ABC Account

COE to WBP Remote Authentication Proof of Concept Report v0.99

31st December, 1999

Change History

The following change history log contains a record of changes made to this document:

Revised Date	Version	Author	Nature of Change
31.12.1999	0.1	David Wozny Paul Steunebrink	First Draft for Peer Review

Distribution List

Name	Role	Representing
David Wozny	Author and 2FA NG Technical Specialist	ABC
Paul Steunebrink	Consultant	DEC

Abbreviations

Term	Definition
AD	Active Directory
ADAM	Active Directory Application Mode
AIA	Authority Information Access
CA	Certification Authority
CAPI	(Microsoft) Cryptographic Application Programming Interface
CDP	CRL Distribution Point
CMS	(ActivIdentity) Card Management System
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RDC	Remote Desktop Client
RDP	Remote Desktop Protocol
SSO/2FA	Simplified Sign-On / Two Factor Authentication (Project)
UPN	Universal Principal Name
WAMB	Work Area Managing Board

Table of Contents

1. Introduction

1.1. Brief

A number of users who primarily log on to the ABC managed COE Active Directory (AD) also have a requirement to logon and access applications and data in the DEC managed WBP AD. This is presently achieved by the COE user having a separate user account in WBP AD; WBP related authorizations are assigned to that account. The COE user connects to the WBP environment from his COE desktop through Remote Desktop Protocol (RDP) connection using the Windows Remote Desktop Client (RDC); a WBP Terminal Service runs a virtual WBP desktop.

The present method is satisfactory for authentication with user name & password (UN&P) to both environments or with UN&P to one and smart card logon to the other environment. A problem arises when smart card logon is enforced on both platforms simultaneously, as the native Windows XP RDC client does not support selection of a secondary (WBP) smart card in addition to the primary (COE) smart card used to logon to Windows.

1.2. Objective

The objective of the COE to WBP remote authentication proof of concept exercise was to investigate potential solutions for consideration in meeting the requirement for COE users to access remote resources in the WBP environment further to mandatory smart card logon in both COE and WBP environments.

The deliverable of the exercise is a report (this document) which describes the different approaches which can be undertaken to achieve the desired functionality. This report analyses the strengths and weaknesses of each approach, however, in no way states a preferred approach.

It is expected that this report will be used to stimulate informed discussion which would likely be used as an input into directing further research, perhaps in a more controlled environment.

1.3. Scope

The following items were in scope of the proof of concept exercise:

- Implementing functionality within the test environment to facilitate concept proving regardless of whether that functionality may be achievable in a production environment
- Certificate enrolment using the standard Microsoft web enrolment pages

The following items were out-of-scope of the proof of concept exercise:

- Compatibility issues with different smart card readers / smart cards, etc.
- Consideration given to lock down of hardware / software
- Testing with a card management system

1.4. Management Summary

This proof of concept exercise deals with a broad scope of potential solutions for a future problem: when smart card logon is enforced on both COE and WBP simultaneously. It should be regarded as an investigation in what is potentially possible. Three scenarios were explored, with clear results achieved from scenarios 1 and 2; and although scenario 3 did not pay off in results, this scenario is considered very promising from a user perspective. Therefore we regard all three scenarios as valid for a potential solution.

In scenario 1 it is the user who solves the problem: he is presented with two cards and two readers and he must pay attention to a proper sequence of events when logging on. Since no changes are made to the backend infrastructure, this scenario appears relatively easy to implement.

In scenario 2 and 3 the user has only one card and one reader which is a significant advantage. However, changes either to Active Directory or the PKI infrastructure are considerable and might be complicated both from operational or organizational point of view.

There is, out of scope of this document and exercise, a related problem known as 'GAK token replacement'. This refers to 2FA to mainframe applications and could be solved through 2FA to WBP. Once a solution for COE and WBP simultaneous smart card logon is chosen a specific scenario could become more preferred over another.

This proof of concept exercise provides a solid base for review within both AAB and ABC. In this review and related discussion a decision should be made regarding further research, its scope (same scenarios or smaller) and with specific requirements in mind.

This exercise has illustrated two things: one is that double smart card logon potentially can be solved; another is that a lot of details need further investigation.

Last but not least, it should be noted that cross-platform 2FA might not be limited between COE and WBP. A strategic solution supported by technical insight might prove highly beneficial in the near future.

2. Scenario 1: Two Cards

2.1. Introduction

The fundamental premise of Scenario 1 is that users have a smart card issued by both COE (HQ1-CA) and WBP (WillemCA) based CAs.

The HQ1-CA certificate is used to perform smart card logon to Windows, whereas the secondary card (and WillemCA certificate) is used for remote authentication to the WBP environment.

2.2. Scenarios

- **Scenario 1A**

  Use the WBP issued smart card (and certificate) to authenticate to a WBP terminal services host using the Windows XP native Remote Desktop Client (v5)

- **Scenario 1B**

  The same as scenario 1A except Remote Desktop Client v6 is installed on the COE workstation

2.3. Preparation

2.3.1. General Environment

An GHI RSTU Bank Root CA was deployed in standalone mode, both the WillemCA in WBP and HQ1-CA in COE were deployed subordinate to this CA.

