THALES

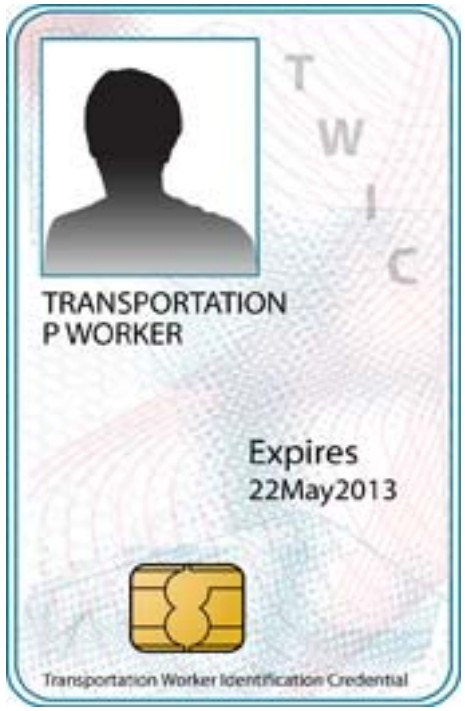
A Study of PKI Failures: Policies are Critical for Success

Brian Phelps
Head of Professional Services EMEA

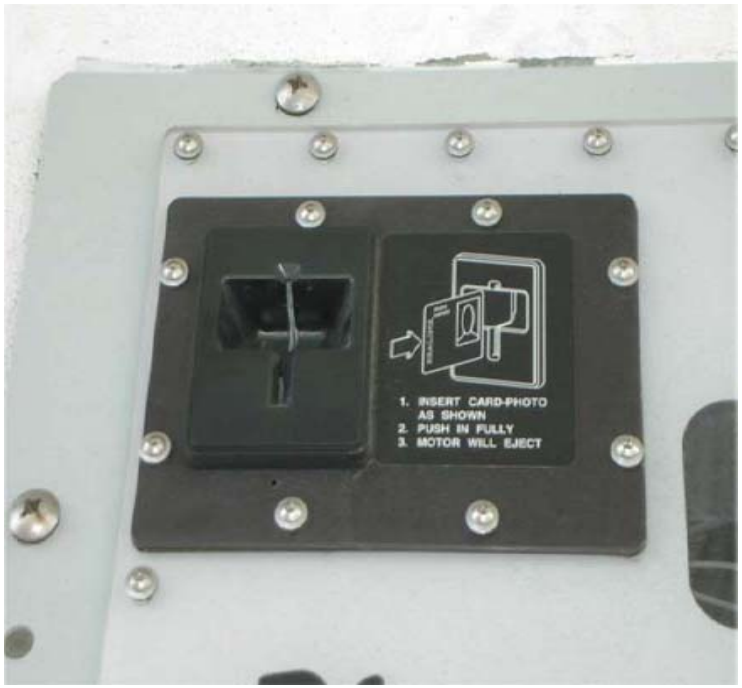
Case Study in PKI failure – US TWIC

Introducing the TWIC Card

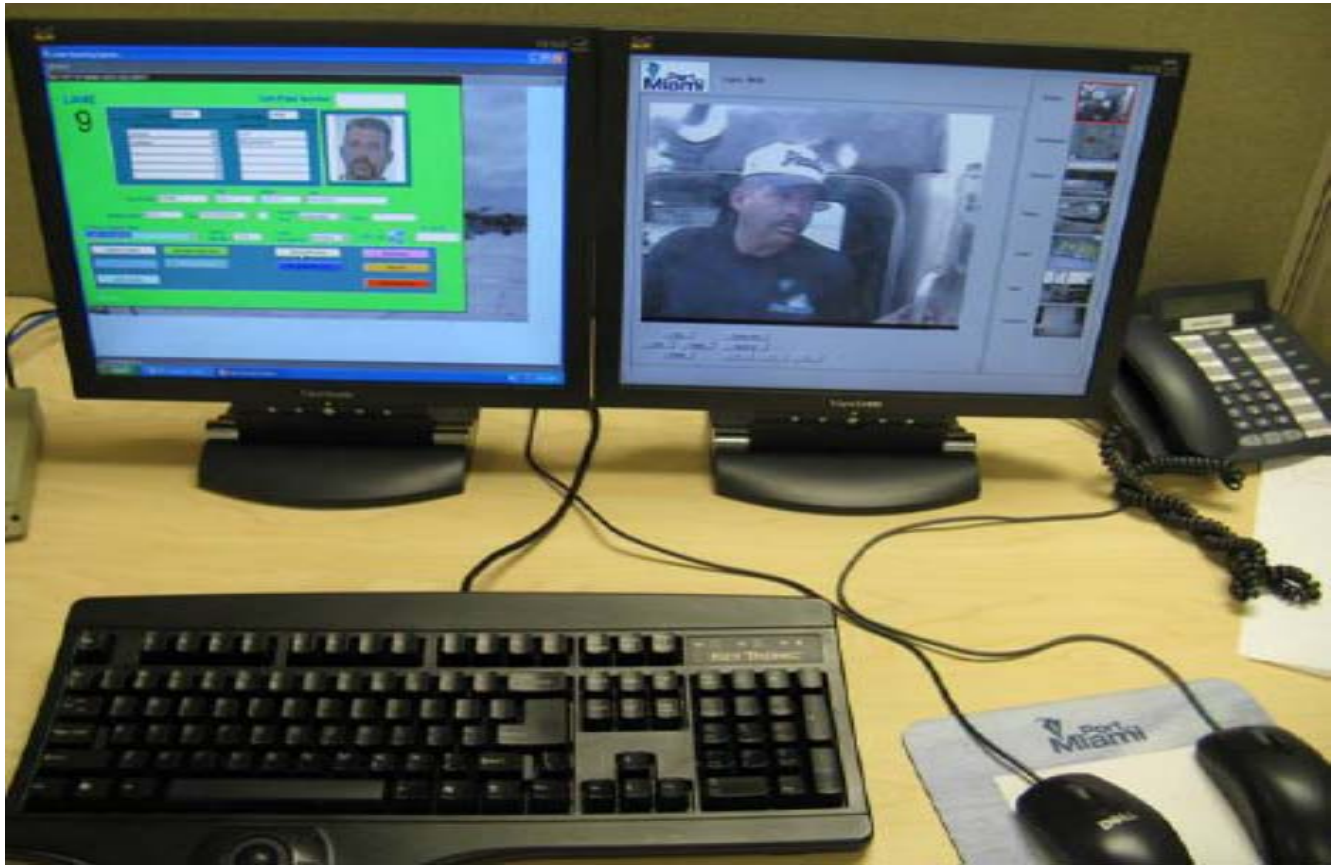
- TWIC – Transportation Worker Identification Credential
- Issued by the US Department of Homeland Security
- Mandated by act of Congress to improve security at USA ports, transportation hubs and other maritime locations
- More than 1.9 million workers including longshoremen, truckers, port employees and others have been required to obtain a TWIC.
- The card costs $132.50 – charged to the applicant, NOT the transport company.



TWIC In Action – Card Reading Station



TWIC In Action – Card Verification Station



TWIC Email – October 22, 2008

TWIC Stakeholders,

On October 21, the government facility that houses the TWIC system experienced a building-wide power outage. Though power was quickly restored, the part of the system that facilitates activations was affected. As we continue to work on resolving this issue, we must reschedule all activation appointments booked through Thursday, October 23; we will also be unable to accommodate activation walk-ins. Enrollment, pre-enrollment and status checks are still available services.

We will provide updates with more information as it becomes available to our Web site, www.tsa.gov/twic, as well as through our help desk,1-866-DHS-TWIC.

Thank you for your patience.

We will send all Stakeholders notification when the situation has been resolved.

The TWIC Outreach Team

TWIC Failure – October 21, 2008

Timeline of a PKI disaster

- Primary TWIC datacenter direct hit by lightning.
- Untested UPS in rack failed. System crashed.
- Untested backup generator started. Power spike throughout the datacenter.
- No failover, no cold standby – single point of failure.
- No DR site ready.
- No off-site backup of key material.
- Online Root PKI HSM destroyed. Root PKI key forever lost.

