

Microsoft®

Microsoft®
tech·ed
IT Professionals | 2008

Be a part of the experience.



Deployment Tips for Security and Strong Authentication

David Wozny
Security Architect
Oxford Computer Group

Agenda

- ▶ PKI and CLM design
- ▶ Protecting private keys (HSMs)
- ▶ Smart card enforcement
- ▶ CLM add-ons (& demo)
- ▶ Revocation matters
- ▶ Operations & gotchas

PKI and CLM Design

PKI and CLM Design

Principal Decisions

- ▶ Hierarchy
 - ▶ Who are you trying to impress ;-)
 - ▶ Three tiers? Unlikely...
- ▶ Key lengths
 - ▶ 4,096 bit?
 - ▶ Compatibility problems?
- ▶ CA certificate validity period

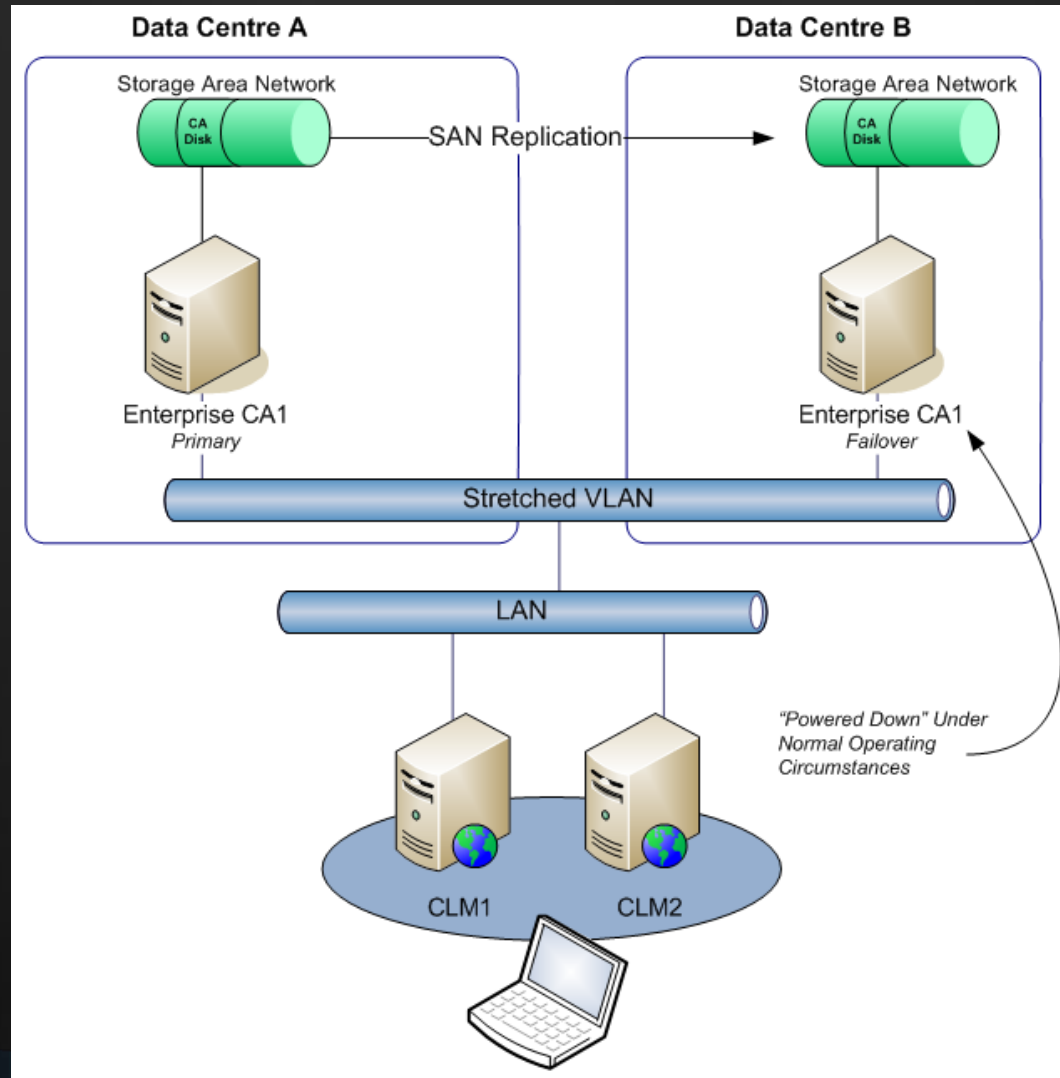
PKI and CLM Design

Availability - Considerations

- ▶ Certification authority server(s)
 - ▶ Principle considerations
 - ▶ Availability for certificate issuance (and key recovery)
 - ▶ Availability for CRL publication
 - ▶ Can't cluster certificate services (on Win2K3)
 - ▶ Can't scale out CA servers (affinity)
 - ▶ Concentrate on *superfast recovery*
 - ▶ SAN booting and mirroring
 - ▶ Snapshots to mitigate software failure

PKI and CLM Design

Availability – Candidate Design



PKI and CLM Design

Availability

- ▶ CLM server(s)
 - ▶ Largely stateless
 - ▶ Scale out easily
 - ▶ Use load balancer or NLBS
 - ▶ Agent certificates need to be identical
 - ▶ Make sure SQL back end is also highly available
- ▶ CRLs
 - ▶ Addressed later...

