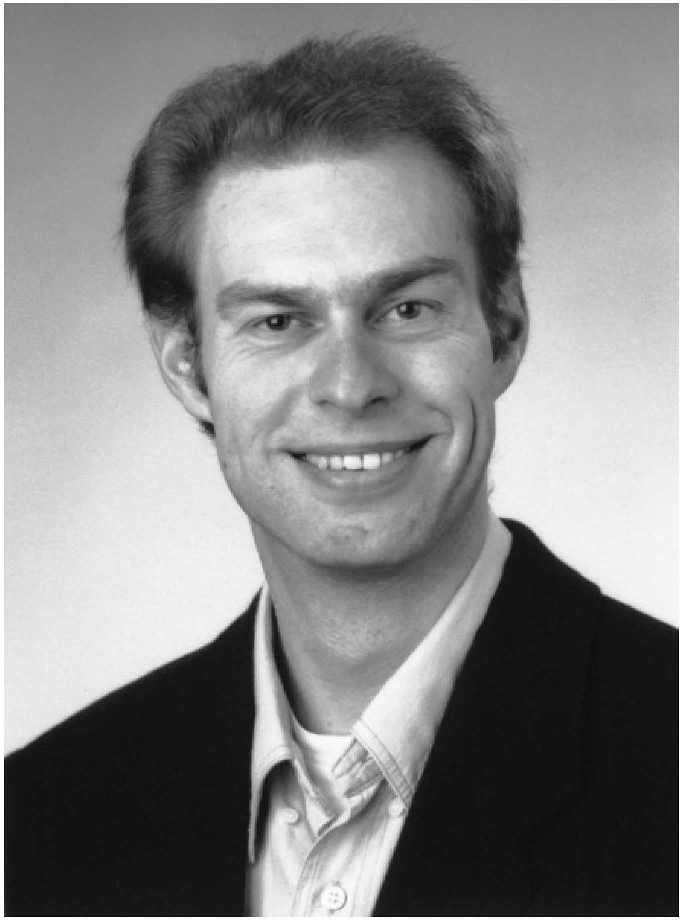
Trust – the root of evil?!

Alexander Bahlo

About Me

- Studies in Business Administration and Computer Science
- Focus on IT Security
- Working as IT Specialist for Customer Care and Lifecycle Support

