PKI is dead, long live our PKI

Why we still decided to do a real life implementation of PKI and how we did it…

SCHUBERG PHILIS

Image: Interrobang, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from stewf's photostream

What is in this talk?

- Why?
- What?
- How?
- Some of our mistakes…
- Why PKI as we know it sucks!

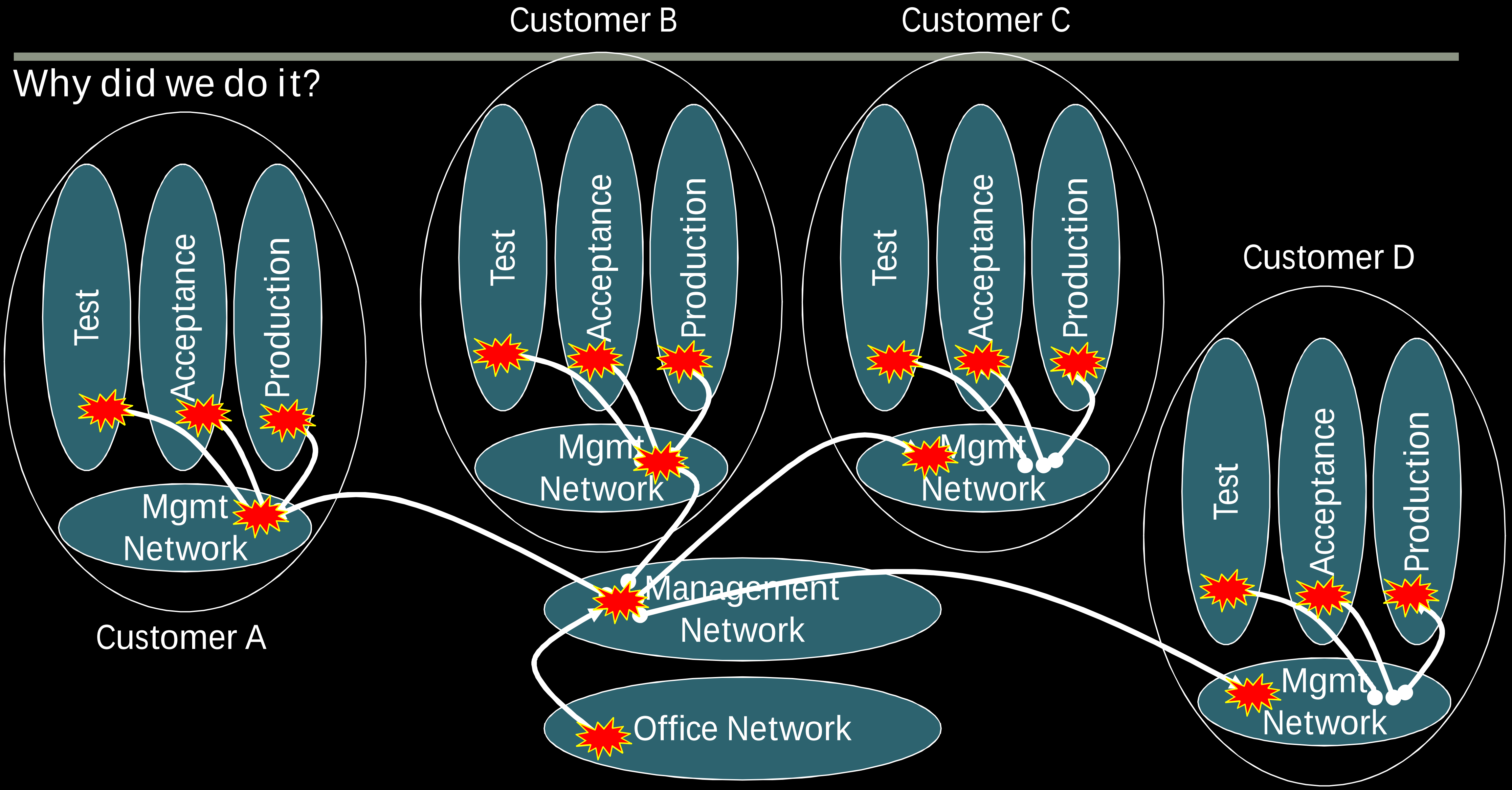
Who am I?

Frank Breedijk

- Security Engineer at Schuberg Philis
- Author of Seccubus
- Blogging for CupFighter.net

Email:	fbreedijk@schubergphilis.com
Twitter:	@seccubus
Blog:	http://www.cupfighter.net
Project:	http://www.seccubus.com
Company:	http://www.schubergphilis.com

Why did we do it?



SCHUBERG PHILIS

Image: And you'll ask yourself, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from silent7seven's photostream

Confusion

Image: Close-up of Voter Card (back), a Creative Commons Attribution (2.0) image from joebeone's photostream

SmartCard authentication

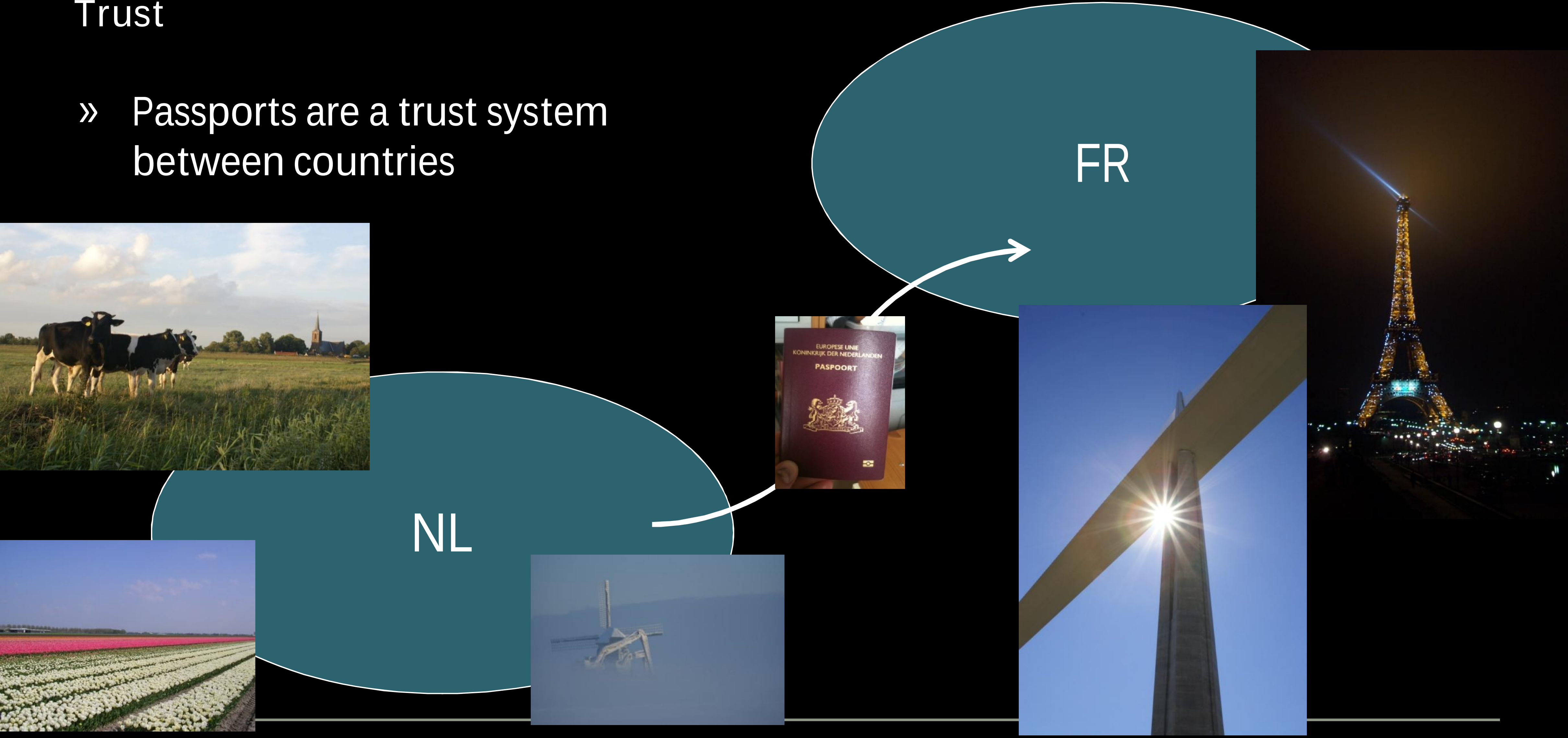
- One smartcard per user
- One PIN to remember

- Can be forwarded across RDP
- Can be used for cross domain authentication
- No need to have domain controller connectivity

