

Rapportage Technische werkgroep Instrumentarium Rechtmatige Toegang

Inhoudsopgave

1.	Voorwoord	3
2.	Inleiding.....	4
2.1	Achtergrond en taakstelling.....	4
2.2	Randvoorwaarden.....	4
2.3	Doel van de rapportage.....	5
3.	TTP en vertrouwelijkheidsdiensten.....	6
3.1	Beleidsnotitie.....	6
3.2	TTP's, PKI's en de organisatie van vertrouwelijkheid	8
4.	Behoeftestelling van de opsporings-, inlichtingen- en veiligheidsdiensten	9
4.1	Juridische kaders	9
4.2	Europese resolutie als kader van de behoeftestelling	10
4.3	Nadere afbakening.....	11
4.4	Verwoording behoeftestelling opsporings- en inlichtingendiensten	11
5.	Technische architecturen geconfronteerd met de behoeftestelling.....	13
5.1	Definitie van een architectuur	13
5.2	Indelen van mogelijke technische architecturen in categorieën	13
5.2.1	Nadere afbakening.....	13
5.2.2	Technische overwegingen	13
5.2.3	Methoden.....	13
5.2.4	Sleutel.....	14
5.2.5	Algoritme	16
5.2.6	Architectuurcategorieën	16
5.3	Confrontatie architectuurcategorieën met de behoeftestelling	19
6.	Samenvatting, conclusie en aanbevelingen	22
6.1	Samenvatting.....	22
6.2	Conclusie.....	23
6.3	Aanbevelingen.....	23
Bijlage 1	Samenstelling/betrokkenen Technische Werkgroep.....	24
Bijlage 2	Overige punten genoemd tijdens de interviews	25

1. Voorwoord

Voor u ligt de rapportage van de *Technische Werkgroep Rechtmatige Toegang*. Deze rapportage is geschreven op basis van een aantal plenaire bijeenkomsten van de werkgroep en een gespreksronde met zowel behoeftestellers van rechtmatige toegang, alsmede met vertegenwoordigers van overheid en bedrijfsleven die betrokken zijn bij TTP-diensten voor vertrouwelijkheid. Tussentijdse concepten zijn verspreid en besproken met de betrokken partijen om zoveel mogelijk commentaar en aanvullingen te verzamelen. Deze commentaren zijn verwerkt in de nu voorliggende versie van het rapport. Hoewel door TNO gestructureerd en geredigeerd is deze rapportage dan ook het product van de technische werkgroep.

De leden van de werkgroep zijn geselecteerd in overleg tussen ECP.NL en de projectgroep Rechtmatige Toegang. De samenstelling van de werkgroep is terug te vinden in bijlage 1. Naast de input van de leden van de technische werkgroep is eveneens gebruik gemaakt van een aantal aan het TTP.NL project gerelateerde documenten.

Structuur van het rapport:

Het rapport valt uiteen in vier delen:

Deel 1. Inleiding

In hoofdstuk 2 wordt kort ingegaan op de achtergrond, taakstelling en randvoorwaarden van de werkgroep. In hoofdstuk 3 wordt vervolgens kort ingegaan op de achtergronden van het verkrijgen van rechtmatige toegang, het daarvoor te hanteren juridische kader, en relevante aspecten die uit beleidsdocumenten ter zake volgen.

Deel 2. Beschrijving behoeftestelling

In hoofdstuk 4 wordt verslag gedaan van de behoeftestelling zoals die bij opsporings- en inlichtingendiensten is gereconstrueerd aan de hand van interviews en documentanalyse.

Deel 3. Beschrijving technische architecturen en confrontatie met behoeftestelling

In hoofdstuk 5 wordt een analyse gegeven op basis waarvan een zestal generieke categorieën van technische architecturen worden benoemd, waarbinnen de huidige en de toekomstige technische middelen voor het verkrijgen van rechtmatige toegang zullen vallen. Vervolgens worden de verschillende architectuurcategorieën geconfronteerd met de behoeftestelling.

Deel 4. Aanbevelingen

Hoofdstuk 6 geeft een korte samenvatting van hetgeen in de eerdere hoofdstukken is beschreven en vervolgt met de conclusie en aanbevelingen van de technische werkgroep.

2. Inleiding

2.1 Achtergrond en taakstelling

In het kader van het Nationaal TTP-project is een Projectgroep Rechtmatige Toegang (RT) ingesteld. Omdat het hier om een maatschappelijk belang gaat zal een brede groep betrokkenen aan de ontwikkeling van een dergelijk, voor alle partijen aanvaardbaar instrumentarium moeten bijdragen. Het relevante bedrijfsleven heeft reeds aangegeven hieraan te willen meewerken, in een 'partnership approach' met de overheid. Indien het bedrijfsleven niet voldoende actief meewerkt aan de ontwikkeling van genoemd instrumentarium, zal de overheid nadrukkelijk overwegen om met nadere wetgeving de behoefte aan rechtmatige toegang in te vullen¹.

De projectgroep heeft tot taak om in een partnership approach tussen behoeftestellers en marktpartijen te onderzoeken in hoeverre een instrumentarium ontwikkeld kan worden dat rechtmatige toegang tot stromende en opgeslagen berichten waarborgt in het geval van vertrouwelijkheids TTP's. De projectgroep RT heeft een technische werkgroep ingesteld die tot taak heeft om vanuit een expliciet technische expertise te onderzoeken of een instrumentarium te ontwikkelen is waarmee rechtmatig afgetapte of anderszins rechtmatig verkregen versleutelde berichten ontcijferd kunnen worden, wederom voor zover die door tussenkomst van openbare TTP's, die versleuteling bij wijze van vertrouwelijkheidsdienst aanbieden, versleuteld worden of zijn. Het voorzitterschap van de technische werkgroep is in handen van TNO.

2.2 Randvoorwaarden

Voor de technische werkgroep is in overleg met de projectgroep een werkplan opgesteld. De in het projectplan van de projectgroep gestelde eisen golden als randvoorwaarden voor het projectplan. Deze hadden onder meer betrekking op de fasering en de uit te voeren taken. Het projectplan van de projectgroep formuleert externe voorwaarden, operationele eisen en ontwerpbeperkingen.

Externe voorwaarden

- De behoeftestellers dienen exact aan te geven wat hun behoeften zijn.
- De behoeftestellers dienen actief te participeren in de voorbereiding van een praktijktest.
- De ontwikkeling van het instrumentarium ligt expliciet bij het bedrijfsleven.

Operationele eisen

Het instrumentarium moet resulteren:

- Ofwel in een situatie waarbij de behoeftestellers kunnen beschikken over de oorspronkelijke informatie zonder dat ze zelf over het benodigde sleutel materiaal beschikken;
- Ofwel in een situatie waarbij de behoeftestellers de beschikking krijgen over het benodigd sleutel materiaal, waarmee ze de oorspronkelijke informatie volledig kunnen herleiden.

Ontwerpbeperkingen

Het instrumentarium mag geen invloed hebben op de onafhankelijkheid tussen de dienstverlening van TTP-diensten voor integriteit en authenticiteit en die voor vertrouwelijkheid.

¹ Tweede Kamer, vergaderjaar 1998-1999, 26581, nr. 1

2.3 Doel van de rapportage

Met instemming van de projectgroep is de technische werkgroep gestart met het maken van een inventarisatie van de eisen van de behoeftezoekers en met het in kaart brengen van technisch mogelijke architecturen voor TTP-vertrouwelijkheidsdiensten. Vervolgens is de behoeftezoeking geconfronteerd met de architecturen. Doel van de rapportage is het aan de projectgroep aangeven van de mogelijkheden en onmogelijkheden voor het verlenen van rechtmatige toegang door TTP's die vertrouwelijkheidsdiensten aanbieden, daarbij is geopereerd vanuit een technisch perspectief.

De betrokken partijen zijn door de projectgroep in overleg met het secretariaat van ECP.NL geïdentificeerd (zie bijlage 1).

3. TTP en vertrouwelijkheidsdiensten

3.1 Beleidsnotitie

In de beleidsnotitie “Nationaal TTP-project”² wordt onder een TTP verstaan:

“Een Trusted Third Party (TTP) is een betrouwbare derde partij die diensten aanbiedt om de betrouwbaarheid van de geautomatiseerde verwerking, uitwisseling en opslag van gegevens tussen partijen te waarborgen³.”

In de beleidsnotitie wordt een vijftal criteria genoemd waarlangs TTP's zijn te onderscheiden. De *eerste* betreft de waarborging van de betrouwbaarheid. Die heeft twee onderscheiden uitwerkingen:

- het waarborgen van *authenticiteit* en *integriteit* van gegevens;
- het waarborgen van de *vertrouwelijkheid* van gegevens.

Inrichting van het sleutelbeheer door de TTP is een *tweede* onderscheidend kenmerk. Sleutelgeneratie, -distributie, -opslag, en -vernietiging kan in het ene uiterste volledig bij de TTP zijn ondergebracht, en kan in het andere uiterste volledig bij de gebruiker zijn ondergebracht. Tussen beide uitersten zijn allerlei mengvormen van sleutelbeheer mogelijk.

Een *derde* onderscheid is die tussen *openbare* (voor iedereen toegankelijke) en *niet-openbare* (bedrijfsinterne) TTP-diensten. De beleidsnotitie handelt uitsluitend over openbare TTP-diensten⁴.

De topologie van de TTP-dienst biedt een vierde onderscheidend kenmerk. Er kan sprake zijn van een *in-line* TTP, een *on-line* TTP, een *off-line* TTP, en tot slot van een *no-line* TTP (zie figuur 1, overgenomen uit de beleidsnotitie, p. 12).

