



Logius  
*Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties*

## Public Key Infrastructure (PKI) voor de overheid

“Overgang naar PKIo G2  
SHA-256 certificaten”

Mark Janssen

23 juni 2011





## Agenda

- Introductie PKIoverheid
- PKIoverheid actoren
- Waarom overgang SHA-256?
- Wat is verschil tussen G2 en SHA-256?
- Minimale eisen aan gebruik G2 en SHA-256
- Werking SSL
- Staat het certificaat in het OS of de browser?
- Voorbeeld niet voldoen aan minimale eisen
- Indicatie gebruik OS in NL
- Indicatie gebruik browser in NL
- Maatregelen
- Belangrijkste maatregel: communicatie
- Vragen?



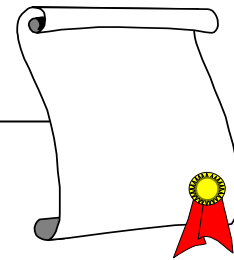
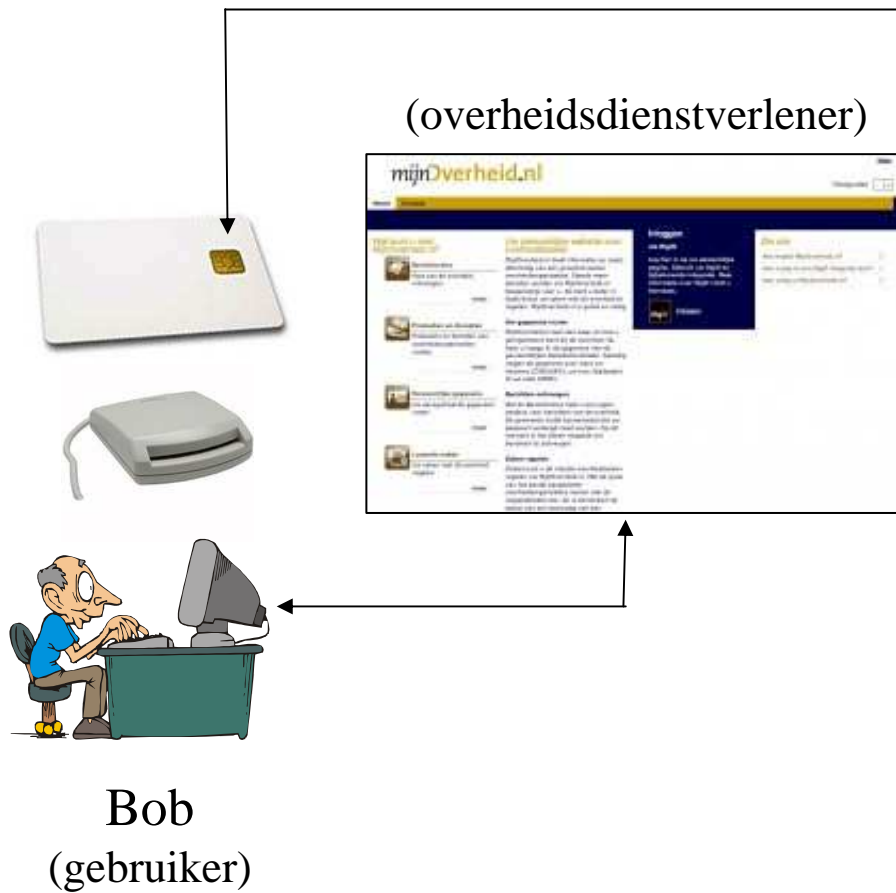


## Introductie PKIoverheid

- Faciliteren gebruik gekwalificeerde elektronische handtekening binnen de overheid;
- Interoperabiliteit (voorkomen eilandvorming);
- Eén Programma van Eisen voor een PKI voor de overheid;
- Uitgevers (CSP's) moeten voldoen aan de eisen van PKIoverheid;
- CSP's (marktpartijen): Digidentity, DigiNotar, ESG, Getronics en QuoVadis;
- Toepassing: overheid naar bedrijven, overheid naar burgers en overheid naar overheid.



