Hoort bij SSG00000028
13

Nationaal TTP-project

Beleidsnotitie
CONCEPT / DISCUSSIESTUK

KPMG EDP Auditors N.V.
Amstelveen, 25 januari 1998
Dit rapport heeft 38 pagina's
RP/TS/ERL/AT/

Inhoudsopgave

0 Managementsamenvatting

Het nationaal TTP-project

Informatie- en communicatietechnologie ontwikkelt zich in een zeer hoog tempo, waarbij de maatschappelijke afhankelijkheid van deze technologie sterk toeneemt. Vertrouwen en veiligheid bij het opslaan van gegevens en het uitwisselen van berichten worden hierdoor steeds belangrijker. Een belangrijke mogelijkheid om deze aspecten te waarborgen is het gebruik van zogenaamde Trusted Third Parties (TTP's), die tezamen een TTP-infrastructuur vormen.

Mede omdat deze mogelijkheid ook internationaal sterk in de belangstelling staat, heeft de Nederlandse overheid begin 1997 besloten tot de uitvoering van het nationaal TTP-project. Deze beleidsnotitie bevat de resultaten van dit nationale TTP-project, dat is uitgevoerd onder de vlag van het Nationaal Actieplan Electronische Snelwegen. Het project is uitgevoerd onder auspiciën van het Ministerie van Verkeer en Waterstaat en het Ministerie van Economische Zaken.

Doelstellingen, scope en uitgangspunten van het nationaal TTP-project

Het nationaal TTP-project kent drie doelstellingen:
- het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten;
- het inventariseren van instrumenten waarmee deze randvoorwaarden gewaarborgd kunnen worden;
- het stimuleren van de ontwikkeling van een Nederlandse TTP-infrastructuur.

Het nationaal TTP-project heeft uitsluitend betrekking op openbare TTP-diensten. Dit zijn TTP-diensten die in beginsel voor alle burgers, bedrijven en instellingen toegankelijk zijn en/of worden aangeboden via een openbare infrastructuur.

Marktwerking en deregulering zijn in het nationaal TTP-project als geldende beleidsuitgangspunten gehanteerd. De ontwikkeling van een TTP-infrastructuur wordt hierbij als een primaire verantwoordelijkheid van de markt beschouwd.

Wat is een TTP?

Trusted Third Parties (TTP's) zijn organisaties die diensten aanbieden om de betrouwbaarheid van elektronische gegevensuitwisseling te bevorderen.

Onder betrouwbaarheid wordt verstaan:
- de *authenticiteit* van gegevens;
- de *integriteit*, ofwel de juistheid en de volledigheid van gegevens;
- de *vertrouwelijkheid* van gegevens.

Wat doet een TTP?

TTP's leveren uiteenlopende diensten aan burgers, bedrijven en instellingen, waaronder:
- diensten voor *authenticiteit* en *integriteit*, zoals het uitgeven van elektronische certificaten die worden gebruikt bij het zetten en controleren van digitale handtekeningen, waarbij de TTP de rol van Certification Authority (CA) vervult, en het bewaren en tijdstempelen van berichten;
- diensten voor *vertrouwelijkheid*, zoals het versleutelen van berichten en transacties, en het aanmaken, verstrekken en bewaren van cryptografisch sleutelmateriaal.

Waarom zijn TTP's belangrijk?

TTP's kunnen door het leveren van specifieke diensten een centrale rol spelen bij de ontwikkeling van een betrouwbare infrastructuur voor electronic commerce. Dit geldt voor TTP's die digitale handtekeningen verzorgen, maar ook voor TTP's die gegevens versleutelen of cryptografisch sleutelmateriaal verstrekken.

Burgers, bedrijven en instellingen zullen een hoge mate van vertrouwen stellen in de diensten die door een TTP worden aangeboden. Dit vertrouwen heeft niet alleen betrekking op de betrouwbaarheid van het berichtenverkeer en opgeslagen gegevens, maar ook op zaken als privacy, aansprakelijkheid, zorgvuldigheid, rechtmatige toegang tot gegevens en internationale aansluiting.

Wat is het belang van randvoorwaarden?

Door middel van randvoorwaarden kan worden zekergesteld dat het in TTP's gestelde vertrouwen gewaarborgd is en kan worden voorkomen dat de belangen van de betrokken partijen worden geschaad. Randvoorwaarden bieden daarbij een referentiekader voor de nationale en internationale wederzijdse erkenning van TTP's, die noodzakelijk is in het kader van grensoverschrijdend elektronisch handelsverkeer.

Wie stelt de randvoorwaarden?

Randvoorwaarden kunnen worden gesteld door alle partijen die een belang hebben bij een betrouwbare TTP-infrastructuur: burgers, bedrijfsleven en overheden, zowel nationaal als internationaal. In het nationaal TTP-project is ernaar gestreefd de belangen van zoveel mogelijk betrokken partijen in overweging te nemen.

Op basis van een uitgebreid onderzoek is een verzameling van randvoorwaarden opgesteld, waaraan elke TTP naar inzicht van de projectgroep zou moeten voldoen. De randvoorwaarden zijn voorgelegd aan een breed samengestelde Consultatiegroep Aanbieders en Gebruikers (CAG) en vervolgens getoetst in een viertal proefprojecten.

Hoe kunnen randvoorwaarden in de praktijk worden gerealiseerd?

Om te bewerkstelligen dat TTP's in de toekomst ook daadwerkelijk aan de opgestelde randvoorwaarden zullen voldoen, beschikt de overheid over verschillende instrumenten, die variëren van regulering en wetgeving tot deregulering en marktwerking. In het nationaal TTP-project zijn deregulering en marktwerking als uitgangspunten gekozen. Het mogelijke maatschappelijk belang van een betrouwbare TTP-infrastructuur is echter zo groot, dat betrokkenheid van de overheid noodzakelijk blijft.

De TTP-kamer

Concreet beveelt de projectgroep de oprichting van een TTP-kamer aan. De TTP-kamer is een overkoepelende organisatie, waarin, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting hebben, en waarbij de in deze beleidsnotitie opgestelde randvoorwaarden worden opgenomen in een bindend reglement.

Wat zijn de voordelen van een TTP-kamer?

Aan het oprichten van een TTP-kamer zijn als belangrijkste maatschappelijke voordelen verbonden:

- het waarborgen van de belangen van de betrokken partijen, zonder dat aanvullende wetgeving of andere vormen van regulering noodzakelijk zijn;
- het bevorderen van de noodzakelijke aansluiting en wederzijdse erkenning tussen Nederlandse TTP's en internationale TTP-infrastructuren;
- het stimuleren van de ontwikkeling van een betrouwbare TTP-infrastructuur door de markt.

Om welke randvoorwaarden gaat het?

Randvoorwaarden verschillen van TTP-dienst tot TTP-dienst. Een primair onderscheid is gemaakt tussen TTP-diensten voor authenticiteit en integriteit en TTP-diensten voor vertrouwelijkheid.

a. TTP-diensten voor authenticiteit en integriteit (digitale handtekening)

Aan deze categorie van TTP-diensten worden onder meer randvoorwaarden gesteld die betrekking hebben op betrouwbaarheid, privacy, interoperabiliteit, onafhankelijkheid, aansprakelijkheid, bezwaar en verhaal.

b. TTP-diensten voor vertrouwelijkheid (versleuteling)

Aan deze categorie van TTP-diensten worden dezelfde randvoorwaarden gesteld als onder (a). Daarnaast worden aanvullende randvoorwaarden gesteld, die betrekking hebben op rechtmatige toegang en exportcontrole.

Een TTP die beide categorieën van TTP-diensten aanbiedt, zal aan beide categorieën van randvoorwaarden moeten voldoen.

Conclusies

Overheid en bedrijfsleven dienen een aantal concrete maatregelen te treffen om de snelle ontwikkeling van een betrouwbare TTP-infrastructuur te bevorderen. Er is vooralsnog geen noodzaak tot het opstellen van aanvullende wet- en regelgeving ten aanzien van TTP's.

Overheid, aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot het oprichten van een TTP-kamer, die waarborgt dat aan de gestelde randvoorwaarden wordt voldaan. In de TTP-kamer hebben, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting.

De overheid dient de oprichting van genoemde TTP-kamer te begeleiden en te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient TTP's die zich bij de TTP-kamer aansluiten te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.

In principe dient de overheid uitsluitend diensten af te nemen van TTP's die zich bij de TTP-kamer hebben aangesloten.

De overheid dient de ontwikkeling en het gebruik van apparatuur en programmatuur die bijdraagt aan een betrouwbare TTP-infrastructuur te stimuleren.

De overheid dient het Nederlandse beleidsmodel in het kader van de wederzijdse erkenning van TTP's internationaal uit te dragen.

De overheid dient na uiterlijk twee jaar de ontwikkeling van TTP-infastructuren in Nederland te evalueren, waarbij wordt getoetst in hoeverre deze infrastructuren aan de gestelde randvoorwaarden voldoen en of de gestelde voorwaarden toereikend zijn.

1 Inleiding

Informatie- en communicatietechnologie ontwikkelt zich in een zeer hoog tempo. De maatschappelijke afhankelijkheid van deze technologie neemt eveneens sterk toe. Vertrouwen en veiligheid bij het opslaan van gegevens en het uitwisselen van berichten worden hierdoor steeds belangrijker. Daarbij zijn drie aspecten van belang. In de eerste plaats is van belang dat een partij voldoende zekerheid heeft over de identiteit van zijn communicatiepartners en de herkomst van berichten en transacties. In de tweede plaats is van belang dat gegevens niet door onbevoegden kunnen worden gewijzigd. In de derde plaats is het van belang dat geen kennis genomen kan worden van informatie door partijen voor wie deze informatie niet bestemd is. Met andere woorden: de *authenticiteit*, *integriteit* en *vertrouwelijkheid* van gegevens, berichten en transacties dienen in voldoende mate gewaarborgd moeten zijn. Deze aspecten zijn in toenemende mate bepalend voor de kwaliteit van dienstverlening in het elektronisch handelsverkeer.

Voor waarborgen van deze kwaliteitsaspecten bestaan tal van technische, organisatorische en juridische maatregelen. In de nabije toekomst kan een belangrijke rol zijn weggelegd voor derde partijen die de betrouwbaarheid van het elektronisch berichtenverkeer kunnen verhogen door het leveren van specifieke ondersteunende diensten ter zake. Zulke partijen worden internationaal algemeen aangeduid als Trusted Third Parties (TTP's). De door deze partijen geleverde ondersteunende diensten zijn in veel gevallen gebaseerd op het gebruik van cryptografische technieken. Zij hebben onder meer betrekking op het verstrekken van elektronische certificaten; het plaatsen en verifiëren van digitale handtekeningen; het vercijferen van elektronisch berichtenverkeer; het genereren, verstrekken, opslaan en/of vernietigen van cryptografisch sleutelmateriaal (sleutelbeheer); het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; en het bewaren en tijdstempelen van elektronische berichten en gegevens, al dan niet in versleutelde vorm.

Het maatschappelijk belang van TTP's bestaat primair uit het bieden van faciliteiten voor een betrouwbare en nationaal en internationaal erkende digitale handtekening, die in het elektronisch handelsverkeer noodzakelijk wordt geacht, en uit het bieden van mogelijkheden voor veilige berichtenuitwisseling voor burgers en bedrijven, waardoor de vertrouwelijkheid van het berichtenverkeer kan worden gewaarborgd.

TTP's kunnen dan ook een belangrijke rol spelen bij de opbloei van een veilige, betrouwbare en beheersbare infrastructuur voor electronic commerce. Om die reden wordt een snelle ontwikkeling van TTP-infrastructuren in brede kring zeer wenselijk geacht. Het maatschappelijk belang van een dergelijke ontwikkeling vereist duidelijkheid omtrent de rol van zowel de overheid als de marktpartijen.

In het kader van het Nationaal Actieprogramma Elektronische Snelwegen (NAP) is daarom het initiatief genomen tot het uitvoeren van het nationaal TTP-project. Dit project vindt plaats onder gemeenschappelijk opdrachtgeverschap van het Ministerie van Economische Zaken en het Ministerie van Verkeer en Waterstaat.

Doel van het project is het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten in Nederland. Daarnaast is onderzocht op welke wijze en met behulp van welke instrumenten zulke randvoorwaarden gewaarborgd zouden kunnen worden. Een andere belangrijke doelstelling van het project is het stimuleren van een verantwoorde ontwikkeling en exploitatie van een Nederlandse TTP-infrastructuur. Het project is uitgevoerd conform de door de projectgroep NAP/TTP goedgekeurde opzet en het projectplan [1,2].

