Bijlage 9

Trusted Third Party diensten voor de Rijksoverheid

Vertrouwen in communiceren

EINDRAPPORT

Dit rapport werd geschreven in opdracht van de heer [redacted] MPA van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties onder eindredactie van [redacted] NLsign b.v

Den Haag, 12 juni 1999

Inhoudsopgave

1. INLEIDING 8

1.1 VRAAGSTELLING 9
1.2 AFBAKENING: TTP-DIENSTEN EN DE RIJKSOVERHEID 9
1.3 WERKWIJZE 11
1.4 LEESWIJZER 11

2. INTRODUCTIE TTP-DIENSTEN 12

2.1 COMMUNICEREN IN VERTROUWEN 12
2.2 AUTHENTICATIE-RAAMWERK 13
2.3 GEBRUIK VAN HET AUTHENTICATIE-RAAMWERK 17
2.4 ONTWIKKELINGSMODEL TTP-DIENSTEN 18
2.5 DE GENERIEKE ARCHITECTUUR VOOR TTP-DIENSTEN 19
2.6 EEN WERELD VAN TTP-DIENSTVERLENERS 21
2.7 SAMENVATTING 22

3. TTP-DIENSTEN VOOR DE RIJKSOVERHEID 24

3.1 WAAROM ZIJN TTP-DIENSTEN VOOR DE RIJKSOVERHEID BELANGRIJK? 24
3.2 DE NUL-OPTIE 28
3.3 ZIJN WE ER MET TTP-DIENSTEN ALLEEN? 30
3.4 CONCLUSIES 30

4. SCENARIO'S VOOR DE INVOERING 32

4.1 INLEIDING 32
4.2 SCENARIO 1: ÉÉN DOMEIN PER BEDRIJFSPROCES 33
4.3 SCENARIO 2: DEPARTEMENTALE DOMEINEN 34
4.4 SCENARIO 3: HET INTERDEPARTEMENTALE DOMEIN 36
4.5 SCENARIO 4: ÉÉN RIJKSOVERHEIDDOMEIN 39
4.6 CONCLUSIES 40

5. ORGANISATORISCHE ASPECTEN 42

5.1 INLEIDING 42
5.2 INRICHTING VAN EEN VERTROUWENSDOMEIN 42
5.3 VERSCHILLEN PER SCENARIO 44

6. UITBESTEDEN OF ZELF INRICHTEN EN BEHEREN? 46

6.1 WAAROM UITBESTEDING? 46
6.2 KERNPUNTEN 47
6.3 VARIANTEN VOOR UITBESTEDING 50
6.4 SAMENVATTING 55

7. CONCLUSIES 57

7.1 CONCLUSIES 57
7.2 AANBEVELINGEN 60

BIJLAGE 1: GERAADPLEEGDE DOCUMENTATIE **62**

BIJLAGE 2: KOSTENBEREKENING **63**

BIJLAGE 3: VERSLAG VAN HET BEZOEK AAN CANADA **71**

BIJLAGE 4: BESCHRIJVING VAN DE TTP MODULES

BIJLAGE 5: DEFINITIES ..... FOUT! BLADWIJZER NIET GEDEFINIEERD.

Managementsamenvatting

De opdracht die ten grondslag ligt aan dit onderzoek is:

'Het opstellen van een architectuur voor TTP-diensten voor eventueel gebruik binnen de overheid. Daarbij ligt het accent op de bestuurlijke en organisatorische aspecten en de technische alternatieven'.

Aan de grondslag van deze studie ligt de meer algemene vraag 'wat kunnen TTP-diensten voor de rijksoverheid betekenen?" En "wat betekent het als de Rijksoverheid TTP-diensten wil gaan gebruiken?" TTP-diensten kunnen een belangrijk middel vormen om binnen de Rijksoverheid te komen tot waarborgen voor authenticiteit, vertrouwelijkheid, integriteit, onweerlegbaarheid en autorisatie bij elektronische uitwisseling van gegevens. TTP-diensten hebben derhalve te maken met het bewerkstelligen van vertrouwen in elektronische informatie-uitwisseling, een vertrouwen dat noodzakelijk is in het licht van toenemend belang van ICT in de overheidscommunicatie.

De Rijksoverheid wordt op twee manieren geconfronteerd met het fenomeen TTP-diensten:
- in haar maatschappelijke functie als regelgever en beschermer van de burgers;
- als zelfstandige organisatie die betrouwbare elektronische diensten vereist voor haar bedrijfsprocessen.

De eerste categorie richt zich uitsluitend op de openbare TTP-diensten die in beginsel voor alle burgers, bedrijven en instellingen toegankelijk zijn en/of worden aangeboden via een openbare infrastructuur.

Dit rapport richt zich op de tweede categorie: de niet-openbare TTP-diensten voor de Rijksoverheid die worden ingezet ten behoefte van eigen bedrijfsvoering en toegankelijk zijn voor alle departementen. Daarin ziet de overheid zich geconfronteerd met een omgeving waarin een veelheid aan TTP-diensverleners bestaat.

Indien de Rijksoverheid nu geen strategische keuze maakt ten aanzien van het gebruik van Indien de overheid zich niet vroegtijdig voorbereid op deze ontwikkelingen, is de kans aanwezig dat zij door externe ontwikkelingen overvallen wordt. De overheid zal zich ten minste op strategisch niveau moeten buigen over de manier waarop men met TTP-diensten voor intern gebruik en voor externe communicatie wil omgaan.

Tot nu toe zijn nog geen departementsbrede afspraken gemaakt op welke wijze met niet-openbare TTP-dienten moet worden omgegaan. Zaken als certificatie van gebruikers, het genereren en beheren van enctyptiesleutels en digitale handtekeningen binnen de Rijksoverheid zijn nog niet geregeld. Voor het bewijzen van de elektronische identiteit wordt gebruik gemaakt van wachtwoordsystemen. Dit soort oplossingen voldoet niet meer aan de betrouwbaarheideisen in de situatie van complexe netwerken als Inter- en Intranetten. Er is een ander raamwerk noodzakelijk dat betrouwbaarheidsdiensten kan bieden tussen de eindpunten van de communicatie: de personen en informatiesystemen die daadwerkelijk met elkaar informatie uitwisselen. Zogenaamde end-to-end beveiliging.

Om betrouwbare end-to-end beveiliging te bieden, dienen de communicerende entiteiten te beschikken over betrouwbare identiteitsbewijzen voor de identificatie, betrouwbare cryptografische sleutels voor vertrouwelijke communicatie en betrouwbare toepassingen om de voorgaande te kunnen gebruiken. Dit zijn precies de kenmerken van een vertrouwensdomein. TTP-diensten en de toepassingen die daarvan gebruik maken bieden dergelijke betrouwbaarheidsdiensten.

De sterkte van het gebruik van TTP-diensten als basis van de betrouwbaarheid voor al deze toepassingen ligt in de uniformiteit. Een beperkt aantal TTP-diensten legt de basis voor het vertrouwen in de herkomst van berichten, de identificatie van personen ten behoeve van toegangsbeveiliging en het waarborgen van de integriteit en exclusiviteit van informatie. Het nu structureel aanpakken van maatregelen ter bevordering van de betrouwbaarheid voorkomt problemen op dit gebied in de toekomst.

Conclusie is in ieder geval dat, wil de Rijksoverheid nu en in de toekomst zakelijk gebruik maken van elektronische informatiediensten ter ondersteuning van de interne bedrijfsvoering, er een strategische keuze moet worden gemaakt voor een architectuur voor elektronische authenticiteit en betrouwbare electronische informatievoorziening.

Indien de Rijksoverheid beslist om TTP-diensten te gebruiken, wordt zij met een aantal vragen geconfronteerd. In het rapport zijn de belangrijkste vragen en mogelijke antwoorden daarop, met hun gevolgen, aangegeven.

De belangrijkste vraag is wel op welke wijze de TTP-diensten het beste binnen de complexe Rijksoverheidsorganisatie ingericht kunnen worden. Een viertal invoeringsscenario's is uitgewerkt om een onderbouwd antwoord op deze vraag te kunnen geven. Deze scenario's richten zich op de bestuurlijke aspecten van de invoering van TTP-diensten binnen de Rijksoverheid. De scenario's zijn:

- de decentraal gestuurde optie waarbij de bedrijfsprocessen de basis vormen voor de inrichting van de TTP-diensten;
- de centraal gestuurde optie waarbij een centrale orgaan de TTP-diensten levert;

en een tweetal tussenvormen:

- het departementaal gestuurde scenario waarbij elk departement zelf TTP-diensten inricht;
- en tenslotte het interdepartementale scenario waarbij er op interdepartementaal niveau kaders worden aangegeven waarbinnen departementen een eigen verantwoordelijkheid hebben om daaraan een eigen invulling te geven.

Geconcludeerd kan worden dat het interdepartementale scenario het beste aansluit bij de bestuurlijke structuur binnen de Rijksoverheid.

Een tweede belangrijke vraag is, welke organisatorische aspecten vervolgens gepaard gaan met de invoering van TTP-diensten. De organisatievorm is uiteraard afhankelijk van de scenario's. Daarom is in algemene zin beschreven welke activiteiten en organisatie-elementen noodzakelijk zijn voor het opzetten en in stand houden van TTP-diensten binnen een vertrouwensdomein. Daarbij zijn de noodzakelijke kwaliteiten van personeel en organisatie aangegeven.

De belangrijkste elementen van een vertrouwensdomein zijn: de TTP-diensten, de toepassingen en de communicerende partijen binnen een domein en cross-certificering met externe domeinen. Ten aanzien van al deze elementen dienen randvoorwaarden te worden gesteld, keuzes te worden gemaakt en beheersactiviteiten te worden ontplooit. Dit alles met het doel TTP-diensten duurzaam in de organisatie onder te brengen.

Tot slot is gekeken naar de mogelijkheden om delen van de TTP-dienstverlening uit te besteden. Uitbesteding van diensten is in principe mogelijk aangezien er in de markt inmiddels een aantal bedrijven zijn die TTP-diensten leveren. In wezen gelden voor het uitbesteden van TTP-diensten dezelfde argumenten als voor de meeste ICT-diensten. Zo kunnen initiële investeringen beperkt worden, kunnen kosten veelal direct gerelateerd worden aan het daadwerkelijke gebruik, kunnen desinvesteringen ten gevolge van veroudering van de techniek beperkt worden en wordt de eigen organisatie niet belast met zaken die zich niet richten op de kernactiviteiten.
Ten aanzien van de vraag of uitbesteding wenselijk is, heeft de overheid een specifieke rol in de maatschappij die aanleiding kan geven om eerder voor uitbesteding aan marktpartijen te kiesen dan voor zelf doen. Voordat men deze keuze maakt, dienen echter een aantal punten goed te worden overwogen. Daartoe zijn een 7-tal specifieke kernpunten genoemd die in overweging moeten worden genomen, dit zijn:

1. Beleid: Welke invloed heeft uitbesteding op de keuzemogelijkheid ten aanzien van het beleid binnen het domein (of beveiligingsniveau)?
2. Exclusiviteit: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de exclusiviteit van gegevens uit te besteden?
3. Integriteit: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de integriteit van gegevens, met name de digitale handtekening, uit te besteden?
4. Privacy: Is het vanuit privacy-oogpunt mogelijk om TTP-diensten uit te besteden?
5. Beschikbaarheid: Hoe zit het met de continuïteit van de dienstverlening bij uitbesteding?
6. Integratie: Is het mogelijk om diensten die zo geïntegreerd zijn met de organisatie uit te besteden?
7. Aansprakelijkheid: Welke invloed heeft uitbesteden op het aansprakelijkheids-vraagstuk?

De vraag is echter of diensten ten behoeve van de beveiliging van de eigen informatie uitbesteed kunnen worden. Om dit te analyseren is een 4-tal uitbestedingsvarianten uitgewerkt:

- Variant 1: Alles zelf doen
- Variant 2: Delen uitbesteden
- Variant 3: Maximaal uitbesteden met gebruik van besloten TTP-diensten
- Variant 4: Maximaal uitbesteden met gebruik van openbare TTP-diensten

De tweede variant biedt de meeste flexibiliteit in combinatie met een beperking van de risico's ten aanzien van de initiële kosten, de veroudering van de technologie en de beschikbare kennis. Ook scoort deze variant goed op de 7-kernpunten.

Dit leidt tot de volgende conclusies:

- Conclusie 1: een raamwerk voor het bewijzen van de elektronische identiteit (authenticatie) is noodzakelijk voor de verdere ontwikkeling van betrouwbare electronische infomatediensten

- Conclusie 2: TTP-diensten bieden een uniform raamwerk voor betrouwbaarheidsdiensten ten behoeve van electronische communicatie en informatiediensten
- Conclusie 3: Er ontstaat een breed draagvlak voor het gebruik van TTP-diensten
- Conclusie 4: Ten aanzien van de inrichting van TTP-diensten binnen de Rijksoverheid scoort het Interdepartementale domein (scenario 3) het best
- Conclusie 5. De Rijksoverheid kan het beste delen van de TTP-diensten zelf opzetten en delen uitbesteden volgens variant 2
- Conclusie 6: de invoering van de niet-openbare TTP-diensten binnen de Rijksoverheid vraagt op het interdepartementale niveau een aantal strategische keuzes

Wij bevelen u daarbij het volgende aan:

- Aanbeveling 1: Om nu een strategische keuze te maken over het gebruik van TTP-diensten binnen de Rijksoverheid.
- Aanbeveling 2: Om de TTP-diensten en voorzieningen zo veel mogelijk gecoördineerd, gezamenlijk in te richten volgens scenario 3: het Interdepartementale domein.
- Aanbeveling 3: Beheer het veranderproces zowel op interdepartementaal als departementaal niveau.
- Aanbeveling 4: Om een combinatie van zelf doen en uitbesteden te kiezen volgens variant 2: delen uitbesteden.
- Aanbeveling 5: Om enkele proefprojecten te starten waarbij verschillende TTP-toepassingen gebruikt worden.

1. Inleiding

Elektronisch communiceren is in opmars binnen de Rijksoverheid. De voornemens die de overheid ten aanzien van dit onderwerp heeft, zijn onder andere weergegeven in het Actieprogramma Elektronische Overheid. Hierin wordt betoogd dat de opkomst van ICT (Informatie- en Communicatie-Technologie) in volle omvang de vier traditionele overheidsfuncties raakt: de ordenende, de sturende, de presterende en de verzorgende.

Het Actieprogramma concentreert zich op de presterende en verzorgende functies van de overheid, oftewel, de rol van de overheid als speler in het maatschappelijk proces. Ten aanzien van deze rol wordt een drietal hoofdgebieden onderscheiden waarop het belang van ICT zich steeds meer doet gelden:

- een goede elektronische toegankelijkheid van de overheid,
- een betere publieke dienstverlening, en
- een verbeterde interne bedrijfsvoering van de overheid.

Het rapport dat nu voor u ligt heeft primair betrekking op het derde onderscheiden gebied waar ICT van belang is voor het functioneren van de overheid: de interne bedrijfsvoering van de overheid. Mede hiervoor is de aanzet gemaakt om te komen tot een overheidsintranet. In het kader van dit overheidsintranet is nadrukkelijk gewezen op het belang van de mogelijkheid van beveiligde elektronische communicatie tussen medewerkers van de overheid - dit wordt in dit kader als een absolute "need to have"-applicatie beschouwd.

Ook het SG-beraad heeft zich concreet met het onderwerp van informatie-beveiliging met betrekking tot ICT bezig gehouden, en het IB-beraad in september 1998 gevraagd een notitie op te stellen inzake beveiliging van het Internet. Door het IB-beraad zijn vier concrete acties opgestart:

- beveiligd end-to-end e-mailverkeer,
- omgaan met TTP's
- overheidscommunicatie-protocol,
- gedragscode voor Internet-gebruik.

De eerste twee acties zijn voor het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB) van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aanleiding geweest een tweetal onderzoeken op te starten: een onderzoek met als doel te komen tot een architectuur voor beveiligde e-mail binnen (onderdelen van) de Rijksoverheid, en een onderzoek met als doel te komen tot een architectuur voor Trusted Third Parties binnen de Rijksoverheid.

Beide onderzoeken zijn uitgevoerd in samenwerking met een consortium bestaande uit NLSign bv, M&I/PARTNERS bv en M&I/STELVIO bv, en met diverse vertegenwoordigers van onderdelen van de Rijksoverheid. De beide onderzoeken hebben geleid tot een tweetal afzonderlijke, maar wel samenhangende, rapporten:

- het voor u liggende rapport "Trusted Third Party diensten voor de Rijksoverheid,

- het rapport "Beveiligde E-mail voor de Rijksoverheid".

Zoals gezegd, het voor u liggende rapport betreft het onderwerp "TTP-diensten voor de Rijksoverheid". Aan de grondslag van deze studie ligt geen concreet probleem waarvoor TTP-diensten kunnen worden ingezet, maar de meer algemene vraag 'wat kunnen TTP-diensten voor de rijksoverheid betekenen?" TTP-diensten kunnen een belangrijk middel vormen om binnen de Rijksoverheid te komen tot waarborgen voor authenticiteit, vertrouwelijkheid, integriteit, onweerlegbaarheid en autorisatie bij elektronische uitwisseling van gegevens. TTP-diensten hebben derhalve te maken met het bewerkstelligen van vertrouwen in elektronische informatie-uitwisseling, een vertrouwen dat noodzakelijk is in het licht van het hiervoor geschetste toenemend belang van ICT in de overheidscommunicatie.

1.1 Vraagstelling

De opdracht die ten grondslag ligt aan dit onderzoek is:

'Het opstellen van een architectuur voor TTP-diensten voor eventueel gebruik binnen de overheid. Daarbij ligt het accent op de bestuurlijke en organisatorische aspecten en de technische alternatieven'.

De focus ligt hierbij nadrukkelijk op communicatie binnen de overheid. Communicatie met externe organisaties en burgers is geen zwaartepunt binnen deze opdracht. Waar zinnig wordt echter wel op de mogelijke consequenties van deze communicatiebehoefte gewezen.

De realisatie van deze opdracht vindt plaats door middel van de beantwoording van de volgende deelvragen:

1. *Wat wordt verstaan onder TTP -diensten?*
2. *Waarom zijn de TTP-dienten voor de Rijksoverheid belangrijk?*
3. *Welke scenario's zijn er bij de invoering van TTP-diensten binnen de Rijksoverheid?*
4. *Welke organisatorische aspecten zijn er bij de invoering van TTP-diensten binnen de Rijksoverheid van het belang?*
5. *Welke keuzes zijn er bij de invoering en de instandhouding van TTP-diensten binnen de Rijksoverheid ten aanzien van uitbesteden of zelf opzetten van een TTP-dienstverlening?*

Met de achtereenvolgende beantwoording van deze vragen gaan we van een hoog abstractieniveau naar een steeds concreter niveau: eerst de afbakening van het onderzoeksterrein (het wat en waarom), vervolgens aangeven we wat er binnen de verschillende onderdelen van de Rijksoverheid geregeld moet worden bij de concrete invoering van TTP-diensten en welke keuzes hierbij gemaakt moeten worden.

1.2 Afbakening: TTP-diensten en de Rijksoverheid

Zonder overdrijven kan gesteld worden dat dé grote drijfveer achter de ontwikkeling van elektronische TTP-diensten gezocht moet worden in de hooggespannen verwachtingen ten aanzien van elektronisch zakendoen oftewel e-commerce. Er is een brede consensus dat het

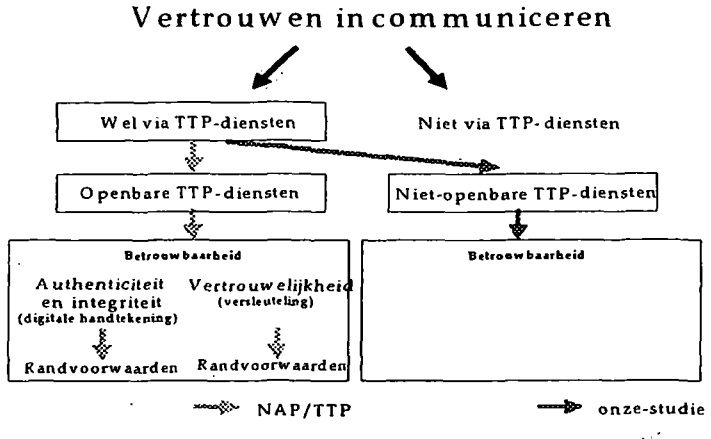
gebrek aan vertrouwen op de elektronische snelweg de commerciële mogelijkheden van e-commerce sterk belemmeren. De eerste vraag die word gesteld voordat men een transactie begint is: weet ik met wie ik zaken doe? En: is die ander te vertrouwen?. Belangrijker is vaak nog het antwoord op de vraag 'wie kan ik aansprakelijk stellen als het fout gaat?' Deze vragen zijn zowel van belang voor de aanbieder van diensten op de elektronische snelweg als de consument.

TTP-diensten, digitale identiteitsbewijzen en digitale handtekeningen bieden vooralsnog de beste mogelijkheden om dit vertrouwen te realiseren. Daarmee bieden TTP's diensten die niet alleen in de e-commercehoek, maar ook in al die situaties waarbij partijen de behoefte hebben om vertrouwelijke en integere communicatie te voeren, ingezet kunnen worden.

TTP-diensten vormen dus een belangrijke schakel in de keten die noodzakelijk is om betrouwbare communicatie op te kunnen zetten op een brede schaal. Gezien dit belang heeft de Nederlandse overheid zich in een vroeg stadium afgevraagd hoe zij op het fenomeen TTP-diensten dient te reageren. In 1997 is in opdracht van de overheid een onderzoek uitgevoerd naar de mogelijke randvoorwaarden die moeten worden gesteld aan aanbieders van TTP-diensten en de TTP-diensten zelf. De belangrijke vraag daarbij voor de overheid was of (nationale) wet- of regelgeving noodzakelijk is.

Dit nationaal TTP-project (NAP/TTP) had uitsluitend betrekking op openbare[2] TTP-diensten. Deze diensten zijn TTP-diensten die in beginsel voor alle burgers, bedrijven en instellingen toegankelijk zijn en/of worden aangeboden via een openbare infrastructuur. Het werkingsgebied van NAP/TTP is dus de publieke dienstverlening.

In tegenstelling tot dat nationaal TTP-project, richt deze studie zich echter op de niet-openbare dienstverlening. In onderstaande figuur wordt een overzicht gegeven van de samenhang tussen het nationaal TTP-project en deze studie:



Figuur 1.1. De samenhang tussen het nationaal TTP-project en deze studie

[2] Eindrapportage Nationaal TTP-project in managementsamenvatting

De TTP-diensten voor de Rijksoverheid die in dit rapport worden beschreven, worden dus ingezet ten behoefte van eigen bedrijfsvoering en zijn toegankelijk voor alle departementen. Waar het NAP/TTP traject zich richtte op de overheid in haar maatschappelijke rol met taken als het beschermen van de burgers en het stimuleren van de economie, heeft deze studie betrekking op de overheid als zelfstandige organisatie.

1.3 Werkwijze

Wij zijn tijdens de studie op de volgende wijze te werk gegaan: om te beginnen is de documentatie bestudeerd om een goed overzicht te krijgen over de context en scope van TTP-diensten voor de Rijksoverheid. In bijlage 1 vindt u een overzicht van de belangrijkste geraadpleegde documentatie

Op basis van deze studie is een groot aantal informatieve en toetsende vragen gesteld aan de leden van de begeleidingsgroep, waaruit een veelheid aan mondelinge en waar mogelijk, schriftelijke informatie is voortgekomen Parallel hieraan hebben we op grond van de (praktijk) ervaring en kennis van de opdrachtnemer een aantal denkmodellen ontwikkeld. Tevens is een bezoek gebracht aan het projectteam dat in Canada verantwoordelijk is voor de implementatie van TTP-diensten voor de Canadese overheid (zie bijlage 3 voor een verslag van dit bezoek). Vervolgens is op basis van de denkmodellen aangegeven hoe de TTP-diensten binnen de Rijksoverheid geïmplementeerd kunnen worden. Tenslotte is een aantal hoofdconclusies getrokken en een aantal aanbevelingen geformuleerd.

De resultaten van de studie zijn bij de begeleidingsgroep en het ACIB getoetst op feitelijke correctheid.

1.4 Leeswijzer

Het rapport dat voor u ligt is opgebouwd uit zeven delen.
Het eerste deel "Inleiding" bestaat uit de vraagstelling en een beschrijving van de werkwijze tijdens de studie. Tevens wordt het onderzoek afgebakend.
Het tweede deel "Introductie TTP-diensten" wordt en vrij uitgebreide introductie gegeven over TTP-diensten en hun toepassingen.
In het derde deel " TTP-diensten voor de Rijksoverheid" geven wij de mogelijkheden en de urgentie van dergelijke diensten voor de Rijksoverheid aan.
In het vierde deel "Scenario's voor de invoering" beschrijven wij een aantal scenario's voor de invoering van de TTP-diensten binnen de Rijksoverheid, gevolgd door de voor- en nadelen van elk van deze scenario's.
In het vijfde deel "Organisatorische aspecten" beschrijven wij mede aan de hand van de scenario's de organisatorische aspecten die samenhangen met de invoering en instandhouding van TTP-diensten.
In het zesde deel "Uitbesteden of zelf doen" legen we het accent op de keuze ten aanzien van het uitbesteden dan wel zelf opzetten van TTP-diensten binnen de Rijksoverheid.
Het zevende deel "Conclusies en aanbevelingen" recapituleert de relevante delen van het rapport en komt tot een aanbeveling.

2. Introductie TTP-diensten

In dit hoofdstuk wordt het terrein waarop dit onderzoek zich richt, beschreven. Dit hoofdstuk beantwoordt de eerste deelvraag:

Wat wordt verstaan onder TTP -diensten?

Allereerst wordt hier ingegaan op het algemeen belang van TTP-diensten bij elektronische communicatie. Vervolgens wordt het algemene "authenticatie-raamwerk" gepresenteerd waarmee TTP-diensten in deze studie beschreven worden. Vervolgens wordt beschreven hoe dit raamwerk wordt gebruikt in toepassingen, en welke ontwikkelingsstadia we kunnen onderscheiden in TTP-dienstverlening. Tenslotte worden de verschillende beschreven componenten samengebracht in een generieke architectuur voor TTP-diensten.

2.1 Communiceren in vertrouwen

De grote vragen bij elektronische interacties zijn: "hoe weet ik met zekerheid met wie ik communiceer?" én "hoe kan ik zorgen dat niemand meeleest én "hoe weet ik dat dit document echt is ". Debet hieraan is vooral de fysieke scheiding. Wie zit er nu echt aan de andere kant van de lijn? Om deze vraag te kunnen beantwoorden is een betrouwbaar raamwerk voor het bewijzen van de identiteit noodzakelijk. Het bewijzen van een identiteit, of in algemenere zin de oorsprong van iets, wordt authenticiteit genoemd. Wil men nu en in de toekomst zakelijk gebruik maken van elektronische informatiediensten dan moet een strategische keuze worden gemaakt voor een architectuur voor authenticiteit.

Voor het bewijzen van de identiteit bestaan verschillende technieken. De meest bekende bestaat uit wachtwoordsystemen: een persoon claimt een identiteit en door het ingeven van het bijbehorende wachtwoord toont hij of zij de authenticiteit daarvan aan. De grote beperking van deze systemen ligt in de noodzaak zich vooraf aan te melden bij het accepterende systeem. Het systeem moet het wachtwoord immers herkennen. Binnen grote gemeenschappen en een grote hoeveelheid van systemen is dit al snel onbeheersbaar. Er ontstaat de behoefte aan een systeem waarbij de authenticiteit kan worden vastgesteld zonder expliciete aanmelding vooraf. Dit wordt ook wel aangeduid met de term 'persistente identiteit': een betrouwbare elektronische identiteit die losstaat van specifieke systemen en omgevingen.

Zoals al is aangegeven aan de hand van wachtwoordsystemen zijn er alternatieve oplossingen[1] voor de hierboven gestelde vragen. Geen van deze oplosingen biedt echter het brede scala aan gebruiksmogelijkheden als TTP-diensten. Naast het bewijs van authenticiteit bieden TTP-diensten ondermeer mogelijkheden voor het waarborgen van de

[1] Bekende voorbeelden zijn wachtwoordsystemen, pin-codes, kerberos authenticatie, pgp voor beveiligde e-mail en gesloten gebruikersgroepen.

exclusiviteit en integriteit van gegevens, sleutelbeheer en onweerlegbare bewijsvoering middels digitale handtekeningen.

2.2 Authenticatie-raamwerk

De wijze waarop een dergelijke authenticatie van een identiteit in de digitale wereld gerealiseerd wordt, verschilt in essentie weinig van de fysieke wereld. Denk daarbij aan het uitgeven van een paspoort. Een vertrouwde instantie, de overheid, geeft een paspoort uit. Door het vertrouwen in de overheid en in de fraudebestendigheid van het paspoort, wordt het paspoort door een grote gemeenschap geaccepteerd als hoogwaardig identiteitsdocument.

In de digitale wereld is een dergelijk op TTP-diensten gebaseerd authenticatie-raamwerk opgebouwd uit een aantal componenten. De meest herkenbare componenten zijn:
1. Certification Authority (CA)
2. Registration Authority (RA)
3. Policy Authority (PA)
4. Trusted Parties en Trusted Third Parties
5. Overige componenten

1. De Certification Authority en het uitgifteproces

Een model waarbij onbekenden een identiteitsbewijs accepteren vergt een autoriteit die voldoende gezag en vertrouwen geniet van de gemeenschap waarvoor zij actief is. De gemeenschap delegeert het vertrouwen aan die autoriteit. Deze autoriteit wordt in de on-line wereld aangeduid met de term Certification Authority (CA). De CA is dus een vertrouwde instantie die een elektronisch identiteitsbewijs uitgeeft.

Om een identiteitsbewijs aan een persoon te binden, dient men een aantal authenticerende kenmerken van die persoon in het identiteitsbewijs op te nemen. Daarbij worden vaak drie typen kenmerken gebruikt:
- iets dat men heeft (paspoort),
- iets dat men weet (wachtwoord) en
- iets dat men is (biometrisch of fysiek kenmerk: pasfoto, handtekening).

Zo is het paspoort zelf iets dat men heeft en de pasfoto, leeftijd en kleur ogen zijn fysieke kenmerken. Bij elektronische identificatie zullen soms andere kenmerken gebruikt moeten worden - men ziet elkaar immers meestal niet, dus heeft een pasfoto geen waarde.

De Certification Authority maakt daarom gebruik van iets dat alleen de eigenaar van het identiteitsbewijs heeft: een geheime cryptografische sleutel van de eigenaar. Omdat een dergelijke sleutel uiteraard niet zonder meer kan worden opgenomen in een publiekelijk beschikbaar identiteitsbewijs, wordt een bepaalde vorm van cryptografie gebruikt waarbij twee verschillende sleutels nodig zijn die strikt bij elkaar horen: een private en een publieke sleutel.

