ECP-EPN

Platform voor de InformatieSamenleving

TTP.NL in de ‘certificatencrisis’

René van den Assem
voorzitter College van Belanghebbenden TTP.NL

ECP-EPN

Platform voor de InformatieSamenleving

1. TTP.NL en toezicht op certificaatdienstverlening
   - Geschiedenis van het TTP.NL-certificatieschema
   - Verhouding wettelijk toezicht – vrijwillige certificatie
   - Werking van het schema
   - Technische aspecten in het schema
2. Hoe gaat het College van Belanghebbenden om met de ontstane crisis?

ECP-EPN

Platform voor de InformatieSamenleving

TTP-overheidsbeleid ?

1997:

Goede kwaliteit van communicatie infrastructuur vanwege maatschappelijke en economische belangen

2000:

Europese richtlijn elektronische handtekening (2000)

Nationaal TTP-project (1997)

Platform voor de InformatieSamenleving

Doelstellingen:

- Formuleren van randvoorwaarden
- Inventariseren borgingsinstrumenten
- Stimuleren ontwikkeling TTP's

Uitgangspunten:

- Zelfregulering, overheid stimulerend
- Internationale aansluiting

ECP-EPN
Platform voor de InformatieSamenleving

Nationaal TTP-project (2)

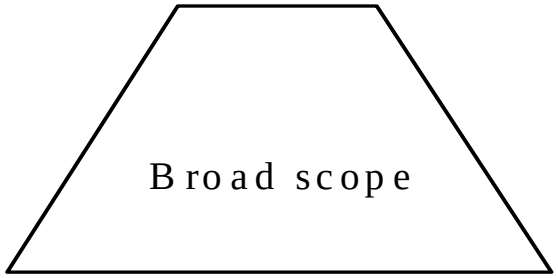
- Resulteerde in TTP-beleidsnotitie van kabinet aan Tweede Kamer (maart 1999)
- Hoofdlijnen:
  - Brede scope
  - Vertrouwen in TTP's door zelfregulering
  - Nadere uitwerking van randvoorwaarden in criteria op basis waarvan TTP gecertificeerd kan worden ("vrijwillige accreditatieregeling")
  - Geen nadere wetgeving nodig (vrije bewijsvoering)