# PKIoverheid actoren



Certificaat uitgevers  
(productie)



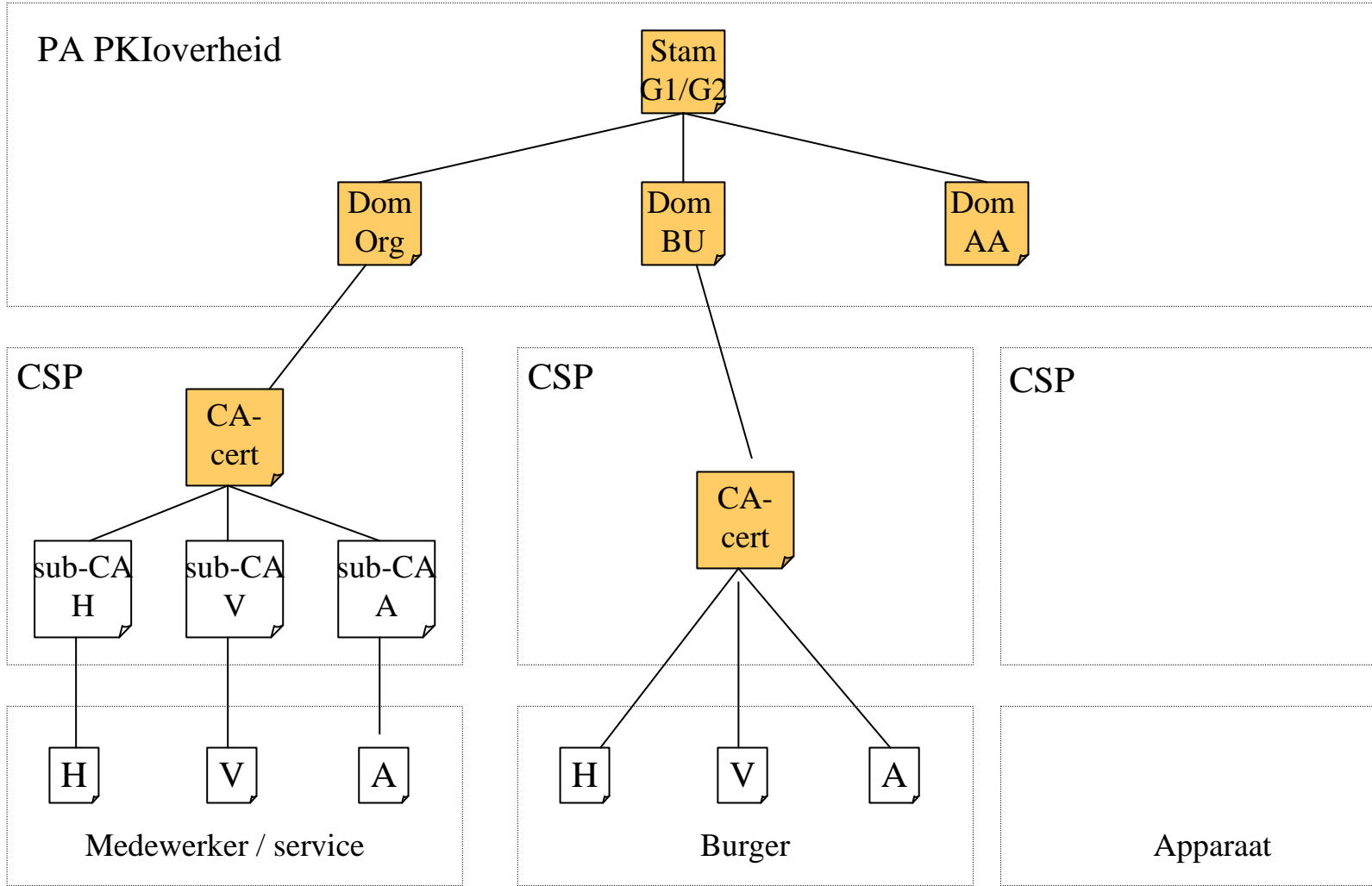
Registratie Autoriteit  
(loket)



Policy Authority  
(beleidsmaker en  
toezichthouder)



Auditor  
(verificatie)



model : 5 niveaus

model : 4 niveaus



## Waarom overgang naar SHA-256?

- In 2005 succesvolle aanval op SHA-1. Nog wel veilig maar toekomstbestendigheid staat onder druk;
- Amerikaanse overheidsorganisatie National Institute for Standards and Technology (NIST) heeft geadviseerd om tot uiterlijk 31 december 2010 SHA-1 certificaten uit te geven en dan over te gaan op een algoritme van de sterkere SHA-2 familie;
- Met het vanaf 1-1-2011 uitgeven van SHA-256 certificaten onder de Staat der Nederlanden Root CA – G2, volgt PKIoverheid dit advies.