Het project is opgedeeld in vier hoofdfasen, te weten:

- Fase 1 - Opstellen projectplan;
- Fase 2 - Formulering randvoorwaarden;
- Fase 3 - Begeleiding en beoordeling pilot-projecten;
- Fase 4 - Opstellen beleidsnotitie.

Het project is in april 1997 gestart en is begin 1998 afgerond.

Hoewel het project is gericht op de nationale situatie, kan het niet los worden gezien van internationale ontwikkelingen. Als belangrijkste reden geldt het inherent mondiale karakter van elektronische dienstverlening in het algemeen en electronic commerce in het bijzonder. Daarnaast geldt de noodzaak de nationale beleidsvorming reeds in de voorbereidende fase af te stemmen op internationaal beleid, zoals dat onder meer verder wordt ontwikkeld door de EU [21] en de OECD [11,20].

Het project wordt gekenmerkt door een resultaatgerichte, pragmatische aanpak, waarbij steeds nauwe afstemming wordt gezocht met internationale ontwikkelingen. De gekozen invalshoek is niet zozeer technisch als wel bestuurlijk, beleidsmatig en juridisch van aard.

In het project is verder een belangrijke plaats ingeruimd voor het inventariseren van belangen en ontwikkelingen aan zowel de vraagzijde als de aanbodzijde van de markt. Hiertoe is in het kader van het project een aantal door de markt aangedragen proefprojecten begeleid en geëvalueerd. Daarnaast is een breed samengestelde Consultatiegroep Aanbieders en Gebruikers (CAG) opgericht, die nauw bij het project is betrokken.

Tenslotte zijn marktwerking en deregulering in het nationaal TTP-project als geldende beleidsuitgangspunten gehanteerd. Dit impliceert onder meer dat de ontwikkeling van een TTP-infrastructuur als een primaire verantwoordelijkheid van de markt wordt beschouwd.

De inhoud van deze beleidsnotitie is als volgt. Sectie 2 bevat een beschrijving van het gehanteerde begrippenkader, de context en de scope van het nationaal TTP-project. Sectie 3 gaat in op de randvoorwaarden inzake TTP-diensten voor authenticiteit en integriteit van gegevens, berichten en transacties. Sectie 4 gaat in op randvoorwaarden inzake TTP-diensten voor vertrouwelijkheid van gegevens, berichten en transacties. Sectie 5 gaat in op de mogelijke instrumenten voor het waarborgen van deze randvoorwaarden. Sectie 6 bevat de conclusies en aanbevelingen van het project.

Bijlage 1 bevat de resultaten van de inventarisatie van de proefprojecten, die is uitgevoerd door de EDP AUDIT POOL. Bijlage 2 bevat een opsomming van de in dit project geraadpleegde bronnen. Bijlage 3 beschrijft de samenstelling van de projectgroep en de Consultatiegroep Aanbieders en Gebruikers.

2 Omschrijving, context en scope

In deze sectie komen achtereenvolgens aan de orde: de betekenis die in de context van het nationaal TTP-project aan de term TTP wordt gehecht, de bij het nationaal TTP-project betrokken partijen, een classificatie van TTP-diensten op basis van verschillende criteria, de stand van zaken rond nationale en internationale beleidsontwikkeling ter zake, de mogelijke randvoorwaarden die op TTP's en TTP-diensten van toepassing zijn, en het instrumentarium om deze randvoorwaarden in de praktijk te waarborgen.

2.1 Omschrijving

De term Trusted Third Party (TTP) is inmiddels algemeen ingeburgerd, maar blijkt soms op uiteenlopende wijzen te worden geïnterpreteerd. In het kader van deze beleidsnotitie wordt de volgende werkdefinitie gehanteerd:

Een Trusted Third Party (TTP) is een betrouwbare derde partij die diensten aanbiedt om de betrouwbaarheid van de geautomatiseerde verwerking, uitwisseling en opslag van gegevens tussen partijen te waarborgen.

Onder betrouwbaarheid wordt verstaan:
- de *authenticiteit* van gegevens;
- de *integriteit*, ofwel de juistheid en de volledigheid van gegevens;
- de *vertrouwelijkheid* van gegevens.

Bedoelde TTP-diensten kunnen onder meer betrekking hebben op: het verstrekken van digitale certificaten; het plaatsen en verifiëren van digitale handtekeningen; het versleutelen van elektronisch berichtenverkeer en/of gegevens; het genereren, verstrekken, opslaan en/of vernietigen van cryptografisch sleutelmateriaal (sleutelbeheer); het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; het bewaren en tijdstempelen van elektronische berichten.

2.2 Betrokken partijen

Bij de ontwikkeling en het gebruik van TTP-infrastructuren is een groot aantal nationale en internationale partijen betrokken. Hierbij kan primair onderscheid worden gemaakt tussen marktpartijen en overheid. Er geldt echter een bijzondere situatie voor partijen met een wettelijke bevoegdheid tot het verkrijgen van elektronische gegevens; het betreft hierbij zowel de marktpartijen als de overheid.

2.2.1 Marktpartijen

De belangrijkste rol is weggelegd voor de *marktpartijen*, ofwel de aanbieders en gebruikers van TTP-diensten. TTP-diensten kunnen worden aangeboden door zeer uiteenlopende commerciële en niet-commerciële organisaties die al dan niet binnen een specifiek marktsegment opereren. Anderzijds kunnen TTP-diensten worden afgenomen door bedrijven, instellingen en burgers. In het nationaal TTP-project is de inbreng van de marktpartijen gewaarborgd door nauwe afstemming met een hiertoe opgerichte Consultatiegroep Aanbieders en Gebruikers, waarvan de samenstelling is weergegeven in bijlage 3.

2.2.2 Overheid

Gezien het maatschappelijk belang zal een rol voor de *overheid* zijn weggelegd in de vorm van beleid, stimulering, wet- en regelgeving en/of toezicht. De algemene gedachte hierbij is dat de overheid

tenminste tot taak heeft om, gebruik makend van het ter beschikking staande instrumentarium, samenleving en burgers te beschermen door onder meer het waarborgen van de betrouwbaarheid van de TTP-dienst, het bevorderen van de nationale en internationale interoperabiliteit, het beschermen van de persoonlijke levenssfeer van de gebruikers van een TTP-dienst en het waarborgen van de rechtmatige toegang tot elektronische gegevens. Daarnaast kan de overheid de totstandkoming van een veilige en betrouwbare TTP-infrastructuur stimuleren. Tenslotte kan de overheid als marktpartij opereren - als afnemer, maar ook als aanbieder van TTP-diensten. De bij het nationaal TTP-project betrokken ministeries zijn weergegeven in bijlage 3.

2.3 Classificatie van TTP-diensten

TTP-diensten kunnen op verschillende wijzen worden geclassificeerd. Deze classificatie is noodzakelijk, omdat het type van een TTP in veel gevallen bepalend is voor de randvoorwaarden die aan de TTP worden gesteld. Achtereenvolgens komen aan de orde: de functionaliteit van de TTP-dienst; de wijze van sleutelbeheer; de openbaarheid van de TTP-dienst; de topologie van de TTP-dienst; en het toepassingsgebied van de TTP-dienst.

.3.1 Functionaliteit van de TTP-dienst

Zoals reeds in de hierboven gegeven werkdefinitie naar voren komt, kan een TTP-dienst uiteenlopende vormen aannemen. Hierbij bestaat een wezenlijk onderscheid tussen TTP-diensten die gericht zijn op het waarborgen van de *authenticiteit* en/of *integriteit* van gegevens, berichten en transacties, en TTP-diensten die gericht zijn op het waarborgen van de *vertrouwelijkheid* van gegevens, berichten en transacties:

a. TTP-diensten voor authenticiteit en integriteit

Onder TTP-diensten voor *authenticiteit en integriteit* vallen onder meer: het verstrekken van digitale certificaten (de TTP vervult hierbij de rol van Certification Authority, CA); het plaatsen en verifiëren van digitale handtekeningen; het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; het beheer van cryptografisch sleutelmateriaal voor authenticiteit en integriteit, uitgezonderd de opslag van geheim sleutelmateriaal ter zake (*private keys*); en het tijdstempelen van elektronische berichten.

b. TTP-diensten voor vertrouwelijkheid

Onder TTP-diensten voor *vertrouwelijkheid* vallen onder meer: het versleutelen van elektronisch berichtenverkeer; en het beheer van cryptografisch sleutelmateriaal voor vertrouwelijkheid.

Het aldus gemaakte onderscheid wordt ook in internationaal verband gemaakt en is in recente internationale beleidsdocumenten van de EU, OECD en APEC [21, 11, 20] als zodanig aanvaard. Het onderscheid is in die zin fundamenteel, dat niet alleen de TTP-diensten zelf, maar ook de hierop van toepassing zijnde randvoorwaarden verschillen. Zo ligt bij TTP-diensten voor *authenticiteit en integriteit* een zware nadruk op randvoorwaarden ten aanzien van betrouwbaarheid, privacy en interoperabiliteit, zoals genoemd in sectie 3, terwijl bij TTP-diensten voor *vertrouwelijkheid* bovendien de in sectie 4 genoemde aanvullende randvoorwaarden ten aanzien van rechtmatige toegang tot gegevens gelden.

Een en ander impliceert overigens niet dat een TTP zijn diensten voor *authenticiteit en integriteit* en zijn diensten voor *vertrouwelijkheid* altijd gescheiden aanbiedt; ook een combinatie van beide diensten is mogelijk. Gegeven de huidige stand van de techniek kunnen beide TTP-diensten eenvoudig en efficiënt met behulp van één enkele technische oplossing worden gerealiseerd.

Het aanbieden van gescheiden oplossingen voor de onderscheiden klassen van TTP-diensten behoort echter zeer wel tot de mogelijkheden. Zo kan een TTP-dienst voor authenticiteit en integriteit worden geboden op basis van een toegevoegde digitale handtekening, waarbij het bericht zelf onvercijferd blijft. Een aanvullende TTP-dienst voor vertrouwelijkheid kan dan bijvoorbeeld bestaan uit het aanleveren van additioneel sleutelmateriaal voor de versleuteling van het bericht zelf. Sleutelmateriaal voor authenticiteit en integriteit kan door de gebruiker eenvoudig ook voor vertrouwelijkheid worden aangewend, tenzij hiertegen door de TTP specifieke technische maatregelen zijn getroffen; voor meer details zij verwezen naar [11, 21].

De internationale aanvaarding van het beleidsmatige onderscheid tussen TTP-diensten voor authenticiteit en integriteit en TTP-diensten voor vertrouwelijkheid kan ertoe leiden dat de TTP-markt deze diensten in toenemende mate gescheiden zal aanbieden. Hoewel gescheiden oplossingen op de markt beschikbaar zijn, worden beide diensten door enkele proefprojecten niet gescheiden aangeboden.

2.3.2 *Wijze van sleutelbeheer*

Een tweede onderscheidend criterium is de wijze waarop het sleutelbeheer is ingericht. Onder sleutelbeheer wordt hierbij verstaan: het genereren, opslaan, distribueren, vernietigen en/of intrekken van sleutelmateriaal. Voor de inrichting van sleutelbeheer bestaan verschillende varianten, waarbij de TTP in meer of mindere mate bij het sleutelbeheer betrokken is.

In het ene uiterste geval zal de TTP zelf sleutelmateriaal genereren, opslaan, distribueren en na verloop van tijd vernietigen. In het andere uiterste geval is de gebruiker zelf volledig verantwoordelijk voor het sleutelbeheer. Ook tussenvormen zijn mogelijk, zoals een vorm waarbij de gebruiker zelf het sleutelmateriaal genereert en zijn openbare sleutel bij een TTP deponeert, of zelfs een vorm waarbij de gebruiker, zij het zeer waarschijnlijk onder strikte voorwaarden, geheim sleutelmateriaal bij een TTP deponeert.

Bij het merendeel van de in fase 3 onderzochte proefprojecten genereert de gebruiker zelf het sleutelmateriaal, waarna hij de openbare sleutel bij een TTP deponeert. De desbetreffende aanbieders hebben geen intenties om te voorzien in de opslag van geheim sleutelmateriaal.

2.3.3 *Openbaarheid van de TTP-dienst*

De openbaarheid van een TTP-dienst vormt een derde belangrijk onderscheidend criterium bij het bepalen van de wenselijke en/of noodzakelijke invloed van de overheid ter zake.

Niet-openbare TTP-diensten worden hierbij gedefinieerd als TTP-diensten die uitsluitend gebruik maken van een eigen infrastructuur en uitsluitend binnen één organisatie worden gebruikt. Voorbeelden hiervan zijn TTP's binnen één bedrijf of instelling, of TTP's die exclusief worden gebruikt door een beperkt aantal bedrijven of instellingen die onderling berichten uitwisselen. Daartegenover staan *openbare TTP-diensten*, gedefinieerd als TTP-diensten die in beginsel gebruik maken van een openbare infrastructuur en/of voor alle burgers, bedrijven en instellingen toegankelijk zijn.