A smart card certificate was issued to the user, David Wozny, from the COE CA server and a second card issued to the user from the WBP CA server. The smart cards used were based upon the WAMB project Giesecke & Devrient SmartCafe Expert 64K using the AET SafeSign middleware (this middleware was also installed on the WBP terminal server).

The post XP-SP2 hotfix to resolve the problem with Kerberos.dll and "friendly UPNs" was applied, KB891849.

All server infrastructure was deployed in a VMware environment using *Vanilla* builds; all workstations were deployed on physical hardware (HP Compaq dc7100SFF workstations), using the embedded USB keyboard based smart card readers and a secondary GemPlus USB smart card reader.

2.3.2. UPN Configuration

Users were defined in COE and WBP as shown in Table 3.

User's Primary Domain	"Downlevel Account" (Domain \ User)	User Principal Name
COE User	aabcoe\dwozny	david.wozny@aabcoe.com
WBP User	aabwbp\dwozny	david.wozny@aabwbp.com

Table 1: Users for Scenario 1

2.4. Scenario 1A: RDC v5

2.4.1. Objectives

In this scenario it was desired to that Windows RDC behaviour with two smart card readers attached. The goal was to logon to Windows using the HQ1-CA issued smart card (certificate) and then present the WillemCA issued smart card (certificate) when authenticating to the WBP terminal services host.

The concept proving environment used for Scenario 1 is shown in Figure 1.

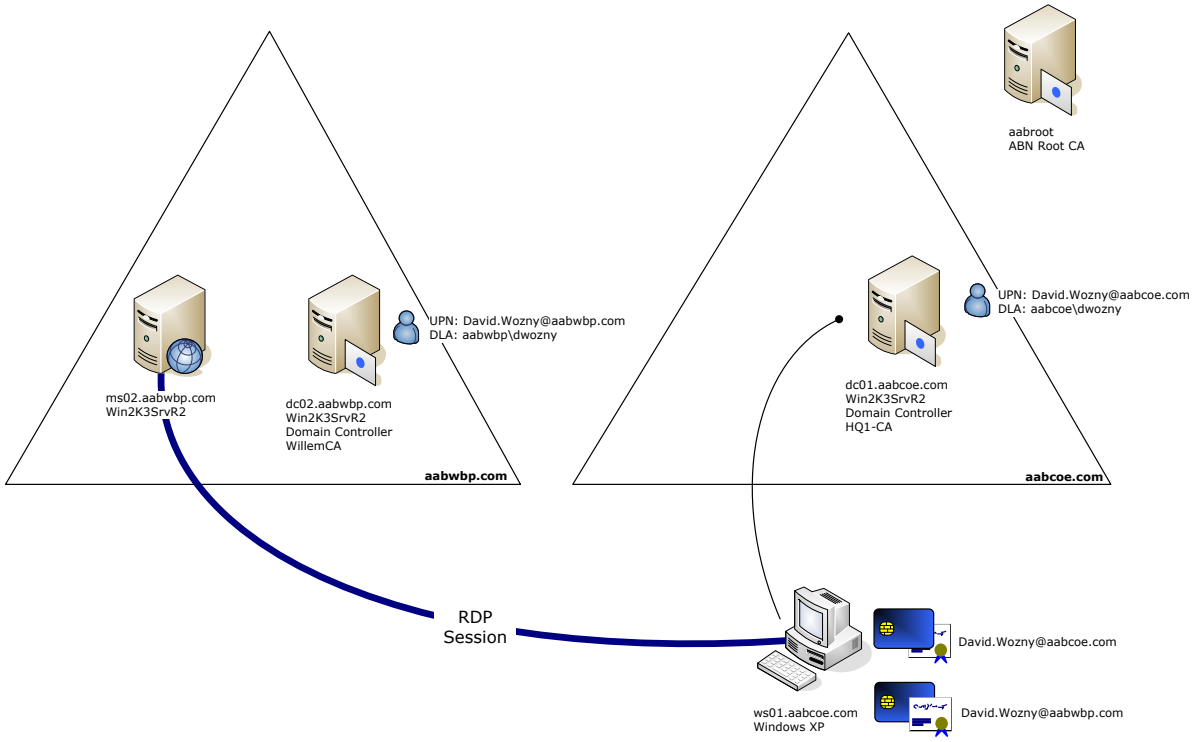

Figure 1: Scenario 1 Proving Environment

2.4.2. Observations

The test showed that the desired functionality was present in Windows XP, however, the user experience was not particularly smooth.

Once the smart card logon to the COE desktop was complete, the Remote Desktop Client software was invoked and targeted to the required host in WBP. It was observed that there was no prompt to select a second reader and the attempt to logon to WBP with the COE certificate failed. Cancellation of the failed authentication prompt and subsequent insertion of the WBP smart card resulted in the correct certificate being presented to the WBP resource on the following authentication attempt.

