com ; d.d. 20-11-1997

6.3.3 Beveiliging bij het elektronisch aanleveren

Beveiliging van de communicatie
De beveiliging van de communicatie is te classificeren als communicatie over een gesloten netwerk met een semi-assymmetrisch versleutelde hashwaarde.
Berichten van het notariskantoor naar het Kadaster worden over een gesloten netwerk verstuurd. Een bericht kan meerdere stukken bevatten. Per stuk wordt een hashwaarde berekend. Deze hashwaarde wordt versleuteld met de privésleutel van de notaris die het digitale equivalent heeft verstrekt. Van het totaal van stukken in een bericht wordt vervolgens de hashwaarde berekend. Deze hashwaarde wordt versleuteld met de privésleutel van het notariskantoor die het bericht aanbiedt. In figuur 6.2 wordt het schematisch weergegeven.



Figuur 6.2: De wijze waarop het digitale equivalent aangeboden wordt bij het Kadaster

Deze vorm van beveiliging zorgt er niet voor dat de stukken onleesbaar verzonden worden. De integriteit van de stukken wordt door de hashwaarde wel vastgesteld. De privésleutel om de hashwaarde zorgt voor identificatie van de notaris die de hashwaarde van het stuk heeft berekend. In principe kan de ondertekening van de hashwaarde gezien worden als de ondertekening van de verklaring van eensluidendheid in de analoge situatie.

Autorisatie in het systeem
De autorisatie in de digitale situatie kent geen verschil met de analoge situatie: de notaris is bij wet bevoegd de notariële akte op te maken en te verlijden en de bewaarder moet hem inschrijven of weigeren. De notaris kan bij afwezigheid worden vervangen door een door de Kamer van Toezicht aangewezen kandidaat-notaris.
De wijze waarop men de autorisatie in het systeem wil regelen is niet duidelijk. Men denkt aan het gebruik van smartcards. Ongeacht de wijze waarop men de toegang tot het systeem wil regelen, de verzender van een bericht zal bij integere berichtgeving aansprakelijk zijn voor de inhoud van het bericht. De autorisatie is dus in principe een interne kwestie voor zowel Kadaster als notaris.

Beveiliging van de opslag
Aan de beveiliging van de opslag is nog geen aandacht besteed.

6.3.4 Inschrijvingsvereisten aan het digitale equivalent van de akte

De wet die uitgaat van de analoge situatie is voor het Kadaster toe te passen op de digitale situatie voor wat betreft de algemene eisen die worden gesteld aan een afschrift van de akte en kadasterformulier: het stuk moet integer en authentiek zijn . De invulling van de inschrijvingsvereisten moet voor de elektronische aanbieding worden aangepast. De inschrijvingsvereisten zullen bij uitvoeringsregeling worden geregeld.

Integriteit van het digitale equivalent van de akte
De integriteit van de elektronische akte wordt door de hashwaarde bepaald (zie hoofdstuk 2 voor uitleg over de hashwaarde). De hashwaarde van een document wordt zowel bij de notaris als bij het Kadaster volgens een afgesproken algoritme berekend. Komen de berekende waarden overeen dan kan men aannemen dat het document tijdens de berichtenuitwisseling niet is gewijzigd.
De integriteit van het digitale equivalent op lange termijn wordt door het gebruik van het (toepassingsonafhankelijke) pdf-formaat bepaald. Het gebruik van het pdf-formaat is een inschrijvingsvereiste.

Identificatie van de afzender
De identificatie bij het Kadaster bestaat uit twee delen. De eerste identificatie gebeurt op notariskantoorniveau, de tweede op stukniveau. In beide gevallen maakt men gebruik van semi-asymmetrische encryptie. Is de ontsleuteling succesvol dan veronderstelt men dat daarmee de afzender geïdentificeerd is. In werkelijkheid is alleen het elektronisch adres van de afzender geïdentificeerd. Iedereen (binnen het notariskantoor) kan gebruik maken van dit adres. De autorisatie van personen bij de notaris met bijvoorbeeld een smartcard kan leiden tot identificatie op persoonsniveau.

Het identificeren van de bewaarder gebeurt op dezelfde wijze als de identificatie van de notaris. De bewaarder doet zijn privésleutel om het bericht en verstuurt het. Krijgt de notaris daar een leesbaar bericht uit dan is de bewaarder geïdentificeerd.

Authenticiteit van het digitale equivalent van de akte
De authenticiteit van het afschrift van akte is (in de functie die hij volgens prof. Hidma vervult, namelijk gelijkluidendheid met de authentieke akte,) bepaald als de integriteit en de herkomst van het digitale equivalent en de identiteit van de afzender zijn vastgesteld.

Nieuw inschrijvingsvereiste
In de huidige voorstellen zal er één nieuw inschrijvingsvereiste voor het elektronisch aanleveren zijn. Als men een digitaal equivalent van de akte wil inschrijven, zal een Verzoek Tot InSchrijving (VTIS) met het digitale equivalent moeten worden meegestuurd. Als dit niet wordt gedaan wordt de elektronische aanlevering van de notariële akte niet als verzoek tot inschrijving behandeld en kan het stuk niet worden ingeschreven. Als bij de technische controle blijkt dat een digitaal equivalent van een akte niet voldoet aan de eisen van integriteit en authenticiteit, zal een verzoek tot inschrijving niet geacht te zijn gedaan. Deze handelwijze zorgt ervoor dat een technisch afgekeurd bericht of digitaal equivalent niet in het register van voorlopige aantekeningen wordt geboekt.

6.3.5 De opslag van de stukken

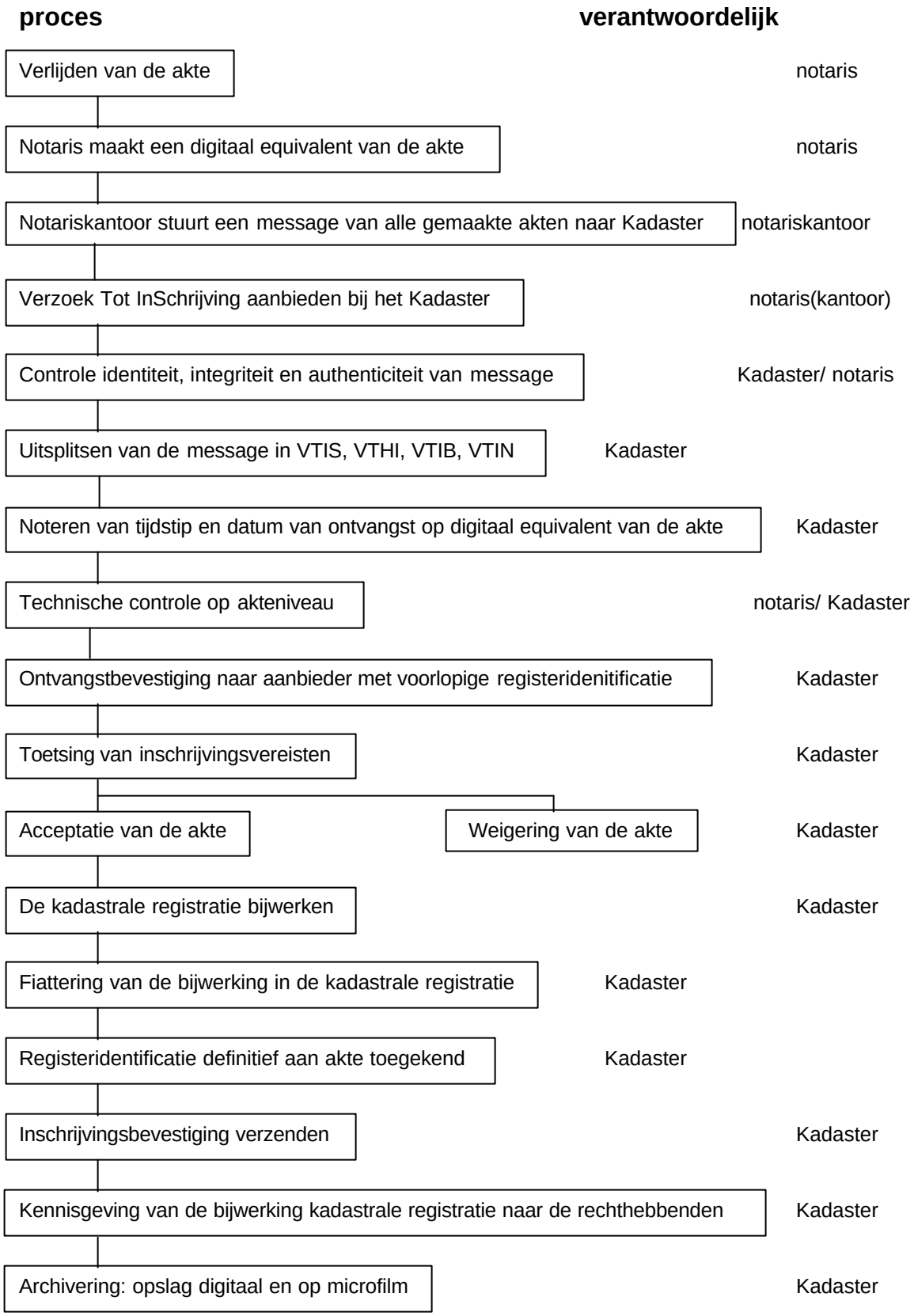
Op dit moment geven de voorstellen aan dat er twee nieuwe soorten openbare registers komen: digitale openbare registers en openbare registers van geanalogiseerde digitale equivalenten. Over de status van de registers ten opzichte van elkaar zijn het Kadaster en de KNB het (nog) niet eens. Het Kadaster wil beide registers dezelfde bewijskracht geven terwijl de KNB de geanalogiseerde openbare registers bij inconsistentie met de digitale openbare registers van doorslaggevende betekenis wil laten zijn.
Het digitaal equivalent van de akte dat is ingeschreven wordt op een duurzaam medium (WORM-plaat) opgeslagen met behoud van de digitale handtekening en de geconstateerde hashwaarde bij inschrijving. Het digitale equivalent wordt daarnaast bij het Kadaster omgezet op microfilm waarbij de digitale handtekening van de notaris wordt vervangen door zijn naam. De bij inschrijving geconstateerde hashwaarde wordt ook op microfilm gezet. Vlak voor de omzetting op microfilm wordt de hashwaarde van het stuk nogmaals berekend om de bewaarder te vrijwaren van frauduleus handelen.

6.3.6 Het nieuwe aanleverproces

De onderstaande stappen worden in het digitale proces per akte doorlopen.

1. De notaris maakt de minuutakte in zijn vereiste vorm op in een tekstverwerkingsprogramma, print de akte uit en ondertekent deze met vermelding van het tijdstip van ondertekening; de notaris verlijdt de akte van levering[114].
2. De notaris maakt een digitaal equivalent van de akte. Van het digitale equivalent wordt de hashwaarde berekend en deze hashwaarde wordt versleuteld met de privésleutel van de notaris.
3. De notaris of notariskantoor biedt een envelop met digitale equivalenten van de akte (het bericht) aan bij het Kadaster[115]. Van het bericht is ook een hashwaarde bepaald en deze is wederom versleuteld met de privésleutel van de aanbieder.
4. Het Kadaster controleert de identiteit van de aanbieder met de publieke sleutel van de aanbieder.
5. Het Kadaster stuurt een bericht van 'bericht-ontvangen' naar de aanbieder.
6. Het Kadaster controleert de integriteit van het bericht.
7. Het Kadaster splitst het bericht uit in een VTIS, VTHI, VTIN of VTIB bericht[116].
8. Per VTIS worden de digitale equivalenten van akten behandeld.
9. Het aangeboden digitaal equivalent van de akte wordt van het tijdstip van aanbieding voorzien[117].
10. Het digitale equivalent krijgt een uniek nummer (de registeridentificatie: datum van inschrijving en een volgnummer) en de status ontvangen.
11. Het Kadaster controleert het digitale equivalent van de akte technisch (juiste formaat, correct ingevuld, elektronische handtekening notaris, integriteit).
12. Als de Verzoek Tot InSchrijving regel correct is, wordt een bewijs van ontvangst met elektronische handtekening van de bewaarder en voorlopige registeridentificatie naar de aanbieder gestuurd met tijdstip van aanbieding[118]. De ontvangstbevestiging geeft aan of de notaris zijn bericht correct heeft gestuurd of niet.
13. Bewaarder toetst de inschrijvingsvereisten en weigert/ accepteert de akte[119].
14. Bewaarder schrijft de akte in (geeft definitief een registeridentificatie aan de akte[120], met handtekening van de bewaarder) of belt de notaris ter verwittiging van de weigering. Na overleg wordt de akte door de notaris opnieuw gestuurd of komt deze in het digitale register van voorlopige aantekeningen terecht. Na inschrijving van het digitale equivalent van de akte in de openbare registers (niet inbegrepen het register van voorlopige aantekeningen) is de voor overdracht van een onroerend zaak vereiste levering geschied.
15. De kadastrale registratie wordt bijgewerkt[121].
16. De mutaties in de kadastrale registratie worden door de bewaarder gefiatteerd. De stukken kunnen op dat moment met de status goedgekeurde mutatie middels AKR door derden uit de openbare registers worden opgevraagd
17. Het Kadaster stuurt een bewijs van inschrijving naar de notaris.
18. De inschrijving komt in het digitale register en is openbaar.
19. De akte wordt digitaal opgeslagen en op microfilm gezet [122].

[114] Artt. 30, 38 Wet op het Notarisambt
[115] Art. 3:89 BW
[116] VTIS = verzoek tot inschrijving nieuw stuk, VTIN = verzoek tot intrekking van de inschrijving, VTHI = verzoek tot hernieuwde inschrijving, VTIB = verzoek tot inschrijving bijhoudingsverklaring
[117] Art. 12 tweede lid Kw heeft dezelfde strekking voor het afschrift van de akte
[118] Artt. 3:18 BW, 3:19 BW en art. 17 Kw
[119] Artt. 3:19 en 3:20 BW
[120] Art. 12 derde lid Kw, artt. 12-15 Kr; de registeridentificatie is te vergelijken met het huidige deel en nummer.
[121] Art. 14 Kb
[122] Art. 9 Kw


proces
verantwoordelijk
Verlijden van de akte
notaris
Notaris maakt een digitaal equivalent van de akte
notaris
Notariskantoor stuurt een message van alle gemaakte akten naar Kadaster
notariskantoor
Verzoek Tot InSchrijving aanbieden bij het Kadaster
notaris(kantoor)
Controle identiteit, integriteit en authenticiteit van message
Kadaster/ notaris
Uitsplitsen van de message in VTIS, VTHI, VTIB, VTIN
Kadaster
Noteren van tijdstip en datum van ontvangst op digitaal equivalent van de akte
Kadaster
Technische controle op akteniveau
notaris/ Kadaster
Ontvangstbevestiging naar aanbieder met voorlopige registeridenitificatie
Kadaster
Toetsing van inschrijvingsvereisten
Kadaster
Acceptatie van de akte
Weigering van de akte
Kadaster
De kadastrale registratie bijwerken
Kadaster
Fiattering van de bijwerking in de kadastrale registratie
Kadaster
Registeridentificatie definitief aan akte toegekend
Kadaster
Inschrijvingsbevestiging verzenden
Kadaster
Kennisgeving van de bijwerking kadastrale registratie naar de rechthebbenden
Kadaster
Archivering: opslag digitaal en op microfilm
Kadaster

6.4 Mogelijke fouten in het aanlever- en verwerkingsproces

De fouten in het aanlever- en verwerkingsproces van het digitaal equivalent van de notariële akte kunnen gelijk aan de analoge situatie worden gescheiden in drie groepen:

1. Fouten door transport van het document
2. Fouten bij de verwerking van het digitaal equivalent van de akte bij het Kadaster
3. Fouten met betrekking tot de inhoud van het document

Per groep worden de fouten in deze paragraaf besproken. Hierbij moet worden benadrukt dat de opgesomde lijst niet uitputtend is maar dat een voor het onderzoek goede indicatie van mogelijke foutenbronnen wordt gegeven.

6.4.1 Fouten door transport van een document

Het vervoer van de akten naar het Kadaster zal over een lijn (telefoon-, kabel, glasvezel, ISDN-lijn) gaan. Tijdens het vervoer van het bericht met de afschriften van akten kunnen er fouten optreden.

Bij de volgende onderdelen van het aanleverproces kunnen door het transport van een document fouten optreden:
1. Het verzenden van het digitaal equivalent van de notariële akte naar het Kadaster
2. Het verzenden van het bericht van afkeuring
3. Het verzenden van de ontvangstbevestiging naar de aanbieder
4. Het verzenden van het bericht van weigering inschrijving
5. Het verzenden van de inschrijvingsbevestiging naar de aanbieder
6. Het verzenden van de nota naar de aanbieder
7. Het verzenden van de kennisgevingen naar rechthebbenden

De fouten die tijdens het transport van documenten kunnen optreden zijn:
a) Het document gaat verloren
b) Het document wordt gewijzigd: tussenkomst onbevoegde(n)
c) Het document wordt dubbel verstuurd
d) Het document dwaalt af: komt in bezit van derden
e) Het document wordt vertraagd
f) Het document wordt onleesbaar

6.4.2 Fouten bij de verwerking van de akte bij het Kadaster

Wanneer het bericht van de aanbieder in de postbus van het Kadaster is gekomen, begint de verwerking van het bericht[123]. Bij de verwerking van het bericht en vervolgens de verwerking van het elektronische digitale equivalent van de akte kunnen fouten optreden. Deze fouten kunnen worden gescheiden in fouten die zonder opzet door het Kadaster gemaakt worden, door fouten waar het Kadaster zelf niets aan kan doen en door doelbewuste fouten door ongeautoriseerd de digitale equivalenten van akten te wijzigen. Tenslotte zal de opslag van het digitale equivalent en de fouten die daarbij kunnen voorkomen aandacht krijgen.