TWIC Failure – Fallout, Costs

What happened next . . .

- TWIC continued to work for access, as only "root CA" functions destroyed.
- 908,097 cards affected – all cards issued before October 21, 2008
- All 900K cards had to be replaced – at the US government's expense. Readers had a 6 month cert – a major effort to replace all cards in time.
- Congressional hearings launched into lack of a backup plan. Extensive press coverage.
- Estimated total cost: $300M

DigiNotar Certificate Authority Breach

Story of Preventable Failure

- On July 10th, 2011 DigiNotar network penetrated
- 300,000 rouge certificates issues for *.google.com, Skype, Facebook, and 527 other domains
- Enabled MITM attack on gmail users
- DigiNotar did not revoke the fake *.google.com certificate until July 29th, 10 days after discovery
- DigiNotar waited until mid-August before publically disclosing the hack

DigiNotar CA Fallout

Dutch Government hired FoxIT to investigate the breach – the final report entitled Black Tulip

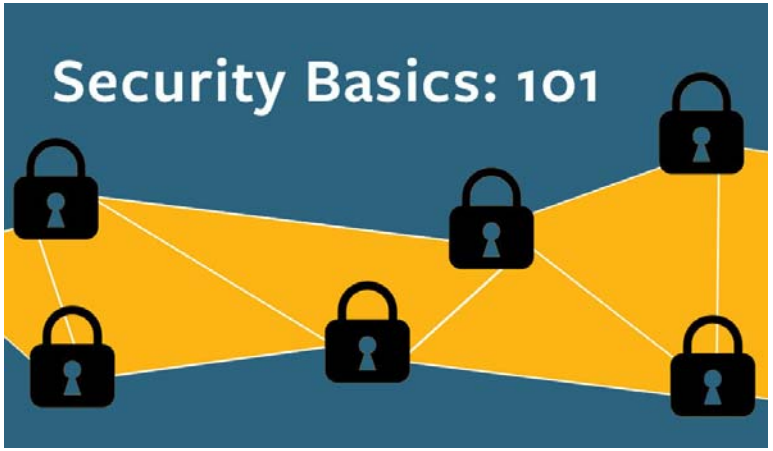
Failings identified read like a “worst case” set of IT security policies

- Out of date security patches
- Poorly segmented network with no SSL/TLS between internal servers
- No server side anti-virus, limited network monitoring tools
- Weak password policy – passwords susceptible to brute-force attack
- No cryptographically signed log files – attackers could hide their tracks

Result: DigiNotar exited CA business, later sold to Vasco

A quick word on ‘Security Basics’

- **‘Security basics’ form an ESSENTIAL underpinning for any PKI deployment**
- **A failure to implement ‘security basics’ could cause any PKI deployment to fail, OFTEN SPECTACULARLY**
- **Things we are talking about – e.g.:**
  - Strong passwords
  - Segregation of duty/”2 person control”
  - Access control/use “principle of least privilege”
  - Patch management
  - Physical Security (e.g. Root CA isolation)
  - Consistent, repeatable processes
- **This is NOT an exhaustive list!**



Good practice & lessons learned – requirements

- **Make sure the project has specified and signed off all requirements up front**
- **To help here, run at least one 'requirement gathering' workshop**
  - Invite all the stakeholders
  - What is the business need for PKI?
  - Note down all requirements & link back to the business need
  - Separate requirements into functional/non-functional
  - Requirements should be written in a clear and un-equivocal manner (i.e. not open to interpretation)
  - Ensure 'assumptions' and 'constraints' are noted
- **If the PKI will issue certificates to any system, application or service which will be used for legal purposes, ensure lawyers are involved**

Good practice & lessons learned – The three 'P's (1/2)

Experience suggests that a PKI is 40% politics, 40% policy & 20% technology

It's not a PKI unless you have the three 'P's – Policy, Processes & Procedures

- But, governance must be proportional to the value of the data/systems that the PKI is being used to protect.
- To determine proportionality, you need a risk assessment!

