Nationaal Cyber Security Centrum
*Ministerie van Veiligheid en Justitie*

Lessons learned from

# The DigiNotar crisis

*from incident response*

*to crisis coordination*

Aart Jochem
NCSC-NL

NIST CA Workshop
Gaitherburg MD - 11 April 2013

# *Pretty Good Privacy*

# public policy aspects of cryptography

National Cyber Security Centre
*Ministry of Security and Justice*

CERT | Software Engineering Institute
Carnegie Mellon

SURF CERT

**Tweede Kamer der Staten-Generaal** **2**

Vergaderjaar 2000–2001

**26 643** **Informatie- en communicatietechnologie (ICT)**

**Nr. 30** **BRIEF VAN DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 juli 2001

Mede namens de Minister van Economische Zaken bied ik u de nota *Kwetsbaarheid op internet (KWINT)* aan. Deze nota is de uitwerking van een in *De Digitale Delta* toegezegde verkenning naar de kwetsbaarheden op internet.

In de nota worden ontwikkelingen geschetst met betrekking tot de maatschappelijke en economische betekenis van internet, risico's en kwetsbaarheden van (het gebruik van) internet geanalyseerd en maatregelen ter zake in een aantal landen aangehaald. Om het maatschappelijk en economisch belang van een goed functionerend internet te behartigen, worden tenslotte de rol van de overheid en een aantal concrete actielijnen beschreven. De actielijnen liggen onder meer op het terrein van voorlichting, stimulering van R&D, het stimuleren van effectief management van informatiebeveiliging in organisaties en het vergroten van het inzicht in de betrouw-baarheid van internet.

De nota hangt inmiddels ook samen met de Motie-Wijn c.s. (26 643, nr. 20) van maart jl. In deze motie komt de vraag naar voren in hoeverre de ICT-ontwikkelingen niet alleen gevolgen hebben voor de kwetsbaarheid van internet, de focus van KWINT, maar ook voor andere vitale infrastructuren zoals energie, financiële dienstverlening etc. In de motie wordt gevraagd een sectoroverschrijdend plan van aanpak inzake de bescherming van vitale infrastructuren op te stellen. Het Kabinet onderkent de noodzaak hiertoe. In september vindt overleg op politiek-bestuurlijk niveau hierover plaats, teneinde te bepalen wat een proportionele aanpak is.

Naast dit overleg over een brede aanpak, wordt de uitvoering van de maatregelen zoals genoemd in de nota KWINT op korte termijn ter hand genomen. Samen met de uitvoering van het Nationaal Continuïteitsplan