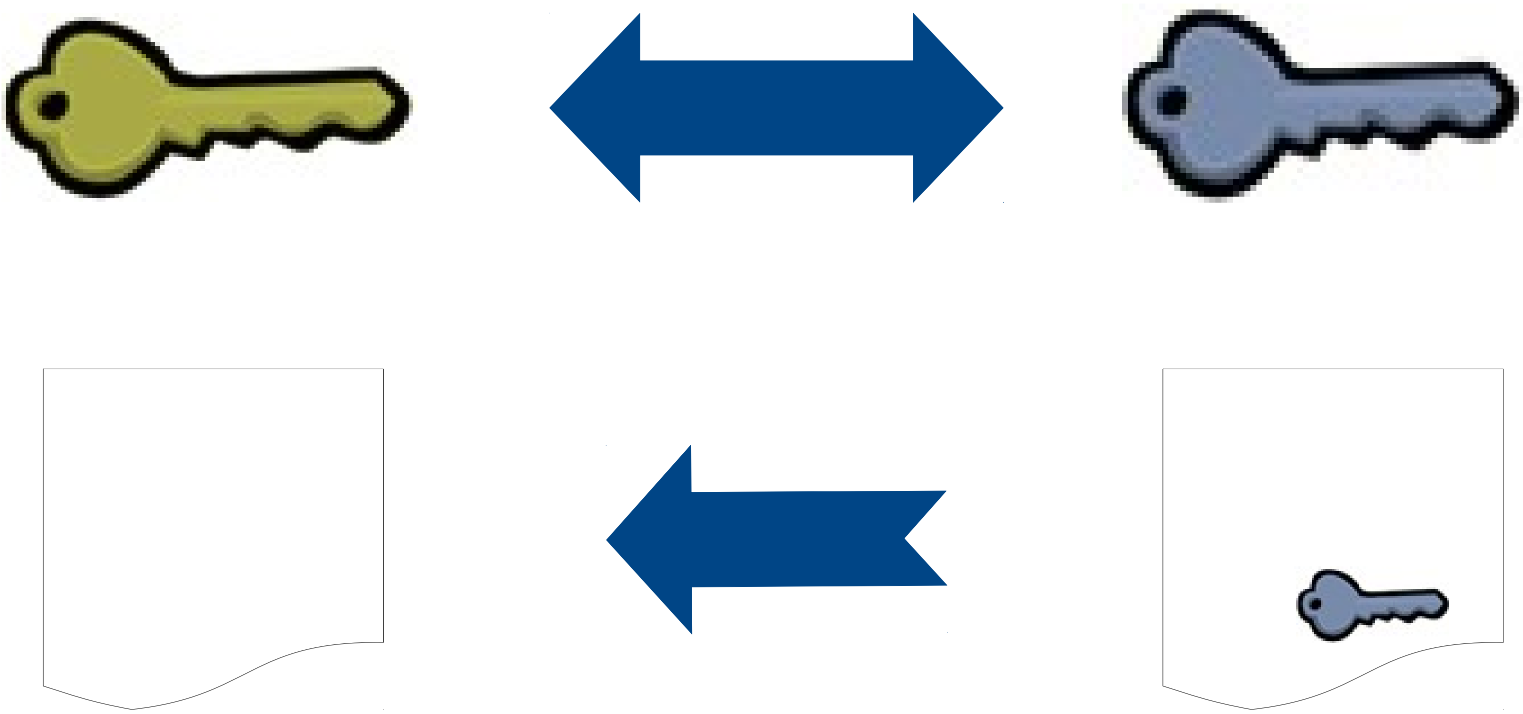


What We Talk About Today

1. PKI & CA Basics
2. The 2011 Cases
3. CAcert as Open Alternative

!