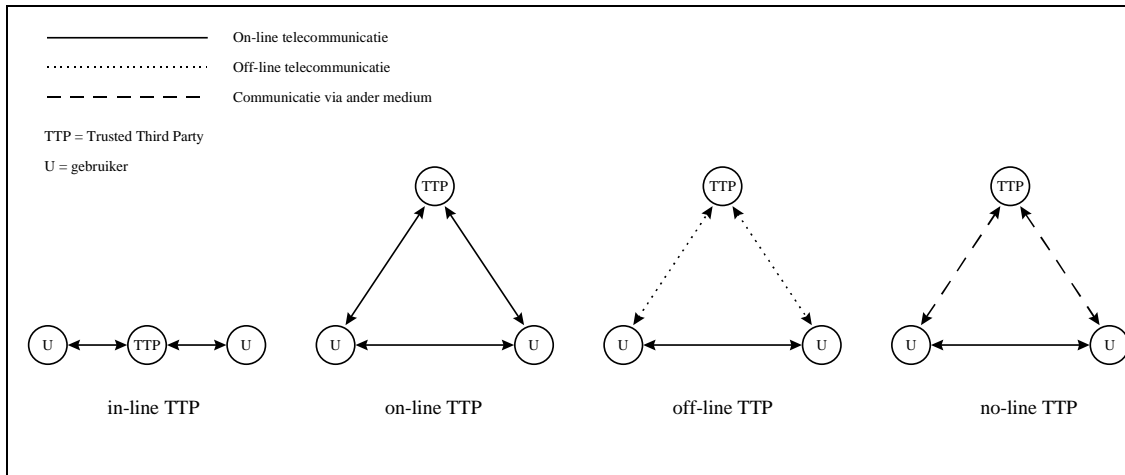
Het laatste onderscheidend criterium is het toepassingsgebied (zorgsector, financiële sector, het notariaat, de dienstensector, de detailhandel, de overheidssector en de accountancy). De differentiatie naar toepassingsgebieden van TTP's roept vragen op omtrent de haalbaarheid en wenselijkheid van het formuleren van een algemeen geldend stelsel van randvoorwaarden dat zowel noodzakelijk als voldoende is voor elke mogelijk denkbare TTP-dienst. Een eerste factor daarbij is dat per toepassingsgebied sprake kan zijn van aanvullende specifieke wet- en regelgeving. Een tweede factor die relateert aan het toepassingsgebied is het kostenaspect. Een stelsel van randvoorwaarden dat is toegesneden op toepassingen die zeer hoge eisen stellen aan een TTP-dienst is naar alle waarschijnlijkheid onnodig kostbaar voor toepassingen die lagere eisen stellen aan een TTP-dienst. De ontwikkeling van minder kostbare TTP-diensten –die een substantieel deel van het totale volume aan TTP-diensten kunnen vormen- zal door een te stringent stelsel van randvoorwaarden niet worden gestimuleerd, maar eerder worden belemmerd. Het formuleren van een te stringent stelsel van randvoorwaarden kan derhalve leiden tot een situatie die strijdig is met het doel van het

² Tweede Kamer, vergaderjaar 1998-1999, 26581, nr. 1

³ Deze definitie sluit nauw aan op INFOSEC93 definitie: “A Trusted Third Party is an impartial organisation delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means.” (In: Peeters & Schasfoort, 1997; 25).

⁴ In de beleidsnotitie wordt de volgende omschrijving aangehouden: “*Niet-openbare TTP-diensten* worden hierbij gedefinieerd als TTP-diensten die uitsluitend gebruik maken van een eigen infrastructuur en uitsluitend binnen één organisatie worden gebruikt ... daartegenover staan *openbare TTP-diensten*, gedefinieerd als TTP-diensten die in beginsel gebruik maken van een openbare infrastructuur en/of voor alle burgers, bedrijven en instellingen toegankelijk zijn.” (Tweede Kamer, vergaderjaar 1998-1999, 26581, nr. 1; p. 11).

nationale TTP-project, namelijk het stimuleren van de ontwikkeling van een nationale TTP-infrastructuur.



Figuur 1 - Topologie van de TTP-dienst (Nationaal TTP-project, 1999, p. 12)

Uitgaande van deze eerste karakterisering van mogelijke TTP-diensten en bijbehorende TTP-infrastructuur komt de beleidsnotitie tot een aantal randvoorwaarden inzake TTP-diensten voor vertrouwelijkheid (paragraaf 4). We concentreren ons hier specifiek op de randvoorwaarden inzake rechtmatige toegang. Het navolgende schema geeft het juridische kader rond de rechtmatige toegang weer.

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

Figuur 2 – Rechtmatige toegang op basis van huidige wet- en regelgeving (Nationaal TTP-project, 1999, p. 22)

Dit schema kan nader aangevuld worden met de verplichtingen die voortvloeien uit de Wet Bijzondere Opsporingsbevoegdheden en mogelijke verplichtingen uit het wetsvoorstel: Wet op de Inlichtingen- en Veiligheidsdiensten. In hoofdstuk 4 gaan we hier nader op in.

In de beleidsnotitie wordt met betrekking tot de waarborging van de rechtmatige toegang geconstateerd dat het internationale gebruik van TTP-diensten voor complicaties kan zorgen, aangezien de Nederlandse wet- en regelgeving niet voldoende aanknopingspunten biedt om in alle gevallen het benodigde sleutel materiaal te achterhalen. Overigens worden voor dit probleem ook oplossingsmaatregelen voorgesteld, bijvoorbeeld in de vorm van de verplichte opslag van een kopie van het geheime sleutel materiaal door een TTP binnen de jurisdictie, met een bewaarplicht en toegang door partijen met rechtmatige toegang.

De beleidsnotitie concludeert dat het nog te vroeg is om nu al uit te gaan van een bepaalde techniek of methodiek om versleutelde gegevens te kunnen ontcijferen. Deze conclusie geldt *mutatis mutandi* ook voor de aannames ten aanzien van de te benutten cryptografische algoritmen door TTP's en de technische omgeving (elektronische netwerken, mobiele telefonie) waarbinnen vertrouwelijkheidsdiensten kunnen worden ingezet. Een vorm van zelfregulering om op deze wijze een zekere toekomstvastheid in te bouwen, heeft de voorkeur boven uitsluitend een verplichtend wettelijk kader. Deze conclusie uit de beleidsnotitie betekent dat aannames over de in Nederland aan te bieden oplossingsrichtingen binnen de verschillende architecturen een enigszins vrijblijvend karakter zullen hebben.

3.2 TTP's, PKI's en de organisatie van vertrouwelijkheid

Hoewel het te vroeg is om te spreken van een uitgekristalliseerde structuur voor TTP's en de wijze waarop TTP's vertrouwelijkheidsdiensten aanbieden, is er in de praktijk wel een zekere ordening zichtbaar. Het kan overigens niet uitgesloten worden dat de zich nu aftekenende ordening slechts een tijdelijke is.

Hoewel exacte gegevens over de Nederlandse situatie ontbreken is een tot nu toe veel aangetroffen werkwijze die waarbij TTP's als *off-line* of *on-line* TTP met name de uitgifte van certificaten beheren en zich dus als Certification Authority opstellen. Het certificaat bevat onder meer (informatie over) het uit te geven sleutelpaar. Dit kan een sleutelpaar voor authenticatie en identificatie zijn (de digitale handtekening), of een sleutelpaar voor vertrouwelijkheid⁵. In de praktijk vindt geen registratie plaats van (de private/geheime) sleutels die voor de digitale handtekening worden uitgegeven. In het algemeen is er wel op zijn minst een optie voor *key recovery* in het geval van een sleutelpaar voor vertrouwelijkheid. Het private deel van de sleutel wordt zo opgeslagen dat deze op enigerlei wijze herleidbaar is.

Sleutelgeneratie kan ook plaatsvinden buiten de CA om. Ingewikkelde constructies van toelevering, *outsourcing*, beheer en organisatie van de sleutelgeneratie, -distributie, -opslag en -vernietiging zijn voorstelbaar, en komen in de praktijk ook voor. Niet alleen de enkele actie van de sleuteluitgifte is van belang voor de rechtmatige toegang, in feite gaat het om de integrale organisatie van de PKI waartoe de TTP behoort. Er zijn inmiddels al organisaties die de gehele PKI als tool aan derden aanleveren. Daarmee zijn deze organisaties niet onmiddellijk zelf TTP; wel kunnen zij een onmisbare schakel vormen in het geval van een *key recovery* procedure.

De sleutelgeneratie kan plaatsvinden bij de CA, maar kan ook plaatsvinden bij de gebruiker, of via een intermediaire organisatie. Verschillende manieren van aanpak komen in de huidige praktijk voor. Zoals gesteld, is er in het algemeen bij het gebruik van een sleutelpaar voor vertrouwelijkheid sprake van een optie tot een vorm van *key recovery*. In sommige gevallen wordt het aan de klant overgelaten of deze daar gebruik van wenst te maken. In andere is een *key recovery* procedure standaard ingebouwd. In weer andere gevallen vergt de *key recovery* procedure toegang tot een Root CA, die niet noodzakelijk in hetzelfde land gevestigd hoeft te zijn als de CA. *Key recovery* moet goed geregeld zijn, om te vermijden dat klanten TTP's aansprakelijkheid kunnen stellen voor niet toegestaan sleutelgebruik.

⁵ Gegeven het huidige gebruik van a-symmetrische crypto-algoritmen is er altijd sprake van een sleutelpaar, bestaande uit een aan elkaar gerelateerde publieke en de private sleutel.

4. Behoeftestelling van de opsporings-, inlichtingen- en veiligheidsdiensten

De behoeftestelling bij de opsporings- en inlichtingendiensten is onderwerp geweest van een inventariserend gesprek met de betreffende leden van de technische werkgroep. Tevens is de Europese resolutie die handelt over de rechtmatige interceptie van telecommunicatie als brondocument geraadpleegd⁶. Tot slot dient de Nederlandse wet- en regelgeving als kader voor de behoeftestelling. In het navolgende komt eerst het juridische kader aan de orde, vervolgens de Europese resolutie en tot slot de bevindingen en de conclusies ten aanzien van de eisen van de behoeftestellers.