De *private sleutel* dient te allen tijde geheim te worden gehouden. De bijbehorende *publieke sleutel* mag, zoals de naam al aangeeft, vrijelijk aan derden worden gegeven. De essentie is dat de bezitter van de private sleutel daarmee onomstotelijk kan aantonen dat de bijbehorende publieke sleutel van hem of haar is. De Certification Authority maakt hiervan gebruik door eerst te controleren of iemand in het bezit is van zowel een private als de bijbehorende publieke sleutel en vervolgens de publieke sleutel, samen met de identiteit (naam) op te nemen in een elektronisch identiteitsdocument. Dit document, dat wordt uitgegeven namens de Certification Authority, wordt een *publieke sleutel certificaat* of kortweg *certificaat* genoemd.

Wat nu nog ontbreekt is een bescherming tegen fraude. Hoe kunnen we garanderen dat het aldus aangemaakte certificaat niet illegaal wordt gewijzigd? Hiertoe verzegelt de Certification Authority het certificaat met zijn eigen digitale handtekening. De digitale handtekening heeft eigenschappen die sterk overeenkomen met de vertrouwde handtekening: slechts één persoon kan een bepaalde handtekening zetten, terwijl iedereen die dat wil deze handtekening kan controleren. Langs elektronische weg maken we daarvoor gebruik van de eerder genoemde private en publieke sleutels. Wat de Certification Authority met zijn private sleutel kan vercijferen, kan iedereen met de bijbehorende publieke sleutel van de CA controleren (ontcijferen).

De Certification Authority zet zijn digitale handtekening door alle informatie in het certificaat met zijn private sleutel te vercijferen. Slechts door gebruik te maken van de publieke sleutel van de CA voor het ontcijferen, kan het certificaat gebruikt worden Dit heeft als bijkomend voordeel dat certificaten die door een Certification Authority zijn uitgegeven, slechts geaccepteerd worden als men de publieke sleutel van die CA wenst te gebruiken. Op deze wijze kan men de autoriteit van de Certification Authority erkennen of afwijzen.

Op een zelfde wijze kan ook een eigenaar van een certificaat digitale handtekeningen zetten: de eigenaar heeft immers ook een private en publieke sleutel! We creëren zo een hiërarchische keten van vertrouwen die begint bij de Certification Authority en eindigt bij een digitale handtekening van een eigenaar van een certificaat. De stappen na ontvangst van een digitale handtekening zijn telkens de volgende:

- Zoek het gebruikerscertificaat waarin de bijbehorende publieke sleutel zit om de handtekening te controleren.
- Het gebruikerscertificaat is ondertekend door een Certification Authority; zoek het CA-certificaat waarin de bijbehorende publieke CA sleutel zit om het certificaat te controleren;
- Controleer of de Certification Authority vertrouwd (erkend) wordt.
  - Zo ja, dan kan de authenticiteit vertrouwd worden en kan de identiteit bepaald worden aan de hand van het gebruikerscertificaat;
  - Zo nee, verwerp de handtekening en wantrouw de authenticiteit of vertrouw het certificaat door een andere wijze van verificatie.

Aangezien telkens dezelfde technieken worden toegepast, kan de keten ook langer gemaakt worden. Zo kunnen hiërarchieën van CA's gecreëerd worden waarbij 'lagere' CA's door 'hogere' CA's worden gecertificeerd.

2. De Registration Authority en het registratieproces

Voordat een Certification Authority een certificaat uitgeeft, dient zij uiteraard overtuigend bewijs te hebben van de te certificeren identiteit. De waarde van een certificaat is sterk afhankelijk van deze identiteitsverificatie. Afhankelijk van de procedures die worden gevolgd, kan men spreken van verschillende vertrouwensniveaus. Het verifiëren van de identiteit wordt veelal uitgevoerd door een instantie die verbonden is met de Certification Authority. Deze instantie wordt de Registration Authority (RA) genoemd. De RA registreert en verifieert de aanvragen en de eigenaren van certificaten[2].

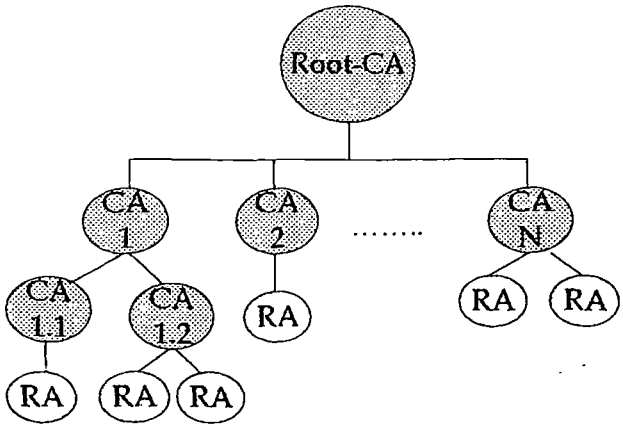
In wat een grove simplificatie kan worden genoemd is de Certification Authority de certificaten fabriek en de Registration Authority het loket.

3. De Policy Authority en de regels

Wat nu nog ontbreekt binnen het authenticatieraamwerk zijn de regels waarbinnen de Certification Authority en Registration Authority hun activiteiten uitvoeren. Daarin wordt bijvoorbeeld bepaald welke identiteitsverificatie moet worden uitgevoerd voordat een certificaat kan worden uitgegeven en de weerstand van het certificaat tegen fraude. Een essentiële component van het raamwerk is dan ook de beleidsmakende instantie: de Policy Authority (PA).

Zoals gezegd kunnen CA's zowel personen als onderliggende CA's certificeren. Op deze wijze ontstaat een hiërarchie van CA's. Dit wordt gebruikt in grote gemeenschappen en om aan een (beperkte) variatie in het beleid tegemoet te komen: elke CA kan een aangepast beleid ondersteunen. De hoogste Certification Authority in de hiërarchie wordt veelal aangeduid met de term 'root-CA'.

In de onderstaande figuur is de hiërarchie van CA's schematisch weergegeven:



[2]. Een andere term die wel wordt gebruikt is de Local Registration Authority (LRA)

Figuur 2.1. De hiërarchie van CA's

4. Trusted Parties en Trusted Third Parties

De Certification Authority en Registration Authority zoals die hierboven beschreven zijn leveren belangrijke TTP-diensten binnen een gemeenschap. Elke partij die een certificaat accepteert dat is uitgegeven door een Certification Authority, dient het vertrouwen in de CA uit te spreken. CA's en RA's zijn dan ook vertrouwde partijen of Trusted Parties (TPs). Binnen een organisatie zou bijvoorbeeld personeelszaken of een beveiligingsdienst deze rol kunnen vervullen.

Indien een TP duidelijk belang zou hebben bij een deel van de gecertificeerde personen, kan het vertrouwen in de diensten aangetast worden. Daarom kan het in sommige gevallen noodzakelijk zijn dat de diensten door een volledig onpartijdige organisatie worden geleverd. In dat geval spreekt men van een Trusted Third Party. De termen TP en TTP hebben dan ook meer te maken met de vorm waarin TTP-diensten worden aangeboden terwijl met CA en RA meer de activiteiten worden aangegeven.

Voor de eenvoud zullen we in dit rapport verder alleen de term TTP(-diensten) gebruiken.

5. Andere elementen in het raamwerk

We hebben nu de meest essentiële componenten en diensten van het authenticatie-raamwerk beschreven: de Policy Authority, Certification Authority en Registration Authority. Naast authenticatie kunnen certificaten ook gebruikt worden voor het beschermen van informatie tegen het ongeautoriseerd wijzigen (integriteit) en het ongeautoriseerd inzien (exclusiviteit) van informatie. Daarbij wordt wederom gebruik gemaakt van certificaten, de digitale handtekening en vercijfering.
Voor een effectieve uitwisseling van certificaten en de daarin opgenomen sleutels is er behoefte aan een distributiefunctie. Deze functie wordt aangeduid met de term Distribution Service (DS[3]). Deze zorgt ook voor bijvoorbeeld het publiceren van een lijst met ingetrokken certificaten.

Daarnaast zijn er TTP-diensten noodzakelijk voor het aanmaken en beheren van sleutels (Key Manager, KM) en het uitgeven van unieke namen binnen een domein (Name Service, NS). In bijlage "Beschrijving TTP-modules" zijn noodzakelijke diensten, die we de *TTP-basisdiensten* zullen noemen, in detail beschreven.

De Distribution Service is net als Policy Authority, Certification Authority en Registration Authority een noodzakelijke component, een TTP-basisdienst. Naast deze noodzakelijke basisdiensten kan het raamwerk ook voorzien in *toegevoegde TTP-diensten*. Voorbeelden hiervan zijn diensten voor:

- het onweerlegbaar aantonen van verzending en ontvangst van berichten
- het bewaren en tijdstempelen van berichten en documenten en

[3]De afkorting DS staat ook voor Directory Service, een standaard voor een gedistribeerde database. Met Distribution Service wordt een algemenere functie bedoeld die ondermeer kan bestaan uit een Directory Service.

- het bewaren van cryptografische sleutels (key escrow/key recovery).

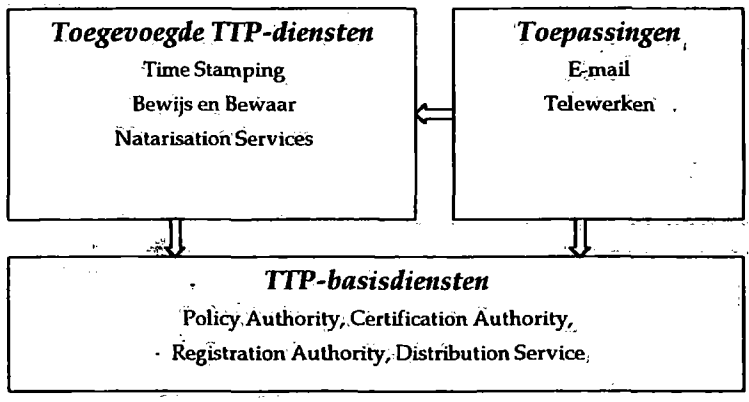
In bijlage "Beschrijving TTP-modules" zijn noodzakelijke de toegevoegde TTP-diensten in detail beschreven.

2.3 Gebruik van het authenticatie-raamwerk

Het doel van dergelijke TTP-diensten is natuurlijk dat ze gebruikt worden. Steeds meer producten en toepassingen kunnen gebruik maken van certificaten voor het authenticeren en vercijferen van elektronische berichten, documenten en communicatie.

Op dit moment zijn de twee meest gebruikte toepassingen van certificaten het beveiligen van elektronische post en het beveiligen van Internettransacties. De standaarden die daarvoor gebruikt worden (S/MIME en SSL) zijn geïmplementeerd in web-browsers en e-mail pakketten die wereldwijd in enorme aantallen worden afgezet. De bekendste voorbeelden zijn de Netscape en Microsoft browsers en e-mail pakketten. Deze leveranciers bieden complete intranet-suites waarbij toegangsbeveiliging en exclusiviteit op basis van TTP-diensten wordt gerealiseerd.
Ook firewall-producten gebruiken steeds vaker certificaten voor het realiseren van Virtual Private Networks: een gesloten bedrijfsnetwerk over een open (Intranet) communicatie-infrastructuur.

In de onderstaande figuur zijn de relaties tussen de basis- en toegevoegde TTP-diensten en de toepassingen schematisch weergegeven:



Figuur 2.2. De relatie tussen basis- en toegevoegde TTP-diensten en toepassingen

We zien daarin dat zowel de toegevoegde TTP-diensten als de toepassingen gebruik maken van de basis TTP-diensten. De toepassingen kunnen verder ook gebruik maken van de toegevoegde TTP-diensten.

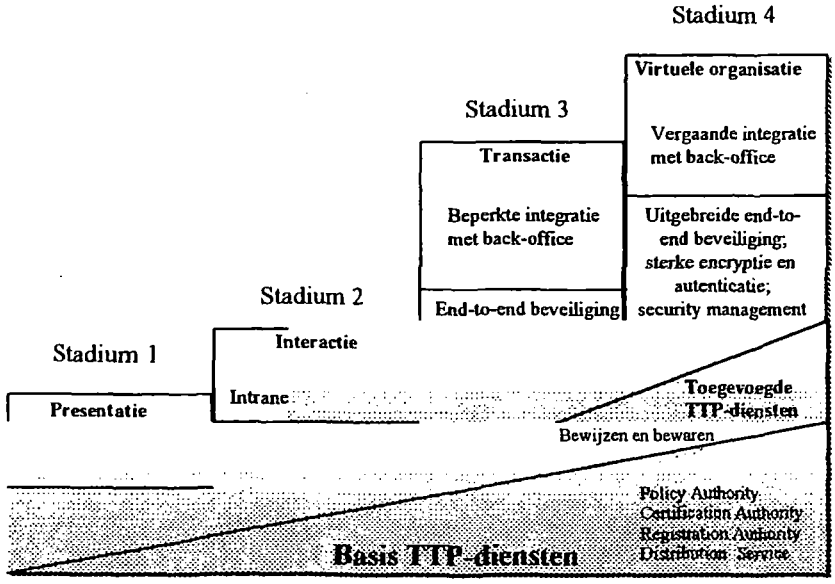
2.4 Ontwikkelingsmodel TTP-diensten

De TTP-dienstverlening staat nog aan het begin van de ontwikkelingen. Uiteraard zijn de basisdiensten beschikbaar. Ook zijn er toepassingen die gebruik maken van deze basisdiensten. Het aantal toepassingen dat gebruik maakt van TTP-diensten neemt zelfs snel toe. Deze toepassingen krijgen ook steeds meer mogelijkheden om in de bedrijfsprocessen en back-office systemen te worden geïntegreerd. Voorbeelden hiervan zijn verschillende E-commerce toepassingen als bestellen en betalen.

We kunnen dan ook een eenvoudig model opstellen voor de ontwikkelingsfasen van TTP-diensten. Aan het begin staan de basisdiensten waar eenvoudige, losstaande toepassingen als e-mail gebruik van maken.
In de tweede fase zien we dat er nieuwe informatiediensten gebruik maken van beperkte TTP-diensten. Deze nieuwe informatiediensten staan nog relatief los van bestaande back-office systemen.
Een stap verder zien we een vergaande integratie met back-office. In deze fase staat de elektronische identiteit los van specifieke systemen en omgevingen.
De laatste fase impliceert volledige integratie met de organisatie. In deze fase worden de grenzen van een organisatie niet meer bepaald door fysieke grenzen maar door communicatiestructuren.

De overgang tussen de verschillende fasen gaat gepaard met ontwikkelingen op het gebied van de toepassingen, de TTP-diensten en uiteraard de organisatie zelf. Naarmate men verder in de evolutie zit, worden er hogere eisen gesteld aan de TTP-diensten. Er zal een behoefte bestaan aan meerdere betrouwbaarheidsniveaus en toegevoegde diensten. De toepassingen zullen zelf ook betrouwbaarder moeten zijn naarmate men er afhankelijker van wordt.

In de volgende figuur is dit schematisch weergegeven:



Figuur 2.3. Ontwikkelingsmodel TTP-dienten

De toepassingen zijn op dit moment tot stadium 2 goed beschikbaar. Aan de ontwikkeling van stadium 3 wordt hard gewerkt. Stadium 4 is nog een uitdaging.

Belangrijk is om te constateren dat een investering in de TTP-basisdiensten niet alleen noodzakelijk is voor de verdere ontwikkeling, maar ook redelijk toekomstvast. Met name deze basisdiensten zouden door de Rijksoverheid in gezamenlijk overleg aangeschaft of ingekocht kunnen worden. In hoofdstuk 4 zal dan ook met name naar de invoering van TTP-basisdiensten gekeken worden.

2.5 De generieke architectuur voor TTP-diensten

In de voorgaande paragrafen is een beschrijving gegeven van de belangrijkste componenten en ontwikkelingen ten aanzien van TTP-diensten. Ter afsluiting van dit hoofdstuk worden deze samengebracht in een generieke architectuur voor TTP-diensten. Deze architectuur is een blauwdruk die de grenzen en bedoelingen van de globale componenten aangeeft.

In essentie zijn er dan de volgende componenten[4]:

- *Vertrouwensdomeinen* waar binnen partijen met elkaar elektronisch communiceren conform de afspraken omtrent de betrouwbaarheid van de elektronische gegevensuitwisseling.
- *Communicerende partijen* die binnen een vertrouwensdomein geregistreerd en geïdentificeerd worden.
- *TTP-diensten* inclusief technologische voorzieningen (waaronder toepassingen) met als doel het realiseren van vertrouwen in communiceren.

In de volgende figuur is dit schematisch weergegeven. Tevens is in die figuur cross-certificering, de brug die communicatie tussen vertrouwensdomeinen mogelijk maakt, aangeven.

Figuur 2.4. De generieke architectuur voor de TTP-diensten

Vertrouwensdomein

De essentiële component van de architectuur is het vertrouwensdomein. Het vertrouwensdomein is het totaal aan TTP-diensten, communicerende partijen (gebruikers), systemen en toepassingen dat valt onder het beleid dat is opgesteld door een Policy Authority, en zich aan dat beleid dient te conformeren. Vertrouwen in communiceren is in principe beperkt tot een vertrouwensdomein. Het beleid bepaalt de mate van vertrouwen die gesteld kan worden in de TTP-diensten, de certificaten en de toepassingen binnen het

[4] Opgemerkt kan worden dat de eerste twee componenten, de vertrouwensdomeinen en de communicerende partijen algemene kenmerken zijn van een architectuur voor betrouwbare communicatie; de TTP-diensten bieden een invulling om de betrouwbaarheidseisen te realiseren.

vertrouwensdomein. De Policy Authority stelt met andere woorden een beveiligingsniveau vast voor het domein.

Het is de taak van de PA om aan te geven waarvoor het domein gebruikt wordt en aan welke eisen door alle communicerende partijen en TTP-diensten voldaan moet worden. Het geëigende instrument daarvoor is het Certificate Policy (CP) document [pkix-4]. Daarin wordt aangegeven wie er deel uit kan maken van het domein, welke diensten toegelaten zijn en welke eisen worden gesteld. In het CP kunnen ook zaken als beperking van de aansprakelijkheid en de rechten en plichten van gebruikers worden aangegeven. Er is dus een één op één relatie tussen een beleid en vertrouwensdomein.

Indien men tussen verschillende vertrouwensdomeinen wil communiceren, zal er tussen die domeinen een nieuwe basis voor het vertrouwen moeten worden geïntroduceerd. Het uitspreken van wederzijds vertrouwen kan pas plaatsvinden na toetsing van elkaars beleid en de implementatie van dat beleid.
Dit kan op twee manieren plaatsvinden: de domeinen kunnen onderling (direct) vertrouwen in elkaar uitspreken (cross-certificering) of men kan het vertrouwen via een gezamenlijke hogere vertrouwensfunctie verkrijgen (third party trust). Dit laatste houdt in essentie in dat men een gezamenlijk vertrouwensdomein definieert. De belangrijkste taak van dit domein is het realiseren van vertrouwen tussen alle onderliggende domeinen. Op deze wijze wordt een hiërarchie van vertrouwen gecreëerd. De taken van het hogere domein kunnen beperkt zijn tot het toetsen van de deelnemende subdomeinen. Het is echter ook mogelijk dat het hogere domein een gezamenlijk beleid opstelt, dat door de subdomeinen wordt geïmplementeerd. Een combinatie hiervan is uiteraard ook mogelijk. In elk geval dient het hogere domein toetsingscriteria te hanteren voor toetreding tot het domein[5].

Communicerende partijen

Bij het verzenden en ontvangen van informatie ter ondersteuning van een bedrijfsproces zijn diverse partijen betrokken. Het betreft zowel personen als informatiediensten (intranetservers, databases, www-servers). Vaak gaat het overigens om de formele functie die iemand bekleedt en niet om de persoon zelf. Een persoon zelf kan meerder functies (rollen) bekleden. Identificatie van de formele functie en de persoon zelf is dan belangrijk.

Binnen een vertrouwensdomein wordt een communicerende partij geregistreerd en geïdentificeerd. Deze identificatie is uniek voor dat domein. Indien een communicerende partij binnen een domein is geregistreerd, dient deze zich te conformeren aan het beleid voor dat domein.

Indien twee partijen die elk tot een ander vertrouwensdomein behoren, met elkaar willen communiceren, is er geen basis voor wederzijds vertrouwen. Hiervoor is het noodzakelijk dat er tussen de beide domeinen afspraken worden gemaakt zoals is aangegeven in de vorige paragraaf.

---

[5] Dit is een problematiek die momenteel in nationaal verband onderzocht wordt in het TTP.NL project.

TTP-diensten

Een belangrijk doel van TTP-diensten is het realiseren van vertrouwen in de communicatie tussen partijen. De eisen die aan de TTP-diensten worden gesteld, hangen af van de bedrijfsprocessen waarmee de communicatie samenhangt.

De kernactiviteiten binnen het domein bestaan uit het beheren van sleutels en digitale identiteitsbewijzen. Indien een departement een eigen domein wil opzetten, zal het hiervoor een aantal organisatie-elementen moeten inrichten. De belangrijkste uitvoerende organisatie-elementen zijn de eerder beschreven Certification Authority en Registration Authority. Voor deze organisatie-elementen geldt primair dat zij aan het Certificate Policy waaronder ze werken, moeten voldoen. De wijze waarop ze het Certificate Policy in hun organisatie hebben geïmplementeerd wordt vastgelegd in het Certification Practice Statement (CPS). Dus zowel een Certification Authority als een Registration Authority dienen een eigen CPS te bezitten waarin hun werkwijze is vastgelegd.

De basisdiensten die in een vertrouwensdomein worden geleverd, zorgen dus voor een betrouwbare identificatie van de partijen. Hiertoe worden digitale identiteitsbewijzen uitgegeven. Afhankelijk van de eisen wordt de identificatie binnen een vertrouwensdomein anders geregeld. Mogelijkheden zijn hier:

- het digitale of elektronische paspoort dat de overheid aan alle burgers zou kunnen aanbieden;
- het identiteitsbewijs (bedrijfspas) dat door een organisatie wordt uitgegeven;
- het identiteitsbewijs (domeinpas[6]) dat door een vertrouwensdomein wordt uitgegeven.

Op basis van deze architectuur worden in het hoofdstuk 4 een aantal scenario's opgesteld voor de invoering van TTP-diensten binnen de Rijksoverheid. Alvorens daartoe over te kunnen gaan, is het noodzakelijk om nader in te gaan op het belang van dergelijke diensten voor de Rijksoverheid. Dit belang staat centraal in het volgende hoofdstuk van dit rapport.

2.6 Een wereld van TTP-dienstverleners

De Rijksoverheid wordt in deze studie dus gezien als een (potentiële) gebruiker van TTP-diensten. Alvorens dieper in te gaan op de keuzes die de overheid hierbij dient te maken, is het noodzakelijk even stil te staan bij de huidige stand van zaken en de verwachtingen omtrent de ontwikkelingen in TTP-dienstverlening en -diensten.

Er ontstaat momenteel een wereld van vele TTP-diensten, zowel gesloten als open. Gesloten diensten vinden in we in min of meer gesloten "vertrouwensdomeinen als dealernetwerken, Internet Service Providers (SURFnet), multinationals (Shell), banken en zelfs overheden (Canada, Australie). Daarnaast ontstaan er publieke TTP-diensten die voor elke burger en rechtspersoon toegankelijk zijn. Voorbeelden zijn: PTT post die met Keymail een electronische variant van aangetekende mail; KPN Telecom en Roccade die de diensten

[6] Een voorbeeld zou een creditcard kunnen zijn; het vertrouwensdomein bestaat ondermeer uit de uitgevende instantie, de houders van de card en de acceptanten.

van het Amerikaanse VeriSign in Nederlands wil gaan leveren en Enschede/SdU die TTP-diensten gaat leveren in combinatie met chipcards.
Ook voor deze publieke TTP-diensten zullen er dus verschillende aanbieders zijn.

In lijn met verschillende projecten en beleidsnotities van de overheid wordt op dit moment zoveel mogelijk overgelaten aan het zelfregulerend vermogen van de samenleving. Voorbeelden: het Nationaal Actieplan Electronic Commerce van het ministerie van Economische Zaken, het rapport van de Commissie Cohen, de nota "Wetgeving voor de elektronische snelweg'.

Conclusie ten aanzien van TTP-diensten is dan, dat het niet waarschijnlijk is dat er één nationale openbare TTP-dienst zal ontstaan, en dat het ook niet noodzakelijk is een dergelijke dienst na te streven. Wel is de verwachting dat TTP-dienstenaanbieders en gesloten initiatieven onderling afspraken zullen maken zodat uitwisseling tussen domeinen mogelijk wordt. De term die daarvoor gebruikt wordt is crosscertificering. De essentie van crosscertificering is het wederzijds verkrijgen van vertrouwen in elkaars diensten, procedures en organisatie.

2.7 Samenvatting

TTP-diensten bieden een elegante oplossing voor een aantal onzekerheden die in de elektronische interacties aanwezig zijn: "hoe weet ik met zekerheid met wie ik communiceer?" én "hoe kan ik zorgen dat niemand meeleest én "hoe weet ik dat dit document echt is ". Om deze vragen te kunnen beantwoorden is een betrouwbaar raamwerk voor het bewijzen van de identiteit noodzakelijk: het authenticatieraamwerk. De basis TTP-diensten zorgen voor een digitale identiteit.
Naast deze digitale identiteit bieden TTP-diensten ondermeer mogelijkheden voor het waarborgen van de exclusiviteit en integriteit van gegevens, sleutelbeheer en onweerlegbare bewijsvoering middels digitale handtekeningen.

In de digitale wereld is een dergelijk op TTP-diensten gebaseerd authenticatie-raamwerk opgebouwd uit een aantal componenten. De meest herkenbare componenten zijn:
- Certification Authority (CA): de autoriteit die de identiteitsbewijzen uitgeeft
- Registration Authority (RA): het loket waar gebruikers de identiteitsbewijzen aanvragen
- Policy Authority (PA): het beleidsorgaan dat de regels vaststelt
- Trusted Parties en Trusted Third Parties: organisaties die TTP-diensten leveren.

Er wordt onderscheid gemaakt tussen *basis* TTP-diensten die in het authenticatieraamwerk aanwezig moeten zijn en *toegevoegde* TTP-diensten die optioneel zijn. Voorbeelden van toegevoegde TTP-diensten zijn:
- het onweerlegbaar aantonen van verzending en ontvangst van berichten
- het bewaren en tijdstempelen van berichten en documenten en
- het bewaren van cryptografische sleutels.

TTP-diensten zijn geen doel op zich: de diensten worden gebruikt binnen een groot aantal toepassingen. Bekende voorbeelden daarvan zijn beveiligde e-mail en beveiligde intranet-servers.

Het geheel van TTP-diensten (en toepassingen) biedt aan communicerende partijen de mogelijkheid om binnen een bepaalde afgebakende omgeving in vertrouwen (veilig) te communiceren. Dit leidt tot de drie essentiele componenten binnen de generieke architectuur voor TTP-diensten:

- *Vertrouwensdomeinen* waar binnen partijen met elkaar elektronisch communiceren conform de afspraken omtrent de betrouwbaarheid van de elektronische gegevensuitwisseling.
- *Communicerende partijen* die binnen een vertrouwensdomein geregistreerd en geïdentificeerd worden.
- *TTP-diensten* inclusief technologische voorzieningen (waaronder toepassingen) met als doel het realiseren van vertrouwen in communiceren.

Belangrijk is om te constateren dat een investering in de TTP-basisdiensten niet alleen noodzakelijk is voor de verdere ontwikkeling, maar ook redelijk toekomstvast. Met name deze basisdiensten zouden door de Rijksoverheid in gezamenlijk overleg aangeschaft of ingekocht kunnen worden. In hoofdstuk 4 zal dan ook met name naar de invoering van TTP-basisdiensten gekeken worden.

3. TTP-diensten voor de Rijksoverheid

Nu duidelijk is wat in dit onderzoek wordt verstaan onder TTP-dienten, dient zich de vraag aan waarom een dergelijke dienst voor de Rijksoverheid van belang zou zijn. Deze vraag wordt in dit hoofdstuk beantwoord, en is in de inleiding als deelvraag 2 geformuleerd:

Waarom zijn de TTP-diensten voor de Rijksoverheid belangrijk?

3.1 Waarom zijn TTP-diensten voor de Rijksoverheid belangrijk?

In de inleiding van dit rapport is aangegeven dat ICT een steeds belangrijker rol speelt in de communicatie van de Rijksoverheid. De Rijksoverheid wordt op dit moment geconfronteerd met toenemende behoefte aan elektronisch "zakendoen" met diverse partijen. Daarnaast is zowel binnen departementen als tussen departementen onderling groeiende behoefte aan elektronische berichtenuitwisseling waarneembaar. Enkele voorbeelden die tijdens een brainstormsessie met de begeleidingsgroep zijn genoemd:

- intradepartementale communicatie ten behoeve van salarismutaties;
- intradepartementale communicatie ten behoeve van het verzamelen van financiële gegevens ten behoeve van belastingcontrole;
- interdepartementale communicatie voor asielaanvragen;
- interdepartementale uitwisseling van kamerstukken;
- interdepartementale communicatie ten behoeve van crisismanagement;
- interdepartementale communicatie ten behoeve van beleidvoorbereiding.

Het is daarbij ook belangrijk te beseffen dat communicatie binnen de Rijksoverheid, of zelfs binnen één departement, alleen de eindpunten van de communicatie aangeeft. Twee ambtenaren van V&W kunnen heel goed 'intern' communiceren over het Internet! Denk verder ook aan toepassingen als telewerken waarbij publieke netwerken worden gebruikt. Betrouwbare identificatie van de communicerende partijen en vertrouwelijkheid spelen hier zeker een rol.
Tenslotte is geconstateerd dat er binnen de Rijksoverheid reeds een aantal TTP-diensten geïmplementeerd is voor het beveiligen van de bedrijfsprocessen. Binnen het Ministerie van Financiën loopt een viertal projecten waarbij TTP-diensten ingezet worden voor het beveiligen van de bedrijfsprocessen[7].

[7] Het betreft hier evenwel processen waarbij er sprake is van gegevensuitwisseling tussen de Rijksoverheid en burgers/bedrijfsleven. We komen hier in het grijze gebied tussen de openbare en de niet-openbare TTP-diensten van paragraaf Afbakening: TTP-diensten en de Rijksoverheid. O.i. kan een niet-openbare (Rijksoverheid) TTP-dientst deze toepassingen ondersteunen. De grens met openbare TTP-diensten wordt pas overschreden, indien de diensten gebruikt worden voor toepassingen tussen burgers/bedrijven onderling.