PKI and CLM Design

High Availability CA on Win2K8

- ▶ Win2K8 Enterprise CA
 - ▶ Truly enterprise class
 - ▶ Two node active / passive failover cluster

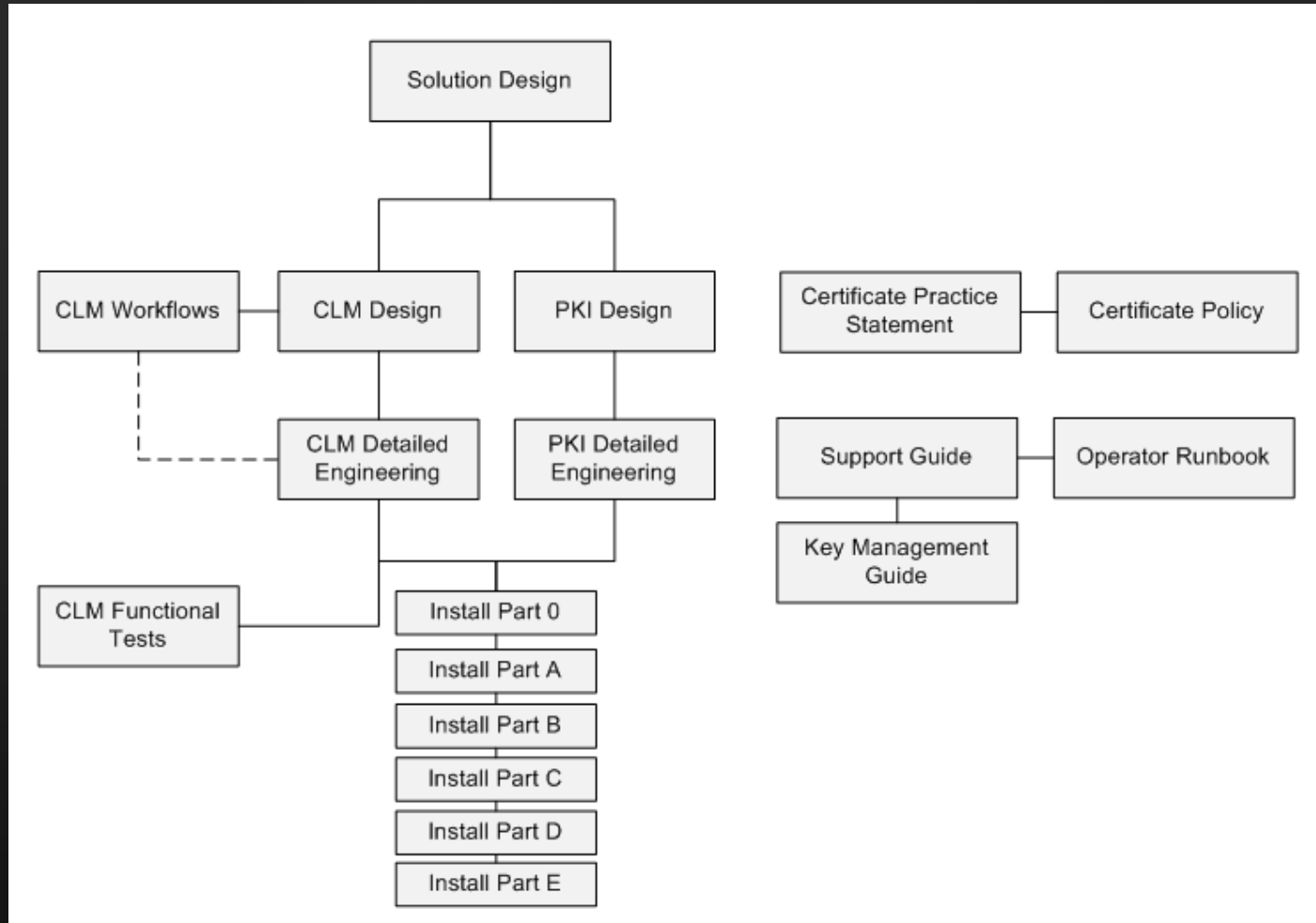
PKI and CLM Design

User Certificates

- ▶ User certificates
 - ▶ No rule enforcing one year!
 - ▶ Excess churn
 - ▶ Make renewal self serviceable
- ▶ SC logon uses UPN
 - ▶ Be careful when changing
 - ▶ Down-level and friendly UPN
 - ▶ Can be used to advantage

PKI and CLM Design

Document Reading Map



PKI and CLM Design

CLM versus “Others”

- ▶ Mini-Driver (Base CSP) capability
- ▶ CLM Auditing: comprehensive and navigable
- ▶ AD leveraging: everything
- ▶ ILM integration: CLM MA
- ▶ Extremely rich workflow
 - ▶ Automated renewal
 - ▶ Recover on behalf simplicity
 - ▶ “Infinite” flexibility with ACLs

PKI and CLM Design

CLM “Go Much Faster” Hotfix

- ▶ The problem
 - ▶ Accessing CLM for first time very slow, but not so bad afterwards
 - ▶ Verification of Authenticode signature on .Net managed application timing out
- ▶ Fix documented in:
 - ▶ KB936707