4.1 Juridische kaders

Hoewel de juridische kaders van belang zijn voor de afbakening van de behoeftestelling, beperken we ons in deze rapportage slechts tot een schets van de meest relevante raamwerken en wetten. De noodzakelijke nadere toetsing en weging van de juridische kaders valt buiten het werkveld en de taakstelling van de technische werkgroep. In figuur 3 vindt een verdere uitwerking plaats van het juridisch kader dat in de beleidsnotitie “Nationaal TTP-project” is weergegeven. Het gaat om het ingediende wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten (Tweede Kamer, vergaderjaar 1997 – 1998, 25 877, nrs. 1-2) en de Wet Bijzondere Opsporingsbevoegdheden⁷.

Juridisch kader	Strafvordering	Staatsveiligheid
Opgeslagen gegevens	Wet Computer Criminaliteit	Wet op de Inlichtingen- en Veiligheidsdiensten
Stromende gegevens	Telecommunicatiewet Wet Bijzondere Opsporingsbevoegdheden	Wet op de Inlichtingen- en Veiligheidsdiensten Telecommunicatiewet

Figuur 3 – Juridisch kader voor behoeftestelling.

In 1993 is het Wetboek van Strafvordering gewijzigd zoals omschreven in de Wet Computercriminaliteit. Het strafvorderlijk instrumentarium (van belang voor het Ministerie van Justitie) werd daarmee uitgebreid met de verplichting tot ontsleutelen van versleutelde data voor zover deze kennis aanwezig was bij aangesprokene. Verdachten kunnen echter niet verplicht worden om data te ontsleutelen die tot hun eigen bewijslast behoren (nemo teneur beginsel). Dit heeft tot gevolg dat in de behoeftestelling tot rechtmatige toegang deze gerealiseerd zal moeten kunnen worden zonder medewerking van de eindgebruiker. Op 15 december 1998 is de nieuwe Telecommunicatiewet in werking getreden die o.a. aftapverplichting voor aanbieders van openbare telecommunicatie infrastructures uitbreidt tot internet service providers en andere aanbieders van openbare telecomdiensten. Aanbieders van openbare telecomdiensten moeten voorzieningen ingebouwd hebben om stromende gegevens beschikbaar te maken. Middels de Wet Bijzondere Opsporingsbevoegdheden (een wijziging van het Wetboek van Strafvordering) kan de belastende informatie bij de openbare telecomdiensten daadwerkelijk worden verzameld. Tijdens het opsporingsproces toetst de rechter commissaris de door de (hoofd)officier van justitie voorgestelde inzet van middelen. Tijdens de rechtszitting wordt de rechtmatigheid daarvan door de rechter nogmaals getoetst.

⁶ Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal of the European Communities, 96/C 329/01

⁷ De behandeling van de Wet op de Inlichtingen- en Veiligheidsdiensten (Tweede Kamer, vergaderjaar 1997-1998, kamerstuk 25 877) is nog niet afgerond. De Wet Bijzondere Opsporingsbevoegdheden is een wijziging van het Wetboek van Strafvordering.

Justitie moet toegang hebben tot alle informatie die beschikbaar gesteld kan worden in de context van strafvordering.

Het juridisch kader dat voor de inlichtingen- en veiligheidsdiensten geldt, wordt enerzijds gevormd door de al eerder genoemde Telecomwet, anderzijds door de Wet op de Inlichtingen- en Veiligheidsdiensten. Voor opgeslagen gegevens is artikel 24, lid 3 van toepassing: “Een ieder die kennis draagt ter zake het ongedaan maken van de versleuteling van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk als bedoeld in het eerste lid, is verplicht het hoofd van de dienst⁸ op diens schriftelijk verzoek alle noodzakelijke medewerking te verlenen om deze versleuteling ongedaan te maken”. Voor stromende gegevens is artikel 25, lid 8 van toepassing: “Een ieder die kennis draagt ter zake van het ongedaan maken van de versleuteling van gesprekken, telecommunicatie of gegevensoverdracht als bedoeld in het eerste lid, is verplicht het hoofd van de dienst op diens schriftelijk verzoek alle noodzakelijke medewerking te verlenen om deze versleuteling ongedaan te maken”.

De informatie die door inlichtingen- en veiligheidsdiensten wordt verzameld, wordt niet gebruikt in een openbaar strafproces.

4.2 Europese resolutie als kader van de behoeftestelling

Een tweede kader voor de behoeftestellers wordt geboden door de Europese resolutie die handelt over de rechtmatige interceptie van telecommunicatie⁹. Door de projectgroep is aan de technische werkgroep aangegeven dat deze resolutie als basis genomen kan worden voor de behoeftestelling. In deze resolutie worden aanbevelingen geformuleerd die aangesloten landen kunnen overnemen in nationale wetgeving. De resolutie omschrijft een groot aantal vereisten waaraan nationale wetgeving tegemoet zou dienen te komen. De eerste twee artikelen van deze resolutie geven een indruk van de eisen waaraan tegemoet moet worden gekomen.

1. “Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that are generated to process the call.”
2. “Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.”

Vervolgens gaat de resolutie in op randvoorwaarden waaraan voldaan moet zijn voor rechtmatige toegang. Deze randvoorwaarden hebben betrekking op de te verkrijgen assistentie van de netwerk/service operators, op de waarborging van een niet te corrumperen interceptie, en op de mogelijkheid om meerdere intercepties tegelijkertijd uit te kunnen voeren.

⁸ Bedoeld wordt: het hoofd van de inlichtingen- en veiligheidsdienst.

⁹ Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal of the European Communities, 96/C 329/01

4.3 Nadere afbakening

Het valt buiten de context van de opdracht van de technische werkgroep om de vereisten van de Europese resolutie volledig te vertalen naar de situatie rond TTP-diensten. In deze opdracht wordt immers 'sec' gekeken naar de TTP-vertrouwelijkheidsdiensten.

De Europese resolutie gaat in essentie over de onderschepping van berichtenverkeer dat verloopt over de telecommunicatie-infrastructuur. Dat kan zowel gaan om gecijferd berichtenverkeer als om niet-gecijferd verkeer. De Europese resolutie stelt zelf dan ook geen nadere eisen aan opzet en levering van door TTP te leveren vertrouwelijkheidsdiensten. Wel geeft de resolutie inzicht in de globale wensen en behoeften van de opsporings- en inlichtingendiensten.

Voor wat betreft de behoeftestelling kan opgemerkt worden dat rechtmatige toegang niet alleen een zaak is van opsporings-, inlichtingen- en veiligheidsdiensten. Ook de eigenaren van de informatie (of bijvoorbeeld hun erfgenamen) hebben rechtmatig toegang tot de oorspronkelijke gegevens. T.b.v. rechtmatige toegang voor de eigenaren/gebruikers zijn door de TTP's voorzieningen ingebouwd. Uit de bijeenkomsten van de technische werkgroep kwam naar voren dat in de meeste gevallen deze toegang echter alleen worden verkregen met medewerking van de eigenaren/gebruikers. Gelet op de eis dat rechtmatige toegang vanuit het perspectief van opsporings- en inlichtingendiensten verkregen dient te kunnen worden zonder medewerking van de eindgebruiker/eigenaren, is de gehanteerde technologie in veel gevallen dan ook niet toereikend. In de gevallen waar de TTP voorzieningen heeft ingebouwd, waarmee buiten de gebruiker om rechtmatige toegang kan worden verkregen, kan de betreffende TTP deze voorzieningen ook benutten voor opsporings- c.q. staatsveiligheidsdoeleinden.

Er zal nog moeten worden bepaald tot hoe ver terug in de tijd TTP's geacht kunnen worden om sleutels te kunnen reconstrueren. Door de opsporings- en inlichtingendiensten wordt voorgesteld om de bewaartermijnen gelijk te stellen aan de bewaartermijnen die in de telecommunicatiewet zijn genoemd.

4.4 Verwoording behoeftestelling opsporings- en inlichtingendiensten

De behoeftestelling die uit de gesprekken met vertegenwoordigers van opsporings- en inlichtingendiensten naar voren komt valt uiteen in drie delen. De eerste twee delen zijn momenteel onderwerp van studie en discussie in parallel lopende trajecten. Het derde deel staat centraal in deze rapportage van de technische werkgroep:

1. Algemene gegevens
(naam, adres, postcode, woonplaats, nummer en soort dienst van personen die gebruik maken van openbare telecommunicatienetwerken of -diensten. Deze zogeheten gebruikersgegevens stellen de opsporingsambtenaar in staat na te gaan met welke persoon hij van doen heeft als hij bijvoorbeeld een bepaald nummer of adres heeft);
2. Verkeersgegevens
(deze gegevens betreffen het telecommunicatieverkeer van de gebruiker. Hierdoor kan inzicht worden verkregen in telecommunicatiegedrag en het patroon van contacten van een persoon);
3. Klare tekst
(de opsporings- en inlichtingendiensten willen dat de tekst begrijpbaar wordt aangeleverd. In principe willen zij geen private sleutels in bezit hebben. Alleen indien het niet anders kan zullen de sleutels ter beschikking moeten worden gesteld).

De behoefte aan “Klare tekst” geldt specifiek voor vertrouwelijkheidsdiensten waar een TTP bij betrokken is en staat dan ook centraal in deze rapportage van de technische werkgroep¹⁰. Indien er verder wordt ingezoomd op de behoefte aan “Klare tekst” blijkt dat ondanks het verschillende wetgevingsregime de feitelijke behoeftestelling van de opsporings- en inlichtingendiensten voor wat betreft “Klare tekst” overeen komt:

- De opsporings- en inlichtingendiensten willen dat de tekst begrijpbaar wordt aangeleverd. In principe willen zij geen private sleutels in bezit hebben. Alleen indien het echt niet anders kan zullen de sleutels ter beschikking moeten worden gesteld;
- Voor stromende gegevens dient ‘real time’ meegekeken te kunnen worden;
- De volledige informatie dient ter beschikking te komen;
- Toegang moet kunnen worden verkregen zonder medewerking en/of medeweten van de eindgebruiker.