Images by Frank Breedijk

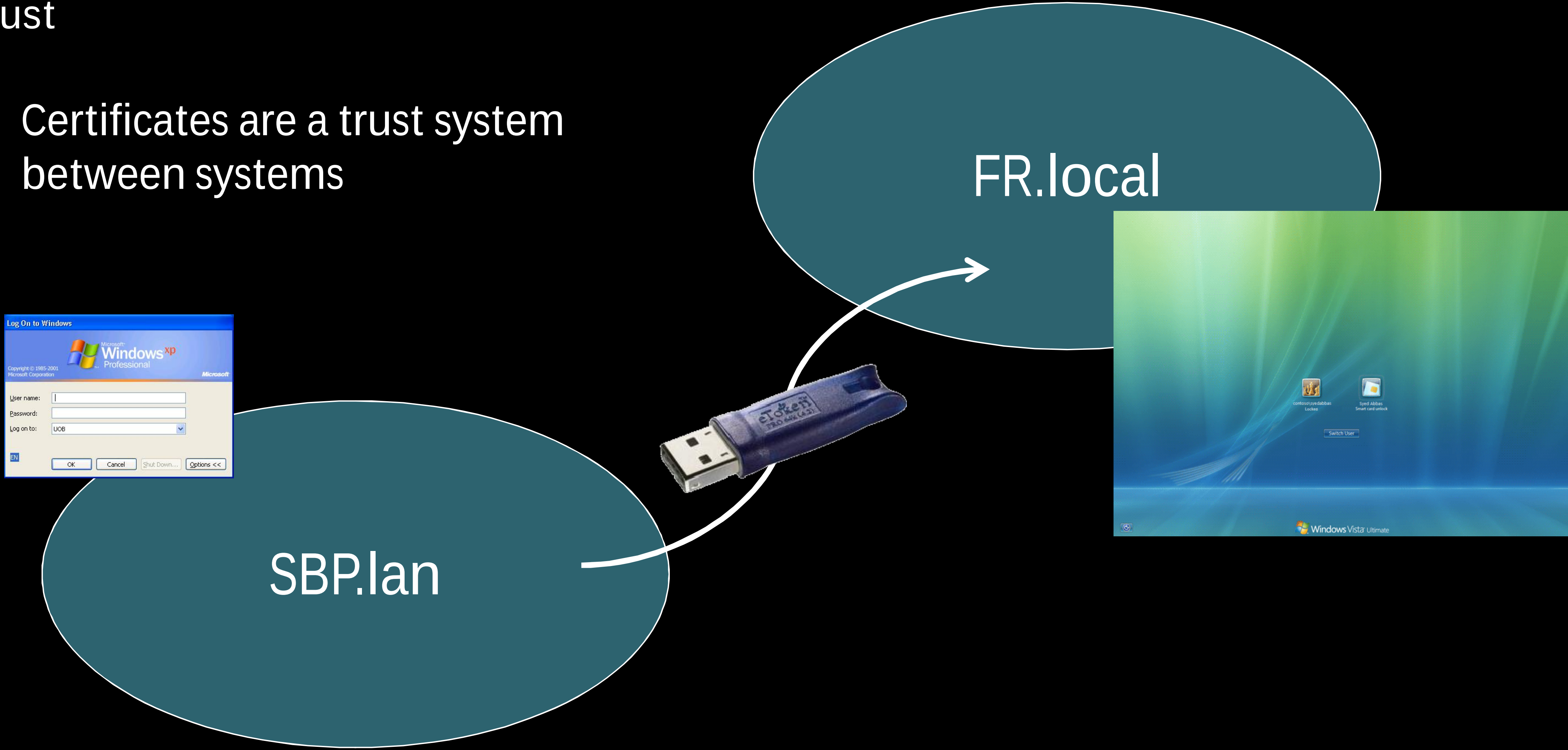
Trust

- Passports are a trust system between countries



Trust

- » Certificates are a trust system between systems



Log On to Windows

Microsoft Windows xp Professional

Copyright © 1985-2001 Microsoft Corporation

Microsoft

User name:

Password:

Log on to: UOB

EN

OK | Cancel | Shut Down... | Options <<

contoso\syedabbas
Locked

Syed Abbas
Smart card unlock

Switch User

Windows Vista Ultimate

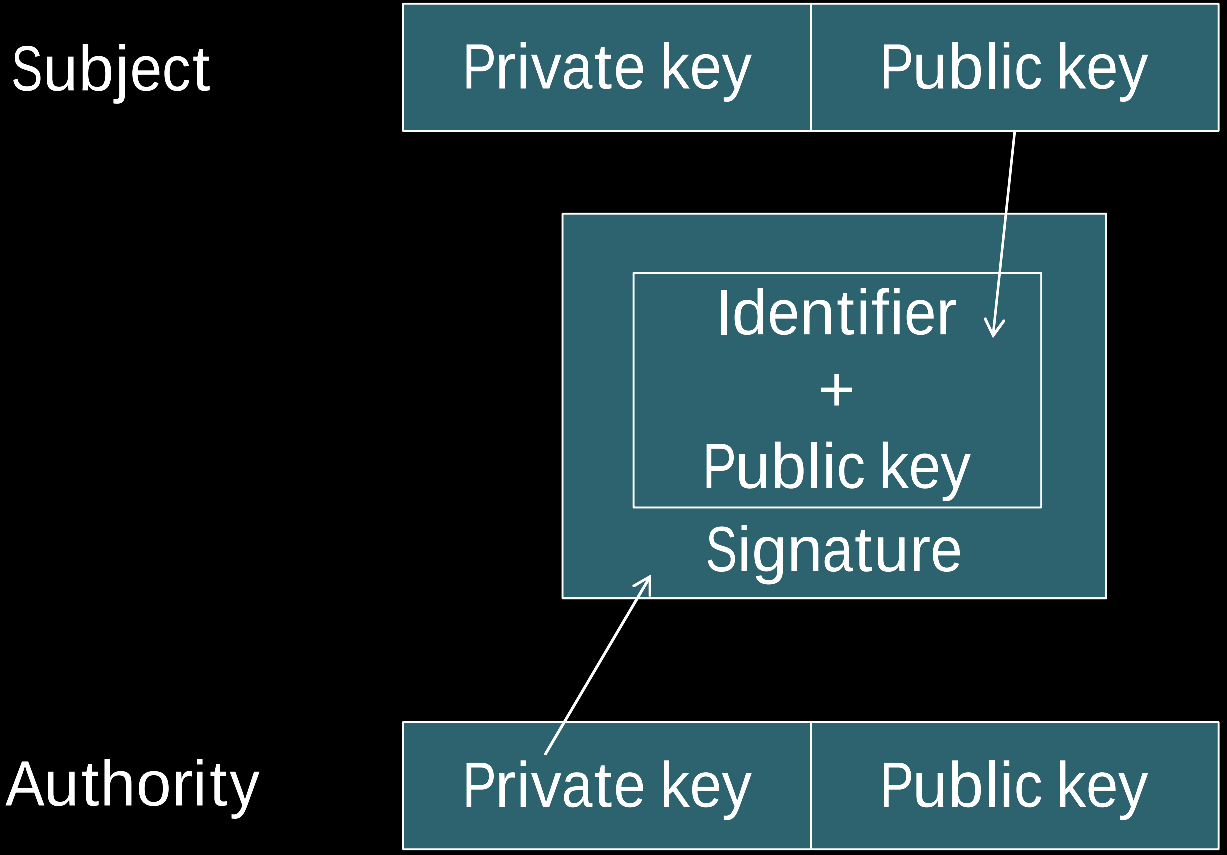
Image: Day 303: My Identity, a Creative Commons Attribution Non-Commercial (2.0) image from 56695083@N00's photostream

PKI is about identity…

- It's about who you are..
- NOT about authorization

Image: seven, a Creative Commons Attribution Share-Alike (2.0) image from genista's photostream

What is a certificate?