TTP-toepassingen ten behoeve van burgers en bedrijven
Zoals in de introductie is gesteld, richt deze studie zich op de interne overheidscommunicatie. Processen binnen de overheid beginnen of eindigen echter veelal bij burgers of bedrijven. Het inrichten van TTP-diensten binnen de Rijksoverheid biedt goede mogelijkheden om de betrouwbaarheid van deze processen te verbeteren. Niet alleen kan de overheid die zelf TTP-diensten gebruikt beter inspelen op externe gebruikers van TTP-diensten (bijvoorbeeld bij elektronische offertetrajecten of financiële transacties). De overheid zou bijvoorbeeld elektronische offertes die digitaal zijn ondertekend dezelfde status kunnen geven als de 'normale' papieren versie. De authenticiteit en integriteit van de ontvangen elektronische offerte is immers gewaarborgd[8].
Maar de overheid kan ook haar diensten voor burgers en bedrijven met behulp van de eigen TTP-diensten (al dan niet uitbesteed) beveiligen. Een goed voorbeeld daarvan is de elektronische belastingaangifte. Samen met het elektronische aangifteformulier kan een persoonlijk certificaat voor de aanvrager worden meegeleverd. Met dezelfde technieken die intern worden toegepast, kan de burger dan haar aangifte digitaal ondertekenen en tijdens transport vercijferen.
Een stap verder is de introductie van digitale identiteitsbewijzen en reisdocumenten. Onafhankelijk van de vraag wie deze zal uitgeven is het cruciaal dat de gebruikte technieken algemeen gebruikt worden. Digitale certificaten en de digitale handtekening gebaseerd op TTP-diensten zijn hiervoor dé kandidaat waarop niet alleen overheden zich richten, maar ook de financiële wereld en het bedrijfsleven (zie de discussie bij de nul optie hierna).

Als mogelijke toepassingsgebieden van TTP-diensten *binnen* de Rijksoverheid kunnen we een aantal groepen onderscheiden die hieronder beschreven worden. Om e.e.a. handen en voeten te geven zullen we een casus introduceren: 'interdepartementale communicatie binnen een werkgroep ten behoeve van beleidsvoorbereiding', afgekort 'beleidsvoorbereiding'.

Beleidsvoorbereiding: introductie

Bij de uitwisseling van notities, commentaar en andere stukken tijdens de is de vertrouwelijkheid (exclusiviteit) van groot belang. De informatie mag alleen bekend worden gemaakt aan de leden van de werkgroep. Voortijdig uitlekken van informatie kan het proces schaden en de verantwoordelijke ministers schade toebrengen.
Een ander probleem bij elektronische documenten is de status. Stel dat een document met langs elektronische weg, bijvoorbeeld per e-mail, wordt verstuurt. Dit document wordt vervolgens opgeslagen en mogelijk veel later, als de ambtenaar het document ophaalt, rijzen de volgende vragen:
- Is dit het officiële document?
- Heeft niet iemand achteraf wijzigingen aangebracht in het document?
- Moet ik dus wel handelen volgens dit document?

Aangezien de vertrouwelijkheid bij e-mail niet gegarandeerd is en men geen sluitende antwoorden op deze vragen krijgt, neemt men de toevlucht tot een gedrukte versie die in een gesloten enveloppe wordt verzonden. We zullen in het verloop van de casus zien hoe

[8] Na effectuering van de Europese richtlijn voor de digitale handtekening verkrijgt de digitale handtekening in veruit de meeste gevallen de zelfde status als de handmatige handtekening.

TTP-diensten en toepassingen deze situatie ten goede kunnen keren.

Bewijs van elektronische echtheid.

Middels de Digitale Handtekening kan worden aangetoond dat een document of bericht 'authentiek' is. Er ontstaat zekerheid over de auteur het feit dat het om een overheidsdocument gaat. De ontvanger kan dus met en gerust hart handelen naar de ontvangen informatie. Dit vormt bijvoorbeeld de basis voor een elektronisch "parafencircuit" dat het traditionele papieren circuit vervangt. Het legt ook de basis voor het langs elektronische weg kunnen verrichten van formele handelingen zoals het afsluiten van overeenkomsten en contracten.

Het officiële document: authenticiteit

Het bewijs van elektronische echtheid geeft de mogelijkheid om de situatie te verbeteren. Nadat de ambtenaar een document heeft opgesteld, ondertekent hij het met zijn digitale handtekening. Hiermee verzegeld hij als het ware het document. Hij verstuurt nu het ondertekende document. Alle leden van de werkgroep kunnen vervolgens controleren dat het document van hem afkomstig is. Ook na langere tijd. Tevens kunnen ze controleren dat het document na ondertekening niet is gewijzigd. Zou dat wel het geval zijn, dan is de handtekening niet meer geldig.

- De leden van de werkgroep weten dus dat dit het officiële document van een collega is.
- Dat niemand achteraf wijzigingen aangebracht kan hebben in het document.
- En kunnen dus gerust handelen volgens dit document!
- Tevens kan de uitwisseling (via bv. E-mail) exclusiviteit worden gegarandeerd door vercijfering (zie ook telewerken)

Wat is hier nu voor nodig? De ambtenaren hebben een sleutelpaar en de toepassing nodig om de handtekening te kunnen zetten. Ze moeten verder de beschikking hebben over het publieke sleutel certificaten van de andere leden van de werkgroep en de toepassing om de handtekening te kunnen controleren.

Bewijs van de identiteit

Personen kunnen zich langs elektronische weg op betrouwbare wijze identificeren met hun certificaten. Toegangsbeveiliging tot informatiediensten (intranet), lokale netwerken en databases kan hiermee doeltreffend worden ingericht. Daarbij hoeven gebruikers zich niet vooraf aan te melden voor een bepaalde dienst en telkens weer wachtwoorden te kiezen. Men kan toegang verlenen middels het voor iedereen binnen de organisatie beschikbare certificaat. Wil men de toegang beperken tot groepen, dan kan men kenmerken die in de certificaten zijn opgenomen gebruiken om in één stap ieder lid van de groep toegang te verlenen: bijvoorbeeld op grond van afdeling of zelf het feit dat men voor de overheid werkt.

Op een zelfde wijze kan men de overheidssystemen beveiligen tegen buitenstaanders (intra-, extranet). Door alleen toegang te verlenen aan bezitters van een door de overheids-TTP uitgegeven certificaat, sluit men buitenstaanders uit.

Het officiële document: intranet server
De secretaris van d werkgroep vindt het versturen van alles stukken naar alle leden van de werkgroep inefficiënt. Waarom zouden we de stukken niet via een documentenserver, die is opgenomen in het intranet, beschikbaar stellen? Op deze manier kan lid de meest actuele (en oude) informatie ook altijd eenvoudig vinden. Uiteraard is het document nog steeds digitaal ondertekend door de secretaris (of ander lid van de werkgroep).
Voorkomen moet worden dat ongeautoriseerden toegang krijgen tot de stukken. Dit lost men op door de toegang te beperken tot leden van de werkgroep die een geldig certificaat hebben dat is uitgegeven door de overheids-TTP.

Indien men toegang zoekt tot de server, controleert deze of de aanvrager een geldig certificaat heeft. Slechts indien dit het geval is, kan het document worden gedownload. De toegang kan zelfs verder worden beperkt tot individuele ambtenaren die lid zijn van de werkgroep door hun certificaat expliciet op te nemen in een autorisatielijst.

Wat is hier nu extra voor nodig? De documentenserver moet de beschikking hebben over het certificaat van de overheids-TTP om de certificaten van de gebruikers te kunnen controleren. Hierbij gebruikt de server het SSL protocol.

Uitwisselen van vertrouwelijke gegevens via openbare, onbetrouwbare kanalen.
Certificaten en TTP-diensten maken het mogelijk om de exclusiviteit van informatie tijdens opslag én transport te waarborgen. Vertrouwelijke notities kunnen tussen ambtenaren worden uitgewisseld zonder dat ze zich behoeven te bekommeren over ongewenste inzage tijdens het transport indien gebruik wordt gemaakt van beveiligde e-mail. Informatie die van beveiligde webservers wordt opgevraagd, is onleesbaar tijdens het transport. Dit biedt, samen met het hierboven beschreven identificatie, ambtenaren de mogelijkheid om informatie op veilig wijze op te halen of ze nu op kantoor zijn of thuis via het Internet. Het is dus mogelijk om een extranet te creëren. Hiermee komt veilig telewerken een stap dichterbij. Aangezien via openbare kanalen betrouwbaar kan worden gecommuniceerd, is een kostenbesparing mogelijk ten opzicht van de veelal duurdere gesloten kanalen[9].

Het officiële document: telewerken
De leden van de werkgroep zijn verspreid over het land. Ook neemt telewerken onder de ambtenaren sterk toe. Men wil daarom de documentenserver via het Internet beschikbaar stellen. De informatie mag echter niet door iedereen worden gelezen.
De toegang tot de server wordt op de hierboven beschreven wijze afgeschermd. De vertrouwelijkheid van de informatie tijdens het transport over het Internet is echter nog een probleem.

De beveiligde documentenserver kan echter eenvoudig zo worden ingesteld dat de informatie die wordt opgehaald, wordt vercijferd tijdens het transport. Dit is een optie binnen het SSL protocol. Na toegangscontrole aan de hand van het certificaat van de ambtenaar wordt er een vercijferde verbinding opgezet zodat alleen die ambtenaar de

[9] Bijvoorbeeld een gesloten netwerk van huurlijnen eventueel aangevuld met lijnvercijfering.

informatie kan lezen. Op deze wijze kunnen de leden van de werkgroep onafhankelijk van plaats en tijd documenten op een betrouwbare wijze van de server halen en er op plaatsen.

Wat is hier nu extra voor nodig? De server moet de beschikking hebben over een eigen certificaat om de gegevens te kunnen vercijferen.

Samengevat kan gesteld worden dat de sterkte van het gebruik van TTP-diensten als basis van de betrouwbaarheid voor al deze toepassingen ligt in de uniformiteit. Een beperkt aantal TTP-diensten legt de basis voor het vertrouwen in de herkomst van berichten, de identificatie van personen ten behoeve van toegangsbeveiliging en het waarborgen van de integriteit en exclusiviteit van informatie.

We kunnen ons dan ook afvragen welke situatie er ontstaat indien men binnen de Rijksoverheid afziet van het inrichten van TTP-diensten: de nul-optie.

3.2 De nul-optie

We behandelen hier de mogelijke gevolgen voor de Rijksoverheid indien deze afziet van het gebruik van TTP-diensten. Daarbij beschouwen we de invloed van externe factoren als het productbeleid van leveranciers en de strategie van andere marktpartijen. Ook wordt bekeken wat de gevolgen kunnen zijn voor de interne informatievoorziening.

Productbeleid leveranciers
Eigenlijk is de eerste vraag of het überhaupt mogelijk is om af te zien van het gebruik van TTP-diensten. Zoals we eerder beschreven hebben, zijn er nationaal en internationaal zeer veel initiatieven die verband houden met TTP-diensten en toepassingen daarvan. Tekenend daarvoor is het gegeven dat vele ICT producten en toepassingen die nu reeds binnen de overheid gebruikt worden, door de leverancier voorbereid zijn om gebruik te maken van TTP-diensten. Grote organisaties als Microsoft, IBM en Netscape hebben zich op strategisch niveau gecommitteerd aan het gebruik van TTP-diensten. Zij zien TTP-diensten als de mogelijkheid om elektronische handel en communicatie betrouwbaar te maken. Zijn de producten nu nog voorbereid, een volgende generatie zou zeer goed minder functionaliteit bieden indien er geen gebruik wordt gemaakt van TTP-diensten. Een aantal beveiligingsproducten vereist nu reeds een certificaat. Bij installatie wordt een (waardeloos) test-certificaat geïnstalleerd en vervolgens aangegeven dat een echt certificaat bij een TTP moet worden opgehaald. Er is dus duidelijk spraken van een push vanuit de aanbieders van ICT-producten.

Marktontwikkelingen
Ook grote bedrijven en marktsectoren richten zich in hun strategie op het gebruik van TTP-diensten. De betrokkenheid van grote Nederlandse ondernemingen bij het opzetten van TTP-diensten onderstreept dit. Voorbeelden zijn: PTT post die met Keymail een electronische variant van aangetekende mail; KPN Telecom en Roccade die de diensten van het Amerikaanse VeriSign in Nederlands wil gaan leveren en Enschede/SdU die TTP-diensten gaat leveren in combinatie met chipcards.
Aan de gebruikerskant gaan multinationals als Shell en Philips zeer waarschijnlijk TTP-diensten gebruiken voor interne en externe communicatie. Zeer belangrijk is verder de

keuze van de banken en credit-card maatschappijen om gebruik te maken van de Secure Electronic Transactions (SET) als standaard voor het elektronische betalingsverkeer. Deze standaard is volledig gebaseerd op het gebruik van digitale certificaten en TTP-diensten. Interpay speelt hierop in met het opzetten van eigen TTP-diensten voor bancair verkeer.
Daarnaast zijn Rijksoverheden in verschillende landen bezig met het opzetten van TTP-diensten voor eigen gebruik. Prominent voorbeeld daarvan is de Canadese overheid. Maar ook in Amerika, Zuid-Afrika en Australië zijn er initiatieven. Ook de EC past TTP-diensten toe, zij het voornamelijk in haar communicatie met het bedrijfsleven.
Dit betekent dat de Rijksoverheid op verschillende gebieden zal worden geconfronteerd met partijen die zullen aandringen op beveiligde communicatie op basis van TTP-diensten. Indien de overheid hier niet op inspeelt, kan dit gezien worden als een 'veroudering' van de overheidscommunicatie. Een stempel dat pijnlijk kan zijn gezien de doelstellingen van de Rijksoverheid op het gebied van ICT en de elektronische overheid.
Vanuit de maatschappelijke rol bestaat dus ook een zekere push om TTP-diensten toe te passen binnen de Rijksoverheid.

Indien de overheid zich niet vroegtijdig voorbereid op deze ontwikkelingen, is de kans dus groot dat zij erdoor overvallen wordt. De overheid zal zich ten minste op strategisch niveau moeten buigen over de manier waarop men met TTP-diensten voor intern gebruik en voor externe communicatie wil omgaan.

Interne organisatie
Zoals gezegd ligt de sterkte van het gebruik van TTP-diensten in de uniformiteit. Meerdere betrouwbaarheidsdiensten (authenticiteit, integriteit, digitale handtekening, vercijfering) worden geleverd en verscheidene toepassingen (e-mail, www-servers, mailservers, newsservers) maken er gebruik van. Het gebruik van TTP-diensten wekt dus uniformiteit in de aanpak in de hand. En daarmee ook de uitwisselbaarheid (interoperabiliteit) tussen diensten en gebruikers.
Neemt men geen gecoördineerde actie, dan zal een situatie ontstaan die vergelijkbaar is met 'eiland-automatisering': iedereen kiest eigen beveiligingsoplossingen die onderling niet samen kunnen werken. Dit zal de effectiviteit van de informatievoorziening binnen de overheid als geheel ernstig kunnen belemmeren. Extra kosten zullen gemaakt moeten worden om de eilanden met elkaar te verbinden. De (nood)oplossingen die daarbij toegepast worden, kunnen makkelijk afbreuk doen aan het betrouwbaarheidsniveau.

Zou men TTP-diensten en certificaten optimaal gebruiken, dan heeft de medewerker slechts één wachtwoord nodig voor alle toepassingen: om het certificaat te activeren. Hij kan daarna transparant gebruik maken van het certificaat voor bijvoorbeeld beveiligde e-mail of het surfen naar beveiligde intranet servers. Om autorisatie te verlenen voor een informatiedienst, zoekt de beheerder de betreffende medewerker op in het adressenboek en kopieert het gevonden certificaat naar de autoristatielijst van de informatiedienst. Indien een medewerker vertrekt, wordt zijn certificaat ingetrokken waardoor zijn autorisaties op alle informatiesystemen vervallen.

Het nu structureel aanpakken van maatregelen ter bevordering van de betrouwbaarheid voorkomt dus problemen in de toekomst. Ofschoon met het inrichten van TTP-diensten en toepassingen de nodige inspanningen gemoeid zijn, bieden deze een goede basis hiervoor.

3.3 Zijn we er met TTP-diensten alleen?

De basis van TTP-diensten ligt in de Internetwereld, met name in de wens om toch betrouwbaar te kunnen communiceren over dit 'onbetrouwbare' medium. Aangezien niemand het Internet bezit, kan men weinig of geen vertrouwen stellen in de verbindingen. Daarom is het vertrouwen bij de eind-entiteiten gelegd. Dit kunnen personen zijn, maar ook computersystemen of informatiediensten. Men spreekt dan van end-to-end beveiliging.
Niet alleen bij het Internet, maar ook bij een op te zetten overheidintranet is het maar de vraag wie de betrouwbaarheid zal kunnen garanderen. Een 'lek' op één plaats kan grote gevolgen hebben voor het gehele intranet.

Om betrouwbare end-to-end beveiliging te bieden, dienen de entiteiten te beschikken over betrouwbare identiteitsbewijzen voor de identificatie, betrouwbare cryptografische sleutels voor vertrouwelijke communicatie en betrouwbare toepassingen om de voorgaande te kunnen gebruiken. Dit zijn precies de kenmerken van een vertrouwensdomein.

Een interessante vraag is nu of we hiermee daadwerkelijk betrouwbaarheid kunnen garanderen. In het Voorschrift Informatiebeveiliging Rijksdienst (VIR) wordt de volgende definitie van betrouwbaarheid gegeven:

Betrouwbaarheid is de mate waarin een organisatie zich kan verlaten op het informatiesysteem voor zijn informatievoorziening.

Vervolgens worden de volgende eigenschappen van betrouwbaarheid gehanteerd:
- *Beschikbaarheid*, de mate waarin een informatiesysteem beschikbaar is op het moment dat de organisatie het nodig heeft.
- **Integriteit**, de mate waarin systeemcomponenten en de daarin opgenomen gegevens, zonder fouten zijn.
- **Exclusiviteit**, de mate waarin de toegang tot informatiesystemen (met name de informatie) beperkt is tot een gedefinieerde groep van gemachtigden.

End-to-end diensten richten zich uiteraard voornamelijk op de informatie aangezien grote delen van de tussenliggende infrastructuren buiten de eindomgeving vallen. Deze eenvoudige constatering leidt er toe dat we aan een aantal kenmerken van betrouwbaarheid niet zonder meer kunnen voldoen.
De exclusiviteit en de integriteit van informatie kan goed worden beschermd. Ten aanzien van het garanderen van de beschikbaarheid, biedt end-to-end beveiliging slechts beperkte middelen. End-to-end beveiliging biedt hier de mogelijkheid om, door goede toegangsbeveiliging op grond van de identiteitsbewijzen, er voor zorgen dat ongeautoriseerde buitenstaanders de diensten niet kunnen blokkeren.

3.4 Conclusies

Als mogelijke toepassingsgebieden van TTP-diensten binnen de Rijksoverheid hebben we een aantal groepen onderscheiden:

Bewijs van elektronische echtheid.
Middels de Digitale Handtekening kan worden aangetoond dat een document of bericht 'authentiek' is. Er ontstaat zekerheid over de auteur het feit dat het om een overheidsdocument gaat.
Bewijs van de identiteit
Personen kunnen zich langs elektronische weg op betrouwbare wijze identificeren met hun certificaten. Toegangsbeveiliging tot informatiediensten (intranet), lokale netwerken en databases kan hiermee doeltreffend worden ingericht.
Uitwisselen van vertrouwelijke gegevens via openbare, onbetrouwbare kanalen.
Certificaten en TTP-diensten maken het mogelijk om de exclusiviteit van informatie tijdens opslag én transport te waarborgen.
Hiermee komt veilig telewerken een stap dichterbij. Aangezien via openbare kanalen betrouwbaar kan worden gecommuniceerd, is een kostenbesparing mogelijk ten opzicht van de veelal duurdere gesloten kanalen
TTP-toepassingen ten behoeve van burgers en bedrijven
De overheid kan ook haar diensten voor burgers en bedrijven met behulp van de eigen TTP-diensten beveiligen. Een goed voorbeeld daarvan is de elektronische belastingaangifte.

Indien de Rijksoverheid geen strategische keuze maakt ten aanzien een raamwerk voor betrouwbare commiunicatie, constateren we een aantal probleemgebieden:

- *Push van leveranciers*: er is duidelijk spraken van een push vanuit de aanbieders van ICT-producten om TTP-diensten te gebruiken voor betrouwbare communicatie en informatiediensten
- *Push van gebruikers:* ook grote bedrijven, marktsectoren en buitenlandse overheden richten zich in hun strategie op het gebruik van TTP-diensten. Dit betekent dat de Rijksoverheid op verschillende gebieden zal worden geconfronteerd met partijen die zullen aandringen op beveiligde communicatie op basis van TTP-diensten.
- *Interne organisatie*: Neemt de Rijksoverheid geen gecoördineerde actie, dan zal een situatie ontstaan die vergelijkbaar is met 'eiland-automatisering': iedereen kiest eigen beveiligingsoplossingen die onderling niet samen kunnen werken. Dit zal de effectiviteit van de informatievoorziening binnen de overheid als geheel ernstig kunnen belemmeren. Extra kosten zullen gemaakt moeten worden om de eilanden met elkaar te verbinden. De (nood)oplossingen die daarbij toegepast worden, kunnen makkelijk afbreuk doen aan het betrouwbaarheidsniveau.

Indien de overheid zich dus niet vroegtijdig voorbereid op deze ontwikkelingen, is de kans dus groot dat zij erdoor overvallen wordt. De overheid zal zich ten minste op strategisch niveau moeten buigen over de manier waarop men met TTP-diensten voor intern gebruik en voor externe communicatie wil omgaan.

Ten slotte wordt geconstateerd dat TTP-diensten niet voor alle problemen een oplossing bieden. Met name ten aanzien van het garanderen van de beschikbaarheid en integriteit van netwerkdiensten en computersystemen bieden TTP-diensten slechts beperkte middelen. Daarentegen kan de exclusiviteit en de integriteit van informatie en diensten goed worden beschermd.

4. Scenario's voor de invoering

In dit hoofdstuk staat een viertal scenario's beschreven, gevolgd door de voor- en nadelen van elk van deze scenario's. Met deze scenario's wordt een antwoord gegeven op de derde deelvraag:

Welke scenario's zijn er bij de inrichting van TTP-diensten binnen de Rijksoverheid?

4.1 Inleiding

De vier scenario's zijn gebaseerd op de generieke architectuur die in hoofdstuk 2 is gepresenteerd. Deze scenario's zijn:), de decentraal gestuurde optie (1e scenario), de centraal gestuurde optie (4e scenario en een tweetal 'gemengde' opties (2e en 3e scenario).

Deze scenario's richten zich op de bestuurlijke aspecten van de invoering van TTP-diensten binnen de Rijksoverheid. Het onderwerp uitbesteding ten aanzien van de invoering en de instandhouding van een TTP-dient staat los van de scenario's en wordt in het hoofdstuk 6 behandeld.

Per scenario wordt eerst het algemene beeld geschetst. Vervolgens worden de gevolgen voor een zevental kernpunten beschreven Dit zijn:

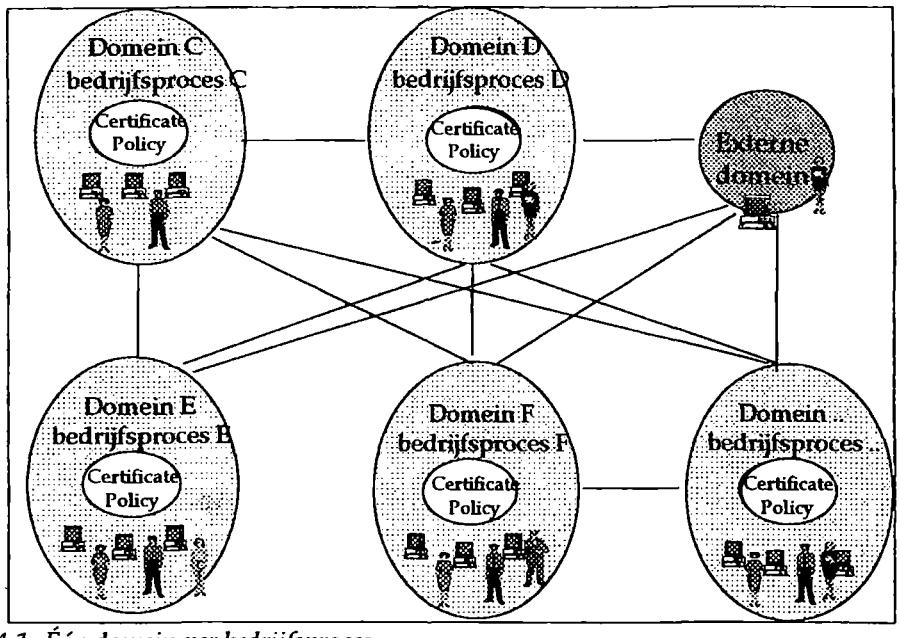
1. Verantwoordelijkheden: wie is eindveranwoordelijke voor de TTP-diensten.
2. Basis TTP-diensten: de inrichting van de noodzakelijke componenten binnen een vertrouwensdomein (Policy Authority, Certification Authority, Registration Authority, Distribution Service, Key Manager).
3. Toegevoegde TTP-diensten: de inrichting van de optionele diensten binnen een vertrouwensdomein.
4. Toepassingen: de toepassingen die gebruik maken van de TTP-diensten.
5. Communicatie binnen de Rijksoverheid: de mogelijkheid om Rijksoverheidbreed in vertrouwen te communiceren.
6. Communicatie met externe domeinen: de mogelijkheid om met externe domeinen in vertrouwen te communiceren.
7. Kosten: de absolute kosten voor implementatie en instandhouding zijn sterk afhankelijk van het beveiligingsniveau. De beschrijving zal dan ook voornamelijk gericht zijn op een kwalitatieve vergelijking tussen de scenario's. Daarbij staat de vraag centraal of kostendeling door gezamenlijke aanschaf mogelijk is. Belangrijke verschillen ontstaan ten aanzien van het noodzakelijke aantal centrale componenten (Certification Authority, Distribution Service, Key Manager en de verdeling van de Registration Authority (het 'loket'). Voor de decentrale componenten - met name de toepassingen - zijn mogelijke volumevoordelen van belang. In bijlage 2 is uiteengezet hoe welke basis is aangehouden voor de kostenbepaling per scenario.

Tot slot worden per scenario de voor en nadelen gegeven.

4.2 Scenario 1: Één domein per bedrijfsproces

Voor elk bedrijfsproces binnen de Rijksoverheid wordt één domein ingericht en wordt het Certificate Policy opgesteld. Daarin wordt bepaald waarvoor het domein gebruikt wordt en aan welke eisen door alle communicerende partijen en TTP-diensten moet worden voldaan. Tevens wordt een organisatorische functie ingericht die zaken als uitgave en intrekken van de persoonlijke digitale identiteitsbewijzen, het cross-certificeren met externe domeinen, beleidsontwikkeling, audit en aansprakelijkheid regelt. Ook de acceptatieprocedure voor applicaties wordt per bedrijfsproces uitgevoerd.

Binnen de Rijksoverheid wordt geen interdepartementaal domein ingericht waarmee het onderlinge vertrouwen tussen de aangesloten departementen wordt gerealiseerd. Indien binnen een bedrijfsproces communicerende partijen met een andere bedrijfsproces willen communiceren, zal het uitspreken van wederzijds vertrouwen pas plaatsvinden na toetsing van elkaars beleid en de implementatie van dat beleid. De volgende figuur illustreert het 1e cenario:



Figuur 4.1. Één domein per bedrijfsproces

In de volgende tabel worden de gevolgen voor de kernpunten beschreven:

Kernpunten	*Omschrijving*
Verantwoordelijkheden	De verantwoordelijkheid voor een bedrijfsproces-domein ligt bij de verantwoordelijke van het bedrijfsproces. Dit leidt uiteindelijk tot een eindverantwoordelijkheid die bij het departement ligt.
Basis TTP-diensten	Deze worden per bedrijfsproces volgens het eigen Certificate Policy ingericht. In een gezamenlijke inrichting hiervan is niet voorzien.
Toegevoegde	Per bedrijfsproces bestaat vrije keuze om deze in te richten wanneer

Kernpunten	*Omschrijving*
TTP-diensten	daartoe de behoefte ontstaat
Toepassingen	Keuze en acceptatie van toepassingen dient per bedrijfsproces te worden uitgevoerd. Specifieke toepassingen kunnen per departement worden gekozen.
Communicatie binnen de Rijksoverheid	Dit dient expliciet te worden geregeld in bilaterale cross-certificatie afspraken tussen de bedrijfsprocessen. Zelfs binnen een departement dienen dus expliciete afspraken te worden gemaakt.
Communicatie met externe domeinen	Dit dient expliciet te worden geregeld in bilaterale cross-certificatie afspraken tussen de bedrijfsprocessen en externe domeinen.
Kosten	De componenten worden per bedrijfsproces aangeschaft en de infrastructuur kan slechts zeer beperkt worden gedeeld. Volumevoordeel voor de decentrale componenten is dus erg beperkt. Voor elk bedrijfsproces dient men een CA in te richten. De RA's moeten per bedrijfsproces ingericht worden.

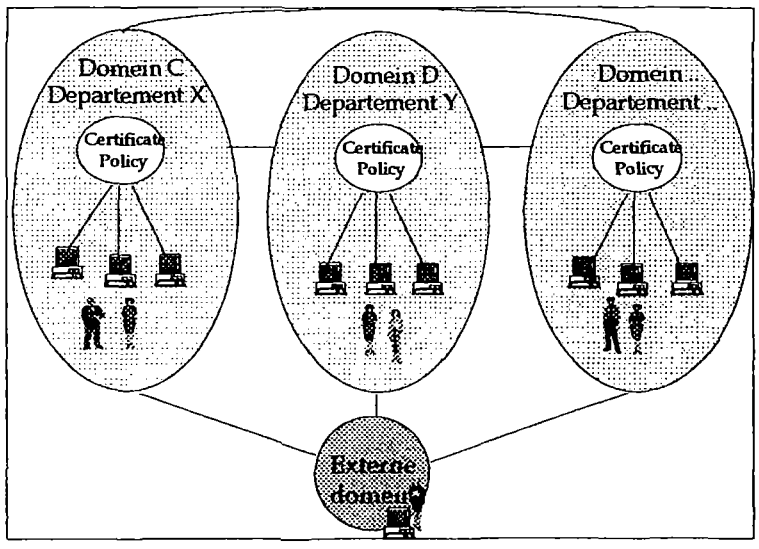
Voordelen:
- Per bedrijfsproces baseline voor vertrouwen.
- Zeer goed mogelijk om specifieke wensen van bedrijfsprocessen in te vullen.