Daarnaast zal de behoeftestelling voor wat betreft “Klare tekst” ingepast moeten worden in een raamwerk waarin ook andere kwesties ten aanzien van het omgaan met de rechtmatig verkregen sleutels zullen moeten worden geregeld. Dat gaat onder meer om:

- Bewaartermijnen; rechtmatige toegang is juridisch gebonden aan termijnen. Indien sleutels verkregen zijn die het mogelijk maken om berichtenverkeer te monitoren zullen technische voorzieningen ingebouwd moeten worden die beletten dat een sleutel na het aflopen van de juridische termijn, waarin de rechtmatige toegang verleend is, nog gebruikt kan worden. In het geval de opsporing niet tot resultaat heeft geleid, zal zonder dat dit kenbaar hoeft te worden gemaakt, een technische voorziening moeten worden ingebouwd die garantie, c.q. uitsluiting van de aansprakelijkheid biedt.
- Vernietiging van sleutelmateriaal; ook in gevallen waarin wel bewijslast is verkregen zal iets geregeld moeten worden omtrent de vernietiging van sleutelmateriaal. Ook dit zou bij voorkeur op een technisch niet te corrumpere wijze plaats moeten vinden¹¹.

¹⁰ Naast deze behoeftestelling zijn er tijdens de gesprekken met de behoeftezoekers, alsmede uit de bestudering van bijvoorbeeld de Europese resolutie gerelateerde behoeftes naar voren gekomen, zoals bijvoorbeeld het verkrijgen van verkeersgegevens. Om de reeds lopende discussies omtrent het aftappen van ISP's en Telco's niet te vermengen met het werk van deze technische werkgroep wordt in deze rapportage alleen gekeken naar de specifieke aspecten uit de behoeftestelling die betrekking hebben op rechtmatige toegang bij vertrouwelijkheidsdiensten door TTP's.

¹¹ Een van de gesprekspartners voerde aan dat een vorm van geïnverteerd gebruik van hashing hiertoe mogelijkheden zou kunnen bieden. Of dit de meest aangewezen manier is, blijft buiten het bestek van deze rapportage. Opgemerkt wordt dat over dergelijke technische beveiligingsmaatregelen al wordt nagedacht.

5. Technische architecturen geconfronteerd met de behoeftestelling

In dit hoofdstuk worden zes generieke categorieën van architecturen geïntroduceerd. Door deze generieke architectuurcategorieën te confronteren met de behoeftestelling wordt het mogelijk om zo toekomstvast mogelijk uitspraken te doen over de keuzes die gemaakt moeten worden ten aanzien van het onderwerp “vertrouwelijkheidsdiensten en rechtmatige toegang”¹².

5.1 Definitie van een architectuur

Voordat de verschillende architecturen kunnen worden gecategoriseerd wordt aangegeven wat in deze rapportage onder een architectuur wordt verstaan.

Een architectuur is een abstracte beschrijving van de technische inrichting die nodig is om een vertrouwelijkheidsdienst aan te bieden. In ons geval komt de beschrijving tot uiting door aan te geven welke specifiek met het aanbieden van vertrouwelijkheidsdiensten samenhangende rol de TTP en de gebruiker (target/verdachte) van een vertrouwelijkheidsdienst speelt. De mogelijke rollen worden in paragraaf 5.2.6 beschreven.

5.2 Indelen van mogelijke technische architecturen in categorieën

Om te komen tot een categorisering van de verschillende architecturen zal eerst worden ingegaan op een aantal technische mechanismen. Achtereenvolgens worden de twee cryptografische methoden en de werking van sleutel en algoritme beschreven, waarna op basis van de mogelijke rollen van de TTP een categorisering van mogelijke architecturen wordt opgezet.

5.2.1 Nadere afbakening

Naast de randvoorwaarden zoals die in sectie 1.2 genoemd zijn, zijn de volgende randvoorwaarden van belang om de probleemstelling in technische en logische zin af te bakenen:

- Het gaat om het verkrijgen van rechtmatige toegang tot informatie die gecijferd is ter bescherming van de vertrouwelijkheid (het gaat dus niet over authenticatie bij digitale handtekeningen).
- Bij de totstandkoming van de gecijfering is op de een of andere manier gebruik gemaakt van een TTP.
- Hoewel de behoeftestelling naast de behoefte aan klare tekst ook de behoefte aan algemene- en verkeersgegevens omvat, wordt in deze rapportage alleen bekeken hoe de behoefte aan klare tekst, vanuit de technologie kan worden ingevuld.

5.2.2 Technische overwegingen

Om rechtmatige toegang te verkrijgen zal ontcijfering plaats moeten vinden. Om te kunnen ontcijferen zijn twee elementen noodzakelijk: de sleutel en het algoritme. In het algemeen zijn er twee soorten cryptografische methoden te onderscheiden die elk van verschillende algoritmen en sleuteltypen gebruik maken. Onderstaand wordt dat verschil eerst duidelijk gemaakt. Vervolgens wordt ingegaan op de aspecten: sleutel en algoritme.

5.2.3 Methoden

Bij het achterhalen van de sleutel is het van belang om te weten wie over deze sleutel beschikt. Voor de gecijfering en ontcijfering van berichten ter bescherming van de

¹² Om te komen tot pro-actieve beleidsvorming is er voor gekozen om een generieke indeling van architectuurcategorieën te maken in plaats van het beschrijven van alle huidige beschikbare technologieën voor het verkrijgen van rechtmatige toegang.

vertrouwelijkheid kunnen we onderscheid maken tussen twee cryptografische methoden. Het sleutelbeheer bij gebruik van deze twee methoden is erg verschillend wat evidente gevolgen heeft voor een eventueel technisch instrumentarium voor rechtmatige toegang. We onderscheiden:

- **Asymmetrische vercijfering.** Bij dit type vercijfering wordt het bericht vercijferd met de publieke sleutel van de ontvangende partij. Alleen de ontvangende partij is in staat om het bericht te ontcijferen omdat die de enige is die de private sleutel kent. De publieke en de private sleutel zijn onlosmakelijk met elkaar verbonden en vormen samen het sleutelpaar. Doorgaans is de publieke sleutel gecertificeerd door een TTP, waardoor de identiteit van de ontvanger gekoppeld is aan de publieke sleutel. Ook bij opslag van informatie kan asymmetrische vercijfering worden toegepast.
- **Symmetrische vercijfering.** Wanneer twee partijen een onderling uit te wisselen bericht op een symmetrische manier willen vercijferen, maken ze gebruik van een geheime sleutel die alleen bij deze twee partijen bekend is. Zowel vercijfering (encryptie) als ontcijfering (decryptie) worden met deze geheime sleutel gedaan. Ook bij opslag van informatie kan symmetrische vercijfering worden toegepast.

De core business van een TTP is het uitgeven en beheren van certificaten. Een certificaat is in feite een digitale handtekening van een TTP op een publieke sleutel waardoor de publieke sleutel aan een bepaalde identiteit wordt gekoppeld. Wanneer een TTP dus direct betrokken is bij de vercijfering van een bericht, is er doorgaans sprake van asymmetrische vercijfering. Dit is het geval wanneer het bericht is vercijferd met een publieke sleutel die door een TTP is gecertificeerd.

Het is echter ook mogelijk dat een TTP indirect bij een vercijfering is betrokken. Bijvoorbeeld wanneer de sleutel (symmetrisch of asymmetrisch) die door de eindgebruiker gebruikt is voor vercijfering, is opgeslagen nadat die sleutel met een door die TTP uitgegeven publieke sleutel is vercijferd (Meer ingewikkelde cryptografische scenario's voor bijvoorbeeld key recovery zijn hier ook denkbaar).

Ook bij het gebruik van sessiesleutels is het mogelijk dat een TTP indirect betrokken is bij de vercijfering. Een sessiesleutel, die meestal symmetrisch is, is een sleutel die twee partijen onderling afspreken voor een bepaalde sessie van berichtenuitwisseling. Om de sessiesleutel vertrouwelijk af te kunnen spreken wordt soms gebruik gemaakt van reeds bestaande asymmetrische sleutels die dan weer door een TTP zijn uitgegeven. Een in de praktijk veel gebruikt protocol dat op deze wijze werkt is het Secure Sockets Layer¹³ (SSL) protocol. Om de sessiesleutel te achterhalen die m.b.v. het SSL protocol is gemaakt, zou een mogelijke oplossing zijn:

1. Achterhaal de benodigde private sleutels van cliënt en server.
2. Onderschep de berichtenuitwisseling gedurende de aanloop van het SSL protocol waarin de sessiesleutel wordt afgesproken.
3. Ontcijfer de berichten in de aanloopfase m.b.v. de private sleutels en construeer met die informatie de sessiesleutel.

Wanneer de sessiesleutel is achterhaald kan het bericht, waar het uiteindelijk allemaal om te doen was, worden ontcijferd.

5.2.4 Sleutel

Voor wat betreft het achterhalen van de sleutel zijn er gedurende de levenscyclus van de sleutel een aantal handelingen aan te wijzen waar mogelijk (achteraf) informatie over de sleutel is te achterhalen. De stappen, in een chronologische volgorde, die hiervoor in aanmerking komen zijn:

1. Generatie van de sleutel die nodig is voor het ontcijferen van het betreffende bericht. In geval van asymmetrische vercijfering wordt er een sleutelpaar gegenereerd: de publieke

¹³ Zie bijvoorbeeld <http://www.surfnet.nl/innovatie/surf-ace/security/doc/ssl.html>

sleutel voor vercijfering en de private sleutel voor ontcijfering (bij gebruik van een digitale handtekening is dit omgekeerd). Bij symmetrische vercijfering wordt één sleutel gecreëerd.