Subject

Private key | Public key

Identifier
+
Public key

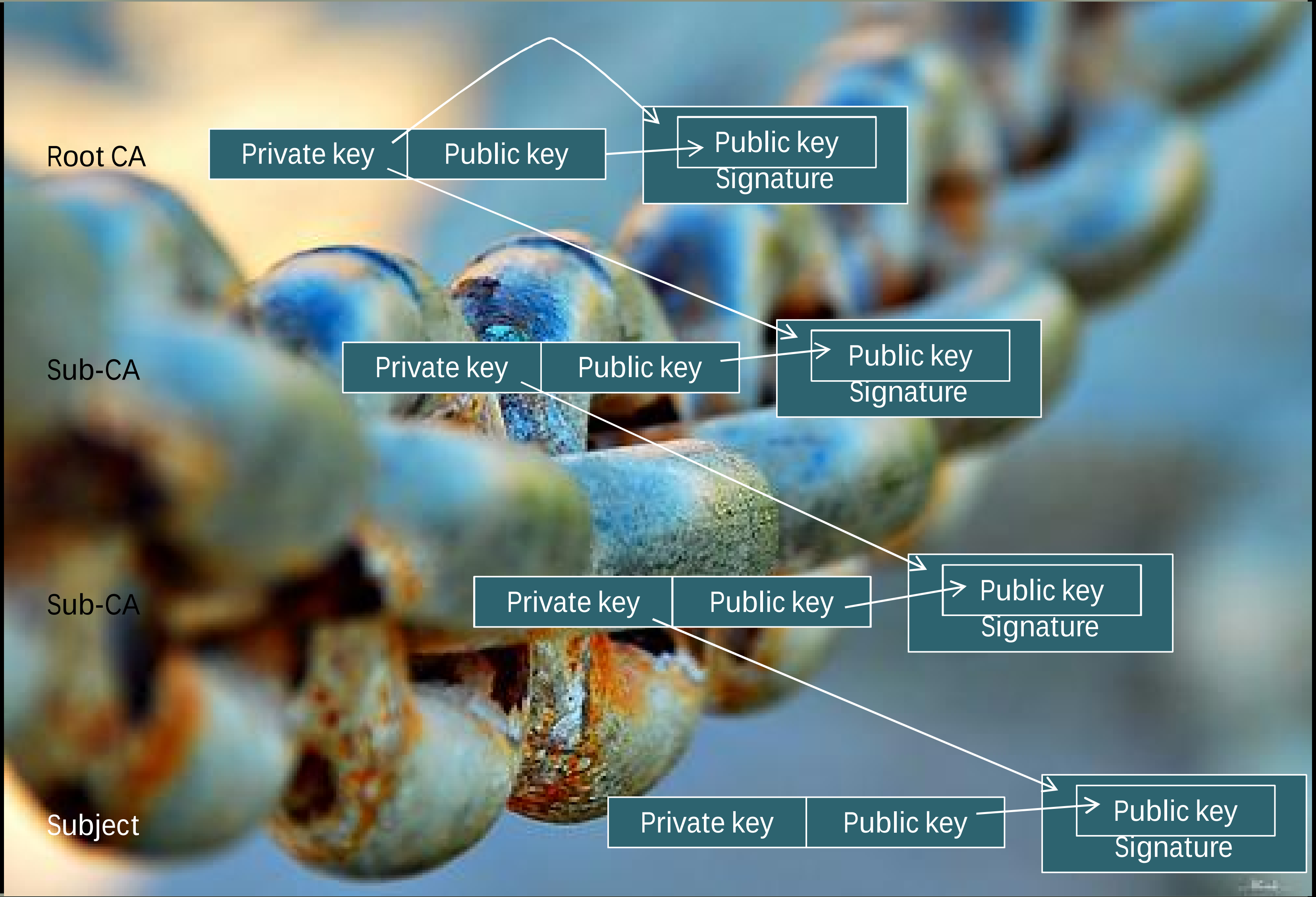
Signature

Authority

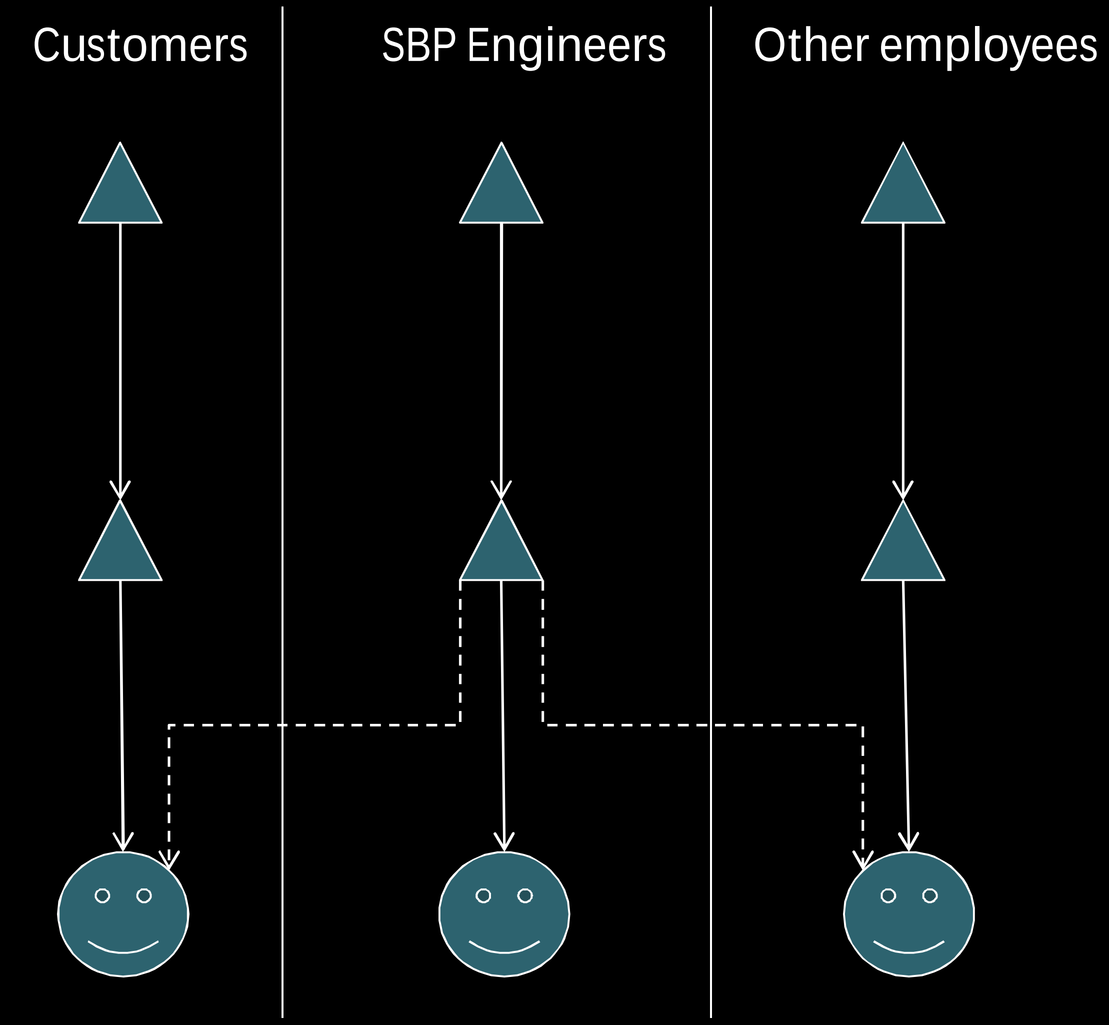
Private key | Public key

Image: Don't Chain Me Down, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from intherough's photostream

Chain



Our original idea



Wrong!

Identity

vs

Authentication

Image by Frank Breedijk

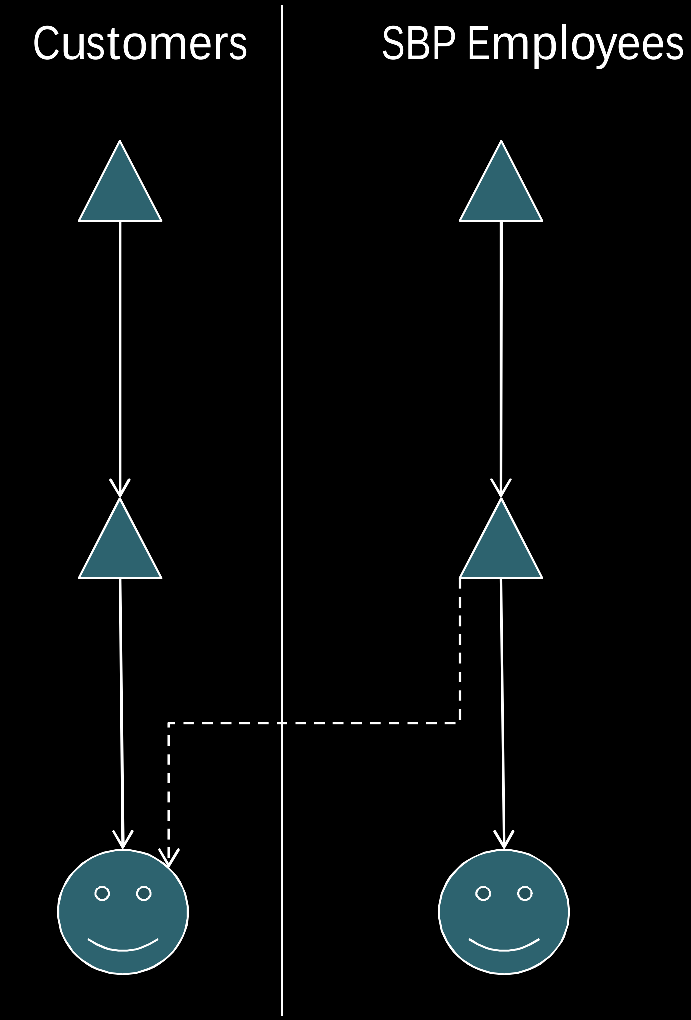
All users are equal…

All users are identified in the same way

SCHUBERG PHILIS

Image: Gene Simmons, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from iceman75's photostream