Even if the WBP card was inserted into the second reader immediately after smart card logon to Windows but prior to establishment of the RDP session then still the first inserted (COE) card was used in the authentication of the RDP session, resulting in a failed logon.

The sequences described above were entirely repeatable.

2.5. Scenario 1B: RDC v6

2.5.1. Objectives

The objective of this scenario was identical to that of Scenario 1A with the exception of determining the enhanced functionality to be gained by installing Remote Desktop Client v6 on the COE workstation.

2.5.2. Observations

RDC v6 introduced a significant user experience enhancement when establishing the RDP session in that it enumerates all smart card readers and the smart cards present therein and presents them to the user in a "friendly manner" to enable an informed selection to be made.

The RDC authentication object picker shows each certificate reference by the issuing CA name and user's display name, as demonstrated in Figure 2.

Figure 2: RDC v6 Smart Card Picker

It was observed that there were a number of smart card reader compatibility issues and the behaviour described above worked best when the GemPlus reader was used to logon to Windows and the HP reader used for the RDP session. However, no further investigation was made since compatibility issues are strictly outside of the scope of this document.

2.6. Conclusions

The RDP experience with RDC v5 was unsatisfactory and confusing and unlikely to be acceptable as a means for providing this service.

Implementing RDC v6 significantly enhanced the user experience and would appear to satisfactorily meet the objectives of Scenario 1.

3. Scenario 2: One Card, One Certificate, Common UPN

3.1. Introduction

The fundamental premise of Scenario 2 is that users have a single certificate issued by the COE certification authority, HQ1-CA. This certificate must be used for smart card logon within the COE AD forest and remote authentication (via RDP) to resources within the WBP AD forest.

There are three main "pre-requisites" required for this certificate to be usable in the WBP forest:

- Subject information in certificates issued by the HQ1-CA is valid in WBP
- The HQ1-CA is trusted within the WBP environment
- The relying party in WBP can retrieve CRLs and build certificate chains from CDP and AIA extensions in certificates issued by the HQ1-CA. It should be noted that CDP and AIA extensions currently employed by the HQ1-CA only employ LDAP references.

The method for satisfying the first two bullet points described above are common to all the sub-scenarios presented here and is described in Section 3.3. CRL retrieval and certificate chain building is the main focus of this scenario and three alternative sub-scenarios considered.

3.2. Scenarios

- **Scenario 2A**

  Publish HQ1-CA CRLs and certificates to an HTTP distribution point which can be reached by WBP relying parties

- **Scenario 2B**

  Implement an AD forest trust between WBP and COE forests to enable reachback by WBP relying parties to COE LDAP locations

- **Scenario 2C**

  Implement a replica of the COE configuration partition to an Active Directory Application Mode (ADAM) server which WBP relying parties can reach to retrieve material from a *pseudo* COE LDAP location

3.3. Preparation

3.3.1. General Environment

An GHI RSTU Bank Root CA was deployed in standalone mode, both the WillemCA in WBP and HQ1-CA in COE were deployed subordinate to this CA.

A smart card certificate was issued to the user, David Wozny, from the COE CA server. The smart card used was the Giesecke & Devrient SmartCafe Expert 64K using the AET SafeSign middleware (this middleware was also installed on the WBP terminal server).

The post XP-SP2 hotfix to resolve the problem with Kerberos.dll and "friendly UPNs" was applied, KB891849.

All server infrastructure was deployed in a VMware environment using *Vanilla* builds; all workstations were deployed on physical hardware (HP Compaq dc7100SFF workstations), using the embedded USB keyboard based smart card readers and a secondary GemPlus USB smart card reader.

3.3.2. User Configuration

Smart card logon to Windows (and RDP connections similarly) uses subject information in the `SubjectAlternativeName` extension in certificates to authenticate users, the extension contains the user's User Principal Name (UPN).

To facilitate the desired interoperability in this scenario, the UPN was configured identically for both COE users and WBP users. To achieve this, an alternate domain suffix (aabb.com) was added to both AD forests and users established as shown in Table 2.

User's Primary Domain	"Downlevel Account" (Domain \ User)	User Principal Name
COE	aabcoe\dwozny	david.wozny@aabb.com
WBP	aabwbp\dwozny	david.wozny@aabb.com

Table 2: Users for Scenario 2

3.3.3. Certificate Trust Configuration

To enable relying parties within the WBP AD forest (typically WBP domain controllers) to trust the HQ1-CA (and certificates issued therewith) it was necessary to publish the HQ1-CA certificate to the following containers in the WBP AD forest:

- `Configuration | Services | Public Key Services | ntAuthCA`
- `Configuration | Services | Public Key Services | AIA`

This publication was achieved using standard `certutil` publishing commands.