KST54719
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2001



# Memorandum Vulnerabilities on the Internet

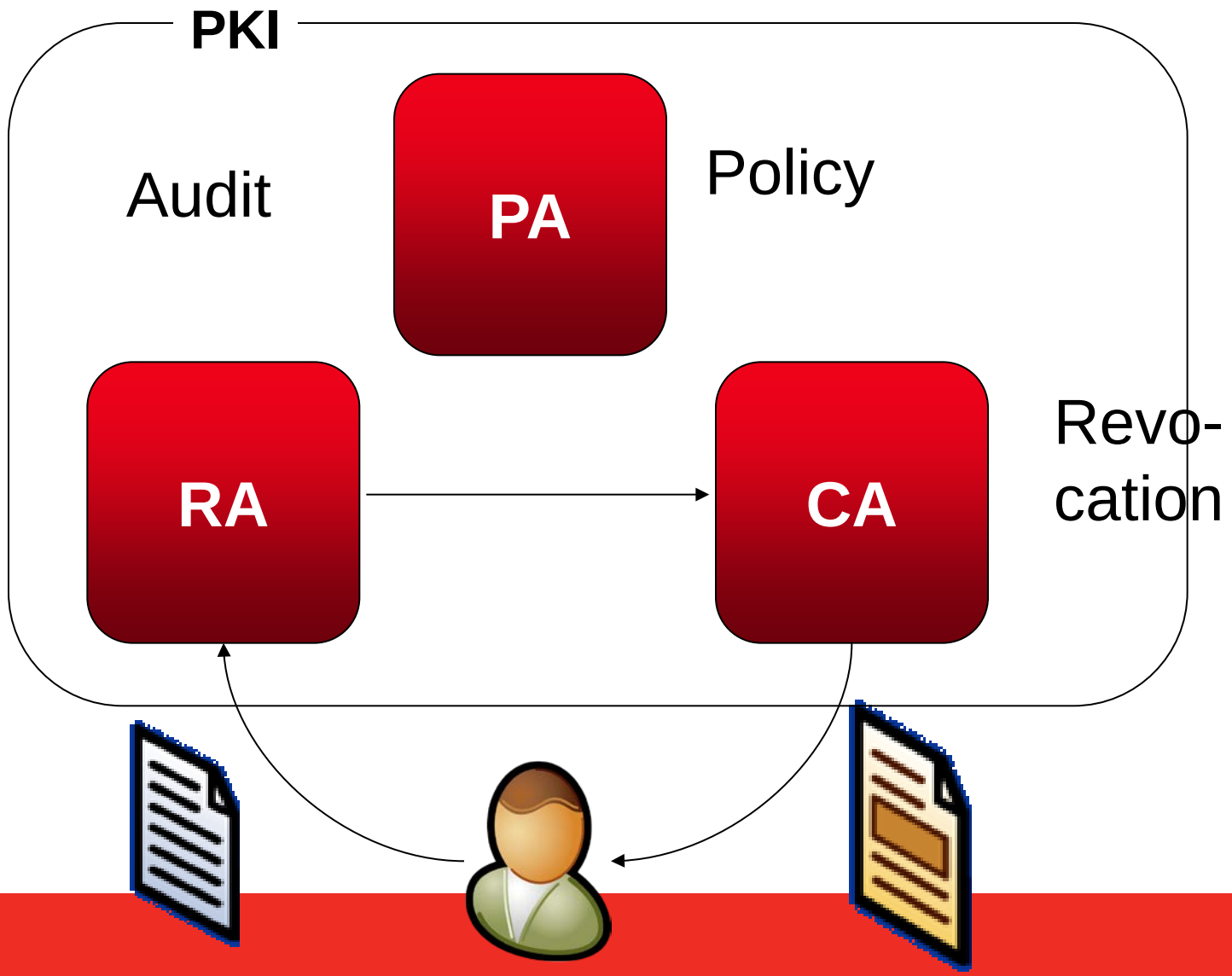
July 2001

National Cyber Security Centre
*Ministry of Security and Justice*

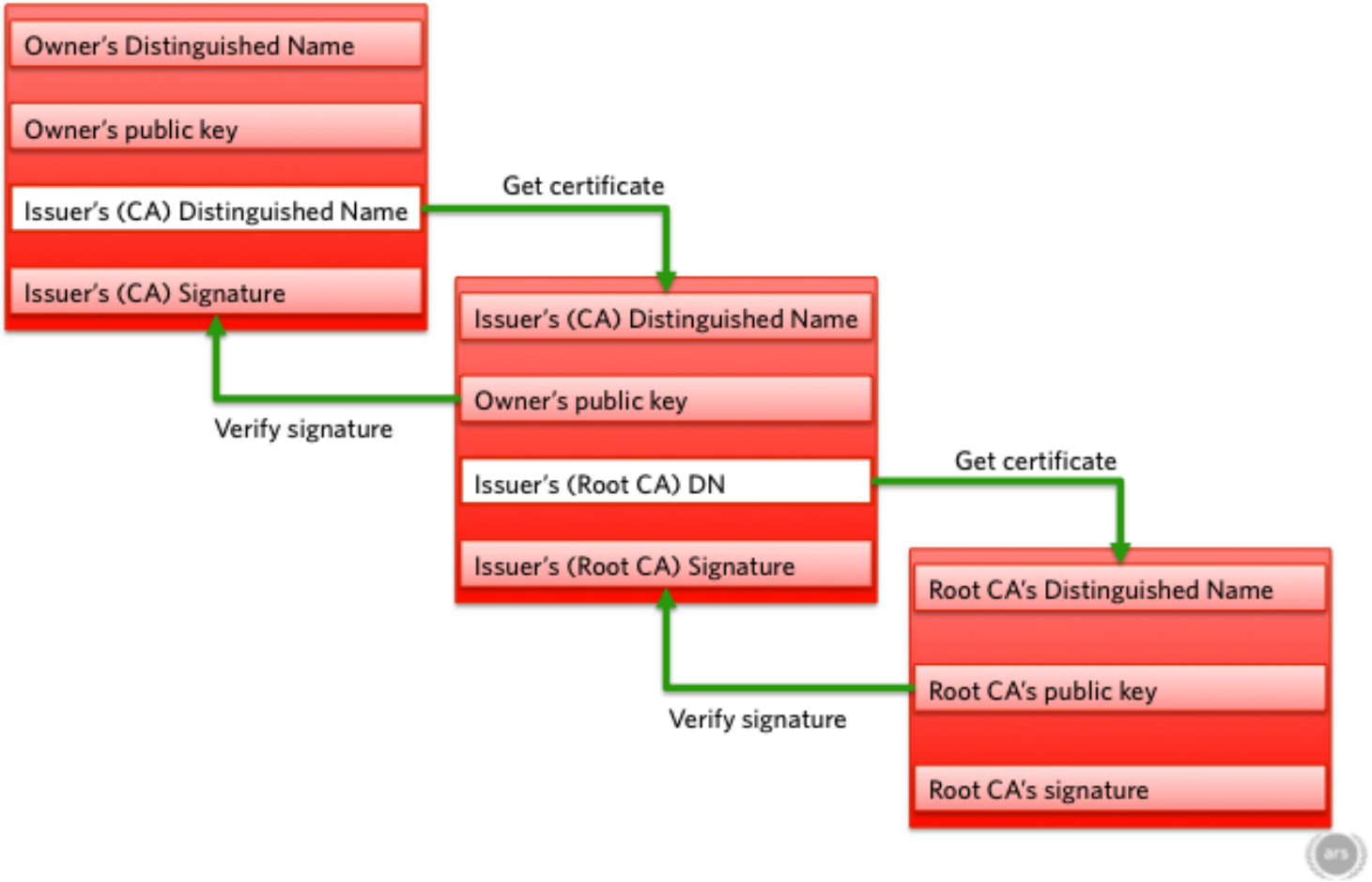
GOV CERT.NL

enisa
European Network and Information Security Agency

Was it Estonia or John?