[123] Zie voor het processchema 6.3.6

Fouten door het Kadaster

Bij het verwerken van het digitaal equivalent van de akte kunnen fouten ontstaan door menselijk handelen en/ of door handelingen uitgevoerd door de computer. De volgende fouten kunnen daardoor optreden:

- bij het legen van de postbus wordt een aangeboden bericht verwijderd, niet behandeld of een ander bericht onterecht eerder behandeld
- het toevoegen van het tijdstip van aanbieding wordt vergeten of gaat verkeerd (millenniumprobleem) op ontvangstbevestiging en/ of inschrijvingsbevestiging
- het tijdstip van aanbieding in ontvangstbevestiging en/ of inschrijvingsbevestiging is onjuist
- de registeridentificatie in ontvangstbevestiging of inschrijvingsbevestiging is niet uniek of onjuist
- de registeridentificatie is niet toegekend of is niet uniek (millenniumprobleem)
- het uitsplitsen van het bericht in digitale equivalenten lukt niet
- het digitaal equivalent van de akte gaat verloren
- het onterecht een ontvangstbevestiging sturen of inschrijvingsbevestiging in plaats van het register van voorlopige aantekeningen mededeling: de bewaarder drukt op een verkeerde toets
- het uitsplitsen van het bericht zorgt voor het kwijtraken van een bestand
- de conversie van de digitale handtekening van de notaris naar zijn naam voor de microverfilming geschiedt onjuist
- het digitale equivalent wordt niet volledig, gewijzigd of niet op microfilm gezet
- systeemuitval

Het uitvallen van het gehele computersysteem heeft als gevolg dat de inschrijving van digitaal equivalenten van akten vertraagd wordt. En met de inschrijving alle vervolgprocessen. De vervreemder krijgt bijvoorbeeld geen geld van de notaris. En de openbare registers zijn niet meer toegankelijk.
Als er geen voldoende maatregelen zijn genomen kunnen ook hashwaarde-algoritmen, sleutels van het Kadaster zelf, de kadastrale registratie, het klantenbestand van het Kadaster en zelfs de openbare registers uitvallen of verdwijnen als het systeem uitvalt.

Fouten in de kadastrale registratie
- het foutief bijwerken van de kadastrale registratie
- het foutief signaleren van de akte

De kadastrale registratie is de toegangspoort tot de openbare registers. Als de kadastrale registratie niet consistent is met de openbare registers, zal de toegangspoort leiden naar een gesloten deur.

Integriteit van de documenten
De bepaling van de integriteit van een digitaal equivalent van de akte gebeurt door computers. Een foute toepassing van het afgesproken algoritme met als gevolg een niet-overeenkomende hashwaarde leidt tot een onterechte weigering tot inschrijving.
Op het bewijs van ontvangst en het inschrijvingsbewijs kan de elektronische handtekening van de bewaarder zijn vergeten.

Autorisatiefouten
De registratie van de vergunninghouders van het Kadaster is in dit geval niet correct. Fouten in de autorisatiebepaling zijn er als de notaris volgens het Kadaster niet bevoegd is een digitaal equivalent van de akte te verstrekken en/ of de aanbieder van een digitaal equivalent volgens het Kadaster niet bevoegd is een digitaal equivalent van een akte aan te bieden.

Fouten zonder schuld van het Kadaster

Fouten die buiten de schuld van het Kadaster om blijven bestaan voor wat betreft het behandelen van de volgorde van de stapel aanbiedingen en beslagen op zakelijke rechten. Deze fouten die net als bij de analoge aanlevering ontstaan door het proces zoals dat in het BW en de Kadasterwet wordt voorgeschreven kunnen niet door de elektronica worden verholpen[124].
Verder kunnen fouten ontstaan door een failliete (software-)leverancier. Als het bedrijf dat de EDI-software specifiek voor KANO geschikt heeft gemaakt failliet gaat, kan het voor een ander softwarebedrijf lastig zijn de software te doorzien en eventuele foutmeldingen te herstellen.

6.4.3 Fouten met betrekking tot de inhoud van de documenten

Fouten in de inhoudelijke juistheid van het digitaal equivalent van de akte
De notaris moet er zorg voor dragen dat aan de eisen die de Wet op het Notarisambt aan de inhoud van de akte stelt is voldaan. De notaris moet er voor zorgen het digitale equivalent daadwerkelijk het equivalent van de notariële akte is.

6.4.4 Foutendetectie in het aanleverproces

Transport van het document

Net als in de analoge situatie bestaat de controle op het transport van het document uit het uitblijven van een bevestiging van ontvangen en inschrijving van het digitaal equivalent van de akte op het (elektronisch) adres van de notaris. Aangezien bij het elektronisch aanleveren de doorlooptijden aanzienlijk worden verkort, worden verloren, verdwaalde en vertraagde documenten eerder ontdekt (en hersteld).
Tussentijdse wijzigingen in het document zorgen ervoor dat het document niet meer integer is. De vergelijking van de hashwaarde van aanbieder en ontvanger zorgt voor een integriteitscontrole. Verandert er iets aan het document dan verandert ook de hashwaarde en is het document niet integer. De bewaarder kan dan het digitaal equivalent van de akte betreft niet inschrijven. De notaris krijgt via de ontvangstbevestiging elektronisch bericht van het geconstateerde verschil en besluit wat verder te doen.
De controle met de hashwaarde kan ook worden toegepast op de ontvangstbevestiging en inschrijvingsbevestiging.

Verwerking van het digitaal equivalent van de akte

Mutatie van de kadastrale registratie
De bijwerking van de kadastrale registratie levert net als in de analoge situatie een foutendetectie voor wat betreft de volgorde van behandeling van het bericht en van het digitaal equivalent van de akte. Ook is er de inhoudelijke controle van het digitaal equivalent van de akte als bijvoorbeeld een kadastraal nummer niet correct is of de vervreemder niet overeenkomt met de vervreemder in de kadastrale registratie.

Computers zijn betrouwbaar
De verwerking van het digitaal equivalent van de akte zal voor het grootste gedeelte door computers gebeuren. Computers maken mits goed geprogrammeerd geen fouten. Fouten met betrekking tot het onjuist registreren van het tijdstip van aanbieding en geen (uniek) registeridentificatienummer toekennen, zullen niet voor mogen komen.
Hetzelfde geldt voor de volgorde van behandeling van de aanbiedingen. De techniek zal geen fouten maken met het bepalen van de volgorde van binnenkomst en de daarmee bepaalde volgorde van behandeling. Mocht het desondanks toch voorkomen dat een digitaal equivalent van een akte door een volgordefout niet kan worden toegepast in de kadastrale registratie dan is daar gelijk de fout ontdekt.

[124] Zie voor een uitleg van de voorbeelden 3.4.2

Systeemuitval
Als het verwerkingssysteem uitvalt (bijvoorbeeld door een stroomstoring) dan leidt dit tot vertraging in de verwerking van het digitaal equivalent van de akte. Dit wordt spoedig ontdekt door degene die verantwoordelijk is voor de verwerking van het digitaal equivalent van de akte.

Fouten met betrekking tot de inhoud van de documenten

Het toetsen van de (inschrijvings)vereisten
De handelingen van de bewaarder kunnen worden bijgehouden in het (inschrijvings)vereisten-volgsysteem. Heeft een bewaarder onterecht een digitaal equivalent van een akte geaccepteerd of geweigerd in te schrijven dan kan hij/ zij in het volgsysteem worden getraceerd en berispt.

Controle van integriteit van de documenten en identiteit van de aanbieder
Voordat het stuk in Elan behandeld wordt is de naam van de afzender gecontroleerd in het portaalsysteem. De controles in het portaalsysteem gebeuren op berichtniveau. Is de naam van de afzender onbekend bij het Kadaster dan wordt het bericht weggegooid.
Is de naam van de afzender bekend bij het Kadaster maar is niet de juiste sleutel gebruikt dan wordt een bericht van afkeuring gestuurd naar het bekende adres.
Is de naam van de afzender bekend, de daarbij behorende sleutel correct, heeft de afzender een vergunning om digitaal aan te leveren en klopt de hashwaarde van de inhoud van het bericht dan is het bericht authentiek gebleken en kan begonnen worden met de verwerking van de 'VTISsen' in Elan.

In Elan wordt de integriteitscontrole en identiteitscontrole op stukniveau gedaan. Per digitaal equivalent van de akte is een hashwaarde berekend. Deze wordt door het Kadaster gecontroleerd. Verder wordt de privésleutel van de notaris ontsleuteld door het Kadaster.

6.5 Aansprakelijkheid binnen het elektronische aanleverproces

In het voorgaande is duidelijk geworden dat in het huidige proces van inschrijving van de notariële akte zowel bij de notaris, de netwerkleverancier als bij het Kadaster problemen kunnen ontstaan. Welke partij aansprakelijk is voor welk deel van het aanlevertraject wordt hierna besproken.

De aansprakelijkheidsverdeling zoals die in de digitale situatie zal gaan bestaan, vloeit voort uit de wet en haar uitvoeringsbepalingen. Onder de wet wordt hier verstaan het Burgerlijk Wetboek, de Kadasterwet, de Wet op het Notarisambt en de Wet op de telecommunicatievoorzieningen. Bij de aansprakelijkheidsbespreking wordt van het proces zoals dat de landelijke werkgroep Elan voor ogen staat uitgegaan. Er is nog geen enkele uitvoeringsregeling over het elektronische aanleveren op papier vastgelegd en het vergunningsstelsel is nog niet in de Kadasterwet geregeld. In de voorwaarden die aan de vergunning worden verbonden kan een partij ervoor zorgen dat voor bepaalde gevallen zijn of haar aansprakelijkheid wordt beperkt of wordt uitgesloten.
De hieronder genoemde partijen zijn bij het proces van aanleveren betrokken en kunnen aansprakelijk zijn voor een deel van het proces.

Het Kadaster
De aansprakelijkheid van het Kadaster is geregeld in artikel 117 van de Kadasterwet. Het Kadaster is jegens betrokkenen aansprakelijk voor schade die zij lijden, doordat in strijd met de wet een inschrijving is geweigerd of is geschied.
Het Kadaster is eveneens aansprakelijk voor alle verdere vergissingen, verzuimen, vertragingen of andere onregelmatigheden van zijn ambtenaren, gepleegd bij het houden van de registers of bij het opmaken of afgeven van afschriften, uittreksels en getuigschriften.

Het Kadaster is aansprakelijk voor de gegevensverstrekking uit haar gegevensdatabank. Indien de verstrekte informatie niet overeenkomt met het digitale equivalent van de notariële akte dan is het Kadaster aansprakelijk. Artikel 117 vierde lid Kw zal moeten worden aangevuld met “en andere gegevensdragers”.
Het Kadaster is aansprakelijk voor de blijvende beschikbaarheid, leesbaarheid van het digitale equivalent en voor de blijvende controles van het equivalent op integriteit en authenticiteit.

De bewaarder van de registers is niet gehouden de juistheid van de verklaring van eensluidendheid te onderzoeken. De Dienst is niet aansprakelijk voor schade voortvloeiend uit onjuistheden en onvolledigheden in het afschrift[125] [126].
Indien de gegevens verstrekt uit de digitale openbare registers niet overeenstemmen met de gegevens uit de analoge openbare registers is het Kadaster aansprakelijk voor de schade die hierdoor is ontstaan.

Voor fouten in de ontvangstbevestiging en inschrijvingsbevestiging van het Kadaster naar de notaris is het Kadaster aansprakelijk. De aansprakelijkheid heeft in dit geval betrekking op de fouten door transport van het document[127].
Voor het niet kunnen ontsleutelen van het bericht doordat de sleutel niet vindbaar is of niet blijkt te werken door een fout in de software en/ of hardware van het Kadaster is het Kadaster eveneens aansprakelijk.

Voor schade veroorzaakt door de uitval van het computersysteem van het Kadaster is het Kadaster aansprakelijk.

Het Kadaster is tenslotte aansprakelijk voor het gebruik van de digitale bewaarderssleutel.

De notaris
De aansprakelijkheid van de notaris is in de Wet op het Notarisambt geregeld in artikel 73[128]: “Behalve in de gevallen, waarin zulks uitdrukkelijk bij deze wet is bepaald, kunnen notarissen, indien daartoe termen bestaan, tot schadevergoeding jegens de belanghebbenden worden veroordeeld, indien de akten, voor hen verleden, uit hoofde van gebrek in den vorm in rechte nietig worden geacht of geoordeeld worden authenticiteit te missen, en verder in alle gevallen, waarin een verpligting bestaat tot schadevergoeding.”.
De Wet op het Notarisambt (oud en nieuw) stelt eisen aan de akte. Het vervullen van deze eisen is een taak van de notaris. Voor het nalaten of onvolledig vervullen van deze eisen is de notaris aansprakelijk.
De notaris is aansprakelijk voor de inhoudelijke juistheid, integriteit en authenticiteit van de minuutakte.
Bij het Kadaster wordt een digitaal equivalent van de akte aangeboden voor inschrijving in de openbare registers. De Kadasterwet en de Uitvoeringsregeling Kadasterwet 1994 stellen in de toekomst eisen aan het digitale equivalent. De notaris is aansprakelijk als het aangeleverde bestand niet een digitaal *equivalent* van de minuutakte is.
De notaris is aansprakelijk voor de inhoudelijke juistheid van het digitale equivalent als de hashwaarde na inschrijving van het digitale equivalent in de digitale openbare registers ongewijzigd is gebleven.

Het aanbieden van de akte laten de rechthebbenden vrijwel altijd over aan de notaris. Deze zorgt dan dat de akte bij het Kadaster aankomt. De notaris is dan aansprakelijk voor het aanbieden van het digitale equivalent van de akte bij het Kadaster.
Voor het niet kunnen ontsleutelen van een bericht van het Kadaster doordat de sleutel van het Kadaster niet vindbaar is of niet blijkt te werken door een fout in de software van de notaris is de notaris eveneens aansprakelijk.

[125] Art. 11 tweede lid Kw
[126] Bij het elektronisch aanleveren wordt niet gesproken van een afschrift maar over een digitaal equivalent van de akte.
[127] Zie hoofdstuk 6.4.1
[128] De bij de Tweede Kamer in behandeling zijnde nieuwe Wet op het notarisambt kent geen specifieke aansprakelijkheidsbepaling meer. De regels van het algemene recht gelden bij inwerkingtreding van de nieuwe wet; Tweede Kamer, vergaderjaar 1995-1996, 23706, nr.6 pagina 42-44

Tenslotte is de notaris aansprakelijk voor het gebruik van de digitale notarissleutel.

Netwerkleverancier: PTT telecom
De aansprakelijkheid van netwerkleverancier wordt geregeld in de Wet op de telecommunicatievoorzieningen (WTV). De aansprakelijkheidsbepaling van de WTV luidt op dit moment als volgt[129]:

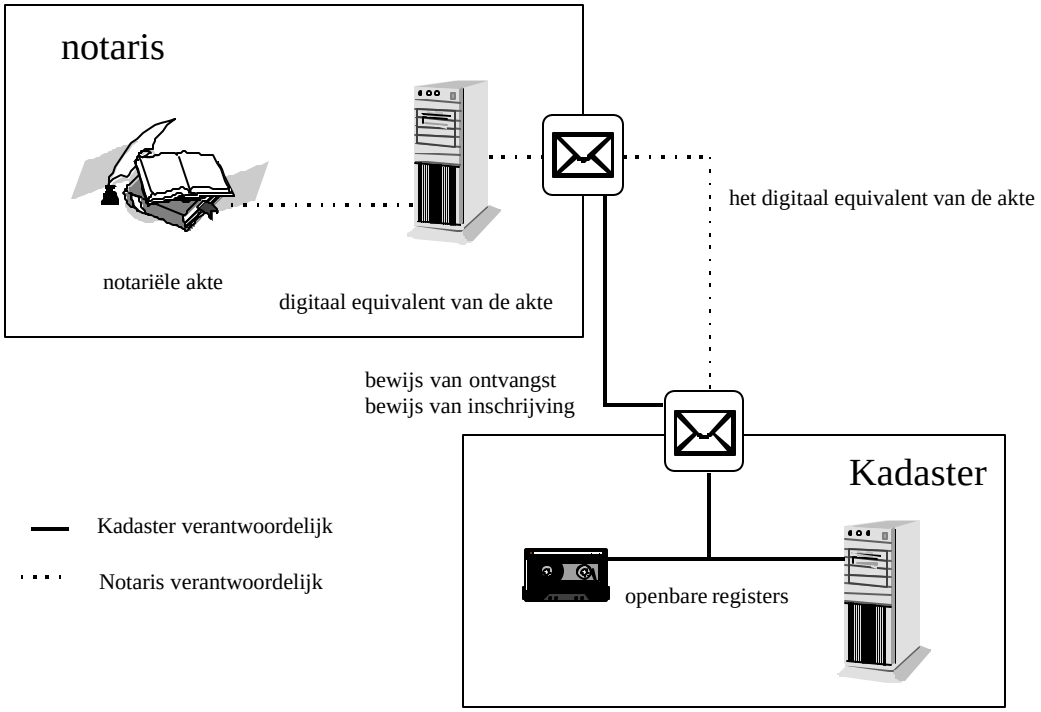
De houder van de concessie is voor schade als gevolg van het niet of niet goed functioneren van de telecommunicatie-infrastructuur en van tekortkomingen krachtens art 4 slechts aansprakelijk indien het schade betreft als gevolg van:
- dood
- een handelen in strijd met artt. 374, 375 WvS
- het niet of onjuist verstrekken, het onzorgvuldig beheren of verwerken van gegevens betreffende gebruikers van de bedoelde diensten en van vaste verbindingen dan wel fouten in administratieve verrichtingen samenhangend met de gegevens.