Revised idea



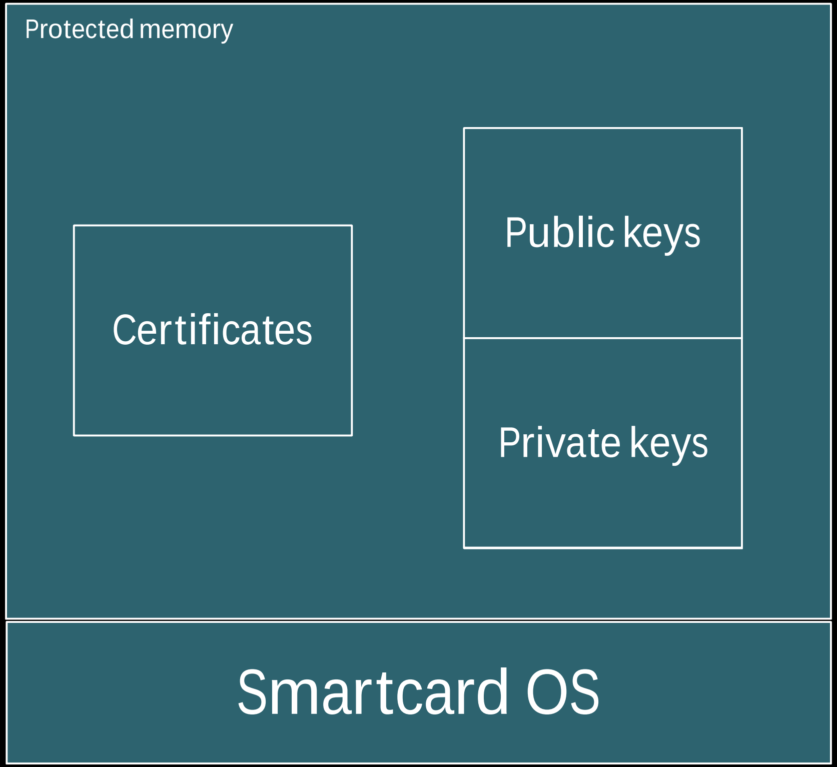
Keep it Simple, Stupid

Protection of keys

Image: Late Check-Out, a Creative Commons Attribution Non-Commercial (2.0) image from telstar's photostream

Image: Close-up of Voter Card (back), a Creative Commons Attribution (2.0) image from joebeone's photostream

Smartcards



Protected memory

Certificates

Public keys

Private keys

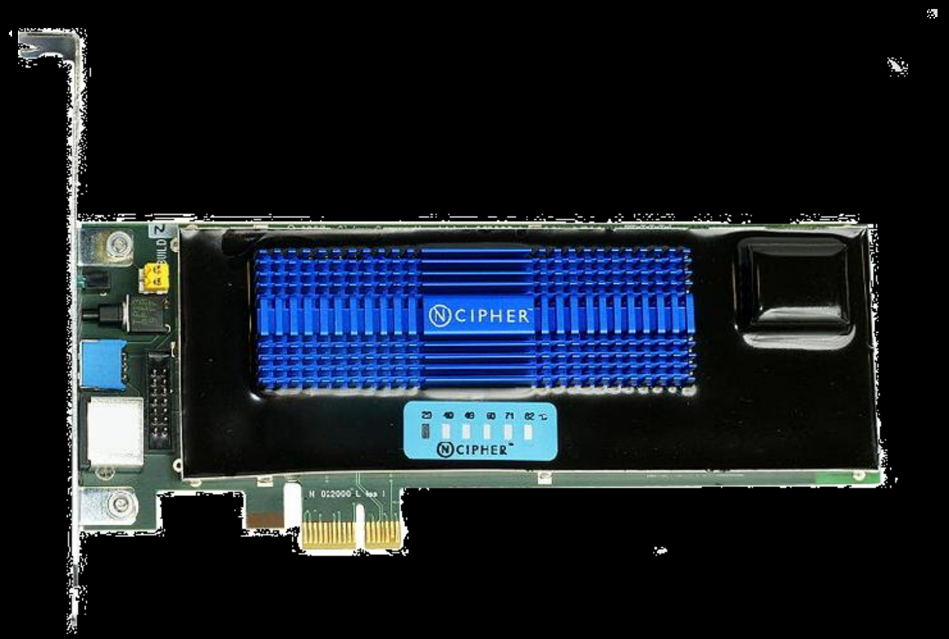
Smartcard OS

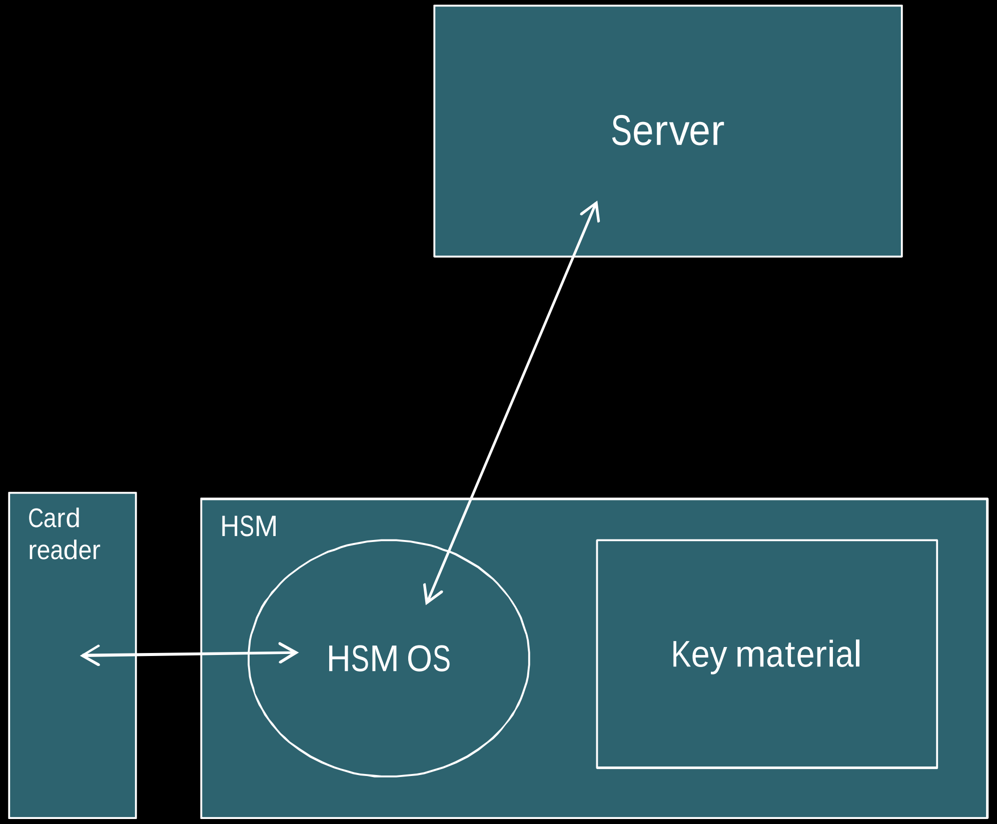
- Smart Cards protect key material
- Material can only be used after authentication
- Private keys cannot be read/copied
- For users

Image: NCipher nShield F3 Hardware Security Module, a Creative Commons Attribution (3.0) Unported Imagefrom WikiPedia