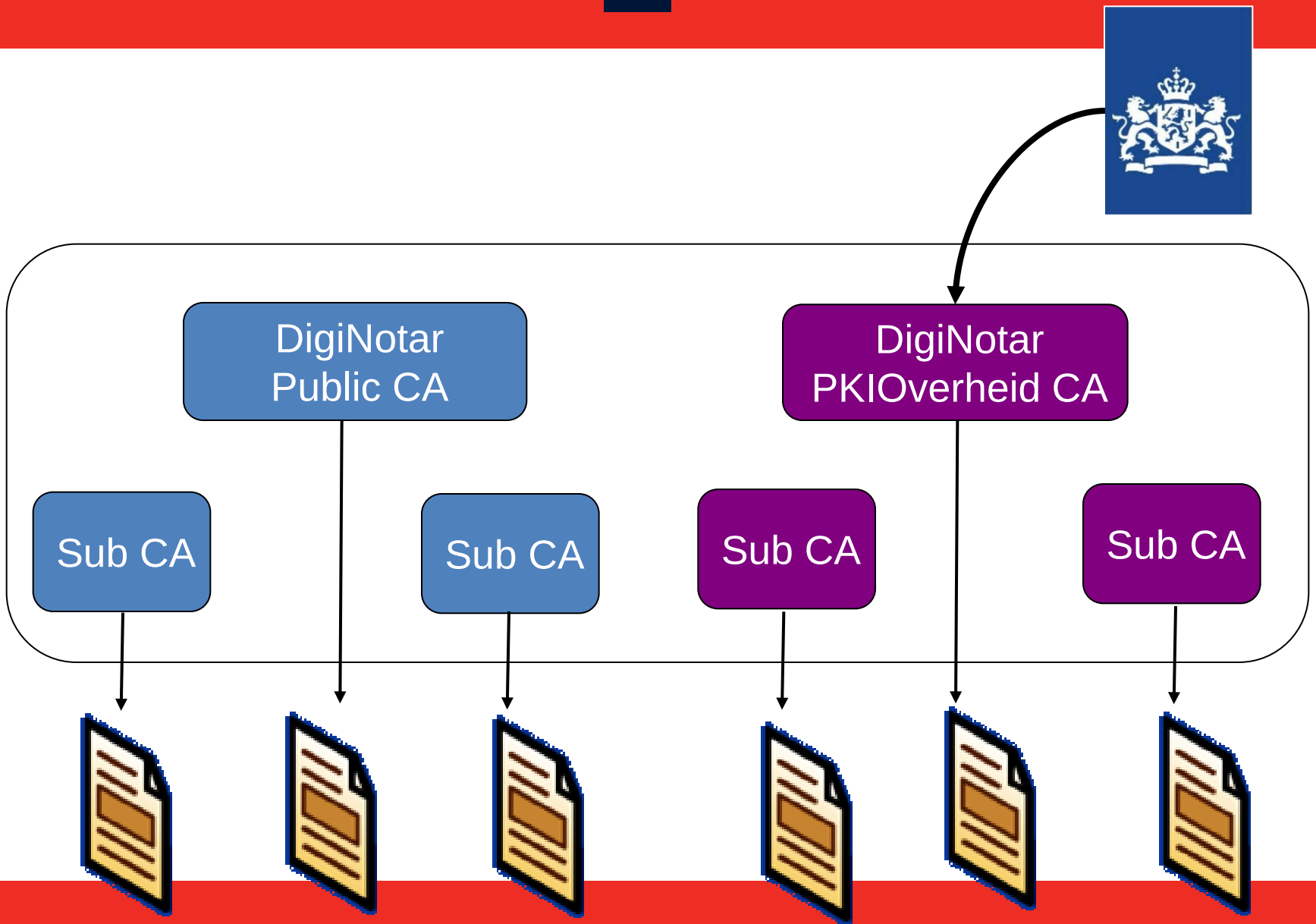

PKI
Audit
PA
Policy
RA
CA
Revo-
cation

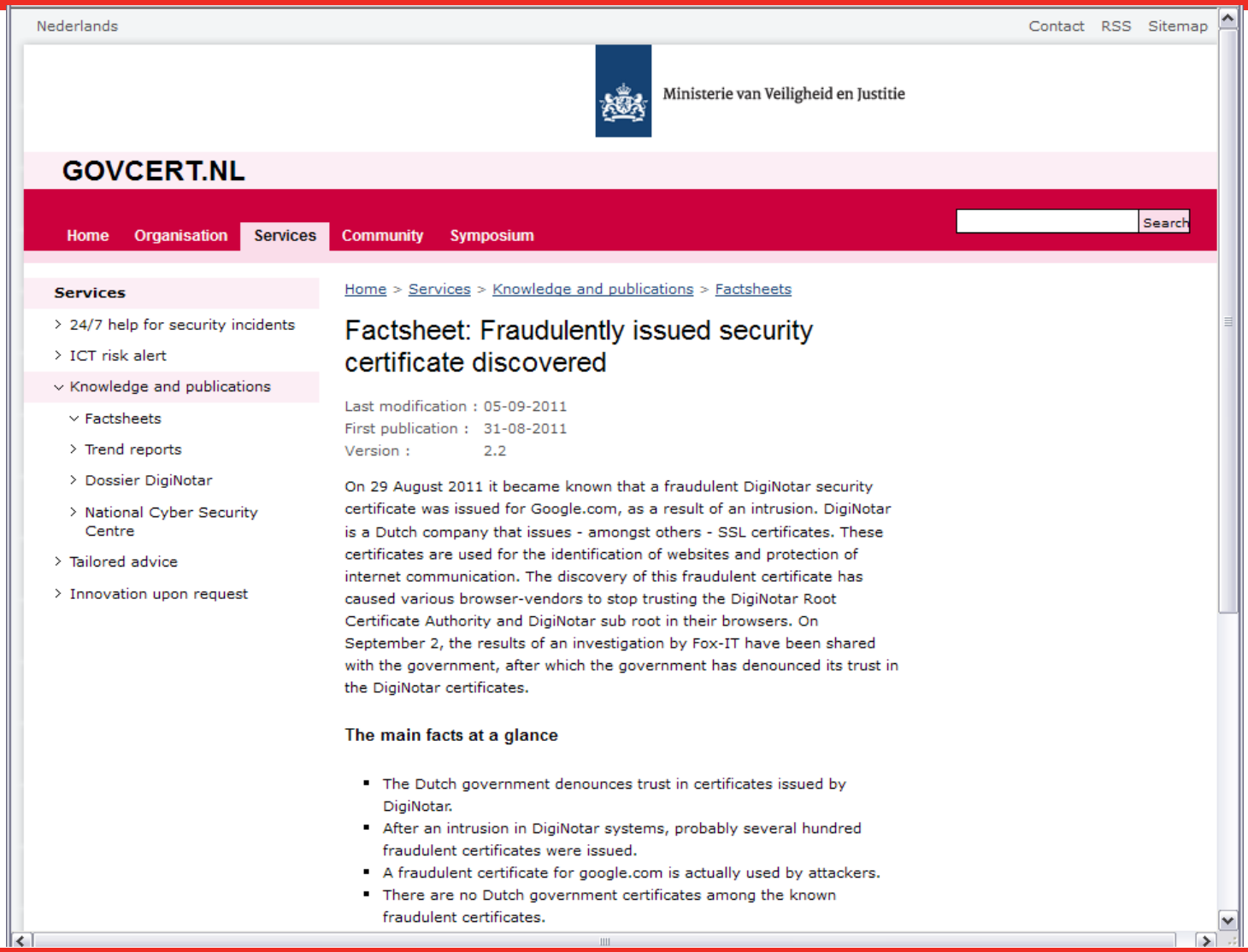
# Chain of trust



DigiNotar
onafhankelijk en vertrouwd op internet

# Video


DigiNotar
Public CA
DigiNotar
PKIOverheid CA
Sub CA
Sub CA
Sub CA
Sub CA



Nederlands Contact RSS Sitemap

Ministerie van Veiligheid en Justitie

GOVCERT.NL

Home Organisation Services Community Symposium Search

Services
- 24/7 help for security incidents
- ICT risk alert
- Knowledge and publications
  - Factsheets
  - Trend reports
  - Dossier DigiNotar
  - National Cyber Security Centre
- Tailored advice
- Innovation upon request

