Logius
Ministry of the Interior and Kingdom Relations

Mitigating the Impact of incidents on the PKIoverheid system

Logius
Ministry of the Interior and Kingdom Relations

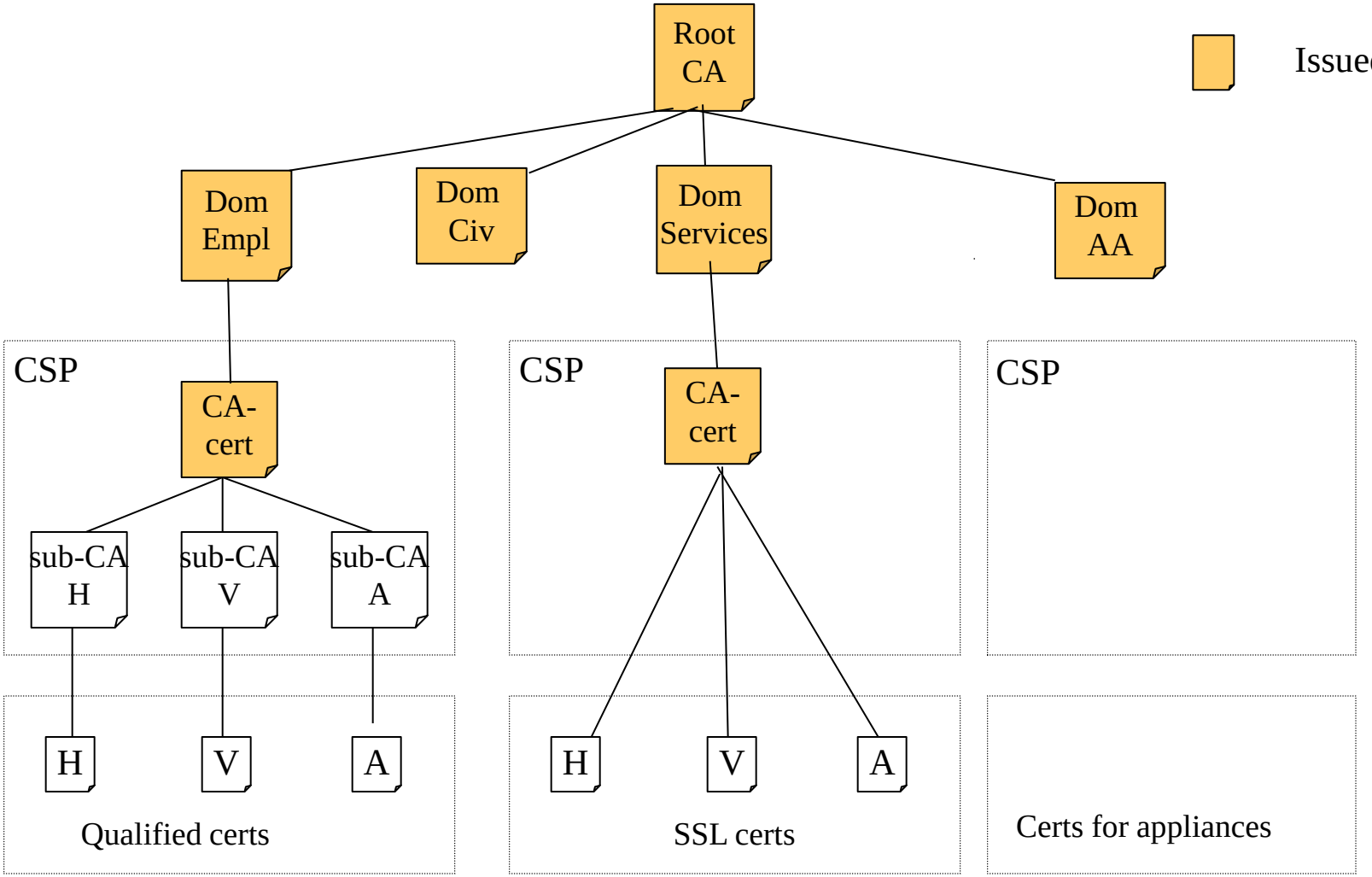
Mitigating the impact of incidents on the PKIoverheid system

Robert van de Rijt
Tactical administrator
Policy Authority PKIoverheid

1 oktober 2013

PKIoverheid

- PKIoverheid is the PKI for the Dutch government (Staat der Nederlanden Root CA);
- The Ministry of Interior and Kingdom Relations (represented by Logius) is the owner of PKIoverheid;
- Certificate Service Providers (CSPs) must comply with the PKIoverheid requirements (CP = Programma van Eisen);
- CP based om ETSI, IETF RFCs, CABforum BR, additional PKIoverheid requirements;
- CSPs are both commercial CAs and some ministries;
- Policy Auhority (PA) PKIoverheid. Tasks: supervision and policy.


Root CA
Issued by the PA
Dom Empl
Dom Civ
Dom Services
Dom AA
CSP
CA-cert
sub-CA H
sub-CA V
sub-CA A
H
V
A
Qualified certs
CSP
CA-cert
H
V
A
SSL certs
CSP
Certs for appliances

Mitigating the impact of incidents

- Root and domain CA certs are offline in a vault;
- PA does not assist hands-on in problem solving of security incidents at a particular CSP;
- Requirements and controls to mitigate the impact on the PKIoverheid system as a whole.

Requirements and controls 1

- More supervision on CSPs;
- Pentests;
- Separation between the PKIoverheid services and other PKI services or hardware infrastructure;
- PKIoverheid services must be separated physically if possible but at least logically;
- Subscribers are urged to have backup certificates;
- CP contains an incident and security breach notification requirement;

Requirements and controls 2

- Extensive logging;
- Cooperation with other government agencies;
- Disaster Recovery plan;
- The PA has trilateral meetings with the ACM and the auditors regularly to level on the current status of the system;
- Private Root CA.

Limiting trust

Compartmentalizing / Limiting trust in certs is a important measure to control and mitigate the impact of security incidents for the PKIoverheid system but certainly also on a more holistic level. For example, limit trust in PKI certs on the basis of:

- Geography – regional trust list browsers;

- Extended key usage - only publicly trusted certs with an EKU of client-server authentication used for setting up an SSL connection;

- specific software / applications – public key pinning, need to have instead of nice to have.