2. Certificatie van de sleutel. Wanneer de sleutel, die gebruikt dient te worden voor ontcijfering van het bericht, gecertificeerd is, is van belang te weten wie de certificatie heeft geregeld. Dit kan alleen het geval zijn bij asymmetrische sleutels. Aangezien bij certificatie alleen de publieke sleutel betrokken is, is bij deze handeling afgezien van de sleutellengte geen informatie omtrent de private sleutel te achterhalen.
3. Transport en distributie van de sleutel. Wanneer de sleutel op een andere plek gegenereerd wordt dan waar hij gebruik wordt, dient de sleutel getransporteerd te worden. Dit kan via een telecommunicatiepad, per brief, diskette, smart card etc. Onderschepping van dit transport is een mogelijkheid om informatie over de sleutel te achterhalen.
4. Installatie en update van de sleutel. Bij ingebruikname van de sleutel wordt de sleutel op het systeem van de gebruiker geïnstalleerd. Wanneer de geldigheidsperiode is verstreken vindt er een update plaats. Het kan zijn dat alle versleutelde informatie eerst met de oude sleutel moet worden ontcijferd en vervolgens met de nieuwe sleutel weer vercijferd, waardoor het systeem extra kwetsbaar is. Mogelijk worden ook hier sporen achtergelaten die tot de sleutel kunnen leiden.
5. De opslag van de sleutel waarmee het bericht ontcijferd kan worden. Met opslag bedoelen we het bewaren van de sleutel zodat de gebruiker indien nodig er gebruik van kan maken. Waar is de sleutel opgeslagen en wie heeft toegang tot de opslag? Mogelijk wordt niet de sleutel zelf opgeslagen maar een gedeelte van de sleutel, een referentie naar de sleutel, of een vercijferde versie van de sleutel. Meer partijen kunnen bij de opslag betrokken zijn.
6. Verificatie. Wanneer de echtheid van een bepaalde sleutel moet worden gecontroleerd bestaat soms de mogelijkheid tot verificatie. Bijvoorbeeld de verificatie van een certificaat bij een TTP, of de verificatie van een symmetrische sleutel bij gebruik van PGP. Omdat de sleutel zelf voor verificatie niet bekend hoeft te worden, zijn de mogelijkheden tot achterhalen van de sleutel bij verificatie gering.
7. Encryptie van het bericht. Wie heeft het bericht versleuteld? In geval van symmetrische vercijfering is de sleutel voor vercijfering en ontcijfering gelijk en is degene die de vercijfering heeft gedaan ook in staat om de ontcijfering te doen, als die tenminste nog steeds over de sleutel beschikt. Bij asymmetrische vercijfering hoeft dit niet het geval te zijn, in het bijzonder bij het beschermen van de vertrouwelijkheid bij het versturen van berichten.
8. Key recovery, archivering e.d. Wie is in staat om de sleutel, die gebruikt dient te worden voor ontcijfering van het bericht, te achterhalen of reconstrueren? Soms zijn key recovery mogelijkheden aanwezig. Soms wordt een sleutel na vernietiging gearchiveerd. Dit biedt extra mogelijkheden om de sleutel te achterhalen.
9. Revocatie van de sleutel. Wanneer een sleutel niet meer geschikt is voor operationeel gebruik kan de sleutel gerevoceerd worden. Wanneer het bericht is te ontcijferen met een gerevoceerde sleutel is deze sleutel mogelijk uit een revocatielijst te achterhalen. Het gaat hier om de situatie waarin een sleutel werd gerevoceerd *nadat* het bericht in kwestie is vercijferd. Ter verduidelijking: wanneer de sleutel gecertificeerd is, blijft het principe gelijk; alleen is er dan sprake van revocatie van het certificaat i.p.v. de sleutel.
10. Vernietiging van de sleutel. Wanneer een sleutel niet meer gebruikt wordt bestaat de mogelijkheid dat hij vernietigd wordt. Alle mogelijke sporen die tot de sleutel kunnen leiden dienen uitgewist te worden. Wanneer dit niet zorgvuldig genoeg gedaan wordt zijn er nieuwe kansen om de sleutel te herleiden.

Er zijn een aantal onderdelen van de sleutel levenscyclus opgesomd, waar mogelijk informatie omtrent de sleutel te achterhalen valt. Wanneer het algoritme bekend is, is er altijd

de mogelijkheid om met brute force alle mogelijke sleutels te proberen maar zelfs wanneer de reken capaciteit daarvoor voldoende aanwezig is, levert een dergelijke aanpak geen real-time toegang tot gecijferde gegevens. Voor de ontwikkeling van een instrumentarium richten wij ons daarom op die gevallen waar het voor alle betrokken partijen duidelijk is hoe de sleutel in zijn geheel direct kan worden gereconstrueerd. In paragraaf 5.2.6 zal hier verder op worden ingegaan.

5.2.5 Algoritme

Behalve de sleutel is het ook van belang om het algoritme te achterhalen dat voor ontcijfering benodigd is. Voor wat betreft het algoritme voor ontcijfering zijn ook een aantal mogelijkheden te onderscheiden. Vaak zal het gebruikte algoritme een publiekelijk bekend algoritme zijn. Veelal wordt tijdens het opzetten van een berichtenuitwisseling door de partijen onderhandeld welke cryptografische algoritmen (of apparatuurversies) er aan beide zijden beschikbaar zijn en welke cryptografie qua sterkte van sleutellengte-algoritme combinatie acceptabel is voor iedere partij. Deze protocolonderhandelingen kunnen onderschept worden, waarna men hetzelfde algoritme kan selecteren uit de eigen bibliotheek resp. kan men via leveranciersinformatie achterhalen welk(e) algoritme(n) door desbetreffende apparatuur ondersteund word(t)(en). Het kan ook zijn dat een gebruiker een eigen algoritme of een modificatie van een bestaand algoritme heeft bedacht. Of dat gebruik is gemaakt van een algoritme dat van een TTP of specifiek bedrijf afkomstig is.

Wanneer er gebruik is gemaakt van een standaard, bekend algoritme is het in het algemeen eenvoudig om het daadwerkelijk gebruikte algoritme te achterhalen. Door namelijk een library bij te houden waar alle bekende algoritmen in zijn opgenomen, is het een kwestie van één voor één deze algoritmen te proberen totdat er een klare tekst uitkomt die zinnig lijkt. Wanneer het verkeerde algoritme wordt gebruikt zal het ontcijferde bericht immers wartaal bevatten.

In het geval dat er geen standaard algoritme gebruikt is en het algoritme op generlei wijze te achterhalen is, zal om het algoritme te achterhalen cryptanalyse moeten worden toegepast. Dit houdt een arbeidsintensieve zoektocht in waarbij via wiskundige omwegen informatie omtrent het algoritme zal moeten worden achterhaald. Een dergelijke oplossing sluit het verkrijgen van real-time toegang tot gecijferde berichten uit.

Er ontstaat een echt probleem voor rechtmatige toegang wanneer het gebruikte algoritme geen algemeen bekend algoritme is en het daadwerkelijk benodigde ontcijferalgoritme op geen enkele wijze te achterhalen valt.

5.2.6 Architectuurcategorieën

Eén van de uitgangspunten (zie 4.1) is dat de gecijfering van de informatie tot stand moet zijn gekomen met behulp van een TTP. De betrokkenheid van die TTP kan behoorlijk variëren. De sleutel kan direct worden opgevraagd wanneer de sleutel bij de TTP is opgeslagen of wanneer de TTP de sleutel kan reconstrueren (key recovery). Het kan ook zijn dat de TTP de sleutel niet alleen kan reconstrueren of helemaal niet in staat is om aan herleiding van de sleutel bij te dragen. Daarnaast is de rol die de eindgebruiker speelt van belang. De architectuurcategorieën worden dan ook vorm gegeven aan de hand van de betrokkenheid van de TTP en de eindgebruiker daarin.

Binnen de verschillende architecturen is een aantal mogelijke rollen te onderscheiden waarbij mogelijk de sleutel of het algoritme bekend kan worden:

- *Sleutelgeneratie*. Wanneer de TTP zorgdraagt voor het genereren van de sleutels betekent dit niet automatisch dat de TTP ook een kopie van de gegenereerde sleutel in zijn bezit heeft. Hiervoor is een aanvullende actie van de gebruiker nodig die in de praktijk niet altijd is ingebouwd. Ook is het mogelijk dat de gebruiker zelf zijn sleutels genereert met behulp van bijvoorbeeld PGP.

- *Encryptie*. In het geval van een in-line TTP verzorgt de TTP de encryptie. In geval van symmetrische encryptie betekent dat ook dat de TTP in staat is om het bericht te ontcijferen. In geval van asymmetrische encryptie hoeft dat niet het geval te zijn. Degene die de encryptie heeft gedaan, kent normaal gesproken ook het algoritme dat nodig is voor decryptie.
- *Sleutelopslag*. De geheime sleutel, in geval van symmetrische encryptie, of de private sleutel, in geval van asymmetrische encryptie, zal zijn opgeslagen in een al dan niet beveiligde omgeving. Dat kan bij de TTP zijn of bij de gebruiker. Wanneer de sleutel op een bepaalde plek is opgeslagen impliceert dit de mogelijkheid tot key recovery. Afhankelijk van de gekozen policy kan de sleutel worden opgehaald met of zonder medewerking van de eindgebruiker. In de praktijk komen beide gevallen voor.
- *Key recovery*. Soms wordt de mogelijkheid tot key recovery geboden. Bijvoorbeeld om, in geval de gebruiker niet meer over zijn sleutel beschikt, deze te reconstrueren zodat versleuteld opgeslagen berichten weer kunnen worden gelezen. Er zijn diverse constructies denkbaar voor key recovery. Belangrijk hierbij is welke partijen noodzakelijk mee moeten werken aan het reconstructieproces. Buiten de TTP en de gebruiker zelf, kan er nog een derde partij betrokken zijn zoals het bedrijf waaraan de PKI is uitbesteed, of een vertrouwenspartij in geval van key escrow.
- *Algoritme-ontwerp*. Wanneer gebruik is gemaakt van standaardapplicaties zal het decryptie algoritme vaak publiek bekend zijn dan wel eenvoudig te achterhalen. In sommige gevallen kan het gaan om een algoritme dat door de gebruiker zelf is ontworpen waardoor het lastiger is om dit algoritme te herleiden.