3.4. Scenario 2A: HTTP CDP

3.4.1. Objective

In scenario 2A, the challenge of CRL retrieval and certificate chain building for certificates issued by HQ1-CA was met by use of HTTP based CDP and AIA extensions. This required reconfiguration of the AAB Root CA prior to commissioning of the HQ1-CA to include the aforementioned extensions in the HQ1-CA's certificate as well as configuration of the HQ1-CA such that all certificates issued by it also contain HTTP extensions, using the following convention:

- `http://pki.GHIRSTU.com/pkidata`

A web server was deployed on a workgroup server (i.e. not a member of either the COE or WBP AD forests) to host the published certificates and CRLs and a new DNS zone created in the WBP AD forest DNS to enable resolution of hosts in the `GHIRSTU.com` DNS domain. The following material was published to IIS server:

- `GHI RSTU Bank Root CA.crl` (root CA CRL)
- `GHI RSTU Bank Root CA.crt` (root CA certificate)
- `HQ1-CA.crl`
- `HQ1-CA.crt`

Both `aabwpb.com` and `aabcoe.com` were configured with Windows 2000 forest and Windows 2000 native domain functional levels.

The concept proving environment used for Scenario 2A is shown in Figure 3.

3.4.2. Observations

The interoperability testing was entirely successful and validated the proposed approach.

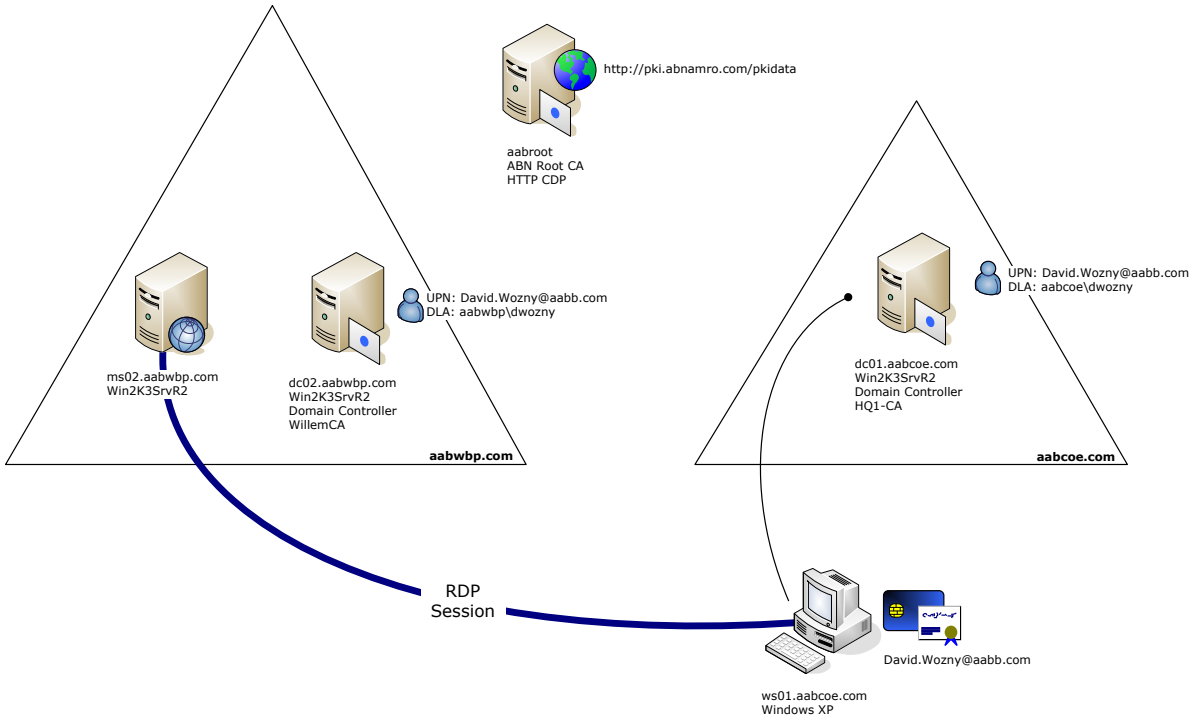

Figure 3: Scenario 2A Proving Environment

3.5. Scenario 2B: Inter-Forest Trust

3.5.1. Objective

In Scenario 2B, the challenge of CRL retrieval and certificate chain building for certificates issued by HQ1-CA was met by implementation of a forest trust between the COE and WBP AD forests. The functional levels of both forests and domains was raised to Windows Server 2003 to enable forests trusts to be established. It should be noted that the forest trusts were implemented in a *completely open manner* with no consideration to reducing necessary entitlement which would be required in a legitimate implementation.

In this scenario, the forest trust provided the capability for the WBP relying party (domain controller) to reach back into the COE forest to retrieve certificates and CRLs from COE LDAP locations.

No HTTP extensions were employed in this scenario and the web server which previously hosted certificate material was decommissioned.

Domain forwarders were configured in both forests to enable DNS name resolution between the two forests to enable the trust.

The concept proving environment used for Scenario 2B is shown in Figure 4.

3.5.2. Observations

The interoperability testing was entirely successful and validated the proposed approach.