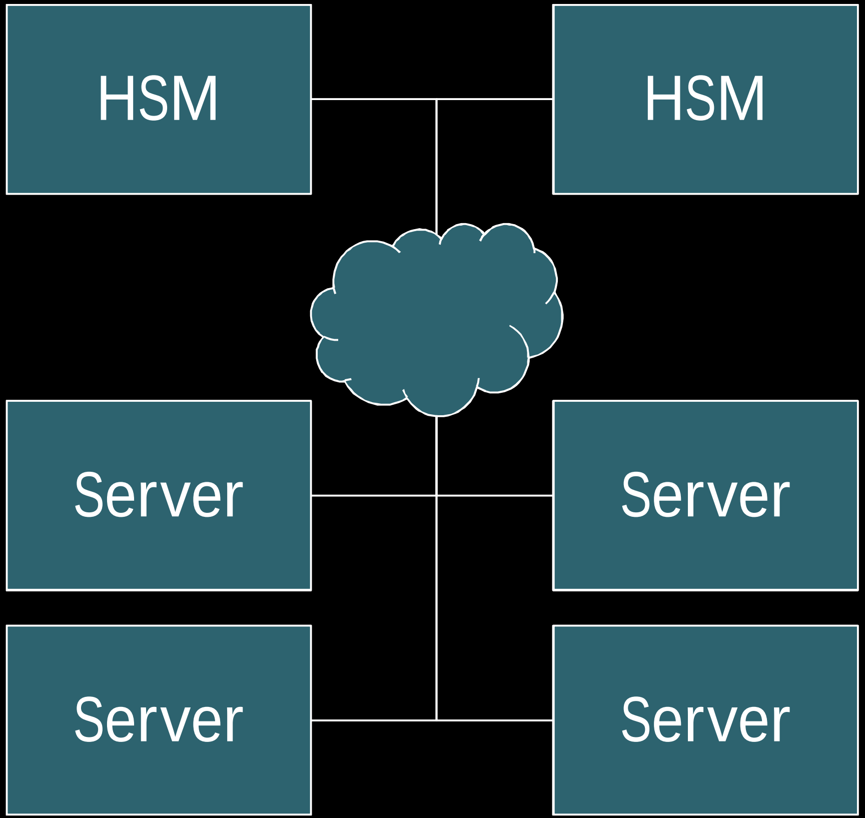
Hardware Security Modules

- Smart Cards for servers
- Authentication often based on Smart Cards





Networked vs non-networked



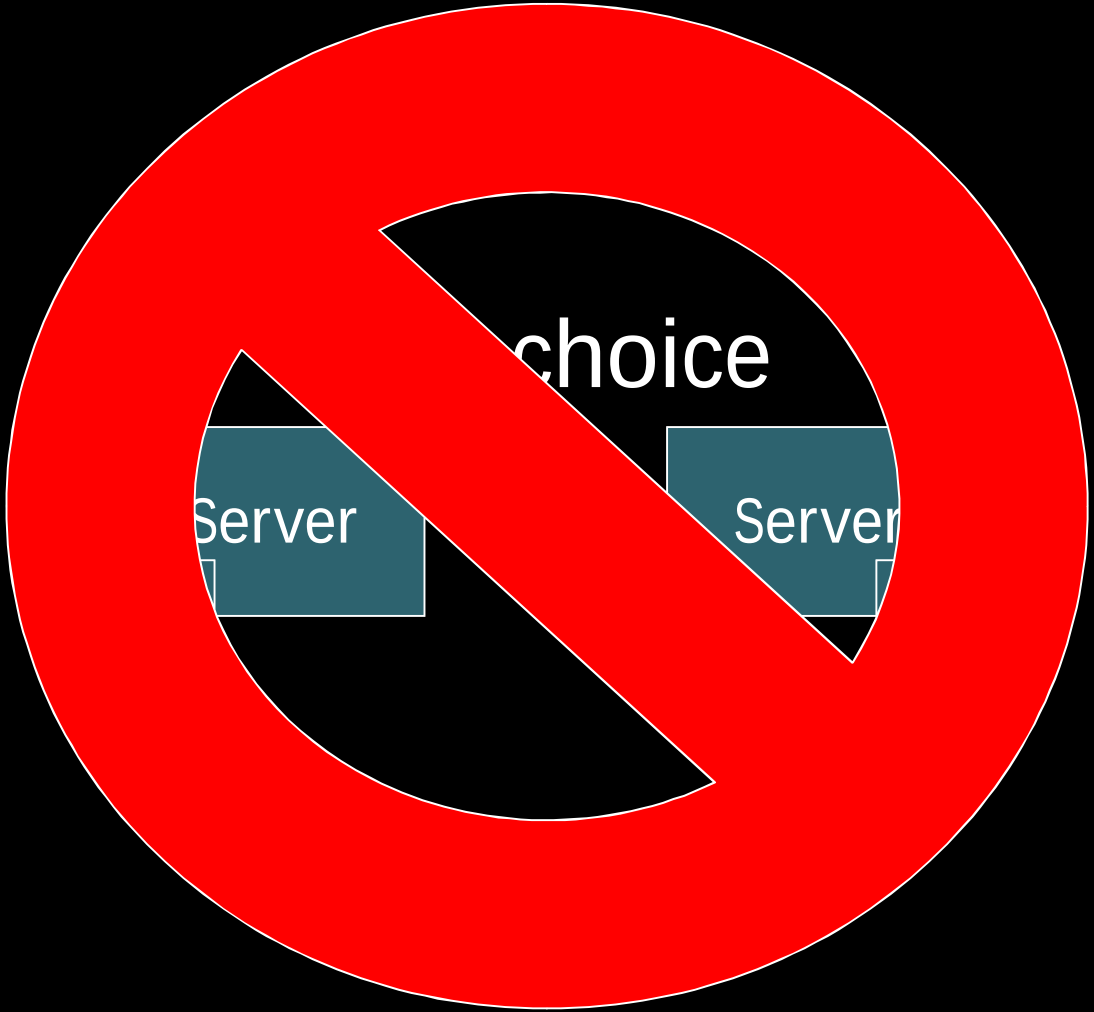


Image: Dollars !, a Creative Commons Attribution No-Derivative-Works (2.0) image from pfala's photostream

Why was this a bad choice?

- There is virtually no redundancy in CAs
- There is no active/active CA setup
- Virtualization is your friend
  - How do you insert a card in a VM?

- How did we do failover?
  - Poor mans failover: SAN boot

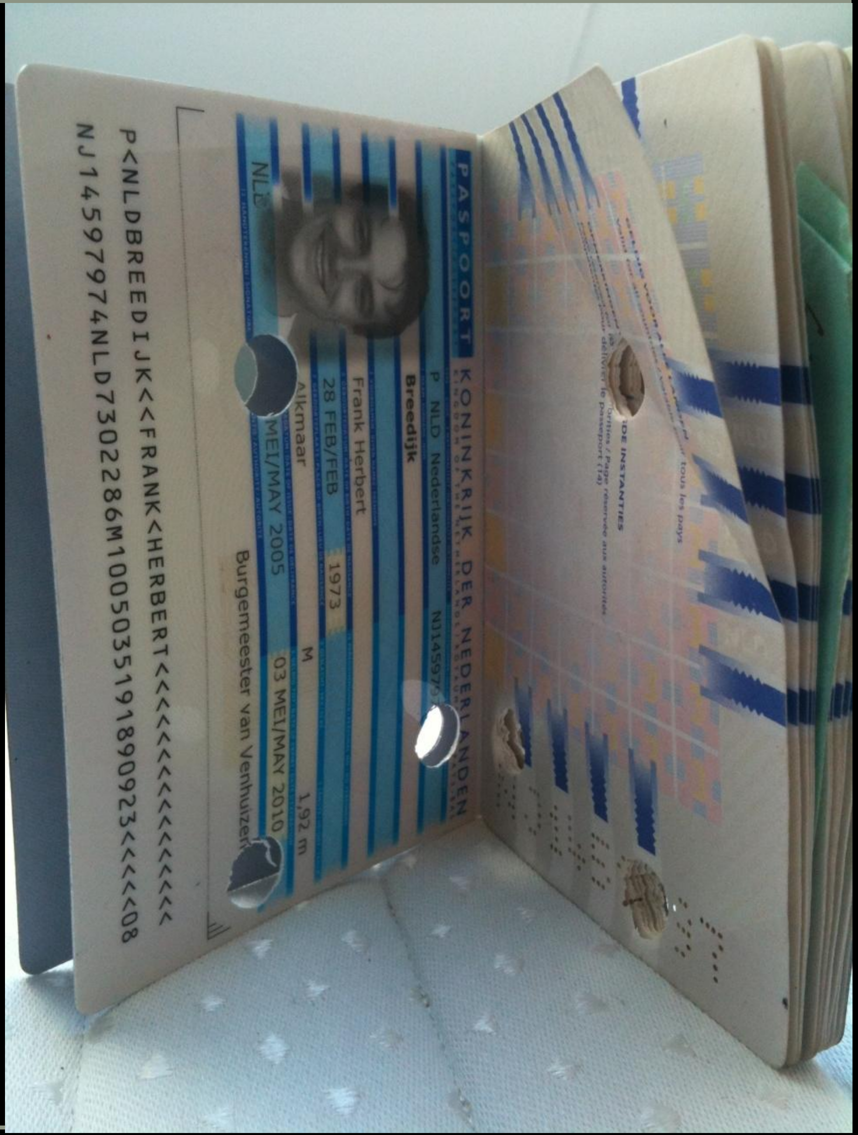
- Do you allways need a HSM?
  - Offline CA - Virtual machine on encrypted hard disk

Image by Frank Breedijk

Certificate revocation

- Invalidating a certificate

- Leavers
- Lost tokens
- Key compromises

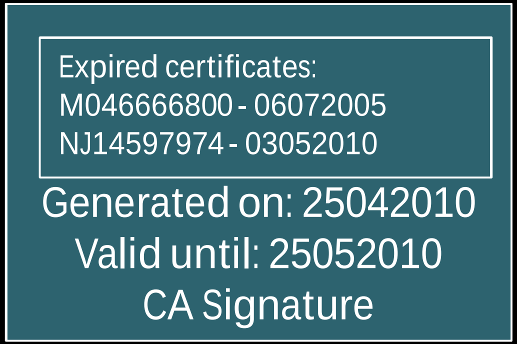


Certificate revocation list

- » List of certificates that has been revoked signed by the CA
- » You can only revoke certificates in your certificate database
- » If the revocation list is unavailable authentication should fail

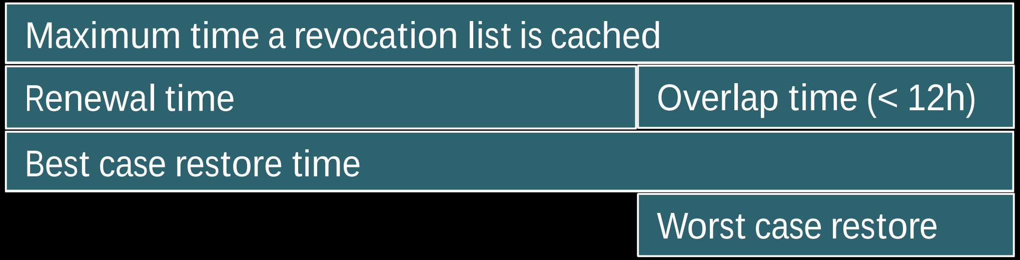
- » Where to publish?
  - » AD
  - » Public website

- » How often to refresh?