Aangezien de functies van sleutelopslag en key recovery enige overlap kunnen hebben, zullen we in dit rapport de volgende scheiding hanteren: onder sleutelopslag verstaan we het in zijn geheel opslaan van de sleutel op een bepaalde plaats zodat tijdens de encryptie van de sleutel gebruik kan worden gemaakt. Dit in tegenstelling tot key recovery, waarbij er mogelijk meerdere partijen betrokken kunnen zijn bij het achterhalen van de sleutel en de sleutel niet noodzakelijk op één bepaalde plek hoeft te zijn opgeslagen. Het doel van key recovery is niet het achterhalen van de sleutel voor gebruik tijdens encryptie, maar het reconstrueren van de sleutel in het geval dat de sleutel onbruikbaar geworden is.

Wanneer we de boven opgesomde rollen variëren kunnen we in principe alle mogelijke architecturen indelen in zes generieke categorieën. Met ‘gebruiker’ wordt in het onderstaande schema de persoon bedoeld die gebruik maakt van een vertrouwelijkheidsdienst. Door de opsporings- en inlichtingendiensten wordt deze persoon ook wel verdachte of target genoemd.

Architectuurcategorie 1. Deze categorie omvat alle architecturen die zich kenmerken doordat de gebruiker van de vertrouwelijkheidsdienst het algoritme zelf heeft ontworpen en waarbij hij de enige is die kennis heeft omtrent het algoritme. In deze categorie architecturen kan de TTP bij minstens één van de rollen generatie, encryptie, opslag of key recovery betrokken zijn.

Architectuurcategorie 2. De architecturen in deze categorie kenmerken zich doordat de gebruiker bij alle rollen betrokken is. Het verschil met de eerste categorie is dat het algoritme publiekelijk bekend is. De rol van de TTP in deze categorie beperkt zich tot deelnemende partij aan de key recovery.

Architectuurcategorie 3. In deze categorie zitten alle architecturen waarbij het algoritme publiekelijk bekend is, en waarbij de private (of geheime) sleutel ook op een plek buiten bereik van de gebruiker is opgeslagen. Binnen deze categorie kan de TTP één of meer van de rollen generatie, encryptie, opslag en key recovery vervullen. Het maakt voor deze architectuurcategorie niet uit wie de key recovery, sleutelgeneratie, encryptie, of sleutelopslag verzorgt.

Architectuurcategorie 4. Deze categorie omvat alle architecturen waarbij het algoritme publiekelijk bekend is en waarbij de gebruiker niet betrokken is bij de key recovery. De TTP zal in elk van deze architecturen bij minstens één van de rollen generatie, encryptie, opslag of key recovery betrokken zijn. Het maakt voor deze architectuurcategorie niet uit wie de key recovery, sleutelgeneratie, encryptie, of sleutelopslag verzorgt.

Architectuurcategorie 5. De architecturen in deze categorie kenmerken zich doordat het algoritme algemeen bekend is, en de gebruiker zowel bij opslag als key recovery betrokken is. Het verschil met categorie 2 is dat een andere partij dan de gebruiker de generatie verzorgt. De betrokkenheid van de TTP in deze categorie is beperkt tot één of meer van de rollen generatie, encryptie of key recovery.

Architectuurcategorie 6. Tijdens de generatie van de sleutel in deze categorie wordt geen kopie buiten de gebruiker opgeslagen. Net als in categorieën 2 en 5 is in deze categorie van architecturen het algoritme algemeen bekend en is de gebruiker zowel bij opslag als bij key recovery betrokken. Het verschil met de architecturen van categorie 2 is echter dat een andere partij dan de gebruiker de encryptie verzorgt. Het verschil met de 5^e categorie is dat de gebruiker zelf de sleutel(s) genereert. De TTP kan in deze architecturen betrokken zijn bij encryptie en/of key recovery.

De bovenstaande omschrijvingen leiden tot het volgende schematische overzicht:

Architectuur-categorie	Generatie	Encryptie	Opslag	Key recovery	Algoritme
1	*	*	*	*	gebruiker
2	gebruiker	gebruiker	gebruiker	gebruiker en TTP nodig	bekend
3	*	*	niet gebruiker	*	bekend
4	*	*	*	gebruiker niet nodig	bekend
5	niet gebruiker	*	gebruiker	gebruiker nodig	bekend
6	gebruiker	niet gebruiker	gebruiker	gebruiker nodig	bekend

* = Deze rol kan door iedere partij gespeeld worden.

Toelichting op de kolommen uit de tabel:

Generatie:	welke partij heeft de sleutel(s) gegenereerd met behulp waarvan de gegevens zijn vercijferd?
Encryptie:	wie is verantwoordelijk voor de daadwerkelijke vercijfering van de gegevens?
Opslag:	welke partij zorgt voor de opslag van de private (of in geval van symmetrische encryptie de geheime) sleutel met behulp waarvan de gegevens zijn vercijferd?
Key recovery:	welke partij is nodig voor het kunnen reconstrueren van de private (of in geval van symmetrische encryptie de geheime) sleutel met behulp waarvan de gegevens zijn vercijferd? Dit kunnen ook meerdere partijen zijn.
Algoritme:	wie heeft kennis van het algoritme waarmee de gegevens zijn vercijferd?

Architectuurcategorie 1 beschrijft feitelijk geen vertrouwelijkheidsdienst die door een TTP wordt geleverd. Deze categorie is toch opgenomen, omdat betrokkenheid van de TTP wel mogelijk is. Dit is bijvoorbeeld het geval wanneer een gebruiker weliswaar een eigen algoritme heeft ontworpen, maar sleutels gebruikt die door een TTP zijn gegenereerd. Het in de praktijk voorkomen van architectuurcategorie 6 lijkt het minst waarschijnlijk.

5.3 Confrontatie architectuurcategorieën met de behoeftestelling

In deze paragraaf wordt per categorie aangegeven wat de consequenties zijn voor het verkrijgen van rechtmatige toegang door opsporings- en inlichtingendiensten en de rol van de TTP daarin.

De behoeftestelling van de opsporings- en inlichtingendiensten valt uiteen in drie delen.

1. Algemene gegevens;
2. Verkeersgegevens;
3. Klare tekst.

Zoals in hoofdstuk 4.4 aangegeven wordt in deze rapportage, die betrekking heeft op vertrouwelijkheidsdiensten, waarbij een TTP betrokken is 'sec' gekeken naar de behoeftestelling voor wat betreft "Klare tekst". Kort samengevat zijn voor deze rapportage de volgende delen uit de behoeftestelling relevant: klare tekst, real time, volledigheid en zonder medeweten van de gebruiker. Daar waar er in deze paragraaf wordt gesproken over de behoeftestelling word dan ook bedoeld klare tekst, real time, volledigheid en zonder medeweten van de gebruiker.

Architectuurcategorie 1. Het onderscheidende in deze categorie is dat het algoritme alleen bij de gebruiker bekend is. De TTP zal in dit geval niet kunnen worden aangesproken op de behoeftestelling. Wel kan de TTP afhankelijk van die rollen die hij wel vervult binnen deze categorie informatie verschaffen aan de opsporings en inlichtingendiensten. Op basis van deze informatie kunnen de opsporings- en inlichtingendiensten vervolgens op een andere wijze, buiten de TTP om, in hun behoeftestelling voorzien. Bijvoorbeeld: de TTP vervult de rol van sleutelopslag, dan kan de TTP de sleutel ter beschikking stellen.

Architectuurcategorie 2. Hoewel het algoritme publiekelijk bekend is kan in de architecturen binnen deze categorie de sleutel niet zonder medewerking van de gebruiker worden achterhaald. De TTP kan niet worden aangesproken op de behoeftestelling. Wel kan de TTP die (deel)informatie die zij ten behoeve van het key recovery mechanisme in haar bezit heeft, ter beschikking stellen aan de opsporings- en inlichtingendiensten.

Architectuurcategorie 3. In deze categorie zitten alle architecturen waarbij het algoritme publiekelijk bekend is en waarbij de private (of geheime) sleutel op een plek buiten bereik van de gebruiker is opgeslagen. Als de sleutel bij de TTP is opgeslagen kan de TTP worden aangesproken op de behoeftestelling. Het is ook mogelijk dat de sleutel bij een andere partij dan de gebruiker of de TTP is opgeslagen. Uiteraard kan de TTP dan alleen die informatie geven waarover zij beschikt, maar niet de volledige behoeftestelling invullen. In dat geval is het voor de behoeftestellers zaak dat zij de partij die verantwoordelijk is voor de sleutelopslag kunnen verplichten om de opgeslagen sleutel te leveren.

Architectuurcategorie 4. In alle gevallen binnen deze categorie is het mogelijk om zonder medewerking van de gebruiker de sleutel te achterhalen middels het key recovery mechanisme. Aangezien ook het algoritme bekend is, is het eenvoudig om het bericht te ontcijferen en zodoende rechtmatige toegang te verschaffen. Een noodzakelijke voorwaarde voor het daadwerkelijk realiseren van rechtmatige toegang is wel dat de partij of partijen (waaronder mogelijk een TTP) die nodig zijn voor de key recovery procedure, verplicht kunnen worden om medewerking te verlenen. Uiteraard kan de TTP alleen op de volledige behoeftestelling worden aangesproken indien zij de key recovery zelfstandig kan uitvoeren.