PKI and CLM Design

CLM “Go Much Faster” Hotfix

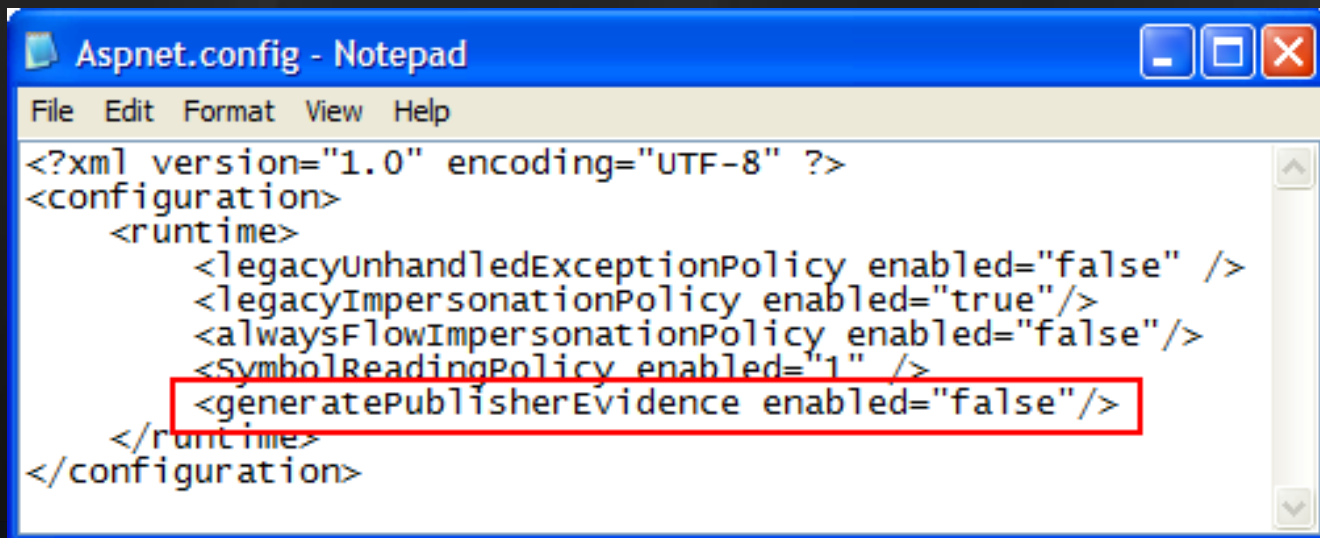
▶ Install KB936707

▶ Open:

- ▶ C:\Windows\Microsoft.Net\Framework\v2.0.50727\aspnet.config

▶ Edit runtime section:

- ▶ `<generatePublisherEvidence enabled="false"/>`



```
Aspnet.config - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8" ?>
<configuration>
  <runtime>
    <legacyUnhandledExceptionPolicy enabled="false" />
    <legacyImpersonationPolicy enabled="true"/>
    <alwaysFlowImpersonationPolicy enabled="false"/>
    <symbolReadingPolicy enabled="1" />
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

Protecting Private Keys

Protecting Private Keys

Hardware Security Modules

- ▶ Why you need an HSM
 - ▶ The risks you're mitigating against
 - ▶ What it doesn't mitigate against
- ▶ Part of the PKI dark arts! Not!

Protecting Private Keys

HSM Vendors and Products



SafeNet



nCipher (Thales)



Protecting Private Keys

HSM Considerations

- ▶ HSM form factors / selection
 - ▶ Root CA: dedicated HSM (PCI / USB)
 - ▶ Online CAs (and CLM servers): network HSM?
 - ▶ Network HSMs: “Must” have HA
 - ▶ Performance benchmarks
- ▶ HSM logical controls
 - ▶ M of N tokens
 - ▶ Be practical - realistic

Protecting Private Keys

HSM Advice

- ▶ Buy premium (super duper) support
- ▶ Develop strict key management policy
- ▶ Regularly audit token holders
- ▶ FIPS 140-2 Level 2 and 3
 - ▶ Tamper assurance and authentication technique
 - ▶ SafeNet – Token (not password) authentication
 - ▶ nCipher – Extra authorisation for key generation

Smart Card Enforcement

Smart Card Enforcement

User Based

The image shows a screenshot of the 'Simone Properties' dialog box in Windows, specifically the 'Account' tab. The dialog box has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Published Certificates', 'Member Of', 'Dial-in', 'Object', 'Security', 'Environment', 'Sessions', 'Remote control', 'Terminal Services Profile', 'COM+', 'General', 'Address', 'Account', 'Profile', 'Telephones', and 'Organization'. The 'Account' tab is selected.

Under the 'Account' tab, there are several fields and options:

- 'User logon name:' with a text box containing 'Simone' and a dropdown menu showing '@ccms.local'.
- 'User logon name (pre-Windows 2000):' with a text box containing 'CCMS\' and another text box containing 'Simone'.
- Buttons for 'Logon Hours...' and 'Log On I.o...'
- An unchecked checkbox labeled 'Account is locked out'.
- 'Account options:' section with a list of checkboxes:
 - Account is disabled
 - Smart card is required for interactive logon (highlighted with a red box)
 - Account is sensitive and cannot be delegated
 - Use DES encryption types for this account
- 'Account expires:' section with radio buttons for 'Never' (selected) and 'End of:' with a date field showing '29 November 2008'.

At the bottom of the dialog box are buttons for 'OK', 'Cancel', and 'Apply'.

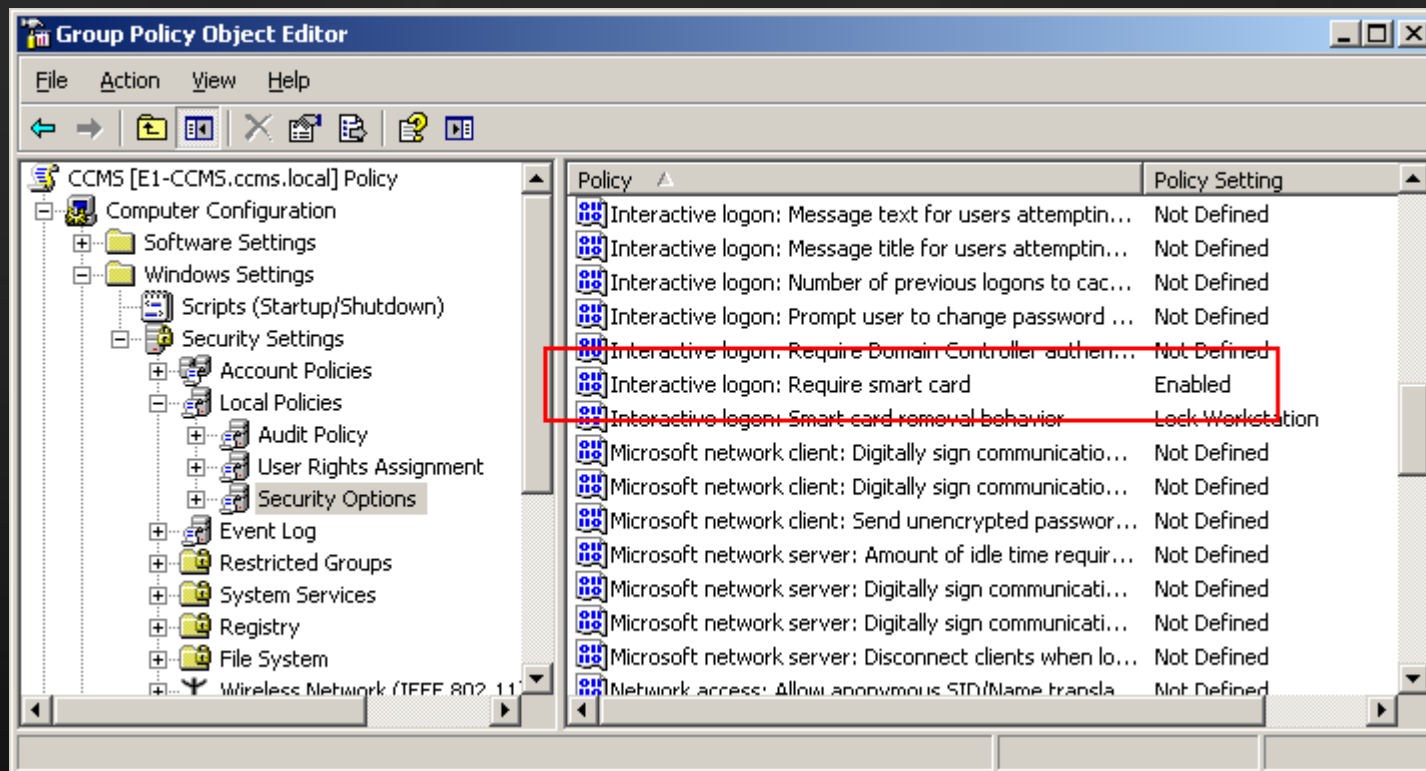
Smart Card Enforcement

User Based

- ▶ “Issuance does not enforce”
- ▶ Directly set on user account (not in GPO)
 - ▶ *Not for faint hearts*
 - ▶ Can be applied programmatically
 - ▶ userAccountControl:262144
 - ▶ Randomises password
 - ▶ Prevents password ageing

Smart Card Enforcement

Computer Based



Smart Card Enforcement

Computer Based

