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

Root CA

Sub CA I

Alice

Bob

Sub CA II

Carl

Doris

Ed
Trust anchor 2/2

Cross-Certified CAs

Root CA

Sub CA I
- Alice
- Bob
- Carl
- Doris

Sub CA I
- Alice
- Bob
- Carl
- Doris

Fox CA

Sub CA I
- Ed
- Flo
- Gron
- Horst

Sub CA I
- Ed
- Flo
- Gron
- Horst

Bridged CAs

Bridge CA

Root CA

Sub CA I
- Alice
- Bob
- Carl
- Doris

Sub CA I
- Alice
- Bob
- Carl
- Doris

Fox CA

Sub CA I
- Ed
- Flo
- Gron
- Horst

Sub CA I
- Ed
- Flo
- Gron
- Horst
What happened in 2011

Security of Dutch government jeopardy
Published on 3 September 2011 - 12:33am

Web credential authority rebuilt
Digicert Malaysia banished from Chrome

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 Logo](image-url)
How about CAcert?

CAcert protects its RA by
- Identification following policies
- Identification checked by at least 2 assurers
- arbitration

CAcert protects its CA by
- Two-Men rule
- Open Source with code reviews
- Audit log of certificate creation
The Main Question

When does CAcert get 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