Naar voren is gekomen dat het voor een gebruiker, die gebruik maakt van een TTP die in architectuurcategorie 3 of 4 valt, relatief eenvoudig is om een situatie te creëren, waardoor hij in een architectuurtype uit de tweede categorie komt. Rechtmatige toegang via de TTP geeft dan weliswaar toegang tot sleutel materiaal, maar nog niet tot de klare tekst. Daartoe zou zo'n gebruiker zelf als CA op kunnen treden door zijn certificaat,

verkregen van een TTP (die in categorie 3 of 4 valt), te gebruiken om nieuwe certificaten uit te geven. Dit kan hij doen door een nieuw sleutelpaar te genereren en de nieuwe publieke sleutel te tekenen met zijn eigen private sleutel¹⁴. Voor de nieuwe certificaten slaat hij de zojuist gegenereerde private sleutel niet op de geëigende plek op, maar zijn handtekening op de nieuwe certificaten is wel legaal en verifieerbaar bij de TTP. Zo kan hij bijvoorbeeld ook een nieuw certificaat voor zichzelf maken en dat bij vertrouwelijkheidsdiensten (bijvoorbeeld met het vrij verkrijgbare PGP) gebruiken.

Architectuurcategorie 5. In deze categorie is de gebruiker zowel bij de sleutelopslag, als bij key recovery betrokken. Ondanks het publiekelijk bekende algoritme kan de TTP dus niet worden aangesproken op de behoeftstelling. Wel kan afhankelijk van de rol(len) die de TTP speelt informatie worden gegeven over de sleutelgeneratie, encryptie of key recovery.

Architectuurcategorie 6. Net als in de categorieën 2 en 5 kan de sleutel niet zonder medewerking van de gebruiker worden achterhaald. De TTP kan in deze architectuur niet worden aangesproken op de behoeftstelling. Wel kan zij afhankelijk van haar betrokkenheid bij encryptie en/of key recovery daar informatie over verschaffen.

Samenvattend kun je concluderen dat in de architectuurcategorieën 3 en 4, waarbij het algoritme bekend is en de sleutel via opslag of via key recovery buiten de gebruiker om achterhaald kan worden, ontcijfering kan worden gerealiseerd. In een groot aantal gevallen binnen deze categorieën zal de TTP aan de behoeftstelling kunnen voldoen. In de architectuurcategorieën 1 en 2 is het niet haalbaar, omdat of het algoritme ontbreekt (architectuurcategorie 1) of de sleutel (architectuurcategorie 2).

De drie TTP's die lid zijn van de werkgroep vallen in architectuurcategorie 2, één TTP biedt architectuurcategorie 3 optioneel aan. In hoeverre zij een relevante afspiegeling zijn van de nog niet uitontwikkelde TTP-infrastructuur kan de technische werkgroep niet beoordelen.

Schematisch leidt het bovenstaande tot het volgende overzicht waarin de vraag wordt beantwoord of de TTP, vanuit de technologie geredeneerd, kan voldoen aan de behoeftstelling:

N = niet mogelijk in deze architectuurcategorie;

J = wel mogelijk in deze architectuurcategorie.

<i>Behoeftstelling voor wat betreft Klare tekst</i>				
<i>Architectuurcategorie</i>	Klare tekst	Real time	Volledige info	Geen medewerking of medeweten eindgebruiker
	1	N	N	N
2	N	N	N	N
3	J*	J*	J*	J*
4	J**	J**	J**	J**
5	N	N	N	N
6	N	N	N	N

Geldt in die gevallen dat: * de TTP een kopie van de sleutel heeft; ** de TTP zelfstandig key recovery kan doen.

De technisch inhoudelijke conclusie is dat het in 4 van de 6 architectuurcategorieën niet mogelijk is om een TTP aan te spreken op het verstrekken van klare tekst. In de twee overige categorieën is deze mogelijkheid er onder de volgende voorwaarden wel: de TTP heeft een

¹⁴ Voor meer technische details over "certificate chains" verwijzen we naar blz. 572 van het *Handbook of Applied Cryptography* van Menezes, van Oorschot en Vanstone, ISBN 0-8493-8523-7, ook beschikbaar op <http://www.cacr.math.uwaterloo.ca/hac/>.

kopie van de sleutel (categorie 3), dan wel de TTP kan zelfstandig key recovery doen (categorie 4).

In de werkgroep, de interviews en de commentaren op de conceptrapportage is door de betrokkenen getracht om per architectuurcategorie te komen tot oplossingen. De gesuggereerde oplossingen (die technisch over het algemeen goed toepasbaar en implementeerbaar zijn) leiden er echter telkens toe dat de TTP in architectuurcategorie 3 of 4 komt te vallen. De vraag die feitelijk voorligt betreft dan ook de wenselijkheid van het in de praktijk voorkomen van de bewuste vier architectuurcategorieën, waarin de TTP vanuit de technologie geredeneerd niet kan worden aangesproken op de behoeftstelling van de opsporings- en inlichtingendiensten.

Zoals eerder opgemerkt geldt de behoefte aan “Klare tekst” specifiek voor vertrouwelijkheidsdiensten waar een TTP bij betrokken is en staat dan ook centraal in deze rapportage van de technische werkgroep.

Daar de TTP-vertrouwelijkheidsdienst onderdeel zal zijn van een totale infrastructuur (waarvan ook Telecomproviders en Internet Service Providers deel uitmaken) kan in de uiteindelijke confrontatie tussen de volledige behoeftstelling en de architectuurcategorieën een totaal overzicht worden gemaakt.

De behoefte aan algemene gegevens en verkeersgegevens valt buiten de context van deze rapportage en is momenteel onderwerp van studie en discussie in parallel lopende trajecten. De werkgroep kan dan ook slechts een inschatting geven van de mate waarin aan de volledige behoeftstelling kan worden voldaan in de verschillende architectuurcategorieën.

Schematisch leidt de confrontatie tussen de volledige behoeftstelling en de architectuurcategorieën tot het onderstaande overzicht. In de derde kolom wordt de door de technische werkgroep bekeken vraag beantwoord of de TTP, vanuit de technologie geredeneerd, kan voldoen aan de behoefte aan klare tekst:

	Algemene gegevens	Verkeersgegevens	Klare tekst
Architectuurcategorie 1	+	+	-
Architectuurcategorie 2	+	+	-
Architectuurcategorie 3	+	+	+*
Architectuurcategorie 4	+	+	+**
Architectuurcategorie 5	+	+	-
Architectuurcategorie 6	+	+	-

*Geldt in die gevallen dat: * de TTP een kopie van de sleutel heeft; ** de TTP zelfstandig key recovery kan doen.*

6. Samenvatting, conclusie en aanbevelingen

6.1 Samenvatting

In de voorgaande hoofdstukken is eerst de behoeftestelling van de opsporings- en inlichtingendiensten in kaart gebracht. Daarna is vanuit technisch perspectief een zestal generieke categorieën van architecturen geïntroduceerd, waarbinnen de huidige en de toekomstige TTP-vertrouwelijkheidsdiensten zullen vallen. Door deze generieke architectuurcategorieën te confronteren met de behoeftestelling wordt inzichtelijk gemaakt in welke gevallen het mogelijk is om aan de behoeftestelling te voldoen.

De totale behoeftestelling valt uiteen in drie delen:

1. Algemene gegevens:
naam, adres, postcode, woonplaats, nummer en soort dienst van personen die gebruik maken van openbare telecommunicatienetwerken of -diensten;
2. Verkeersgegevens:
deze gegevens betreffen het telecommunicatieverkeer van de gebruiker;
3. Klare tekst:
de opsporings- en inlichtingendiensten willen dat de tekst begrijpbaar wordt aangeleverd. In principe willen zij geen private sleutels in bezit hebben. Alleen indien het niet anders kan zullen de sleutels ter beschikking moeten worden gesteld.

De behoefte aan “Klare tekst” geldt specifiek voor vertrouwelijkheidsdiensten waar een TTP bij betrokken is en staat dan ook centraal in deze rapportage van de technische werkgroep. Van belang daarbij is dat de “Klare tekst” kan worden verkregen buiten de gebruiker om. De behoefte aan algemene gegevens en verkeersgegevens valt buiten de context van deze rapportage en is momenteel onderwerp van studie en discussie in parallel lopende trajecten. De werkgroep kan dan ook slechts een inschatting geven van de mate waarin aan de behoeftestelling voor wat betreft algemene- en verkeersgegevens kan worden voldaan in de verschillende architectuurcategorieën.

Daar de TTP-vertrouwelijkheidsdienst onderdeel zal zijn van een totale infrastructuur (waarvan ook Telecomproviders en Internet Service Providers deel uitmaken), wordt hieronder schematisch een overzicht gegeven van de confrontatie tussen de volledige behoeftestelling en de architectuurcategorieën.

In de derde kolom wordt de door de werkgroep onderzochte vraag beantwoord of de TTP, vanuit de technologie geredeneerd, kan voldoen aan de behoefte aan klare tekst:

	Algemene gegevens	Verkeersgegevens	Klare tekst
Architectuurcategorie 1	+	+	-
Architectuurcategorie 2	+	+	-
Architectuurcategorie 3	+	+	+*
Architectuurcategorie 4	+	+	+**
Architectuurcategorie 5	+	+	-
Architectuurcategorie 6	+	+	-

*Geldt in die gevallen dat: * de TTP een kopie van de sleutel heeft; ** de TTP zelfstandig key recovery kan doen.*

6.2 Conclusie

De technisch inhoudelijke conclusie is dat het in 4 van de 6 architectuurcategorieën niet mogelijk is om een TTP aan te spreken op het verstrekken van klare tekst. In de twee overige categorieën is deze mogelijkheid er onder de volgende voorwaarden wel: de TTP heeft een kopie van de sleutel (categorie 3), dan wel de TTP kan zelfstandig key recovery doen (categorie 4).

In de werkgroep, de interviews en de commentaren op de conceptrapportage is door de betrokkenen getracht om per architectuurcategorie te komen tot oplossingen. De gesuggereerde oplossingen leiden er echter telkens toe dat de TTP in architectuurcategorie 3 of 4 komt te vallen. Vraag die voorligt betreft dan ook de wenselijkheid van het in de praktijk voorkomen van de verschillende architectuurcategorieën. Vanuit de technische werkgroep kan deze vraag vanzelfsprekend niet beantwoord worden.