Expired certificates:
M046666800 - 06072005
NJ14597974 - 03052010

Generated on: 25042010
Valid until: 25052010
CA Signature



Maximum time a revocation list is cached

Renewal time | Overlap time (< 12h)

Best case restore time

Worst case restore

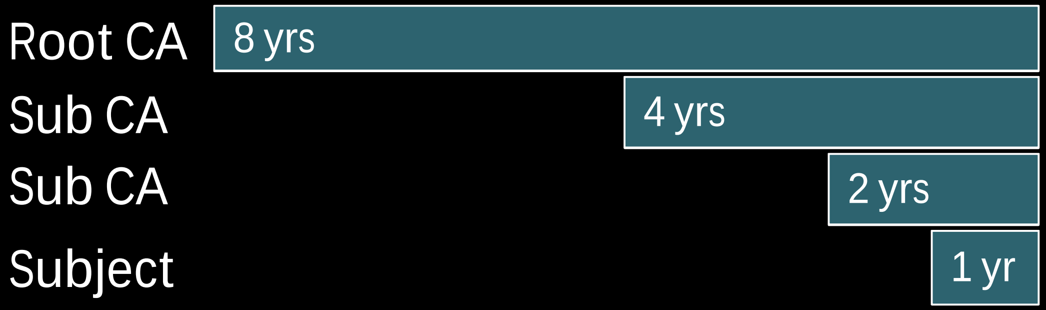
Remember:

- » Authentication
- » Not authorization!

Image: Yes! It's My Birthday! And It's My Footprint :D, a Creative Commons Attribution (2.0) image from hamed's photostream

Certificate lifetime

- Certificates have a natural lifetime
- Special consideration should be given to CA certificates



Root CA 8 yrs

Sub CA 4 yrs

Sub CA 2 yrs

Subject 1 yr

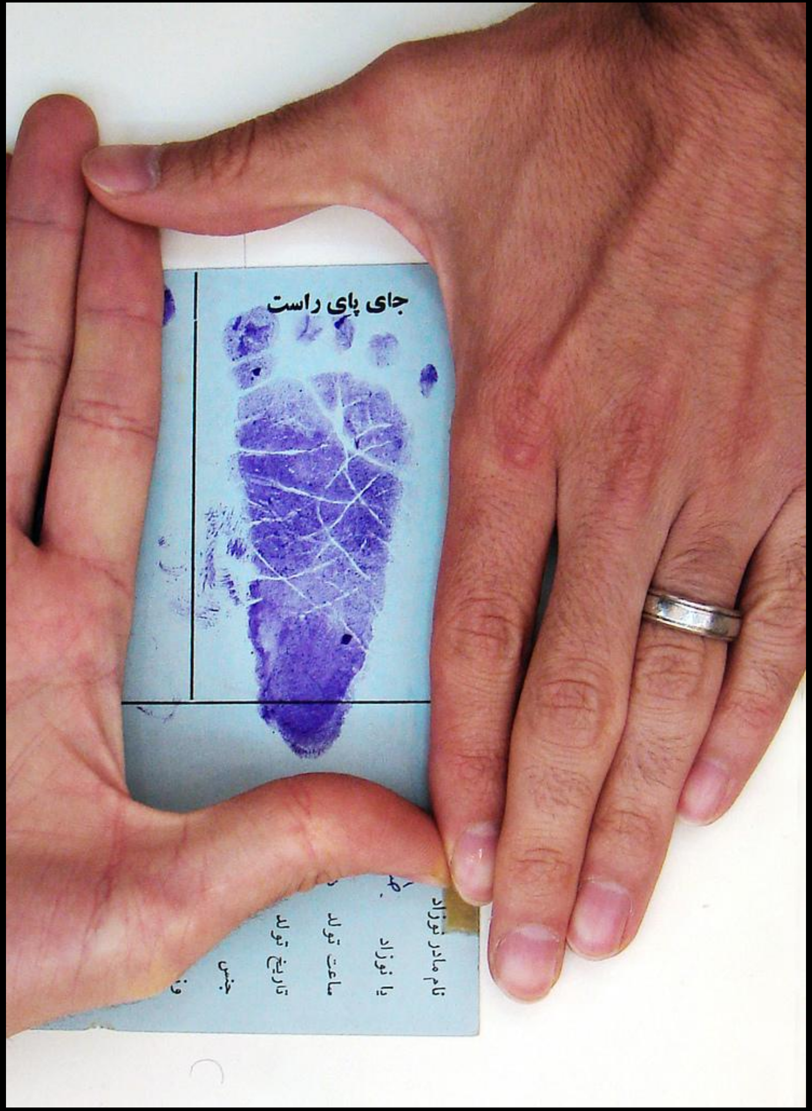


Image: Off-site backup for Dallas companies, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from alexmuse's photostream

Backup and Restore

- Be prepared to build a prototype first
- Your prototype will fail
- Important things to backup:
  - Certificate DB
  - Key Material
  - Settings
- Important tools:
  - CertUtil
  - You HSM backup tools
  - Regedit

RTFM isn’t allways good…

At some point our AD registrations got “funny”…

- We decided to reinstall the the CA, since we did have a backup
- Reinstalled the machine
- Reused the certificate
- Restored the Registry

AD registration did not correct itself

Three setup states

SetupState 1

- Initial setup

SetupState 2

- This is where AD registration happens

SetupState 3

- Setup is done

At the end of SetupState 1 you import the registry which sets the setup state to 3

Image: 198/365 It's fair weather a Creative Commons Attribution No-Derivative-Works (2.0) image from gibsonselectric's photostream

Managing certificates

http://localhost/certsvr

» Only practical for small amount of users

Microsoft Certificate Lifecyle Management

» Better for more users
» Allows self service
» Reasonable straight forward
» You have to ‘program’ your tokens yourself

Aladdin Token Management System

» Better for more users
» Allows self service
» Reasonable straight forward
» ‘Programs’ Aladdin tokens for you

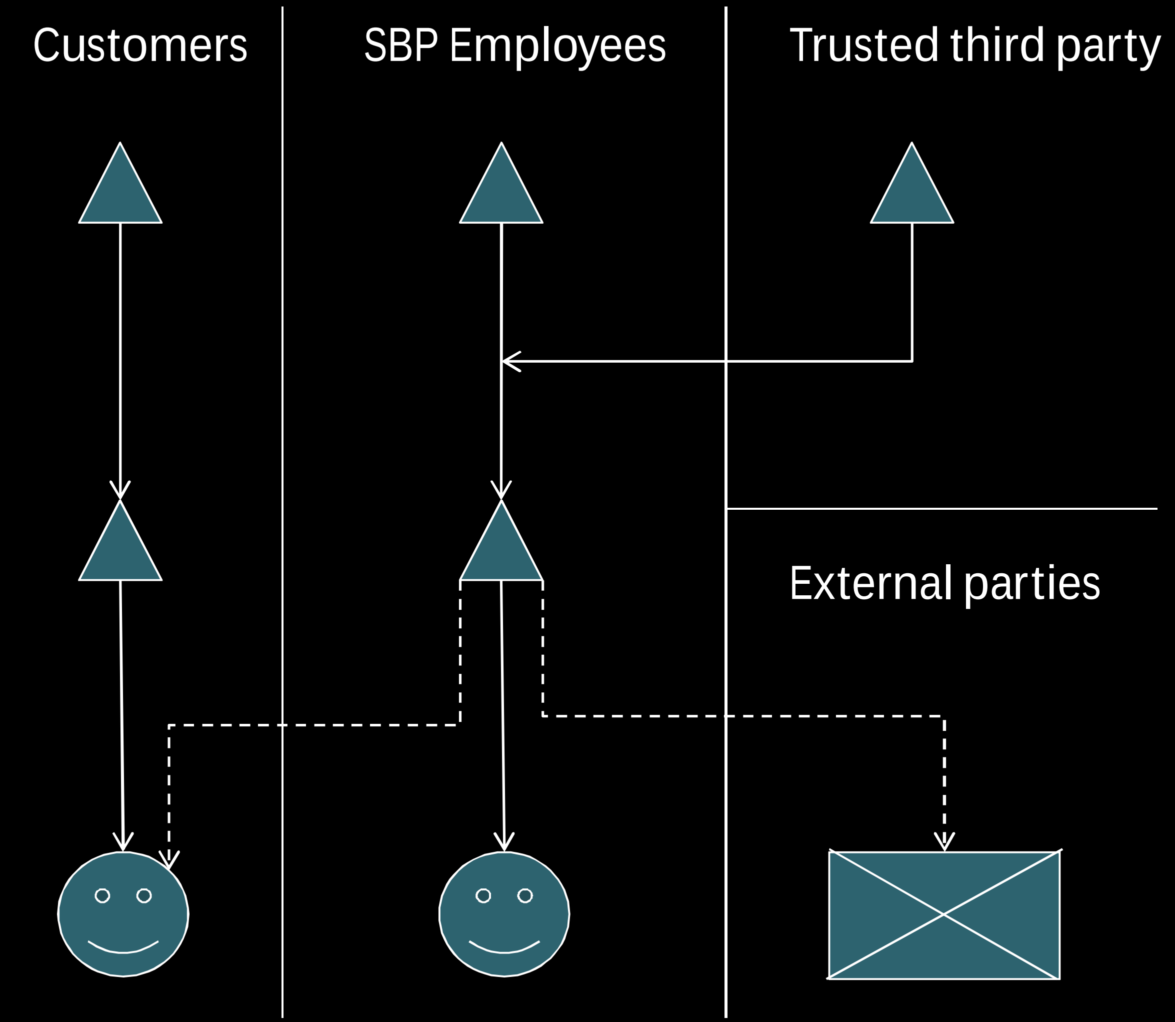
Image: Just one from all the gems, a Creative Commons Attribution (2.0) image from unclassified's photostream