## Wat is verschil tussen G2 en SHA-256?

- G2 refereert aan de tweede generatie van de hiërarchie van de PKI voor de overheid onder de Staat der Nederlanden Root CA - G2;
- Deze hiërarchie is gebaseerd op het verbeterde en meer toekomstbestendige SHA256 algoritme.



## Minimale eisen aan gebruik G2 en SHA-256

### Besturingssysteem

Microsoft

Mac OS

Microsoft

### Internetbrowser

Mozilla

Opera

### Minimale versie voor eindgebruikers

Windows XP SP3, i.c.m. Internet Explorer 6, Google Chrome.

Mac OS X 10.5.5

### Minimale versie voor afnemers

Windows Server 2003 SP1/SP2 (met hotfix KB 938397 of KB 968730), Windows Server 2008

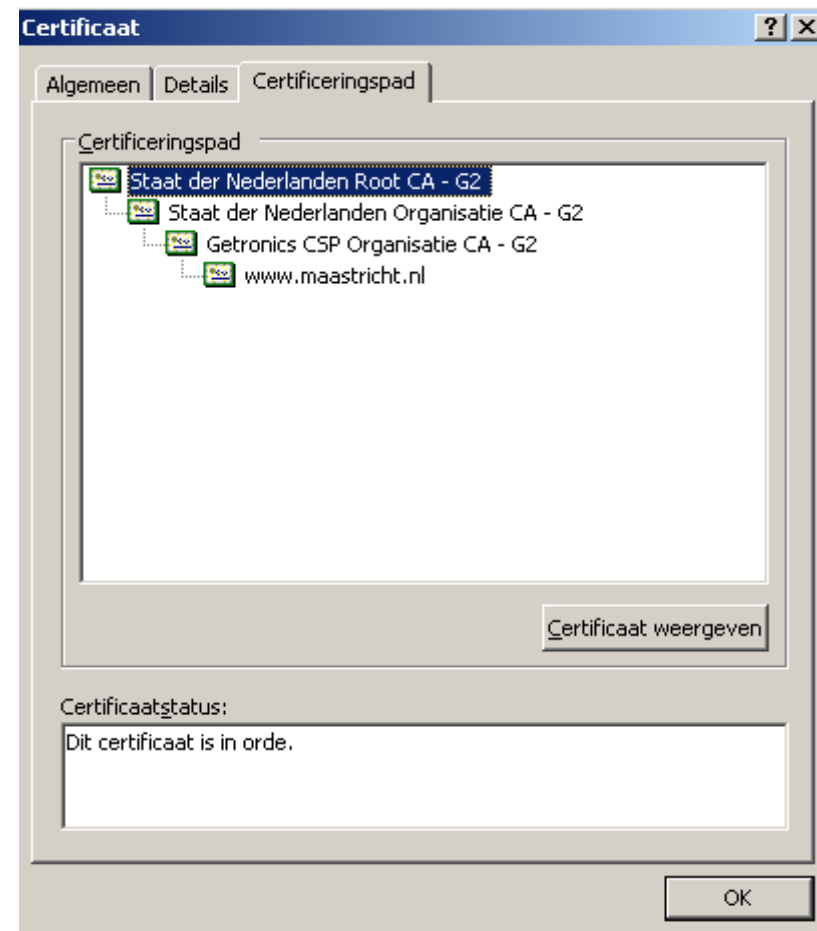
### Minimale versie

Firefox 3.5.9 tot 3.5.x en 3.6.2 tot 3.6.x

10.00



# Werking SSL (<https://www.maastricht.nl/>)



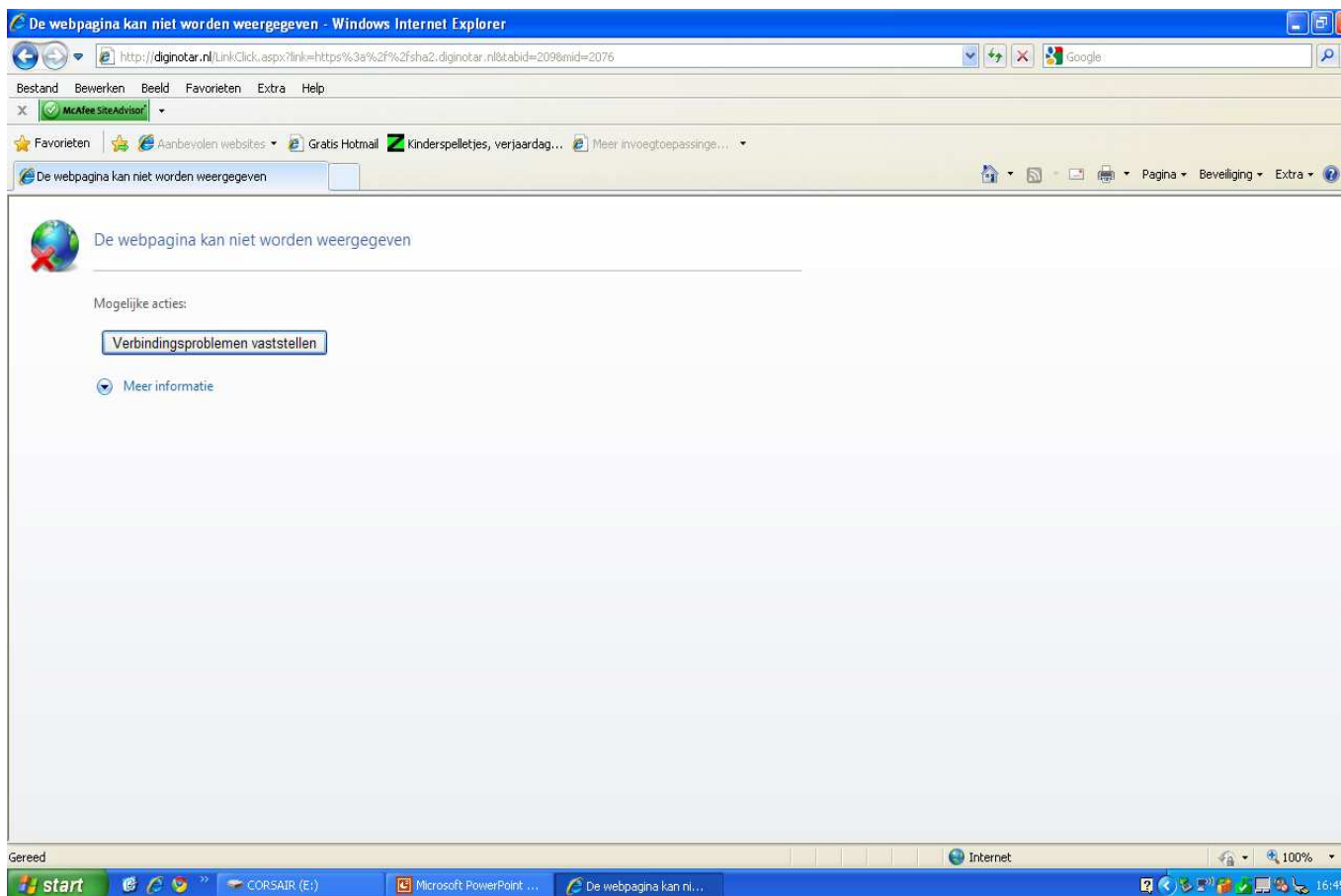


## Staat het certificaat in het OS of de browser?

- De browsers Internet Explorer, (Apple) Safari en Google Chrome hebben geen eigen Certificate Store. Deze browsers maken gebruik van de Certificate Store van het van toepassing zijnde besturingssysteem (OS). Om die reden is de juiste versie van het besturingssysteem hierbij relevant.
- De browsers Firefox en Opera hebben wel een eigen Certificate Store. Om die reden is de juiste versie van de browser hierbij relevant.