- ▶ Set by GPO (computer scope)
 - ▶ Often used for critical assets
 - ▶ Password ageing still enforced
 - ▶ Roll-out timing issues
- ▶ Prevents logon with local (SAM) accounts

Smart Card Enforcement

Users or Admins (or Both?)

▶ Admins

- ▶ Privilege elevation via redirection
 - ▶ MSTSC, runas, net use
 - ▶ Need CSP on remote (RDP) server
- ▶ Interactive login in the data centre
 - ▶ Smart card reader “on a nail”
- ▶ Two readers at desktop

▶ Users

- ▶ SC logon isn't SSO
 - ▶ Kerberos TGT

Smart Card Enforcement

Consequences

▶ Known Issues

- ▶ Outlook web access (OWA)
- ▶ Outlook anywhere (RPC / HTTPS)
- ▶ VPN clients
- ▶ Roaming dialers
- ▶ Mobile users

▶ Solutions

- ▶ Kerberos constrained delegation (KCD)
- ▶ WIP

Smart Card Enforcement

Exception Management Scenarios

- ▶ Broken or lost card
 - ▶ Post replacements?
 - ▶ Need cached logon
- ▶ Blocked PIN
 - ▶ Need to logon to do unblock, unless VISTA
- ▶ Revert to password
 - ▶ Not effective until network connected logon

Smart Card Enforcement

Exception Management Tactical Options

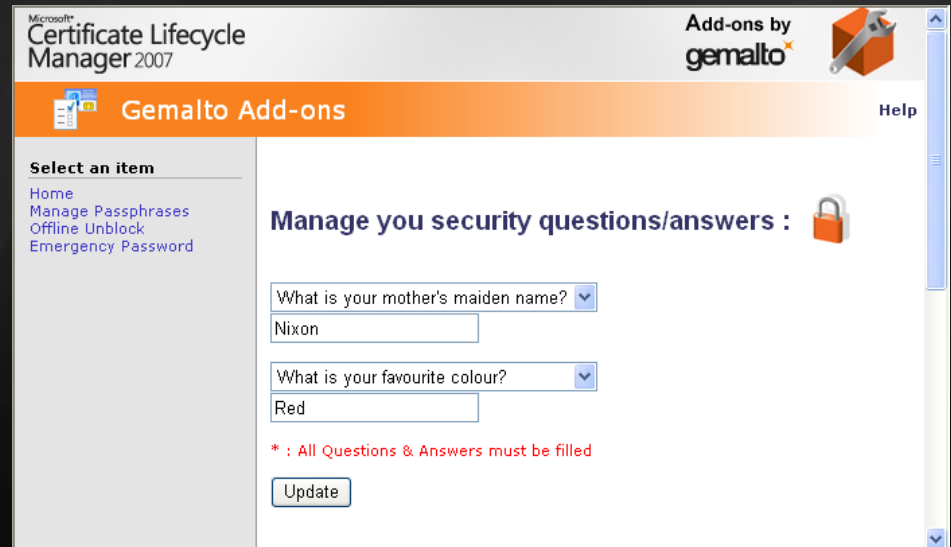
- ▶ Make VPN prior to Active Directory logon?
- ▶ Log on using kiosk type account to access unblock
 - ▶ Need a cached logon
 - ▶ Tough call to get account sufficiently hardened
 - ▶ Potential to access C-drive of any computer


CLM Add-Ons

CLM Add-Ons

Secret Questions and Answers

- ▶ Validate users calling in
 - ▶ Answers set during enrolment
 - ▶ Users can update
 - ▶ Flexibility on Q&A policy
 - ▶ Answers stored in AD
 - ▶ Used for:
 - ▶ Emergency passwords
 - ▶ Offline unblock

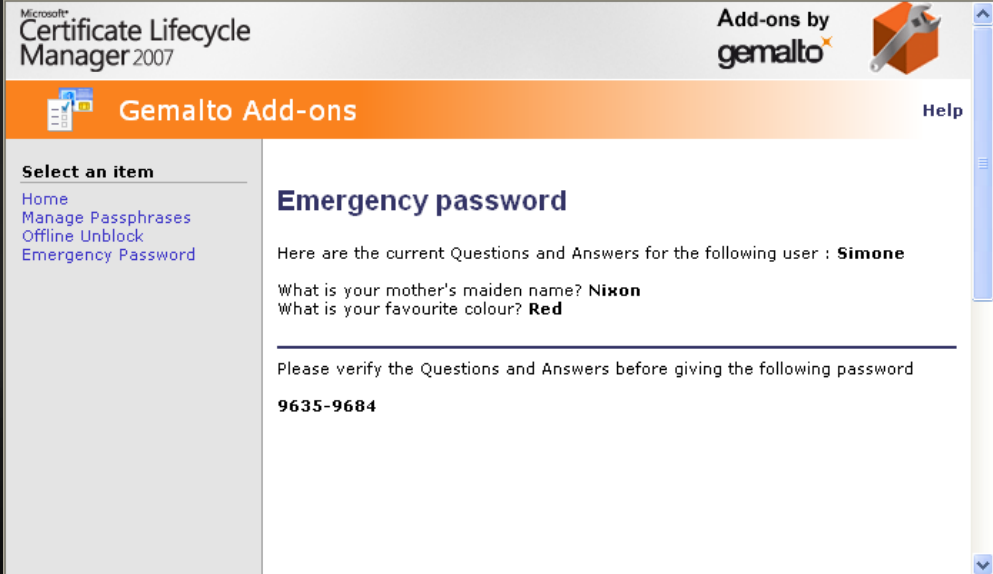


The screenshot displays the Microsoft Certificate Lifecycle Manager 2007 web interface. The top navigation bar includes the Microsoft logo, 'Certificate Lifecycle Manager 2007', and 'Add-ons by gemalto'. Below this is an orange banner for 'Gemalto Add-ons' with a 'Help' link. A left-hand menu titled 'Select an item' contains links for 'Home', 'Manage Passphrases', 'Offline Unblock', and 'Emergency Password'. The main content area is titled 'Manage your security questions/answers : '. It features two dropdown menus: 'What is your mother's maiden name?' with 'Nixon' selected, and 'What is your favourite colour?' with 'Red' selected. A red asterisk warning states '* : All Questions & Answers must be filled'. An 'Update' button is located at the bottom of the form.

CLM Add-Ons

Emergency Password

- ▶ HDEP ordinarily unknown to users
 - ▶ Injected into cached credentials
 - ▶ Seeded from unique key, user and time
 - ▶ Policy for:
 - ▶ Validity period
 - ▶ HDEP length
 - ▶ Re-use, etc.



The screenshot shows the Microsoft Certificate Lifecycle Manager 2007 interface. The title bar includes "Microsoft Certificate Lifecycle Manager 2007" and "Add-ons by gemalto". The main content area is titled "Gemalto Add-ons" and "Emergency password". The interface displays the following information:

Select an item

- Home
- Manage Passphrases
- Offline Unblock
- Emergency Password

Emergency password

Here are the current Questions and Answers for the following user : **Simone**