PKI Basics



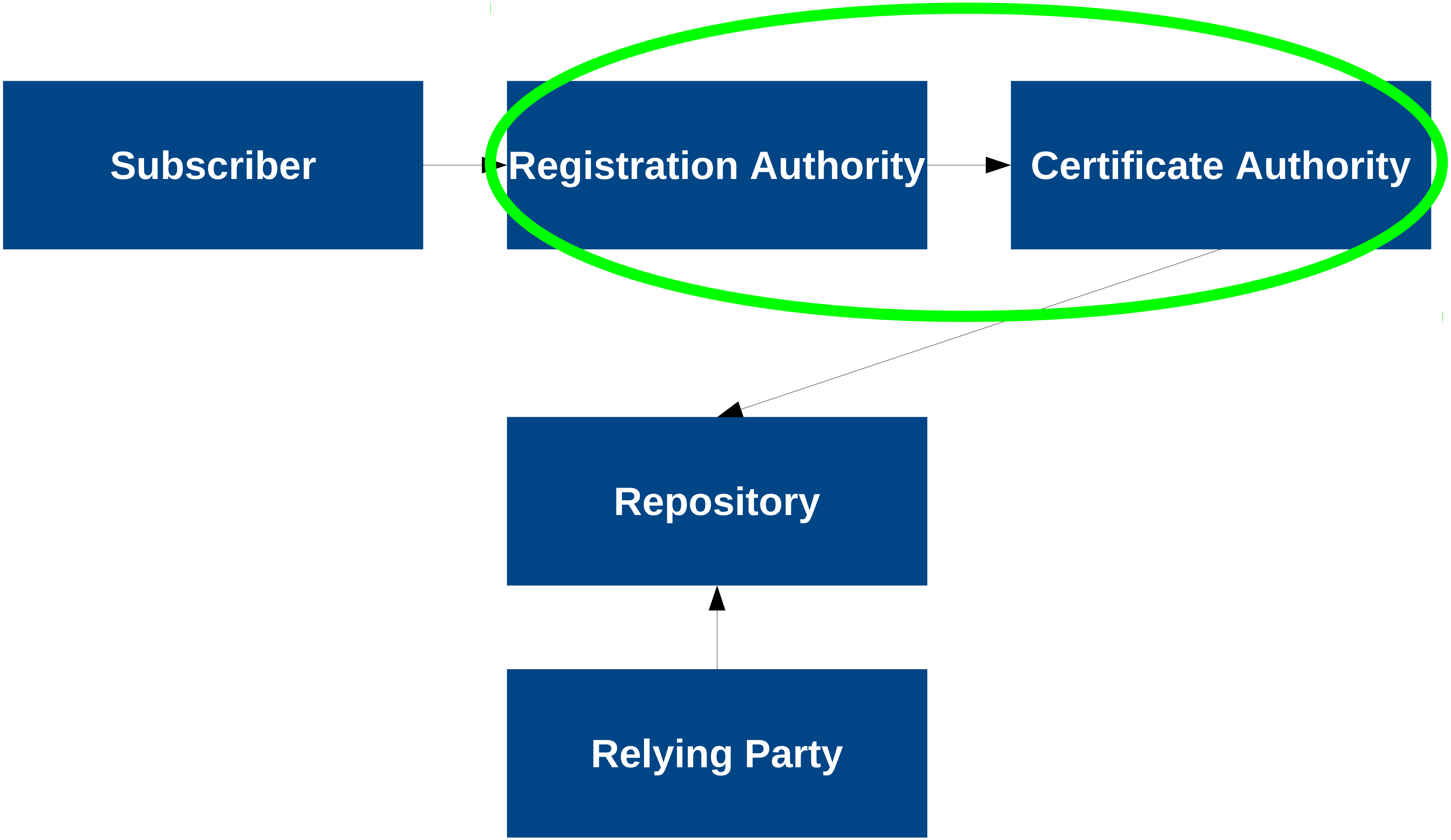
Private Key

Public Key