Nadelen
- Duurste optie: per bedrijfsproces +/- 500.000 aanschaf, 10% exploitatiekosten.
- Minst efficiënte optie. Alles wordt individueel (decentraal binnen bedrijfsonderdeeldelen van een departement per bedrijfsproces) geregeld. Voor elk bedrijfsproces moet een eigen domein worden opzet.
- Aansprakelijkheid moet per bedrijfsproces worden geregeld.
- De organisatie (inclusief personeel) kan moeilijk omgaan met complexe beveiligingsniveaus. Meerdere niveaus zijn ook technisch nog niet goed te realiseren met name in de applicaties ontbreekt het aan voldoende ondersteuning hiervan.
- Geen RO- of departementbrede baseline voor vertrouwen. Het vertrouwen in de interdepartementale communicatie en met externe domeinen wordt zeer mogelijk (bijna onmogelijk) te verwezenlijken. Bilaterale cross-certificeringsafspraken tussen de bedrijfsprocessen en met externe domeinen zijn zeer complex en noodzakelijk.

4.3 Scenario 2: Departementale domeinen

Door elk departement wordt één departementaal domein ingericht. Daardoor ontstaat een departementbrede baseline voor vertrouwen. Elke departement stelt een Certificate Policy op. Daarin wordt bepaald waarvoor het departementale domein gebruikt wordt en aan welke eisen door alle communicerende partijen en TTP-diensten moet worden voldaan. Tevens wordt binnen een departement een organisatorische functie ingericht die zaken als uitgave en intrekken van de persoonlijke digitale identiteitsbewijzen, het cross-certificeren met externe domeinen, beleidsontwikkeling, audit en aansprakelijkheid regelt. Ook de acceptatieprocedure voor applicaties wordt door departementen zelf uitgevoerd. Daardoor ontstaat een departementbrede baseline voor vertrouwen.

Binnen de Rijksoverheid wordt geen interdepartementaal domein ingericht waarmee het onderlinge vertrouwen tussen de aangesloten departementen wordt gerealiseerd. De departementen regelen dit zelf. Indien een departement met een ander departement wil communiceren, zal het uitspreken van wederzijds vertrouwen pas plaatsvinden na toetsing van elkaars beleid en de implementatie van dat beleid. De volgende figuur illustreert het 2e cenario:



Figuur 4.2. Scenario 2: Departementale domeinen

In de volgende tabel worden de gevolgen voor de kernpunten beschreven:

Kernpunten	*Omschrijving*
Verantwoordelijkheden	De verantwoordelijkheid ligt bij de individuele departementen.
Basis TTP-diensten	Deze worden per departement volgens het eigen Certificate Policy ingericht. In een gezamenlijke inrichting hiervan is niet voorzien. Indien de verschillen in het beleid per departementaal domein groot zijn, is gezamenlijke inrichting ook niet mogelijk.
Toegevoegde TTP-diensten	Departementen hebben vrije keus om deze in te richten wanneer daartoe de behoefte ontstaat
Toepassingen	Keuze en acceptatie van toepassingen dient per departement te worden uitgevoerd. Specifieke toepassingen kunnen per departement worden gekozen.
Communicatie binnen de Rijksoverheid	Dit dient expliciet te worden geregeld in bilaterale cross-certificatie afspraken tussen de departementale domeinen. Indien de verschillen in het beleid per departementaal domein groot zijn, is cross-certificering niet mogelijk.
Communicatie met externe domeinen	Dit dient expliciet te worden geregeld in bilaterale cross-certificatie afspraken tussen de departementale domeinen en externe domeinen.
Kosten	De componenten worden per departement aangeschaft en de infrastructuur

Kernpunten	*Omschrijving*
	kan slechts zeer beperkt worden gedeeld. Volumevoordeel voor de decentrale componenten is dus beperkt tot de omvang van de departementen. Elk departement dient een CA in te richten. De RA's kunnen optimaal ingericht worden binnen de departementen.

Voordelen:

- Een departement-brede baseline voor vertrouwen.
- Mogelijk om specifieke wensen van departementen te vullen.
- Elk department kan zelf bepalen wanneer men overgaat tot de implementatie binnen het departement.

Nadelen:

- Veel duurder dan 3e en 4e scenario:

13 x departementaal domein (+/- 500.000 aanschaf, 10% exploitatiekosten);

- Minder doeltreffende optie. Eén beleid voor de interdepartementale communicatie is niet mogelijk. Dit wordt niet centraal aangestuurd. Aangesloten departementen moeten alles individueel regelen.
- Geen RO-brede baseline voor vertrouwen .
- De organisatie (inclusief personeel) kan moeilijk omgaan met meerdere (departementale) beveiligingsniveau. . Meerdere niveaus zijn technisch ook nog niet goed te realiseren. Met name in de applicaties ontbreekt het aan voldoende ondersteuning hiervan.
- Aansprakelijkheid wordt decentraal geregeld.

Beperkte bedrijfsprocesbrede baseline voor vertrouwen. Het vertrouwen in de interdepartementale communicatie en met externe domeinen is zeer moeilijk te verwezenlijken. Bilaterale cross-certificeringsafspraken tussen de individuele departementen en met externe domeinen zijn noodzakelijk

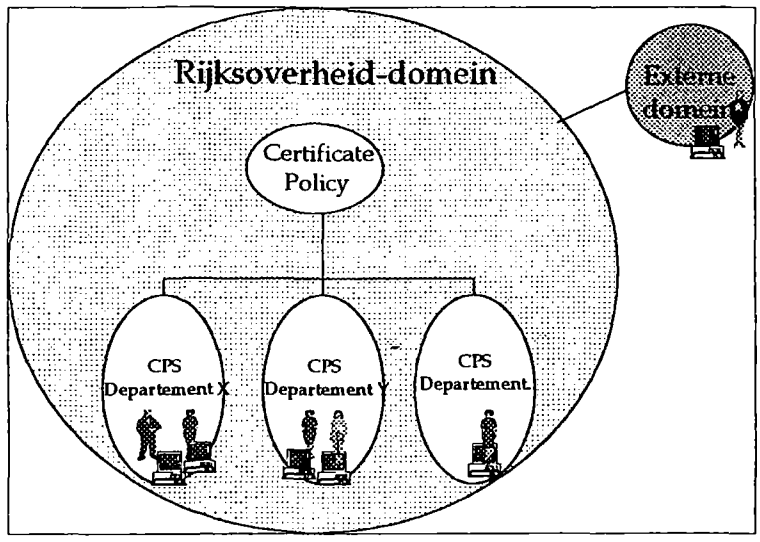
4.4 Scenario 3: Het interdepartementale domein

Binnen de Rijksoverheid wordt een interdepartementaal domein ingericht waarmee het onderlinge vertrouwen tussen de aangesloten departementen wordt gerealiseerd. Daardoor wordt een RO-brede baseline voor vertrouwen met daarop beperkte variatie per departement gecreëerd.

Op interdepartementaal niveau worden door een centrale Policy Authority de richtlijnen opgesteld waaraan de CP's moeten voldoen. Daarin wordt bepaald waarvoor het interdepartementale domein gebruikt wordt en aan welke minimale eisen door alle communicerende partijen en TTP-diensten moet worden voldaan. Tevens wordt een centrale organisatorische functie ingericht die zaken als het cross-certificeren met externe domeinen, beleidsontwikkeling, audit en aansprakelijkheid centraal regelt. Ook de acceptatieprocedure voor applicaties kan centraal worden uitgevoerd. Ook kan de centrale organisatie een baseline Certificate Policy opstellen die door departementale domeinen kan worden overgenomen.

Voor de communicatie tussen de departementale domeinen wordt centraal een Certification Authority ingericht die de deelnemende departementale CA's certificeert. Op deze wijze creëert men een hiërarchie van vertrouwen binnen de Rijksoverheid.

Elk departement kan zich (ook later) aansluiten bij het domein. Deelname aan het interdepartementale domein betekent dus het conformeren aan het beleid van dit domein. Elk aangesloten departement moet voldoen aan in de richtlijnen vastgesteld beleid. Tevens wordt door elke departement het eigen Certificate Policy opgesteld door een departementale Policy Authority. Departementen kunnen echter ook de centrale baseline Certificate Policy overnemen. Beperkte variaties in de implementatie van het beleid kunnen in dit laatste geval in de Certification Practice Statements van de verschillende TTP-diensten (bijvoorbeeld CA en RA) uitgewerkt worden. De volgende figuur illustreert het 3e scenario:



Figuur 4.3. Scenario 3: Het interdepartementale domein

In de volgende tabel worden de gevolgen voor de kernpunten beschreven:

Kernpunten	*Omschrijving*
Verantwoordelijkheden	De verantwoordelijkheid voor de departementale invulling van het Interdepartementale beleid ligt bij de individuele departementen.
Basis TTP-diensten	Deze zullen sterk bepaald worden door de centrale richtlijnen en eventueel het centrale Certificate Policy. Beperkte variaties worden opgenomen in departementale CPs of CPS-en. Gezamenlijke inrichting van de basisdiensten is dus goed mogelijk.
Toegevoegde TTP-diensten	Behoeven niet gezamenlijk te worden ingericht. Departementen hebben vrije keus om deze in te richten wanneer daartoe de behoefte ontstaat. De centrale richtlijnen dienen daarbij als leidraad.
Toepassingen	Keuze en acceptatie van toepassingen kan efficiënt centraal worden uitgevoerd voor toepassingen waar een brede basis voor is. Specifieke toepassingen kunnen per departement worden gekozen.
Communicatie binnen de	Dit is expliciet geregeld middels de centrale richtlijnen en de hierarchie van

Rijksoverheid	CA's waarbij departementale CA's door de centrale root-CA worden gecertificeerd.
Communicatie met externe domeinen	Dit kan efficiënt centraal worden geregeld in cross-certificatie afspraken tussen het interdepartementale domein en de externe domeinen. Ook bestaat de mogelijkheid dat individuele departementale domeinen bilateraal cross-certificatie afspraken maken met externe domeinen.
Kosten	Veel componenten kunnen centraal worden aangeschaft en de infrastructuur kan voor een deel worden gedeeld. Er kan dus worden geprofiteerd van het volumevoordeel voor de decentrale componenten en het delen van centrale componenten. Departementen kunnen een eigen CA inrichten of gezamenlijk gebruik maken van één CA. De RA's kunnen optimaal ingericht worden binnen de departementen.

Voordelen:

- Meest doeltreffende optie. Eén beleid voor de interdepartementale communicatie is mogelijk. Dit wordt centraal ondersteund. Aangesloten departementen behoeven niet alles individueel te regelen. Het is ook mogelijk om specifieke wensen van departementen in te vullen. Voor een specifieke situatie kan een departement eigen domeinen opzetten.
- Een RO-brede baseline voor vertrouwen.
- Indien men overeenstemming heeft over de gezamenlijke structuren, kan elk department zelf bepalen wanneer men overgaat tot de implementatie binnen het departement.
- De organisatie (inclusief personeel) kan goed omgaan met het uniforme beveiligingsniveau.
- Aansprakelijkheid kan centraal en/of departementaal worden geregeld.
- Sluit meest aan de bestaande bestuurlijke structuren binnen de RO. Voor gezamenlijke belangen kan gebruik gemaakt worden van een gezamenlijk opgerichte organisatorische functie. De specifieke behoeftes vallen binnen de directe verantwoordelijkheid van de individuele departementen.
- Indien een departementaal domein aangesloten is bij het interdepartementale domein, kunnen zaken als cross-certificering, beleidsontwikkeling, audit en aansprakelijkheid efficiënt centraal worden geregeld. Ook kan de acceptatieprocedure voor applicaties centraal uitgevoerd worden. Heeft men speciale eisen of kiest men om andere redenen om niet aan te sluiten bij het interdepartementale domein, dan zal men deze zaken in principe zelf moeten regelen.
- Minder duur dan het de voorgaande scenario's[10]; maar duurder dan het 4e scenario.
  - voor het interdepartementale domein: +/- 250.000 aanschaf, 10% exploitatiekosten[11];
  - per specifiek (optioneel) departementaal domein: +/- 500.000 aanschaf, 10% exploitatiekosten. Deze investering kan echter veelal gedeeld worden door meerdere departementen waardoor de kosten veel lager uitvallen.

[10] Grote kostenbesparingen zijn mogelijk door het delen van bijvoorbeeld de CA infrastructuur. Zie bijlage 2. Maar ook in de voorbereidende activiteiten als beleidsontwikkeling, toetsen van toepassingen en selectieprocedures.

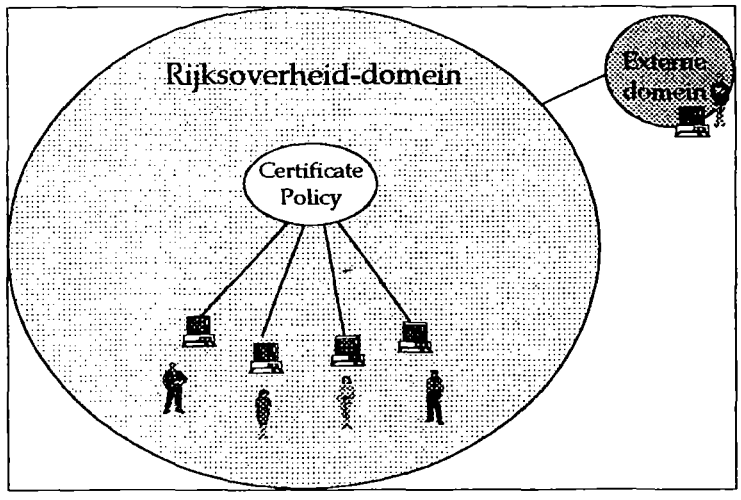
[11] Dit bedrag is lager dan voor een 'normale' CA aangezien de interdepartementale CA slechts beperkte functionaliteit hoeft te bieden: alleen voor het cross-certificeren met externe domeinen en het certificeren van departementale CA's. Deze handelingen hebben een zeer lage frequentie en klein volume.

Nadelen:

- Interdepartementale afstemming is noodzakelijk voordat tot implementatie kan worden overgegaan.

4.5 Scenario 4: Één Rijksoverheiddomein

Binnen de Rijksoverheid wordt één domein ingericht, waarmee het onderlinge vertrouwen tussen alle departementen wordt gerealiseerd. Daardoor wordt een RO-brede baseline voor vertrouwen gecreëerd. Elk departement moet zich bij het domein aansluiten. In het Certificate Policy(CP) bepaalt de centrale Policy Authority waarvoor het domein gebruikt wordt en aan welke eisen door alle communicerende partijen en TTP-diensten moet worden voldaan. Tevens wordt een centrale organisatorische functie ingericht die zaken als uitgave en intrekken van de persoonlijke digitale identiteitsbewijzen, het cross-certificeren met externe domeinen, beleidsontwikkeling, audit en aansprakelijkheid centraal regelt. Ook de acceptatieprocedure voor applicaties wordt centraal uitgevoerd. De volgende figuur illustreert het 4e scenario:



Figuur 4.4. Scenario 1: Één Rijksoverheiddomein

In de volgende tabel worden de gevolgen voor de kernpunten beschreven

Kernpunten	*Omschrijving*
Verantwoordelijkheden	De departementen delegeren verantwoordelijkheden voor het Rijksoverheid domein aan de centrale Policy Authority.
Basis TTP-diensten	Deze worden bepaald door het centrale Certificate Policy. Gezamenlijke inrichting hiervan is dus vereist.
Toegevoegde TTP-diensten	Moeten gezamenlijk worden ingericht. Departementen hebben geen vrije keus om deze in te richten wanneer daartoe de behoefte ontstaat.
Toepassingen	Keuze en acceptatie van toepassingen kan efficiënt centraal worden uitgevoerd voor toepassingen waar een brede basis voor is. Specifieke toepassingen per departement worden niet toegestaan.
Communicatie binnen de Rijksoverheid	Dit is impliciet geregeld aangezien er slechts één vertrouwensdomein is.
Communicatie	Dit kan efficiënt centraal worden geregeld in bilaterale cross-certificatie

met externe domeinen	afspraken tussen het Rijksoverheiddomein en de externe domeinen.
Kosten	Alle componenten kunnen centraal worden aangeschaft en de infrastructuur kan worden gedeeld. Er kan optimaal worden geprofiteerd van het volumevoordeel voor de decentrale componenten en het delen van centrale componenten. De RA's kunnen optimaal ingericht worden binnen de Rijksoverheid.

De voor- en nadelen van dit scenario kunnen als volgt worden weergegeven:

Voordelen:
- Goedkoopste optie: +/- 500.000 aanschaf, 10% exploitatiekosten. Meeste efficiënte optie. Er is één beleid en alles wordt centraal geregeld. De aangesloten departementen behoeven niet alles individueel te regelen.
- Een RO-brede baseline voor vertrouwen.
- Het vertrouwen in de interdepartementale communicatie en met externe domeinen is het makkelijkst te verwezenlijken. Bilaterale cross-certificeringsafspraken tussen de individuele departementen en met externe domeinen zijn niet nodig
- De organisatie (inclusief personeel) kan goed omgaan met het uniforme basisbeveiligingsniveau.

Nadelen:
- Sluit niet aan bij de bestaande bestuurlijke structuren binnen de RO. Een centrale organisatorische-functie valt buiten de directe verantwoordelijkheid van de individuele departementen.
- Aansprakelijkheid dient centraal te worden geregeld; hiervoor is geen bestaande organisatiestructuur voorhanden.
- Niet mogelijk om specifieke wensen van departementen te vullen.

4.6 Conclusies

De volgende scenario's kunnen als basis voor de invoering van TTP-diensten bij de Rijksoverheid dienen:
- één domein per bedrijfsproces
- één domein per departement
- één interdepartementaal domein
- één RO-domein

Het eerste scenario is het meest complexe scenario, maar biedt de meeste flexibiliteit om specifieke wensen van bedrijfsprocessen in te vullen. Dit scenario biedt echter geen RO-brede en geen departementbrede base-line voor vertrouwen. Het sluit niet aan bij de bestaande bestuurlijke structuren binnen departementen en de RO. Dit scenario zou het gevolg kunnen zijn van de nul optie als geschetst in hoofdstuk 3.
Het vierde scenario is het minst complexe scenario, maar het sluit niet aan bij de bestaande bestuurlijke structuren binnen de RO. Dit scenario biedt een RO-brede baseline voor vertrouwen.
Het tweede scenario biedt de beste mogelijkheid om specifieke wensen per departement in te vullen. Dit scenario biedt echter geen RO-brede baseline voor vertrouwen.

Het derde scenario sluit van de vier het best aan bij de bestaande bestuurlijke structuren binnen de RO. Er kan optimaal gebruik worden gemaakt van beschikbare kennis en middelen. Dit scenario biedt een RO-brede baseline voor vertrouwen met daarop beperkte variatie per departement.

Samenvattend scoren de verschillende scenario's als volgt op de kernpunten:

Invalshoeken	Één RO-domein	Één interdepartementale domein	Één domein per departement	Één domein per bedrijfsproces
Kosten/complexiteit	++	+	-/+	--
Aansluiten aan besturing binnen RO	--	++	+	-
RO-brede baseline voor vertrouwen	++	+	--	--
Departementbrede baseline voor vertrouwen	++	++	++	--
Invulling specifieke wensen	-	-/+	+	++
Doeltreffendheid	++	+	-/+	--
Aansprakelijkheid	-	+	+	-/+
Technische haalbaarheid (beveiligingsniveaus)	++	+	-/+	--

5. Organisatorische aspecten

In dit hoofdstuk worden aan de hand van de in hoofdstuk 4 gepresenteerde scenario's de organisatorische aspecten beschreven. Hiermee wordt de vierde deelvraag van dit onderzoek beantwoord:

> *Welke organisatorische aspecten zijn er bij de invoering van TTP-diensten binnen de Rijksoverheid van het belang?*

5.1 Inleiding

Bij het opzetten en in stand houden van TTP-diensten, dient een organisatie aan een aantal onderwerpen aandacht te besteden. Per vertrouwensdomein dienen een aantal activiteiten te worden uitgevoerd. Aangezien we in het voorgaande hoofdstuk een aantal scenario's hebben beschreven die verschillen in aantal en locatie van vertrouwensdomeinen, zullen er verschillen optreden ten aanzien van de noodzakelijke organisatie.
In dit hoofdstuk zullen dan ook eerst de activiteiten beschreven worden die voor elk domein noodzakelijk zijn om vervolgens de verschillen per scenario aan te geven. Hierbij wordt nog geen aandacht besteed aan de vraag of men activiteiten zelf moet doen of kan uitbesteden. Dit komt in het volgende hoofdstuk aan de orde.

5.2 Inrichting van een vertrouwensdomein

In hoofdstuk 2 zijn de belangrijkste elementen van een vertrouwensdomein beschreven: de TTP-diensten, de toepassingen en de communicerende partijen binnen een domein en cross-certificering met externe domeinen. Ten aanzien van al deze elementen dienen randvoorwaarden te worden gesteld, keuzes te worden gemaakt en beheersactiviteiten te worden ontplooit. Dit alles met het doel TTP-diensten duurzaam in de organisatie onder te brengen.

Daarbij onderscheiden we de activiteiten in 4 categorieën met verschillende subcategorieën:

1. *Beleidsontwikkeling*
2. *Voorbereiding en specificatie,* met de subcategorieën
   - Selectie toepassingen
   - Selectie TTP-diensten
   - Infrastructuur en aanbesteding
3. *Invoering in de organisatie*
4. *Instandhouding en beheer,* met de subcategorieën:
   - Operationeel beheer
   - Helpdesk
   - Audit en controle

1. Beleidsontwikkelingen

Als eerste activiteit dienen, vanuit de behoefte binnen het vertrouwensdomein, algemene beleidsuitgangspunten en randvoorwaarden te worden opgesteld. Dit gebeurt in afstemming met de overige activiteiten. Hiermee wordt divergentie in de resultaten voorkomen en worden de voorwaarden gecreëerd om activiteiten te delegeren.
Deze uitgangspunten dienen vervolgens uitgewerkt te worden in beleidsdocumenten voor het domein. Dit resulteert uiteindelijk in het Certificate Policy voor het domein en het beleid ten aanzien van cross-certificering.
Om deze activiteit uit voeren, is kennis noodzakelijk van de (bestuurlijke) organisatie, de mogelijkheden van TTP-diensten en toepassingen, juridische kennis (inclusief IT recht) en (IT) beveiliging.

2. Voorbereiding en specificatie

Selectie van toepassingen
De toepassingen die binnen het domein wenselijk zijn dienen te worden geselecteerd op grond van functionele behoeftes binnen de Rijksoverheid. Het is belangrijk om een of meerdere toepassingen te selecteren die bij de invoering van TTP-diensten als eerste 'afnemer' van die diensten zal optreden. Beveiligde e-mail is hiervoor een interessante optie. Uiteraard kunnen in de loop der tijd toepassingen worden toegevoegd.
Om deze activiteit uit voeren, is kennis noodzakelijk van de behoefte binnen de organisatie en de bestaande toepassingen. Tevens dient de expertise aanwezig te zijn om te beoordelen of toepassingen geschikt zijn om het gewenste beveiligingsniveau met TTP-diensten te realiseren is.

Selectie van TTP-diensten
Naast de basis TTP-diensten dient, op grond van beleidsuitgangspunten en de geselecteerde toepassingen, een keuze te worden gemaakt voor toegevoegde TTP-diensten binnen het domein. Na de selectie dienen de TTP-diensten in detail te worden gespecificeerd. Dit resulteert in een aantal specificaties in de vorm van Certification Practise Statements (CPSs).
Om deze activiteit uit voeren, is diepgaande kennis noodzakelijk van de mogelijkheden van TTP-diensten en de gevolgen voor de organisatie. Voor het opstellen van de CPSs is verder juridische kennis en inzicht in (werkwijze en structuren binnen) de organisatie noodzakelijk.

Infrastructuur en aanbesteding
Op grond van de voorgaande activiteiten dient een infrastructuur te worden opgesteld. Producten en diensten worden geselecteerd, ontwikkeld of ingekocht. Toetsing van producten en diensten tegen de gestelde eisen vormt daarbij een belangrijk onderdeel.
Om deze activiteit uit voeren, is kennis nodig voor het uitvoeren van infrastructurele projecten. Verder is kennis noodzakelijk van de markt en de mogelijkheden van TTP-diensten.

3. Invoering in de organisatie

Zeer belangrijk is de voorbereiding van de invoering van de TTP-diensten en toepassingen in de organisatie. Wie gaat de TTP-diensten leveren?

Vragen die beantwoord moeten worden zijn bijvoorbeeld: 'Worden toepassingen die gebruik maken van TTP-diensten voorgeschreven of is er een keuzemogelijkheid op basis van een want-to-have/need-to-have' en 'Worden bestaande toepassingen vervangen of worden nieuwe toepassingen toegevoegd?'
Het resultaat van deze activiteit is een invoeringsstrategie en een organisatie die goed voorbereid is op de invoering en in stand houding van de TTP-diensten en toepassingen.
Om deze activiteit uit voeren, is diepgaande kennis noodzakelijk van de organisatiestructuur, de IT processen en de processen die gepaard gaan met TTP-diensten.

5. Instandhouding en beheer

Operationeel beheer
De nodige aandacht dient te worden besteed aan het inrichten van het operationeel beheer. Dit is niet alleen nodig om de continuïteit van de dienstverlening te garanderen maar heeft ook een belangrijke functie bij het in stand houden van het beveiligingsniveau tijdens het dagelijks gebruik.
Hiervoor is een IT-beheersorganisatie noodzakelijk met een grote mate van beveiligingsbewustzijn. Daarnaast is een meer administratieve organisatie noodzakelijk voor het dagelijks beheer van de diensten (RA functie: uitgifte en intrekken certificaten e.d.).

Helpdesk
Uiteraard dient er een helpdesk te worden ingericht ter ondersteuning van de gebruikers en de beheerders. Onderscheid wordt gemaakt tussen 1e-lijnssupport dat zo dicht mogelijk bij de eindgebruiker staat en 2e-lijnssupport dat gericht is op de techniek en de technische dienstverlening.
De helpdeskmedewerkers dienen goed op de hoogte te zijn van de TTP-diensten en de toepassingen die daarvan gebruik maken.

Audit en controle
Om het beveiligingsniveau in stand te houden dienen activiteiten te worden opgezet om alle relevante elementen periodiek te controleren. Afwijkingen dienen te worden gerapporteerd en gecorrigeerd. Aandacht dient daarbij niet alleen te worden besteed aan de TTP-diensten maar ook aan de toepassingen en de gebruikers. Dit resulteert in een controleschema dat waarborgt dat de omgeving gedurende de levenscyslus betrouwbaar is.
Hiervoor is een audit organisatie noodzakelijk die bekend is met de bedrijfsprocessen en de specifieke TTP-diensten en de eisen die daaraan worden gesteld[12] (bijvoorbeeld EDP audit pool).

5.3 Verschillen per scenario

In de voorgaande paragraaf hebben we de hoofdactiviteiten beschreven. Daarbij is geen uitspraak gedaan over de vorm waarin of de plaats binnen de Rijksoverheid waar een

[12] Inclusief externe eisen ten gevolge van wet- en regelgeving (op TTP-gebied: digitale handtekening).

activiteit belegd wordt. In de onderstaande tabel wordt dit per scenario van hoofdstuk 4 aangegeven.

	Scenario 1: Domein per bedrijfsproces	Scenario 2: Departementale domeinen	Scenario 3: Interdepartementaal Domein	Scenario 4: RO domein
Beleidsontwikkeling	Ad-hoc	D	ID (taskforce)	ID (centraal orgaan)
Selectie toepassingen	Ad-hoc	D	ID (+D)	ID (werkroep)
Selectie TTP-diensten	Ad-hoc	D	ID (+D)	ID (werkroep)
Infrastructuur en aanbesteding	Ad-hoc	D	ID (+D)	ID (werkroep)
Invoering in de organisatie	Ad-hoc	D	D	D
Operationeel beheer	Ad-hoc	D	D	D
Helpdesk	Ad-hoc	D	1e lijns: D. 2e lijns: ID (+ D)	1e lijns: D 2e lijns: ID.
Audit en controle	Ad-hoc	D (+ID)	ID (+D)	ID

ID = InterDepartementaal, D = Departementaal, (+ID/D) = optioneel ook door D/ID.

6. Uitbesteden of zelf inrichten en beheren?

In hoofdstuk 5 lag het accent op de organisatorische aspecten van het gebruik van TTP-diensten binnen de Rijksoverheid. In dit hoofdstuk ligt het accent op de keuze ten aanzien van uitbesteden of zelf opzetten van TTP-diensten binnen de Rijksoverheid. Hiermee wordt de vijfde deelvraag van dit onderzoek beantwoord:

> *Welke keuzen zijn er bij de invoering en de instandhouding van TTP-diensten binnen de Rijksoverheid ten aanzien van uitbesteden of zelf opzetten van een TTP dienstverlening?*

Ten aanzien van de invoering en de instandhouding van TTP-diensten kan de overheid beslissen of men delen daarvan zelf wil implementeren of uitbesteden. Er is een scala aan mogelijkheden voor het uitbesteden van elementen binnen een vertrouwensdomein. In dit hoofdstuk zullen de mogelijkheden en de consequenties beschreven worden.

Paragraaf 6.1 geeft een beknopt overzicht van de meer generieke argumenten voor uitbesteding. In 6.2 wordt een aantal specifieke kernpunten ten aanzien van de uitbesteding van TTP-diensten beschreven. In 6.3 worden vervolgens 4 opties beschreven voor het uitbesteden die variëren van geen uitbesteding tot maximale uitbesteding. Per variant wordt de invloed op de kernpunten geanalyseerd.

6.1 Waarom uitbesteding?

Uiteraard is de eerste vraag die gesteld moet worden waarom men überhaupt de TTP-dienstverlening zou uitbesteden. In wezen gelden voor TTP-diensten dezelfde argumenten als voor de meeste ICT-diensten. Zo kunnen initiële investeringen beperkt worden, kunnen kosten veelal direct gerelateerd worden aan het daadwerkelijke gebruik, kunnen desinvesteringen ten gevolge van veroudering van de techniek beperkt worden en wordt de eigen organisatie niet belast met zaken die zich niet richten op de kernactiviteiten.

Met name ten aanzien van de veroudering van de technologie bestaan er risico's indien men alles zelf wil inrichten. Techniek en standaarden voor TTP-diensten en de toepassingen die daarvan gebruik maken, zijn nog steeds sterk in ontwikkeling.

Het zelf opzetten van TTP-diensten vergt zeer specifieke kennis die veelal moeilijk binnen de organisatie te vinden is. Het inhuren van externe kennis en opleiding zal noodzakelijk zijn, wil men zelf TTP-diensten inrichten.