Home > Services > Knowledge and publications > Factsheets

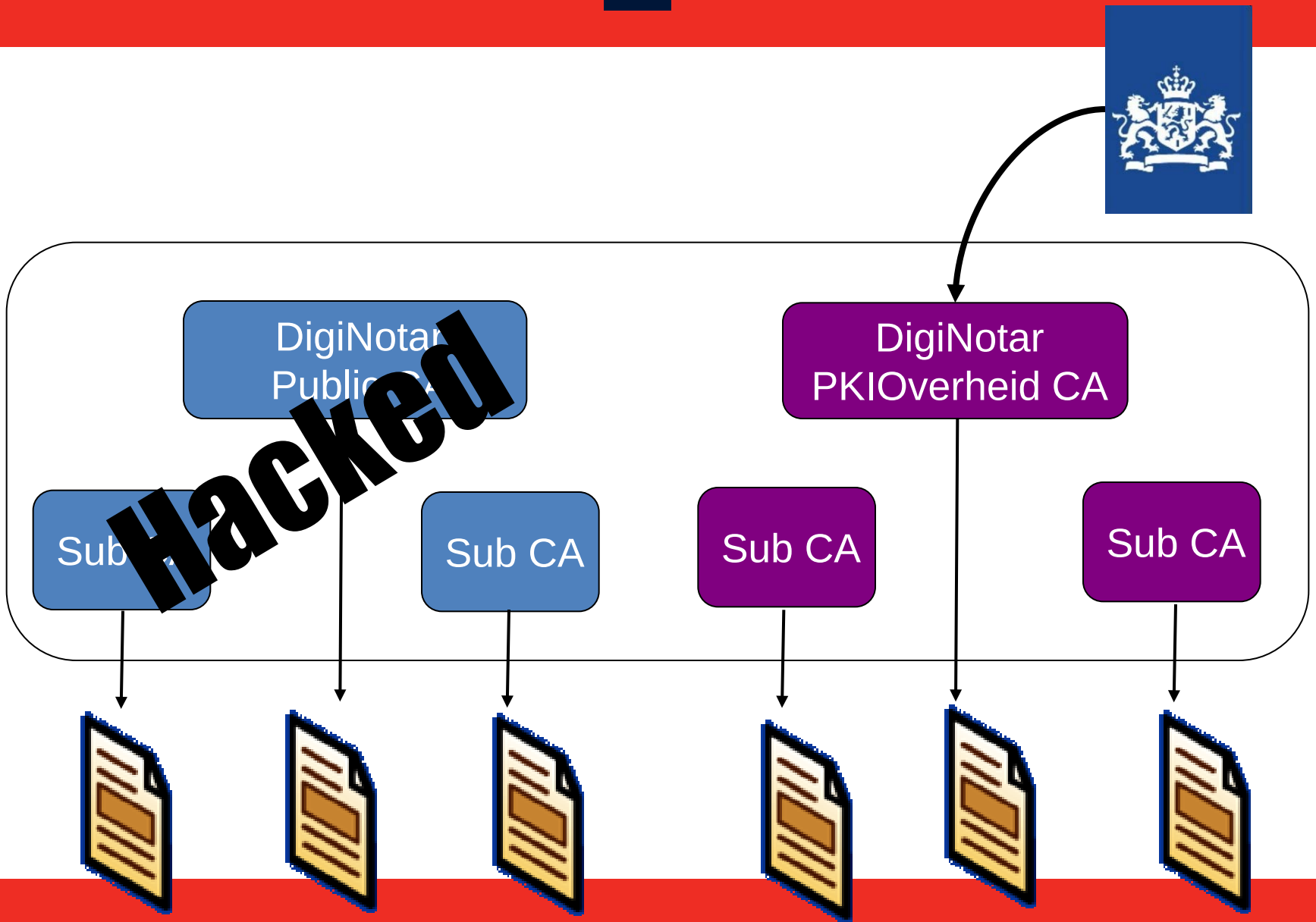
# Factsheet: Fraudulently issued security certificate discovered

Last modification : 05-09-2011
First publication : 31-08-2011
Version : 2.2

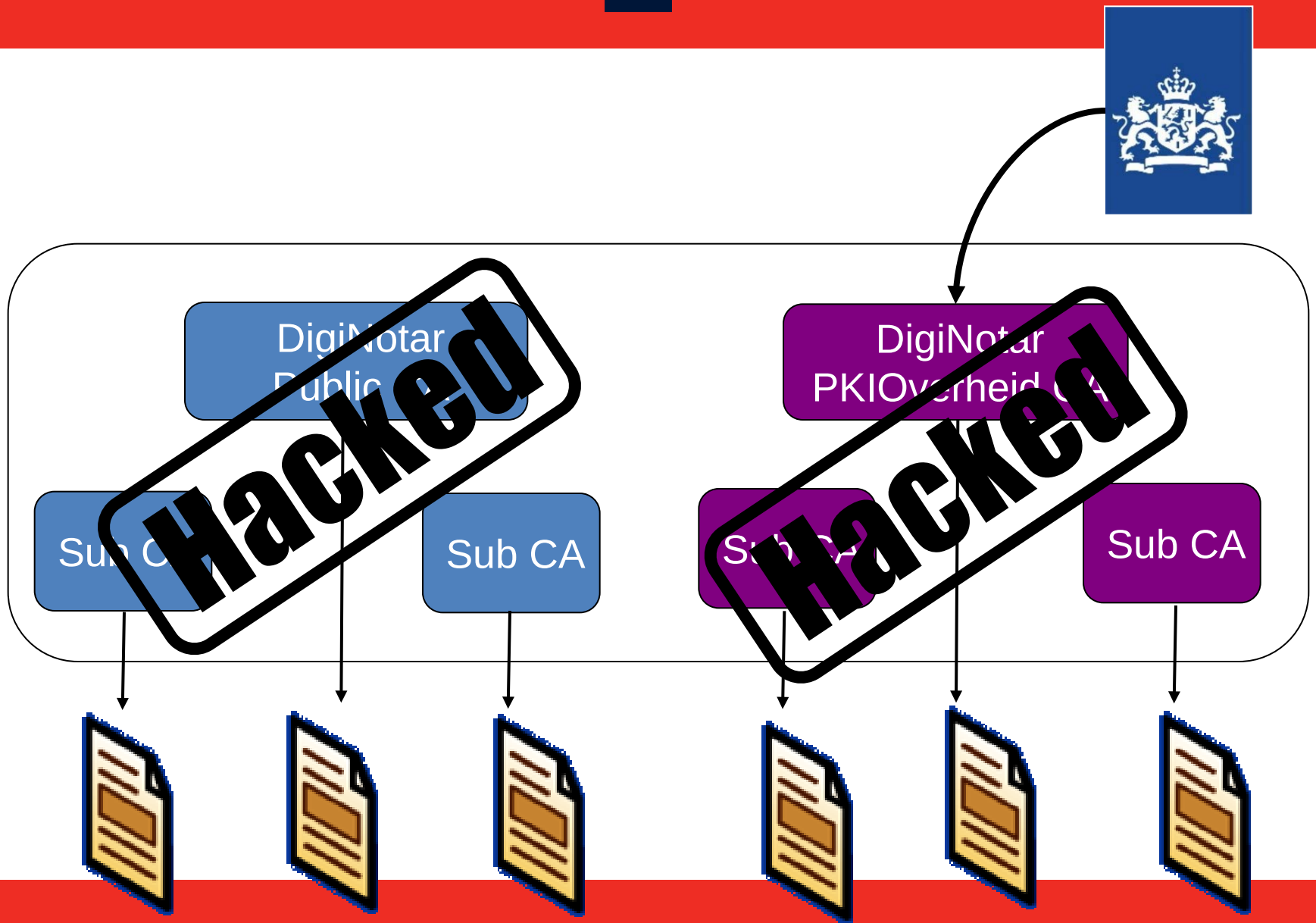
On 29 August 2011 it became known that a fraudulent DigiNotar security certificate was issued for Google.com, as a result of an intrusion. DigiNotar is a Dutch company that issues - amongst others - SSL certificates. These certificates are used for the identification of websites and protection of internet communication. The discovery of this fraudulent certificate has caused various browser-vendors to stop trusting the DigiNotar Root Certificate Authority and DigiNotar sub root in their browsers. On September 2, the results of an investigation by Fox-IT have been shared with the government, after which the government has denounced its trust in the DigiNotar certificates.