What is your mother's maiden name? **Nixon**
What is your favourite colour? **Red**

Please verify the Questions and Answers before giving the following password

9635-9684

CLM Add-Ons

Offline Unblock

- ▶ Validate users calling in
- ▶ Integrated with CLM functionality

The screenshot displays the Microsoft Certificate Lifecycle Manager 2007 interface. The top left corner shows the Microsoft logo and the text "Certificate Lifecycle Manager 2007". The top right corner features the "Add-ons by gemalto" logo. Below the header, there is an orange banner with the text "Gemalto Add-ons".

On the left side, there is a navigation menu titled "Select an item" with the following links: Home, Manage Passphrases, Offline Unblock, and Emergency Password.

The main content area displays the following information:

- Header: "Here are the current Questions and Answers for the following user : **Simone**"
- Questions and Answers:
 - What is your mother's maiden name? **Nixon**
 - What is your favourite colour? **Red**
- Instruction: "Please select the correct active card associated to the user :"
- Selected Card: A radio button is selected next to the card ID "{ef8b0f0e-0157-5113-268c-b30f2d05ffff}"
- Instruction: "then verify the Questions and Answers before asking for the challenge and click Calculate"
- Form fields:
 - Challenge:
 - Response:
- Button: "Calculate"

CLM Add-Ons demo

Revocation

Revocation

CRL 101



▶ CRL “parameters”

- ▶ Publication time: 06:00 on 20/11/08
- ▶ Base CRL period: 4 days
- ▶ CRL overlap: 4 days
- ▶ Clock skew: 15 mins

Revocation

A CRL Validity Period Formula ;-)

Base CRL Period = CA Server Fix SLA + Troubleshooting Time

- ▶ Don't underestimate troubleshooting time
 - ▶ Is it the CA, HSM, AD, permissions, etc.?
 - ▶ You'll always try least invasive options first
 - ▶ Need teams gathered for restore (perhaps)

Revocation

Certificate Revocation Lists

- ▶ Certificate revocation lists - criticality
 - ▶ CA availability versus freshness
 - ▶ Delta CRLs?
- ▶ LDAP or HTTP?
 - ▶ AD LDAP (LDAP:///cn=my CA, cn=...)
 - ▶ IIS farm (or CLM servers)
 - ▶ Out-of-band file transfer to HTTP
 - ▶ Manual CRL signing
- ▶ Large CRLs can be killers for VPN devices

Revocation

Certificate Revocation Lists

- ▶ Caching behavior
 - ▶ Application dependant
 - ▶ CRL cached for authoritative period
 - ▶ Cache cannot be reliably purged
- ▶ Stale CRL fix for SC logon
 - ▶ KB887578
 - ▶ Only for Windows SC logon (not VPN, etc.)

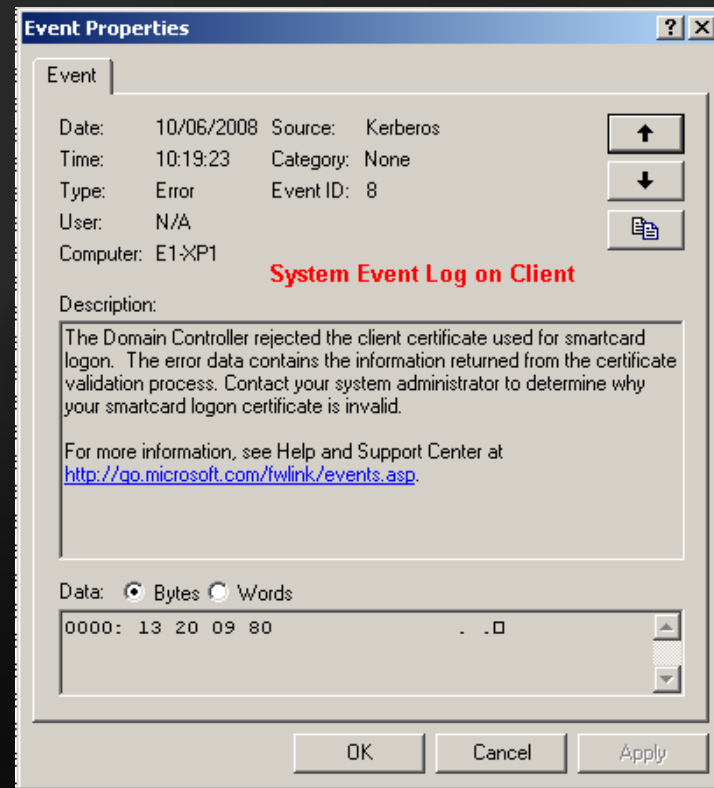
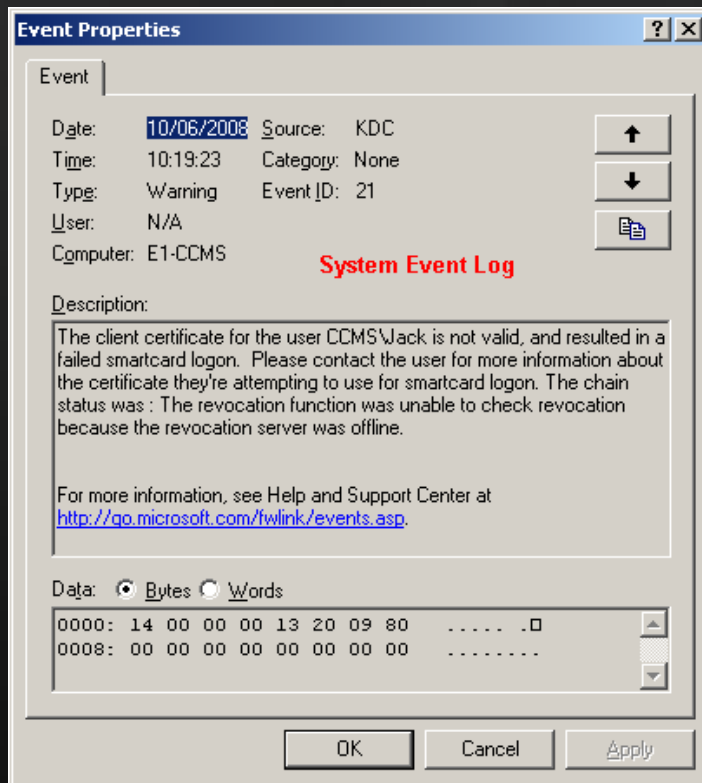
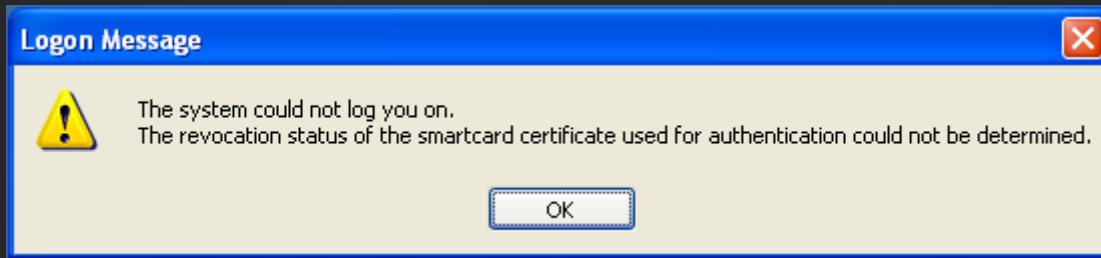
Revocation

Offline Servers

- ▶ Offline CA CRLs
 - ▶ Dilemma:
 - ▶ Regularity versus necessity
 - ▶ Sensible to have 52 weeks + 8 week overlap

Revocation

Event Log Entries



Revocation

Online Certificate Status Protocol (OCSP)

- ▶ Native capability in Win2K8 CA and VISTA
- ▶ Come to IDA04-IS
 - ▶ 14:40 in room 132

Operations

Operations

Admin Key Diversification

- ▶ You MUST do this!
 - ▶ Smart cards can only be managed by CLM instantiation which issued card