De beperking van de aansprakelijkheid van de concessiehouder kan niet als[130]:
- schade is ontstaan uit zijn eigen handelen of nalaten
- er opzet is schade te veroorzaken
- roekeloosheid van de concessiehouder tot schade leidt

De Wet op de telecommunicatievoorzieningen wordt op korte termijn ingrijpend veranderd. De veranderingen worden mede ingegeven door nieuwe Europese regelgeving, liberalisering van de telecommunicatievoorzieningen in het algemeen en de ontwikkelingen in omringende landen[131]. Een wettelijk geregelde beperking van aansprakelijkheid voor aanbieders van telecommunicatiediensten of van telecommunicatienetwerken, van welke aard deze ook mogen zijn, past primair niet bij de strekking van EG-regelgeving. In de nieuwe situatie zal de telecommunicatieoperator de normale contractuele mogelijkheden tot beperking van zijn aansprakelijkheid ten dienste staan. Contractpartijen bepalen dus in de toekomst de beperking van de aansprakelijkheid zelf in plaats van de wetgever. De dienstaanbieders krijgen dus de mogelijkheid hun aansprakelijkheid niet, gedeeltelijk of geheel uit te sluiten. Dit kan de concurrentieverhoudingen ten goede komen. De aansprakelijkheidsbepalingen kunnen afhankelijk van de omstandigheden van het geval in strijd komen met de redelijkheid en billijkheid. Hierdoor zouden voor bedrijfsmatige opererende aanbieders van openbare telecommunicatienetwerken en -diensten dan ook zeer grote risico's kunnen ontstaan. Deze risico's zijn echter verzekerbaar[132].

Softwareleverancier, hardwareleverancier, service-provider
De aansprakelijkheid van genoemde partijen zal door hen contractrechtelijk zoveel mogelijk worden uitgesloten.

[129] Art. 12 eerste lid WTV
[130] Art. 12 derde lid WTV
[131] Tweede Kamer, vergaderjaar 1996-1997, 25533, nr. 3, hoofdstuk 7.1 Aansprakelijkheid
[132] Het Verbond voor Verzekeraars heeft verklaard dat in beginsel de aansprakelijkheid van aanbieders van telecommunicatie te verzekeren is. De verzekeraars hebben er niet bij vermeld tegen welke prijs de aansprakelijkheid te verzekeren is.



Figuur 6.2 Het digitale aanleverproces schematisch weergegeven

6.6 Conclusies

De problemen die het elektronisch aanleveren van het digitale equivalent met zich meebrengt heeft het Kadaster in samenwerking met het notariaat grotendeels onderkend en met de voorgenomen wijziging van de Kadasterwet is een juridische oplossing gevonden om het elektronisch aanleveren mogelijk te maken. De (vorm)vereisten aan het digitale equivalent zullen in de nog te wijzigen Uitvoeringsregeling Kadasterwet worden opgenomen. De aanbieding van de digitale stukken zal anders dan in de analoge situatie worden gekoppeld aan een vergunningsstelsel. De huidige gang van zaken bij de aanbieding rechtvaardigt dit en door in de vergunning eisen te stellen aan de applicatie van de vergunninghouder zal de communicatie op een betrouwbare wijze plaatsvinden.

Het stuk moet bij het Kadaster worden aangeboden met behoud van integriteit en authenticiteit. Door de toepassing van hashwaarden en semi-asymmetrische encryptie worden deze juridische eisen technisch ingevuld. Het stuk zal over een gesloten netwerk worden aangeboden aan het Kadaster. De autorisatie tot de systemen is nog niet geregeld.
De encryptie die zal worden toegepast is slechts bedoeld voor de identificatie van afzenders en notaris en niet voor de beveiliging van de documenten.

Na de toetsing van de inschrijvingsvereisten door een medewerker van het Kadaster zal het digitale equivalent worden opgeslagen op een duurzaam digitaal medium (optische WORM-plaat). De openbare registers bestaan dan uit digitale openbare registers en de bestaande analoge openbare registers.
Naast digitale openbare registers wil het Kadaster openbare registers van geanalogiseerde digitale equivalenten van notariële akten.
De aansprakelijkheid van het Kadaster heeft vanaf het moment van inschrijven betrekking op de juistheid en volledigheid van de gegevens als blijkt dat de digitale openbare registers niet overeenstemmen met de

analoge openbare registers. Is dit niet het geval dan is de notaris aansprakelijk voor de overeenstemming van het digitale equivalent van de akte met de minuutakte en de inhoudelijke juistheid en volledigheid van het digitale equivalent van de akte.

De netwerkleverancier kan zijn aansprakelijkheid op basis van de huidige Wet op de telecommunicatievoorzieningen (WTV, Stb. 520) grotendeels uitsluiten.

Over de mogelijke rol van een TTP neemt het Kadaster in afwachting van de (juridische) ontwikkelingen op dit moment omtrent TTP's een afwachtende houding aan. Vooralsnog zal het Kadaster zelf de sleutelgeneratie verzorgen.

Kritische reflectie
De digitale aanlevering is een werkwijze die in deze tijd van Internet, digitale gegevensuitwisseling, e-mail, elektronisch belasting aangeven doen past. Binnen niet al teveel tijd moet het mogelijk zijn om van Internet een stuk uit de openbare registers in te zien en eventueel een gewaarmerkt digitaal stuk geleverd te krijgen. De verwerking gaat sneller, door het gebruik van computers worden er minder fouten gemaakt en de technische invulling van de juridische eisen maakt de digitale openbare registers betrouwbaarder dan de huidige openbare registers reeds zijn.
De voorgenomen opslag van het stuk op microfilm doet afbreuk aan het toekomstperspectief. De controles op integriteit en authenticiteit gaan verloren en de omzetting is een bron van fouten extra.

Mocht men toch besluiten de digitale stukken te analogiseren dan zal een onafhankelijke EDP-audit die de juistheid van de conversie continue controleert van zeer groot belang zijn om de rechter te kunnen overtuigen van de correcte werking van de conversie.

Risico's als het uitvallen van een computersysteem en een computerkraak door een hacker zijn niet uit te sluiten. Een 'kraak' (wijziging) van een digitaal equivalent is te constateren als bij het verstrekken van (digitale) informatie uit de digitale openbare registers een integriteitscontrole van het stuk plaatsvindt.

Toekomstige problemen?
Of de huidige techniek de gewenste duurzaamheid kan waarmaken is volgens experts twijfelachtig. De conversie van de digitale equivalenten van de akten naar een duurzamer digitaal medium kan ervoor zorgen dat het Kadaster in de (verre) toekomst ook aansprakelijk wordt voor de inhoudelijke juistheid van alle digitaal equivalenten van de akten in de digitale openbare registers.

Meer in de nabije toekomst heeft de elektronische aanlevering gevolgen voor de inhoud van de openbare registers. Naast de bestaande en nieuwe analoge stukken op microfilm komen er geanalogiseerde digitale equivalenten in de openbare registers. Deze krijgen wellicht dezelfde status hoewel de geanalogiseerde openbare registers geen enkele controle op integriteit en authenticiteit meer in zich hebben. De huidige analoge openbare registers hebben dit wel!
Aangezien er ook digitale openbare registers zullen gaan bestaan, moeten de huidige microfilm archieven gedigitaliseerd of gescand worden. Daarnaast kan het zo zijn dat er in het digitale openbare register een derde soort stuk terecht komt: het gescande geanalogiseerde digitale equivalent. Als bij het Kadaster namelijk de hashwaarde is veranderd, dan moet het analoge openbare register de doorslag geven. Het niet correcte stuk in de digitale openbare registers moet worden verwijderd uit deze registers en worden vervangen door een gescande versie van het microfilmstuk. Ieder van deze stukken heeft zijn eigen controleniveau qua integriteit van het stuk en identiteit van de notaris.

7. Ervaringen met EDI elders

7.1 Inleiding

In de logistieke sector heeft men veel ervaring met EDI opgedaan. De eisen die men daar aan de documenten en/ of berichten stelt, zijn niet vergelijkbaar met de Kadaster - notaris branche. Men stelt daar hoge eisen aan de snelheid van de berichtgeving. Daardoor wordt er zo min mogelijk gebruik gemaakt van beveiligingsmethoden. KANO stelt echter de veiligheid van de berichtgeving boven de snelheid ervan.
Verder zijn er aantal initiatieven in Nederland bij organisaties die vergelijkbaar zijn met KANO. Bill Of Lading Europe (BOLERO) bijvoorbeeld waar het cognossement vervangen wordt door een elektronisch equivalent. En het Rotterdams Douane Systeem (RODOS) waar de aangifte van doorvoer en opslag van goederen elektronisch kan worden gedaan. Deze twee projecten zijn echter pilotprojecten en echte ervaring met EDI heeft men (nog) niet.
Bij de aangifte van in- en uitvoer van goederen bij de Douane heeft men wel ruime ervaring met EDI. Ook bij de Amsterdamse Effectenbeurs heeft men ervaring met de elektronische handel in effecten met behulp van EDI. Omdat de eisen bij de Douane en de Amsterdamse Effectenbeurs aan het stuk als communicatiemiddel vergelijkbaar zijn met KANO, worden in dit hoofdstuk de situaties bij de Douane en bij de Amsterdamse Effectenbeurs beschreven.

7.2 Douaneformaliteiten: Sagitta

Sagitta[133] is het systeem dat voor de in- en uitvoeraangifte bij de Douane in Nederland wordt gebruikt. De situatie bij de Douane is op een aantal in hoofdstuk 1 genoemde punten vergelijkbaar met de Kadaster - notaris situatie: de waarde van het document dat uitgewisseld wordt is groot. Daardoor wordt veel waarde gehecht aan betrouwbare communicatie, het aantal communicerende partijen is beperkt en er is vertrouwen tussen de communicerende partijen, met name tussen de Douane en de afnemers van de douaneproducten.
Het logistieke proces waar het in-, of uitvoeren van goederen toe kan behoren, moet zo min mogelijk vertraging oplopen. Door de elektronische aangifte is de afhandeling van de aangifte door de Douane efficiënter geworden en is de vertraging in het logistieke proces tot een minimum beperkt. De efficiëntie bij de Douane heeft geleid tot de mogelijkheid meer mensen in te zetten voor de fysieke controle van de aangifte. Van alle aangiften die worden gedaan wordt ongeveer 5% gecontroleerd.
De elektronische aangifte kan alleen worden gedaan door bedrijven die hier een vergunning voor hebben gekregen. Voordat de vergunning wordt verleend wordt een testperiode ingesteld. Zijn alle tests positief verlopen dan kan de vergunning worden verleend. De vergunning is hoofdzakelijk aan expediteurs, dienstverleners en importeurs verleend.

7.2.1 Hoe werkt Sagitta?

Wanneer men goederen Nederland wil invoeren moet men daar aangifte van doen bij de Douane. Sinds 1989 kan dit elektronisch. Sagitta maakt gebruik van EDI. In plaats van per aangifte de vereiste schriftelijke bescheiden naar de Douane te brengen kunnen deze bescheiden op het kantoor van de aangever worden ingevuld en worden verzonden. Nadat de aangifte is ontvangen, wordt door de Douane een ontvangstbevestiging naar de aangever gestuurd. De computer van de Douane beslist of de aangifte

[133] Sagitta staat voor: Systeem voor de Automatische Gegevensverwerking van Invoeraangiften met Toepassing van Telematica voor het doen van Aangifte.

fysiek gecontroleerd wordt[134] of dat de invoer zonder controle mag plaatsvinden[135]. Deze beslissing wordt automatisch naar de aangever gestuurd. Dit bericht overhandigt de aangever aan de grens aan de douanebeambte. Deze verifieert aan de hand van de kenmerken of het geprinte authentiek is en gaat eventueel over tot de fysieke controle van de aangifte. De aangever weet dus van tevoren of zijn lading wordt gecontroleerd of niet.

Het aangifteproces per stap:

1. De aangever zendt de aangiften via datacommunicatie naar Sagitta.
2. Aangiftecontrole door Sagitta niet-fysiek.
3. Bericht aanvaard, aangehouden of afgehandeld.
4. Aangiftecontrole door de Douane fysiek indien de melding aangehouden bij stap 3 is gekomen.
5. Opslag van de aangiftebescheiden.
6. Verstrekking van de aangiftegegevens aan afnemers douane producten.

7.2.2 Beschrijving van de partijen

De Nederlandse Douane
De Douane controleert de in-, uit- en doorvoer van goederen en heft en int bij invoer verschuldigde belastingen en binnenlandse accijnzen.

De aangever
De aangever kan iedereen zijn die goederen in-, of uitvoert. De elektronische aangifte is met name handig voor bedrijven die regelmatig aangifte ten invoer of ten uitvoer doen.

7.2.3 Wettelijke basis van het elektronisch aangifte doen

De wettelijke basis voor het doen van aangifte van in- of uitvoer van goederen resp. in of uit Nederland ligt in een drietal wetten: de Algemene wet inzake rijksbelastingen (AWR, Stb. 499), het Communautair douanewetboek (CDW) en de Douanewet (DW, Stb. 737).

Artikel 1, tweede lid tweede volzin, AWR luidt:
Voor de toepassing van deze wet worden onder rijksbelastingen tevens verstaan rechten bij invoer en rechten bij uitvoer als bedoeld in artikel 1, tweede lid, onderscheidenlijk derde lid, van de Douanewet.

De wettelijke basis voor het doen van invoer- of uitvoeraangifte is in *artikel 8 AWR* geregeld:
Ieder die is uitgenodigd tot het doen van aangifte, is gehouden aangifte te doen door:.....

De *toepassingsverordening Communautair douanewetboek artikel 4bis* regelt de mogelijkheid tot het doen van elektronische aangifte:
1. De douaneautoriteiten kunnen toestaan dat formaliteiten op de door hen te bepalen voorwaarden en met inachtneming van de beginselen van de douanewetgeving met behulp van systemen voor automatische gegevensverwerking worden vervuld.
2. Toestemming om formaliteiten met behulp van systemen voor automatische gegevensverwerking te vervullen kan slechts worden verleend wanneer met name maatregelen voor controle van de bron en voor de bescherming van gegevens tegen ongeoorloofde toegang, verlies, wijziging of vernietiging zijn genomen.

[134] De aangever krijgt dan de mededeling: aangifte wordt aangehouden.
[135] De aangever krijgt dan de mededeling: aangifte is aanvaard.

Artikel 5 derde lid AWR regelt de elektronische aangifte verder:
Indien de douaneaangifte is gedaan met gebruikmaking van de automatische gegevensverwerking in de zin van artikel 4bis van de toepassingsverordening Communautair douanewetboek kan de uitnodiging tot betaling worden vastgesteld door het opmaken van een elektronisch bericht.

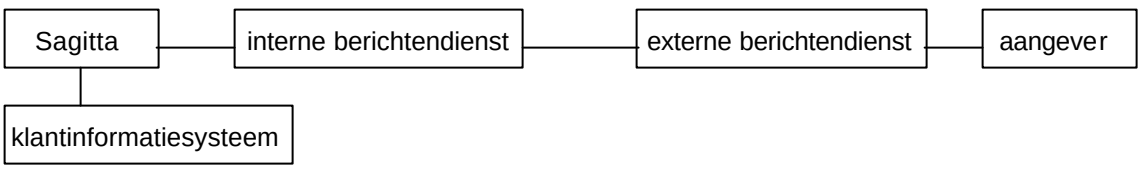
De elektronische aangifte is gekoppeld aan een vergunningsstelsel welke is geregeld in *artikel 32, eerste lid, Douaneregeling (Stcrt. 94)*:
Aangiften kunnen, door degenen aan wie daartoe een vergunning is verleend, elektronisch worden gedaan. In de vergunning kan het doen van een elektronische aangifte worden beperkt tot bepaalde douaneregelingen.

De wettelijke grondslag voor het gebruik van digitale vervanging van de analoge handtekening is te vinden in het *Communautaire douanewetboek artikel 4ter*:
Wanneer de formaliteiten worden vervuld met behulp van systemen voor automatische gegevensverwerking stellen de douaneautoriteiten vast door welke techniek, die eventueel op het gebruik van codes berust, de handtekening wordt vervangen.