Het nationaal TTP-project heeft uitsluitend betrekking op openbare TTP-diensten.

2.3.4 *Topologie van de TTP-dienst*

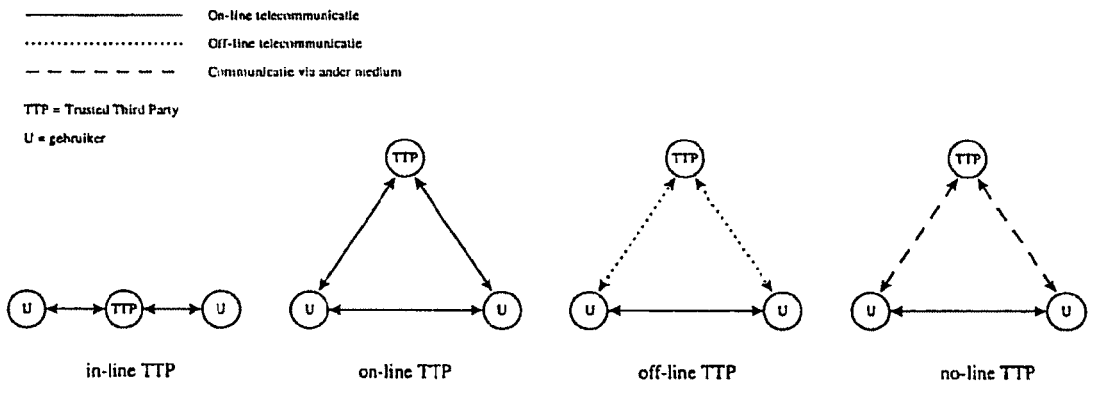
De topologie van een TTP-dienst - in het kader van het nationaal TTP-project geïnterpreteerd als: de positie die de TTP-dienst inneemt in de communicatie tussen partijen - wordt als vierde belangrijke indelingscriterium gehanteerd. Gegeven de huidige stand van de techniek kan op dit moment onderscheid worden gemaakt tussen drie TTP-topologieën, waarbij wordt aangesloten op gangbare definities van onder meer het ETSI [11] (zie figuur 1):

- de *in-line TTP*, die met elk van de aangesloten partijen een direct of indirect telecommunicatiepad onderhoudt, waarbij deze partijen onderling uitsluitend via de TTP met elkaar communiceren;

- de *on-line TTP*, die met tenminste één van de met elkaar communicerende partijen een telecommunicatiepad onderhoudt, terwijl deze partijen onderling ook een afzonderlijk telecommunicatiepad onderhouden;
- de *off-line TTP*, die gedurende de communicatie tussen twee partijen geen telecommunicatiepad met deze partijen onderhoudt, maar de benodigde communicatie op een ander tijdstip voert.

Daarnaast wordt in deze beleidsnotitie een vierde TTP-type onderscheiden, dat kan worden beschouwd als een bijzondere variant van de off-line TTP:

- de *no-line TTP*, die gebruik maakt van andere communicatiemedia dan een telecommunicatienetwerk, zoals post.



Figuur 1 - Topologie van de TTP-dienst

Het hier gemaakte onderscheid is om twee redenen van belang. Allereerst zal de topologie van de TTP-dienst mede bepalend zijn voor mogelijke wetgeving die op de TTP van toepassing is; zo vallen in-line, on-line en off-line TTP's wel onder de Telecommunicatiewet (zie sectie 4), maar no-line TTP's niet. Daarnaast is de topologie van de TTP-dienst van invloed op specifieke problemen die optreden in het kader van rechtmatige toegang; zie hiervoor sectie 4.

2.3.5 *Toepassingsgebied van de TTP-dienst*

Het vijfde indelingscriterium voor TTP-diensten is het toepassingsgebied. In de toekomst kunnen TTP-diensten in uiteenlopende sectoren van de maatschappij voor verschillende toepassingen worden aangewend. Voorbeelden hiervan zijn de financiële sector, de dienstensector, de zorgsector, de accountancy, de overheidssector, de detailhandel en het notariaat.

Binnen elke sector kunnen TTP-diensten worden gebruikt voor de ondersteuning van specifieke toepassingen, producten en/of diensten. Elke toepassing zal daarbij specifieke eisen aan de gebruikte TTP-dienst stellen, waardoor uiteenlopende TTP-diensten zullen ontstaan. Een dergelijke differentiatie geldt in de huidige samenleving voor vrijwel elke technologie en elke dienst. Reeds op dit moment worden in de markt "op maat gesneden" TTP-diensten aangeboden, die zijn afgestemd op de eisen van specifieke toepassingen. Het is overigens denkbaar dat één TTP-dienst voor de ondersteuning van meerdere toepassingsgebieden zal worden gebruikt, waarbij de eisen van de hoogst geclassificeerde toepassing zullen prevaleren.

De differentiatie naar toepassingsgebieden van TTP's roept vragen op omtrent de haalbaarheid en wenselijkheid van het formuleren van een algemeen geldend stelsel van randvoorwaarden dat zowel

noodzakelijk als voldoende is voor elke mogelijk denkbare TTP-dienst. Hierbij zijn twee factoren van belang.

In de eerste plaats zullen naast algemene wettelijke en overige randvoorwaarden ook specifieke eisen op een TTP-dienst van toepassing zijn, die voortvloeien uit specifieke wet- en regelgeving voor de door de TTP-dienst ondersteunde maatschappelijke functie. Een voorbeeld hiervan is de vigerende wet- en regelgeving voor het bankwezen, het notariaat, de advocatuur, de accountancy en de zorgsector, die onverkort op in deze sectoren gebruikte TTP-diensten van toepassing zal zijn.

In de tweede plaats speelt het kostenaspect een rol. Een stelsel van randvoorwaarden dat is toegesneden op toepassingen die zeer hoge eisen stellen aan een TTP-dienst is naar alle waarschijnlijkheid onnodig kostbaar voor toepassingen die lagere eisen stellen aan een TTP-dienst. De ontwikkeling van minder kostbare TTP-diensten - die een substantieel deel van het totale volume aan TTP-diensten kunnen vormen - zal door een al te stringent stelsel van randvoorwaarden niet worden gestimuleerd, maar juist worden belemmerd. Het formuleren van een te stringent stelsel van randvoorwaarden kan derhalve leiden tot een situatie die strijdig is met het doel van het nationaal TTP-project, namelijk het stimuleren van de ontwikkeling van een nationale TTP-infrastructuur.

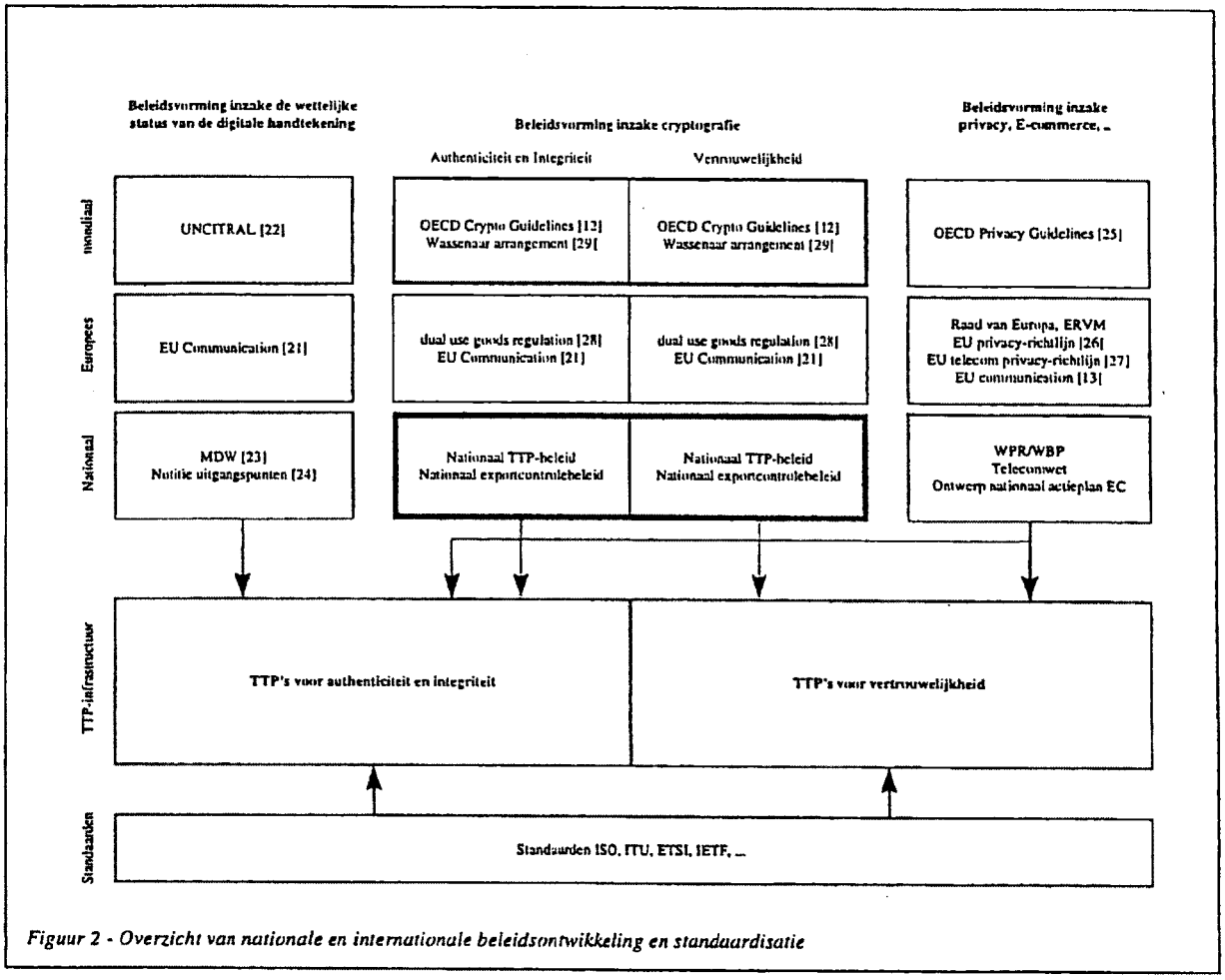
Om bovengenoemde reden is ervoor gekozen niet zozeer een volledig en alomvattend stelsel van mogelijke randvoorwaarden voor alle mogelijke TTP-diensten te definiëren, als wel een stelsel van minimumrandvoorwaarden op te stellen dat voor alle klassen van TTP-diensten van toepassing moet zijn. Aanvullende randvoorwaarden kunnen dan door de markt worden opgesteld voor nog te onderscheiden klassen van TTP's, waarbij het toepassingsgebied of de vereiste graad van betrouwbaarheid als criteria voor classificatie zouden kunnen dienen.

2.4 Marktontwikkeling

De markt voor TTP-diensten bevindt zich in de beginfase van zijn ontwikkeling. Deze ontwikkeling verloopt minder stormachtig dan nog maar kort geleden werd verwacht. Hetzelfde geldt voor de ontwikkeling en aanvaarding van internationale standaarden ter zake. De bevindingen uit de inventarisatie van de proefprojecten onderbouwen deze stelling. Naar alle waarschijnlijkheid spelen hierbij vele factoren een rol. Zo lijkt de ontwikkeling van TTP-diensten mede te wachten op een verdere ontwikkeling van electronic commerce, terwijl de opbloei van electronic commerce mede afhankelijk lijkt te zijn van de beschikbaarheid van een betrouwbare TTP-infrastructuur. Het nationaal TTP-project heeft tot doel de ontwikkeling van een TTP-infrastructuur te stimuleren en zo de gesignaleerde impasse te doorbreken.

2.5 Beleidsontwikkeling

De nationale en internationale beleidsontwikkeling inzake TTP's staat niet op zichzelf, maar moet worden geplaatst binnen de bredere context van de ontwikkeling van internationaal en nationaal beleid inzake: cryptografie; de juridische status van digitale handtekeningen; privacy en electronic commerce. Daarnaast speelt de ontwikkeling van internationale standaarden voor TTP's, waaronder Certification Authorities (CA's). In figuur 2 is de context van het nationaal TTP-project schematisch weergegeven. Voor meer informatie zij verwezen naar de referenties in figuur 2.