External trust

Because we do not all live on the same island

Image: Landing, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from andrewpescod's photostream

The original idea



Forget it!

It's a wild goose chase

Image: the weakest link, a Creative Commons Attribution Non-Commercial (2.0) image from darwinbell's photostream

It is theoretically possible

- Send your initial CSR to two CAs
- Both CAs will create a certificate for you
- You can only install one of them

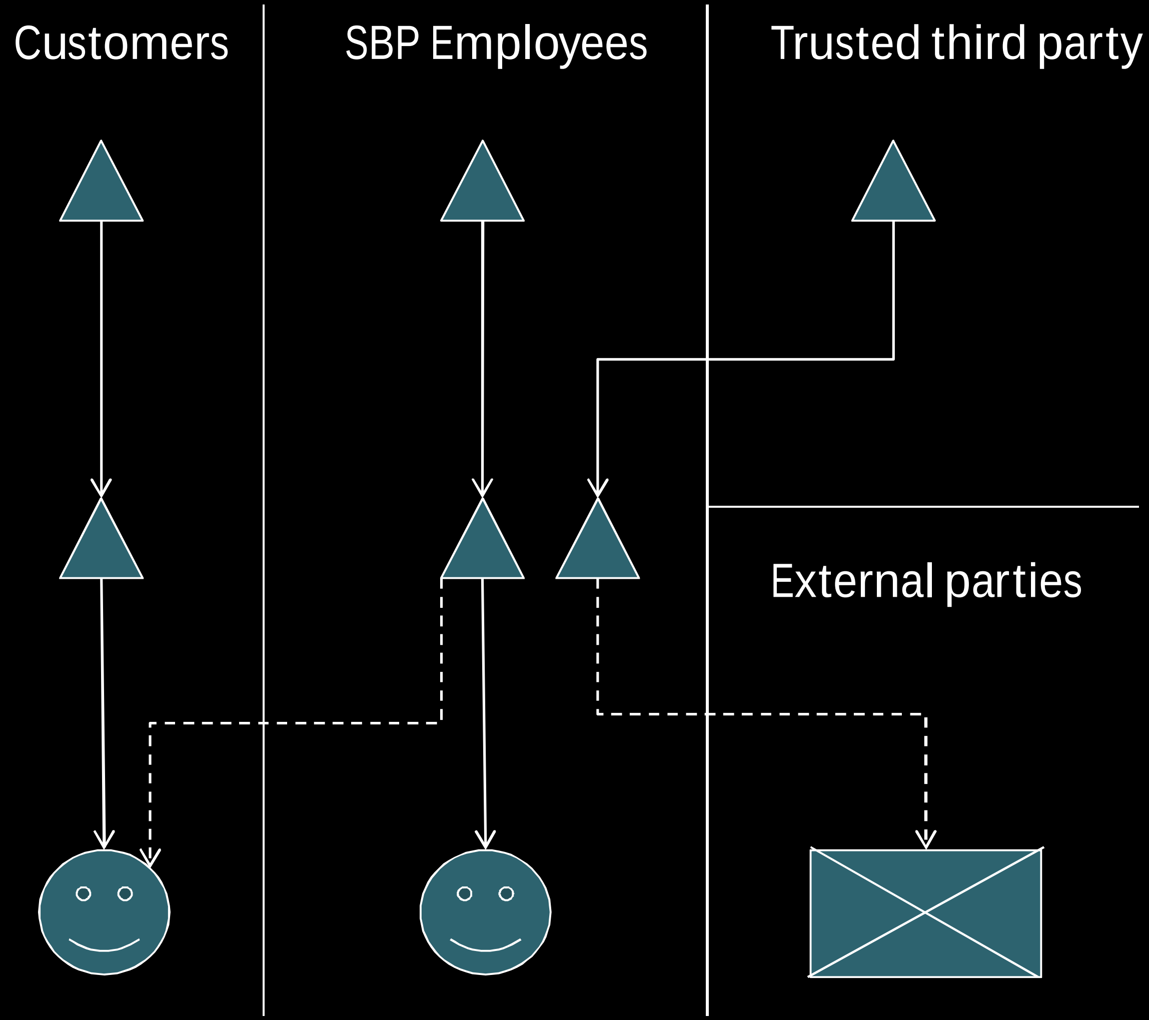
If you use your own root CA

- Outlook will always select the wrong chain for external validation

If you use the External Root CA

- SmartCards will be provisioned with the wrong chain

How it turned out



- An additional sub-CA was needed
- Trusted Third Parties will require a HSM
- This also allows for policy differences between email and login certificates

Image: Yes, a Creative Commons Attribution Non-Commercial (2.0) image from diebmx's photostream

Does it work?

Yes it does…

Image: = // =, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from antphotos's photostream

It’s not a perfect system

Image: All mine :), a Creative Commons Attribution (2.0)
image from 16048742@N08's photostream

Too many CAs

My firefox:

- 216 Certificate Authorities

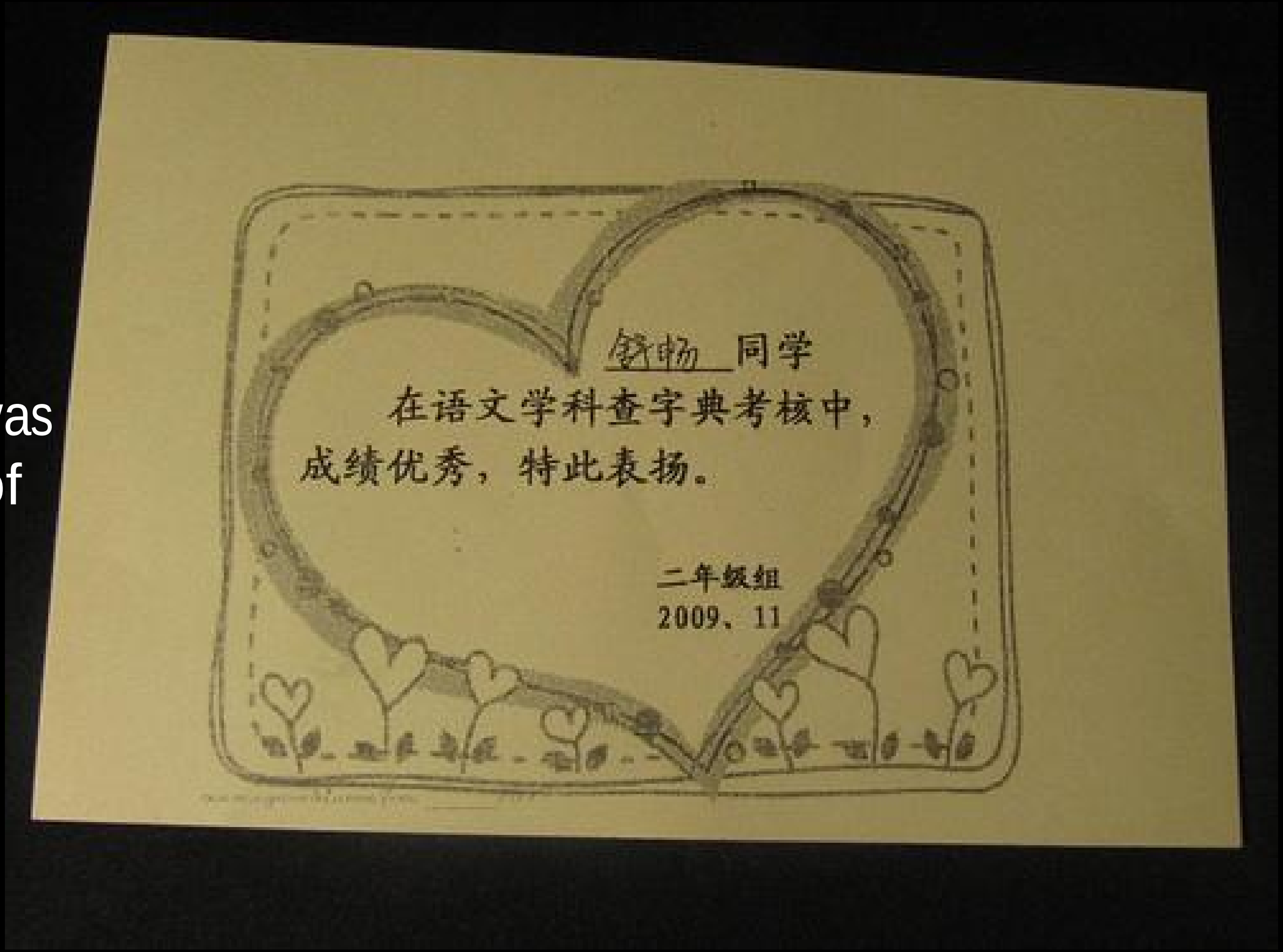
Microsoft Root CA program (2009):