 - ▶ Admin key is encrypted in CLM database

Microsoft Smart Card Base CSP
Specify the settings you want to use with the Microsoft Smart Card Base Cryptographic Service Provider (CSP).

Diversify Admin Key
Admin key initial value (hex):

Smart Card Initialization Provider
 Default
 Custom:

Smart card initialization provider data:

Operations

Admin Key Diversification

- ▶ No diversification?
- ▶ Easy to reset PIN

.NET Utilities

Reader Selection

There is 1 smart card connected:

Currently Selected Reader:

Card in Selected Reader: .NET V2

Card Serial Number: 57011351268CB30F2D05FFFF

Utilities

[Change PIN](#)
[Unblock PIN](#)

[Card Information](#)
[Certificate Management](#)

[Cryptogram Calculator](#)

It helps you unblocking the PIN of your Smart card.

Challenge:

Admin key:

Response:

New PIN:

Confirm PIN:

Unblock *Un-Diversified* Card demo

Operations

Focus on Post Issuance Lifecycles

- ▶ It's not just about enrolment!!!
 - ▶ Renewal, duplicate, temporary, replacement, etc.
- ▶ Inevitable workflow design behaviour...
 - ▶ Will start with overly complex workflow
 - ▶ Will model these in a POC
 - ▶ Will streamline and reduce complexity
- ▶ Takeaway – get off paper and into a POC ASAP

Operations

Smart Card PINs

- ▶ PIN rules
- ▶ PIN blocking
 - ▶ Num lock key switching off
- ▶ Offline PIN unblocks
 - ▶ Do not respect PIN rules
- ▶ Empirical evidence
 - ▶ PIN blocks reasonably slight
 - ▶ Lost / forgotten cards biggest problem

Operations

Gotchas

- ▶ Be careful deleting AD accounts of leavers
 - ▶ Make's life tough for CLM based key recovery
- ▶ Third party GINA stubs
 - ▶ Other (lesser ;-)) 2FA capabilities
 - ▶ Single sign-on
 - ▶ Simplified sign-on (FDE pre-boot)
 - ▶ Emergency password recovery

Operations

Maintain a Strict Schedule

- ▶ Offline CRL publication
- ▶ CA certificate renewal
- ▶ Auditing of token holders
- ▶ CLM agent certificate renewal
- ▶ Web site certificate renewal
- ▶ Don't allow CLM agent account passwords to expire

Operations

CA Disaster Recovery

- ▶ Computer account password change
 - ▶ Beware!
 - ▶ KB216393 doesn't apply

Operations

Converged / Hybrid Corporate Card?

- ▶ Physical access
 - ▶ Greater political rather than technical challenges
 - ▶ Where to do card printing?
- ▶ GemAlto .Net cards incorporate OTP assemblies
 - ▶ Can use offline reader for unmanaged PC use case

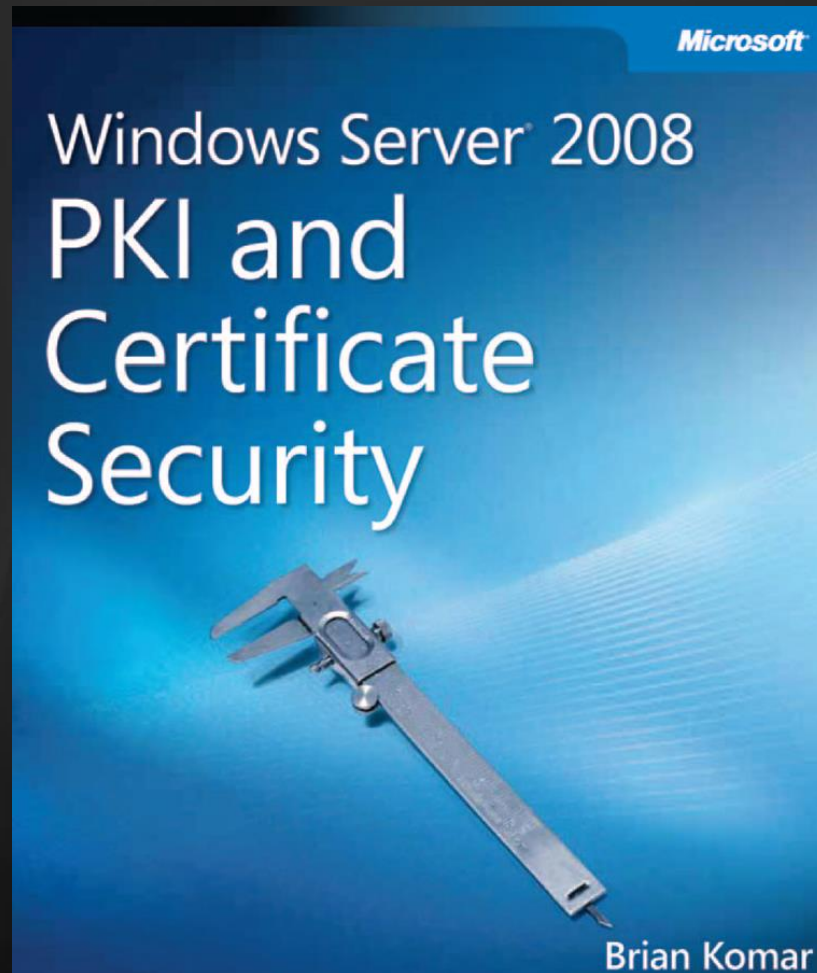
Operations

Leverage Investment

- ▶ Use SC authentication for FDE and IAG
 - ▶ Most FDE solutions enable simplified sign on
- ▶ Leverage CLM for EFS
 - ▶ Greatly reduces recovery complexity whilst providing higher assurance

How to Look Good...

Never Leave Home Without This



Microsoft

Windows Server® 2008 PKI and Certificate Security

Brian Komar

Call to Action

- ▶ Don't overdesign
- ▶ Always bear in mind the ticking time bomb
- ▶ Plan for post issuance use cases
- ▶ Pay attention to exception scenarios

Resources

Reading Material

- ▶ MS PKI papers and articles
 - ▶ www.microsoft.com/pki
- ▶ MS PKI “Bible”
 - ▶ Windows Server 2008 PKI and Certificate Security

Resources

Online