7.2.4 Beveiliging

De berichten die de Douane krijgt en verstuurt zijn niet beveiligd in de zin van onleesbaar gemaakt. Er wordt wel gebruik gemaakt van de integriteitscontrole met behulp van de hashwaarde. Daarnaast zijn er een aantal andere vormen van beveiliging:

- de aangifte moet zijn verzonden vanuit een aansluiting waarvoor de vergunning geldt. Er is sprake van een gesloten netwerk (closed user group). De aangifte kan alleen door vergunninghouders worden gedaan. In de vergunning staan voorwaarden en bepalingen waar de aangever aan moet voldoen. Deze worden door de Douane gecontroleerd
- het aangeversnummer. De aangever krijgt een uniek nummer welke hij/ zij in het verzendbericht moet vermelden
- aangifte-identificatie. De aangifte krijgt een uniek aangiftegetal. Dit getal is opgebouwd uit de volgende elementen: aangeversnummer, aangiftejaar en maximaal 8 cijfers als volgnummer. De aangever bepaalt dit getal. De enige voorwaarde is dat het uniek is
- De aangever maakt gebruik van toegangscode en gebruikerscode. Het Message Transfer System controleert de gebruikers door deze codes te vergelijken met het netwerkadres van de afzender. Ofwel een controle tussen het logische en fysieke adres
- telepad verbinding; dial-up/ dial-back voorziening: als een aangifte wordt gedaan wordt de aangever door de Douane teruggebeld en de aangever kan zo zijn aangifte doen
- juistheid van datum/tijd (moment van verzenden, aanbieden van een bericht ten opzichte van het systeem datum/tijd). Is de verhouding tussen verzenden en ontvangen in juiste verhouding?
- in het systeem is bekend wie welke aangifte behandeld. Iedereen heeft een login en een wachtwoord. Dit wordt bepaald in de voorwaarden van de applicaties
- versturen van een ontvangstbevestiging naar de aangever[136]
- geen rechtstreekse communicatie met de aangever:



[136] De ontvangstbevestiging die de douane verplicht verzendt staat in 99 van de 100 aangevers uit. Dit komt doordat het bericht 'aanvaard' of 'aangehouden' zeer snel erna komt (seconden tot minuut).

Externe controles
De Douane heeft voor het informatieverstrekkingssysteem iemand ingehuurd die bij ingebruikneming van het systeem kijkt of het systeem functioneert zoals het behoort te functioneren. Het ministerie van Landbouw Natuurbeheer en Visserij verlangt jaarlijks de mededeling van een onafhankelijk accountantskantoor dat het systeem functioneert zoals ze dat behoort te doen.

Toekomstige ontwikkeling beveiliging
De invoering van encryptie wordt in het kader van Sagitta-2000 overwogen. Over een TTP wordt wel gesproken en dan met name over de functie van key-management (sleutelbeheer asymmetrisch). De Centrale beheereenheid Douane (CBED) zou deze rol kunnen gaan vervullen.

7.2.5 Toetsing van de elektronische aangifte

Naast de inhoudelijke toetsing door de Douane moet de Douane ook de integriteit en authenticiteit van de aangifte controleren. De integriteit van het document wordt bepaald aan de hand van de hashwaarde. De hashwaarde wordt afhankelijk van de voorwaarden van de vergunning met de aangever bepaald op basis van alle data-elementen of slechts gedeelten van deze elementen.

De authenticiteit van de aangifte wordt bepaald door aangifte-identifcatie, een telepad verbinding en door de faciliteiten behorend bij het X.400 protocol. De aangifte moet zijn verzonden vanuit een aansluiting waarvoor de vergunning geldt.

Formaat van de aangifte
Het aangifteformulier is een standaardformulier en is in een berichtenstructuur verwerkt met behulp van EDIFACT. Dit formaat is standaard en toepassingsonafhankelijk.

Tijdstip van ontvangst
De aangifte wordt geacht te zijn ingediend op het tijdstip waarop het EDI-bericht door de douaneautoriteiten wordt ontvangen (artikel 222 toepassingsverordening CDW).
In de *vergunning* wordt dit nader gespecificeerd:
Bij een elektronische aangifte geldt als tijdstip van aangifte en aanvaarding, het ogenblik waarop de elektronische aangifte door de Berichtendienst aan het systeem van de Belastingdienst ter beschikking worden gesteld.

Schriftelijke aangiften
Een schriftelijk ingediende aangifte wordt digitaal gemaakt door de essentialia in het digitale systeem in te voeren.

7.2.6 Opslag van de aangifte

De hashwaarden van de aangiften worden twee maanden bewaard. Daarna worden de hashwaarden verwijderd. De oorspronkelijke aangifte moet tien jaar[137] bewaard blijven bij de aangever. De Douane bewaart de oorspronkelijke aangifte zonder de bijbehorende hashwaarde twintig jaar. Daarna gaan de aangiften naar het Rijksarchief.

7.2.7 Verstrekking van douaneprodukten

Productschappen
De productschappen baseren zich bij de behandeling van subsidieaanvragen op de gegevens die ze dagelijks van de Douane krijgt. Zij willen daarom zekerheid omtrent de juistheid en volledigheid van de

[137] Kamerstuk 25753 is een wetsvoorstel deze termijn in de Douanewet te verkorten naar zeven jaar.

gegevens. De Douane communiceert met een ‘centraal productschap’. Dit centrale productschap verdeelt de douaneberichten weer onder de 8 productschappen.
De integriteit van deze gegevens wordt op twee niveaus door hashwaarden bepaald. Het eerste niveau is op interchange niveau. Dit is het niveau waarop Douane en het centrale productschap communiceren. De Douane stuurt vele aangiften tegelijk in een envelop naar dit centrale punt. Van deze envelop wordt een hashwaarde bepaald en meegestuurd. De berekende hashwaarde wordt daarnaast ook naar het centrale punt gefaxt.
Het tweede niveau is het aangifteniveau. De oorspronkelijke aangifte wordt met de hashwaarde naar het centrale punt gestuurd. Deze stuurt het naar één van de 8 productschappen. Daar wordt de hashwaarde op aangifteniveau opnieuw berekend.

Interchange Agreement
Douane en productschap hebben een service-contract gesloten. Hierin staan de procedures die moeten worden gevolgd bij problemen.
Als er een fout is opgetreden in het bericht dan is de hashwaarde veranderd en moet de Douane daar binnen twee maanden van op de hoogte worden gebracht. Dit is in de praktijk binnen een uur. De technische voorzieningen worden per half jaar geanalyseerd en indien nodig aangepast. Dit gebeurt in overleg met de beheerders van productschap en Douane.

7.2.8 Aansprakelijkheid

De aansprakelijkheid wordt geregeld onder andere in artikel 199 van de toepassingsverordening van de Communautaire douanewet. De aangever is aansprakelijk voor:
- de juistheid van de in de aangifte verstrekte gegevens
- de echtheid van de bijgevoegde stukken
- het nakomen van alle verplichtingen die samenhangen met het plaatsen van de betrokken goederen onder de desbetreffende regeling

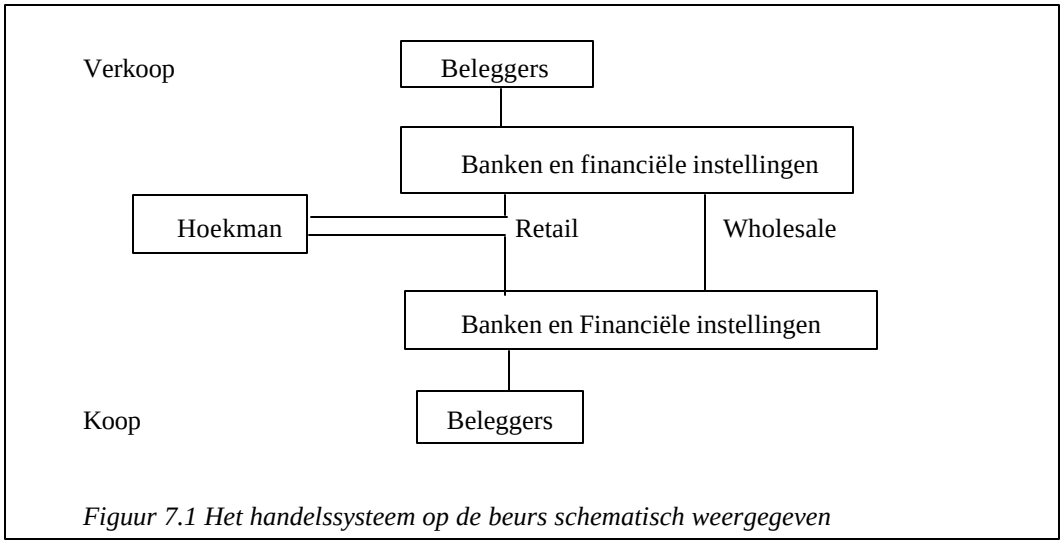
In de vergunningsvoorwaarden is ook een bepaling opgenomen die impliciet betrekking heeft op de aansprakelijkheid van een onvolledige, niet-authentieke aangifte.

Een elektronische aangifte wordt niet geaccepteerd indien:
- één of meer vereiste gegevens bij een volledige aangifte ontbreken
- één of meer ingevolge wettelijke voorschriften vereiste bescheiden bij een volledige aangifte niet in de aangifte zijn vermeld als zijnde in het bezit van de vergunninghouder
- in de aangifte een ander persoon dan de vergunninghouder als aangever is aangeduid
- de aangifte is verzonden vanuit een aansluiting waarvoor de vergunning niet geldt
- de aangifte één of meer gegevens bevat die onjuist zijn of niet voldoen aan de voor de berichtstructuur voorgeschreven specificatie

De correctheid van de aangifte blijkt uit de informatie uit het klantinformatiesysteem en de fysieke controles uitgevoerd door de Douane.
De aansprakelijkheid ten opzichte van de analoge situatie is niet verschoven of veranderd.

7.2.9 Conflicten

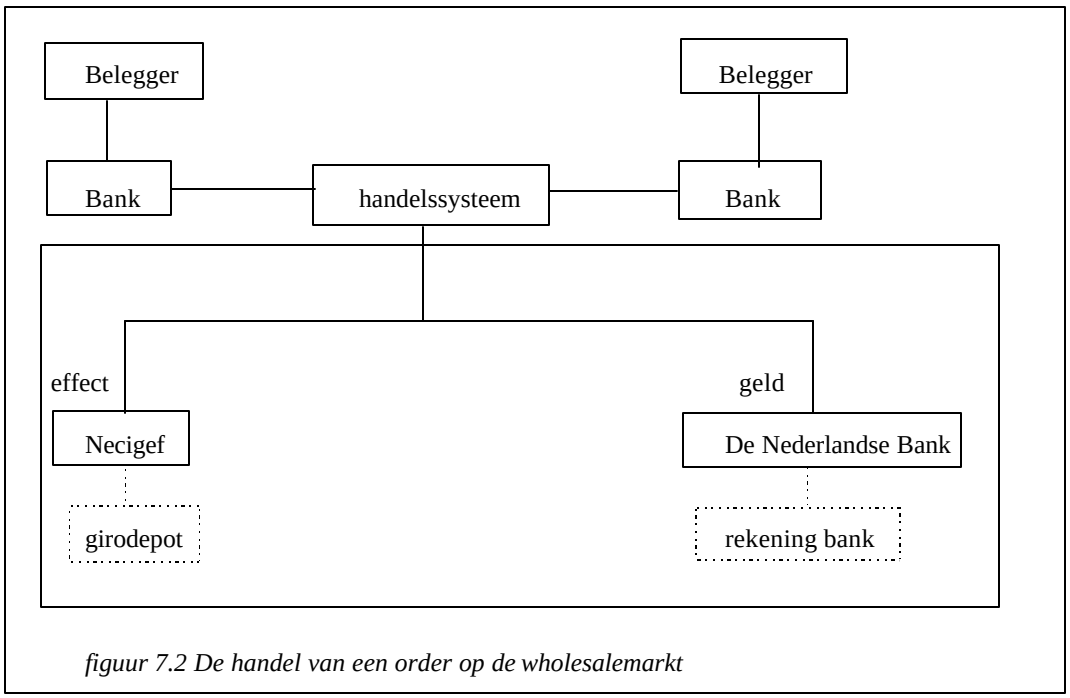
Ontkenning van aangiften is, voor zover bekend, niet voorgekomen. Er bestaat dan ook geen discussie over. Er zijn adequate maatregelen tegen genomen.
In de vergunning is een conflictenbehandeling opgenomen en verder zijn er op service-niveau overeenkomsten die regelen wat bijvoorbeeld te doen met zoekgeraakte berichten.
Conflicten bestaan hoofdzakelijk met betrekking tot douane-inhoudelijke zaken.



Figuur 7.1 Het handelssysteem op de beurs schematisch weergegeven

Wholesalemarkt[138]

Het systeem zoals dat op de beurs werkt is marktafhankelijk. De belegger geeft zijn bank of financiële instelling opdracht een order uit te voeren. Dit kan zowel een koop of een verkoop van een effect zijn. De bank brengt deze order naar de beurs waar het in het handelssysteem wordt verhandeld. Op de wholesalemarkt neemt bij het sluiten van een 'deal' zowel de koper als de verkoper contact op met Necigef en De Nederlandse Bank. Necigef zorgt voor de goederenrechtelijke levering (=overschrijving van het aandeel van de klant in het betreffende girodepot) en De Nederlandse Bank voor de financiële afhandeling van de transactie. Dit proces wordt op realtime basis van het principe van 'levering tegen betaling'. De handelspartijen houden een transactierisico op elkaar; het tegenpartij risico wordt niet overgenomen door Necigef en DNB.

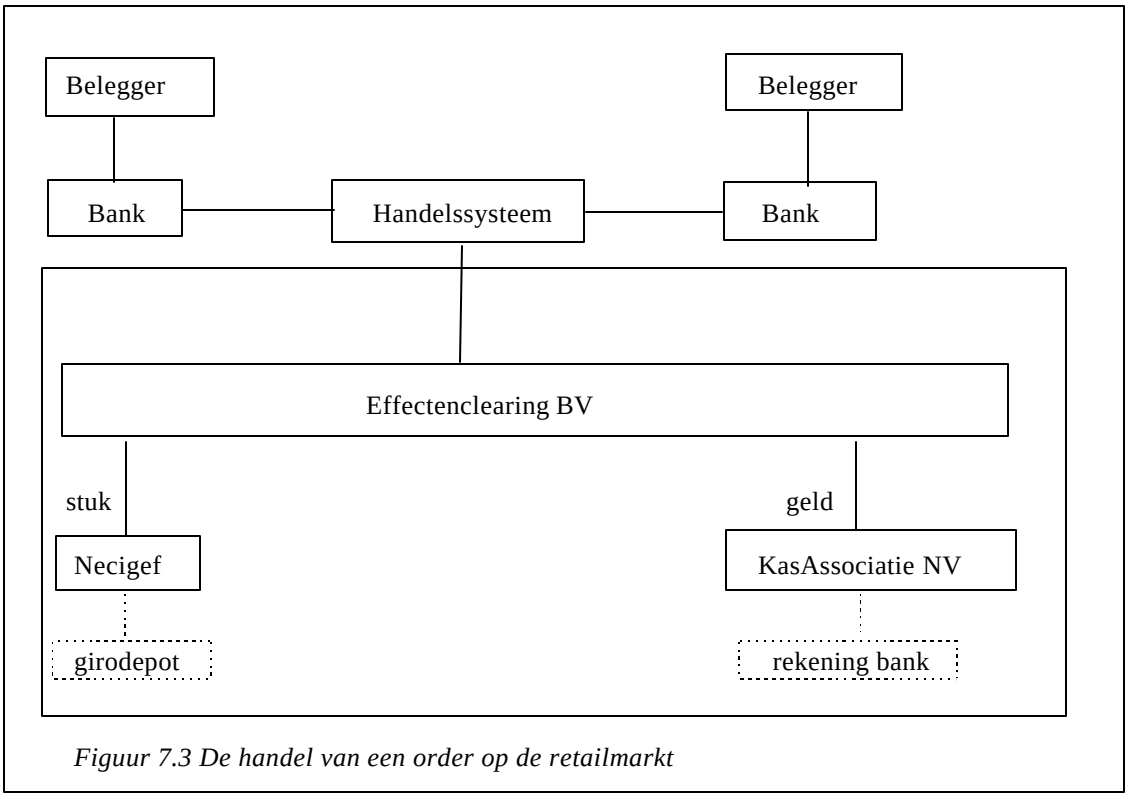


figuur 7.2 De handel van een order op de wholesalemarkt

[138] Zie figuur 7.2

Retailmarkt[139]

Op de retailmarkt wordt na het sluiten van een 'deal' direct Effectenclearing BV ingeschakeld. Deze instelling (100% dochter van AEX) neemt voor zowel de koper als de verkoper de schuldverplichting over. Dit wil zeggen de effectenclearing zorgt voor de afwikkeling van de transactie namens partijen bij de Necigef en de Kas Associatie NV. Necigef zorgt voor de goederenrechtelijke levering (=overschrijving van het aandeel van de klant in het betreffende girodepot) en Kas associatie NV voor de financiële afhandeling van de transactie. Deze transacties vinden slechts één keer per dag plaats.



Figuur 7.3 De handel van een order op de retailmarkt

7.3.2 Wettelijke basis

De wettelijke basis van de handel in effecten ligt in de Wet toezicht effectenverkeer 1995 (Wte 1995, Stb. 574). In deze wet wordt o.a. geregeld welke instantie zich beurshouder mag noemen, onder welke voorwaarden een beurs mag worden gehouden en aan welke eisen een effecteninstelling moet voldoen om te mogen handelen op de beurs van de beurshouder. Instellingen die willen handelen moeten bijvoorbeeld in het bezit zijn van een vergunning als bedoeld in de Wte 1995. Vergunningen worden verleend door de Stichting toezicht effectenverkeer (Ste). In verband hiermee heeft Ste de verantwoordelijkheid voor het toezicht op de Toegelaten instellingen voor wat betreft de wettelijke eisen die aan vergunninghouders worden gesteld. Naast de Wte 1995 zijn het de Nadere regeling toezicht effectenverkeer 1995 (Stcrt. 250) en het Besluit toezicht effectenverkeer 1995 (Stb. 623) die verplichtingen aan de handelede instellingen opleggen.