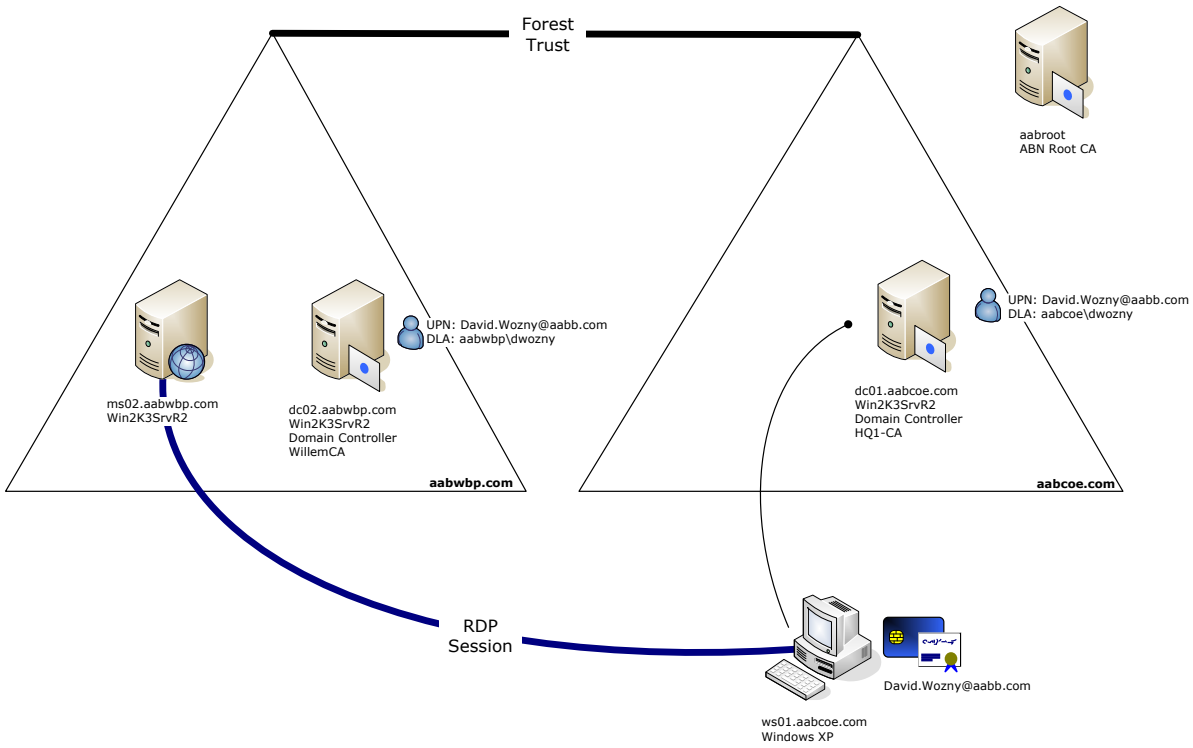

Figure 4: Scenario 2B Proving Environment

3.6. Scenario 2C: ADAM Replica

3.6.1. Objective

In scenario 2C, the challenge of CRL retrieval and certificate chain building for certificates issued by the HQ1-CA was to be met by deploying a server with Active Directory Application Mode (ADAM). This server would be configured with a replica of the configuration naming context objects (containing the pertinent CA certificate and CRL material) from the COE AD forest.

New namespace referrals and DNS forwarders would be configured in the WBP forest to enable WBP relying parties to locate aforementioned material in the ADAM replica.

This scenario does not have any requirement for HTTP extensions or IIS servers and no requirement for trusts between the two AD forests.

The concept proving environment used for Scenario 2C is shown in Figure 5.

3.6.2. Observations

It was not possible to validate this approach due to a lack of necessary ADAM skills.