- 104 organizations
- 285 Certificate Authorities
- Excluding intermediates

Image: Chinese School Certificates, a Creative Commons
Attribution (2.0) image from ivanwalsh's photostream

Any CA can certify anything…

Would you still trust your bank if it was registered with a Chinese chamber of commerce?



舒畅 同学

在语文学科查字典考核中，

成绩优秀，特此表扬。

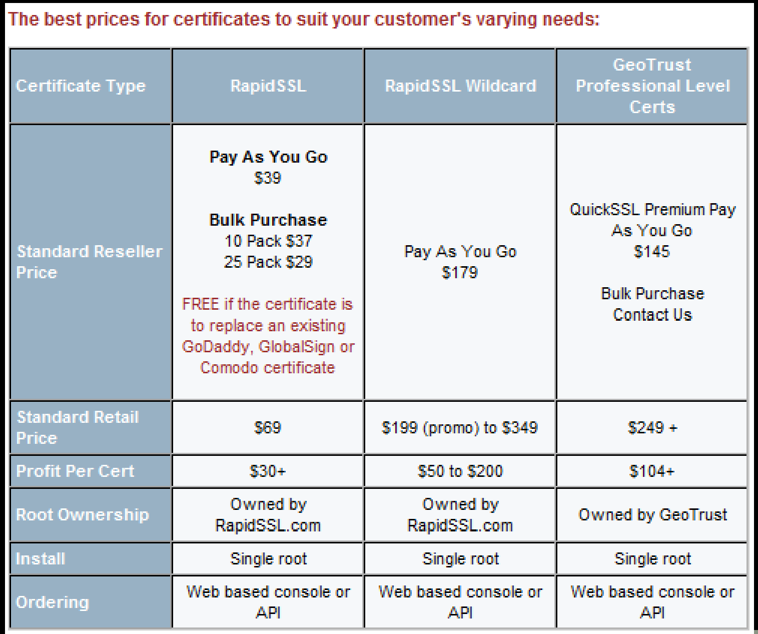
二年级组

2009、11

Image: Credit Crunch, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from bitzcelt's photostream

CAs are commercial organisations…

- A sold certificate means revenue
- Time spent on validation is overhead
- Becoming a reseller is easy
- Certificates only cost about $40



The best prices for certificates to suit your customer's varying needs:

Certificate Type	RapidSSL	RapidSSL Wildcard	GeoTrust Professional Level Certs
Standard Reseller Price	**Pay As You Go** $39 **Bulk Purchase** 10 Pack $37 25 Pack $29 FREE if the certificate is to replace an existing GoDaddy, GlobalSign or Comodo certificate	Pay As You Go $179	QuickSSL Premium Pay As You Go $145 Bulk Purchase Contact Us
Standard Retail Price	$69	$199 (promo) to $349	$249 +
Profit Per Cert	$30+	$50 to $200	$104+
Root Ownership	Owned by RapidSSL.com	Owned by RapidSSL.com	Owned by GeoTrust
Install	Single root	Single root	Single root
Ordering	Web based console or API	Web based console or API	Web based console or API

Many CA attacks in the past

Moxie Marlinspike

- Using a subject certificate as CA certificate
- SSL strip
- Null byte terminated wildcard certificate

Dan Kaminsky

- Null byte terminated wildcard certificate
- MD2 and MD5 certificates

Mike Zusman

- Attack against CA web application

Marsh Ray & Steven Dispensia

- TLS Renegotiation gap

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik and Benne de Weger

- MD5 collision to create a rogue CA certificate

Image: tofu man, a Creative Commons Attribution Non-Commercial Share-Alike (2.0) image from arimoore's photostream

Possible solutions…

- DNS Sec
- IPv6
- Trust On First Use (TOFU)
- Perspectives

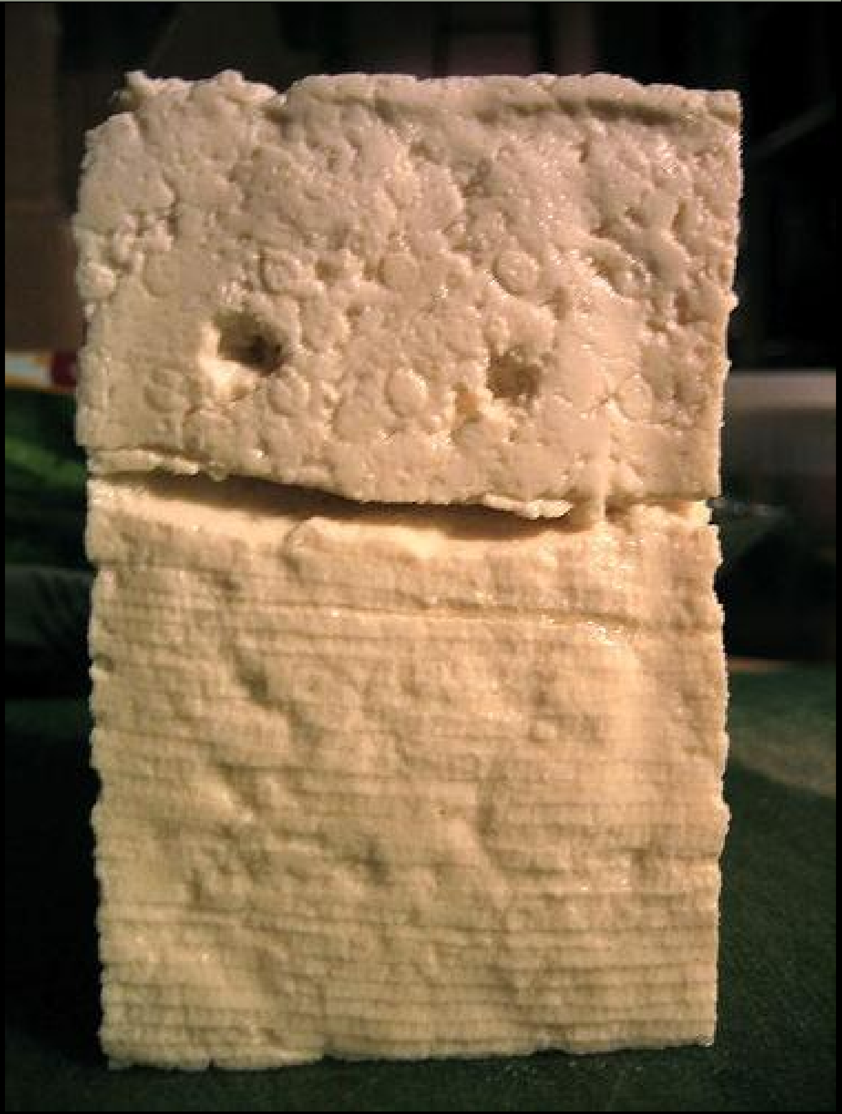


Image by Frank Breedijk

Conclusion

You too can build a PKI

- » The devil is in the details
- » There are plenty of details

PKI as we know it from SSL

- » The system has become too big and too commercial
- » Can it still be trusted?
- » We need an alternative

Small PKI systems are still useful

Conclusion

The global PKI system is dead or maybe dying

But a purpose built PKI system is still worth the effort

?