Plain Text

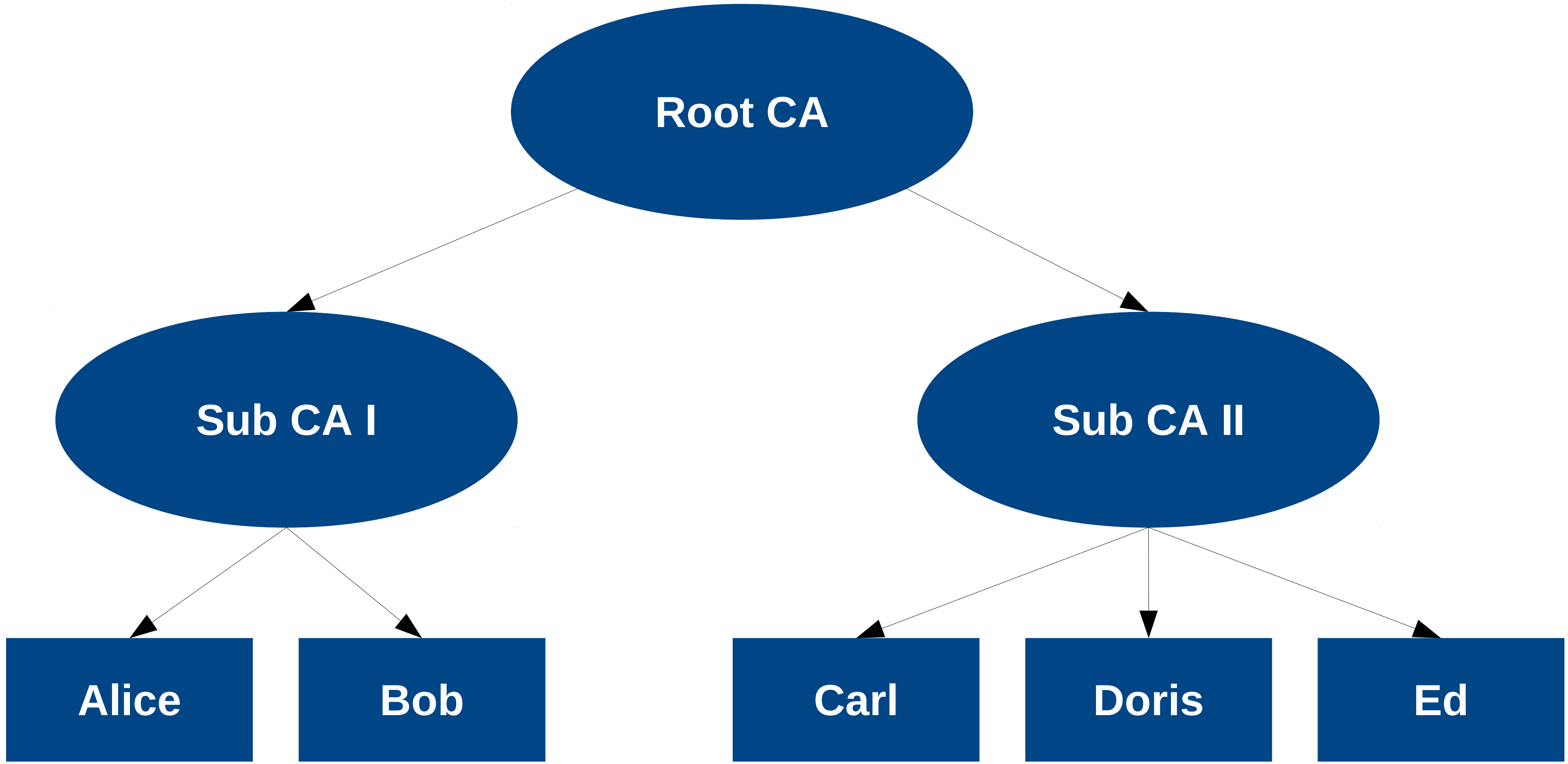
Encrypted Message

What Is A CA?