Figuur 2 - Overzicht van nationale en internationale beleidsontwikkeling en standaardisatie

2.6 Totstandkoming randvoorwaarden

In het kader van het nationaal TTP-project is geïnventariseerd aan welke randvoorwaarden een TTP-infrastructuur zou moeten voldoen. Deze inventarisatie heeft als volgt plaatsgevonden:

- de betrokken ministeries hebben aangegeven welke randvoorwaarden in het kader van hun specifieke taakstelling en problematiek noodzakelijk worden geacht;
- vervolgens is een inventarisatie en analyse uitgevoerd van randvoorwaarden zoals die in nationale en internationale beleidsdocumenten, discussiestukken en standaarden naar voren komen;
- de hieruit voortvloeiende verzameling mogelijke randvoorwaarden is in conceptvorm ter commentaar voorgelegd aan de leden van de projectgroep van het nationaal TTP-project en aan de leden van de Consultatiegroep Aanbieders en Gebruikers;
- de mogelijke randvoorwaarden zijn door de EDP AUDIT POOL verder uitgewerkt in deelaspecten en gehanteerd als inventarisatiecriteria voor een viertal pilot-projecten;
- het commentaar van de leden van de projectgroep, het commentaar van de Consultatiegroep Aanbieders en Gebruikers en de resultaten van de inventarisatie van de proefprojecten zijn in onderhavige beleidsnotitie verwerkt.

De resulterende randvoorwaarden worden nader beschreven in de secties 3 en 4, waarbij primair onderscheid wordt gemaakt tussen randvoorwaarden inzake TTP's voor authenticiteit en integriteit en randvoorwaarden inzake TTP's voor vertrouwelijkheid.

2.7 Instrumenten voor het waarborgen van randvoorwaarden

Naast het formuleren van de randvoorwaarden zelf is een belangrijke doelstelling van het nationaal TTP-project geweest te onderzoeken op welke wijze deze randvoorwaarden binnen een zich ontwikkelende TTP-infrastructuur kunnen worden gewaarborgd.

Allereerst zal de vereiste borging haar grondvesten moeten vinden in bestaande wet- en regelgeving. Nederland kent een uitgebreide algemene en specifieke wet- en regelgeving die mede is gericht op het beschermen van de maatschappij in het algemeen en de consument in het bijzonder. Deze bescherming wordt mede gerealiseerd door het waarborgen van de kwaliteit van de door marktpartijen geleverde diensten en het vaststellen van een vorm van toezicht daarop. Bestaande wet- en regelgeving ter zake zal ook onverkort op TTP-diensten van toepassing zijn.

Pas als bestaande wet- en regelgeving onvoldoende blijkt om de noodzakelijke randvoorwaarden te kunnen waarborgen, dienen aanvullende oplossingen te worden overwogen. Overheid en bedrijfsleven beschikken hiervoor over een aantal instrumenten die variëren in de mate van regulering en overheidsinvloed. In dit geval is sprake van een spectrum, met strikte regulering aan het ene uiterste, volledige deregulering aan het andere uiterste, en tal van mengvormen daar tussenin, zoals een vergunningenstelsel, aansluiting bij een bij wet ingestelde of wettelijk erkende organisatie met zelfregulering, aansluiting bij een door de marktpartijen zelf ingestelde organisatie met zelfregulering, certificatie met overheidstoezicht, en certificatie zonder overheidstoezicht. Deze vormen zullen verder worden besproken in sectie 5.

3 Randvoorwaarden inzake TTP-diensten voor authenticiteit en integriteit

3.1 Inleiding

Onder TTP-diensten voor *authenticiteit en integriteit* vallen onder meer: het verstrekken van digitale certificaten; het plaatsen en verifiëren van digitale handtekeningen; het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; het beheer van cryptografisch sleutelmateriaal voor authenticiteit en integriteit, met uitzondering van de opslag van geheim sleutelmateriaal *(private keys)*; en het tijdstempelen van elektronische berichten. Binnen TTP-diensten voor authenticiteit en integriteit wordt vaak onderscheid gemaakt tussen de Registration Authority (RA), die de legitimatie van aangesloten gebruikers verzorgt, en de Certification Authority (CA), die electronische certificaten ten behoeve van deze gebruikers verstrekt.

Over een aantal randvoorwaarden die op deze categorie van TTP's van toepassing zijn, bestaat bij de betrokken partijen een zekere consensus. Deze randvoorwaarden hebben onder meer betrekking op de wettelijke status van digitale handtekeningen, op de betrouwbaarheid van de geleverde TTP-dienst en de TTP zelf, op de bescherming van de persoonlijke levenssfeer, en op internationale interoperabiliteit.

Een groot aantal van de in het nationaal TTP-project ingebrachte randvoorwaarden is algemeen van aard en is, als normale eisen van professionaliteit, in wezen van toepassing op elke dienst; andere randvoorwaarden zijn wel specifiek voor TTP-diensten. De in deze sectie beschreven randvoorwaarden kunnen worden beschouwd als minimumrandvoorwaarden die in feite op elke categorie van TTP-diensten van toepassing zijn, ongeacht het toepassingsgebied.

Op TTP-diensten voor authenticiteit en integriteit zijn in beginsel geen randvoorwaarden inzake rechtmatige toegang van toepassing, mits de TTP, door het treffen van specifieke maatregelen, voldoet aan de voorwaarde dat de bedoelde TTP-dienst en het desbetreffende sleutelmateriaal uitsluitend voor authenticiteit en integriteit kunnen worden gebruikt. Alvorens in te gaan op de randvoorwaarden zelf, zal eerst de juridische status van digitale handtekeningen worden besproken.

3.2 Juridische status van digitale handtekeningen

De juridische status van digitale handtekeningen is op dit moment onderwerp van onderzoek. In internationaal verband vindt beleidsvorming plaats door UNCITRAL [22]. In Europees verband is een mededeling uitgevaardigd. Hierin wordt aangekondigd dat de EU toewerkt naar een Europese richtlijn ten aanzien van wederzijdse erkenning van digitale handtekeningen. Het Ministerie van Justitie en het Ministerie van Economische Zaken zijn momenteel betrokken bij een MDW-project ter zake [23]. Daarnaast werkt een projectgroep onder voorzitterschap van het Ministerie van Justitie aan een notitie inzake uitgangspunten van wetgeving op de elektronische snelweg [24], waarbij onder meer aandacht wordt geschonken aan de juridische status van digitale handtekeningen.

Onderzoek naar de juridische status van digitale handtekeningen is gerelateerd aan het nationaal TTP-project, maar valt buiten de voor dit deelproject gedefinieerde scope. De onderliggende TTP-infrastructuur is geen voorwaarde voor de juridische erkenning van de digitale handtekening, maar zal wel bijdragen aan de bewijskracht ervan.

3.3 Betrouwbaarheid

Verreweg de belangrijkste randvoorwaarden die in het nationaal TTP-project naar voren zijn gekomen, hebben betrekking op de betrouwbaarheid van zowel de TTP-dienst als de organisatie die deze dienst levert: de TTP zelf. De gebruikers van een TTP-dienst zullen een hoog vertrouwen moeten kunnen stellen in de organisatie die deze TTP-dienst aanbiedt. Voor TTP's is betrouwbaarheid dan ook van essentieel belang. Deze eis beperkt zich niet tot individuele TTP's, maar heeft betrekking op de gehele internationale TTP-infrastructuur.

De ruime betekenis van het begrip betrouwbaarheid maakt een nadere opsplitsing in deelaspecten noodzakelijk, die kunnen worden onderverdeeld in eisen ten aanzien van de TTP-organisatie en eisen ten aanzien van de TTP-dienst. In het kader van het nationaal TTP-project is een aantal betrouwbaarheidseisen geformuleerd, die navolgend zullen worden toegelicht.

3.3.1 Betrouwbaarheid van de TTP-organisatie

De volgende betrouwbaarheidseisen zijn van toepassing op de TTP:

- *rechtmatig handelen* - TTP's dienen in elke zin van het woord te handelen in overeenstemming met het nationaal en internationaal recht;
- *financiële positie* - de financiële positie van de TTP-organisatie dient voldoende waarborgen te bieden ten aanzien van de betrouwbaarheid en continuïteit van de TTP-dienst;
- *bedrijfscontinuïteit* - de continuïteit van TTP-diensten dient zoveel mogelijk te worden gewaarborgd, ook in geval van overname, fusie, bedrijfsstaking of faillissement;
- *beveiliging* - de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en informatiesystemen binnen de TTP-organisatie dienen door het treffen van een adequaat stelsel van beveiligingsmaatregelen te zijn gewaarborgd tegen schade voortvloeiend uit onder meer calamiteiten, storingen, alsmede opzettelijk en onopzettelijk menselijk handelen. De in 1994 door het Ministerie van Economische Zaken uitgegeven Code voor Informatiebeveiliging lijkt een goede basis te bieden voor de beveiliging van TTP-organisaties, waarbij de hoge betrouwbaarheidseisen die aan een TTP worden gesteld aanvullende maatregelen noodzakelijk kunnen maken. De Information Technology Security Evaluation Criteria (ITSEC) en daarop mede gebaseerde Common Criteria bieden hierbij wellicht een goede basis voor de evaluatie van de gebruikte IT-producten;
- *personeel* - eigenaren, aandeelhouders, directie, management en personeel van de TTP-organisatie moet kunnen worden vertrouwd ten aanzien van de haar toevertrouwde taken;
- *authenticatie* - bij het nemen van beslissingen en het uitvoeren van handelingen door management en medewerkers van de TTP-organisatie dient de identiteit van de betrokken personen steeds ondubbelzinnig te worden vastgesteld;
- *autorisatie* - specifieke bevoegdheden dienen duidelijk en ondubbelzinnig aan specifieke functies en functionarissen binnen de TTP-organisatie te zijn toegewezen;
- *functiescheiding* - er dient een adequate controletechnische scheiding te bestaan tussen beschikkende, bewarende, uitvoerende en controlerende functies binnen de TTP-organisatie, onder meer inzake sleutelbeheer;
- *toezicht* - om de betrouwbaarheid van een TTP-organisatie te waarborgen, zal regelmatig door een onafhankelijke instantie moeten worden gecontroleerd of de TTP-organisatie voldoet aan een vooraf opgesteld pakket van eisen en randvoorwaarden, en of dit pakket van eisen en randvoorwaarden toereikend is om de gewenste graad van betrouwbaarheid te bereiken. Voor het realiseren van een dergelijke vorm van toezicht zijn verschillende modellen denkbaar, die in sectie 5 worden uitgewerkt. Tevens kan op deze plaats nogmaals worden benadrukt dat op TTP-organisaties die diensten leveren ten behoeve van specifieke maatschappelijke functies ook de bijbehorende wettelijke vereisten ten aanzien van toezicht en controle van toepassing zullen zijn;

- *zorgvuldigheid* - de TTP dient uitsluitend gegevens aan derden te verstrekken indien hiertoe een aantoonbare wettelijke grondslag bestaat. Het is van groot belang dat de gebruikers van een TTP-dienst erop kunnen vertrouwen dat een eventuele verstrekking van gegevens uitsluitend onder strikte voorwaarden zal plaatsvinden, en dan nog alleen indien hiertoe een aantoonbare wettelijke grondslag bestaat, waarbij de TTP-organisatie zich van de rechtmatigheid van een verzoek tot medewerking zal moeten overtuigen. Geheime cryptografische sleutels die uitsluitend worden gebruikt voor authenticiteit en integriteit (*private keys*) zullen nooit en te nimmer aan derden mogen worden verstrekt;
- *beheer van bedrijfsmiddelen* - de ontwikkeling en het beheer van informatietechnologie en andere bedrijfsmiddelen binnen de TTP dienen te zijn ingericht volgens algemeen aanvaarde kwaliteitsnormen;
- *onafhankelijkheid* - de TTP dient niet gebonden te zijn aan één of meer bestaande partijen en geen belang te hebben bij de te beveiligen informatie;
- *transparantie* - de TTP dient inzicht te geven in de gehanteerde werkwijze, om toetsing van de TTP-organisatie en de TTP-dienst mogelijk te maken.

.2 Betrouwbaarheid van de TTP-dienst

De volgende betrouwbaarheidseisen zijn van toepassing op de TTP-dienst:

- *betrouwbare technologie* - de gebruikte technologie dient voldoende betrouwbaar te zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van de geautomatiseerde gegevensverwerking te waarborgen;
- *documentatie* - het ontwerp, de implementatie, het beheer en het gebruik van de TTP-dienst dienen adequaat gedocumenteerd te zijn;
- *sleutelbeheer* - sleutelbeheer dient op betrouwbare wijze te geschieden.

In tabel 1 is een overzicht van randvoorwaarden inzake betrouwbaarheid weergegeven.