- ▶ OCG online demonstrations
 - ▶ www.oxfordcomputergroup.com/resources.aspx
- ▶ PKI newsgroup
 - ▶ microsoft.public.security.crypto

Q & A

Related Content

Monday, November 3rd

IDA304: Integrating strong authentication into provisioning and compliance processes with Microsoft Identity Lifecycle Manager "2"	4:00-5:15pm
SEC303: Introducing Forefront Client Security 2.0	5:45-7:00pm

Tuesday, November 4th

IDA301: Identity Lifecycle Manager 2 (Part 1): Empowering users with self-service identity management solutions	10:45-12:00pm
IDA309: Windows Server 2008 R2 Active Directory: What's Coming Up?	1:30-2:45pm
IDA310: Windows Vista PKI Enhancement in Windows 7 and Windows Server 2008 R2	3:15-4:30pm
SEC311: Going Virtual with the Intelligent Application Gateway and a Sneak Peak at the Future!	3:15-4:30pm
SEC403: Forefront Security for Exchange Server: Advanced Spam and AntiMalware Scanning Today and Tomorrow	5:00-6:15pm
IDA305: Active Directory Rights Management Services (AD RMS) - End to End	5:00-6:15pm

Wednesday, November 5th

OFC311: Microsoft Forefront Security for SharePoint: The Next Generation of Collaboration Security	9:00-10:15am
IDA302: Identity Lifecycle Manager 2 (Part 2): Expressing and enforcing business policy	1:30-2:45pm
SEC305: Introduction to Microsoft Forefront Codename Stirling	1:30-2:45pm
IDA306: Connecting Active Directory to Microsoft Cloud Services	3:45-5:00pm
SEC204: Hybrid Messaging Security for Exchange Server	3:45-5:00pm
IDA401: Using Active Directory Domain Services for Linux Servers	5:30-6:45pm

Visit the Identity & Security booths for a detailed guide to activities at TechEd EMEA

Related Content

Thursday, November 6th

IDA308: Windows Server 2008 Active Directory Best Practices	8:30-9:45pm
IDA313: Notes from the Field: Deploying Microsoft Identity Lifecycle Manager 2007 Certificate Management	10:15-11:30am
IDA402: Successful deployment tips for Security and Strong Authentication	1:00-2:15pm
SEC317: Using Network Access Protection (NAP) in combination with FCS	1:00-2:15pm
IDA303: Identity Lifecycle Manager 2 (Part 3): Extensibility and provisioning with ILM 2	2:40-3:55pm
DA311 : "Geneva" Claims Based Access: Universal sign-in utilizing AD, CardSpace and federation	4:20-5:35pm

Friday, November 7th

IDA307: Active Directory Information Security - Where is the boundary?	9:00-10:15am
SEC316: A Technical Preview and Deep Dive of Next Generation ISA Server	9:00-10:15am
IDA403: A DS Geek's Notes from the Field - Active Directory Uncovered	10:45-12:00pm
IDA312: "Geneva" Security Token Services: Infrastructure services for SOA security and federation	3:15-4:30pm

Visit the Identity & Security booths for a detailed guide to activities at TechEd EMEA

Resources for IT Professionals

Microsoft®
tech.ed
Online

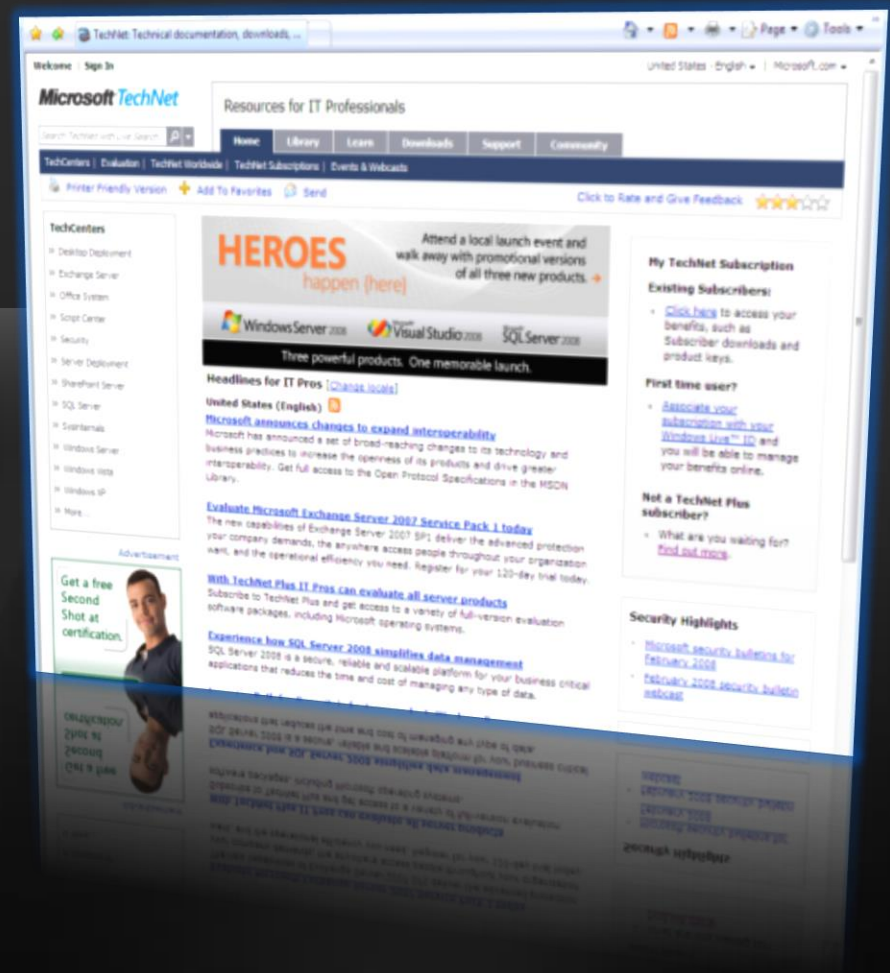
www.microsoft.com/teched

Tech·Talks Tech·Ed Bloggers
Live Simulcasts Virtual Labs

Microsoft® TechNet

<http://microsoft.com/technet>

Evaluation licenses, pre-released products, and MORE!



Microsoft[®]

Your potential. Our passion.[™]

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.