Daarnaast heeft de overheid een specifieke rol in de maatschappij die aanleiding kan geven om eerder voor uitbesteding aan marktpartijen te kiesen dan voor zelf doen. Voordat men deze keuze maakt, dienen echter een aantal punten goed te worden overwogen. Deze 'kernpunten' zijn in de volgende paragraaf beschreven.

6.2 Kernpunten

Ten aanzien van de vraag of uitbesteding wenselijk is, behandelen we in deze paragraaf een 7-tal kernpunten die in overweging moeten worden genomen[13]. De kernpunten hebben betrekking op de volgende vragen:

1 *Beleid*: Welke invloed heeft uitbesteding op de keuzemogelijkheid ten aanzien van het beleid binnen het domein (of beveiligingsniveau)?
2 *Exclusiviteit*: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de exclusiviteit van gegevens uit te besteden?
3 *Integriteit*: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de integriteit van gegevens, met name de digitale handtekening, uit te besteden?
4 *Privacy*: Is het vanuit privacy-oogpunt mogelijk om TTP-diensten uit te besteden?
5 *Beschikbaarheid*: Hoe zit het met de continuïteit van de dienstverlening bij uitbesteding?
6 *Integratie*: Is het mogelijk om diensten die zo geïntegreerd zijn met de organisatie uit te besteden?
7 *Aansprakelijkheid*: Welke invloed heeft uitbesteden op het aansprakelijkheidsvraagstuk?

1. Welke invloed heeft uitbesteding op de keuzemogelijkheid ten aanzien van het beleid binnen het domein (of niveau beveiligingsniveau)?
In hoofdstuk 3 is aangegeven dat een vertrouwensdomein een bepaald beveiligingsniveau realiseert. Dit niveau wordt bepaald door het vigerende beleid binnen dat domein. In hoofdstuk 5 is dan ook als eerste activiteit bij het opzetten van een domein het vaststellen van het beleid opgenomen. In geval van uitbesteding van diensten is het dan ook belangrijk om te bekijken in hoeverre het gewenste beveiligingsniveau wordt beïnvloed door het inkopen van diensten. Of anders geformuleerd: in hoeverre de vrijheid van keuze ten aanzien van het beveiligingsniveau wordt beïnvloed door uitbesteding of zelf doen.

2. Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de exclusiviteit van gegevens uit te besteden?
De eerste vraag die men zich dient te stellen is, of men een cruciale beveiligingsfunctie ten behoeve van het geheim houden van informatie wenst uit te besteden. In wezen gaat het daarbij om het risico dat de externe dienstverlener toegang kan verkrijgen tot informatie die de Rijksoverheid juist wenst af te schermen. Bij dit risico spelen twee belangrijke aspecten: aggregatie van informatie en het belang dat de externe dienstverlener bij de informatie heeft.

Met *aggregatie* van informatie wordt bedoelt het 'opeenhopen' van informatie. Naarmate een externe organisatie meer informatie van de Rijksoverheid beschikbaar heeft, wordt het interessanter en veelal ook eenvoudiger daar misbruik van te maken. Het grootste risico hierbij is de aggregatie van vercijferde gegevens in combinatie met het sleutelmateriaal dat noodzakelijk is om de gegevens te ontcijferen.

[13] In het NAP/TTP rapport wordt aanbevolen dat de overheid alleen gebruik maakt van bij de (op te richten) TTP-kamer aangesloten en gecontroleerde TTP-dienstverleners gebruik te maken. Het is aan te bevelen om de overwegingen die hier worden genoemd te toetsen tegen de randvoorwaarden die de TTP-kamer aan TTP-dienstverleners stelt en eventueel aanvullende eisen te formuleren.

Met het *belang van de externe dienstverlener* wordt de (economische) waarde van de informatie voor die dienstverlener bedoelt. Want net als elke organisatie in Nederland heeft de dienstverlener te maken met de Rijksoverheid. De dienstverlener is belastingplichtig, kan opdrachten voor de overheid uitvoeren, subsidie ontvangen of afhankelijk zijn van vergunningen. Ook kunnen er conflicten ontstaan tussen de dienstverlener en de Rijksoverheid of individuele departementen. Het kan daarom voor een dienstverlener interessant zijn om toegang te verkrijgen tot vertrouwelijke overheidsinformatie of tijdelijk de dienstverlening op te schorten. De schade is hierbij veelal al toegericht op het moment van het incident en detectie achteraf heeft slechts een zeer beperkte effect.

Ook kan het vertrouwen in de overheid als betrouwbare bewerker van privacy-gevoelige gegevens worden geschaad indien de dienstverlener onzorgvuldig omgaat met gevoelige gegevens van de Rijksoverheid. In enkele gevallen is het zelfs niet toegestaan registraties buiten de verantwoordelijke overheden onder te brengen. Een voorbeeld daarvan zijn bepaalde politieregisters.

3. Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de integriteit van gegevens, met name de digitale handtekening, uit te besteden?
Net als ten aanzien van de exclusiviteit kan men zich afvragen of het wenselijk is om de diensten ten behoeve van het creëren van digitale handtekeningen aan een externe dienstverlener over te laten. Hiermee krijgt deze dienstverlener de mogelijkheid in handen om zich als een medewerker van de Rijksoverheid uit te geven en namens deze op frauduleuze wijze (rechts)handelingen te verrichten.

Het grootste risico hierbij is het misbruik maken door de externe dienstleverancier van de sleutels die noodzakelijk zijn voor het creëren van digitale handtekeningen.

Een ander probleem heeft te maken met de noodzakelijkerwijs lange bewaartermijn voor gegevens die noodzakelijk zijn voor het (achteraf) kunnen controleren van de geldigheid van een digitale handtekening. Indien deze gegevens door een externe dienstverlener worden bewaard, is de continuïteit van deze dienst een belangrijk aandachtspunt. Zie de discussie hieronder over 'continuïteit'.

4. Is het vanuit privacy-oogpunt mogelijk om TTP-diensten uit te besteden?
Een verder aandachtspunt zijn privacy aspecten die gepaard gaan met het leveren van TTP-diensten. Privacygevoelige informatie over aanvragers van certificaten zal verwerkt en opgeslagen worden bij de TTP's ten behoeve van beheersfuncties. Maar ook het beheer van certificaten kan veel vertellen over de positie van een individu. Als een certificaat op een zwarte lijst wordt geplaatst, kan dat ontslag of overplaatsing inhouden. Deze mutaties dienen zoveel mogelijk te worden afgeschermd. Dit is met name relevant wanneer men voor openbare TTP-diensten zou kiezen waarbij certificaten en zwarte lijsten op publiek toegankelijke (directory/database) servers worden geplaatst.

5. Hoe zit het met de continuïteit van de dienstverlening bij uitbesteding
Misschien wel het belangrijkste aspect is de vraag welke zekerheden externe dienstaanbieders kunnen leveren ten aanzien van de continuïteit van de dienstverlening.

Organisaties kunnen fuseren (ook internationaal), diensten afstoten en zelfs failliet gaan. Dit kan de continuïteit van de dienstverlening ernstig aantasten.
Fusies kunnen er toe leiden dat bijvoorbeeld de bewuste scheiding tussen meerdere TTP-dienstaanbieders om aggregatie tegen te gaan, teniet wordt gedaan.
Bij een faillissement of fusie bestaat niet alleen het gevaar dat de dienstverlening stagneert. Het kan er ook toe leiden dat sleutelmateriaal en andere gegevens bij een andere onderneming terecht komen.

Gezien de omvang van een eventuele aanbesteding zal men Europese aanbestedingsprocedures moeten volgen. Gevoelige informatie zou daarbij zelfs in het buitenland kunnen komen. Een zelfde situatie ontstaat indien een externe dienstleverancier wordt overgenomen door een buitenlands bedrijf. Dit kan problemen opleveren ten aanzien van het geldend recht en verschillen in privacy-wetgeving. Bij eventuele tenders dient men hiermee rekening te houden.

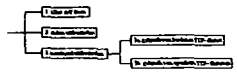
6. Is het mogelijk om diensten die zo geïntegreerd zijn met de organisatie uit te besteden?
In paragraaf 2.6 is te zien dat de TTP-dienstverlening op termijn sterk zal zijn geïntegreerd met de bedrijfsprocessen binnen de organisatie. Dit vergt snelle reactietijden, optimale toegang tot gegevens en flexibiliteit van de verschillende TTP-diensten. Met name het beheer van certificaten en zwarte lijsten en het daaraan gekoppelde autorisatiebeheer zal zeer intensief zijn. Contractueel en technisch zal hiermee rekening moeten worden gehouden indien gebruik wordt gemaakt van externe dienstverleners

7. Welke invloed heeft uitbesteden op het aansprakelijkheidsvraagstuk?
Aansprakelijkheid in verband met de levering van TTP-diensten is een belangrijk punt van discussie waarover verschillende meningen bestaan. In [duthler] wordt deze discussie uitgebreid behandeld. De garanties ten aanzien van de aansprakelijkheid van externe aanbieders van TTP-diensten zal echter altijd beperkt zijn tot een financiële aansprakelijkheid. De grote vraag is, of dit voor de specifieke situatie van de Rijksoverheid effectief is. Welke genoegdoening levert een financiële tegemoetkoming in het geval dat een minister in de problemen komt door fouten van een TTP? Uiteraard kan de 'stok achter de deur' van een financiële aansprakelijkheid voor een TTP-dienstaanbieder een sterke motivatie zijn om zorgvuldig te werken, zoals [dutler] ook aangeeft. Het probleem van externe aanbieders is momenteel de uiterst beperkte mogelijkheid om zich (in Nederland) tegen aansprakelijkheid te verzekeren. Dit leidt er veelal toe dat de aanbieders van TTP-diensten zich sterk beperken in hun aansprakelijkheid[14]. Bij uitbesteding is te overwegen om afspraken te maken over onafhankelijke arbitrage en/of een geschillencommissie.

[14] De aansprakelijkheid is veelal geheel uitgesloten (wat echter onder het Nederlands recht niet mogelijk is), dan wel beperkt tot de directe schade (de kosten die voor de dienst worden betaald).

6.3 Varianten voor uitbesteding

Ten aanzien van het uitbesteden van TTP-diensten kunnen een aantal varianten worden aangegeven. Deze varianten zijn in de onderstaande boomfiguur aangegeven. In het vervolg van deze paragraaf beschrijft de gevolgen van de verschillende keuzen.



Om een indicatie te geven van de verschillen in kosten per uitbestedingsvariant, wordt in een tabel aangegeven welke van de activiteiten van hoofdstuk 5 zelf, en welke door externe leveranciers kunnen worden uitgevoerd.

Variant 1: Alles zelf doen

Deze keuze houdt in dat men alle activiteiten uit hoofdstuk 5 zelf uitvoert. Producten worden gekocht of ontwikkeld en de diensten worden door de eigen organisatie geleverd.

Kosten

Beleidsontwikkeling	Selectie toepassingen	Selectie TTP-diensten	Infrastructuur en aanbesteding	Invoering in de organisatie	Operationeel beheer	Helpdesk	Audit en controle
zelf	zelf	zelf	zelf	zelf	zelf	zelf	zelf

Beleid
Men heeft maximale vrijheid in het opstellen van het beleid en het bepalen van het beveiligingsniveau.

Exclusiviteit
Indien er voor gekozen wordt om zo veel mogelijk zelf te doen, kunnen de problemen die in 6.1 zijn geconstateerd, worden voorkomen. Toch is het verstandig scheiding aan te brengen tussen de interne organisatie-onderdelen die de verschillende TTP-diensten gaan leveren om (interne) fraude te voorkomen.

Digitale handtekening
Indien er voor gekozen wordt om zo veel mogelijk zelf te doen, kunnen de problemen die in 6.1 zijn geconstateerd, worden voorkomen. Toch is het verstandig scheiding aan te brengen tussen de interne organisatie-onderdelen die de verschillende TTP-diensten gaan leveren om (interne) fraude te voorkomen.

Privacy
De problemen zijn beperkt tot de eigen omgeving.

Continuïteit
De continuïteit is goed gegarandeerd aangezien de Rijksoverheid zelf de diensten levert.

Integratie
Integratie binnen de eigen organisatie is goed te realiseren aangezien men zelf de diensten specificeert en levert. Alle informatie is beschikbaar.

Aansprakelijkheid
Dit zal geheel intern geregeld moeten worden.

Variant 2: Componenten uitbesteden.

Dit is de meest flexibele keuze ten aanzien van uitbesteden. Deze keuze houdt in dat men met name de 'beleidsontwikkeling' en de 'voorbereiding en specificatie' zelf verricht. De activiteiten die vallen onder 'instandhouding en beheer' worden of zelf gedaan of uitbesteed. Diensten worden dus of ingekocht of ontwikkeld en door de eigen organisatie geleverd. Door een goede keuze tussen uitbesteden of zelf doen, kunnen veel van de problemen die in 6.2 zijn geconstateerd, worden voorkomen.

Kosten

Beleidsontwikkeling	Selectie toepassingen	Selectie TTP-diensten	Infrastructuur en aanbesteding	Invoering in de organisatie	Operationeel beheer	Helpdesk	Audit en controle
zelf	zelf	zelf/extern	zelf/extern	zelf/extern	zelf/extern	zelf/extern	zelf/extern

Beleid
Men heeft grote vrijheid in het opstellen van het beleid en het bepalen van het beveiligingsniveau. In die gevallen waar voor uitbesteding wordt gekozen, zal de Rijksoverheid in essentie aan een TTP-dienstenaanbieder vragen om het eigen beleid te implementeren.

Exclusiviteit
Door een afgewogen verdeling tussen zelf doen en/of uitbesteden bij meerdere partijen kunnen de problemen die in 6.1 zijn geconstateerd, worden voorkomen.

Digitale handtekening
Door een afgewogen verdeling tussen zelf doen en/of uitbesteden bij meerdere partijen kunnen de problemen die in 6.1 zijn geconstateerd, worden voorkomen.

Privacy

Publikatie van certificaten en zwarte lijsten met ingetrokken certificaten kan voor het publiek worden afgeschermd. Privacy-problemen dienen contractueel met de eventuele leverancier worden afgedekt.

Continuïteit
De continuïteit kan deels goed gegarandeerd worden indien de Rijksoverheid zelf de diensten levert.

Integratie
Integratie binnen de eigen organisatie is goed te realiseren aangezien men de diensten grotendeels zelf specificeert en deels levert. De meeste informatie is beschikbaar.

Aansprakelijkheid
Dit zal deels intern geregeld moeten worden. Met externe aanbieders kunnen afspraken worden gemaakt over de aansprakelijkheid.

In bijlage "Beschrijving TTP-modules" wordt ten behoeve van de keuze voor uitbesteding per TTP-module aangegeven wat de voor- en nadelen van uitbesteding zijn.

Variant 3: Gebruik van besloten TTP-diensten

Het grote verschil met de inkoop van openbare TTP-diensten is gelegen in het feit dat in dit geval specifieke TTP-diensten opgezet worden door de dienstleverancier aan de hand van de specificaties van de klant. De TTP-diensten worden ook alleen aan die klant geleverd.

Kosten

Beleidsontwikkeling	Selectie toepassingen	Selectie TTP-diensten	Infrastructuur en aanbesteding	Invoering in de organisatie	Operationeel beheer	Helpdesk	Audit en controle
zelf	zelf	zelf/extern	extern	extern	extern	extern	zelf/extern

Beleid
In dit geval zal de Rijksoverheid in essentie aan een TTP-dienstenaanbieder vragen om het eigen beleid te implementeren. De variatie in het beleid dat door een TTP-aanbieder wordt ondersteund zal wel beperkt worden door de organisatie, infrastructuur en procedures van de aanbieder.

Exclusiviteit
Het risico kan beperkt worden door gegevens te verdelen over meerdere partijen. Zo kan sleutelbeheer bij een andere organisatie ondergebracht worden als een archieffunctie.
Daarnaast dient men marktpartijen te kiezen die zeer beperkte belangen hebben bij het kennis nemen of laten lekken van overheidsinformatie.
Het is mogelijk om meerdere partijen te selecteren aangezien de diensten opgezet worden op basis van specificaties die zijn opgesteld door de eigen organisatie.

Digitale handtekening

Het risico kan wederom beperkt worden door gegevens te verdelen over meerdere partijen. Zo kan sleutelbeheer voor digitale handtekeningen bij een andere organisatie ondergebracht worden als een archieffunctie.
Daarnaast dient men marktpartijen te kiezen die zeer beperkte belangen hebben bij het kennis nemen of laten lekken van overheidsinformatie.

Privacy
Publikatie van certificaten en zwarte lijsten met ingetrokken certificaten zullen in een database worden geplaatst die voor de dienstleverancier toegankelijk is voor beheer, het publiek krijgt geen toegang. Privacy-problemen kunnen contractueel met de leverancier worden afgedekt.

Continuïteit
Dit aandachtspunt leidt er toe om bij de keuze van een externe dienstverlener aandacht te besteden aan verschillende aspecten van die organisatie zoals de stabiliteit en betrouwbaarheid. Het is in dit licht zinnig om te verwijzen naar de generieke eisen aan een TTP-organisatie en dienst die zijn opgesteld in het kader van het NAP/TTP project en het vervolg daarop het TTP.NL project.

Integratie
Integratie met de eigen organisatie is redelijk tot goed te realiseren. De eisen en wensen dient men in de specificaties voor de te leveren diensten opnemen.

Aansprakelijkheid
Met externe aanbieders kunnen afspraken worden gemaakt over de aansprakelijkheid.

Variant 4: Gebruik van openbare TTP-diensten

Kosten

Beleidsontwikkeling	Selectie toepassingen	Selectie TTP-diensten	Infrastructuur en aanbesteding	Invoering in de organisatie	Operationeel beheer	Helpdesk	Audit en controle
selectie	Zelf	extern	extern	extern	extern	extern	extern

Beleid
Als de Rijksoverheid (departementen) van een openbare TTP diensten afneemt, bepaalt de oepenbare TTP het beleid. Tevens is het geen gesloten domein voor de Rijksoverheid maar een openbaar domein waar ook externen deel van zullen uitmaken. In dit geval zal de Rijksoverheid het door een openbare TTP-domein vastgestelde beleid moeten volgen. Men is dus niet vrij om een eigen beveiligingsniveau te kiezen. Het is maar zeer de vraag of dit gezien de verwachte diversiteit aan eisen geschikt is voor alle situaties binnen de Rijksoverheid. Overigens is een belangrijk gevolg hiervan dat normaliter elke ambtenaar een contract zal moeten afsluiten met de TTP-aanbieder, en niet collectief via de werkgever.

Exclusiviteit
Het risico kan beperkt worden door gegevens te verdelen over meerdere partijen. Zo kan sleutelbeheer bij een andere organisatie ondergebracht worden als een archieffunctie.

Daarnaast dient men marktpartijen te kiezen die zeer beperkte belangen hebben bij het kennis nemen of laten lekken van overheidsinformatie.

Deze vorm van maximale uitbesteding maakt het echter moeilijk om meerdere aanbieders te selecteren aangezien alle openbare TTP-aanbieders een eigen, veelal afwijkend beleid hebben. Aggregatie van gegevens is dus moeilijk te voorkomen.

Digitale handtekening
Het risico kan wederom beperkt worden door gegevens te verdelen over meerdere partijen. Zo kan sleutelbeheer voor digitale handtekeningen bij een andere organisatie ondergebracht worden als een archieffunctie.
Daarnaast dient men marktpartijen te kiezen die zeer beperkte belangen hebben bij het kennis nemen of laten lekken van overheidsinformatie.
Zoals hierboven gemeld maakt deze vorm van maximale uitbesteding het echter moeilijk om meerdere aanbieders te selecteren.

Privacy
Publikatie van certificaten en zwarte lijsten met ingetrokken certificaten zullen in een publiekelijk toegankelijke database worden geplaatst. Dit kan ernstige conflicten veroorzaken met privacy-regels.

Continuïteit
Dit aandachtspunt leidt er toe om bij de keuze van een externe dienstverlener aandacht te besteden aan verschillende aspecten van die organisatie zoals de stabiliteit en betrouwbaarheid. Het is in dit licht zinnig om te verwijzen naar de generieke eisen aan een TTP-organisatie en dienst die zijn opgesteld in het kader van het NAP/TTP project en het vervolg daarop het TTP.NL project.

Integratie
Integratie met de eigen organisatie is niet eenvoudig te realiseren. De mogelijkheden om de 'eigen' certificaten te beheren zijn beperkt. Gebruik van certificaten voor bijvoorbeeld toegangsbeveiliging stuit vooral op logistieke problemen aangezien men de bron van de certificaten (de Certification Authority en Directory Service) niet in eigen beheer heeft. De aanvraagprocedures zullen conform het openbare TTP-beleid zijn en dus veelal slecht integreren met de eigen organisatie. Zo zullen er geen loketten binnen de Rijksoverheid zijn.
Overigens is er een tendens aanwezig waarbij organisaties zich kunnen classificeren voor het uitgeven van certificaten namens een openbare TTP: de Registration Autoriteit functie wordt dus vanuit de TTP uitbesteed. Daarbij dient de toekomstige RA te voldoen aan eisen die de TTP stelt aan RAs.

Uiteraard kan volledig gebruik gemaakt worden van de service die door de openbare TTP wordt geleverd voor haar klanten. Aan specifieke wensen kan slechts voldaan worden indien deze niet met het beleid van de publieke TTP in conflict zijn.

Aansprakelijkheid
De externe aanbieders zullen standaard regelingen hebben ten aanzien van de aansprakelijkheid. Deze zijn veelal (vooralsnog) beperkt.

6.4 Samenvatting

In wezen gelden voor het uitbesteden van TTP-diensten dezelfde argumenten als voor de meeste ICT-diensten. Zo kunnen initiële investeringen beperkt worden, kunnen kosten veelal direct gerelateerd worden aan het daadwerkelijke gebruik, kunnen desinvesteringen ten gevolge van veroudering van de techniek beperkt worden en wordt de eigen organisatie niet belast met zaken die zich niet richten op de kernactiviteiten.

Met name ten aanzien van de veroudering van de technologie bestaan er risico's indien men alles zelf wil inrichten. Techniek en standaarden voor TTP-diensten en de toepassingen die daarvan gebruik maken, zijn nog steeds sterk in ontwikkeling.

Het zelf opzetten van TTP-diensten vergt zeer specifieke kennis die veelal moeilijk binnen de organisatie te vinden is. Het inhuren van externe kennis en opleiding zal noodzakelijk zijn, wil men zelf TTP-diensten inrichten.

Ten aanzien van de vraag of uitbesteding wenselijk is, heeft de overheid een specifieke rol in de maatschappij die aanleiding kan geven om eerder voor uitbesteding aan marktpartijen te kiesen dan voor zelf doen. Voordat men deze keuze maakt, dienen echter een aantal punten goed te worden overwogen. Daartoe zijn een 7-tal specifieke kernpunten genoemd die in overweging moeten worden genomen. De kernpunten hebben betrekking op de volgende vragen:

1. Beleid: Welke invloed heeft uitbesteding op de keuzemogelijkheid ten aanzien van het beleid binnen het domein (of beveiligingsniveau)?
2. Exclusiviteit: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de exclusiviteit van gegevens uit te besteden?
3. Integriteit: Is het wenselijk om een belangrijke beveiligingsdienst ten behoeve van de integriteit van gegevens, met name de digitale handtekening, uit te besteden?
4. Privacy: Is het vanuit privacy-oogpunt mogelijk om TTP-diensten uit te besteden?
5. Beschikbaarheid: Hoe zit het met de continuïteit van de dienstverlening bij uitbesteding?
6. Integratie: Is het mogelijk om diensten die zo geïntegreerd zijn met de organisatie uit te besteden?
7. Aansprakelijkheid: Welke invloed heeft uitbesteden op het aansprakelijkheids-vraagstuk?

Deze aspecten zijn afgezet tegen een 4-tal uitbestedingsvarianten:
1. Alles zelf doen
2. Delen uitbesteden
3. Maximaal uitbesteden met gebruik van besloten TTP-diensten
4. Maximaal uitbesteden met gebruik van openbare TTP-diensten

De eerste variant geeft een optimale invulling van de 7 kernvragen. Dit gaat echter gepaard met hoge initiële kosten, de genoemde risico's ten aanzien van de veroudering van de technologie en de beschikbare kennis.

De vierde variant beidt erg weinig flexibiliteit (ten aanzien van het beleid) en levert problemen ten aanzien van het daadwerkelijk te bereiken niveau van vertrouwen. Deze

scoort laag ten aanzien van de 7 kernvragen. Verder zullen ambtenaren individuele contracten moeten aangaan met de openbare TTP voor de levering van diensten.
De derde variant, waarbij de diensten grotendeels volgens de wensen van de Rijksoverheid worden opgezet, biedt duidelijk voordelen ten aanzien van het vierde scenario ten aanzien van de flexibiliteit en de 7 kernpunten. Dit mede aangezien het eenvoudiger mogelijk is om van meerdere aanbieders diensten af te nemen.

De tweede variant biedt de meeste flexibiliteit in combinatie met een beperking van de risico's ten aanzien van de initiële kosten, de veroudering van de technologie en de beschikbare kennis. Ook scoort deze variant goed op de 7-kernpunten.

7. Conclusies

In dit rapport is verslag gedaan van een onderzoek naar TTP-diensten binnen de Rijksoverheid. Ten aanzien van deze TTP-diensten komen wij tot de volgende hoofdconclusies:

- Conclusie 1: een raamwerk voor het bewijzen van de elektronische identiteit (authenticatie) is noodzakelijk voor de verdere ontwikkeling van betrouwbare electronische informatiediensten
- Conclusie 2: TTP-diensten bieden een uniform raamwerk voor betrouwbaarheidsdiensten ten behoeve van electronische communicatie en informatiediensten
- Conclusie 3: Er ontstaat een breed draagvlak voor het gebruik van TTP-diensten
- Conclusie 4: Ten aanzien van de inrichting van TTP-diensten binnen de Rijksoverheid scoort het Interdepartementale domein (scenario 3) het best
- Conclusie 5. De Rijksoverheid kan het beste delen van de TTP-diensten zelf opzetten en delen uitbesteden volgens variant 2
- Conclusie 6: de invoering van de niet-openbare TTP-diensten binnen de Rijksoverheid vraagt op het interdepartementale niveau een aantal strategische keuzes

In de volgende paragraaf wordt elk van deze conclusies uitgewerkt en toegelicht.

7.1 Conclusies

Conclusie 1: een raamwerk voor het bewijzen van de elektronische identiteit (authenticatie) is noodzakelijk voor de verdere ontwikkeling van betrouwbare electronische infomatediensten

Een aantal onzekerheden die in de elektronische interacties aanwezig zijn remmen de ontwikkeling: "hoe weet ik met zekerheid met wie ik communiceer?" én "hoe kan ik zorgen dat niemand meeleest én "hoe weet ik dat dit document echt is ". Om deze vragen te kunnen beantwoorden is een betrouwbaar raamwerk voor het bewijzen van de identiteit noodzakelijk: het authenticatieraamwerk.

Op dit moment wordt binnen de Rijksoverheid voor het bewijzen van elektronische identiteiten voornamelijk gebruik gemaakt van wachtwoordsystemen. Dit soort oplossingen voldoet niet meer aan de betrouwbaarheideisen in de situatie van complexe netwerken als Inter- en Intranetten. Er is een ander raamwerk noodzakelijk dat betrouwbaarheidsdiensten kan bieden tussen de eindpunten van de communicatie: de personen en informatiesystemen die daadwerkelijk met elkaar informatie uitwisselen. Zogenaamde end-to-end beveiliging.

Wil de Rijksoverheid nu en in de toekomst zakelijk gebruik maken van elektronische informatiediensten ter ondersteuning van de interne bedrijfsvoering van de overheid

dan moet een strategische keuze worden gemaakt voor een architectuur voor elektronische authenticiteit.

Conclusie 2: TTP-diensten bieden een uniform raamwerk voor betrouwbaarheidsdiensten ten behoeve van electronische communicatie en informatiediensten

TTP-diensten bieden een elegante raamwerk voor het bewijzen van de identiteit: het authenticatieraamwerk. De basis TTP-diensten zorgen voor een digitale identiteit.
Naast deze digitale identiteit bieden TTP-diensten ondermeer mogelijkheden voor het waarborgen van de exclusiviteit en integriteit van gegevens, sleutelbeheer en onweerlegbare bewijsvoering middels digitale handtekeningen.

De sterkte van het gebruik van TTP-diensten als basis van de betrouwbaarheid voor al deze toepassingen ligt in de uniformiteit. Een beperkt aantal TTP-diensten legt de basis voor het vertrouwen in de herkomst van berichten, de identificatie van personen ten behoeve van toegangsbeveiliging en het waarborgen van de integriteit en exclusiviteit van informatie. Het nu structureel aanpakken van maatregelen ter bevordering van de betrouwbaarheid voorkomt problemen op dit gebied in de toekomst.

Conclusie 3: Er ontstaat een breed draagvlak voor het gebruik van TTP-diensten

Er ontstaat momenteel een wereld van vele TTP-diensten, zowel gesloten als open. Gesloten diensten vinden in we in min of meer gesloten vertrouwensdomeinen als dealernetwerken, Internet Service Providers (SURFnet), multinationals (Shell), banken en zelfs overheden (Canada, Australië). Daarnaast ontstaan er publieke TTP-diensten die voor elke burger en rechtspersoon toegankelijk zijn. Voorbeelden zijn: PTT post die met Keymail een electronische variant van aangetekende mail; KPN Telecom en Roccade die de diensten van het Amerikaanse VeriSign in Nederlands wil gaan leveren en Enschede/SdU die TTP-diensten gaat leveren in combinatie met chipcards.

Dit betekent dat de Rijksoverheid niet alleen staat in het gebruik van TTP-diensten en biedt mogelijkheden om op grond van de zelfde structuren en technieken op betrouwbare wijze te communiceren met burgers, organisaties en overheden in Nederland en het buitenland.

Conclusie 4: Ten aanzien van de inrichting van TTP-diensten binnen de Rijksoverheid scoort het Interdepartementale domein (scenario 3) het best

Tijdens de studie zijn er de volgende scenario's onderkend:
- één domein per bedrijfsproces
- één domein per departement
- één interdepartementaal domein
- één RO-domein

Het eerste scenario is het meest complexe scenario, maar biedt de meeste flexibiliteit om specifieke wensen van bedrijfsprocessen in te vullen. Dit scenario biedt echter geen RO-brede en geen departementbrede base-line voor vertrouwen. Het sluit niet aan bij de

bestaande bestuurlijke structuren binnen departementen en de RO. Dit scenario zou het gevolg kunnen zijn van de nul optie als geschetst in hoofdstuk 3.
Het vierde scenario is het in theorie het minst complexe scenario, maar het sluit niet aan bij de bestaande bestuurlijke structuren met eigen departementale verantwoordelijkheden. Dit scenario biedt wel een RO-brede baseline voor vertrouwen.
Het tweede scenario biedt de beste mogelijkheid om specifieke wensen per departement in te vullen. Dit scenario biedt echter geen RO-brede baseline voor vertrouwen.
Het derde scenario sluit van de vier het best aan bij de bestaande bestuurlijke structuren binnen de RO. Er kan optimaal gebruik worden gemaakt van beschikbare kennis en middelen. Dit scenario biedt een RO-brede baseline voor vertrouwen met daarop beperkte variatie per departement. Indien men overeenstemming heeft over de gezamenlijke structuren, biedt dit scenario verder de mogelijkheid dat elk departement zelf bepaalt wanneer men overgaat tot de daadwerkelijke implementatie binnen het departement.