Certificate Policy should come first

- Use RFC 3647 as a guide (Section 6)
  - Plenty of commercial CA policies on the Internet BUT don't just copy!
- Get legal assistance if the PKI underpins legal activities
- An agreed policy provides justification for all design & implementation activities going forward (also helps if auditors need to be pacified!)
- Provides confidence in governance measures

Good practice & lessons learned – The three 'P's (2/2)

A 'process' is made up of 'procedures'

- All PKI operations should be documented
- Required processes and procedures will become apparent from the Certificate Policy. E.g.:
  - Certificate Issuance
  - Certificate Revocation
  - Physical Security Controls
  - Disaster Recovery
- Don't forget HSM processes/procedures too!

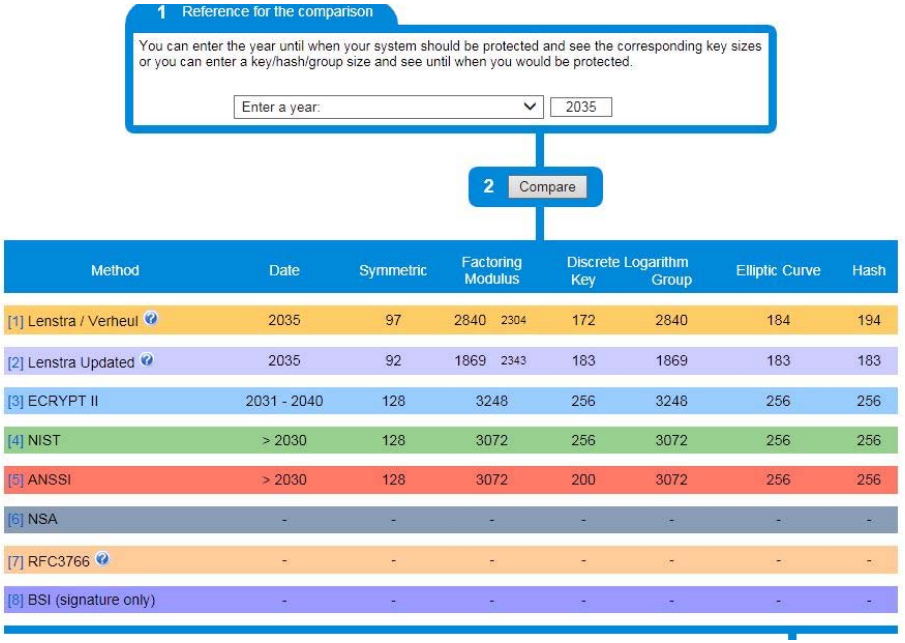
Recommend that customers complete the Certificate Policy first before doing any further design or deployment work

Thales PS has significant experience in this area and can help!

Good practice & lessons learned – cryptographic algorithms & key sizes

Algorithms and key sizes chosen should be based on:

- Risk assessment/organisation security policies
- The lifetime of the CA certificate and End Entity certificates to be issued
  - www.keylength.com (recommendations based on various standards)
- The Subscriber & Relying Party applications/services that will make use of the certificates
  - THIS is generally the MAJOR constraint!
  - If using RSA, avoid RSA key sizes < 2048



Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
[1] Lenstra / Verheul	2035	97	2840 2304	172	2840	184	194
[2] Lenstra Updated	2035	92	1869 2343	183	1869	183	183
[3] ECRYPT II	2031 - 2040	128	3248	256	3248	256	256
[4] NIST	> 2030	128	3072	256	3072	256	256
[5] ANSSI	> 2030	128	3072	200	3072	256	256
[6] NSA	-	-	-	-	-	-	-
[7] RFC3766	-	-	-	-	-	-	-
[8] BSI (signature only)	-	-	-	-	-	-	-

Good practice & lessons learned – certificate lifetimes

Certificate lifetimes should be chosen based on:

- Risk assessment/organisation security policies
- Exposure of cryptographic keys (i.e. how often will the associated private key be used, where will the associated private key be stored?)
- Assurance level provided by the certificate (i.e. stringency of the certificate issuance process)