Richtlijn 1999/93/EG

Platform voor de InformatieSamenleving

The two main objectives of the directive

Free internal market for electronic signatures and certification services

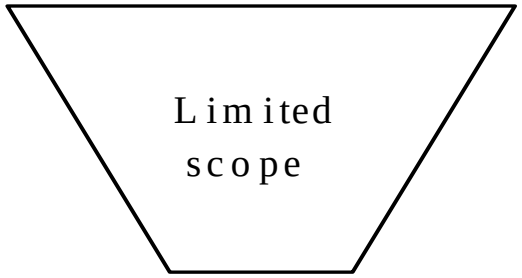


All kinds of electronic signatures

All kinds of certification services

All kinds of signature products

Legal equivalence of electronic signatures with hand-written signatures



Only under certain conditions

Only for specific purposes

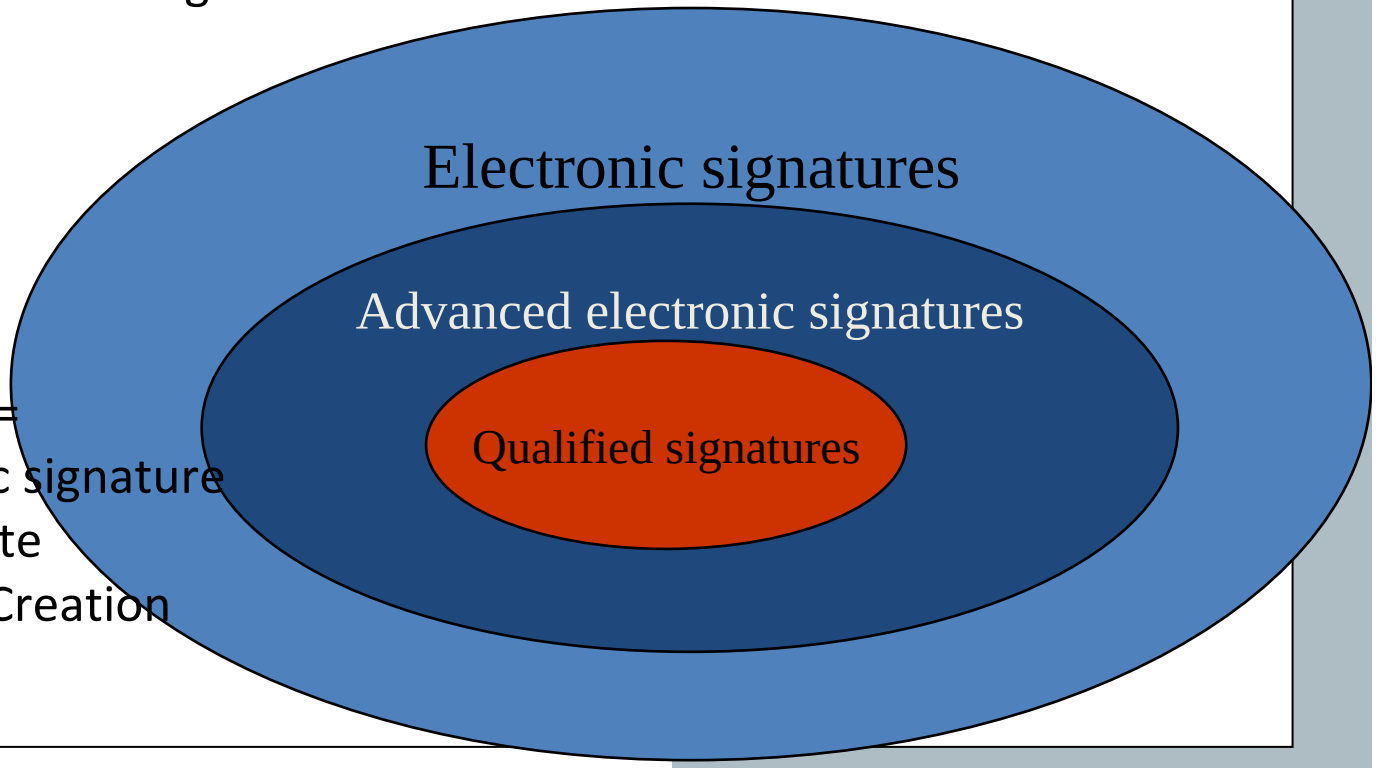
with many exceptions

ECP-EPN

Platform voor de InformatieSamenleving

Richtlijn EHT, rechtsgeldigheid

- General principle (art. 5.2): Legal effect for all electronic signatures
- Second principle (art.5.1): certain electronic signatures get the same legal effect as hand-written signature



Qualified signature =
Advanced electronic signature
+ Qualified Certificate
+ Secure Signature Creation Device (SSCD)

Nationaal TTP-project (3)

Platform voor de InformatieSamenleving

- Concept nationale minimumeisen aan TTP's.
- Beleid richt zich met komst van de richtlijn primair op de (gekwalificeerde) elektronische handtekening. De rest wordt vrijgelaten !
- ETSI TS 101 456, uitwerking vd eisen aan uitgevers van gekwalificeerde certificaten. Nieuwe basis voor vrijwillige certificatie.
- TTP.NL schema, beheer bij ECP EPN. Daadwerkelijk beheer door betrokkenen, College van Belanghebbenden.

Beleidsevaluatie 2004

ECP-EPN
Platform voor de InformatieSamenleving

- TTP Beleid in 2004 geëvalueerd
- Constateringen
  - Verenging in beleid naar elektronische handtekening.
  - Marktbehoefte op andere gebieden, wordt goed door markt opgepakt.
  - TTP-beleid geen harde randvoorwaarde voor e-handel etc.

- Algemene mening: Doorgaan rondom hoge niveau, zo mogelijk stimuleren gebruik. Pas daarna verbreden.
- Geen aanvullende regulering en toezicht, mede in verband met hoge kosten.