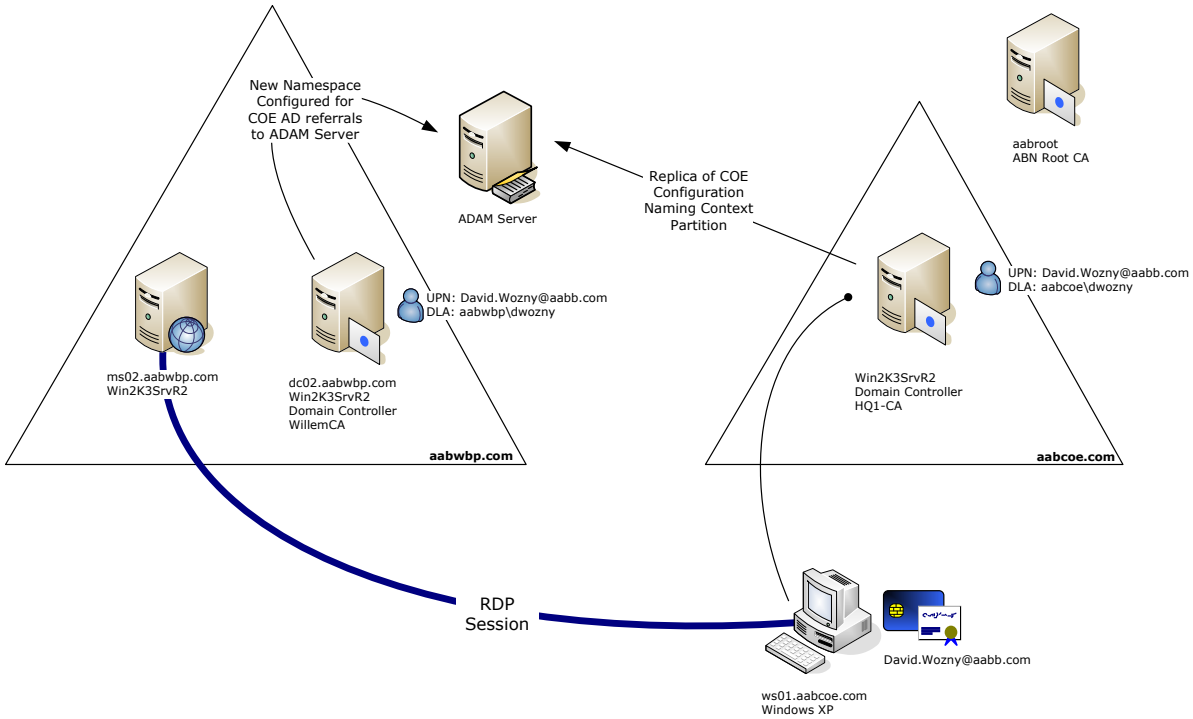

Figure 5: Scenario 2C Proving Environment

3.7. Conclusions

The scenarios showed that the biggest challenge of the "one certificate" methodology is the retrieval of CRL and CA certificate chain material referenced in certificates presented to WBP relying parties.

The HTTP CDP methodology is perhaps the easiest to implement from an operational and technical perspective if one doesn't consider the fact that it would require the redeployment of the HQ1-CA! HTTP is generally seen as a neutral CRL and CA certificate distribution point and it makes sense to include this extension type when deploying a CA. It should be noted that at the time of designing the HQ1-CA, interoperability with WBP was strictly out of scope.

The forest trust requires the least change from a pure PKI perspective, however, implementation of forests trusts is something that would require significant consideration and effort due to both technical challenges (the forests are currently configured as Windows 2000 mode) and operationally (DEC and ABC).

The ADAM methodology seemingly may provide the middle ground between the two options in that it doesn't require redeployment of HQ1-CA to implement HTTP extensions, neither does it require forest trust establishment between COE and WBP. However, it was not possible to prove this method during the course of the exercise.

It should also be noted that a basic premise of the Scenario 2 variations is that a common UPN can be configured for both COE and WBP environments, if possible, it would be expected that the users' *Lotus Notes* email addresses would be employed for this purpose.

4. Scenario 3: One Card, Dual Certificates

4.1. Introduction

The fundamental premise of Scenario 3 is that users have a single smart card which possesses certificates issued by both the HQ1-CA (for COE) and WillemCA (for WBP). Hence, when authenticating against a COE resource, the HQ1-CA issued certificate would be presented and when authenticating against a WBP resource the WillemCA issued certificate would be presented.

A limitation of Windows XP is that the MSGINA does not support selection of multiple certificates during the logon process, it can only select certificates in slot 0 on a smart card. Similarly, when using smart card authentication for the purpose of establishing an RDP session, the "smart card picker" does not provide the capability to select multiple certificates on a single card.

To overcome this limitation, it was necessary to deploy Windows Vista as the client workstation in COE and as a remote host in WBP.

The "one card – multiple certificates" presents a different challenge than Scenario 2, with much reduced complexity in terms of pure PKI requirements in the context that there is no requirement for WBP relying parties to trust HQ1-CA certificates nor retrieve HQ1-CA CRLs from the COE AD forest.

Of course, additional complexity in ensuring that a single card can be used for certificate issuance and usage in both COE and WBP is not insignificant given different card management systems, etc., however, that is outside of the scope of this document.

4.2. Scenarios

- **Scenario 3A**

  Prove dual certificate smart card logon to Windows XP and Windows Vista

- **Scenario 3B**

  Logon to Windows XP or Vista using the COE certificate whilst presenting the WBP certificate during RDP connection

4.3. Preparation

4.3.1. General Environment

An GHI RSTU Bank Root CA was deployed in standalone mode, both the WillemCA in WBP and HQ1-CA in COE were deployed subordinate to this CA.

A smart card certificate was issued to the user, David Wozny, from the COE CA server. A second certificate was installed onto the smart card from the WBP CA server. On a second card the order of enrolment was reversed. Since logon with a smart card to Windows Vista was not successful with the Giesecke & Devrient SmartCafe Expert 64K card using the AET SafeSign middleware (this middleware was also installed on the WBP terminal server) testing was done with the Gemalto .NET card (a.k.a. Axalto Cryptoflex .NET card).