Subscriber
Registration Authority
Certificate Authority
Repository
Relying Party

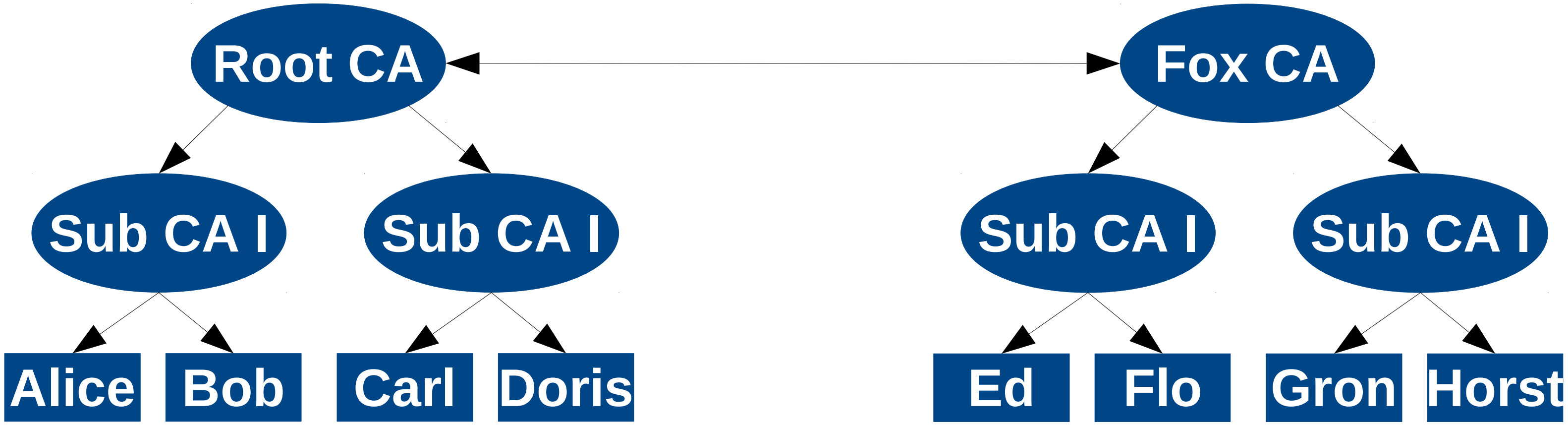
Trust Anchor 1/2

Hierarchical CA

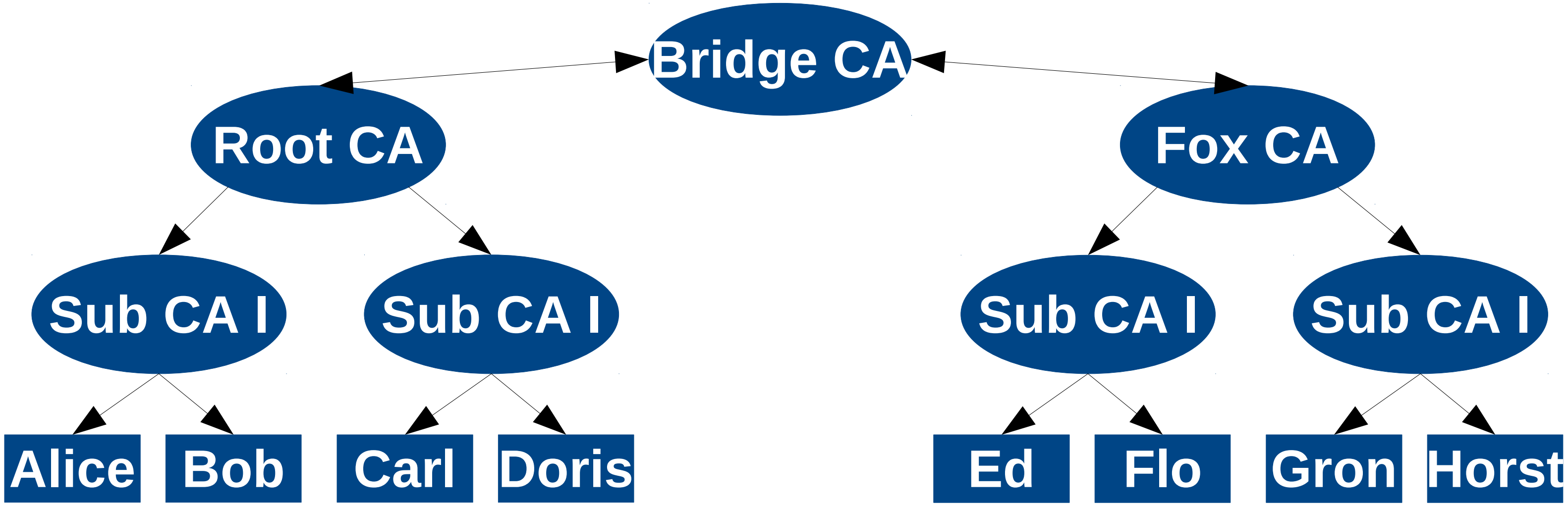


Trust anchor 2/2

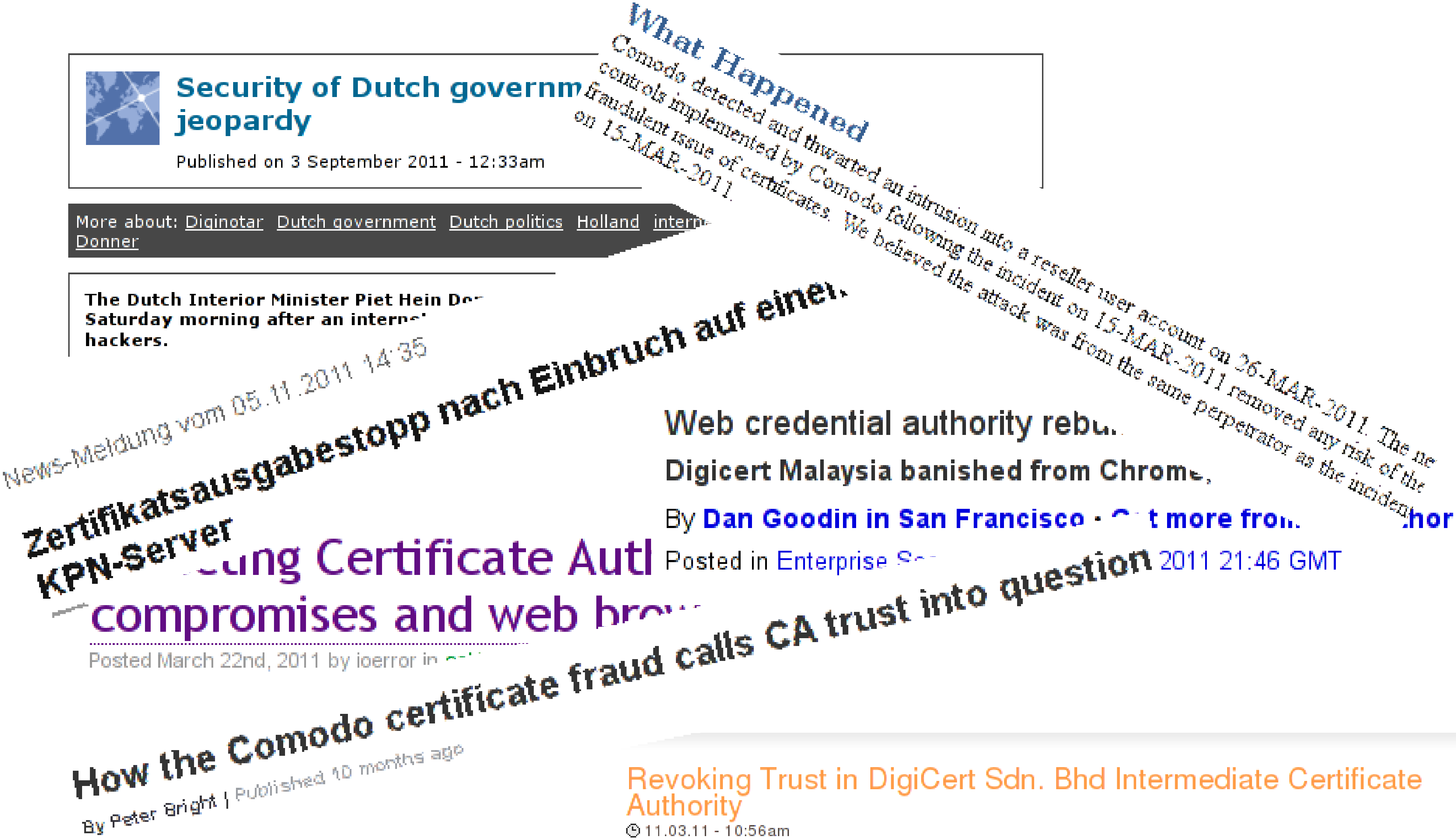
Cross-Certified CAs



Bridged CAs



What happened in 2011



Security of Dutch governm jeopardy

Published on 3 September 2011 - 12:33am

More about: Diginotar Dutch government Dutch politics Holland intern Donner

The Dutch Interior Minister Piet Hein Do Saturday morning after an intern hackers.

What Happened

Comodo detected and thwarted an intrusion into a reseller user account on 26-MAR-2011. The ne
controls implemented by Comodo following the incident on 15-MAR-2011 removed any risk of the
fraudulent issue of certificates. We believed the attack was from the same perpetrator as the inciden
on 15-MAR-2011

News-Meldung vom 05.11.2011 14:35

Zertifikatsausgabestopp nach Einbruch auf einer KPN-Server

Web credential authority rebu

Digicert Malaysia banished from Chrome,

By Dan Goodin in San Francisco · t more from hor

Posted in Enterprise 2011 21:46 GMT

ing Certificate Autl compromises and web br

Posted March 22nd, 2011 by ioerror in

How the Comodo certificate fraud calls CA trust into question

By Peter Bright | Published 10 months ago

Revoking Trust in DigiCert Sdn. Bhd Intermediate Certificate Authority

11.03.11 - 10:56am

Why do commercial CAs fail?

- Only basic verification of subscriber
- Certificates without any verification possible
- Reselling of CA-Services
  - Lack of control over the Intermediate CAs
  - Policies are not enforced over the trust chain
- Usage of weak keys is unknown to the public
- Server intrusion is not communicated

Browsers still trust these CAs!

Lessons Learned?

What need to be done:

- Open Policies & open Governance
- Transparent Processes
- IT Security and Data Protection
- Exact Identity Check

There is one open and free CA that lives this:

CAcert

How about CAcert?

CAcert protects its RA by

- Identification following policies
- Identification checked by at least 2 assurers
- arbitration

Registration Authority

CAcert protects its CA by

- Two-Men rule
- Open Source with code reviews
- Audit log of certificate creation

Certificate Authority

The Main Question

? ?

When does CAcert gets into the browsers?

? ? ?

Questions & Answers

Your Questions, Please!

Thank You For Your Attention!

Visit us at https://cacert.org

Contact me:

Alexander Bahlo

alex@cacert.org