ECP-EPN

Platform voor de InformatieSamenleving

Eisen aan TTP's

- Richtlijn Elektronische Handtekeningen
  - Bijlage II: eisen aan certificatiedienstverleners die gekwalificeerde certificaten afgeven
- In Wet Elektronische handtekeningen, wijziging TW
  - Telecommunicatiewet, art. 18.15: Een certificatiedienstverlener … voldoet aan de eisen, gesteld bij of krachtens Algemene Maatregel van Bestuur
- AMvB Besluit elektronische handtekeningen
- Regeling Elektronische handtekeningen

ECP-EPN

Platform voor de InformatieSamenleving

Eisen aan TTP's (2)

AMvB Besluit elektronische handtekeningen

- Art. 2
  Een certificatiedienstverlener... voldoet aan de volgende eisen:
  a) betrouwbare middelen, betrouwbare procedures
  b) procedures en processen overeenkomstig een beschreven
  kwaliteitssysteem dat in overeenstemming is met de laatste ontwikkelingen op het gebied van kwaliteitssystemen
  c) maakt uitsluitend gebruik van betrouwbare systemen en producten
  e) voldoende financiële middelen
  f) personeel in dienst dat deskundig is
  ...

ECP-EPN

Platform voor de InformatieSamenleving

Eisen aan TTP's (3)

Regeling elektronische handtekeningen

- Vertaling naar concrete standaarden.
- Degene die voldoet aan ETSI TS 101 456 wordt vermoed te voldoen aan eisen in Besluit EH.

Toezicht versus Markttoegang

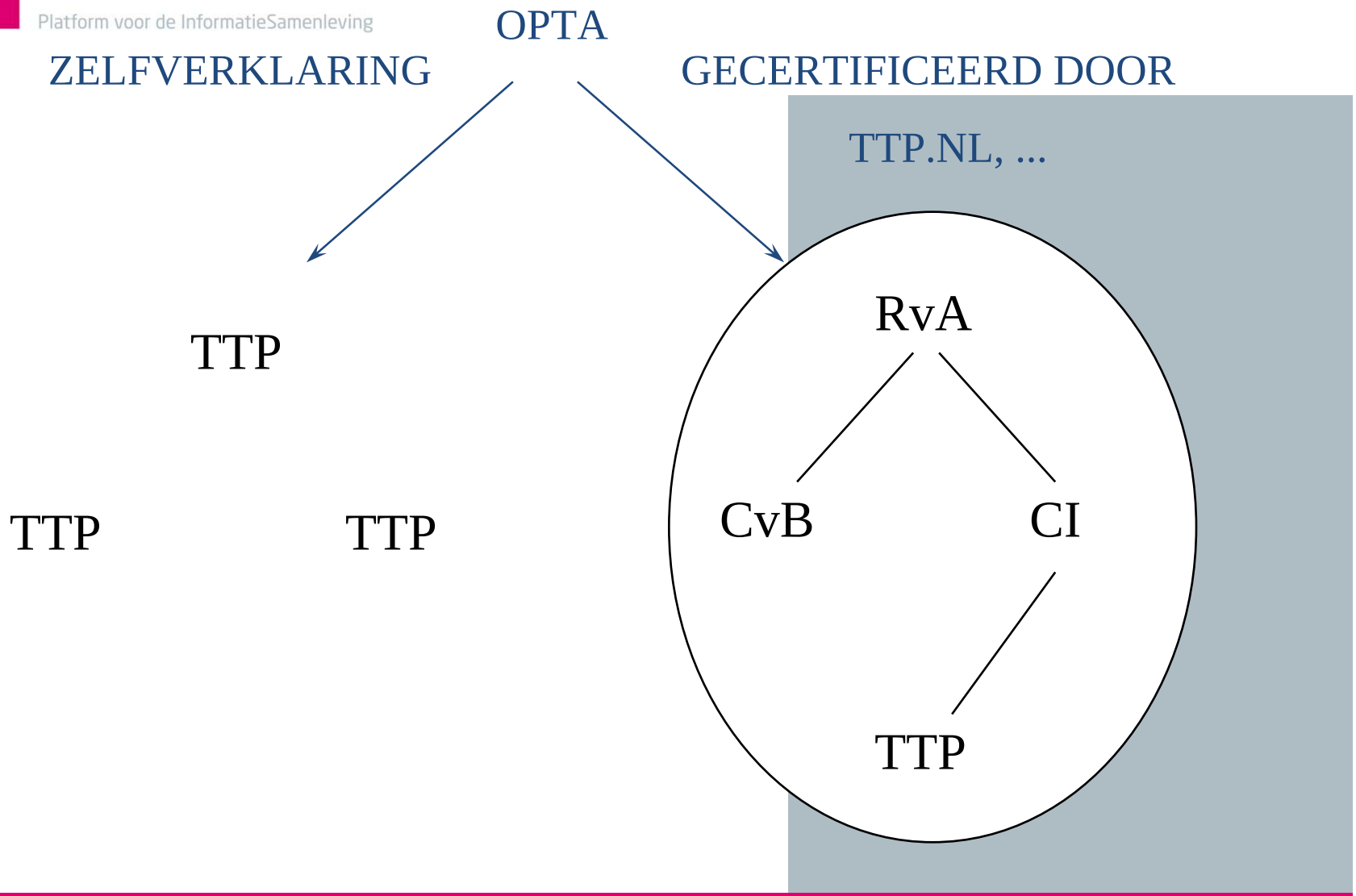
ECP-EPN
Platform voor de InformatieSamenleving