TTP-organisatie	**TTP-dienst**
rechtmatig handelen	betrouwbare technologie
financiële positie	documentatie
bedrijfscontinuïteit	sleutelbeheer
beveiliging	
personeel	
authenticatie	
autorisatie	
functiescheiding	
toezicht	
zorgvuldigheid	
beheer van bedrijfsmiddelen	
transparantie	
onafhankelijkheid	

Tabel 1. Overzicht van randvoorwaarden inzake betrouwbaarheid

Tenslotte zij opgemerkt dat de betrouwbaarheid van een TTP-dienst mede afhankelijk zal zijn van de betrouwbaarheid van de gebruikers van die dienst. Daardoor kunnen niet alleen aan de aanbieders, maar ook aan de gebruikers van een TTP-dienst eisen worden gesteld.

3.4 Privacy

Inzake privacy is zowel door de overheid als door enkele marktpartijen benadrukt dat de bescherming van de persoonlijke levenssfeer van de gebruikers van een TTP-dienst bijzondere aandacht behoeft. De Wet persoonsregistraties, die, onder invloed van de Europese privacy-richtlijn [26], naar verwachting in de loop van 1998 zal worden vervangen door de Wet bescherming persoonsgegevens, is vanzelfsprekend ook op TTP's van toepassing. Daarnaast is er de EU Telecommunicatie Privacy-richtlijn [27], die is geïmplementeerd in de nieuwe Telecommunicatiewet.

In het geval van TTP's valt onder de noemer privacy onder meer te denken aan de beveiliging van certificaten en/of openbare sleutels. Een certificaat heeft hierbij als primaire functie een identiteit te binden aan de publieke sleutel van een sleutelpaar. De geheime sleutel van het sleutelpaar is alleen behouden aan de eigenaar. Daarnaast kan een certificaat andere informatie bevatten. Een verzameling certificaten moet daarom worden beschouwd als een persoonsregistratie.

Om de herleidbaarheid van certificaten en sleutelmateriaal naar natuurlijke personen te beperken, kan worden overwogen gebruik te maken van privacy-enhanced technology (PET). Een voorbeeld is het gebruik van pseudo-identiteiten bij de uitwisseling van persoonsgegevens.

Aanbevolen wordt een privacy-gedragscode voor TTP's op te stellen, waarin het treffen van nadere maatregelen ter zake verder wordt uitgewerkt. Deze gedragscode kan als randvoorwaarde in een certificeringstraject (zie sectie 5) worden ingebouwd.

3.5 Interoperabiliteit

De ontwikkeling van een betrouwbare, breed toepasbare en economisch haalbare TTP-infrastructuur voor authenticiteit en integriteit kan slechts succesvol zijn, indien nauwe aansluiting wordt gevonden bij nationale en internationale ontwikkelingen.

Deze aansluiting heeft twee aspecten.

Allereerst moeten de technische interoperabiliteit tussen nationale en internationale TTP-infrastructuren gewaarborgd zijn. De internationale situatie kent een groot aantal technische standaarden op het gebied van interfaces, protocollen en algoritmen, waartoe onder meer de standaarden van de ETSI, ITU, ISO en IETF en verschillende *de facto* standaarden gerekend mogen worden. Overheden kunnen bij standaardisatie een stimulerende en activerende rol spelen.

In de tweede plaats is in het kader van interoperabiliteit wederzijdse erkenning van nationale en internationale TTP's noodzakelijk. Hierbij geldt dat wederzijdse erkenning pas mogelijk is indien deze TTP's voldoen aan een gelijkwaardig stelsel van randvoorwaarden, waarbij in het internationale geval ook moet worden gestreefd naar de wederzijdse erkenning van digitale handtekeningen in de desbetreffende landen. In enkele landen, zoals Duitsland en de Verenigde Staten, bestaat reeds wetgeving op dit vlak. Wederzijdse erkenning tussen verschillende nationale en internationale TTP's kan worden gerealiseerd op basis van overeenkomsten in combinatie met wederzijdse toetsing; het verdient aanbeveling hiermee vanuit Nederland reeds zo snel mogelijk een aanvang te maken. Ook hierbij kan de overheid een stimulerende en activerende rol spelen. Hierbij zal rekening moeten worden gehouden met een zich snel ontwikkelend internationaal raamwerk, waarbinnen de in Nederland geldende randvoorwaarden zo efficiënt mogelijk ingepast moeten kunnen worden.

In fase 3 van het TTP-project is naar voren gekomen dat interoperabiliteit door de onderzochte TTP's van groot belang wordt geacht. Hierbij dient te worden aangetekend, dat niet is onderzocht of en in hoeverre de proefprojecten interoperabel zijn.

3.6 Overige randvoorwaarden

Naast bovengenoemde randvoorwaarden is een aantal aanvullende randvoorwaarden geformuleerd:

- *bezwaar- en beroepsmogelijkheden* - de gebruikers van een TTP-dienst dienen in staat te worden gesteld bezwaar of beroep aan te tekenen bij een onafhankelijke beroepsinstantie. De gebruiker van een TTP dient te beschikken over laagdrempelige mogelijkheden tot het indienen en afhandelen van klachten, waarbij de mogelijkheden en termijnen voor het indienen van klachten, alsmede de termijn van behandeling duidelijk aan de gebruiker kenbaar worden gemaakt;
- *aansprakelijkheid* - de TTP-organisatie dient, onder zekere voorwaarden, aansprakelijkheid voor de door haar geleverde diensten en/of verrichte transacties te aanvaarden. Om aansprakelijkheidsvraagstukken te kunnen beantwoorden wordt een eenduidige en onweerlegbare vastlegging van uitgevoerde activiteiten door de TTP onmisbaar geacht;
- *klachtenregeling* - er dient een klachtenregeling te zijn, alsmede een mogelijkheid tot schadeverhaal bij, bijvoorbeeld, onrechtmatige verstrekking van sleutelmateriaal aan derden; een dergelijke compromittering dient hoe dan ook altijd onverwijld door de TTP aan de gebruiker te worden gemeld;
- *keuzevrijheid* - ter bevordering van de vrije marktwerking en om de individuele wensen van de consument te kunnen behartigen dient de consument altijd een vrije keuze te kunnen maken bij de selectie van een TTP en van specifieke TTP-diensten. Er mag met andere woorden geen sprake zijn van "gedwongen winkelnering", bijvoorbeeld als gevolg van een monopoliepositie. Dit geldt ook voor commerciële producten die het gebruik van TTP's mogelijk maken;
- *geen vertrouwelijkheidsfuncties* - een TTP in deze categorie mag niet willens en wetens meewerken aan het gebruiken van sleutelmateriaal, dat is bestemd voor authenticiteit en integriteit, voor de versleuteling van gegevens;
- *exportcontrole* - op TTP-diensten voor authenticiteit en integriteit zijn randvoorwaarden van toepassing inzake exportcontrole van cryptografische producten; zie hiervoor sectie 4.4.

4 Randvoorwaarden inzake TTP-diensten voor vertrouwelijkheid

4.1 Inleiding

Onder TTP-diensten voor *vertrouwelijkheid* vallen onder meer: het vercijferen van elektronisch berichtenverkeer; en het beheer van cryptografisch sleutelmateriaal voor vertrouwelijkheid.

De hierbij behorende randvoorwaarden hebben onder meer betrekking op betrouwbaarheid, rechtmatige toegang, exportcontrole en interoperabiliteit.

4.2 Betrouwbaarheid

De randvoorwaarden inzake de betrouwbaarheid van TTP-diensten voor vertrouwelijkheid wijken niet af van de randvoorwaarden inzake de betrouwbaarheid van TTP-diensten voor authenticiteit en integriteit.

Aanvullend kan worden gesteld dat een TTP vertrouwelijk dient om te gaan met medewerking aan de rechtmatige verkrijging van bepaalde gegevens en/of sleutelmateriaal door hiertoe wettelijk bevoegde instanties. Evenzo dient de TTP vertrouwelijk om te gaan met de uit een dergelijke medewerking voortvloeiende informatie.

4.3 Rechtmatige toegang

Deze categorie van randvoorwaarden heeft betrekking op de rechtmatige toegang tot gegevens, zowel door de gebruiker als door andere partijen.

De *gebruiker* zal voor de toegang tot zijn gegevens altijd moeten kunnen beschikken over het geheime sleutelmateriaal waarmee de oorspronkelijke gegevens zijn versleuteld. Voor de gebruiker van een TTP-dienst voor vertrouwelijkheid is het verlies van sleutelmateriaal een reëel risico. Bij verlies of verminking van dit sleutelmateriaal zijn de oorspronkelijke gegevens immers niet langer toegankelijk. Sleutelverlies kan daarom grote gevolgen hebben voor de continuïteit van een organisatie, maar ook voor de individuele gebruiker. De risico's van sleutelverlies kunnen tot een aanvaardbaar niveau worden teruggebracht door reservekopieën van sleutels te bewaren (*key escrow*) of ervoor te zorgen dat sleutelmateriaal te herleiden is (*key recovery*). Een TTP die zorg draagt voor sleutelbewaring en/of herleidbaarheid ontslaat zijn gebruiker van de taak deze maatregel zelf te treffen.

Niet alleen de gebruikers van een TTP-dienst, maar ook *andere partijen* met rechtmatige toegang tot bepaalde gegevens hebben baat bij een vorm van sleutelbewaring en/of herleidbaarheid. Voor deze partijen is of wordt de wettelijke bevoegdheid tot het verkrijgen van bepaalde elektronische gegevens op dit moment geregeld door middel van specifieke wet- en regelgeving. Zulke wet- en regelgeving is onder meer van toepassing op curatoren, medische instellingen, de advocatuur, opsporingsdiensten met wettelijke bevoegdheid, zoals politie, FIOD en AID, en de inlichtingen- en veiligheidsdiensten. In de wet wordt onderscheid gemaakt tussen rechtmatige toegang tot opgeslagen gegevens en rechtmatige toegang tot telecommunicatieverkeer.

De randvoorwaarden die in dit verband op de TTP van toepassing zijn, zijn afhankelijk van de topologie van de TTP-dienst (zie 2.2.3). *In-line TTP's* kennen reeds een medewerkingsverplichting bij een rechtmatig verzoek, waarbij de in-line TTP als telecommunicatiedienst[1] wettelijk verplicht is om het oorspronkelijke signaal aan te leveren. Bij *on-line*, *off-line* en *no-line TTP's* kan, zoals beschreven

[1] Zie de Telecommunicatiewet, Memorie van Toelichting.

in sectie 2.2, onderscheid worden gemaakt tussen de gevallen waarin sleutelmateriaal wordt opgeslagen door de gebruiker enerzijds of door de TTP anderzijds.

Wordt het sleutelmateriaal opgeslagen door de gebruiker zelf, dan ontstaat een situatie die voor de gebruiker vanuit het oogpunt van risicobeheersing aanvaardbaar kan zijn, maar voor andere partijen met rechtmatige toegang tot gegevens niet in alle gevallen toereikend zal zijn. Op de TTP is in dit geval geen enkele randvoorwaarde van toepassing. Het merendeel van de in fase 3 onderzochte TTP's heeft het sleutelbeheer zodanig ingericht, dat alleen de gebruiker zelf over het geheime sleutelmateriaal beschikt (zie bijlage 1).