**The main facts at a glance**

- The Dutch government denounces trust in certificates issued by DigiNotar.
- After an intrusion in DigiNotar systems, probably several hundred fraudulent certificates were issued.
- A fraudulent certificate for google.com is actually used by attackers.
- There are no Dutch government certificates among the known fraudulent certificates.


DigiNotar
Public
Hacked
DigiNotar
PKIOverheid CA
Sub
Sub CA
Sub CA
Sub CA

H - G


DigiNotar
Public
Sub CA
Hacked
DigiNotar
PKIOverheid
Sub CA
Hacked
Sub CA

From: Erik de Jong (GOVCERT.NL)
Sent: vrijdag 2 september 2011 23:59
To: Alle medewerkers GOVCERT.NL
Subject: De middernachtscrisishaiku

Het is tijd voor de traditionele [1] middernachtscrisishaiku.

**Trust builds up slowly**
**SSL certificates**
***Poooof* trust gone like that**

[1] Elke traditie kent een begin.

GOVCERT.NL
T +31 70 888 75 55
I www.govcert.nl
E info@govcert.nl
PGP Fingerprint: 5EF4 6F80 7530 1583 E140  D918 BC24 36AC 1045 1333

From: Aart Jochem (GOVCERT.NL)
Sent: zaterdag 3 september 2011 23:51
To: Alle medewerkers GOVCERT.NL
Subject: RE: De middernachtscrisishaiku

