

**Verslag vergadering TTP Coördinatie groep**

Vergadering: 2001-02  
Datum: 22 maart 2001  
Locatie: Mövenpick Hotel te Voorburg

*Aanwezig*

Arie van Bellen	ECP.NL (voorzitter)
Jacob Boersma	ECP.NL (interim secretaris)
Marjolijn Durinck	ECP.NL
Ronald v.d. Luit	Ministerie van Verkeer en Waterstaat
Jan Willem van Boven	Roccade
Louis v.d. Linden	OPTA
Rob van Eijl	OPTA
Ton Pronk	POA
Patrick Paling	KPMG
Frank Schasfoort	PWC
Astrid Kogels	Blue X
Dick Rufi	Ministerie van Economische Zaken
Martin Buys	Ministerie van Economische Zaken
Tony de Bos	Diginotar
Ben Schuurink	KPN
Rob Weemhoff	IBM
Anne den Oudsten	Interpay NL BV
Ronald Houtsma	PKI Overheid
Bert Snel	Siemens
Tjalling Ament	Siemens
Arie Noteboom	ABN AMRO

**1. Opening door Arie van Bellen; Vaststelling agenda**

De voorzitter heet de aanwezigen welkom en geeft een korte inleiding omtrent de stand van zaken rondom TTP.NL. Het schema en de criteria zijn afgerond en zullen op zeer korte termijn als brochure op de markt worden gebracht. De organisatiestructuur bestaat uit een centraal college van deskundigen (CCvD) en een toezichthouder in de vorm van de OPTA. Ook het registreren van TTP's wordt een taak van de OPTA. De OPTA zal hierover een korte presentatie geven. Het plan is om in september een seminar TTP.NL te organiseren waarbij de eerste certificaten aan TTP's zullen worden uitgereikt.

De agenda wordt vastgesteld:

Op verzoek van Martin Buys worden agendapunten 3 (OPTA presentatie door Louis v.d. Linden) en 4 ( de afstemming van TTP.NL met Rechtmatige toegang) omgedraaid. Agendapunt 5 (accreditatie- en certificatieproces) zal door Ton Pronk worden toegelicht. Bij afwezigheid van René van den Assem zal ook agendapunt 6 (de stand van zaken workshop EESSI) door Ton Pronk worden toegelicht.

## 2. Verslag vorige vergadering (18 januari 2001)

Het verslag wordt goedgekeurd.

## 3. Afstemming TTP.NL en Rechtmatige Toegang

Arie van Bellen geeft een toelichting op het project Rechtmatige Toegang (RT). De behoeftezoekers (Justitie, de BVD en de MID) hebben een wettelijke bevoegdheid tot het aftappen van telecommunicatieverkeer, maar deze bevoegdheid is ineffectief voor zover de afgetapte informatie versleuteld is. De behoeftezoekers kunnen dan ook een belang hebben bij rechtmatige toegang tot de oorspronkelijke inhoud van versleuteld elektronisch berichtenverkeer door tussenkomst van een TTP die vertrouwelijkheidsdiensten aanbiedt.

Een jaar geleden is onder begeleiding van de ministeries van V&W en EZ het project RT gestart. Er werd een projectgroep ingericht met als onafhankelijke voorzitter Piet van Dijken (Shell). Verder bestond deze projectgroep uit overheid en enkele marktpartijen. Er werd ook een Technische Werkgroep ingericht welke contact had met meerdere marktpartijen, nadrukkelijk ook de TTP's. De Technische Werkgroep kwam tot de conclusie dat er twee scenario's bestaan waarbij het mogelijk is rechtmatige toegang te verlenen, te weten bij key-escrow en key-recovery. Deze conclusie werd teruggerapporteerd aan de Stuurgroep RT. Besloten werd om aan te haken bij TTP.NL en criteria en een schema op te stellen voor TTP's die vertrouwelijkheidsdiensten aanbieden. Wanneer TTP's vertrouwelijkheidsdiensten willen aanbieden zullen zij moeten voldoen aan de criteria die daarvoor gelden, dat wil zeggen dat zij hun vertrouwelijkheidsdiensten zo moeten inrichten dat zij in staat zijn rechtmatige toegang te verlenen (dmv key-escrow of key-recovery) Dit is echter een voorlopige oplossingsrichting.