Wordt sleutelmateriaal door de TTP opgeslagen, dan zijn daarmee niet alleen de belangen van de gebruiker, maar ook de belangen van de partijen met rechtmatige toegang tot bepaalde gegevens gediend. Rechtmatige toegang tot zulk sleutelmateriaal - en de medewerking hierbij door de TTP, zie tabel 2 - zal immers geregeld zijn op grond van vigerende wet- en regelgeving. De opsporingsdiensten hebben de bevoegdheid tot het opvragen van opgeslagen gegevens en daarmee tot opgeslagen sleutelmateriaal in het kader van de WCC (art. 125i WSv); in de nieuwe Wet Computercriminaliteit is het niet verlenen van medewerking aan een verzoek tot beschikbaarstelling van cryptografische sleutels strafbaar gesteld. Een en ander is schematisch weergegeven in figuur 3. De inlichtingen- en veiligheidsdiensten kennen op dit moment geen bevoegdheid tot het opvragen van opgeslagen gegevens; in het ontwerp van de nieuwe Wet op de Inlichtingen en Veiligheidsdiensten (WIV) is echter voorzien in een verplichting ten aanzien van het verlenen van medewerking door degenen die kennis dragen van het ongedaan maken van de versleuteling van (a) gegevens opgeslagen of verwerkt in een geautomatiseerd werk; (b) gesprekken, telecommunicatie of gegevensoverdracht die door de dienst zijn afgetapt. Aan de medewerking door de TTP zijn een aantal voor de hand liggende randvoorwaarden verbonden; zo zal de TTP onverwijld medewerking dienen te verlenen, zal strikte geheimhouding bij het verlenen van zulke medewerking moeten worden betracht, zal de TTP een vertrouwenspersoon in dienst moeten hebben voor de vertrouwelijke afhandeling van verzoeken tot rechtmatige toegang, en dient de TTP inzage te geven in de gebruikte encryptietechnieken.

gegevens / encryptie	**transport** **rechtmatige interceptie**	**opslag** **rechtmatige toegang**
encryptie door TTP	**in-line TTP** TTP levert oorspronkelijk signaal aftapregulering Telecomwet	**on-line, off-line en no-line TTP** TTP levert oorspronkelijke gegevens medewerkingsverplichting WCC
encryptie door gebruiker	**on-line, off-line en no-line TTP** *on-line/off-line TTP* levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC en Telecomwet TTP levert oorspronkelijk signaal aftapregulering Telecomwet *no-line TTP* levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC	**on-line, off-line en no-line TTP** TTP levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC

Figuur 3 - Rechtmatige toegang in het kader van opsporing en informatievergaring op basis van huidige wet- en regelgeving

Bij het internationaal gebruik van TTP's doet zich een specifiek probleem voor als de betrokken partijen voor encryptie sleutelmateriaal gebruiken dat is gegenereerd door, verstrekt door en/of gedeponeerd bij een buitenlandse TTP. De Nederlandse wet- en regelgeving biedt onvoldoende aanknopingspunten om zulk sleutelmateriaal te achterhalen; de buitenlandse TTP zal niet gehouden zijn het sleutelmateriaal aan Nederlandse instanties te verstrekken. Een mogelijke maatregel om hieraan tegemoet te komen lijkt de verplichte opslag van een kopie van het geheime sleutelmateriaal door een TTP binnen de jurisdictie, met een bewaarplicht en toegang door partijen met rechtmatige toegang. Eventueel zou hiervoor een hiërarchische internationale TTP-infrastructuur kunnen worden opgezet, waarbij vertrouwelijkheidssleutels altijd worden opgeslagen door TTP's binnen de onderscheiden jurisdicties; interoperabiliteit van deze TTP's is hiervoor een noodzakelijke vereiste. Een andere mogelijkheid is het opstellen van overeenkomsten, zoals rechtshulpverdragen, tussen jurisdicties inzake het in klare tekst verstrekken van gegevens en/of sleutelmateriaal door TTP's, waarbij verzoeken hiertoe via de nationale overheidsdiensten kunnen verlopen. In al deze gevallen betreft het maatregelen met verstrekkende gevolgen, die bovendien, mede door de noodzakelijke internationale afstemming, niet eenvoudig zullen kunnen worden getroffen.

Samenvattend kan worden geconcludeerd dat de bewaring en/of herleidbaarheid van bepaald sleutelmateriaal voor vertrouwelijkheid door de TTP zowel uit het oogpunt van de gebruiker als uit het oogpunt van de andere betrokken partijen zekere voordelen biedt. Leveranciers van hardware en software waarmee TTP-diensten kunnen worden gerealiseerd, brengen in toenemende mate producten op de markt waarbij faciliteiten voor sleutelbewaring en herleidbaarheid zijn ingebouwd.

Aan het bewaren en/of herleiden van sleutelmateriaal zijn echter ook andere consequenties verbonden, die onder meer betrekking hebben op de vereiste integriteit en vertrouwelijkheid van het opgeslagen sleutelmateriaal en, daarmee samenhangend, de bescherming van de persoonlijke levenssfeer van de gebruikers van de TTP. Bovendien kunnen de hiermee samenhangende risico's slechts door een adequaat stelsel van randvoorwaarden worden ondervangen, waardoor sleutelbewaring en/of herleidbaarheid voor de aanbieder van een TTP-dienst kosten met zich mee zullen brengen.

Mede om bovengenoemde redenen zijn de bewaring en de herleidbaarheid van sleutelmateriaal door TTP's nog steeds het onderwerp van internationale controverse. Bewaring en/of herleidbaarheid van sleutelmateriaal zijn daarom in deze beleidsnotitie niet als randvoorwaarden opgenomen. In verband met de risico's die met sleutelverlies gepaard kunnen gaan worden sleutelbewaring en/of herleidbaarheid in deze beleidsnotitie als aanbevelingen opgenomen. Een overzicht van de randvoorwaarden is gegeven in tabel 2.

verstrekken van beschikbaar sleutelmateriaal (on-line, off-line en no-line TTP)
levering van het oorspronkelijke signaal (in-line TTP)
redelijke bewaartermijn gegevens (in-line, on-line, off-line en no-line TTP)
onverwijlde medewerking door TTP
geheimhouding door TTP
vertrouwenspersoon bij TTP

Tabel 2 - Overzicht randvoorwaarden inzake rechtmatige toegang

4.4 Exportcontrole

Ook TTP's dienen te voldoen aan de vigerende wet- en regelgeving inzake exportcontrole.

Cryptografische producten, met inbegrip van software, zijn met uitzondering van een aantal producten zoals voor banktoepassing, mobiele telefonie en Pay-TV, onder exportcontrole gebracht op grond van multilaterale afspraken in het Wassenaar Arrangement. Deze afspraken komen voort uit internationale en nationale veiligheidspolitieke overwegingen.

Voor de ontwikkeling van een betrouwbare infrastructuur voor electronic commerce is het gebruik van cryptografische producten in toenemende mate van belang. Het exportcontrole beleid is er dan ook op gericht om deze ontwikkeling zo min mogelijk te belemmeren. In het Wassenaar Arrangement komt derhalve exportcontrole van cryptografische hardware en software uitvoerig aan de orde met als inzet om een aantal van die producten van de exportcontrole lijst af te voeren en om de procedures voor exportcontrole te versoepelen. Het Ministerie van Economische Zaken (DGBEB) heeft bij deze onderhandelingen de coördinerende taak en is tevens verantwoordelijk voor de afgifte van exportvergunningen.

De exportcontrole op cryptografische producten en op producten welke cryptografische producten bevatten, is gestoeld op de volgende wettelijke basis:

1. In en Uitvoerwet (Stb. 1988, 228);
2. Uitvoerbesluit strategische goederen 1963 (Stb. 1981, 118);
3. Verordening (EG) nr. 3381/94 van de Raad van de Europese Unie van 19 december 1994. De verordening introduceert een communautair systeem voor de uitvoer van goederen voor tweeërlei gebruik. In het daarmee verbonden Raadsbesluit nr. 94/942/GBVB is de lijst met de betrokken goederen opgenomen. In categorie 5 deel 2 van deze lijst staan de cryptografische producten waarvoor een vergunning vereist is beschreven. Als tijdelijke maatregel geldt dat ook voor de levering binnen de Gemeenschap voor cryptografische producten een vergunning is vereist (Annex IV).

Bovengenoemde wet- en regelgeving is ook van toepassing op de export van cryptografische hardware en software voor TTP-diensten. Indien een TTP tot export van cryptografische producten zou willen overgaan, zal hiervoor op dit moment eerst een vergunning bij de Centrale Dienst voor In- en Uitvoer moeten worden aangevraagd.

Tenslotte zij opgemerkt dat de randvoorwaarden inzake exportcontrole ook van toepassing zijn op TTP-diensten voor authenticiteit en integriteit; zie sectie 3.6.

4.5 Interoperabiliteit

Voor TTP-diensten voor vertrouwelijkheid gelden in beginsel dezelfde randvoorwaarden inzake interoperabiliteit als voor TTP-diensten voor authenticiteit en integriteit (zie 3.5), uitgezonderd hetgeen is gesteld inzake de wederzijdse erkenning van digitale handtekeningen.

4.6 Overige randvoorwaarden

Voor TTP-diensten voor vertrouwelijkheid gelden in beginsel dezelfde overige randvoorwaarden als voor TTP-diensten voor authenticiteit en integriteit (zie 3.6).

5 Instrumenten voor het waarborgen van randvoorwaarden

5.1 Inleiding

Na de opsomming van randvoorwaarden in de secties 3 en 4 rijst de vraag hoe deze randvoorwaarden in de praktijk zouden kunnen worden gewaarborgd.

Overheid en bedrijfsleven beschikken hiertoe over een aantal instrumenten die variëren in de mate van regulering en overheidsinvloed. Ook in dit geval is sprake van een spectrum, met strikte regulering aan het ene uiterste, volledige deregulering aan het andere uiterste, en tal van mengvormen daar tussenin, zoals een verplicht vergunningenstelsel, aansluiting bij een bij wet ingestelde of wettelijk erkende organisatie met zelfregulering, aansluiting bij een door de marktpartijen zelf ingestelde organisatie met zelfregulering, certificatie met overheidstoezicht, en certificatie zonder overheidstoezicht.

Volledige zelfregulering stuit op bezwaren, die samenhangen met het belang van TTP-diensten voor een samenleving die zich meer en meer verlaat op inherent kwetsbare informatietechnologie. De overheid heeft in deze tot taak de burger tegen onaanvaardbare risico's te beschermen. Daarnaast zal de overheid moeten waarborgen dat de belangen van partijen met een wettelijke bevoegdheid tot het verkrijgen van elektronische gegevens voldoende worden bewaakt. In het MDW-rapport Normalisatie en Certificatie is door de ministers van Economische Zaken en Justitie aangegeven onder welke omstandigheden voor certificatie gekozen kan worden, en onder welke omstandigheden een nauwere betrokkenheid van de overheid gerechtvaardigd is. Maatschappelijk belang is hierbij een essentieel criterium. Volledige zelfregulering lijkt om deze reden niet gerechtvaardigd.

Aan het opstellen van nieuwe wet- en regelgeving en een strikte vorm van toezicht door de overheid zijn echter andere consequenties verbonden:

- wetgeving is relatief kostbaar, hetgeen vragen oproept omtrent proportionaliteit;
- wetgeving is weinig flexibel, terwijl flexibiliteit in de zich nog sterk ontwikkelende TTP-markt een noodzakelijke vereiste is;
- bestaande wetgeving lijkt voldoende mogelijkheden voor het waarborgen van randvoorwaarden te bieden;
- wetgeving is niet in overeenstemming met het huidige regeringsbeleid van deregulering en marktwerking, dat als uitgangspunt van het nationaal TTP-project geldt;
- door het opstellen van wetgeving zou Nederland in internationaal verband een uitzonderingspositie innemen.

Het kiezen van de instrumenten waarmee de gestelde randvoorwaarden kunnen worden gewaarborgd, komt derhalve neer op het vinden van een balans tussen regulering en deregulering. De vraag is hoe deze balans kan worden gevonden.

Door enkele marktpartijen is voorgesteld een toezichthoudende instelling op afstand van de overheid op te richten, vergelijkbaar met de OPTA of de Registratiekamer. Op basis van het uitgangspunt van deregulering en marktwerking stelt de projectgroep voor het waarborgen van de in deze beleidsnotitie genoemde randvoorwaarden in beginsel aan de markt zelf over te laten. Het oprichten van een beroepsorganisatie voor TTP's, onder begeleiding en stimulering van de overheid, is hierbij als veelbelovende mogelijkheid naar voren gekomen. Dit voorstel zal hieronder nader worden toegelicht.

5.2 TTP-kamer

Aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot de oprichting van een landelijke organisatie voor TTP's, onder begeleiding en stimulering van de overheid (zie figuur 4). Deze organisatie zal verder als "TTP-kamer" worden aangeduid.

Hierbij gelden tenminste de volgende overwegingen:

- in de TTP-kamer hebben zowel de marktpartijen als de overheid zitting;
- aansluiting bij de TTP-kamer door marktpartijen dient op vrijwillige basis plaats te vinden;
- de TTP-kamer dient een openbare registratie van aangesloten TTP's te kennen;
- de TTP-kamer dient in overleg met de andere betrokken partijen een bindend algemeen reglement (*Certification Practice Statement*) voor TTP-diensten op te stellen, waarin de rechten en plichten van de gebruikers en aanbieders van de TTP-dienst worden aangegeven en tenminste de in deze beleidsnotitie opgestelde randvoorwaarden inzake digitale handtekeningen, betrouwbaarheid, privacy, interoperabiliteit, rechtmatige toegang enzovoorts zijn opgenomen;
- elke bij de TTP-kamer aangesloten TTP zal handelen in overeenstemming met het aldus opgestelde reglement;
- het reglement dient periodiek of anders wanneer nodig te worden geëvalueerd en, indien nodig, te worden herzien;
- de TTP-kamer dient te onderzoeken of voor bepaalde TTP-diensten aanvullende randvoorwaarden moeten worden opgesteld, die door een TTP kunnen worden vastgelegd in een specifieke aanvulling op het reglement;
- elke bij de TTP-kamer aangesloten TTP dient zelf een specifiek reglement op te stellen, dat is toegesneden op de geleverde TTP-diensten. Dit specifieke reglement dient tenminste het algemeen reglement te omvatten;
- de TTP-kamer dient een klachtenregeling en een vorm van tuchtrecht te kennen;
- de TTP-kamer dient zorg te dragen voor aansluiting bij internationale ontwikkelingen;
- elke bij de TTP-kamer aangesloten TTP dient periodiek te worden gecertificeerd door een door de Raad voor de Accreditatie geaccrediteerde organisatie. De in deze beleidsnotitie opgestelde randvoorwaarden dienen daarvoor te worden vertaald naar hanteerbare certificatiecriteria;
- bij de TTP-kamer aangesloten TTP's dienen uitsluitend elektronische certificaten te accepteren van TTP's die gecertificeerd zijn als boven beschreven of TTP's waarmee een nationale of internationale overeenkomst tot wederzijdse erkenning (*Mutual Recognition Agreement*) is gesloten.