- Wens vanuit TTP.NL: zelfregulering, vrijwillige certificatie.
- Richtlijn
  - Open interne markt voor diensten en producten! Automatische erkenning elders toegelaten CSP's en SSCD-producten (veilige middelen cf annex III)
  - Geen voorafgaande machtiging voor verlenen TTP-dienstverlening (randvoorwaarde)
  - Toezicht op TTP's die gekwalificeerde certificaten afgeven aan het publiek (verplichting !!)
  - Mogelijkheid voor vrijwillige accreditatieregeling

Toezicht en vrijwillige certificatie

ECP-EPN

Platform voor de InformatieSamenleving



ECP-EPN

Platform voor de InformatieSamenleving

‘Toezicht’

Vrijwillige certificatie

- Certificatie-instellingen worden door de RvA geaccrediteerd om CSP’s te kunnen certificeren tegen het TTP.NL-schema
- CI’s beoordelen Certificatie Service Providers en verlenen TTP.NL-certificaat
- De schema-eigenaar en het beheer van het schema worden periodiek beoordeeld door de RvA

Wettelijk toezicht

- OPTA doet toezicht op CSP’s die gekwalificeerde certificaten uitgeven. Registratieverplichting. Voldoen aan eisen (ETSI TS 101 456 + wettelijke eisen)

Overig

- Logius ziet toe op naleving van de extra eisen i.h.k.v. PKIoverheid

ECP-EPN

Platform voor de InformatieSamenleving

Werking TTP.NL schema

Management systeem

– Het TTP.NL-schema beoordeelt primair of er een goed werkend *management systeem* is

Technische vereisten

– ETSI TS 101 456 verwijst naar diverse technische vereisten en daarop wordt ook geaudit:

- Gecertificeerde cryptografische modules
- IT audit op ‘Betrouwbare systemen’ verplicht
- Deze aspecten niet OK, dan geen TTP.NL-certificaat!

ECP-EPN

Platform voor de InformatieSamenleving

Uitbreiding TTP.NL-schema

- TTP.NL-schema is later uitgebreid
  - niet-gekwalificeerde certificaten uit te geven (ETSI TS 102 042), b.v. voor Extended Validation SSL certificaten
  - dienstverlening op het gebied van time stamping aan te bieden (ETSI TS 102 023)