De Wet giraal effectenverkeer (Wge, Stb. 333) regelt de handel in girale effecten. Er is een centraal instituut dat toezicht houdt op het girale effectenverkeer en dit instituut bepaalt of instellingen worden toegelaten als aangesloten instelling bij het instituut. Tevens is dit instituut beheerder van het girodepot

[139] Zie figuur 7.3

en bepaalt het welke effecten geschikt zijn voor opslag in dit depot. Op basis van de Wge zijn er een aantal beschikkingen genomen die van toepassing zijn op het girale effectenverkeer.

Naast de bovengenoemde wetten zijn er nog verscheidene wetten (Wet toezicht beleggingsinstellingen bijvoorbeeld), besluiten en andere regelingen waaraan de handel in effecten is onderworpen.
Toegelaten instellingen zijn op grond van de met AEX afgesloten toelatingsovereenkomst ook onderworpen aan de reglementen en voorschriften die AEX onder meer met betrekking tot de handel en afwikkeling van beurstransacties vaststelt[140].

7.3.3 Beschrijving van de partijen betrokken bij de beurs

De partijen die op de beurs handelen zijn toegelaten instellingen. Beleggers moeten door deze instellingen op de beurs hun orders laten uitvoeren. Voor de definitieve afhandeling van een order wordt Necigef samen met De Nederlandse Bank (Kasassociatie N.V.) ingeschakeld.

Amsterdam Exchanges
Amsterdam Exchanges (AEX) is beurshouder in de zin van artikel 22 Wet toezicht effectenverkeer 1995 en als zodanig verantwoordelijk voor de adequate functionering van de door haar gehouden beurzen en de bescherming van de beleggers die op die beurzen handelen. Amsterdam Exchanges staat onder toezicht van de Minister van Financiën.
Per 1 januari 1997 is AEX verantwoordelijk voor regelgeving en controle op het gebied van de handel, de notering, de afwikkeling en de bewaring ten aanzien van de door haar geëxploiteerde beurzen en systemen. AEX is verantwoordelijk voor toetsing aan en controle op de naleving van de beurseigen regels die aanvullend zijn ten opzichte van de wettelijke voorschriften.

Rabobank
De Rabobank is een kredietinstelling als bedoeld in artikel 7 tweede lid onder h van de Wet toezicht effectenverkeer 1995 en kan op basis hiervan handelen zonder een vergunning. De bank is wel gehouden aan de eisen die aan de voorwaarden die in de wet voor vergunninghouders gelden.
De Rabobank is dus een toegelaten instelling en te kwalificeren als een intermediair tussen belegger en beurs. De opdracht van de belegger brengt de bank naar de beurs. Als de order is geslaagd brengt de bank het geld of het effect naar de belegger. De belegger heeft daarvoor een effectenrekening en een betaalrekening bij de bank lopen. De bank is ook beheerder van het verzameldepot als bedoeld in Hoofdstuk 2 van de Wet giraal effectenverkeer.

Necigef
Het ontstaan van Necigef eind jaren 70 is te danken aan het toenemende aantal effectentransacties op de beurs. De effectentransacties werden steeds riskanter en kostbaarder. Het gevolg was dat men zocht naar methoden die het effectenverkeer efficiënter en betrouwbaarder maakten. Dit werd bewerkstelligd door het vervangen van papieren effecten door girale effecten. De Wet op het giraal effectenverkeer (Wge) en daarmee de komst van het Nederlands centraal instituut voor gemeenschappelijk effectenverkeer (Necigef) hangen hier nauw mee samen.

Necigef is belast met de verzorging van het effectengiroverkeer en het bewaren, beheren en administreren van effecten. Dit ten behoeve van de aangesloten instellingen.
Daarnaast zijn er nog een tweetal andere taken. Ze bepaalt of aandelen die worden aangeboden voor bewaring geschikt zijn om in bewaring te nemen of niet. Hiervoor zijn toelatingscriteria opgesteld.
Ook stelt het instituut bij algemene maatregel van bestuur toelatingseisen aan instellingen die effecten in bewaring willen geven[141].

[140] De voorwaarden zijn gedeponeerd bij de Kamer van Koophandel Amsterdam onder depotnummer 5109.
[141] De eisen zijn in artikel 2 van de Beschikking ex artikel 1 Wet giraal effectenverkeer neergelegd.

Necigef staat onder toezicht van De Nederlandse bank en moet zich onthouden van enig risicovolle activiteit.

Necigef beheert het girodepot en voert tevens de administratie van dit depot. Wijzigingen in de aandelen van de aangesloten instellingen kunnen door een administratieve handeling plaatsvinden. De grondslag is te vinden in artikel 41 Wge: “Levering tussen aangesloten instellingen van een aandeel in een girodepot geschiedt door bijschrijving op de naam van de verkrijgende instelling in het daartoe bestemde deel van de administratie van het centraal instituut”. Er is sprake van een effectengiro: de aandelen in het depot verwisselen van eigenaren in plaats van de concrete aandelen.
De aandelen zijn fysiek opgeslagen en bijna volledig bij Necigef gecentraliseerd. De transacties gaan allemaal met de computer.
De gemiddelde transactiewaarde tussen instituut en instelling is ongeveer vijftig miljoen gulden.

Aangesloten instellingen bij Necigef
De aangesloten instellingen bij Necigef zijn banken en andere financiële instellingen. Deze instellingen moeten voldoen aan de eisen die in de Wge worden gesteld. Voldoet men niet (meer) aan de eisen dan heeft Necigef de bevoegdheid de instelling uit te sluiten van deelname. De aandelen die men in bewaring van Necigef wil geven moeten voldoen aan de voorwaarden die Necigef heeft voor de in bewaring te nemen aandelen heeft opgesteld.

Beleggers
De klant van de bank die de bank opdracht geeft namens hem of haar orders te verstrekken op de Amsterdamse Effectenbeurs is de belegger.

7.3.4 Communicatie belegger - Rabobank

Als een klant wil beleggen via Internet (open netwerk) dan moet hij/zij dit aanvragen bij de bank of een andere aangesloten instelling bij AEX. De bank geeft dan een gebruikerscode en een digipass aan de aanvrager. Door de digipass heeft hij toegang tot zijn beleggersrekening bij de bank. Als hij een order wil doorvoeren dan moet na invulling van de velden opnieuw een berekening met behulp van de digipass worden gemaakt. Deze code wordt naar de bank gestuurd en daar gecontroleerd. Na constatering van dezelfde waarde wordt de order, indien mogelijk, uitgevoerd.
Bij een volgende order zal de digipass een andere code berekenen zodat sprake is van een one-time-token principe.

Beveiliging

Naast de integriteitsbeveiliging en de authenticatie als waarborg vindt het onleesbaar maken plaats met behulp van Secure Sockets Layer (SSL2) encryptie. Dit is een symmetrische encryptievorm[142].
De encryptie is slechts bedoeld om de gegevens (het hele document) onleesbaar te maken.

De autorisatie van de personen die toegang hebben tot het systeem vindt plaats met de pincode op de digipass.

De bank geeft direct na ontvangst een ontvangstbevestiging aan de klant. Orders worden bevestigd door de terugmelding van orders. De niet verwerking van een transactie wordt eveneens gemeld aan de klant

[142] http://www.camb.opengroup.org/RI/www/prism/ ; d.d. 10-02-1998

Toetsing van de berichtgeving

Integriteit
De integriteit van het bericht wordt bepaald door de software van de bank deze berekend een controlegetal (hashwaarde) op het moment dat de klant aangeeft de order te willen verzenden. Het controlegetal moet in de digipass worden ingevoerd. De code die de digipass dan geeft, moet met de order meegezonden worden. De code is uniek voor de cliënt in combinatie met zijn order[143]. Ontsleuteling van de hashwaarde met de "tegen"-digipasssleutel leidt tot de hashwaarde.

Authenticiteit
De identiteit van de afzender wordt door middel van een soort inbelaccount gerealiseerd. De code van de digipass samen met de unieke gebruikerscode zorgt voor verificatie van de klant.

Opslag

De opslag van de gegevens wordt digitaal gedaan. Oude gegevens worden slechts voor statistische doeleinden gebruikt.

Aansprakelijkheid

De aansprakelijkheid van de bank voor fouten is tot een minimum beperkt. Beleggers zijn gehouden aan de bepalingen van de Algemene Bankvoorwaarden, de bepalingen van de Algemene voorwaarden voor de Effectendienstverlening en daardoor is de belegger ingevolge artikel 29 onderworpen aan de reglementen van de Vereniging voor de Effectenhandel, de reglementen van het Nederlands Centraal Instituut voor Giraal Effectenverkeer B.V., en het Nederlands Interprofessioneel Effectencentrum NIEC B.V., alsmede aan alle andere reglementen, voorschriften en gebruiken, die ten tijde waarop en ter plaatse waar die handelingen worden verricht van toepassing zijn[144]. Tevens is de belegger onderworpen aan de Algemene voorwaarden terugmelding van orderuitvoering.

Enkele bepalingen uit de Algemene Bankvoorwaarden:

Artikel 5 Risico van zendingen
Indien de bank in opdracht van de cliënt gelden of effecten aan de cliënt of aan derden zendt, geschiedt die verzending voor risico van de bank.

Artikel 11 Bewijskracht bankadministratie
Tegenover de cliënt strekt een door de bank getekend uittreksel uit haar administratie tot volledig bewijs, behoudens door de cliënt geleverd bewijs.

Artikel 13 Goedkeuring bankbescheiden
Indien de cliënt de inhoud van bevestigingen, rekeningafschriften, nota's of andere opgaven van de bank aan de cliënt niet heeft betwist binnen twaalf maanden nadat die stukken redelijkerwijs geacht kunnen worden de cliënt te hebben bereikt, geldt de inhoud van die stukken als door de cliënt te zijn goedgekeurd. Indien in dergelijke stukken rekenfouten voorkomen, is de bank bevoegd en verplicht die rekenfouten te herstellen, ook nadat genoemde termijn van twaalf maanden is verstreken.

Artikel 14: Verlies etc. van formulieren
De cliënt dient de door de bank aan hem ter beschikking gestelde formulieren, informatiedragers en communicatiemiddelen zorgvuldig te bewaren en te behandelen.

[143] Binnen een bepaalde tijd moet de code ingevoerd zijn bij de order. Wanneer er teveel tijd tussen de hashwaarde berekening en de invoering van de hashwaarde inzit, zal de verzending niet plaatsvinden; de code wordt mede op basis van het tijdsaspect berekend.
[144] De verstrekking van de voorwaarden genoemd in artikel 29 van de 'Algemene voorwaarden voor de effectendienstverlening' aan cliënten van de Rabobank stelt te hoge eisen aan de dienstverlening van de Rabobank.

Indien de cliënt enige onregelmatigheid zoals verlies, diefstal of misbruik met betrekking tot die formulieren, informatiedragers of communicatiemiddelen constateert, dient hij daarvan terstond mededeling te doen aan de bank. Tot het moment waarop de bank deze mededeling ontvangt zijn de gevolgen van het gebruik van die formulieren, informatiedragers of communicatiemiddelen voor rekening en risico van de cliënt, tenzij de cliënt aantoont dat de bank schuld te verwijten is. Daarna zijn die gevolgen voor rekening en risico van de bank, tenzij de bank aantoont de cliënt opzet of grove schuld. etc.

Artikel 27: Gebreken van effecten
De bank is aansprakelijk voor gebreken van effecten die door de cliënt zijn verkregen uit transacties die de bank heeft uitgevoerd met zichzelf als wederpartij of uit transacties in effecten die zijn toegelaten tot de officiële notering op de Officiële Markt of de Parallelmarkt van de Amsterdamse Effectenbeurs.

Artikel 31: Aansprakelijkheid van de bank
De bank is niet aansprakelijk voor storingen in de elektriciteitsvoorziening, in communicatieverbindingen of in apparatuur of programmatuur van de bank of van derden.

Enkele voorwaarden uit de Algemene voorwaarden voor de Effectendienstverlening:

Artikel 19: Bijzondere omstandigheden
Onverminderd de regeling in de Algemene Bankvoorwaarden is de Bank ingeval van bijzondere omstandigheden (onder meer uitvallen ordersystemen) niet gehouden jegens Cliënt opdrachten uit te voeren binnen de daarvoor gebruikelijke tijden, tenzij er sprake is van opzet of grove schuld van de Bank.

Enkele bepalingen uit de Algemene voorwaarden terugmelding van orderuitvoering[145].

Artikel 5.3: Verplichtingen klant
De klant is zelf verantwoordelijk voor het gebruik van de ontvangen informatie en de beveiliging van de door hem gekozen toegangsmogelijkheid tot de informatie tegen onbevoegde kennisneming door derden.

Artikel 7: Aansprakelijkheid
1. De bank is niet aansprakelijk voor enige schade, die niet voortvloeit door haar opzet of grove schuld is ontstaan en die direct of indirect voortvloeit uit:
- gehele of gedeeltelijke niet beschikbaarheid van (de faciliteiten van) de mogelijkheid om langs elektronische weg berichten te ontvangen;
- gehele of gedeeltelijke opschorting door de bank van het gebruik van de mogelijkheid om langs elektronische weg berichten te ontvangen door de klant;
- verstrekking van onjuiste en/of onvolledige informatie over saldi en/of mutaties en/of overige bankdiensten;
- niet-nakoming van ingevolge deze voorwaarden op de klant en/of de volmachtgever rustende verplichtingen.

2. Voor misverstanden, verminkingen, vertragingen of niet behoorlijk overkomen van berichten ten gevolge van het gebruik van de elektronische communicatie tussen bank en cliënt is de bank slechts aansprakelijk voor zover haar opzet of grove schuld te verwijten is.

Conflicten

Bij de geschillen- en klachtencommissie waar de bank zich aan onderworpen heeft kunnen klanten geschillen aanhangig maken. Ook staat de weg naar een bevoegde Nederlandse rechter open. De

[145] http://www.rabobank.nl/doelgroep/beleggen/effectenrekening/voorwaarden.asp ; d.d.10-2-1998

klachten- en geschillencommissie is niet gehouden aan de voorwaarden die bank en klant zijn overeengekomen[146].

7.3.5 Communicatie Rabobank-beurs

De informatie die de bank en beurs met elkaar uitwisselen zijn orders en beursinformatie. De orders zijn vertrouwelijk, de informatie openbaar.
De Rabobank heeft (nog) geen toelatingsovereenkomst met de AEX gesloten. Men is over de voorwaarden nog in onderhandeling.

Beveiliging

Het merendeel van de communicatie is informatie van de beurs en bevat geen vertrouwelijke informatie.
Orders en andere financiële zaken zijn met een password en user-id beveiligd.
De berichtenuitwisseling tussen de Rabobank en Amsterdam Exchanges gebeurt over een gesloten netwerk.
Er wordt geen encryptie gebruikt slechts procedurele beveiligingsmethoden zoals de verevening van de transacties van een dag en de orderbevestiging. Ook wordt er met volgnummers van transacties gehandeld.

Op basis van een wachtwoord en een user-id is de toegang tot de systemen geregeld.

Toetsing van de berichten

Integriteit
De integriteit van het bericht wordt niet bepaald en/ of gecontroleerd.

Authenticatie
Het gesloten netwerk is gebaseerd op het X.25 protocol, samen met een inbelaccount maakt dit dat de bank weet dat ze met de beurs communiceert.

Opslag

De opslag van de gegevens is digitaal. Administratieve zaken worden tien jaar opgeslagen op een ROM - schijf. Dit wordt zowel door AEX als door de Rabobank gedaan. Overige zaken worden slechts twee jaar opgeslagen en worden hoofdzakelijk voor statistische doeleinden gebruikt.

Conflicten

Klachten worden voorgelegd aan een interne commissie van de AEX. Deze commissie bestaat uit onafhankelijke deskundigen die een bindend oordeel vellen over de klacht.

Aansprakelijkheid

De aansprakelijkheid voor de toegang tot de systemen ligt bij de beheerders van de systemen. Rabobank is verantwoordelijk voor de toegang en het gebruik van zijn systemen.
AEX sluit haar aansprakelijkheid bijna volledig uit in de voorwaarden verbonden aan de toelatingsovereenkomst. Alleen voor schade veroorzaakt door opzet of grove nalatigheid stelt men zich aansprakelijk.

[146] De beurskrach van oktober 1989 zorgde ervoor dat orders door een capaciteitsgebrek van de AEX-effectenbeurs met grote vertraging werden verhandeld. Dit leidde tot schade bij zowel banken als klanten van de bank. De schade van klanten van de bank kwam toen, door een uitspraak van de klachten- en geschillencommissie volledig voor rekening van de banken. Het beroep van de banken op schuld van AEX werd afgewezen.

AEX staat onder toezicht van een EDP-auditor (KPMG) en doet structureel toezicht en onderhoud aan haar systemen. Van grove schuld zal dus geen sprake kunnen zijn. Blijft over de frauduleuze medewerker.

Enkele bepalingen uit het Handelsreglement:

Artikel 1.3
Uitsluitend toegelaten instellingen kunnen een aansluiting op het schermensysteem krijgen. Zij dienen hiervoor een overeenkomst te sluiten met een door AEX aangewezen leverancier.

1.4 AEX is nimmer aansprakelijk voor schade ten gevolge van het uitvallen van het Schermensysteem, storingen en andere tekortkomingen in het functioneren van het Schermensysteem.