Conclusie 5. De Rijksoverheid kan het beste delen van de TTP-diensten zelf opzetten en delen uitbesteden volgens variant 2

Aangezien er nu reeds meerdere TTP-dienstenaanbieders en productleveranciers zijn, is het mogelijk om (delen van) de dienstverlening uit te besteden aan derden.

De aspecten die daarbij spelen zijn zijn afgezet tegen een 4-tal uitbestedingsvarianten:
1. Alles zelf doen
2. Delen uitbesteden
3. Maximaal uitbesteden met gebruik van besloten TTP-diensten
4. Maximaal uitbesteden met gebruik van openbare TTP-diensten

De eerste variant geeft een optimale invulling van de diensten. Dit gaat echter gepaard met hoge initiële kosten, risico's ten aanzien van de veroudering van de technologie en de beschikbare kennis.

De vierde variant biedt erg weinig flexibiliteit (ten aanzien van het beleid) en levert problemen ten aanzien van het daadwerkelijk te bereiken niveau van vertrouwen. Verder zullen ambtenaren individuele contracten moeten aangaan met de openbare TTP voor de levering van diensten.
De derde variant, waarbij de diensten grotendeels volgens de wensen van de Rijksoverheid worden opgezet, biedt duidelijk voordelen ten aanzien van de vierde variant op deze punten. Dit mede aangezien het eenvoudiger mogelijk is om van meerdere aanbieders diensten af te nemen.

De tweede variant biedt de meeste flexibiliteit in combinatie met een beperking van de risico's ten aanzien van de initiële kosten, de veroudering van de technologie en de beschikbare kennis.

Conclusie 6: de invoering van de niet-openbare TTP-diensten binnen de Rijksoverheid vraagt op het interdepartementale niveau een aantal strategische keuzes

De invoering van de niet-openbare TTP-diensten binnen de Rijksoverheid vraagt van het management op het interdepartementale niveau een aantal strategische keuzes:

- het bepalen van een gemeenschappelijk stelsel van betrouwbaarheidseisen op het gebied van de interdepartementale communicatie en beveiliging binnen de Rijksoverheid;
- bepalen welk scenario gevolgd wordt bij de invoering van TTP-diensten binnen de Rijksoverheid;
- het bepalen van de beleidslijnen ten aanzien van "zelf doen of uitbesteden".

Beleidslijnen ten aanzien van de invoering van de niet-openbare TTP-diensten binnen de Rijksoverheid dienen ook afgestemd te zijn op andere beleidsbeslissingen, onder andere op het informatiebeveiligingsbeleid en het ICT-beleid.

7.2 Aanbevelingen

Wij bevelen u het volgende aan:

Aanbeveling 1: Om nu een strategische keuze te maken over het gebruik van TTP-diensten binnen de Rijksoverheid.

Geen keuze maken betekent dat men overvallen zal worden door zowel interne als externe ontwikkelingen. Reeds nu zien we op verschillende plekken binnen de Rijksoverheid losstaande initiatieven die gemakkelijk kunnen leiden tot geïsoleerde 'beveiligde eilanden'. Op termijn zal dit kunnen leiden tot extra kosten. Gezien de initiatieven in de markt kan dit ook leiden tot het beeld van een overheid die achteropraakt bij het leveren van een betrouwbare electronische informatievoorziening.

Aanbeveling 2: Om de TTP-diensten en voorzieningen zo veel mogelijk gecoördineerd, gezamenlijk in te richten volgens scenario 3: het Interdepartementale domein.

Voor efficiënte betrouwbare communicatie tussen de verschillende departementen en tussen de Rijksoverheid en externe vertrouwensdomeinen is dit scenario aan te bevelen. Het sluit goed aan bij de bestaande structuren binnen de Rijksoverheid, biedt departementen de mogelijkheid eigen variaties aan te brengen terwijl het toch uitwisselbaarheid tussen departementen garandeert. De mogelijkheden tot betrouwbare communicatie met externe domeinen is door de aanwezigheid van de interdepartementale component efficiënt te regelen. Ook qua kosten komt dit scenario goed uit de vergelijking. Indien men overeenstemming heeft over de gezamenlijke structuren, biedt dit scenario verder de mogelijkheid dat elk department zelf bepaalt wanneer men overgaat tot de daadwerkelijke implementatie binnen het departement.

Aanbeveling 3: Beheer het veranderproces zowel op interdepartementaal als departementaal niveau.

- Zorg voor een orgaan op hoog interdepartementaal niveau dat als stuurgroep zal fungeren;

- Laat een gezamenlijk interdepartementale werkgroep de beleidsuitgangspunten en randvoorwaarden opstellen;
- Zet een projectorganisatie op (interdepartementaal en/of departementaal) rondom de invoering van de niet-openbare TTP-diensten;
- Biedt departementen de mogelijkheid om op eigen snelheid tot daadwerkelijke invoering over te gaan

Aanbeveling 4: Om een combinatie van zelf doen en uitbesteden te kiezen volgens variant 2: delen uitbesteden.

Uitbesteding biedt niet alleen voordelen ten aanzien van de (financiële) risico's, maar zal daarnaast ook een stimulans zijn voor de Nederlandse TTP-markt.
Daarbij wordt aanbevolen om zeker uitbesteding te overwegen van die componenten waarbij de technologie een risico vormt (met name de CA dienst). En om die componenten die cruciaal zijn voor het beveiligingsniveau en/of fraudegevoelig zijn (met name sleutelbeheer) zelf te beheren.
De registratiedienst (RA) is verder dusdanig geïntegreerd met de organisatie dat uitbesteding daarvan zorgvuldig overwogen moet worden.

Aanbeveling 5: Om enkele proefprojecten te starten waarbij verschillende TTP-toepassingen gebruikt worden.

TTP-diensten zijn geen doel op zich maar lever ondersteunen een scala van toepassingen. Daarom is het belangrijk om, naast het opzetten van de (basis-) TTP-diensten ook enkele toepassingen te introduceren. Mogelijke concrete toepassingen zijn beveiligde e-mail, telwerken, de electronische adressengids en beveiliging van het overheidsintranet.

Bijlage 1: geraadpleegde documentatie

Brondocumenten:

[aeo] *Actieprogramma Elektronische Overheid.* Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1998.

[a&k] *Handleiding A&K-Analyse.* Den Haag: ACIB, juli 1996.

[burton] *Network Strategy Report Public Key Infrastructure Architecture*, The Burton Group, v1, 9 juli 1997

[cert] *Overview of Certification Systems: X.509, CA, PGP and SKIP*, MCG, 1998

[dutler] *Met recht een TTP!, Een onderzoek naar juridische modellen voor een Trusted Third Party*, Anne-Wil Duthler, Kluwer, 1998.

[goc] *Government of Canada Public Key Infrastructure – White Paper*, February 1998

[hand] *Geschriften en handtekening, een achtehaald concept?*, S. Huydecoper, R. Van Esch, ITeR reeks nr. 7, Samson bedrijfsinformatie, 1997

[hand2] *De juridische status van de Digitale Handtekening*, S. Van der Hof, ITeR reeks nr. 7, Samson bedrijfsinformatie, 1997

[hand3] *Proposal for a European Parliament and Council Directive on a common ramework for electronic signatures*, European Commission, 1998

[intra] Haalbaarh*eidsstudie Overheidsintr@net;* Eindrapport. Den Haag: Het Expertise Centrum, 1998.

[istev] *Legal Issues of Evidence and Liability in the Provision of Trusted Service (CA and TTP services)*, ISTEV, Final report, oktober 1998

[kpmg] *Eindrapportage Nationaal TTP-project*, Ministerie van Economisch Zaken, Ministerie van Verkeer en Waterstaat, KPMG EDP Auditors N.V , 1 maart 1998.

[pkcs] *PKI protocols en definities*, Public Key Cryptography Standards, RSA Corporation

[pkix] *Internet Public Key Infrastructure series (PKIX)*, Internet Drafts, IETF

[vir] *Voorschrift Informatiebeveiliging Rijksdienst*, Ministerie van Binnenlandse Zaken, 1994.

[vir2] *Handboek Informatiebeveiliging Rijksdienst*, Ministerie van Binnenlandse Zaken, 1994.

Overigen:

- Verslagen en documenten van de werkgroepen binnen het nationale TTP.NL project;
- Productinformatie, white-papers en overige informatie van TTP-diensten en productenleveranciers.

Bijlage 2: Kostenberekening

In deze bijlage wordt aangegeven welke aspecten zijn meegenomen in de kostenbepaling en welke buiten beschouwing zijn gelaten.

Relatie met de scenario's van hoofdstuk 4
Voor de kostenberekening is uitgegaan van het derde scenario van hoofdstuk 5: het interdepartementale domein. Het aantal CA's en de mogelijkheid om CA's te delen is sterk afhankelijk van de keuze ten aanzien van het scenario. Met name bij het interdepartementale domein, zijn er zeer goede mogelijkheden om CA's gezamelijk in te richten voor meerdere departementen. Ook kan bespaard worden op de extra infrastructuur die noodzakelijk is om de continuïteit van de CA dienstverlening te garanderen. Meerdere departementale CA's kunnen één uitwijk-CA opzetten voor noodgevallen. Dit is veelal niet mogelijk bij scenario 2 aangezien het beleid (en dus de inrichting van de diensten) tussen de departementale CA's in dat geval te sterk kan verschillen.

Relatie met de uitbestedingsvarianten
Scenario 3 is voor drie uitbestedingsvarianten doorberekend: alles zelf doen, delen uitbesteden en maximaal uitbesteden bij een openbare TTP. Bij alles zelf doen zijn verder twee uiterste situaties geschetst: één waarbij maximaal door de departementen wordt samengewerkt (optimaal delen van infrastructuur) en een situatie waarbij elk departement een eigen infrastructuur opzet.
Opgemerkt moet worden dat bij de variant waarbij delen worden uitbesteed, de kostprijs per werkplek/medewerker strerk wordt bepaald door de contractonderhandelingen. Met name bij zeer grote volumes (bijvoorbeeld voor een digitaal identiteitsbewijs) kan de kostprijs (veel) lager uitvallen dan de hier gehanteerde 40 gulden.

Basis voor de kostenberekening
De kostenberekeningen zijn gebaseerd op de belangrijkste basisdiensten die binnen een vertrouwensdomein ingericht moeten worden: de CA en de RA. Voor de overige basisdiensten is een kostenschatting in dit stadium nagenoeg onmogelijk. Bij enkele professionele CA producten worden de DS en KM meegeleverd. De KM en PUA's (de toepassingen als e-mail clients) kunnen, afhankelijk van de wensen, in prijs variëren tussen de 0 en vele honderden guldens per werkplek.
Er is uitgegaan van 100.000 ambtenaren binnen de Rijksoverheid verdeeld over 13 departementen.

Personele kosten
Ten aanzien van de personele kosten is een richtprijs van 100.000 per fte per jaar aangehouden. De gegeven aantallen fte's kunnen veelal ingevuld worden door bestaande functionarissen in deeltijd. Bijvoorbeeld bij automatiserings-/helpdeskmedewerkers of medewerkers van personeelszaken.

De CA

Voor het leveren van de CA diensten zijn verschillende producten op de markt beschikbaar. Daarbij zijn grofweg twee categorieën te onderscheiden: de 'instap' producent en de professionele producten. De instap producten zijn niet geschikt voor grote volumes (enkele duizenden gebruikers) en bieden onvoldoende functionaliteit en betrouwbaarheid voor het beoogde doel.
De professionele producten variëren uiteraard in prijs. Belangrijk is dat bij de meeste producten zowel betaald wordt voor het product zelf als een prijs per uitgegeven (actief) certificaat.

Voor de prijs van de professionele producent zelf, inclusief hardware platform, wordt hier een richtbedrag van 250 kfl. aangehouden. Veelal is echter redundantie gewenst om de beschikbaarheid van de CA diensten te kunnen garanderen.
De prijs per certificaat is sterk afhankelijk van het volume. We houden een richtprijs aan van 40 gulden per certificaat in voor de 'delen uitbesteden' variant en 100 gulden voor het uitbesteden bij een openbare TTP[15]. In het geval dat de Rijksoverheid alles zelf doet, is de kostprijs per certificaat opgenomen als een onbeperkte licentie.

De kosten voor de instandhouding worden begroot op 10% van de aanschafprijs op jaarbasis.

Voor het (technisch) beheer van de CA wordt uitgegaan van 2 fte's waarbij in gedachten moet worden gehouden dat de CA diensten mogelijk 24 uur per dag, 365 dagen per jaar beschikbaar moeten zijn.

De RA

De kosten voor de RA dienst zijn voornamelijk personele kosten. Aangezien de RA dicht bij de gebruikers van de diensten staat, het is het loket voor de medewerkers, dient de RA toegankelijk te zijn voor de medewerkers. Voor een optimale verdeling van de RA 'loketten' maakt het daarom niet veel uit welk scenario gekozen wordt.

Materieel
Bij de CA producten worden veelal losse RA modules aangeboden. De gemiddelde kosten daarvan worden hier begroot op 25 kfl per RA werkplek.

Personeel
Hiervoor is de volgende formule gebruikt[16]:
Per mutatie is gemiddeld ongeveer 1 uur nodig. Op jaarbasis vinden mutaties plaats op 40% van het volume[17]. Hiermee is ongeveer 1 fte noodzakelijk per 4000 medewerkers (1 fte = 1600 uur).

[15] PTT-post hanteert momenteel een prijs van 120 gulden per certificaat.
[16] Deze berekening is conservatief; dit is mede afhankelijk van de verificatieprocedures en mogelijke combinatie daarvan met andere processen (b.v. uitgifte bedrijspas)
[17] Tijdens de introductie van de TTP-diensten zal dit percentage uiteraard 100% bedragen.

Voorbereidingskosten: projectorganisatie en beleidsontwikkeling
De voorbereidingskosten zijn relatief onafhankelijk van de scenario's en varianten. Het betreft de activiteiten die noodzakelijk zijn voor de interdepartementale afstemming en definitie van de architectuur, de beleidsontwikkeling, specificatie en aanbestedingstrajecten.

Voor specifieke kennis wordt uitgegaan van de inhuur van 3 externe deskundigen op TTP-gebied (deeltijd; technisch/juridisch). Daarnaast zal de projectorganisatie kunnen bestaan uit medewerkers van geïnteresseerde departementen die op basis van detachering participeren. Verder wordt uitgegaan van een doorlooptijd van 3 jaar.

De kosten hiervoor worden beraamd op 2.25 miljoen gulden.

Overzichten
In de volgende tabellen en grafieken zijn de kosten weergegeven. De eerste pagina geeft een vergelijking tussen de verschillende scenario's. In de daaropvolgende grafieken is dit grafisch weergegeven. Tevens zijn de kosten omgerekend naar een kostprijs per werkplek (uitgaande van 100.000 werkplekken).
Tot slot zijn de berekeningen per scenario afzonderlijk in detail weergegeven.

Resume

Vergelijking van de kosten voor drie uitbestedingsvarianten van het "Interdepartementale domein" scenario.
De kosten zijn onderverdeeld in:
- Investeringskosten (eenmalig)
- Jaarlijkse kosten, onderverdeeld in:
  - beheerskosten
  - personele kosten
  - kosten per werkplek/medewerker (kosten voor certificaten)

Variant 1: Alles zelf doen.
Zowel CA's als RA's worden zelf ingericht. Producten worden aangeschaft inclusief onbeperkte licentie voor het verstrekken van certificaten. De kosten zijn verder onderverdeeld in een scenario waarbij maximaal door de departementen wordt samengewerkt (delen van infrastructuur) en een scenario waabij elk departement een eigen infrastructuur opzet. Dit levert de volgende kostenplaatje op:

	Maximaal samenwerken	Minimaal samenwerken
Investeringskosten	1.500.000	8.400.000
Jaarlijkse kosten:		
Beheerskosten	150.000	890.000
Personele kosten (fte's)	29 (2.900.000)	53 (5.300.000)
Kosten per werkplek/medewerker	0	0

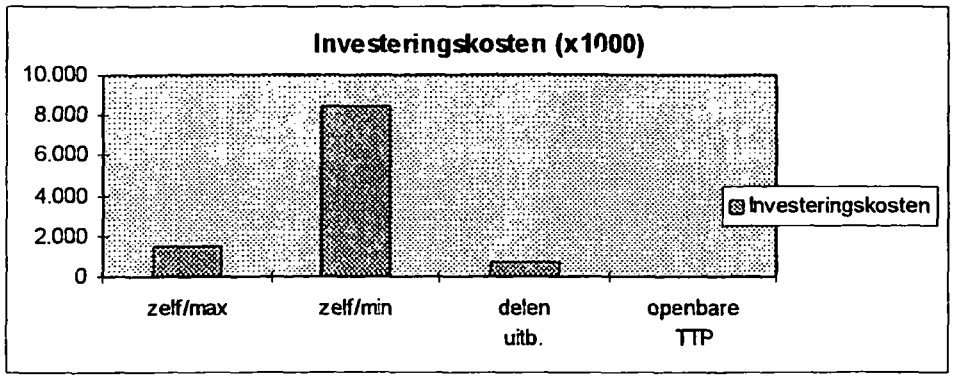
Variant 2: Delen uitbesteden.
De CA diensten worden uitbesteed aan een externe dienstenleverancier. De RA's worden zelf ingericht. Producten voor de RA worden (via de aanbieder) aangeschaft.

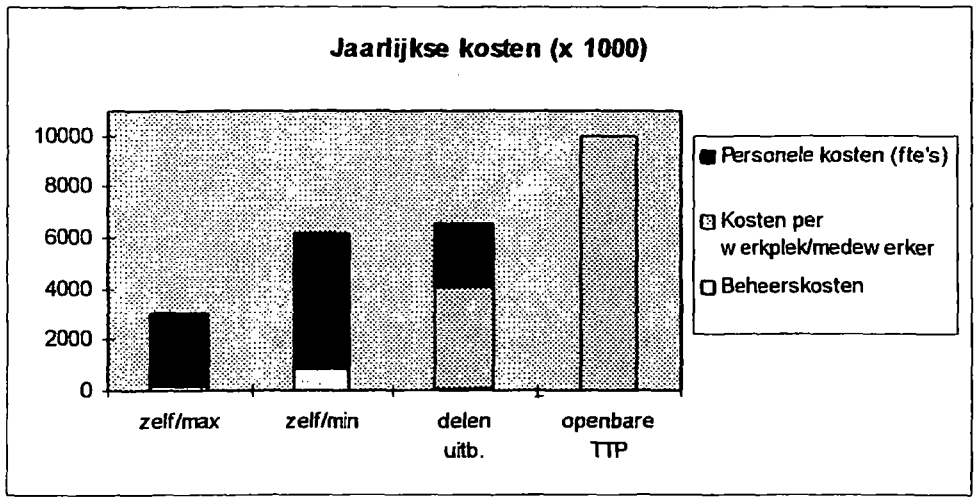
Investeringskosten	675.000	
Jaarlijkse kosten:		
Beheerskosten	63.000	
Personele kosten (fte's)	25 (2.500.000)	
Kosten per werkplek/medewerker	4.000.000	(fl 40,- per certificaat)

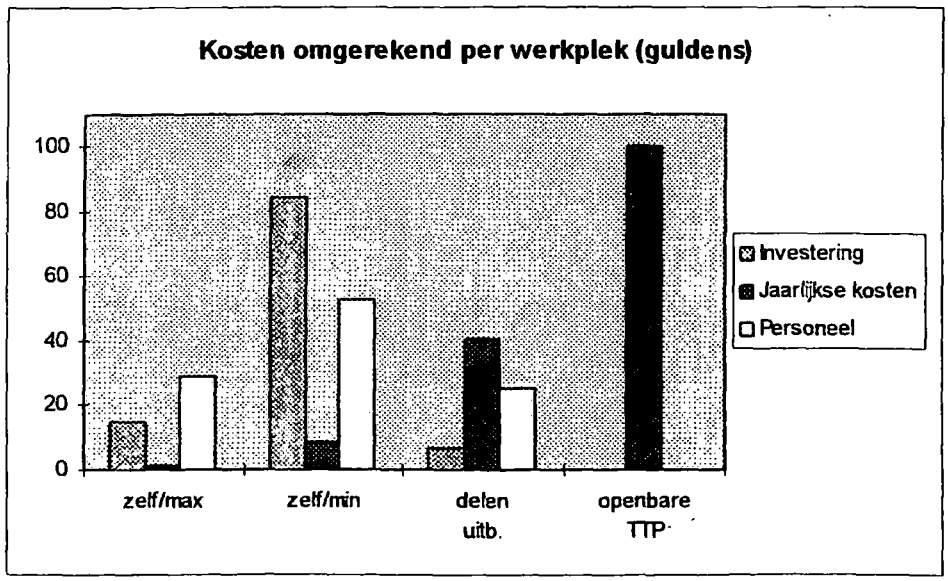
Variant 3: Maximaal uitbesteden bij een Openbare TTP.
De CA en RA diensten worden uitbesteed aan een externe dienstenleverancier.

Investeringskosten	0	
Jaarlijkse kosten:		
Beheerskosten	0	
Personele kosten (fte's)	0	
Kosten per werkplek/medewerker	10.000.000	(fl 100,- per certificaat)

Resume


Investeringskosten (x1000)
10.000
8.000
6.000
4.000
2.000
0
zelf/max
zelf/min
delen uitb.
openbare TTP
Investeringskosten


Jaarlijkse kosten (x 1000)
10000
8000
6000
4000
2000
0
zelf/max
zelf/min
delen uitb.
openbare TTP
Personele kosten (fte's)
Kosten per werkplek/medewerker
Beheerskosten


Kosten omgerekend per werkplek (guldens)
100
80
60
40
20
0
zelf/max
zelf/min
delen uitb.
openbare TTP
Investering
Jaarlijkse kosten
Personeel

Kostenindicatie voor het interdepartementale domein, zonder uitbesteding

Interdepartementaal

Investeringskosten

	Prijs	Aantal	Kosten	
CA product	250	1	250	redundant tbv beschikbaarheid is minder
RA product per werkplek	25	2	50	relevant gezien de beperkt aantal mutaties
				registreert alleen departementale CA's en externe domeinen
Totaal investeringskosten			*300*	

Instandhoudingskosten

10% van de investeringskosten	30

Personele kosten

	fte's	
Beheer CA	2	
RA	0,1	
Totaal personele kosten	*2,1*	*fte's*

Departementaal

Investeringskosten

	Maximale samenwerking			Minimale samenwerking			
	Prijs	Aantal	Kosten	Prijs	Aantal	Kosten	
CA product	250	2	500	250	26	6.500	redundant tbv beschikbaarheid
RA product per werkplek	25	25	625	25	25	625	
Onbeperkte licentie	100	1	100	100	13	1.300	
Totaal investeringskosten			*1.225*			*8.425*	

Instandhoudingskosten

	Prijs	Aantal	Kosten			
10% van de investeringskosten			123			843

Personele kosten

	fte's		fte's	
Beheer CA	2		26	
RA	25		25	
Totaal personele kosten	*27*	*fte's*	*51*	*fte's*

Kosten per werkplek/medewerker

	Prijs	Aantal	Kosten	
certificaten	0	100000	0	Bij het zelf doen is dit in de onbeperkte licentie opgenomen (investering)

Kostenindicatie voor het Interdepartementale domein, uitbesteding CA; RA zelf inrichten.

Interdepartementaal

Investeringskosten

	Prijs	Aantal	Kosten	
CA product	0	0	-	redundant tbv beschikbaarheid is minder rele
RA product per werkplek	25	2	50	registreert alleen departementale CA's en ext
Totaal investeringskosten			*50*	

Instandhoudingskosten

10% van de investeringskosten	5

Personele kosten

	fte's	
Beheer CA	0	
RA	0,1	
Totaal personele kosten		*0,1 fte's*

Departementaal

Investeringskosten

	Maximale samenwerking			Minimale samenwerking			
	Prijs	Aantal	Kosten	Prijs	Aantal	Kosten	
CA product	0	0	-	0	0	-	redundant tb
RA product per werkplek	25	25	625	25	25	625	
Onbeperkte licentie	0	0	-	0	0	-	
Totaal investeringskosten			*625*			*625*	

Instandhoudingskosten

	Prijs	Aantal	Kosten			
10% van de investeringskosten			63			63

Personele kosten

	fte's		fte's	
Beheer CA	0		0	
RA	25		25	
Totaal personele kosten		*25 fte's*		*25 fte's*

Kosten per werkplek/medewerker

	Prijs	Aantal	Kosten
certificaten	40	100000	4000

Kostenindicatie voor het Interdepartementale domein, maximaleuitbesteding bij openbare TTP

Interdepartementaal

Investeringskosten

	Prijs	Aantal	Kosten	
CA product	250	0	-	redundant tbv beschikbaarh
RA product per werkplek	25	0	-	registreert alleen departeme
Totaal investeringskosten			-	

Instandhoudingskosten

10% van de investeringskosten	-

Personele kosten

	fte's
Beheer CA	0
RA	0
Totaal personele kosten	*0 fte's*

Departementaal

Investeringskosten

	Prijs	Aantal	Kosten	
CA product	250	0	-	
RA product per werkplek	25	0	-	
Totaal investeringskosten			-	

Instandhoudingskosten

	Prijs	Aantal	Kosten	
10% van de investeringskosten			-	

Personele kosten

	fte's		
Beheer CA	0		
RA	0		
Totaal personele kosten	*0*		*fte's*

Kosten per werkplek/medewerker

	Prijs	Aantal	Kosten	
certificaten	100	100000	10000	per jaar

Bijlage 3: Verslag van het Bezoek aan Canada

Background

Nortel had some ideas about PKI back in 1993. Department of Defence (DoD) and Canadian Security Facility (CSF) put together a Public Key Infrastructure (PKI) project to develop these ideas. In 1995, 7 departments financed the PKI project for securing sensitive but unclassified information
By that time there was a 'blind fate' that PKI would be a good way forward to the 'paperless office'. Also WGs on e-commerce and e-government came up with related requirements for security services. PKI was seen as a perfect enabler.
Government of Canada (GoC) invested 7 million in the Entrust product development. The GoC does not feel obliged to use only Entrust products in the future. It should be an open system. Results are submitted to standardisation bodies like ISO and IETF (PKIX). PKIX is the main guideline for the GoC. Products should be "PKIX complaint". Apart form the 7 million-dollar investment Entrust licences are negotiated for the GoC PKI members.

The Interdepartmental PKI taskforce started in April 1998. Before that date discussion focussed on the need for legislation or regulation by means of policy. The conclusion by the end of 1997 was that policy was the right instrument. It was also concluded that liability was subject to risk-management and not a inhibitor.
The first CP was published in 1997 but revised in March-August 1998. Version 3 was finalised in December 1998. Both CP and CPS are based on the IETF PKIX standards. Extensions have been necessary.

Work on the TB policy started in August 1998 and is now coming to a last review. Work on the cross-certification guideline document has started in January 1999. Internal release is expected in April 1999. External release not before the end of 1999.

The GoC should be delivered by the end of 1998, but has been delayed. The GoC approach towards PKI rollout can be described as "If we build it, they (the departments) will use it".

PKI offers a robust solution for (at maximum) low grade classified information (~ sensitive but unclassified). It enables a uniform approach towards IT security, but applications are not directly included. GoC intend to use PKI solutions also for some kinds of classified information like cabinet communications.

Requirements

The goal was to set up a PKI for GoC use (within GoC). So a private PKI, not a public. But expansion towards private enterprises and citizens is not excluded. The way forward however is not clear.
There was a key requirement that Key Recovery was to be included in the system for corporate information while maintaining the Digitale Signature integrity. (rem: this requirement form the bases for the Entrust double key-pair solution).

Other requirements include:
- Support of multiple policies (multiple CPs)
- Use of 'approved products' through an approval team

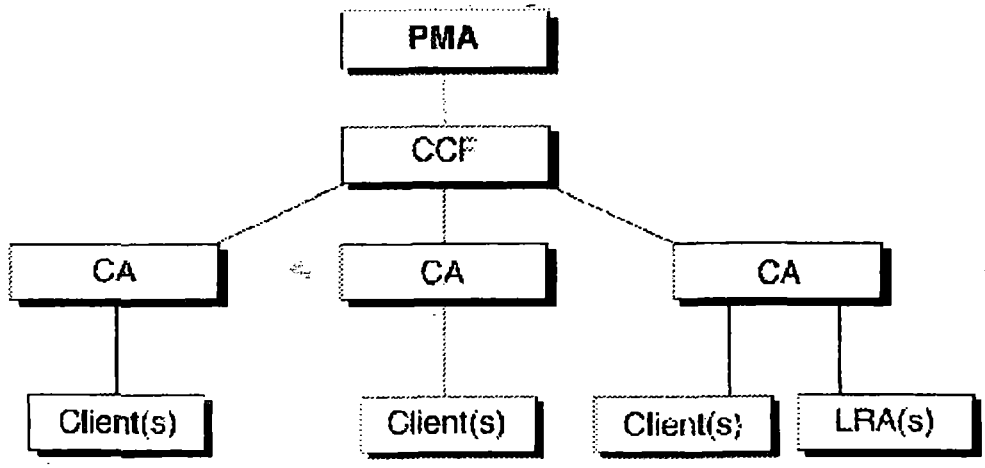
- Availability of a key-rollover system (key updates)
- Bridge-CA model for cross-certification through a 'top-CA' (the Canadian Central Facility (CCF).

The goal was to have COTS products for the GoC PKI. Development was and is in close relation with Entrust. But other suppliers should be able to compete.
The foreseen evolution of the PKI infrastructure towards the Privilege Management Infrastructure (PIM) requires the addition of authorisation and labelling of information. Some work is done in this field. Labels will not be time-sensitive.
The extensive use of XML is foreseen within the PKI. It will support workflow processing and form signing.

Organisation

At the top of the organisation of the GoC PKI is the President of the Treasure Board.
Next in the hierarchy is the Policy Management Authority (PMA). The PMA gives orders to the Canadian Central Facility (CCF). The CCF is a highly technical organisation that makes no policy or political decisions but only executes orders form the PMA. This is to avoid disputes.

The tasks of the CCF are limited to certifying underlying Certification Authorities (CA's) certification with external domains. So it forms a root-CA. CA's are at the departmental level. Each CA has one or more Local Registration Authorities assigned to it. This model is depicted below.