**When trust revoked**
**Computers silenced in rack**
**You and me remain**

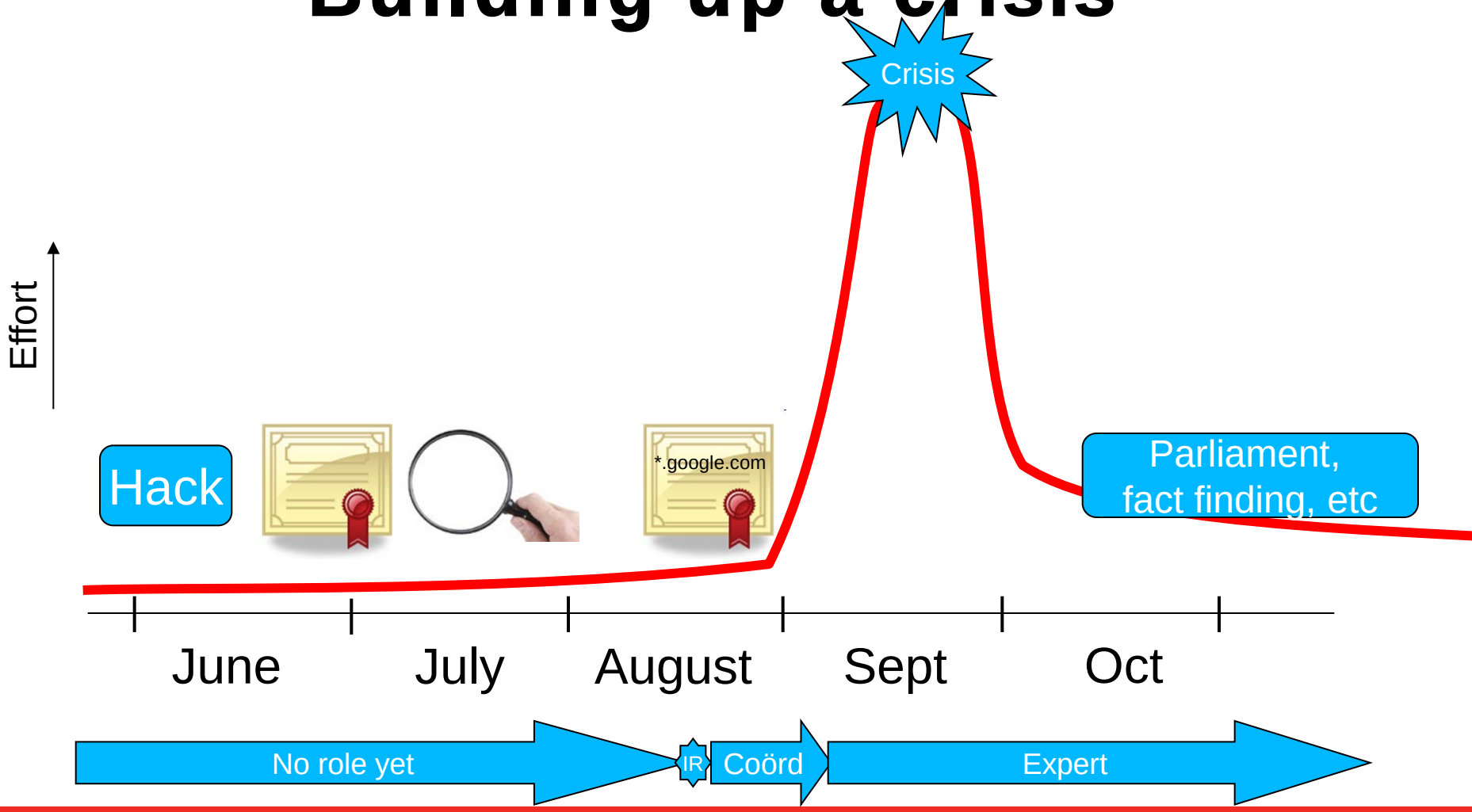
Aart

From: Bob (GOVCERT.NL)
Sent: Maandag 5 september 2011 23:58
To: Alle medewerkers GOVCERT.NL
Subject: RE: De middernachtscrisishaiku