ECP-EPN

Platform voor de InformatieSamenleving

Het DigiNotar incident

- **Vooraf** Het ‘DigiNotar incident’ heeft primair betrekking op SSL-certificaten, waarvoor geen TTP.NL certificaat is afgegeven
- DN komt uiterst laat naar buiten, steeds grotere aantallen gehackte certificaten. Logging en administratie afgegeven certificaten ook gehackt.
- Fox IT
  - Ook hack-sporen op PKI systemen voor gekwalificeerde certificaten.
  - Tekortkomingen in de technische beveiliging
- Overheid pakt management PKIo dienstverlening bij DN over
- OPTA doet (kort) onderzoek en trekt registratie DN in
- DN gaat failliet, TTP.NL certificaat ingetrokken

Meningen en vragen

Platform voor de InformatieSamenleving

Gehoorde meningen

- Marktpartijen zijn onbetrouwbaar en alleen op inkomsten gericht. TTP dienstverlening kan niet aan marktpartijen worden overgelaten, zeker nu het vitale infra gebleken is.
- De toezichtsconstructie is veel te ingewikkeld. De overheid moet streng toezien!
- TTP dienstverlening is een te marginale business waardoor de beveiliging het kind van de rekening wordt
- Het toezicht is veel te procedureel, er wordt veel te weinig op de techniek gelet
- De eisen aan TTP's moeten worden aangescherpt

Vragen voor TTP.NL

- Is in de uitvoering van de management system audit door PwC voldoende gelet op de technische aspecten?
- Is voldoende helder wat een TTP moet aantonen en een CI moet controleren op het gebied van betrouwbare systemen en overige technische infra? Ligt de bewijsvoering en de controle hierop ook vast?
- Zijn de technische eisen aan TTP's wel voldoende gericht op dit soort hack-incidenten? (Hoe zit dat met onuitwisbare logging bijvoorbeeld?)

ECP-EPN

Platform voor de InformatieSamenleving

Werkgroep met een missie

In afstemming met de actoren:

- Bepaal welke assurance er over de techniek gewenst is.
- Werk een precisering van het TTP.NL-schema uit (guidance) om duidelijkheid te bieden aangaande IT audit verplichtingen en mate van assurance.
- Zoek support voor een verbreding van het TTP.NL-schema naar (EV)SSL-certificaten. Single audit.
- Eventueel: de daadwerkelijke eisen aan de techniek
  - Maak een vergelijking van gehanteerde normen;
  - Aanvullende eisen relevant in het licht van dit soort dreigingen?
  - Inbreng in standaardisatie gremia
- Doe achter de schermen mee aan de discussie over eventuele alternatieve vormen van toezicht.

ECP-EPN

Platform voor de InformatieSamenleving

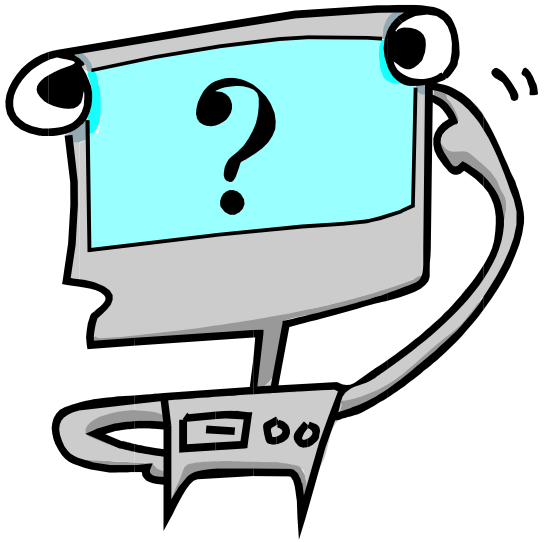
Verdere toekomst

- SSL certificaten vooral geregeld via browserfabrikanten. Centrale rol CA/Browser Forum.
- Uniforme eisen in wording. (Baseline requirements CA/B Forum). Mogelijk vervolg: harmonisering met ETSI. Via die route in auditpraktijk.

- Inherente problemen huidige model
  - Vele partijen (> 600), alle vertrouwd
  - Web of Trust achtige benaderingen beter alternatief?
  - Mijn beeld: Geen goede alternatieven voorhanden.

Vragen

Platform voor de InformatieSamenleving



Rene.vandenAssem@vka.nl
0653576982