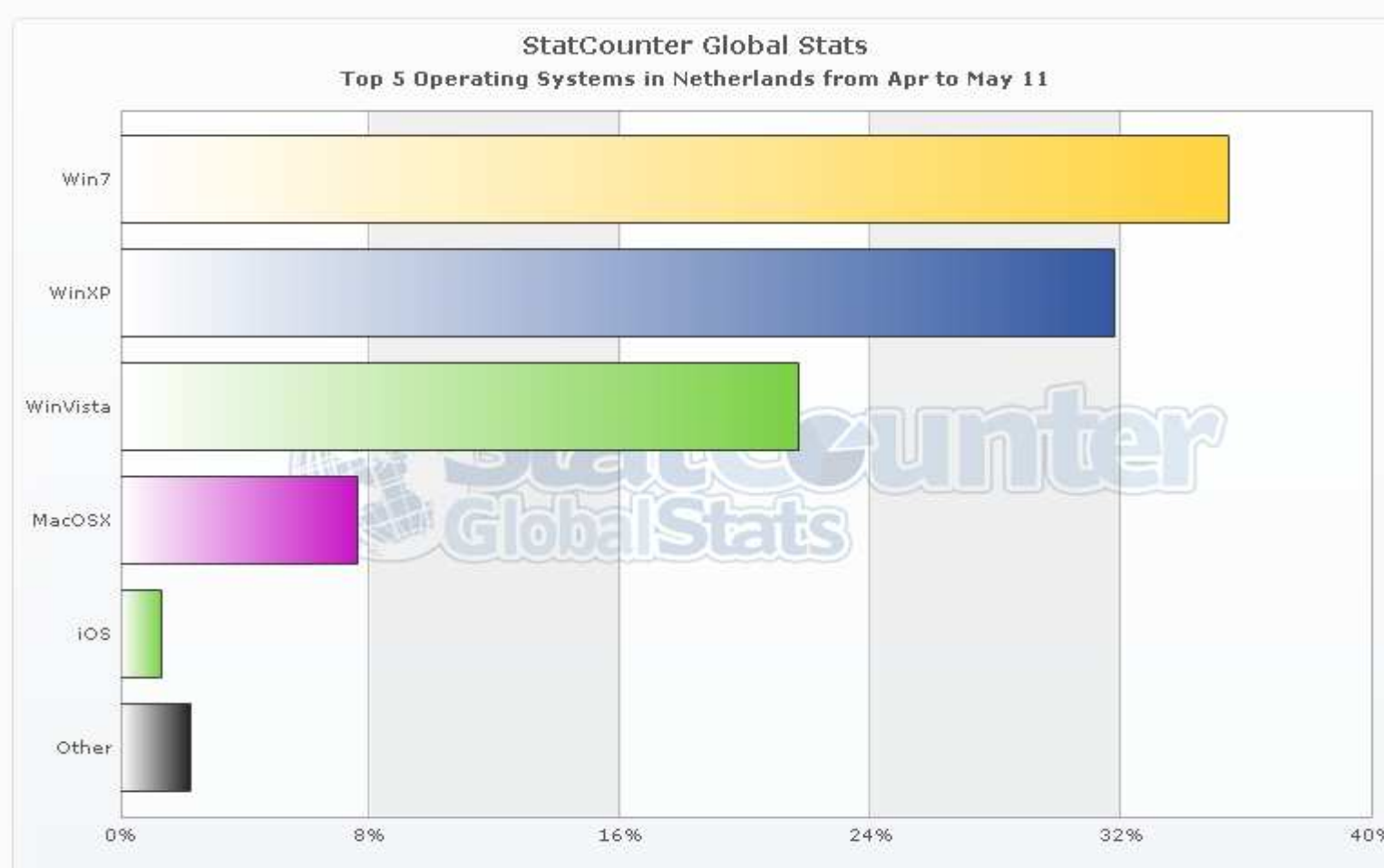


## Voorbeeld (Niet voldoen aan minimale eisen)



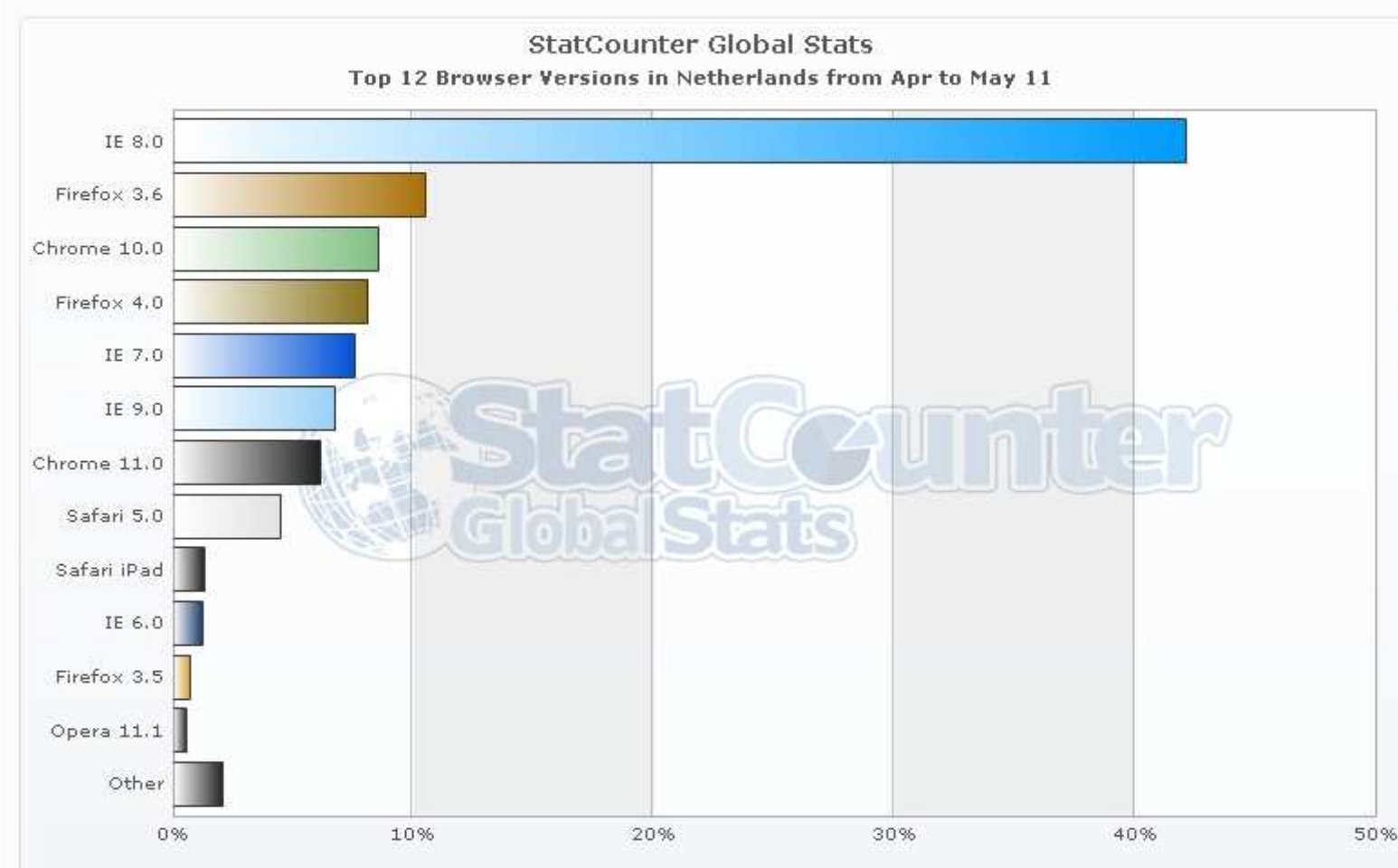


## Indicatie gebruik OS in NL





## Indicatie gebruik browser in NL





## Maatregelen

- Alle Logius voorzieningen zijn SHA-256 proof;
- SHA-2 staat sinds 2010 op lijst met gangbare open standaarden van FS;
- PKIoverheid leveranciers hebben al veel gecommuniceerd over SHA-256 naar hun klanten.



## Belangrijkste maatregel: communicatie

Reeds gedaan:

- Op 11-11-2010 en 19-4-2011 e-mail aan 3000 afnemers;
- Logius webpagina:  
<http://www.logius.nl/producten/toegang/pkioverheid/documentatie/certificaten-pkioverheid/staat-der-nederlanden-g2/toepasbaarheid/>
- <http://www.logius.nl/producten/toegang/pkioverheid/documentatie/certificaten-pkioverheid/staat-der-nederlanden-g2/veelgestelde-vragen/>
- VOORLOPIGE planning DigiD:
  - mei 2012: plaatsen PKIo G2 SSL certificaten op website;
  - eind 2012: plaatsen PKIo G2 server certificaat t.b.v. afnemers.



# Vraag & Antwoord