The post XP-SP2 hotfix to resolve the problem with Kerberos.dll and "friendly UPNs" was applied, KB891849. Next, the Microsoft Base Smart Card CSP hotfix was installed, KB909520, was installed on any Windows XP or Windows Server 2003 system used for enrolling certificate to the smart card or for logging on with that card.

All server infrastructure was deployed in a VMware environment using *Vanilla* builds; all workstations were deployed on physical hardware (HP Compaq dc7100SFF workstations), using the embedded USB keyboard based smart card reader.

4.3.2. User Configuration

There is no requirement for a common UPN in both COE and WBP AD forests, hence, native UPNs were used during the testing as shown in Table 3.

User's Primary Domain	"Downlevel Account" (Domain \ User)	User Principal Name
COE User	aabcoe\dwozny	david.wozny@aabcoe.com
WBP User	aabwbp\dwozny	david.wozny@aabwbp.com

Table 3: Users for Scenario 3

4.3.3. Middleware

No middleware was installed on the Windows workstations (XP/Vista) and terminal servers (Server 2003 or Vista) except for the MS Base Smart Card CSP hotfix (XP/Server 2003).

4.4. Scenario 3A: SC Logon Only

4.4.1. Objective

In scenario 3A, the sole objective was to prove that a smart card possessing certificates issued by both WillemCA and HQ1-CA could be used to perform smart card logon to both COE computers and WBP computers.

Two cards were prepared, card S3-1 and S3-2. On card S3-1 the WillemCA certificate was injected first and the HQ1-CA certificate second. No specific card slot was assigned, both were automatically enrolled. The second card – S3-2 – had the two certificates enrolled in reverse order.

The concept proving environment used for Scenario 3A is shown in Figure 6.

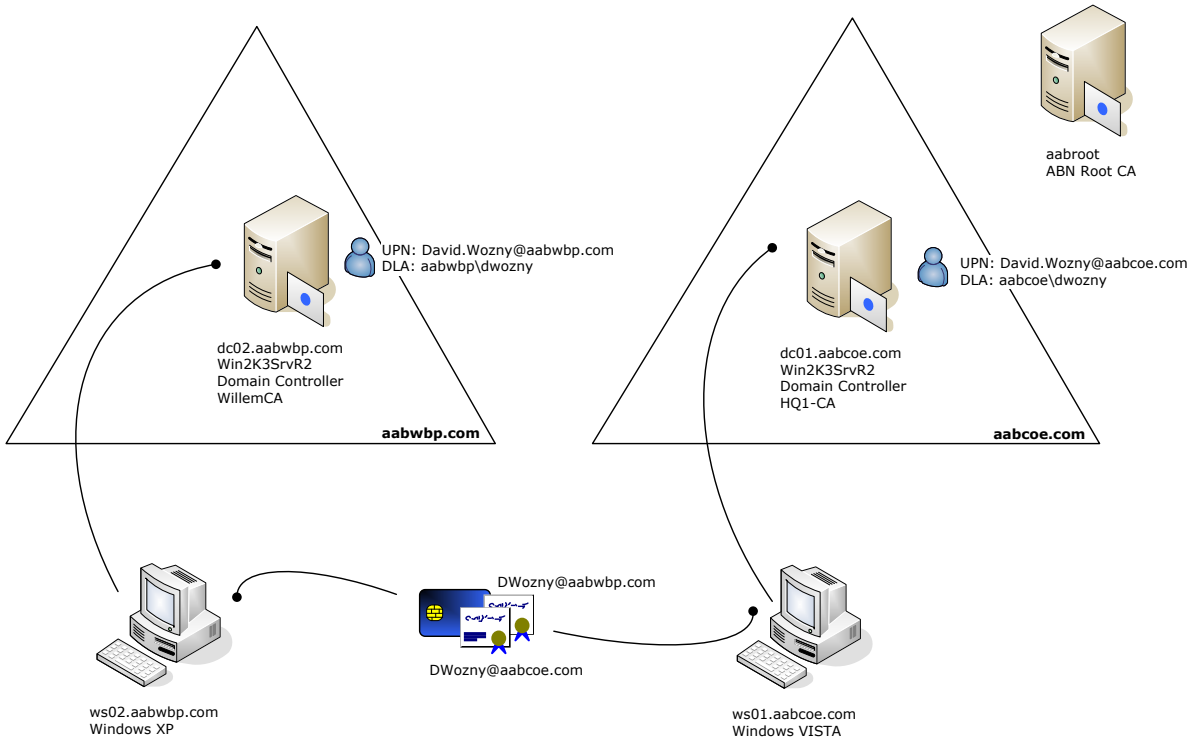

Figure 6: Scenario 3A Proving Environment

4.4.2. Observations

From a Windows XP workstation in the COE domain (aabcoe.com) successful interactive logon was possible with card S3-1 only (HQ1-CA certificate was issued as second certificate). From a Windows

Server 2003 system in the WBP domain (aabwbp.com) successful interactive logon was possible with card S3-2 only (WillemCA certificate was issued as second certificate).