De Stuurgroep besloot dat er een onderzoek moet worden verricht naar de economische effecten van de verplichting om rechtmatige toegang te verlenen. Wanneer daaruit blijkt dat de voorgenomen oplossingsrichting economisch niet haalbaar is, zal hiervan worden afgezien. De aanwezigen wordt gevraagd om, samen met enkele andere deskundigen, mee te werken aan dit onderzoek. Benadrukt wordt dat het koppelen van RT aan TTP.NL geen belemmering mag vormen voor de ontwikkelingen bij TTP.NL. TTP.NL gaat gewoon door, RT ziet specifiek op aanvullende criteria voor TTP's die vertrouwelijkheidsdiensten aanbieden. Martin Buys vult aan dat er een verschil zit in de criteria van TTP.NL en die van RT, omdat de laatste minder vrijblijvend en vrijwillig zullen zijn dan de TTP.NL-criteria. Bij RT is er geen sprake van zelfregulering maar van 'verplichte zelfregulering'. Jan-Willem van Boven vraagt hoe het precies geregeld is in de wet. Martin Buys antwoordt dat uit de wet volgt dat TTP's die geen sleutelmateriaal hebben, ook geen medewerking kunnen verlenen. Maar de bedoeling is dat TTP's in de toekomst niet meer kunnen stellen geen sleutelmateriaal te beheren, omdat zij verplicht zijn hun vertrouwelijkheidsdiensten zo in te richten dat rechtmatige toegang mogelijk is.

Tony de Bos stelt dat er dus twee sleutelparen moeten worden verstrekt. Eén paar voor authenticiteit en integriteit en één paar voor vertrouwelijkheid. Bert Snel merkt hierbij op dat het voor een gebruiker relatief eenvoudig is om rechtmatige toegang door de overheid te omzeilen. Een gebruiker kan zelf optreden als CA en zijn, door een TTP gekregen certificaat, gebruiken om nieuwe certificaten uit te geven. Hij kan dus een nieuw certificaat voor zichzelf maken en dat voor vertrouwelijkheid gebruiken. De nieuwe private sleutel die hij dan genereert, slaat hij niet op bij een TTP. Rob Weemhoff voegt daaraan toe dat een gebruiker ook zijn authenticatiesleutel kan misbruiken door deze tevens als vertrouwelijkheidssleutel te

gebruiken. Een TTP is in beide gevallen niet in staat om rechtmatige toegang te verlenen. Bert Snel zegt dat het voor bijvoorbeeld banken onmogelijk is alle sleutels te bewaren. Vanwege veiligheid wordt er bij transactieverkeer vaak van sleutel gewisseld. Dit betekent dat er tienduizenden sleutels per dag bewaard zouden moeten worden. Martin Buys geeft aan dat de behoeftestellers wel degelijk de beperkte effectiviteit van de gekozen oplossing onderkennen, maar daaraan toch vasthouden omdat dit - hoe beperkt dan ook- nog altijd effectiever is dan niets doen.

Ben Schuurink vraagt zich af of het meewerken aan een economische effectenrapportage wel zin heeft. Gezien het feit dat dit onderzoek parallel loopt met het opstellen van de criteria, lijkt het hem een gelopen race. Dick Rufi verzekert de TTP's dat het zeker geen gelopen race is en dat het van belang is om mee te werken aan het onderzoek. Niet alleen om aan te tonen dat het economisch onhaalbaar kan zijn, maar ook uit oogpunt van effectiviteit. Wanneer namelijk blijkt dat vanwege de Nederlandse plannen klanten van TTP's naar het buitenland zullen vertrekken, heeft de oplossing voor de behoeftestellers geen effect meer. Bert Snel laat weten dat alle argumenten met betrekking tot economische haalbaarheid en effectiviteit al in de Technische Werkgroep RT naar voren zijn gekomen, maar dat de plannen blijkbaar toch zijn doorgezet. Ronald van der Luit reageert hierop door te vertellen dat er ook tussen de ministeries onderling patstellingen bestaan en dat het daarom toch nuttig kan zijn de argumenten nog een keer naar voren te brengen. Ook Martin Buys en Dick Rufi bevestigen dit. Martin Buys stelt een ontmoeting tussen de Coördinatiegroep TTP.NL en de Stuurgroep RT voor, zodat het contact niet via andere kanalen loopt en de standpunten rechtstreeks aan de Stuurgroep kunnen worden doorgegeven. Arie van Bellen vindt dit een uitstekend idee. Schuurink stelt voor om dan ook duidelijkheid te vragen omtrent het begrip economische haalbaarheid: wat is nog economisch haalbaar en wat niet, waar ligt de grens? Arie zegt toe een brief naar de Stuurgroep RT sturen met daarin opgenomen het verzoek om een ontmoeting met de Coördinatiegroep TTP.NL en een lijst van gerichte vragen die zullen worden gesteld tijdens deze ontmoeting. Hiermee wordt agendapunt 3 afgesloten.

#### **4. OPTA**

"OPTA en de Digitale Handtekening".

De OPTA reikt handouts van de presentatie uit evenals folder over de OPTA.

De taken zoals de OPTA gaat krijgen komen voort uit het nieuwe telecom-wetsvoorstel (implementatie van de EU Richtlijn Elektronische Handtekeningen).

Een "bewijs van accreditatie" (kreet uit de Richtlijn) is een door TTP.NL afgegeven certificaat. TTP's heten in de richtlijn certificatie dienstverleners.