1.6 Toegelaten Instellingen dienen er op toe te zien dat hun aansluiting op het Schermensysteem alleen wordt gebruikt door personen die hiertoe zijn geautoriseerd door de Toegelaten Instelling. Ongeautoriseerd gebruik van het Schermensysteem en de aansluiting daarop is te allen tijde voor rekening en risico van de desbetreffende Toegelaten Instelling.

1.7 De administratie van AEX, waaronder tevens begrepen dienen te worden de door het Schermensysteem verwerkte gegevens, gelden als dwingend bewijs in de relatie tussen AEX en de Toegelaten Instelling en tussen de Toegelaten Instellingen onderling, behoudens de mogelijkheid tot het leveren van tegenbewijs.

7.3.6 Communicatie Necigef en aangesloten instelling

Necigef moet op basis van collectieve depots van (fysieke) effecten de girale overdracht van effectentegoeden mogelijk maken. Eén van de belangrijkste doelstellingen is de centralisatie van alle effectenbewaring in Nederland, dat wil zeggen fysieke bewaring en de administratie inclusief het beheer van alle in Nederland 'liggende' effecten geschieden op een centrale plaats door een gespecialiseerd, neutraal en (be)veilig(d) instituut, bij Necigef.

Beveiliging

De partijen communiceren met elkaar over een gesloten netwerk. Dit netwerk is bekend onder de naam NECICOM. Hierbij wordt tevens van MAC[147,148]gebruik gemaakt. Hiermee wordt ten eerste de herkomst van het bericht geverifieerd en ten tweede de integriteit. Voor de herkomst van het bericht wordt gebruikt gemaakt van een bilaterale sleutel gebruikmakend van het DES-algoritme (symmetrisch).
De integriteit van het bericht wordt door een getal bepaald. Deze wordt met de generatiesleutel berekend en met de verificatiesleutel geverifieerd.
Eens per half jaar wordt de bilaterale sleutel verwisseld. Bij de aangesloten instelling wordt dan in twee delen een transportsleutel geïnstalleerd. Onder deze transportsleutel wordt de bilaterale sleutel verstuurd.

De communicatie gaat als volgt in zijn werk:

1. Toegelaten instelling A maakt een bericht.
2. A berekent met zijn generatiesleutel (≈ de publieke sleutel van Necigef) de hashwaarde.
3. Het bericht wordt door Necigef met de verificatiesleutel (≈ de privésleutel van Necigef) geverifieerd.
4. De transactie wordt, indien de wederpartij de tegengestelde opdracht geeft, uitgevoerd.

[147] Een MAC-sleutel is een sleutel die door 'hardware' gegenereerd wordt. Dit leidt tot grotere sleutels dan met software-algoritme als RSA mogelijk is. De MAC-sleutel kan echter alleen door de computers waar de MAC-kaart is aangebracht gegenereerd worden.
[148] http://www.rs6000.ibm.com/resource/aix_resource/pubs/redbooks/htmlbooks/sg244579.00/4579c27.htm ; d.d. 20-02-98

Procedurele beveiliging
De berichten van klanten komen in een postbus en worden direct in behandeling genomen. Als het proces daar aanleiding voor vindt wordt er een retourbericht gestuurd. Per klant wordt bijvoorbeeld een opdrachtvolgordenummer geregistreerd. Als na opdracht 2 geen opdracht 3 maar opdracht 4 komt, krijgt de klant hier bericht van en wordt de opdracht (tijdelijk) gestopt. Als er twee keer opdracht nummer 2 binnenkomt wordt de tweede nummer 2 niet in behandeling genomen. De klant krijgt ook hier bericht van. Per klant is er een inkomend en uitgaand nummer! Ditzelfde is ook bij de klant aanwezig.
Beide partijen moeten dezelfde opdracht geven: hetzelfde aandeel hetzelfde bedrag etc. Als dit niet klopt is er een vermoeden van een fout en wordt de transactie gestopt.

De machine die de opdrachten verwerkt heeft een capaciteit van twee keer het dagvolume. De datalijnen hebben dagelijks een bezettingsgraad van 30%. Als nodig kan deze capaciteit opgeschroefd worden. Real-time wordt een ontvangstbevestiging naar de klant gestuurd. Als deze uitblijft dan wordt dit gemeld.

Er is een interne controle en controle van externe accountants.

Eisen aan stukken

Een aandeel in een girodepot is overdraagbaar. De aandelen staan op naam van de aangesloten instelling. Het instituut is verplicht tot teruggave aan de aangesloten instelling van effecten uit het girodepot tot een hoeveelheid die overeenkomt met hetgeen door instelling in bewaring is gegeven; de instelling heeft geen recht op teruggave van dezelfde stukken.

Een belegger kan altijd de fysieke uitlevering van zijn effecten vragen. Alleen als er uitgeleverd kan worden mag er giraal effectenverkeer plaatsvinden. Dit is één van de eisen die Necigef stelt aan de toelating van instellingen die giraal mogen handelen.
Fondsen waarvan geen uitlevering mogelijk is kunnen niet worden opgenomen in de effectengiro. Bij de instellingen die verzameldepots houden, de aangesloten instellingen van Necigef, moeten zodanig samengestelde voorraden worden aangehouden dat aan deze uitleveringsplicht (art.26 Wge) kan worden voldaan. Hetzelfde geldt voor Necigef voor zover het betreft het recht op uitlevering van de aangesloten instellingen (art 45 Wge).

De effecten die aan Necigef aangeboden worden, worden opgeslagen in een kluis. Necigef maakt de effecten geschikt voor de effectengiro. Dit is een administratieve handeling (vergelijkbaar met het invoeren van de essentialia van een akte in AKR). De integriteit en authenticiteit van het effect zijn niet belangrijk. Het gaat bij de handel om de integriteit en authenticiteit van de berichten die uitgewisseld worden.

Aansprakelijkheid

De aansprakelijkheid is geregeld in het reglement voor girodepots. Necigef is aansprakelijk voor schade ontstaan door opzet of grove nalatigheid van Necigef.

7.3.7 Conclusie

De handel in effecten op de Amsterdamse Effectenbeurs is vergelijkbaar met de KANO situatie. Aan het bericht worden vergelijkbare eisen als KANO aan het stuk doet gesteld. Net als bij de Douane geldt dat de eisen die het Kadaster aan de duurzaamheid van het formulier stelt, niet vergelijkbaar zijn met de situatie op de beurs.

De situatie bij de Amsterdamse Effectenbeurs is te scheiden in de communicatie tussen belegger en bank, tussen bank en beurs, en tussen bank en Necigef.

De communicatie tussen bank en beurs en de communicatie tussen bank en Necigef is wettelijk geregeld, resp. in de Wte 1995 en de Wge. Verder zijn er vele regels waar toegelaten instellingen aan gehouden zijn.
De communicatie tussen belegger en bank is zeer veilig. De communicatie tussen bank en beurs is nauwelijks beveiligd en de communicatie tussen bank en Necigef is adequaat beveiligd.
De beurs en Necigef sluiten hun aansprakelijkheid ten opzichte van de bank voor alle schade uit tenzij deze is voortgekomen uit opzet of grove nalatigheid van beurs of Necigef. De bank sluit zijn aansprakelijkheid ten opzichte van de belegger eveneens uit behoudens opzet of grove nalatigheid van de bank.

8. Conclusies & aanbevelingen

8.1 Conclusies

In dit onderzoek staat de volgende probleemstelling centraal:

Welke invloed heeft het door EDI aanleveren en verwerken van de notariële akte bij het Kadaster op de aansprakelijkheidsverdeling tussen partijen en hoe kan deze verdeling, mede gezien ervaringen met EDI elders, juridisch worden vormgegeven?

De aansprakelijkheidsverdeling bij het elektronisch aanleveren verschuift niet ten opzichte van de analoge situatie als de techniek het behoud van integriteit, authenticiteit, leesbaarheid en beschikbaarheid van het stuk waarborgt.
Voor de juridische vormgeving van het elektronisch aanleveren, moet de Kadasterwet en de Uitvoeringsmaatregelen Kadasterwet worden gewijzigd. De aanbieding van de elektronische stukken kan net zoals bij de Douane en de Amsterdamse Effectenbeurs worden gekoppeld aan voorwaarden. Deze voorwaarden kunnen worden opgelegd in een vergunningsstelsel of door een Interchange Agreement. Een Trusted Third Party is voor het Kadaster alleen van belang als deze de rol van Certification Authority (CA) vervult.
De eisen die het Kadaster moet stellen aan de elektronische stukken zijn op de korte termijn vergelijkbaar met de aangifte bij de Douane en de berichtenuitwisseling bij de Effectenbeurs. Echter op lange termijn (~ honderd jaar) hebben de documenten van Douane en Effectenbeurs geen waarde meer terwijl de stukken in de openbare registers dat wel kunnen hebben. De eisen die het Kadaster terecht stelt aan het stuk voor wat betreft de technische waarborgen op (zeer) lange termijn zijn niet van toepassing op de vergeleken branches.

Bij de bepaling van de aansprakelijksheidsverdeling zijn een aantal trajecten te onderscheiden waar de aansprakelijkheid aan ontleend wordt:

- transport van het stuk
- invulling van de eisen aan het stuk
- toetsing van de inschrijvingsvereisten
- de opslag van het stuk

Transport van het stuk
Hoewel artikel 3:89 BW stelt dat zowel verkrijger als vervreemder de akte kan doen inschrijven, is het de notaris die als aanbieder in de huidige analoge situatie aansprakelijk is als het stuk niet, vertraagd en/ of gewijzigd bij het Kadaster wordt aangeboden. In de digitale situatie zal het niet anders zijn, tenzij de voorgestelde wetswijziging voor wat betreft de koppeling van de aanbieding met een vergunning niet door de parlementaire behandeling komt omdat dit niet in overeenstemming is met het bedoelde in artikel 3:89 BW.

Invulling van de eisen aan het stuk
De Wet op het Notarisambt uit 1842 en de Kadasterwet stellen aan het in te schrijven stuk inhoudelijke eisen en fysieke eisen.
De notaris is in de huidige situatie aansprakelijk voor de correcte invulling van de eisen van het stuk. In de nieuwe situatie is dit niet anders.

Toetsing van de inschrijvingsvereisten
Het Burgerlijk Wetboek en Kadasterwet stelt dat de bewaarder aansprakelijk is voor de inschrijving van stukken en de weigering van een inschrijving van stukken.
Het Kadaster is en blijft aansprakelijk voor de toetsing van de inschrijvingsvereisten zoals deze in de Kadasterwet en de Uitvoeringsregeling Kadasterwet 1994 zijn gesteld.

De opslag van het stuk
De eisen aan de opslag van een stuk zijn niet expliciet juridisch geregeld. Het Kadaster is aansprakelijk voor de opslag van het stuk in de openbare registers. Hierbij dient het Kadaster zorg te dragen voor de beschikbaarheid, leesbaarheid, integriteit en authenticiteit van het stuk. Zowel voor de opslag van het analoge als het digitale stuk is het Kadaster aansprakelijk.
De aansprakelijkheidsverdeling verschuift niet ten opzichte van de analoge situatie als het ingeschreven stuk na inschrijving beschikbaar, leesbaar integer en authentiek is; de notaris blijft aansprakelijk voor de inhoudelijke juistheid van het stuk.
Indien echter het Kadaster de integriteit, de authenticiteit, beschikbaarheid en/ of leesbaarheid van de ingeschreven stukken niet heeft gewaarborgd, is het aansprakelijk voor de gegevens die het verstrekt. Daarbij maakt het niet uit of dit een inzage in de kadastrale registratie of een gewaarmerkt afschrift uit de openbare registers betreft.
Aangezien de waarborgen blijvend (eeuwig) moeten zijn, stelt dit zware eisen aan het opslagmedium.

Het is mogelijk de gestelde juridische eisen technisch te vervullen. De hashwaarde is de nieuwe integriteitswaarborg, met de digitale handtekening (privésleutel) wordt de ondertekenaar van het stuk geïdentificeerd. De aanlevering van het stuk op een toepassingsonafhankelijk formaat en de opslag op Write Once Read Many-plaat (WORM-plaat) met bijbehorende randapparatuur zorgt ervoor dat het stuk leesbaar blijft.
Verder moeten alle soft- en hardware die integriteit, authenticiteit en leesbaarheid waarborgen blijvend behouden blijven, behoudens de mogelijkheid om ongewijzigd de gegevens op WORM te kopiëren naar een ander medium.

De hierboven genoemde technologische invulling van de juridische eisen zal het Kadaster volledig vervullen. Verder wil het Kadaster in de huidige voorstellen naast digitale openbare registers ook openbare registers van geanalogiseerde digitale equivalenten van de notariële akte ter waarborg van de leesbaarheid van de gegevens in de openbare registers. De conversie van digitaal naar analoog, betekent een verlies van integriteit en authenticiteit van het stuk. Enige waarde kan aan de microfilm stukken worden gehecht indien de conversieprocessen van privésleutel naar de naam van de ondertekenaar en van het digitale stuk naar het geanalogiseerde stuk op microfilm door een onafhankelijke EDP-auditor continue worden getoetst.
Slechts indien de notaris zelf het geanalogiseerde digitale stuk met zijn minuutakte heeft vergeleken en de eensluidendheid aan het Kadaster heeft bevestigd, heeft de microfilm dezelfde status als het nu heeft; nl. gelijkluidendheid met de minuutakte. Gezien de praktische haalbaarheid is deze optie niet relevant: de omzetting van de digitale stukken naar microfilm is voor de digitale openbare registers nauwelijks een toegevoegde waarde.

EDI elders
In het onderzoek is het systeem dat de invoeraangifte bij de Douane regelt en de wijze waarop op de Amsterdamse Effectenbeurs aandelen worden verhandeld, nader bekeken. Beide branches zijn voor wat betreft de waarde van het document vergelijkbaar met de notariële akte. In beide situaties wordt met een beperkte (en bekende) groep gecommuniceerd. De waarde die in beide situaties wordt gehecht aan betrouwbare communicatie is groot. Echter de duurzaamheid van de opslag speelt zowel bij de Douane als bij de beurs een ondergeschikte rol. Daarmee samenhangend is de aansprakelijkheid alleen op korte termijn in beide branches relevant. De Douane is aansprakelijk voor de controle van de aangifte, de aangever voor de inhoudelijke juistheid van de aangifte.

Op de beurs sluiten alle partijen hun aansprakelijkheid, behoudens opzet en/ of grove nalatigheid, ten opzichte van de afhankelijke partij uit. Necigef en Amsterdam Exchanges ten opzichte van de banken en de banken ten opzichte van de belegger.

Kritische reflectie in het algemeen
Het Kadaster speelt met de elektronische aanlevering in op de wensen van de grote klanten en waarschijnlijk wordt binnen niet al te grote termijn ook het Kadaster voor 'de gewone man' zeer toegankelijk. Overheidsloket 2000 zal hier een prominente rol vervullen maar het moet mogelijk zijn één stap verder te gaan: de openbare registers op Internet.
Zover is het echter nog niet. Met het project Elan is wel de basis gelegd om de openbare registers op het Internet op termijn te raadplegen. Met de technologische invulling van de juridische eisen is het voor een ieder met de juiste randapparatuur en software mogelijk de integriteit en authenticiteit van de gegevens uit de digitale openbare registers te controleren.

Als aan alle randvoorwaarden wordt voldaan, wordt het aanbieden en verwerken van stukken sneller, beter en veiliger dan de huidige werkwijze zonder dat de aansprakelijkheidsverdeling verschuift ten opzichte van de analoge situatie. Daarmee en met de grotere toegankelijkheid van de openbare registers wordt de rechtszekerheid bij het maatschappelijk verkeer in vastgoed nog sterker bevordert dan reeds het geval is.

8.2 Aanbevelingen

Op basis van dit rapport en met name op basis van een vergelijking tussen de hoofdstukken 4 en 5 en hoofdstuk 6 zijn de volgende punten ter handhaving van de aansprakelijkheidsverdeling aanbevelenswaardig:

1. Zorg ervoor dat de systemen regelmatig getoetst worden door een onafhankelijke EDP-auditor.

2. Houd de gebruikte authenticatiemethode actueel ter voorkoming van misbruik van de sleutels.

3. Realiseer een digitaal schaduwarchief van de openbare registers
   In plaats van geanalogiseerde digitale stukken op microfilm kan een digitaal schaduwarchief dezelfde beoogde rol vervullen. De meerwaarde van een digitaal schaduwarchief is veel groter dan een geanalogiseerd archief.

4. Waarborg de toegankelijkheid van de stukken in de digitale openbare registers en waarborg het behoud van integriteit en authenticiteit van de stukken.
   Zorg er voor dat de opslag van alle gebruikte hard- en software alsmede de opslag van de digitale stukken onder optimale omstandigheden plaatsvindt.

5. Verstrek de stukken uit de digitale openbare registers alleen elektronisch met een houdbaarheidstermijn van het stuk. De houdbaarheidstermijn moet afhankelijk zijn van de periode waarin de digitale handtekening van de bewaarder geacht wordt onkraakbaar te zijn.

6. Controleer voordat de stukken uit de openbare registers worden verstrekt eerst de integriteit en authenticiteit van het stuk.

Verder verdienen de volgende meer algemene punten aanbeveling:

7. Standaardiseer stukken
   Hoewel niet alle situaties door middel van standaardisatie ondervangen kunnen worden, verdient het, mede met het oog op de elektronische gegevensverstrekking, aanbeveling om de stukken zoveel mogelijk gestandaardiseerd aan te bieden.

8. Beveilig de communicatie tussen aanbieder en Kadaster met toepassing van volledige asymmetrische encryptie zodat het zeker is dat alleen het Kadaster kennis neemt van de inhoud van de stukken.