The PKI uses public X.500 services. The content is a problem due to privacy regulations. General data on GoC employees may be made available publicly. But (eventual) data on citizens not. External employees (temp workers) are required to sign a contract with Terms and Conditions in which they will give their consent to this.

Lower government (municipal, province level) are involved but are waiting for the moment. Still one successful project has been implemented using PKI. Return on investment was 1 year with a 90% increase in service time for customers.

There are some 15 WG involved for a total of 300 people. The inter departmental PKI workforce is 15 man strong and is expected to grow to 20 persons. Many discussions were still needed on technical and operational issues. They were late in discovering the essential role of the directory service. Started as a PKI activity, the directory service is now part of a much broader GoC WG. This reflects the fact that the directory service will be used for much more than the PKI alone.

Certificate Policy development has only started in early 1998 and is now finished with the publishing of the 4 levels.

PKI introduction strategies

There are two general strategies emerging. Within the more 'PKI aware' departments the introduction of PKI starts with the forming of a PMA like policy body which defines the departmental policy and procedures.
For the other departments the need for (PKI enabled) secured applications seem to be the drive behind the PKI implementation. This is a much more business driven approach.
The marketing strategy could be to fill in the PKI need when felt by a department rather than selling PKI.

CA policy

They have defined 4 levels of CP's to manage the different risks. They are:
1. rudimentary assurance
2. basic assurance
3. medium-level assurance
4. high assurance

The decision on which CP level to use lies within the departments. The developed CPs are not mandated but examples that could be used by departments. The CPs are mandated in one case: the CCF root must confirm to these CPs.

Each CP has a different liability paragraph. The amounts mentioned must be seen as recommended minimal amounts. Departments may accept higher levels of liability but do so at their own risk. Claims are paid from a central fund in which each department contributes according to a certain key factor. Liability is restricted to the CA operation and services. Applications are explicitly excluded from liability. CA operations are self-insured by the GoC.

Applications are expected to be CP aware so they can act according to the certificate policy encountered in a certificate. If they are not, this must be dealt with in policies and procedures. They expect that the defined P level 3 will be the GoC general level for certificates. Level 3 is the medium-level assurance CP. There is no clear view on the issue of exchanging information between different CP levels. It is assumed that a department that receives a certain level certificate will deal with it according to the associated CP.

Treasure Board Policy

The PKI taskforce felt (and got feedback) that the CP was not the right instruments to be implemented by departments. Therefore they started the development of the Treasure Board policy document (TB). This is a "Policy for Public Key Infrastructure Management". Management bodies are located within each department that should implement the policy. The TB will be sent to 58 departments and bodies. The development of the TB took ca. 4 months. The TB is based on the CPs but contains only the essential, mandated parts.
The TB policy descibed what departments must do to implement the CPs. It is a Treasury Board policy that is imposed upon participating departments. Is follows the 'standard' GoC policy process. Departments should use the TB policy, not the CP. The CP is to be used by CA's.
An introduction on PKI is included within the TB policy to create awareness. This in not normally done in TB policy documents. The TB policy also explains the difference between CP and CPS. The developed CPs are models, each department has to develop it's own CP in theory. They may however adopt one or more of the model CPs.

Two model agreements are included: one for internal GoC employees and one for external personnel. External personnel have to sign an agreement in which the Terms and Conditions are explicitly accepted. This is essential for limiting the liability. GoC personnel have to be informed of the Terms and Conditions.

Departments may buy CA services form external service providers but the responsibility for the service remains with the Department. They have to set up a "virtual CA" with CPS. They may also take services from another Departments' CA and adopt their CA's practises.

All back-up key material must remain within Canada. But a CA supplier may well be a foreign company. All certificates must be issued in the name of Her Majesty. Each CA must operate a repository. Repositories of all CA's must be interoperable and be registered. Disclosure of private confidentiality keys only with the consent of the owner or when required by law. There is no requirement to use GoC generated keying material only in case of non-GoC employees. Self-generated private keys are not stored for key recovery.

All CA's are subject to their Departments' internal audit. TB monitors compliance to CP through the internal audit reports.
The GoC has no plans to seting up a CA/TTP licensing scheme.

Costs

The current cost for PKI is 75$ per seat. This has to be reduces through central GoC licensing.

Community

The discussion whether or not the GoC PKI will deliver CA services to citizens is still open. A decision is expected this year (based on...?).

Business case
The killer-application will be secure e-mail according to GoC. The final scope of the PKI will be to achieve an infrastructure for authorisation called the Privilege Management Infrastructure (PIM).

At this moment there is a sound basis for marketing PKI as the basic infrastructure for a broad range of secure applications.
In an example project application of PKI resulted in vast paper savings and better (faster) services delivery to customers.

Lessons learned

- Technology and policy go hand in hand with PKI.
- Avoid marketing PKI as a (set of) end-user application(s). PKI enables secure end-user applications, it does not include them. The marketing strategy could be to fill in the PKI need when felt by a department rather than selling PKI.
- Many application-related problems are brought forward to the PKI taskforce. These issues should be isolated and dealt with elsewhere (e.g. archiving digitised data processing).
- The development of a CPS model (as opposed to a CP model) has been proposed but was rejected. The diversity between the departments is too big to accommodate for this.
- Don't exaggerate liability issues. They are not so problematic as often thought.
- The CP requires close collaboration between lawyers and technical specialists.

Bijlage 4: TTP modules

TTP diensten voor de rijksoverheid

gave

1. **TTP-MODULES** .....

1.1 INLEIDING .....
1.2 TTP-BASISMODULES .....
1.3 OPTIONELE TTP-MODULES .....

1. TTP-modules

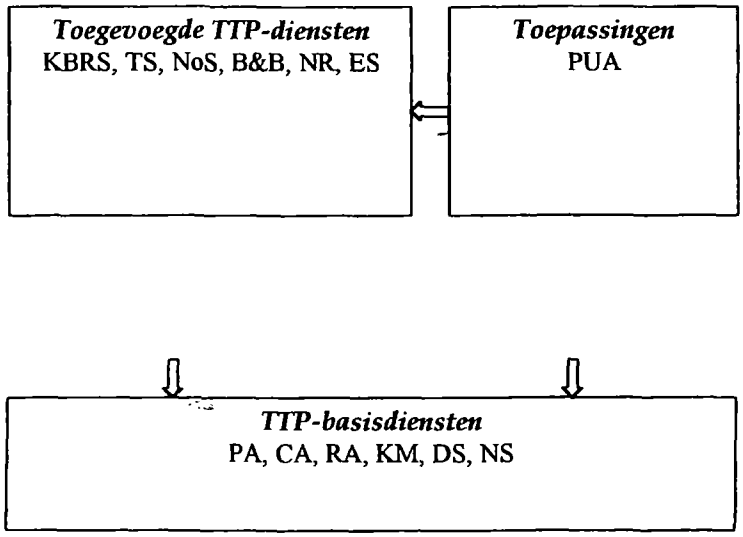
1.1 Inleiding

Deze bijdrage geeft een overzicht van de diverse TTP-diensten op een modulaire wijze. Op deze manier wordt inzichtelijk gemaakt welke specifieke kenmerken en eisen verbonden zijn met een bepaalde TTP-dienst. Hiermee kunnen beslisprocessen ten aanzien van zelf doen of uitbesteden worden ondersteund. Tevens biedt de lijst een gedetailleerd inzicht in de verschillende diensten voor diegenen die betrokken zijn bij het specificeren en inrichten van diensten binnen de organisatie.

Een aantal van de TTP modules dient ter ondersteuning van de essentiële processen zoals het uitgeven en intrekken van certificaten. Deze modules dienen dus aanwezig te zijn binnen elke domein dat gebruik maakt van TTP diensten. Deze modules hebben de status 'basis'.

Andere TTP modules worden gebruikt voor het leveren van diensten die niet essentieel zijn maar toegevoegd kunnen worden aan het domein: de toegevoegde TTP-diensten. Deze modules hebben de status 'optioneel'.

Dit is in onderstaande figuur weergegeven.



De volgende modules worden beschreven:

De basis TTP-diensten

PA, de Policy Authority

CA, de Certification Authority

KM, de Key Manager

RA, de Registration Authority

DS, de Distribution Service

NS, de Naming Service

De toepassinggen

PUA, de Public Key User Agent

De toegevoegde TTP-diensten (optioneel)

KBRS, de Key Backup and Recovery Service.

TS, de Time Stamping service

NoS, de Notary Service

B&B, de Bewijs en Bewaar dienst

NR, de Non-repudiation Service

ES, de Exclusiviteits Service

1.2 TTP-Basismodules

TTP MODULE:	Policy Authority (PA)
Functionaliteit	Het vaststellen en controleren van het beleid waaronder certificaten en de daaraan gerelateerde (TTP-) diensten worden geleverd en waaraan alle entiteiten binnen het domein zich dienen te conformeren.
Status	Basis
Afhankelijkheden	Werkt samen met alle andere genoemde componenten.
Privacy aspecten	Het beleid van de PA dient te voldoen aan de relevante privacy-wetgeving (WPR, WBP).
Relevante wetgeving	De PA dient rekening te houden met alle relevante wetten en regels die gelden voor de componenten die binnen het vertrouwensdomein opgenomen zijn.
Organisatorische aspecten	De PA is een beleidsorgaan. Het draagt op het hoogste niveau de verantwoordelijkheid voor het vertrouwensdomein en de organisatie daarvan. Naast het opstellen van het beleid, dient de PA ook te voorzien in een uitvoerende en controlerende organisatie. Vertegenwoordigers van alle deelnemende partijen binnen een vertrouwensdomein dienen betrokken te zijn bij de PA. De PA dient voldoende autoriteit te hebben om namens de betrokken partijen te beslissen en de verantwoordelijkheden te dragen.
Technische aspecten	De PA kent als zodanig geen technische elementen.
Kosten	De belangrijkste kostenpost van de PA wordt gevormd door de personele kosten.
Uitbesteding	De PA is cruciaal voor een vertrouwensdomein. Uitbesteding is niet mogelijk. Wel kunnen de inhoudelijke activiteiten worden uitbesteed en kan kennis worden ingehuurd.
Opmerkingen	De PA bepaalt de regels en de grenzen van een (of meerdere) vertrouwensdomein(en). De PA stelt de diensten en het betrouwbaarheidsniveau vast voor een bepaald domein. Het bepaalt de spelregels en voorwaarden waaraan alle betrokken partijen (minimaal) moeten voldoen. Of communicatie tussen domeinen mogelijk is, wordt sterk bepaald door de overeenkomsten en verschillen in het beleid als bepaald door de PAs. De PA stelt eisen aan ondermeer: - Het uitgifteproces van certificaten - Het verificatieproces - De betrokken TTP organisaties - De gebruikers en acceptanten van certificaten en TTP-diensten (relying parties) Het meest voor de hand liggende middel daartoe is de Certificate Policy (CP) [PKIX] waar nodig aangevuld met andere beleidsdocumenten

TTP MODULE:	Policy Authority (PA)
	en regelementen. Er is echter ook een tendens naar een definitie waarbij de PA een sterk controlerende of zelfs licentieverstrekkende rol heeft. In Nederland lijkt de TTP-kamer deze rol te gaan vervullen.
Referenties	PKIX: Policy Certification Authority (PCA) GoC PKI: Policy Management Authority (PMA) Root Authority

TTP MODULE:	Certification Authority (CA) service
Functionaliteit	Verantwoordelijk voor het vaststellen en garanderen van de authenticiteit van publieke sleutels. Dit houdt in het aanmaken van een ondertekend digitaal certificaat (X.509) waarmee de publieke sleutel gekoppeld wordt aan een identiteit (Distinguished Name). Daarnaast het beheren van certificaten en het intrekken (revocation) van uitgegeven certificaten.
Status	Basis
Afhankelijkheden	Werkt samen met de RA, NS module. Veelal met de: DS, KM modules. Optioneel met de:KBRS module.
Privacy aspecten	De CA accumuleert, bewerkt en publiceert grote hoeveelheden persoonsgebonden informatie waaronder zogenaamde 'zwarte lijsten' met certificaten die ingetrokken zijn. Naleving van Europese en nationale privacy wetgeving is dan ook zeer belangrijk.
Relevante wetgeving	- Europese regel- en wetgeving omtrent de Digitale Handtekening - privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Encryptieregulering: mogelijke regulering m.b.t. de plicht om geheim sleutelmateriaal beschikbaar te stellen onder strikte voorwaarden kan relevant zijn indien de CA deze sleutels zou (kunnen) bezitten. Dit aspect is echter ondergebracht bij de KM en KBRS. - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering.
Organisatorische aspecten	De CA bestaat uit deels zwaar beveiligde, zeer betrouwbare IT systemen voor het maken en beheren van certificaten. Strikte procedures dienen te worden opgesteld en nageleefd. Het personeel dient goed opgeleid te zijn voor haar taken en een groot beveiligingsbewustzijn te hebben. De CA diensten dienen 24 uur per dag, 7 dagen per week beschikbaar te zijn. De CA dient zo onafhankelijk mogelijk te zijn t.a.v. de entiteiten die worden gecertificeerd om verstrengeling van belangen te voorkomen. De CA is vooral uitvoerend en dient te zijn afgeschermd van beleidsmatige (politieke) discussies. De CA dient alleen te worden aangestuurd door de PA.

TTP MODULE:	Certification Authority (CA) service
	Alle handelingen van de CA dienen voor audit doeleinden te worden gelogd. De CA dient door andere partijen te kunnen worden getoetst ten behoeve van bijvoorbeeld cross-certificering tussen domeinen. In dit licht zijn met name de activiteiten binnen het project TTP.NL van belang
Technische aspecten	De CA bestaat uit zwaar beveiligde, zeer betrouwbare IT systemen voor het maken en beheren van certificaten. De gehele organisatie dient daarop ingesteld te zijn. Dit geldt zowel voor de IT infrastructuur, het personeel en de fysieke omgeving. De CA diensten dienen voor alle entiteiten binnen het vertrouwensdomein beschikbaar te zijn. Relevante standaarden zijn vooral: IETF PKIX-serie, ISO/IEC/ITU X.509 en X.500, RSA PKCS-serie.
Kosten	- personele kosten: ca. 3-5 fte's indien RAs de registratie voeren - IT infrastructuur: ca. 300-500 kfl. - Overige infrastructuur: beveiligde ruimtes, bewaking, uitwijkvoorzieningen Deze kostenindicaties betreffen het inrichten van een fysieke CA. Meerdere CA-diensten (virtuele CA's) kunnen op dezelfde fysieke infrastructuur geplaats worden. Hiermee kunnen aanzienlijke kostenbesparing bereikt worden. Voorwaarde daarbij is dat het beleid voor de verschillende virtuele CA's in hetzelfde of een vergelijkbaar vertrouwensdomeinen werkzaam zijn. Zowel bij produkten voor het zelf inrichten van CA's als bij het inkopen zijn verschillende licentie strategieën mogelijk. In vele gevallen zijn de kosten deels afhankelijk van het aantal uit te geven certificaten.
Uitbesteding	De CA vormt het hart van het domein. Een CA bestaat voornamelijk uit een zwaar beveiligde technische infrastructuur waar de digitale identiteitsbewijzen worden gemaakt en ondersteunende infrastructuren voor het beheren en publiceren van digitale identiteitsbewijzen en aanverwante gegevens. Implementatie en instandhouding van de CA infrastructuur kan goed uitbesteed worden. Daarbij dient de CA in haar CPS aan te tonen hoe zij het beleid binnen een domein naleeft. Controle op naleving hiervan is noodzakelijk. Scheiding van functies is in dit geval uiterst belangrijk. Het beheer van certificaten dient strikt gescheiden te zijn van systeem- en technisch beheer. De beschikbaarheid van de CA dienst is een belangrijk aandachtspunt.
Opmerkingen	Een CA kan ook (alleen) tot taak hebben het Certificeren van hiërarchisch onderliggende CA's. De hiërarchisch hoogste CA wordt ook wel root CA of top CA genoemd. Over het algemeen wordt het publiceren van certificaten en CRL beschouwd als een verplichting van de CA. Dit betekent dat de CA altijd

TTP MODULE:	Certification Authority (CA) service
	samenwerkt met (een deel van) de DS functie.
Referenties	

TTP MODULE:	Key Manager (KM) service
Functionaliteit	Het aanmaken, uitgeven, bewaren, intrekken en vervangen van sleutels.
Status	Basis
Afhankelijkheden	Werkt samen met de: CA module voor het certificeren van publieke sleutels; RA module voor het controleren van het bezit van sleutels. Optioneel met de: PUA module voor het genereren en opslaan van sleutelmateriaal voor eind-entiteiten; KBRS module voor het bewaren en beschikbaarstellen van sleutelmateriaal onder vastgestelde omstandigheden. De KM kan zowel centraal als decentraal ingericht worden. Dit is een van de belangrijke keuzen in de totale PKI architectuur. De centraal ingerichte KM maakt het archiveren van sleutelmateriaal eenvoudiger. De organisatie loopt echter risico's ten aanzien van aansprakelijkheid indien sleutelmateriaal van gebruikers wordt (of kan worden) misbruikt. Bij het decentraal (bij de gebruikers) genereren en bewaren van sleutelmateriaal is het daarentegen erg moeilijk om de KBRS-module te implementeren.
Privacy aspecten	Sterk afhankelijk van de wijze waarop deze dienst is ingericht. Essentieel is het te allen tijde geheim houden van persoonsgebonden sleutelmateriaal.
Relevante wetgeving	- privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Encryptieregulering: mogelijke regulering m.b.t. de plicht om geheim sleutelmateriaal beschikbaar te stellen onder strikte voorwaarden kan relevant zijn indien de CA deze sleutels zou (kunnen) bezitten. Dit aspect is echter in het model ondergebracht bij de KM en KBRS. - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering.
Organisatie	De noodzakelijke organisatie is sterk afhankelijk van de wijze waarop deze dienst is ingericht. Indien de KM functie is geïntegreerd met de werkomgeving van de eindgebruiker (PUA module, decentrale

TTP MODULE:	Key Manager (KM) service
	inrichting) dient de gebruikte applicatie vooraf te worden goedgekeurd. De eindgebruiker dient voldoende te zijn geïnstrueerd. Indien gekozen wordt voor een centrale KM zijn de eisen die aan de organisatie gesteld worden grotendeels vergelijkbaar met die voor de CA waarbij nog een sterker accent ligt op de geheimhouding. De distributie van sleutelmateriaal naar de gebruikers vormt daarbij een cruciale schakel. Binnen de Rijksoverheid is op dit terrein veel ervaring binnen het Nationaal Bureau voor de Verbindingsbeveiliging. Tenminste één aanbieder van TTP-producten (Entrust) biedt het sleutelbeheer geïntegreerd aan in haar productlijn. Scheiding van de verantwoordelijkheden voor het sleutelbeheer en het certificatenbeheer dient desondanks te worden nagestreefd om mogelijkheden tot fraude te beperken.
Uitbesteden	In geval van decentrale sleutelgeneratie is uitbesteding niet mogelijk. Bij centrale generatie dient men zeer strenge beveiligingseisen stellen aan de organisatie die deze dienst levert en de dienst zelf. Geheime (private) sleutels mogen nooit in verkeerde handen komen. De belangrijkste vraag daarbij is of men deze cruciale beveiligingsfunctie wenst uit te besteden. Afhankelijk van het beleid en het beveiligingsniveau zou de distributie en opslag van sleutels (en certificaten) middels smartcards plaats kunnen vinden. Van een aantal potentiële TTP-dienstenaanbieders (o.a. Enschede/SdU) is bekend dat ze deze vorm van dienstverlening willen aanbieden. Dit lijkt vooralsnog een van de meest realistische opties om het sleutelbeheer uit te besteden.
Opmerkingen	Wordt ook wel Key Generator, Key Generation [5], Key Mangement Facility genoemd. Bij deze module spelen aspecten als nationale veiligheid, exportbeperkingen en rechtmatige toegang (door de overheid) een belangrijke rol. Zorgvuldig sleutelbeheer in algemene zin en met name het archiveren van sleutelmateriaal is van groot belang voor het (achteraf) bewijzen van rechtshandelingen. - Voor het kunnen controleren van een digitale handtekening is het noodzakelijk dat de publieke sleutels gedurende de levensduur van de handtekening beschikbaar blijft op een betrouwbare wijze (als gewaarmerkt certificaat, zie Notary Service). - Voor het kunnen ontcijferen van vercijferde berichten is het noodzakelijk dat de private- of vercijfersleutels gedurende de levensduur van een bericht beschikbaar blijven. (Zie Key Backup and Recovery Service (KBRS) module.) Zowel het genereren als het bewaren van private en geheime sleutels stelt zeer hoge eisen aan de

TTP MODULE:	Key Manager (KM) service
	beveiliging van de TTP-organisatie. Mede gezien de tendensen in de (internationale) wetgeving wordt er echter voor gekozen om Key Recovery en/of Escrow als aparte modules op te voeren en niet als onderdeel van de KM. Zo gaan de Europese wetgeving (Italië, Duitsland en richtlijnen EU) er van uit dat de CA geen private sleutels mag bewaren maar wel genereren. Bewaren van sleutels is de taak van de Private Key Trusted Service KBRS) [5].
Referenties	

TTP MODULE:	Registration Autority (RA) service
Functionaliteit	Het verwerken van certificaataanvragen, de verificatie van de gegevens in de aanvraag (de identiteit) en de autorisatie van de aanvraag. Dit omvat ondermeer het (procedureel) leggen van een associatie tussen de publieke sleutel en een aanvragende persoon/entiteit. Optioneel: - Certificaat beheer voor de gebruikers (inclusief intrekken). - Het uitgeven van de certificaten. - Het bepalen van autorisaties die in het certificaat worden opgenomen of daarmee verbonden zijn.
Status	Basis
Afhankelijkheden	Werkt samen met de CA module voor het aanmaken en beheren van het certificaat. Optioneel met de: NS voor het bepalen van de unieke Distinguished Name; DS module voor het publiceren van certificaten; CA module voor het intrekken van certificaten; KBRS modules voor het bewaren en terugwinnen van sleutelmateriaal.
Privacy aspecten	De RA accumuleert en bewerkt grote hoeveelheden persoonsgebonden informatie waaronder informatie voor de zogenaamde 'zwarte lijsten' met certificaten die ingetrokken zijn. Ten behoeve van de verificatie van de identiteit van de aanvrager worden verschillende gegevensbanken geraadpleegd. Beslissing over het al dan niet autoriseren van certificatie worden gedocumenteerd. Naleving van Europese en nationale privacy wetgeving is dan ook zeer belangrijk.
Relevante wetgeving	- privacywetgeving: WPR, WBP - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering.
Organisatorische apecten	De RA is het loket van het vertrouwensdomein. De RA functie heeft dus een sterke relatie met de organisatie en de personen waarvoor certificaten worden aangemaakt. De RA dient zo dicht mogelijk bij de gebruikers te staan. Verder vergt deze dienst veelal een koppeling met bijvoorbeeld een personeelsadministratie voor het autoriseren van gebruikers. Afhankelijk van de geografische spreiding van de gebruikers en de omvang van de gebruikersgroep zijn meerdere fysieke RA's noodzakelijk.

TTP MODULE:	Registration Autority (RA) service
Technische apspecten	De RA vergt in de meeste gevallen geen uitgebreide technische voorzieningen. Voor beheer is meestal een on-line verbinding met de CA noodzakelijk, bijvoorbeeld naar de website van de CA. Toegang tot deze beheerssystemen dient goed beveiligd te zijn. In de meeste gevallen volstaat een simpele PC as basisvoorziening.
Kosten	- personeel: een RA vergt voornamelijk administratief personeel. Per fysieke RA is ca. 1 fte noodzakelijk per 3000 gebruikers. Initieel, bij de eerste registratie, kan dit getal hoger zijn. - IT infrastructuur: circa 15 kfl per RA medewerker.
Uitbesteding	Gezien de verankering in de organisatie ligt uitbesteding van deze functie niet voor de hand.
Opmerkingen	Afhankelijk van de locatie van de KM functie, dient de RA of CA ook een controle uit te voeren op het bezit van de private sleutel door de aanvrager. Dit is het geval indien de KM lokaal bij de aanvrager de sleutels genereert. In dit document wordt de RA module gezien als het loket waar de gebruikers hun certificaten kopen. Daarbij hoort o.i. ook het verlenen van service. Een gebruiker wil tegenwoordig een duidelijk aanspreekpunt. Zo zien we ook een rol voor de RA in het proces voor het intrekken van een certificaat. De goede mogelijkheden voor de combinatie van de RA functie met certificaat beheersfuncties (ongeldig maken certificaten e.d.) versterkt dit.
Referenties	

TTP MODULE:	Distribution Service (DS)
Functionaliteit	Het beschikbaar stellen en/of uitwisselen van digitale certificaten. Optioneel: - Het beschikbaar stellen van CRL. - Het beschikbaar stellen van CP/CPS.
Status	Basis
Afhankelijkheden	Werkt samen met de: CA, RA en PUA Optioneel met: alle andere TTP modules.
Privacy aspecten	De DS zorgt voor de distributie en het publiceren van de certificaten, de zwarte lijsten en aanverwante informatie. In vele gevallen dient de verspreiding om privacyredenen beperkt te blijven tot die groep die deze informatie daadwerkelijk nodig heeft. Dit is een belangrijk aandachtspunt bij het inrichten van de DS.
Relevante wetgeving	- privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering.
Organisatorische aspecten	De DS vormt het adresboek van het vertrouwensdomein. Het plannen van de DS service binnen een X.500 Directory service (zie technische aspecten) is een van de belangrijkste stappen. Daarbij dient terdege rekening te worden gehouden met de wenselijkheid om (op termijn) te koppelen met bijvoorbeeld andere departementale Directories. Dit vergt op zijn minst interdepartementale afspraken over structuren en naamgeving die worden gehanteerd binnen de DS. De namen die gebruikt worden bij het uitgeven van certificaten dienen in de DS structuur te passen. Via de DS kunnen additionele gegevens worden geassocieerd met certificaten en dus met de gecertificeerde personen. Dit is van groot belang voor bijvoorbeeld autorisatiebeheer. Naarmate TTP-diensten dus verder geïntegreerd zijn met de organisatie, wordt de DS belangrijker. Een gecoördineerde aanpak is essentieel aangezien de DS voor een veelvoud aan diensten

TTP MODULE:	Distribution Service (DS)
	gebruikt zal worden. De behoefte aan een DS dienst is dan ook als belangrijk aandachtspunt uit de studie naar het overheidsintranet naar voren gekomen. Binnen de RO is dientengevolge een aparte studie gewijd aan deze problematiek.
Technische aspecten	De meest voor de hand liggende standaard voor het inrichten van de DS is de ISO/IEC/ITU X.500 standaard voor een gedistribueerde database, 'de Directory' genaamd. De meeste PKI CA-producten kunnen met X.500 interfacen via het Lightweight Directory Acces Protocol (LDAP). Beschikbaarheid en toegankelijkheid van de DS voor alle entiteiten in een vertrouwensdomein is uiterst belangrijk. Voor een afscherming van privacy-gevoelige gegevens dient de DS te zijn voorzien van een goed toegangscontrole mechanisme. Sommige PKI toepassingen bieden een geïntegreerde functionaliteit voor het uitwisselen van gebruikerscertificaten. Dit is met name het geval voor de S/MIME standaard voor beveiligde e-mail. In mindere mate geldt dit voor de SSL standaard voor het opzetten van beveiligde sessies.
Uitbesteding	De DS vormt ondermeer het adresboek van het vertrouwensdomein. De mogelijkheden tot uitbesteding worden sterk bepaald door het type informatie dat beschikbaar wordt gesteld. Om privacy redenen kan het publiekelijk beschikbaar stellen grote problemen opleveren. Voor een gesloten gebruikersgroep is het verder de vraag of men deze gegevens buiten deze gemeenschap beschikbaar wil stellen. De DS fungeert veelal ook als basis voor toegangsbeveiliging en autorisatiebeheer. De daarmee gepaard gaande integratie met de eigen systemen spreekt voor een eigen implementatie. Indien globale toegankelijkheid van de DS belangrijk is, kunnen bestaande openbare directory services voordeel bieden. Bij uitbesteding zijn garanties voor de beschikbaarheid en toegankelijkheid van de DS essentieel.
Opmerkingen	Wordt ook wel Directory Service, Key Repository of Certificate Directory [2] genoemd. O.i. is dit echter een te beperkte naamgeving. Delen van de DS kunnen evengoed worden gerealiseerd door gebruikers onderling. Dit gebeurt nu reeds veelal voor het uitwisselen van S/MIME e-mail certificaten.
Referenties	ISO/IEC/ITU X.500 Directory service; LDAP; S/MIME specificaties

TTP MODULE:	Name Server (NS) service
Functionaliteit	Het genereren van unieke namen (Distinguished Names, DNs) binnen het PKI domein. De NS is een 'onderliggende' functionaliteit en stelt als het ware randvoorwaarden aan de naamgeving die door CA, RA en DS kan worden gehanteerd. De meeste aspecten zijn dan ook beschreven bij die TTP-modules.
Status	Basis
Afhankelijkheden	Werkt samen met de CA en RA module voor het vaststellen van de DN. De PA dient de randvoorwaarden te stellen aan de te gebruiken syntax.
Privacy aspecten	De gebruikte namen dienen te voldoen aan de WPR en WBP.
Relevante wergeving	- privacywetgeving: WPR, WBP
Organisatorische aspecten	Interdepartementale afstemming van de naamgeving is zeer belangrijk voor onderlinge uitwisseling en koppeling van (DS) diensten. Indien men aansluiting zoekt bij openbare (DS) diensten, zal men aan globale regels gebonden zijn. Dit kan conflicten opleveren met bijvoorbeeld bestaande e-mail en computeradressen.
Technische aspecten	De NS als zodanig kent geen technische aspecten. Wel in relatie met de CA en DS module. Standaarden voor de naamgeving worden gegeven in de ISO/IEC/ITU standaarden X.500/X.509.
Opmerkingen	Normaliter dienen de namen die zijn opgenomen in certificaten (ten minste) binnen een domein uniek te zijn. Dit is echter afhankelijk van het beleid als bepaald door de PA (en eventueel aangescherpt door de CA). Een veel gezien beleidsuitgangspunt is de eis dat één specifieke DN altijd naar dezelfde unieke (natuurlijke) rechtspersoon of entiteit moet wijzen. Dit sluit dus uit dat twee personen onder dezelfde DN worden geregistreerd. Het sluit niet uit dat één persoon onder dezelfde DN meerdere certificaten verkrijgt. Interessant is natuurlijk de vraag of er binnen de overheid unieke DNs moeten worden uitgegeven of binnen kleinere eenheden, bijvoorbeeld departementen.