De OPTA kijkt alleen naar uitgevers van gekwalificeerde certificaten. Aan het certificaat zelf kun je zien of het gekwalificeerd is (met een vinkje). De OPTA houdt van deze TTP's een register bij, of ze nou bij TTP.NL aangesloten zijn of niet. De OPTA werkt reactief (klachtgestuurd). Het gaat om een onafhankelijk onderzoek, maar bij geaccrediteerde aanbieders zal eerst met TTP.NL worden afgestemd.

Probleempunt: kosten op jaarbasis voor de TTP's worden hoog per TTP, omdat er maar zo weinig partijen in deze markt zijn (naar verwachting). Er is overleg met DGTP of deze kosten wellicht uit de Schatkist kunnen worden betaald.

Op dit moment staat er nog niets over de Elektronische Handtekening op de OPTA website,

maar dit is wel de bedoeling. Het wetsvoorstel Elektronische Handtekening is nu naar Raad van State. Zodra deze openbaar is zal ECP.NL het wetsvoorstel ook krijgen en kunnen verspreiden.

Afgesproken wordt dat voor de volgende bijeenkomst het onderwerp “toelichting wettelijk kader” op de agenda komt te staan.

De baten van het toezicht: klant van de TTP heeft meer rechtszekerheid als hij een gekwalificeerde handtekening zet. OPTA is er vooral om 'vrije jongens' te controleren die niet bij TTP.NL zitten maar wel beweren aan de Richtlijn te voldoen. J.W.van Boven vraagt zich af of die OPTA kosten niet de-stimulerend zijn en dus in strijd met de richtlijn? T. de Bos: ‘er zijn al heel veel kosten om te voldoen, die OPTA kosten zijn dan nog een soort 'slagroom op het toetje’

## **5. Accreditatie- en certificatieschema**

ECP.NL wil wel bemiddelen om TTP's als eerste te laten certificeren door auditors. Het is echter aan de marktpartijen zelf.

T. Pronk: Accreditatie hier is NIET hetzelfde als de term bij de OPTA. Een bedrijf als KEMA, PwC of KPMG wil auditen, certificeren, en moet daarvoor eerst ge-ACCREDITEERD worden. Het kader waar we over praten is vrijwillige certificatie (dus niet de 'snelle jongens' waar de OPTA vooral op moet letten). Bij accreditatie moet er een witness van de RvA mee met een audit. Het is een vrij subtiel proces, dat discreet moet gebeuren (omdat accreditatie niet zeker is). Het traject is vergelijkbaar met dat van de CvI/BS7799 indertijd. Nodig zijn dus een auditor en een klant (TTP) nodig die willen. Dit is een langdurig proces, dus het moet wel snel van start gaan, willen we dit jaar nog een traject afronden. Er is ook internationale afstemming tussen RvA's waarbij dus ook buitenlandse witnesses zouden kunnen worden ingezet. Er staat nu dus al veel klaar.

Vraag: wat is de geldigheidsduur?

A: In principe 3 jaar, daarna moet opnieuw een audit worden aangevraagd (en tussentijds is er jaarlijks een (lichtere) controle uitvoeren.

Er is een CCvD dat het schema van TTP.NL gaat bewaken. Dit college is gecombineerd met het college voor bewaking van het schema voor BS7799.

V: wat is de rol van interne reviews (om tijd & kosten te besparen)?

A: hier zijn zeker constructies voor. Sterker nog, internal auditing is heel belangrijk wil je de externe auditor tevreden kunnen stellen.

V: is er voor het TTP Schema ook een internationale component?

A: ja, het TTP.NL schema is gebaseerd op de Europese norm ETSI TS101-456 van EESSI. In Europa (EC/EER) is er dus een uniform normenkader (we gebruiken de etsi standaard). Er is bovendien veel contact geweest met Amerika.

## **6. Stand van zaken Workshop EESSI**

Onder de EESSI stuurgroep (René van de Assem heeft zitting in deze Stuurgroep) vallen groepen van ETSI en CEN. De ETSI norm is af, maar de CEN normen (over technische onderwerpen) moeten nog worden voltooid. Er wordt nu gekeken naar gebruiken van bv. Finread standaard. Het niet af zijn van de CEN criteria moet ons niet weerhouden van

beginnen met certificeren. B. Snel: Bedenk wel dat veel CEN stukken nog niet openbaar zijn.

### **7. Rondvraag en sluiting**

De voorzitter sluit de vergadering en dankt de aanwezigen.

De volgende vergadering zal plaatsvinden op donderdag 17 mei, van 14:00-16:30 uur bij VNO-NCW.

Actiepunten:

- Brief naar de Stuurgroep RT
- Ronald van der Luit op de agenda voor 17 mei as. (uitleg elektronische handtekening)