De belangrijkste rol van de overheid dient te bestaan uit het stimuleren van de ontwikkeling van de TTP-kamer en een TTP-infrastructuur die voldoet aan de in de beleidsnotitie gestelde randvoorwaarden, het internationaal uitdragen van het Nederlandse beleidsmodel in het kader van de wederzijdse erkenning van digitale handtekeningen en het wegnemen van de handelsbelemmeringen voor cryptografische goederen en producten op de interne Europese markt.

De overheid dient hiertoe een aantal concrete maatregelen te treffen, die hieronder worden opgenoemd.

De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.

De overheid dient TTP's die zich aansluiten bij de TTP-kamer actief te stimuleren, bijvoorbeeld door het beschikbaar stellen van subsidies of kredieten; aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

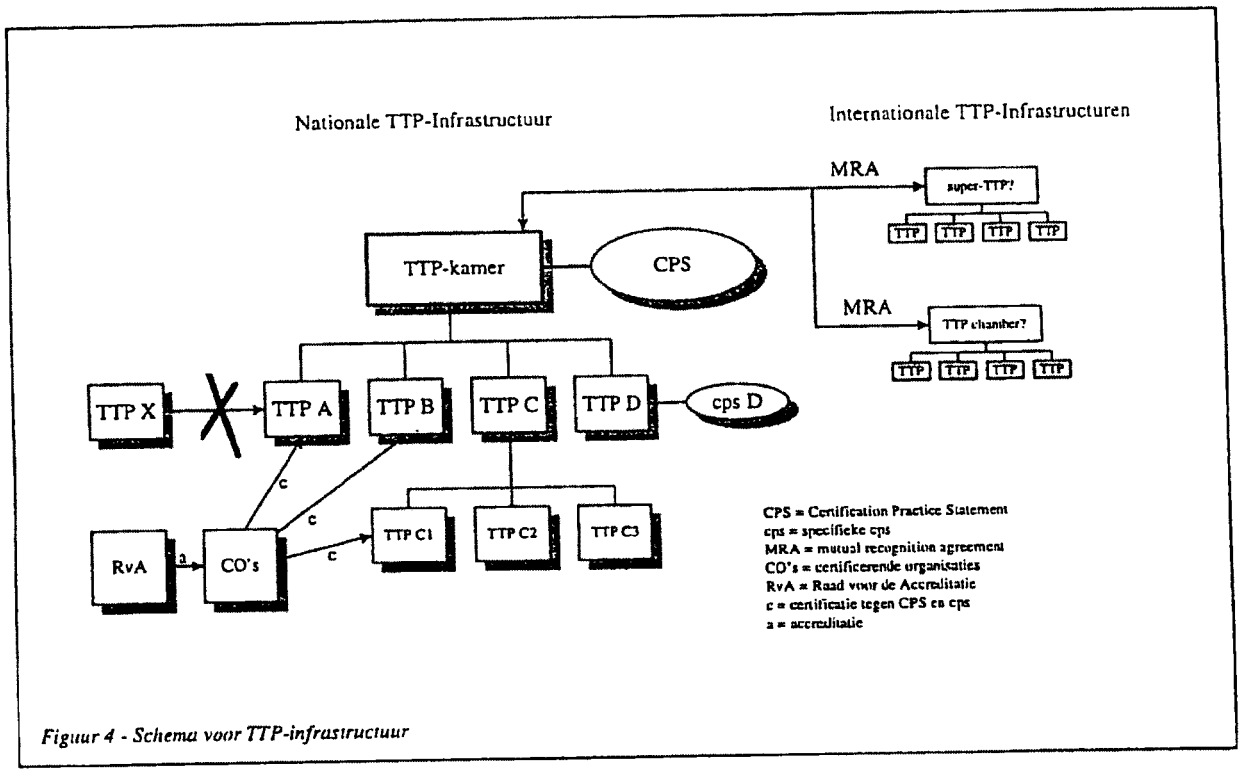
De overheid dient een actieve rol te spelen op het gebied van voorlichting en onderwijs.

De overheid dient aansluiting bij de TTP-kamer in principe als eis te stellen aan TTP's die diensten aan de overheid leveren.

De overheid dient de ontwikkeling van specifieke apparatuur en programmatuur die voldoet aan de gestelde randvoorwaarden te stimuleren.

De overheid dient het functioneren van een aldus op te richten TTP-kamer na een periode van twee jaar te evalueren. Na deze periode zou eventueel, indien noodzakelijk, alsnog tot aanvullende wet- en regelgeving kunnen worden overgegaan.

De uiteindelijke samenstelling, taakstelling en positionering van de TTP-kamer zijn nog onderwerp van discussie. Overheid en marktpartijen dienen zo snel mogelijk een initiatief te nemen met de verdere uitwerking hiervan.



Figuur 4 - Schema voor TTP-infrastructuur

6 Conclusies

Overheid en bedrijfsleven dienen concrete maatregelen te treffen om de snelle ontwikkeling van een betrouwbare TTP-infrastructuur te bevorderen. Er is vooralsnog geen noodzaak tot het opstellen van aanvullende wet- en regelgeving ten aanzien van TTP's.

Overheid, aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot het oprichten van een TTP-kamer, die waarborgt dat aan de gestelde randvoorwaarden wordt voldaan. In de TTP-kamer hebben, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting.

De overheid dient de oprichting van genoemde TTP-kamer te begeleiden en te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.

De overheid dient TTP's die zich bij de TTP-kamer aansluiten te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

In principe dient de overheid uitsluitend diensten af te nemen van TTP's die zich bij de TTP-kamer hebben aangesloten.

De overheid dient de ontwikkeling en het gebruik van apparatuur en programmatuur die bijdraagt aan een betrouwbare TTP-infrastructuur te stimuleren.

De overheid dient het Nederlandse schema in het kader van de wederzijdse erkenning van TTP's uit te dragen.

De overheid dient na uiterlijk twee jaar de ontwikkeling van TTP-infastructuren in Nederland te evalueren, waarbij wordt getoetst in hoeverre deze infrastructuren aan de gestelde randvoorwaarden voldoen en of de gestelde voorwaarden toereikend zijn.

Bijlage 1 - Resultaten fase 3

Uitgebracht aan:

Ministerie van Economische Zaken,
Directoraat-Generaal voor Industrie en Diensten
Directie Elektronica, Diensten en Informatietechnologie
en
Ministerie van Verkeer en Waterstaat
Hoofddirectie Telecommunicatie en Post

Datum: 19 december 1997

Betreft: rapport inzake uitkomst inventarisatie toepasbaarheid mogelijke randvoorwaarden TTP op basis van de versie d.d. 19-09-97

1 Inleiding

Deze bijlage bevat een samenvatting van het rapport met de uitkomsten van de inventarisatie die is verricht met betrekking tot de implementatie van de mogelijke randvoorwaarden op basis van de versie d.d. 19-09-97 bij een viertal TTP-organisaties en -diensten. Deze inventarisatie is verricht door de EDP AUDIT POOL in samenwerking met de Technische Universiteit Delft in het kader van fase 3 van het 'Projectplan NAP/TTP' d.d. 7 juli 1997.

2 Opdracht

De inventarisatie is in opdracht van het Ministerie van Verkeer en Waterstaat en het Ministerie van Economische Zaken uitgevoerd conform bovengenoemd projectplan.

3 Doelstelling inventarisatie

De doelstelling van de inventarisatie was om, ten behoeve van de rapportage in fase 4, met betrekking tot het stuk 'NAP/TTP - Inventarisatie van mogelijke randvoorwaarden - Discussiestuk' versie d.d. 19 september 1997 (hierna te noemen: 'Mogelijke randvoorwaarden'), na te gaan in hoeverre deze in fase 2 van het project geformuleerde mogelijke randvoorwaarden in de praktijk toepasbaar zijn voor een operationele TTP-dienst.

4 Objecten van onderzoek

De objecten van onderzoek zijn de 'Mogelijke randvoorwaarden' en het daarop gebaseerde evaluatiekader zoals die zijn geformuleerd ten aanzien van de TTP-organisatie en de TTP-dienst in relatie tot de vier geselecteerde pilot-projecten.

5 Scope en reikwijdte werkzaamheden

De scope en reikwijdte van de door ons gedefinieerde werkzaamheden moeten worden bezien in de context van het gestelde in het hiervoor onder 1 genoemde projectplan en onder 3 vermelde discussiestuk d.d. 19-09-97.

Voor de goede orde wordt opgemerkt, dat:

- waar in het projectplan sprake is van het begrip 'beoordelen' gelezen moet worden 'inventariseren'
- tijdens de onderzoeksperiode door de leden van de Consultatiegroep Aanbieders en Gebruikers commentaar is geleverd op de set 'Mogelijke randvoorwaarden' d.d. 19-09-97 waarop de inventarisatie is gebaseerd. Met dit commentaar is alleen rekening gehouden voor zover het de vier pilot-organisaties betreft.

De opdracht omvatte niet het vormen van een oordeel of de 'Mogelijke randvoorwaarden' noodzakelijk en voldoende zijn voor het realiseren van een betrouwbare TTP-organisatie en -dienst.

6 Aanpak en werkwijze

1. Volgens het projectplan is in fase 2 een raamwerk opgesteld dat is vastgesteld door de projectgroep. Daarin is een verzameling van basisvoorwaarden opgenomen die zijn gerelateerd aan de criteria betrouwbaarheid, aansprakelijkheid, privacy, interoperabiliteit, rechtmatige toegang en onafhankelijkheid. De normen hebben betrekking op de TTP-organisatie en -dienst van de pilot-organisatie en zijn nader onderverdeeld in organisatorische en technische voorzieningen. Een aantal van deze voorwaarden is van toepassing op alle TTP-diensten, terwijl sommige voorwaarden slechts van toepassing zijn op specifieke klassen van TTP-organisaties en -diensten.

2. Uitgaande van dit raamwerk 'Mogelijke randvoorwaarden' d.d. 19-09-97 hebben wij de belangrijkste aspecten van organisatorische en technische aard uitgewerkt in een evaluatiekader. De inhoud van dit kader is in de concept-fase afgestemd met de opdrachtgevers. Dit kader is verstrekt aan de pilot-organisaties en is gehanteerd als de basis voor de inventarisatie.

3. Het evaluatiekader is ingevuld door elk van de vier bij de inventarisatie betrokken TTP-organisaties en - diensten. Verder is schriftelijke informatie verkregen en zijn interviews gehouden. Bij de inventarisatie is door ons nagegaan in welke mate de in het evaluatiekader gedefinieerde aspecten van organisatorische en technische aard toepasbaar zijn bij de operationele TTP-organisatie en -dienst. Tevens is aan de hand van het evaluatiekader nagegaan of de 'Mogelijke randvoorwaarden' d.d. 19-09-97 aanvulling of nadere uitwerking behoeven.

4. De besprekingsverslagen van de interviews zijn in de concept-fase met de pilot-organisaties afgestemd.

5. Met de betrokken TTP-organisaties is overeengekomen dat over de verkregen informatie alleen in geanonimiseerde vorm zal worden gerapporteerd. Daartoe is een geanonimiseerde samenvatting van de antwoorden met betrekking tot het evaluatiekader opgesteld.

6. In hoofdstuk 6 zijn de hoofdlijnen vermeld die bij de inventarisatie naar voren zijn gekomen. Deze hoofdlijnen dienen als invoer voor de beleidsnotitie die in het kader van fase 4 van het projectplan is voorzien.

7 Hoofdlijnen uitkomst inventarisatie

De hoofdlijnen van de uitkomsten van de inventarisatie en de daarbij naar voren gebrachte opmerkingen zijn hieronder weergegeven.

7.1 Volwassenheid TTP-dienst

De mate waarin de TTP-dienst ten tijde van de inventarisatie operationeel was, verschilde per pilot-organisatie.

De uitkomsten van de inventarisatie zijn door deze omstandigheid voor een deel gebaseerd op uitspraken en inzichten van de geïnterviewden, die niet konden worden getoetst aan de hand van een feitelijke implementatie van de TTP-dienst.