TTP MODULE:	Name Server (NS) service
Uitbesteding	Deze functie is sterk verbonden met de RA functie. Zie aldaar.
Referenties	ISO/IEC/ITU X.500/X.509

TTP MODULE:	Public Key User Agent (PUA)
Functionaliteit	Het leveren aan eindgebruikers (of systemen) van toepassingen die gebruik maken van TTP-diensten middels standaarden als S/MIME (beveiligde e-mail) en SSL (toegangscontrole en beveiligde sessies).
Status	Basis
Afhankelijkheden	Werkt samen met de CA module voor het certificeren van sleutels en het controleren van CRLs; DS module voor het distribueren van certificaten en controleren van CRLs; KM module voor het genereren en opslaan van de eigen sleutels. Optioneel met: alle overige modules
Relevante wetgeving	- *Exportregulering ten aanzien* van cryptografie in de verschillende landen die PUA's produceren; Akkoord van Wassenaar. - privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Encryptieregulering: mogelijke regulering m.b.t. de plicht om geheim sleutelmateriaal beschikbaar te stellen onder strikte voorwaarden kan relevant zijn indien de CA deze sleutels zou (kunnen) bezitten. Dit aspect is echter in het model ondergebracht bij de KM en KBRS.
Organisatorische aspecten	De correcte (veilige) werking van de verschillende PUA's is van het grootste belang voor het beveiligingsniveau dat binnen een vertrouwensdomein wordt gerealiseerd. PUA's zorgen voor het daadwerkelijke zetten van een digitale handtekening en het vercijferen van berichten. Daarbij hebben ze – direct of indirect – toegang tot geheim sleutelmateriaal. De betrouwbaarheidseisen die aan een PUA worden gesteld, dienen dan ook overeen te komen met het beveiligingsniveau dat binnen een domein is vastgesteld. Het is dan ook noodzakelijk om binnen een vertrouwensdomein vast te stellen

TTP MODULE:	Public Key User Agent (PUA)
	welke PUA's (en daarmee veelal toepassingen en producten) toegelaten zijn. Indien fouten (bugs) worden geconstateerd, dienen maatregelen te worden genomen.Tevens dienen gebruikers voldoende kennis te hebben om de PUA's veilig te bedienen. De gebruikers moeten de beveiliging niet kunnen ondermijnen door instellingen te manipuleren. Dit vergt een scheiding tussen applicatiebeheer en de gebruiksmogelijkheden.
Technische aspecten	Zoals is aangegeven, is de beveiliging en betrouwbaarheid van de PUA's van groot belang voor het beveiligingsniveau dat binnen een vertrouwensdomein wordt gerealiseerd. Afhankelijk van het niveau, dient men eisen te stellen aan de gebruikte technieken en producten. Zo zal men voor een hoger beveiligingsniveau bijvoorbeeld eisen dat de cryptografische bewerkingen in tamper-proof hardware plaatsvinden. Voor lagere niveaus kan men daarentegen software gebruiken. Ook moeten de PUA's uiteraard geschikt zijn voor de cryptografische algoritmen en sleutellengtes die binnen het domein zijn vereist. Dit kan problemen opleveren ten aanzien van exportbeperkingen in de landen die dergelijke producten produceren. Een belangrijke tekortkoming van vele PUA's is op dit moment de beperkte mogelijkheden om de zwarte lijsten met ingetrokken certificaten on-line te controleren. De verwachting is dat hierin in de nabije toekomst beter voorzien zal zijn.
Opmerkingen	Onder de PUA vallen toepassingen als beveiligde e-mail clients (S/MIME), beveiligde webbrowsers en -servers (SSL). De PUA's kunnen geïntegreerd zijn met andere TTP-modules. Dit is met name het geval voor de DS en KM modules.
Uitbesteding	De PUA vormt de toepassing van de eindgebruikers en kan normaliter niet uitbesteed worden.
Referenties	

1.3 Optionele TTP-modules

TTP MODULE:	Key Backup and Recovery Service (KBRS)
Functionaliteit	Het in bewaring houden van sleutels voor key-recovery/escrow doeleinden. Key-Recovery geeft de mogelijkheid om geheim sleutelmateriaal te herstellen onder vastgestelde voorwaarden. Key-escrow geeft de eigenaar en derden de mogelijkheid om sleutelmateriaal te bemachtigen onder vastgestelde voorwaarden. Opm.: Steeds vaker duikt in de literatuur en wetgeving het onderscheid op tussen een CA en een TTP. Het verschil dat daarbij gemaakt wordt, bestaat hierin dat de TTP toegang heeft tot geheim sleutelmateriaal van de klanten, terwijl de CA deze mogelijkheid absoluut niet heeft. Dit is echter een erg strikte definitie van TTPs die tekort schiet in de context van dit rapport. (De CA kan dan gezien worden als een Trusted Party, TP i.p.v. TTP.) Opm.: Het bewaren van publieke sleutels is een taak die meestal door de CA wordt uitgevoerd. Dit kan echter ook in combinatie met de KBRS.
Status	Optioneel
Afhankelijkheden	Werkt samen met de: KM module voor het genereren van sleutels. Volgens de Europese concept richtlijn en Italiaanse/Duitse wetgeving is deze dienst onverenigbaar met de CA module.
Privacy aspecten	Het vrijgeven van persoonsgebonden geheime sleutels dienst aan strikte regels verbonden te zijn. Het feit dat sleutels opgeslagen worden en de voorwaarden waaronder sleutels vrijgegeven worden aan derden, dienen bekend te zijn bij de eigenaar. Tenzij wetgeving dit verbiedt, dient de eigenaar op de hoogte te worden gesteld van het feit dat zijn sleutels worden vrijgegeven. Het is aan te bevelen om een organisatorische scheiding op te werpen tussen de instantie die de sleutels in bewaring houdt en een registratie waarmee sleutels aan personen worden gekoppeld.
Relevante wetgeving	- Exportregulering ten aanzien van cryptografie in de verschillende landen die PUA's produceren; Akkoord van Wassenaar. - privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin

TTP MODULE:	Key Backup and Recovery Service (KBRS)
	TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Encryptieregulering: mogelijke regulering m.b.t. de plicht om geheim sleutelmateriaal beschikbaar te stellen onder strikte voorwaarden. - Wet op de Computer Criminaliteit.
Organisatorische aspecten	De KBRS is uiteraard een zeer gevoelige en kwetsbare component van een vertrouwensdomein. Er worden uiterst zware eisen gesteld aan de beveiliging van de KBRS, zowel in technische als organisatorische zin. Alle handelingen dienen vastgelegd te worden voor audits achteraf. De voorwaarden waaronder en aan wie sleutels vrijgegeven mogen worden, dienen helder te zijn. Toch is deze component in de meeste gevallen noodzakelijk voor een vertrouwensdomein binnen organisaties. De vercijferde informatie is immers veelal van levensbelang voor de organisatie. Indien een medewerker sleutels verliest of om welke reden dan ook zijn sleutels niet meer kan gebruiken, dient de informatie voor de organisatie beschikbaar te kunnen worden gesteld. De KBRS voorziet in deze behoefte. Indien de KBRS wordt aangeboden binnen een vertrouwensdomein, zal deze ook voor bijvoorbeeld strafvervolging toegankelijk zijn. De wijze van de invoering van de KBRS is sterk afhankelijk van de keuze voor centrale of decentrale KM. In het geval van een decentrale KM, zal KBRS vooral op organisatorische en procedurele wijze moeten worden gerealiseerd. De gebruiker die decentraal sleutels genereert, zal deze als het ware moeten deponeren in de KBRS. Bij een centrale KM kan sleutelmateriaal direct in kopie opgeslagen worden in de KBRS module. In alle gevallen dienen procedurele en technische maatregelen te voorkomen dat geheim sleutelmateriaal kan worden misbruikt. Zoals eerder gemeld, is het aan te bevelen om een organisatorische scheiding op te werpen tussen de instantie die de sleutels in bewaring houdt en een registratie waarmee sleutels aan personen worden gekoppeld.
Technische aspecten	De KBRS is eigenlijk alleen van belang voor sleutelmateriaal dat gebruikt wordt voor het vercijferen van documenten ten behoeve van de vertrouwelijkheid. De KBRS is niet van toepassing op sleutels die gebruikt worden voor het zetten van digitale handtekeningen. Dit ondermijnt de waarde van de digitale handtekening. Het vrijgeven van deze laatste sleutels, maakt alle handtekening die daarmee gezet zijn onbetrouwbaar (tenzij ze via de Time Stamping

TTP MODULE:	Key Backup and Recovery Service (KBRS)
	service (TS) aantoonbaar voor de datum van vrijgave zijn gewaarmerkt.) Dit betekent dat een goed systeem dat KBRS ondersteunt, gebruik dient te maken van verschillende sleutelparen: één voor vertrouwelijkheid en één voor authenticiteit en integriteit. Dan wel een (technische) oplossing dient te bieden voor het terugwinnen van de geheime vercijfersleutel zonder dat daarbij de private sleutel voor authenticiteit en integriteit worden gecompromitteerd. Indien men gebruik wil maken van KBRS is deze scheiding dan ook de belangrijkste eis. Uiteraard dient het gehele proces van transport en opslag van sleutelmateriaal bijzonder goed te zijn beveiligd.
Opmerkingen	
Uitbesteding	Net als de KM levert de KBRS een essentiële beveiligingsfunctie. Men dient zeer strenge beveiligingseisen stellen aan de organisatie die deze dienst levert en de dienst zelf. Geheime (private) sleutels mogen nooit in verkeerde handen komen. De belangrijkste vraag daarbij is of men deze cruciale beveiligingsfunctie wenst uit te besteden. De meeste publieke TTP-dienstenleveranciers bieden vooralsnog geen mogelijkheden voor het in bewaring houden van geheim sleutelmateriaal.
Referenties	[7] KBRS, [3] Private Key Trusted Service (PKTS)

TTP MODULE:	Time Stamping (TS) service
Functionaliteit	Het onweerlegbaar dateren van elektronische documenten en/of berichten.
Status	Optioneel
Afhankelijkheden	Werkt samen met de PUA
Opmerking	De TS is een 'document certification' of 'document notarisation' dienst. Een Notarisation Service

TTP MODULE:	Time Stamping (TS) service
en	is een meer algemene dienst die niet slechts het bestaan van een document op een bepaald moment in de tijd vaststelt maar daarnaast ook instaat voor de waarheid/geldigheid op een bepaald moment van meer generieke uitingen. TS voorziet (sec) niet in het bewaren van eventuele bewijsstukken. Deze dienst wordt wel geleverd door bijvoorbeeld de Bewijs & Bewaar module (B&B, zie verderop in de lijst). De TS voorziet in de behoefte aan een werkelijk onafhankelijke en betrouwbare vaststelling van het tijdstip waarop een handeling is verricht. Ofschoon er meestal een tijdstempel is opgenomen in een digitale handtekening, is dit niet betrouwbaar voor derden. De tijd die wordt gebruikt is normaliter de lokale tijd van de computer waar de handtekenig wordt gezet. Deze systeemtijd is veelal eenvoudig te wijzigen door de gebruiker. De TS functie kan er ook voor zorgen dat een handtekening die is gezet met een certificaat dat later is ingetrokken, zijn geldigheid behoudt. Het tijdstempel bewijst immers aan dat de handtekening voor het intrekken is gezet.
Privacy aspecten	De TS zou eventueel de te tijdstempelen informatie kunnen inzien. Dit dient uitgesloten worden. Overigens kan volstaan worden met het tijdstempelen van vercijferde berichten of de zogenaamde hashwaarde (een gecomprimeerde weergave van een bericht). Zie in dit licht ook de voorwaarden die aan de TS worden gesteld in de IETF Internet draft 'Time Stamp Protocols'.
Relevante wetgeving	- privacywetgeving: WPR, WBP - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering.
Organisatorische aspecten	Bij de TS functie is met name de bewijskracht in geval van geschillen van belang. Dat betekent dat de TS functie ook bij voorkeur door een onafhankelijke partij, dus een echte TTP, moet worden ingericht. De TS functie kan vergaand geautomatiseerd worden uitgevoerd. Verantwoordelijkheid en aansprakelijkheid is gezien de bewijskracht van groot belang. Beide partijen zullen de geleverde diensten moeten erkennen. Een beroepsinstantie of geschillencommissie is wenselijk.
Technische aspecten	De TS is in wezen een dienst waarbij gebruik wordt gemaakt van certificaten. De TS maakt een document waarin het oorspronkelijke document en een tijdstempel zijn opgenomen. Dit document wordt door de TS digitaal ondertekend. De TS maakt dus als het ware een eigen soort certificaat met een gegarandeerde tijd van aanmaken.

TTP MODULE:	Time Stamping (TS) service
	Essentieel zijn daarbij een 'absoluut' betrouwbare tijd en betrouwbare apparatuur voor het maken en verzegelen van het tijdstempel-certificaat. De TS maakt daarbij in wezen gebruik van een zwaar beveiligde PUA. Zie de eisen aldaar. De infrastructuur van de TS moet goed zijn beveiligd en zijn opgesteld in een beveiligde ruimte. Standaarden voor de TS dienst zijn nog in een concept fase. Relevant lijkt met name de IETF PKIX serie.
Uitbesteding	*Bij de TS functie is de bewijskracht in geval van geschillen van belang.* Dat betekent dat de TS functie ook bij voorkeur door een onafhankelijke partij, dus echte TTP, moet worden ingericht. Uitbesteding is dus zeker te overwegen. Voor interne controle kunnen uiteraard ook interne TS functies worden ingericht. De daadwerkelijk waarde daarvan is echter beperkt. Zo zou men interne fraude door het wijzigen van de lokale systeemtijd kunnen detecteren.
Referenties	[2] "De aanhechtingen van de exacte tijd aan een bepaald elektronisch document, bericht of transactie." [aba] "(1) To create a notion that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation; or (2) Such a notation appended, attatched of referenced."

TTP MODULE:	Notary Agent Service (NoS)
Functionaliteit	Het controleren van een digitale handtekening of verklaring op een bepaald moment, met als doel het onweerlegbaar vastleggen daarvan.
Status	Optioneel
Afhankelijkheden	Maakt gebruik van de TS module
Opmerkingen	De NoS voorziet in de behoefte aan een werkelijk onafhankelijke en betrouwbare vaststelling van het tijdstip waarop een bericht werd aangeboden en de geldigheid van de digitale handtekening die aan dat bericht verbonden is. Ofschoon er meestal een tijdstempel is opgenomen in een digitale handtekening, is dit niet betrouwbaar voor derden. De tijd die wordt gebruikt is normaliter de lokale tijd van de computer waar de handtekening wordt gezet. Deze systeemtijd is veelal eenvoudig te wijzigen door de gebruiker. De handtekening zelf kan ook vals zijn of later worden ontkend. Daarom controleert de NoS de geldigheid van de digitale handtekening op het moment van Notarisation als onderdeel van de NoS. Ook de NoS is een dienst waarbij gebruik wordt gemaakt van certificaten. De NoS maakt een document waarin het oorspronkelijke document en een tijdstempel zijn opgenomen nadat de digitale handtekening verbonden met het document door de NoS is gecontroleerd. Dit document wordt door de NoS digitaal ondertekend. De NoS maakt dus als het ware een eigen soort certificaat met een gegarandeerde tijd van aanmaken. De NoS kan daarmee ook het probleem met het herstellen van het verleden van vertrouwensrelaties opvangen. Door te verklaren dat er op het moment van natarisation een vertrouwensrelatie bestaat, behoeft dit verleden niet te worden bewaard. (Denk aan inter-domein relaties.)
Privacy aspecten	Zie TS module
Relevante wetgeving	Zie TS module

TTP MODULE:	Notary Agent Service (NoS)
Organisatorische aspecten	Dezelfde aspecten als voor de TS zijn van belang. Aangezien de NoS vooraf ook de geldigheid van een digitale handtekening controleert, dient de NoS toegang te hebben tot de actuele lijst van ingetrokken certificaten – de 'zwarte lijst'. Dit kan technisch of procedureel ingericht worden. De NoS dient bij te houden op grond van welke beleid (welke vertrouwensrelatie) een handtekening goedgekeurd wordt. Dit is van belang bij het herstellen van het verleden van vertrouwensrelaties tussen (tijdelijk) gecross-certificeerde domeinen.
Technische aspecten	Essentieel voor de NoS zijn daarbij een 'absoluut' betrouwbare tijd en betrouwbare apparatuur voor het controleren van digitale handtekeningen en voor het maken en verzegelen van het tijdstempel-certificaat. Beschikbaarheid van een actuele lijst met ingetrokken certificaten is daarbij noodzakelijk. De NS maakt daarbij in wezen gebruik van een zwaar beveiligde PUA. Zie de eisen aldaar. De infrastructuur van de NoS moet goed zijn beveiligd en opgesteld in een beveiligde ruimte. Er zijn voor zover bekend nog geen standaarden op dit gebied.
Uitbesteden	Bij de NoS functie is de bewijskracht in geval van geschillen van belang. Dat betekent dat de NS functie ook bij voorkeur door een onafhankelijke partij, dus echte TTP, moet worden ingericht. Uitbesteding is dus aan te bevelen. Voor interne controle kunnen uiteraard ook interne NoS functies worden ingericht. De daadwerkelijk waarde daarvan is echter beperkt. Zo kan men interne conflicten ten aanzien van het verleden van vertrouwensrelaties (b.v. gewijzigde bevoegdheden) detecteren.
Referenties	[3], [4], part 4

TTP MODULE:	Bewaar en Bewijs (B&B) service
Functionaliteit	Het bewaren van (gewaarmerkte) elektronische documenten eventueel voor latere bewijsvoering.
Status	Optioneel
Afhankelijkheden	Optioneel met de: TS module voor het tijdstempelen van te bewaren documenten; de NoS module voor Notarisation van te bewaren documenten.
Opmerkingen	Dit onderwerp heeft duidelijke raakvlakken met de activiteiten die binnen de Rijksoverheid zijn opgestart op het gebied van elektronische duurzaamheid en digitale archivering.
Privacy aspecten	Komen overeen met de eisen die aan archiefdiensten worden gesteld.
Relevante wetgeving	- privacywetgeving: WPR, WBP - Regelgeving omtrent bewijs en bewaring: relevant in algemene zin t.a.v. de bedrijfsvoering. - Archiefwet
Organisatorische aspecten	De B&B dienst is een elektronische variant van een normaal archief. Een speciaal probleem dat optreedt is de archivering van vercijferde documenten. De gearchiveerde documenten dienen uiteraard te kunnen worden ontcijferd gedurende de bewaartijd. Hiervoor zijn verschillende opties waaronder het ontcijferen voor archivering of het archiveren van de bijbehorende sleutels (en het onderhouden van de relatie tussen sleutels en documenten.) Op het gebied van archivering en digitale duurzaamheid worden momenteel studies uitgevoerd binnen de Rijksoverheid. We verwijzen hier naar de resultaten van die studies.
Technische aspecten	Zie ook organisatorische aspecten. Er zijn voor zover bekend geen standaarden op dit gebied.
Uitbesteding	Uitbesteding is op zich goed mogelijk. Binnen de Rijksoverheid is echter een uitgebreid systeem voor het archiveren van documenten en berichten aanwezig. Genoemde activiteiten inventariseren de mogelijkheden om dit ook voor digitale informatie in te richten. Uitbesteding of niet zal daarbij een issue zijn.
Referenties	

TTP MODULE:	Non-Repudiation (NR) service
Functionaliteit	Het onweerlegbaar vastleggen ten behoeve van het onweerlegbaar aantonen dat bepaalde elektronische documenten op een bepaald moment bestonden of uitgewisseld werden. Zowel het moment van verzending als bezorging kan daarbij middels een tijdstempel onweerlegbaar worden vastgelegd.
Status	Optioneel
Afhankelijkheden	Werkt samen met de TS module voor het tijdstempelen van te bewaren documenten Optioneel met de: NS module voor Notarisation van te bewaren documenten; B&B module voor het bewaren van documenten
Opmerkingen	
Privacy aspecten	Zie TS, NoS en B&B modules.
Relevante wetgeving	Zie TS, NoS en B&B modules.
Organisatorische aspecten	Zie TS, NoS en B&B modules.
Technische aspecten	Zie TS, NoS en B&B modules. De logische plaats van de NR is tussen de communicerende partijen. Berichten worden dus via de NR verzonden. Daarbij dient de NR zo dicht mogelijk bij de zender en ontvanger te zijn gelokaliseerd. Er zijn voor zover bekend geen standaarden op dit gebied.
Uitbestedeen	De NR functie is een combinatie van de TS, NS en B&B functies. Bij de NR functie is met name de bewijskracht in geval van geschillen van belang. Dat betekent dat de NR functie ook bij voorkeur door een onafhankelijke partij, dus een echte TTP, moet worden ingericht. Uitbesteding is daarom goed mogelijk. Voor interne controle kunnen uiteraard ook interne NR functies worden ingericht. Dit zou

TTP MODULE:	Non-Repudiation (NR) service
	voor eisen ten aanzien van de openbaarheid van bestuur ingezet kunnen worden. Handelingen van de overheid zijn daarmee achteraf bijzonder goed aantoonbaar.
Referenties	

TTP MODULE:	Exclusiviteits Service (ES)
Functionaliteit	Het in-line vercijferen van berichten en communicatie tussen communicerende partijen..
Status	Optioneel
Afhankelijkheden	Werkt samen met de KM en DS module voor het verkrijgen van vercijfersleutels en certificaten. Optioneel met de: NS module voor Notarisation van te bewaren documenten; B&B module voor het bewaren van documenten
Opmerkingen	Deze dienst komt overeen met de TTP-dienst voor vertrouwelijkheid zoals gedefinieerd in het NAP/TTP rapport.
Privacy aspecten	De ES krijgt vertrouwelijke informatie toegezonden die vercijferd verzonden moet worden. Deze mag nooit in handen komen van medewerkers van de ES of derden.
Relevante wetgeving	- Exportregulering ten aanzien van cryptografie in de verschillende landen die PUA's produceren; Akkoord van Wassenaar. - privacywetgeving: WPR, WBP - Wet Telecommunicatie Voorzieningen, Telecommunicatiewet kan afhankelijk van de vorm waarin TTP-diensten worden aangeboden (met name publieke diensten) van belang zijn i.v.m. rechtmatige toegang (tot vercijferde informatie). - Encryptieregulering: mogelijke regulering m.b.t. de plicht om geheim sleutelmateriaal beschikbaar te stellen onder strikte voorwaarden.
Organisatorische aspecten	De ES is uiteraard een zeer gevoelige en kwetsbare component van een vertrouwensdomein. Er worden uiterst zware eisen gesteld aan de beveiliging van de ES, zowel in technische als organisatorische zin. Alle handelingen dienen vastgelegd te worden voor audits achteraf. De voorwaarden waaronder en aan wie sleutels eventueel vrijgegeven mogen worden, dienen helder te zijn.
Technische	Er worden bijzonder zware eisen gesteld aan de betrouwbaarheid van de ES dienstverlening en infrastructuur. Uiteraard dient het

TTP MODULE:	Exclusiviteits Service (ES)
aspecten	gehele proces van transport en opslag van sleutelmateriaal bijzonder goed te zijn beveiligd. De logische plaats van de ES is tussen de communicerende partijen. Berichten worden dus via de ES verzonden. Daarbij dient de ES zo dicht mogelijk bij de zender en ontvanger te zijn gelokaliseerd. Er zijn voor zover bekend geen standaarden op dit gebied.

ezien de cruciale rol die de ES speelt bij het garanderen van de exclusiviteit van de informatie van de Rijksoverheid lig
.tbesteding niet voor de hand.

AP/TTP

Bijlage 5: Definities

TTP diensten voor de rijksoverheid

Bij de definitie is steeds aangegeven uit welke bron de definitie stamt. Indien bij een begrip meerdere definities staan kan een bepaalde voorkeur worden gegeven op basis van de bron van de definitie. Deze principe voorkeur is:

1. ISO
2. CEN
3. PKIX
4. Overige

A

AUTHENTICATION.

ENTITY AUTHENTICATION.

Definition according to ISO/IEC 9798-1 en ISO 10181-2. The corroboration that an entity is the one claimed.

DATA ORIGIN AUTHENTICATION.

Definition according to ISO/IEC 9798- 1. The corroboration that the source of the data is as claimed.

C

CERTIFICATE

Definition according to ISO 9594-8. User certificate, public key certicate: The public keys of a user, together with some information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.
Definition according to the European Commission (article 2 of the "Common framework for electronic signatures"). A qualified certificate means unique data which links a signature verification device to a person , confirms the identity of that person and meets the requirements laid down in " Annex A of the Common framework for electronic signatures".
Definition according to X.509. A certificate is a digitally signed statement from one entity, saying that the public key of some other entity bas some particular value.

CERTIFICATE POLICY (CP)

Definition according to SEISIPKIX(X.509). A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

CERTIFICATION AUTHORITY (CA)

Definition according to ISO/IEC 9594-8. An authority trusted by one ore more users to create and assign certificates. Optionally the certification authority may create the users' keys.
Definition according to the European Commission. A certification service provider means a person who or entity which issues certificates or provides services related to electronic signatures to the public.
Definition according to ISO 7816-8. A Certification Authority (CA) is a trusted third party, that establishes a proof that links a public key and other relevant information to its owner..
Definition according to X.509. These are entities (e.g. businesses) which are trusted to sign (issue) certificates for other people. They usually have some kind of legal responsibilities.
Definition according to KPMG on behave of ECP.NL members. CA's represent the people, processes, and tools to create digital certificates that securely bind the names of the users to their public keys.

CERTIFICATION PRACTICE STATEMENT (CPS).

Definition according to SEISIPKIX(X.509)1 ABA. A statement of the practices which a certification authority employs in issuing certificates.

D

DIGITALE SIGNATURE

Definition according to ISO 7498-2. Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient..
Definition according to the NCP. Result of a cryptographic transposition in which the person carrying out the process uses his secret key5 with the objective of providing non-repudiation of the source and integrity or the message content.

E

ELECTRONIC SIGNATURE

Definition according to the European Commission. Electronic signature means a signature in digital form in, or attached to, or logically associated with, data and used by a signatory to indicate that signatory's approval of the content of that data and which meets the following requirements :. Is uniquely linked to the signatory . Is capable of identifying the signatory . Is created using means that the signatory can maintain under his sole control; and . Is linked to the data to which it relates in such a manner that it is revealed if the data is subsequently altered..

ENTITY

Definition according to X.509. An entity is a person, organization, program, computer, business, bank or something else you're trusting to some degree.

IDENTIFICATION

Definition according to the NCP. Determination of the identity of a person or a good.

K

KEY (CRYPTOGRAPHIC)

Definition according to the NCP. The unique code which can be linked to an algorithm. This combination encrypts or decrypts data by a complex mathematical translation.

KEY GENERATION

Description key generation in relation with digital signatures according to the European Commission. The keys, which can also be generated by the user himself must be effectively unique and tamper proof (which is practically given by the choice of an appropriate key length and generation procedure). Otherwise the digital signature cannot be allocated fr legal relations in a reliable manner to data for which it has been generated and via the key to only one certain person o entity.

KEY MANAGEMENT

Definition according to the NCP. Procedures for generating, storing, exchanging, filing and erasing a key. The success of every security mechanism which can be used for encryption, largely depends on the effectiveness of the key management.

N

NON-REPUDIATION

Definition according to ISO/IEC 9548-8. Protects against the signing entity falsely denying some action.
Definition of mr Weemhofbased on ISOI/IEC 13888-1 and 7498-2. Non-repudiation is a security service to provide irrefutable proof to counter an entity's false denial of having participated in all or part of the communication.

P

PRIVATE KEY

Definition according to ISO/IEC 9548-8. (In a public key cryptosystem) that key of a user's key pair which is known only by that user .
Definition according to X.509. Private keys are secret numbers which are supposed to be known only to a particular entity. One is always associated with a single public key.

PUBLIC KEY INFRASTRUCTURE

Definition according to KPMG on behave of ECP .NL members. The complete system that is required to provide public-key encryption and digital signatures is known as a public-key infrastructure.

PUBLIC KEY

Definition according to ISO/IEC 9548-8. (In a public key cryptosystem) that key of a user'5 pair which is publicly known.
Definition according to X.509. Public keys are numbers associated with a particular entity, and are intended to be known to every-one who needs to have trusted interactions with that entity.

PUBLIC-KEY CRYPTOSYSTEM

Definition according to the NCP. A cryptosystem in which a key has generally known and secret components. A public key is known to everyone, the secret key only to the specific holder. In order to send a message, the sender encrypts it with the help of his own secret key and the public one of the receiver. The receiver uses his own secret key and the public key of the sender to decode.

R

REGISTRATION AUTHORITY

Definition according to PKIX (X.509). An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

SECRET KEY

Definition according to SEIS. A key used in symmetric encryption where the sender and receiver of encrypted messages uses the same secret key.

SESSION KEY

Definition according to FIPS-185, Escrowed Encryption Standard. The cryptographic key used by a device to encrypt and decrypt data during a session.

SIGNATORY

Definition according to the European Commission. Signatory means a person who creates an electronic signature.

T

TIME STAMP

Description of time stamping according to the European Commission. Time stamping is used in situations in legal relations, where proof of the exact time of a certain action (transmission, creation or receipt of a document or the time at which a declaration of intent is made) is crucial.

TTP (TRUSTED THIRD PARTY)

Definition according to the NCP. Impartial Organization delivering business confidence, through commercial and technical security features to an electronic transaction. It supplies technically and legally reliable means of carrying out5 facilitating, producing independent evidence about and/or arbitrating on electronic transactions. Its services are provided and underwritten by technical, legal, financial and/or structural means..
Definition according to KPMG on behave of ECP.NL members. A trusted Third Party is a party that is trusted by participants within a transaction and delivers , trust services' for digital exchange of data (electronic commerce)

ISO/IEC JTC 1/SC 27 Een TTP is een beveiligings autoriteit of diens agent, die vertrouwd wordt door andere entiteiten t.a.v. de beveiligingsdiensten waarin ze voorziet. Als een TTP de beveiligings autoriteit is voor een bepaald domein, dan kan het vertrouwen beperkt blijven tot dat domein.Definition according to CEN (PT 37).
A security authority or its agent, trusted by other principal with respect to security-related services.

V

VERIFICATION

Definition according to ISO/IEC 14888- 1. Een proces waarbij de input wordt gevormd door het getekende bericht, de verificatie sleutel en de domein parameters, en die als Output geeft het resultaat van de verificatie van de handtekening : geldig of niet geldig.
Definition according to the NCP. Checking someone' s signature using a reference value of the signature (visual or automated).

X

X.500

X.509 also known as ISOI/IEC 9594
Definition according to X.509. This Recommendation International Standard defines a framework for the provision of authentication services by Directory to its users. The title of this standard is: Information Technology-Open systems Interconnection- The directory Authentication framework.