9. Zorg voor procedurele beveiliging om het verlies van een bericht te constateren.

Literatuurlijst

Boeken en bescheiden

Amsterdamse Effectenbeurs, *Beurs en effecten; De beurshandel en de vormen van beleggen*. Amsterdam: Veen uitgevers, 1991.

Asser-Mijnssen-de Haan , *Zakenrecht (algemeen goederenrecht).* Deventer: Kluwer, 1992.

'Axtent verklaart hackers de oorlog'. *Automatisering Gids,* vrijdag 13 februari 1998, 32e jaargang nummer 7, pagina 5.

Bannier, F.A.W., 'Risico en het Recht'. *NTT de zee*, jaargang 17, no. 3 maart 1998, pagina 103-107.

Boer, B.M. de, 'Sagitta'. *Informatie*, jaargang 33 nr. 2 pagina 68-75.
BOLERO Rulebook. London: Denton Hall, Working Draft (4), 1995.

Boom, W.H. van, 'Certain legal aspects of electronic bills of lading'. Tilburg, 1996.

Brief van 28 december 1977 betreffende de opschorting van overbrenging van archiefbescheiden van het Kadaster.

Brouwer*, Kadasterwet; Tekst van de wet, Toelichting B-3*. Lelystad: Koninklijke Vermande B.V., 1995.

Centrale douaneadministratie, *Aangevershandleiding RODOS*. Apeldoorn: versie 2.0 juli 1996.

De Dienst voor het kadaster en de openbare registers, *Boekwerk Kadaster algemeen (herdruk september 1997).*

De Dienst voor het kadaster en de openbare registers, *Kadaster jaarverslag 1993.*

De Dienst voor het kadaster en de openbare registers, *Kadaster jaarverslag 1994.*

De Dienst voor het kadaster en de openbare registers, *Kadaster jaarverslag 1995.*

De Dienst voor het kadaster en de openbare registers, *Kadaster jaarverslag 1996.*

De Dienst voor het kadaster en de openbare registers, *Kadastraal Vastgoedinformatie Systeem*. Apeldoorn, 1997.

De nieuwe handelssystemen op de Amsterdamse Effectenbeurs. Amsterdam: Amsterdamse effectenbeurs, 1995.

Dellemijn, A.N., 'Amsterdamse Effectenbeurs start centrale (uit)leenfaciliteit'. *Bank- en Effectenbedrijf*, november 1993 pagina12-13.

Dubbelt, W., *De openbare registers; administratie van de zakelijke rechten op onroerend goed*. 2e druk. Ministerie van VROM, Dienst van het Kadaster en de Openbare Registers, 1979.

Dumortier, J., 'Multimediale wetgeving in Duitsland: een inspirerend voorbeeld?*'. Computerrecht* 1998/1, pagina 2-3.

EDIFORUM, NNI, *Bewaren en bewijzen, deel I: Wet- en regelgeving*. 1995.

EDIFORUM, NNI, *Bewaren en bewijzen, deel II: Praktijkrichtlijn*. 1995.

Esch, R.E. van, 'Het elektronisch identificatiemiddel en volmacht'. *NJB,* 24 september 1992 afl.33, pagina 1073-1080.

Esch, R.E. van, en C. Prins e.a., *Recht en EDI, Juridische aspecten van elektronisch berichtenverkeer*. Deventer: Kluwer, 1993.

Franken, H., e.a., *Beschikken en automatiseren.* Samson HD Tjeenk Willink, 1993.

Franken, H., e.a., *De notaris en het elektronisch rechtsverkeer*. Lelystad: Koninklijke Vermande, 1996.

Graaf, F. de, e.a., *Juridische aspekten van netwerken*. Rapport N.I.V.R-studiecommissie, Nederlandse Vereniging voor Informatica en Recht, april 1990.

Greef, K. de, 'De (on)deugdelijkheid van het elektronisch bewijs; juridische consequenties EDI nog onduidelijk'. *Account,* mei 1995, pagina 24-26.

Haak, K.F., 'Kroniek van het vervoerrecht; Unificatie: quo vadis*?' NJB* , 15 maart 1996, afl. 11 pagina 426-429.

Hidma, en Van Velten, *Adviezen digitaal aanleveren notariële akten (EDI).* Februari 1996.

Hof, S. van der, *De juridische status van de digitale handtekening*. Alphen aan den Rijn/
Diegem: Samson bedrijfsinformatie bv, 1997. ITeR reeks nummer 7.

Hofman, W.J., *EDI handboek: elektronische gegevensuitwisseling tussen organisaties*. Amsterdam: Uitgeverij Tutein Nolthenius, 1989.

Huydecoper, S., en R. van Esch, *Geschriften en handtekeningen: een achterhaald concept?* Alphen aan den Rijn/ Diegem: Samson bedrijfsinformatie bv, 1997. ITeR reeks nummer 7.

In- en uitvoeruitgifte doen met SAGITTA. Rotterdam: Belastingdienst Douane, 1994.

Ipenburg, F. van, 'RODOS, Klaar voor het grote werk'. *Douane nieuwsbrief*, elfde jaargang nummer 3, oktober 1997, pagina 6.

Joosten, ingenieur- verificateur W., Intern rapport van onderzoek naar microverfliming van de openbare registers. Amsterdam, 22 februari 1958.

Kampert, H.A., *EDI onder controle.* Handboek EDP-auditing-afl. 10 (juli 1995) B.5.5.3.

Karssen, M. van, 'Beursintroductie'*, Beursintroductie: handleiding voor het introduceren van ondernemingen op de Amsterdamse Effectenbeurs*. Alphen aan den Rijn: Samson, 1987.

Koops, B.J., 'Notaris, ik houd mijn sleutels liever zelf'. *Computerrecht* 1997/4

Mitrakas, A., *Open EDI and Law in Europe, A regulatory Framework*. The Haque/Boston/London: Kluwer Law International, 1997.

Mourik, M.J.A. van, 'De essentialia van het notarisambt'. *NJB*, 19 mei 1995 afl. 20, pagina 731-737.

Net, D.J. van der, *Electronic Data Interchange, naar een papierloos tijdperk*. Kluwer bedrijfswetenschappen, 1994.

Notarieel Juridisch Bureau, 'Recente Rechtspraak: Arrondissementsrechtbank te 's- Gravenhage 28 september 1984, Rolnr. 82/6164'. *WPNR,* 5761 pagina 750-751.

'Notarissen willen te veel in elektronische beveiliging'. *Automatisering Gids*, vrijdag 19 september 1997, 31e jaargang, nr. 38 pagina 9.

'Oki beproeft identificatie via oog'. *Automatisering Gids*, vrijdag 30 januari 1998, 32e jaargang, nr. 5.

Prins, J.E.J, 'Juridisch bewijs en kunstmatige-intelligentie systemen'. *RM themis,* 1995/2, pagina 47-60.

Prinsen, M.J., e.a., *Rapport staatscommissie inzake het Kadaster*. 's Gravenhage: Staatsuitgeverij, 1980.

Proceedings Digital Security, deuren en sleutels in de informatiewererld. Symposium Elektrotechniek TU Delft, 13 mei 1997.

Rutte, Ch. W., 'Stukkenloze effecten'. *TVVS,* 1992 nr. 92/3 pagina 63-65.

Schultz, J.F.H., *EDI: kansspel, machtspel of samenspel?* Alphen aan den Rijn: Samson bedrijfsinformatie bv, 1994.

Schut, E., en E. Wiersema, *Betrouwbaarheid elektronische berichten in betalingsverkeer*.Alphen aan den Rijn/ Diegem: Samson bedrijfsinformatie bv, 1997. ITeR reeks nummer 7.

The Bolero project 1997, *The Bolero Service, Business requirements Specification version 1.0*.

The Technology Research Staff of NARA, *Digital Imaging and optical digital data disk storage systems, log-term access strategies for federal agencies, Technical Information Paper No. 12*. Maryland 20740-6001: National Archives and Records Administration, 1994.

Velten, A.A. van, 'Iets over het nodeloos vervoeren van karton'. *WPNR* 1993/6082 pagina 145.

Verstappen, L.C.A., B.C.M. Waaijer, e.a., *Kadaster, openbare registers en de rechtspraktijk*. Nijmegen: Vermande, 1991.

Vincent, L.J.K., 'Eigendom van effecten in het effectengiro-systeem'. *De naamloze vennootschap,* 75/ 2 februari 1997, pagina 42-49.

Vlist, P. van der, e.a, *EDI in de Gezondheidszorg*. Alphen aan den Rijn/ Zaventem: Samsom bedrijfsinformatie, 1992.

Westerbrink, B.N., e.a., *Juridische aspecten van het Internet*. Amsterdam: Otto Cramwinckel uitgever te Amsterdam, 1996.

Zevenbergen, J.A*.,* Nederlandse stelsel van grondboekhouding, een 'geprivatiseerde' vorm van een positief stelsel'. *WPNR,* 96/6240 pagina 727-731.

Zwanikken, G.G., 'Volmacht per fax'. *WPNR,* 94/6135 pagina 327-329.

Internet

Algemene achtergrond artikelen:
Http://canada.justice.gc.ca/Commerce/chapitre/ch10_en.txt ; d.d. 06-01-1998
Http://cla.org/eclawbook/ecl_09.htm ; d.d. 16-01-1998
Http://www.abode.com ; d.d. 20-11-1997
Http://www.aex.nl/aexnaam.html ; d.d. 11-12-1997
Http://www.ecworld.org/Resource_Center/Agora/Roadmap/chapt08.html ; d.d. 16-01-1998
Http://www.notaris.nl ; d.d. 30-10-1997
Http://www.notaris.nl/knb/home.html ; d.d. 01-12-1997
Http://www.nrc.nl/W2/Lab/Profiel/Beurs/kwestie.html ; d.d. 06-01-1998
Http://www.rabobank.nl/data/demo_telebankieren_rel2/demo_13.html ; d.d. 10-02-1998
Http://www.rabobank.nl/doelgroep/beleggen/effectenrekening/voorwaarden.asp ; d.d. 10-02-1998

Encryptie:
Http://cwis.kub.nl/~frw/people/hof/ds-new.htm ; d.d. 16-01-1998
Http://ourworld.computerserve.com/homepage/ckuner/digsig.htm ; d.d. 16-01-1998
Http://rs6000.ibm.com/resource/aix_resource/pubs/redbooks/htmlbooks/sg244579.00/4579c27.html ; d.d. 10-02-1998
Http://www.camb.opengroup.org/RI/www/prism/ ; d.d. 10-02-1998
Http://www.computerbar.org/comp3d.htm ; d.d. 16-01-1998
Http://www.efga.org/digsig/sb97_103.html ; d.d. 16-01-1998
Http://www.rsa.com ; d.d. 20-11-1997
Http://www.securitydynamics.com/securvar/down31.html ; d.d. 20-11-1997
Http://www.ss.ca.gov/digsig/digsigfaq.htm ; d.d. 16-01-1998

Kenmerken van opslagmedia:
Http://archive.eso.org/articles/data-storage/RND-OPT-WRM-12I.html ; d.d. 18-03-1998
Http://community.bellcore.com/lesk/auspres/aus.html ; d.d. 17-03-1998
Http://esdis.gsfc.nasa.gov/msst/conf1996/B2_3Stutz.html ; d.d. 20-03-1998
Http://nist.gov ; d.d. 24-03-1998
Http://outoften.doc.ic.ac.uk/~nd/surprise_97/journal/vol1/ary/index.html ; d.d. 24-03-1998
Http://www.aiim.org ; d.d. 24-03-1998
Http://www.clir.org/cpa/reports/lesk2 ; d.d. 26-03-1998
Http://www.clir.org/cpa/reports/lynn/3-3.html#term ; d.d. 26-03-1998
Http://www.clir.org/cpa/reports/weber ; d.d. 26-03-1998
Http://www.clir.org/film/discussion.html ; d.d. 26-03-1998
Http://www.nara.gov ; d.d. 20-03-1998
Http://www.oclc.org/oclc/presres/micrographic/pres_microfilm.html ; d.d. 14-03-1998
Http://www.onlineinc.com/pempress/cdr/ch1.html ; d.d. 17-03-1998
Http://www.rlg.org ; d.d. 20-03-1998
Http://www.sony-cp.com/_D/Products/Storage/WORM/FAQ.html ; d.d. 14-03-1998

Tweede Kamerstukken

Kamerstuk 1996 - 1997 - 1998, 20644, nr. 30 -33, Tweede Kamer. *Informatievoorziening openbare sector*; nota “Naar toegankelijkheid van overheidsinformatie”.

Kamerstuk 1996 - 1997- 1998, 23706, nr. 10 - 21 Tweede Kamer. *Wet op het notarisambt*.

Kamerstuk 1996 - 1997, 24036, nr. 54, Tweede Kamer. *Marktwerking, deregulering en wetgevingskwaliteit*; Brief ministers met vooortgangsnotitie.

Kamerstuk 1997 - 1998, 25533, nr. 3, Tweede Kamer. *Telecommunicatiewet.*

Kamerstuk 1997 - 1998, 25753, nr 1 - 3, Tweede Kamer. *Wijziging van Boek 2 van het Burgerlijk Wetboek en van enige andere wetten in verband met de verkorting van de bewaartermijn van boeken, bescheiden en andere gegevensdragers.*

Kamerstuk 1997 -1998, 25880, nr. 1 - 2, Tweede Kamer. *Wetgeving voor de elektronische snelweg.*

Kamerstuk 1997 - 1998, 25892, nr. 1 - 2, Tweede Kamer. *Wet bescherming persoonsgegevens.*

Bijlage 1: Voorwaarden elektronische aanbieding van afschriften van de notariële akte bij het Kadaster op te nemen in een vergunning of Interchange Agreement (juridische deel)

Het Kadaster wil het aanbieden van elektronische afschriften van notariële akten mogelijk maken in een vergunningsstelsel en daarmee binden aan voorwaarden. De onderstaande voorwaarden zijn op persoonlijke titel, mede op basis van de EDI-modelovereenkomst van EDIforum, gemaakt. De strekking van de voorwaarden is door het Kadaster als uitgangspunt genomen voor de bespreking van het vergunningsstelsel met KPMG. De voorwaarden kunnen ook worden toegepast op een Interchange Agreement, indien het Kadaster daartoe mocht besluiten.

Doelstelling en toepassingsgebied

Deze vergunning is een vergunning als bedoeld in de Kadasterwet 2000 artikel 11A.

Definities

De Dienst: de Dienst voor het kadaster en de openbare registers
De aanbieder: degene die het stuk aanbiedt bij de Dienst
De ondertekenaar: degene die het stuk dat bij de Dienst is aangeboden heeft ondertekend
De vergunninghouder: degene aan wie de vergunning is verleend
Bericht: een samenstel van stukken bedoeld voor inschrijving aangeboden door één (rechts)persoon of een samenstel van (rechts)personen
Stukken: het stuk bedoeld voor inschrijving opgemaakt door een daartoe bevoegd ambtenaar
VTIS: verzoek tot inschrijving vermeldende de essentialia vereist voor de elektronische aanbieding van het stuk bij de Dienst
Integer stuk: een stuk waarvan onomwonden vaststaat dat deze ongewijzigd is ontvangen en na ontvangst bij de ontvangende partij ongewijzigd is gebleven
Authentiek stuk: een stuk waarvan onomwonden vaststaat dat deze afkomstig is van een persoon of instantie bevoegd dit stuk te verstrekken
Technisch afgekeurd stuk: stuk welke ingevolge de technische controles van de Dienst niet als integer en/ of authentiek kan worden beschouwd

Geldigheid en totstandkoming van de vergunning

De vergunning wordt verleend aan (rechts)personen die aan de in de Technische bijlage onder artikel .... gestelde eisen hebben voldaan en blijven voldoen.
De Dienst heeft het recht de vergunning in te trekken als niet meer wordt voldaan aan de gestelde voorwaarden voor de verlening.
Indien de vergunninghouder niet binnen zes maanden nadat de test- en aansluitprocedure is aangevangen, voldoet aan de gestelde eisen en specificaties wordt de vergunning ingetrokken.

Wijze van aanbieding

De Dienst schrijft stukken slechts in in de openbare registers als deze bij aanbieding als zodanig kenbaar worden gemaakt aan de Dienst.
Alleen door een Verzoek Tot InSchrijving aan het stuk toe te voegen voldoet de aanbieder aan de eis van kenbaarheid.
Het verzoek tot inschrijving moet voldoen aan de eisen die bij uitvoeringsregeling worden gesteld.

Indien in één bericht meerdere stukken tegelijk worden verzonden, dient de identiteit van de afzender van het bericht en de integriteit van het bericht onomwonden vast te staan.

Toelaatbaarheid van digitale stukken als bewijsmateriaal

In geval van een geschil vormen de digitale openbare registers van de Dienst bewijs voor de daarin vervatte feiten, tenzij het tegendeel wordt bewezen.

Het bewijs van ontvangst heeft tot het moment van het ontvangen van het bewijs van inschrijving een bewijsrechtelijke status in de zin dat het stuk dat is vermeld op het bewijs van ontvangst is ontvangen.
De Dienst accepteert het bewijs van ontvangst als bewijsstuk als de authenticiteit en de integriteit van het bewijs van ontvangst onomwonden kan worden aangetoond. (evt. door een onafhankelijke instantie)

Het bewijs van inschrijving heeft de bewijsrechtelijke status in de zin dat het op het bewijs van inschrijving vermelde stuk is ingeschreven in de openbare registers.
De Dienst accepteert een bewijs van inschrijving als bewijsstuk als de integriteit en authenticiteit van het bewijs van inschrijving onomwonden kan worden aangetoond.