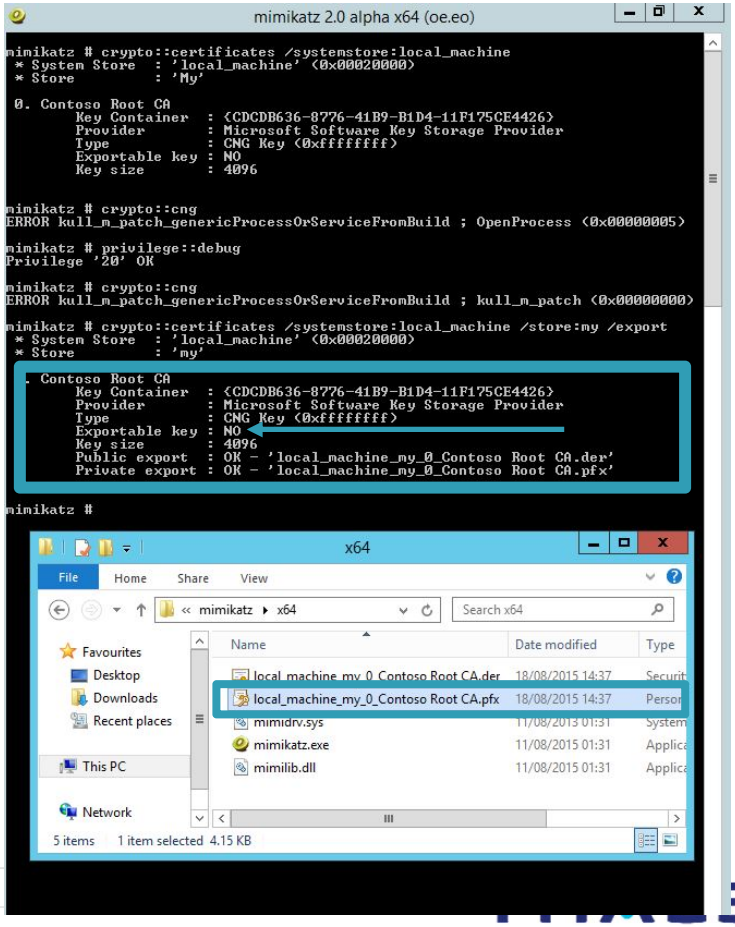
Root CA cert lifetime often twice as long as Issuing CA cert lifetime (e.g. 20 years vs 10 years)

Good practice is to renew certificates between 50% & 80% of expired lifetime

- Note that much more planning is required for renewal of a CA certificate
- UK PKI expert: "Precipitous CA key/certificate renewals are one of the major causes of PKI failures"

‘Not-so-good practice’ - Storing CA private keys in software

- **CA private keys marked as exportable by default**
  - Required for backups to work!
- **Anyone with local admin privileges and access to the CA can export the private key**
- **Tools such as ‘mimikatz’ can export the private key, even if the key is marked as ‘non exportable’ for some reason**
- **Combine this with a remote code execution vulnerability & it could be devastating**



OPEN

Good practice – key generation & HSMs

A HSM is not a panacea – it is one aspect of 'security basics'

- See Diginotar!

Important keys should be protected using a HSM

- Microsoft & Gartner have both published papers stating as much
- Consider not only CA private keys but also those used by services such as NDES and OCSP

Key compromise is costly and expensive

- Especially true if a CA private key is compromised, consider the operational cost of reissuing all End Entity certificates
- Cost of a HSM is probably less, factor into risk assessments

Thales Group in Qatar

Key Facts of Thales in Qatar

- Thales has operated in Qatar for 35 years – today employs 270 people locally
- Historically Thales has been a key supplier to the Qatar Armed Forces
- Thales today provides IFE systems for Qatar Airways
- On the Doha Metro, Thales provides train control signalling, telecoms, an operations centre and automated fare collection systems.
- At Hamad International Airport, Thales provides 13,000 video cameras and 3,000 access control points
- 100% of ATM transactions in Qatar are protected by Thales HSMs. Customers include the Qatar Central Bank and QNB.

THALES