**Bits, elements of trust**
**Gateways to precious freedom**
**Sorry, revoked**

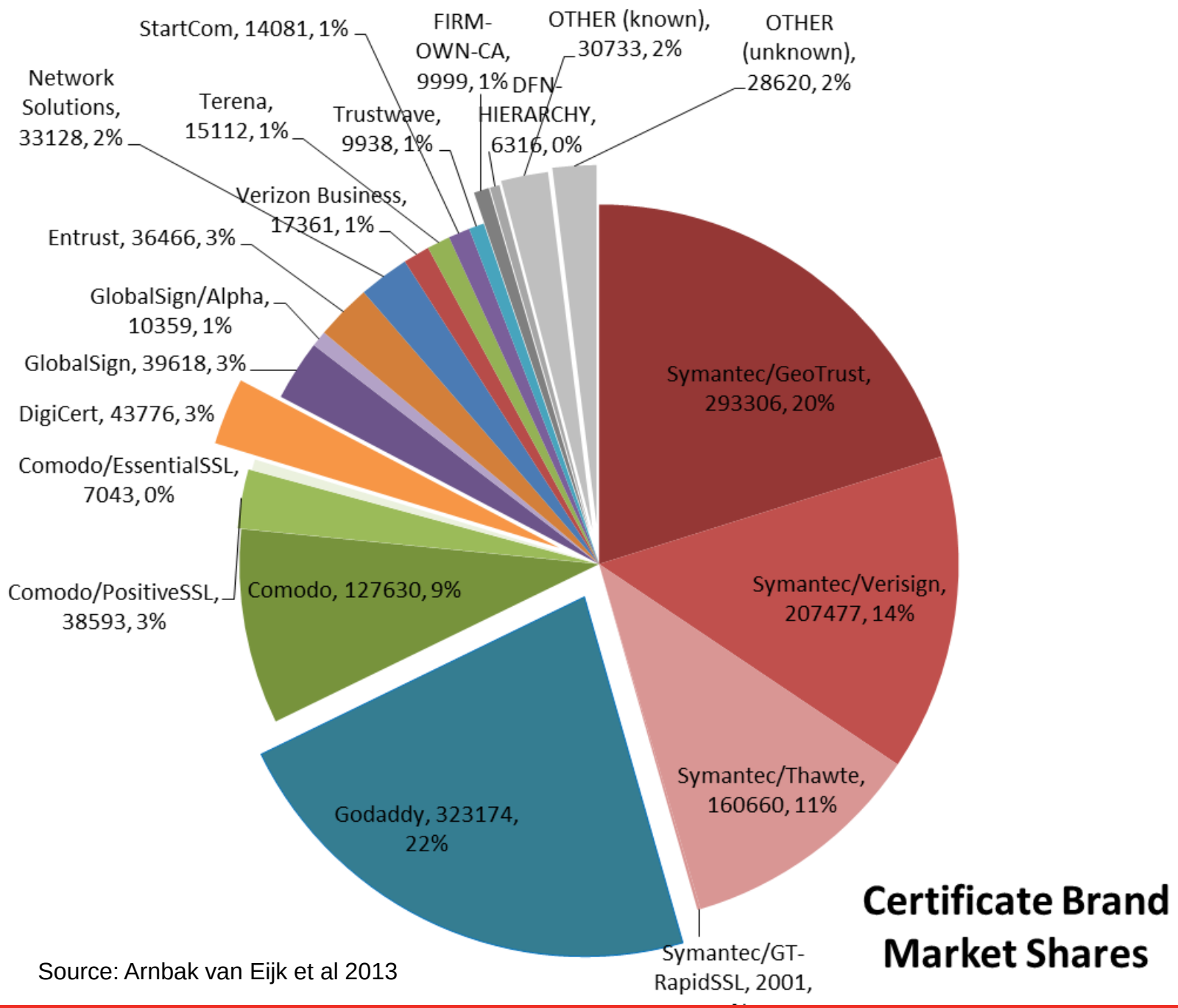
Bob

# Building up a crisis



# What's next?

- The DigiNotar crisis is over…
    - ….but the PKI-crisis is not




**Certificate Brand Market Shares**

Source: Arnbak van Eijk et al 2013

# A PKI is a critical infrastructure

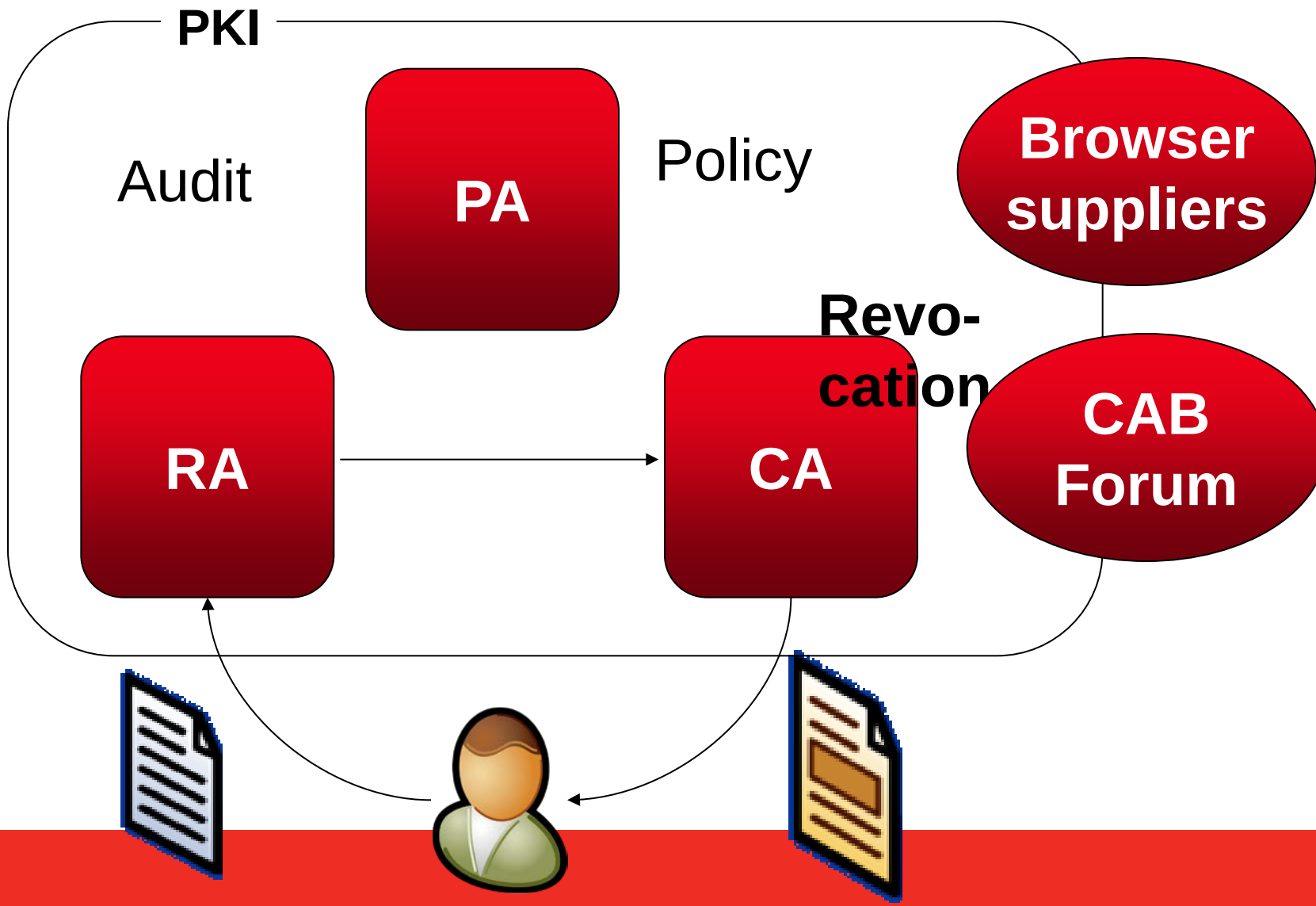
- Treat it like one
- Create awareness
- Monitor the RA’s and CA’s
- Strengthen oversight

# Manage certificate as assets

- Have an inventory
- Add to asset management system
- Provide for backups or cross-signing

# Support secure techniques

- That’s why we are here
- Adopt DNSSEC


PKI
Audit
PA
Policy
Browser suppliers
Revo-cation
RA
CA
CAB Forum

# CA-failure response

- Provide for a grace period of two weeks before an anounced revocation of a CA

# The DigiNotar Crisis

*from incident response*

*to crisis coordination*

# Questions?

***Aart Jochem***
aart.jochem () ncsc .nl

**Credits:**
**Security Economics and Value-Chain Governance of HTTPS Communications**
Axel M. Arnbak+, Nico A.N.M. van Eijk+, Hadi Asghari* & Michel J.G. van Eeten*1
To be presented at WEIS 2013