De constatering van een niet integer en/of authentiek bewijs van inschrijving respectievelijk bewijs van ontvangst moet binnen een ..... dagen bij de Dienst worden gemeld. Wordt er niet binnen deze termijn gereageerd dan wordt de bewijs van inschrijving resp. bewijs van ontvangst geacht met behoud van integriteit en authenticiteit te zijn ontvangen. Derhalve kan niet van de Dienst worden verlangt alsnog een bewijs van inschrijving betreffende het reeds ingeschreven stuk te verstrekken.

Na inschrijving hebben de volgende stukken hun (bewijsrechtelijke) functie verloren:
- bewijs van ontvangst als bedoeld in art. 3:18 BW
- het bericht
- het VTIS

Verwerking en ontvangst van de stukken

De elektronische postbussen van de Dienst en vergunninghouder zijn 24 uur per dag bereikbaar.

Stukken die onderdeel uitmaken van een groter geheel en bij aankomst bij de Dienst niet direct te herkennen zijn als stuk bedoeld voor inschrijving, worden geacht te zijn aangeboden op het tijdstip van ontvangst van het geheel waar het stuk deel van uitmaakte.

Indien de vergunninghouder de ontvangstbevestiging niet binnen één werkdag heeft ontvangen kan hij, nadat hij de Dienst daarvan in kennis heeft gesteld, het stuk als niet verzonden behandelen.

De vergunninghouder (ondertekenaar) verklaart dat bij overeenkomende hashwaarde bij respectievelijk de Dienst en de vergunninghouder en identificatie van de vergunninghouder door de Dienst met zijn in deze vergunning vermelde publieke sleutel dat de gegevens in het digitale equivalent van de notariële akte in overeenstemming zijn met de authentieke notariële akte.

Een elektronische aanbieding wordt niet geaccepteerd indien[149]:
- er geen Verzoek Tot InSchrijving aan het stuk is toegevoegd
- het stuk technisch wordt afgekeurd
- de aanbieder geen vergunning heeft om elektronisch aan te bieden
- de ondertekenaar geen vergunning heeft om elektronisch te ondertekenen

Van technische afgekeurde berichten of stukken wordt de aanbieder en/ of ondertekenaar voor zover mogelijk middels een aantekening op het bewijs van ontvangst op de hoogte gesteld.

Een technisch afgekeurd stuk of bericht wordt na ....dagen vernietigd. Binnen deze termijn kunnen betrokkenen bezwaar tegen de afkeuring indienen bij de Dienst.
Na deze termijn kan geen beroep meer worden gedaan op het disfunctioneren van de computersystemen en andere apparatuur van de Dienst alsmede op andere fouten die door het gebruik van deze apparatuur zouden kunnen zijn ontstaan.

Beveiliging van de stukken

Partijen verbinden zich ertoe de beveiligingsprocedures en -maatregelen om de stukken te beschermen tegen de risico's van onbevoegde toegang, wijziging, vernietiging, of verlies uit te voeren en in stand te houden.

Onder beveiligingsprocedures en- maatregelen wordt tevens verstaan het van de oorsprong, het verifiëren van de integriteit, de niet-afwijzing van de oorsprong en ontvangst en de vertrouwelijkheid van de stukken.

Bij elk bericht en stuk zijn de beveiligingsprocedures en -maatregelen verplicht voor het verifiëren van de oorsprong en de integriteit om de verzender te identificeren en om voor elk bericht en stuk na te gaan of het volledig en niet verminkt is.

De aanbieder van het stuk draagt zorg voor een betrouwbare wijze van het transport van het stuk. De Dienst draagt zorg voor voldoende waarborgen ter controle van de integriteit en de authenticiteit van het stuk.

Indien het gebruik van beveiligingsprocedures en -maatregelen leidt tot de afwijzing van een bericht of de ontdekking van een fout in een bericht, stelt de ontvanger de verzender hiervan direct na constatering op de hoogte.

Partijen verplichten zich de beveiligingsprocedures en -maatregelen periodiek te onderwerpen aan een onafhankelijke toetsing van een EDP-auditor.

Indien daar aanleiding voor bestaat, besluit het bestuur van de Dienst de beveiligingsprocedures en -maatregelen aan te passen. (aan het beveiligingsniveau dat het bestuur van de Dienst noodzakelijk acht.)

Registratie en opslag van stukken

De stukken elektronisch aangeboden aan de Dienst worden zo spoedig mogelijk na inschrijving vervangen door analoge equivalenten. De partij die na inschrijving en vervanging van het digitale stuk door microfilm door de Dienst is geregistreerd als ondertekenaar is aansprakelijk voor de juistheid en de volledigheid van dat stuk.

Beroep op onjuistheden en onvolledigheden in dat stuk kan vier weken na het tijdstip van aanbieding worden aangetekend bij de Dienst.

[149] Deze weigeringsgronden niet in te schrijven zijn dus andere dan reeds bestaande inschrijvingsvereisten

Na deze termijn van vier weken kan geen beroep meer worden aangetekend tegen de volledigheid en/ of juistheid van de analoge openbare registers.

(Indien blijkt dat de digitale openbare registers niet overeenstemmen met de analoge openbare registers zijn de analoge openbare registers van doorslaggevende betekenis.)

De stukken die de Dienst worden aangeboden, mogen niet door anderen dan de Dienst voor doeleinden worden gebruikt die geheel of ten dele de functie die de Dienst in het maatschappelijk verkeer uitoefent, vervullen of kunnen gaan vervullen.

Operationele eisen

Communicatiemiddel
In de technische bijlage stellen partijen het te gebruiken communicatiemiddel vast.

Operationele apparatuur
Alle apparatuur, programmatuur en diensten die nodig zijn voor het verzenden, ontvangen, vertalen, registreren, opslaan en controleren van de herkomst en de integriteit van een stuk dienen voor de partijen ter beschikking te worden gesteld en gehouden.

Technische specificaties en eisen

In de technische bijlage worden de technische, organisatorische en procedurele bijzonderheden en eisen voor het gebruik van technieken voor de elektronische aanlevering overeenkomstig de bepalingen van deze vergunning opgenomen.

Aansprakelijkheid

De Dienst is niet aansprakelijk voor door de vergunninghouder geleden verlies of schade als gevolg van te late nakoming of niet nakoming van verplichtingen op grond van de bepalingen van deze vergunning wanneer de traagheid of dat verzuim veroorzaakt werd door een verhindering die de macht van die partij te boven ging en waarmee redelijkerwijs geen rekening kon worden gehouden op het tijdstip van het aangaan van de vergunning of waarvan de gevolgen niet konden worden voorkomen of ondervangen.

Indien de vergunninghouder zich wendt tot een tussenpersoon voor diensten zoals overbrenging, registratie of verwerking van een bericht en/ of stuk, is de vergunninghouder aansprakelijk voor schade die rechtstreeks voortvloeit uit handelingen, fouten of verzuimen van deze tussenpersonen bij het verrichten van deze werkzaamheden.

Schade ontstaan door het gebruik van de (computer-)systemen van de vergunninghouder door onbevoegden kan niet aan de Dienst worden tegengeworpen.

De houder van de privésleutel is aansprakelijk voor de blijvende verificatie van zijn of haar privésleutel.

Indien een stuk integer en authentiek door de Dienst is ontvangen, is de Dienst, ingevolge art. 117 tweede lid Kadasterwet, aansprakelijk indien blijkt dat het stuk zijn integriteit en/ of authenticiteit heeft verloren.

Oplossing van geschillen

Arbitrageclausule
Alle geschillen die voortvloeien uit de voorwaarden gesteld in deze vergunning of daarmee verband houdende, met inbegrip van kwesties betreffende het bestaan, de geldigheid of de beëindiging daarvan worden ter definitieve beslechting voorgelegd aan de arbitrage van drie personen, aan te wijzen door partijen in onderling overleg of indien overeenstemming niet mogelijk is door de commissie voor de behandeling van automatiseringsverschillen, in overeenstemming met en met inachtneming van de procedurevoorschriften van de Dienst (en de Koninklijke Notariële Beroepsorganisatie).

Toepasselijk recht

Op de voorwaarden gesteld in deze vergunning is het Nederlands recht van toepassing.

Vertrouwelijkheid en bescherming van persoonsgegevens

De partij die stukken ter inschrijving in de openbare registers aan de Dienst aanbiedt, verklaart deze stukken conform de in de Wet bescherming persoonsgegevens (WBP) gestelde eisen omtrent de bescherming van persoonsgegevens te verzenden.

Formaat

Een stuk bedoeld voor inschrijving wordt overeenkomstig de uitvoeringsregeling aangeboden op het pdf-formaat.

Digitale handtekening

De digitale handtekening van de aanbieder van een bericht dient ter verificatie van de identiteit van de aanbieder.

De identificatie van de Dienst en de vergunninghouder gebeurt met asymmetrische encryptiemethoden. De sleutels die men hiervoor gebruikt zijn uniek en worden door een Certification Authority (CA) gegarandeerd.
De Dienst stelt jaarlijks een lijst vast van CA's waar de vergunninghouder zijn of haar sleutel moet deponeren.

(De CA heeft de plicht het openbare deel van de sleutelcombinatie te bewaren op een (wettelijk) voorgeschreven manier.)

De publieke sleutel van de Dienst is gedeponeerd bij abcdef onder website http://www.abcdef.com, sleutelnummer.....
De publieke sleutel van de vergunninghouder is gedeponeerd bij..... onder website.....
De publieke sleutel van de aanbieder is gedeponeerd bij..... onder website.....

Wijziging van de bovenvermelde sleutelcombinatie is slechts toegestaan indien de Dienst daar tijdig van op de hoogte wordt gesteld.

Integriteit van het stuk

De integriteit van het bericht wordt bepaald door de hashwaarde. De wijze waarop deze hashwaarde berekend wordt, is in de technische bijlage nader gespecificeerd.

De hashwaarde die de aanbieder heeft berekend wordt beveiligd met de privésleutel van de aanbieder.

De integriteit van het stuk wordt bepaald met de hashwaarde. De wijze waarop deze hashwaarde berekend wordt, is in de technische bijlage nader gespecificeerd.

De hashwaarde die de ondertekenaar heeft berekend wordt beveiligd met de privésleutel van de ondertekenaar.

Verstrekking van gegevens uit de openbare registers

De gegevens uit de openbare registers worden in hetzelfde formaat verstrekt als zij zijn aangeboden.

Bijlage 2: Verklarende woordenlijst

Analogiseren	De omzetting van digitale gegevens naar een analoog medium
Authenticatie	Authenticiteit controleren
Authenticiteit	Zekerheid ten aanzien van de echtheid van een bericht of persoon (identiteit)
Authentificatie	Authenticiteit controleren
Autorisatie	De bevoegdheid tot het aanmaken, verzenden of ontvangen van berichten
Asymmetrische encryptie	Vorm van encryptie waarbij de afzender de gegevens versleutelt met behulp van zijn geheime privésleutel en met de publieke sleutel van de beoogde ontvanger. De publieke sleutel kan alleen worden ontsleuteld met de geheime privésleutel van de ontvanger en de privésleutel van de afzender alleen met zijn publieke sleutel die openbaar is; syn. Public key system
Beveiliging	Het onleesbaar maken van gegevens en met voldoende zekerheid de integriteit en de authenticiteit van de gegevens kunnen waarborgen teneinde misbruik van de gegevens te voorkomen en/ of te constateren
Biometrie	Vorm van persoonsherkenning, of -verificatie aan de hand van een uniek lichamelijk kenmerk
Certification Authority	Organisatie die de generatie, verificatie en certificatie van elektronische sleutels verzorgd
Duurzaamheid	Raadpleegbaar, authentiek en voor mensen leesbaar blijven
EDI	Electronic Data Interchange; de geautomatiseerde, elektronische uitwisseling van gestructureerde en genormeerde gegevens tussen computers van verschillende organisaties
Encryptie	De algemene benaming voor de techniek die het mogelijk maakt gegevens onleesbaar te maken, het zgn. encrypten (versleutelen) van gegevens
Hacker	Persoon of organisatie die wederrechtelijk toegang tot eens anders computersysteem verkrijgt en daar gegevens inziet, kopieert, wijzigt of laat verdwijnen
Hashwaarde	Voor een document uniek getal waarmee de integriteit van het document mee wordt gecontroleerd. Een wijziging in het document leidt tot een andere hashwaarde
Identificatie/ Identificeren	Verificatie van de herkomst van het bericht Bewijzen dat men de persoon is, voor wie men zich uitgeeft
Integriteit	Inhoudelijk en fysiek gelijk en volledig blijven van een document
Internet	Wereldwijd computernetwerk
Kadastrale	Verzameling essentialia van stukken uit de openbare registers welke de actuele civielrechtelijke toestand van onroerend goed weergeeft en de toegangspoort tot de openbare registers vormt

registratie	Het wederrechtelijk toegang tot eens anders computersysteem verkrijgen en daar gegevens inzien, kopiëren, wijzigen en/ of laten verdwijnen
Kraken	Het risico van falende computersystemen in het jaar 2000 ten gevolge van de vaststelling van jaartallen in geheugens in twee posities (98 in plaats van 1998)
Millenium-probleem	De verzending van het bericht kan door de afzender niet worden ontkend
Non-repudiation	Techniek waarbij versleutelde gegevens, gebruikmakend van digitale sleutel, leesbaar worden gemaakt
Ontsleutelen	Verzameling van rechtskracht hebbende stukken waarin de weergave van de civielrechtelijke toestand van onroerend goed wordt gegeven
Openbare registers	Vorm van encryptie waarbij de afzender de gegevens versleutelt met behulp van zijn geheime privésleutel en de ontvanger de gegevens ontsleuteld met behulp van de publieke sleutel van de afzender, die openbaar is
Semi-assym-metrische encryptie	Aanbieder van telecommunicatiediensten
Service- provider	Pasje met een processorchip, dat daardoor zelf gegevens kan bewerken
Smartcard	Vorm van encryptie waarbij de afzender en de ontvanger van dezelfde geheime sleutel gebruik maken voor het versleutelen en het ontsleutelen van de gegevens
Symmetrische encryptie	Systeem dat in een netwerkomgeving als onafhankelijke partij tot taak heeft de authenticiteit en integriteit van het elektronisch (handels)verkeer te garanderen
Trusted Third Party	Zie encryptie
Versleutelen	Optische beeldplaat die één keer wordt beschreven en daarna slechts kan worden gelezen
WORM-plaat	

Bijlage 3: Afkortingenlijst

AKR	Automatisering Kadastrale Registratie
AWB	Algemene wet bestuursrecht
AWR	Algemene wet inzake rijksbelastingen
BW	Burgerlijk Wetboek
CA	Certification Authority
CDW	Communautair douanewetboek
CRC	Cyclic Redundancy Check
CUC	Computer Uitwijk Centrum
DOR	Digitale openbare registers
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DW	Douanewet (Stb. 553)
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Trade
EDP-audit	Electronic Data Processing-audit
Elan	Het project Elektronisch aanleveren
IA	Interchange Agreement
ISO	International Organisation for Standaardisation
KANO	Kadaster en notarisbranche
Kb	Kadasterbesluit
KNB	Koninklijke Notariële beroepsorganisatie
Kr	Kadasterregeling van 14 april 1994
KVS	Kadastraal Vastgoedinformatie Systeem
Kw	Kadasterwet (Stb. 186)
MAC	Message Authentication Code
MDC	Modification Detection Code
Necigef	Nederlands centraal instituut voor gemeenschappelijk effectenverkeer
PBO	Publiekrechterlijk Bestuursorgaan
PDF	portabel document format
RSA	Rivest, Shamir and Adleman; asymmetrische encryptie
Rv	Wetboek van Burgerlijke Rechtsvordering
Sagitta	Systeem voor de Automatische Gegevensverwerking van Invoeraangiften met Toepassing van Telematica voor het doen van aangifte
Ste	Stichting toezicht effectenverkeer
TTP	Trusted Third Party
UNCID	Uniform rules of conduct for interchange of trade data by teletransmission
VIS	verificatie informatie systeem
VROM	Volksgezondheid, ruimtelijke ordening en milieubeheer
VTIS	verzoek tot inschrijving
WBP	Wet bescherming persoonsgegevens
Wge	Wet giraal effectenverkeer (Stb. 333)
WORM-plaat	Write Once Read Many plaat
WPR	Wet persoonsregistraties (Stb. 665)
Wte	Wet toezicht effectenverkeer 1995 (Stb. 574)
WvS	Wetboek van strafrecht
ZBO	Zelfstandig Bestuursorgaan

Bijlage 4: Geraadpleegde personen

Amsterdam Exchanges
dhr. M. Eleveld, medewerker afdeling juridische zaken
dhr. T. Bouman, medewerker afdeling toezicht beurshandel

BOLERO
dhr. Bijsterveld, projectleider BOLERO

EDIFORUM
mevr. N. Docter, medewerkster EDIFORUM

Necigef
dhr. Hengeveld, directeur Necigef

Rabobank Nederland
dhr. K. Versteeg, medewerker afdeling juridische zaken
dhr. M. van Luiten, medewerker afdeling elektronische dienstverlening
dhr. Schumacher, medewerker helpdesk externe communicatie

RODOS
dhr. F. van Ipenburg, projectleider RODOS

Sagitta
dhr. E. Bruins, beleidsmedewerker Douane