Bij de nog niet operationele TTP-diensten konden de randvoorwaarden door middel van interviews toch worden getoetst doordat belangrijke keuzes voor het realiseren van een volledig operationele TTP-dienst reeds waren gemaakt.

7.2 Mogelijke randvoorwaarden

De uitkomst van de inventarisatie naar de set van 'Mogelijke randvoorwaarden' versie d.d. 19-09-97, die is opgesteld in het kader van fase 2 van het projectplan, geeft aanleiding tot de volgende opmerkingen:

- de set anticipeert in onvoldoende mate op de (verwachte) praktijksituatie;
- de set is onduidelijk en/of multi-interpretabel;
- de set als geheel wordt door de pilot-organisaties te zwaar geacht;
- de set houdt onvoldoende rekening met:
  - TTP-diensten die een verschillend niveau van 'trusted' bieden;
  - aanloopsituaties waarin nog niet aan alle randvoorwaarden kan worden voldaan;
  - degene voor wie de set bestemd is (voor de TTP-organisatie intern, het marktsegment, alle TTP-organisaties);
  - de wenselijkheid versus toepasbaarheid en haalbaarheid van randvoorwaarden;
  - de actoren/aspecten die de voorwaarden bepalen (TTP-organisaties intern, marktsegment, marktmechanisme, overheid).

7.3 Terminologie

De meningen van de pilot-organisaties lopen sterk uiteen ten aanzien van de inhoud en de strekking van het begrip 'onafhankelijkheid' dat in de 'Mogelijke randvoorwaarden' is omschreven als financiële en bestuurlijke onafhankelijkheid. Uit de interviews is gebleken, dat de pilot-organisaties het begrip 'onafhankelijkheid' soms anders interpreteren. In de betekenis van 'belangenverstrengeling' zien de pilot-organisaties onafhankelijkheid enerzijds als noodzakelijke randvoorwaarde voor het bewerkstelligen van het begrip 'trusted'. Anderzijds zien de pilot-organisaties het juist als een voordeel voor het realiseren van een 'trusted-niveau' indien de TTP-organisatie onderdeel van een gevestigde organisatie uitmaakt. In een dergelijke situatie wordt wel de noodzaak onderkend voor het realiseren van organisatorische functiescheidingen.

Daarnaast komen bij de pilot-organisaties verschillen naar voren ten aanzien van het begrip onafhankelijkheid in relatie tot het begrip 'koppelverkoop'. Dit betreft de scheiding tussen de TTP-organisatie als certificaten-uitgevende-instantie en de TTP-diensten waarbij deze certificaten worden toegepast. Een aantal van de pilot-organisaties ziet deze scheiding als een essentiële randvoorwaarde.

7.4 Scheiding CA/RA

Ten aanzien van de randvoorwaarde 'functiescheiding' is de mening van de in de inventarisatie betrokken pilot-organisaties dat het in ieder geval vanuit de praktijk gezien wenselijk is scheiding aan te brengen tussen de functie van Registration Authority (RA) en die van Certification Authority (CA). Het is echter moeilijk deze scheiding bij kleine TTP-organisaties of TTP-organisaties in oprichting te realiseren.

7.5 Sleutelbeheer

Bij het merendeel van de TTP-organisaties wordt het creëren van de sleutelparen door de klanten verricht. De TTP-organisatie geeft alleen certificaten uit. In die situaties is key escrow (het bewaren

van private sleutels door een TTP-organisatie) niet mogelijk, tenzij de klant zelf hiertoe mocht besluiten. De consequentie daarvan is, dat een groot deel van de randvoorwaarden niet, of slechts ten dele, van toepassing is. De belangrijkste voorbeelden hiervan zijn een onuitwisbare en volledige verslaglegging van transacties alsmede de herleidbaarheid van sleutelmateriaal.

Doordat generatie van sleutelmateriaal niet bij de TTP-organisatie plaats vindt heeft dit voor TTP-organisaties als voordeel het beperken van de aansprakelijkheid tegen ongeautoriseerde kennisname van data en het niet kunnen vervullen van een rol bij key escrow. De verantwoordelijkheid (en daarmee de aansprakelijkheid) in de richting van de klanten wordt daarmee tevens beperkt.

7.6 Continuïteit

Bij de pilot-organisaties bestaat eenheid van opvatting ten aanzien van de noodzaak om de continuïteit te waarborgen, bijvoorbeeld door het stellen van eisen ten aanzien van de overdracht van de dienstverlening.

7.7 Gebruik van sleutelmateriaal

De TTP-organisatie kan niet voorkomen dat sleutelparen ten behoeve van digitale handtekeningen door de klant worden aangewend ten behoeve van encryptie, anders dan door gebruik te maken van specifieke algoritmen (Digital Signature Algorithm - DSA) of specifieke apparatuur.

7.8 Wederzijdse erkenning

De in de inventarisatie betrokken TTP-organisaties onderschrijven de noodzaak om te komen tot de een of andere vorm van wederzijdse (inter)nationale erkenning, zowel voor het eigen marktsegment als de facto voor alle TTP-diensten voor het creëren van voorwaarden voor interoperabiliteit. Implementatie van mechanismen voor wederzijdse erkenning is echter niet eenvoudig (zelfs niet binnen een marktsegment) en vergt een actieve en stimulerende rol van de overheid.

7.9 Abstractheid mogelijke randvoorwaarden

De formulering van de mogelijke randvoorwaarden is te abstract. Daardoor kunnen de randvoorwaarden in onvoldoende mate worden gecontroleerd, hetgeen problemen kan opleveren bij de certificering en erkenning van een TTP-organisatie.

7.10 Rol overheid

De onderzochte pilot-organisaties zijn verdeeld over de mate waarin de overheid een rol moet spelen bij het tot stand komen van een set van randvoorwaarden voor adequate TTP-diensten. (Bijna) operationele TTP's zijn geneigd hun eigen intern ontwikkelde normen als randvoorwaarden voor anderen te zien. TTP-organisaties in oprichting willen zo min mogelijk regulering door de overheid.

7.11 TTP-kamer

De pilot-organisaties zijn van mening, dat een oplossing gevonden moet worden tussen enerzijds regulering van randvoorwaarden door de overheid en anderzijds dit geheel over te laten aan de marktwerking. De meeste pilot-organisaties vinden dat ten minste gestreefd moet worden naar de instelling van een zogenaamde TTP-kamer. Deze kamer moet worden belast met ten minste:

- een niet verplichte certificering van TTP-organisaties op basis van door haar opgestelde minimum randvoorwaarden;
- het realiseren van internationale erkenningen.

Over de verhouding van een dergelijke kamer tot (de rol van) de overheid hebben de pilot-organisaties geen uitspraken gedaan.

7.12 Aanvullende randvoorwaarden

De inventarisatie heeft uitgewezen dat het aanbeveling verdient in de set met mogelijke randvoorwaarden rekening te houden met de volgende situaties:

- outsourcing van TTP-functies;
- sleutelgeneratie bij klanten dan wel de TTP-organisatie.

7.13 Vastlegging en bewaring van informatie

De TTP-organisaties zijn terughoudend in het aanvaarden van voorwaarden met betrekking tot vastlegging en bewaring van informatie, anders dan strikt noodzakelijk is voor de primaire doelstelling van de dienstverlening en het afleggen van externe (publieke) verantwoording.

8 Tot slot

Gaarne zijn wij bereid de inhoud van deze rapportage nader toe te lichten.

HET HOOFD EDP AUDIT POOL

w.g.

[redacted]

Bijlage 2 - Literatuur

Bij het opstellen van deze beleidsnotitie zijn de volgende bronnen geraadpleegd:

1. Opzet TTP-project in het kader van het Nationaal Actieprogramma Elektronische Snelwegen, 19 februari 1997
2. Projectplan NAP/TTP, KPMG Management Consulting / KPMG EDP Auditors, 4 juli 1997
3. Voorwaarden te stellen aan Trusted Third Parties t.b.v. TTP-project NAP, drs. R. van der Luit, Ministerie van Binnenlandse Zaken, 2 juni 1997, Stg. CONFIDENTIEEL
4. Overzicht randvoorwaarden, ing. J. van der Spek, Ministerie van Defensie, Centrale Organisatie/Bureau Beveiligingsautoriteit, 3 juni 1997
5. Randvoorwaarden voor het aanbieden en het gebruik van TTP-diensten, ir. S.B. Bootsma, Ministerie van Justitie, 3 juni 1997
6. TNO Fysisch en Elektronisch Laboratorium, Trusted Third Parties en Key Escrow, maart 1997
7. Gesetz zur digitalen Signatur (Signaturgesetz-SigG) - Referententwurf, Stand: 19. September 1996 - en verordnung zur digitalen Signatur (Signaturverordnung - SigV) - Referententwurf: Stand: 19. September 1996 - (Engelse versie beschikbaar als SOG-IS document 012/97,5 March 1997)
8. Ministry of Finance Finland, Electronic identification and Electronic Citizen Card, Helsinki, 29 October 1996
9. Ministry of Research and Information Technology Denmark, Draft Bill for Act on Digital Signature etc, IT-Policy Office, J nr 9601756, 14 November 1996
10. Information Society initiative, Licensing of Trusted Third Parties for the provision of encryption services, Public Consultation Paper on Detailed Proposals for Legislation, March 1997
11. ETSI, Technical Committee, Reference Technical Report, DEG/SEC-003000, Requirements for Trusted Third Party Services, Version 0.0.7, 26 March 1997
12. OECD, Cryptography Policy Guidelines, 27 March 1997
13. A European Initiative in Electronic Commerce, COM(97)157
14. Text of Administration March 12 Key Recovery Draft Legislation
15. MDW-rapport Normalisatie en Certificatie, MDW-werkgroep Certificering, februari 1996
16. Verslag van werkbijeenkomst Cryptografiebeleid, Canberra 9-11 juli 1997, mw. drs. H. de Brabander-Ypes
17. Commentaar op mogelijke randvoorwaarden t.b.v. NAP/TTP-project, drs. R. van der Luit, Ministerie van Binnenlandse Zaken - vertrouwelijk
18. Japan paper, Working meeting on international cooperation on cryptography policy, Canberra, 9-11 juli 1997
19. ISO/IEC JTC1/SC27, PDTR 14516, Guidelines for the use and management of Trusted Third Parties, 9 juni 1997
20. APEC Task Group on Public Key Authentication, OECD, 20-21 October 1997
21. Ensuring Security and Trust in Electronic Communication, Draft Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (97) 503
22. Draft Uniform Rules on Electronic Signatures, United Nations Commission on International Trade Law (UNCITRAL), Working Group on Electronic Commerce, 32th session, Vienna, 19-30 January 1998.
23. MDW-rapport Juridische Status Digitale Handtekening, Ministerie van Justitie en Ministerie van Economische Zaken (nog niet beschikbaar)
24. Uitgangspunten van wetgeving op de elektronische snelweg, Ministerie van Justitie, concept d.d. 8 december 1997

25. OECD Privacy guidelines
26. EU Privacy-richtlijn
27. EU Telecom Privacy-richtlijn
28. Dual use goods regulation (zie 4.4)
29. Wassenaar Arrangement (zie 4.4)

Bijlage 3 - Betrokken partijen

Leden van de projectgroep NAP/TTP

[redacted]

Ministerie van Verkeer en Waterstaat (HDTP) (voorzitter)
Ministerie van Verkeer en Waterstaat (HDTP)
Ministerie van Verkeer en Waterstaat (HDTP)
Ministerie van Economische Zaken
Ministerie van Economische Zaken
Ministerie van Economische Zaken
Ministerie van Financiën (EDP AUDIT POOL)
Ministerie van Financiën (EDP AUDIT POOL)
Technische Universiteit Delft
Ministerie van Algemene Zaken
Ministerie van Binnenlandse Zaken
Ministerie van Binnenlandse Zaken
Ministerie van Defensie
Ministerie van Justitie
KPMG EDP Auditors
KPMG EDP Auditors

Leden van de Consultatiegroep Aanbieders en Gebruikers

[redacted]

Academisch Ziekenhuis Leiden (Dienst CDIV)
Consumentenbond
Coopers & Lybrand
IBM Nederland B.V.
Interpay Nederland B.V.
KEMA Nederland B.V.
KNB
Ministerie van Binnenlandse Zaken (ACIB)
Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
Nederlandse Vereniging van Banken
Nlnet B.V.
NLSign B.V.
Percomad B.V.
Philips Crypto B.V.
PTT Post B.V.
Rabobank Nederland N.V.
RCC
Reginet B.V.
Registratiekamer
Shell Information Services B.V.
Stichting Ediforum
Vereniging van KvK en Fabrieken
VNO/NCW