6.3 Aanbevelingen

1. Schep op korte termijn duidelijkheid over de wenselijkheid van het in de praktijk voorkomen van de verschillende architectuurcategorieën. De ontwikkeling van de TTP-infrastructuur gaat immers gewoon door.
2. Benader de vragen voor wat betreft rechtmatige toegang niet 'sec' vanuit de technologie, maar betrek alle relevante aspecten. Vanuit de marktpartijen is in de werkgroep aangegeven dat de totstandkoming van een volwaardige TTP-infrastructuur in Nederland grotendeels van andere dan technische aspecten zal afhangen. Een aantal van de genoemde aspecten is terug te vinden in bijlage 2.
3. Laat de TTP-organisatie vrij in haar keuze voor individuele technische oplossingen binnen die architectuurcategorieën waar rechtmatige toegang verleend kan worden. Via het reeds opgezette TTP-certificatieschema (eigenaar ECP.NL) kunnen de benodigde technische standaarden voor het verlenen van rechtmatige toegang onderdeel gaan vormen van de TTP-normen en TTP-certificatiecriteria. Op deze wijze wordt aan het uitgangspunt van zelfregulering via een publiek/private partnership approach voldaan.

Bijlage 1 Samenstelling/betrokkenen Technische Werkgroep

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, dhr. E. van de Laan en dhr. F. van Kampen. Dhr. W. Knijf was betrokken bij de gespreksronde.
- Informatie Communicatie Technologie Organisatie (ITO), dhr. K. Jaspers
- Ministerie van Justitie, dhr. S.B. Bootsma was betrokken bij de gespreksronde.
- Nederlands Forensisch Instituut, dhr. E. van Eijk was betrokken bij de gespreksronde.
- Ministerie van Defensie, dhr. J. van Tuyl. Dhr. W. Timmers was betrokken bij de gespreksronde.
- IBM/Tivoli Secureway, dhr. R.G. Weemhof
- DigiNotar, mw. A.H. Tollenaar
- Nederlandse Vereniging van Banken (NVB), dhr. M.A.A. Sonnemans
- Philips Crypto, dhr. C.G.G.M. Reniers
- Defensie Telematica Organisatie, dhr. M.J. Rooth
- Nationaal Chipcard Platform, dhr. J. van Arkel
- Roccade Megaplex, dhr. J. Berends en dhr. S. Steenbergen. Dhr. M. Huijbers dhr. J.W. van Boven en dhr. H. Cimen waren betrokken bij de gespreksronde.
- PriceWaterhouseCoopers, dhr. O.A. Vermeulen en dhr. E. Verheul waren betrokken bij de gespreksronde.
- Nationaal Bureau voor Verbindingsbeveiliging (NBV), dhr. R. Doijen was betrokken bij de gespreksronde.
- KPN, dhr. B. Schuurink

Van TNO is aan de gesprekken deelgenomen door dhr. T. Veugen, dhr. M. van Lieshout en dhr. H.J. Vink (voorzitter technische werkgroep).

Bijlage 2 Overige punten genoemd tijdens de interviews

Tijdens de interactie binnen de technische werkgroep kwam een aantal niet technische aspecten/overwegingen naar boven die wellicht van belang zijn voor de doorontwikkeling van de TTP-infrastructuur in Nederland. Om deze informatie niet verloren te laten gaan is ten behoeve van de projectgroep rechtmatige toegang deze bijlage aan de rapportage van de technische werkgroep toegevoegd. De verschillende opmerkingen zijn niet getoetst op juistheid en volledigheid, maar kunnen wel gebruikt worden als input voor de discussie binnen de projectgroep.

Opmerkingen van juridische aard:

- Het tijdig afsluiten van rechtmatige toegang. Wanneer de termijn van een gerechtelijk bevel afloopt en er niet voldoende bewijs is verzameld, beschikt de opsporingsinstantie nog steeds over het sleutelmateriaal. Er zijn technische oplossingen nodig om in zo'n geval onrechtmatige toegang te voorkomen.
- Voordat er afgetapt kan worden is een gerechtelijk bevel noodzakelijk. In de huidige wetgeving zijn daar meerdere ministeries bij betrokken wat mogelijk vertraging oplevert.
- Aangezien het wettelijk kader rondom rechtmatige toegang momenteel sterk in beweging is, is het lastig om aanbevelingen voor de toekomst te geven.
- Wanneer is een TTP als Nederlands aan te merken? Indien Verisign (US) als Signing Authority (SA) optreedt is er dan feitelijk sprake van een Nederlandse TTP.
- In hoeverre vallen voor specifieke beroepsgroepen TTP-vertrouwelijkheidsdiensten onder het ambtsgeheim.
- In verband met het opslaan van private sleutels door TTP's of opsporings- en inlichtingendiensten zal met het oog op de aansprakelijkheid het e.e.a. nader moeten worden geregeld.

Opmerkingen van financiële aard:

- Wie betaalt er voor het verlenen van rechtmatige toegang? Hierbij is ook belangrijk om te weten hoeveel informatie de behoeftezoekers willen vergaren, bijvoorbeeld 10% of 80% van alle berichten? Wanneer er vaak een verzoek zou worden ingediend voor rechtmatige toegang, zou dit ten koste kunnen gaan van de huidige bedrijfsvoering van een TTP en zou bijvoorbeeld een geldelijke vergoeding nodig zijn.

Opmerkingen van marketingtechnische aard:

- Een aantal marktpartijen geeft aan dat het door de TTP opslaan van sleutels (private key's) zal leiden tot een kleiner marktaandeel en kiest daarom bewust voor het niet zelf opslaan van sleutels.
- De commerciële vraag naar 'key recovery' is zeer beperkt (eerder wordt bewust gevraagd deze mogelijkheid uit te sluiten). De door de TTP's gehanteerde technologie is dan ook over het algemeen zo opgezet dat rechtmatige toegang niet zonder medewerking of medeweten van de eindgebruiker verkregen kan worden.
- Vanuit de marktpartijen werd erop gewezen dat de ontwikkelingen rond rechtmatige toegang zich niet afspeelen in een nationaal vacuüm. De ontwikkeling van een TTP-infrastructuur speelt zich af in een internationaal speelveld. Het is zaak om ervoor te zorgen dat Nederlandse spelers niet bij voorbaat kansloos zijn, doordat ze aan eisen moeten voldoen die voor andere spelers niet gelden, en daardoor mogelijk aan geloofwaardigheid of aan economische slagkracht inboeten. Hoewel de concurrentieproblematiek formeel niet tot de taakstelling van deze werkgroep behoort is een goede aanpak van dit soort vraagstukken wel van groot belang om überhaupt een ontwikkeling van Nederlandse TTP-spelers te bevorderen.

- De in de technische werkgroep vertegenwoordigde TTP's geven aan dat zij niet actief marketen voor vertrouwensdiensten. De huidige vraag, alsmede de verwachte vraag naar dit soort diensten is laag.

Opmerkingen betreffende de praktische implementatie:

- De beheersbaarheid van de informatie. Je zult informatie over de afgetapte lijn moeten krijgen om de juiste sleutel bij de juiste TTP te kunnen halen. De TTP en de law enforcement agency dienen gescheiden te zijn met een interface daartussen die zowel technisch, juridisch als procedureel goed in elkaar moet zitten.
- On-line toegang tot e-mail. Het tijdsaspect zal per behoeftesteller variëren maar het zal lastig zijn om op zeer korte termijn toegang te krijgen tot de klare tekst. Er dient een centrale instantie te komen voor alle opsporings-, inlichtingen- en veiligheidsdiensten.
- Gezien de snelle opeenvolging van nieuwe technieken, standaarden en formaten is het moeilijk om nu oplossingen te bedenken die voor langere tijd te handhaven zijn. Een mogelijke oplossing zal conceptueel van aard moeten zijn.
- Doordat er vanuit de praktijk weinig vraag is naar key-recovery bij gecommuniceerde berichten zal het lastig zijn om regelgeving voor rechtmatige toegang op willekeurig afgetapte berichten te realiseren.
- Opgemerkt wordt dat de gebruikte technologie inherent instabiel en daardoor kwetsbaar is. Het toevoegen van additionele technologie om rechtmatige toegang te verzorgen zal leiden tot meer instabiliteit.
- Indien besloten wordt om specifieke architectuurcategorieën als ongewenst te benoemen kan dat leiden dat grote gevolgen voor bestaande diensten. Bijvoorbeeld de bancaire TTP-dienstverlening zou in de huidige gekozen opzet niet kunnen worden gecontinueerd.

Opmerkingen van procedurele aard:

- De behoeftestelling zal ingepast moeten worden in een raamwerk waarin ook andere kwesties ten aanzien van het omgaan met de rechtmatig verkregen sleutels zullen moeten worden geregeld. Dat gaat onder meer om:
 - Bewaartermijnen; rechtmatige toegang is gebonden aan termijnen. Vastgesteld zal moeten worden hoe lang de TTP sleutelmateriaal vast zal moeten houden. Daarnaast zal in die gevallen dat sleutels gebruikt worden voor het verkrijgen van rechtmatige toegang zekerheid ingebouwd moeten worden die belet dat een sleutel na het aflopen van de termijn nog gebruikt kan worden. In het geval de opsporing niet tot resultaat heeft geleid, zal zonder dat dit kenbaar hoeft te worden gemaakt, een garantie geboden moeten worden dat de sleutel niet meer door bijvoorbeeld de behoeftestellers gebruikt kan worden, zonder dat het subject van wie de berichten onderschept zijn hier kennis van heeft of krijgt.
 - Vernietiging van sleutelmateriaal; ook in gevallen waarin wel bewijslast is verkregen zal iets geregeld moeten worden omtrent de vernietiging van sleutelmateriaal. Ook dit zou bij voorkeur op een technisch niet te corrumperen wijze plaats moeten vinden.