With a Vista workstation interactive logon was successful with both cards. This was true from both domains. During interactive logon, Vista presents the user all connected smart card readers and for each inserted card all certificates. Next, Vista allows the user to select a certificate, enter a PIN for the card and logon.

The options presented when attempting to logon in this scenario can be seen in Figure 7.

Figure 7: Vista Dual Certificate Logon

4.5. Scenario 3B: RDP Connectivity to WBP

4.5.1. Objective

In scenario 3B, the objective was to logon at the COE Windows XP or Vista workstation (using the HQ1-CA issued certificate) and establish an RDP session to a Windows Vista or Server 2003 based WBP computer (using the WillemCA issued certificate).

The smart card configuration was exactly the same as described in Section 4.4.1.

The concept proving environment used for Scenario 3B is shown in Figure 8.

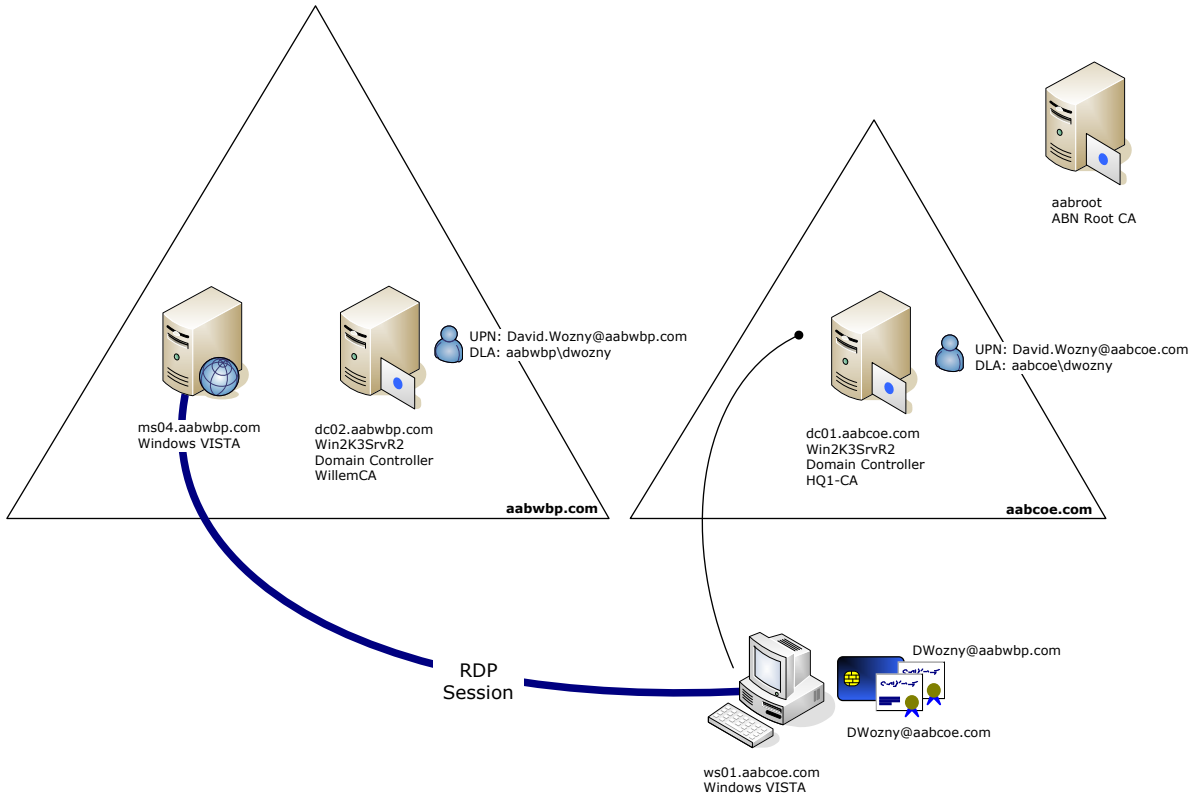

Figure 8: Scenario 3B Proving Environment

4.5.2. Observations

In scenario 3A (interactive smart card logon only) two different workstations (Windows XP and Vista) and two different cards (both with a WillemCA and a HQ1-CA certificate, enrolled in different order) were introduced. The reason behind these different options is to review how the workstation and its RDC version and certificate order on the card affect RDP logon.

For terminal server or remote desktop the same selection of operating systems exists: Windows Server 2003 or Vista. Note that Windows Server 2008 (beta3) was also tested for comparison with Vista. Since its behaviour as remote desktop was the same as Vista in all options, it was left out of this report.

With the introduction of Windows Vista (and Server 2008) a new version of Remote Desktop Client (RDC) was introduced: version 6. This version is available for Windows XP as well and provides a more sophisticated interface for smart card selection. This test will show whether it also allows for certificate selection on a card.

This mix of different cards, workstations, RDC versions and terminal servers boils down to eight options for scenario 3B, listed in the table below.

Option	Smart card	COE workstation / RDC version	WBP terminal server	Result
1.	S3-1	XP / RDC v5	Server 2003	failed
2.	S3-1	XP / RDC v5	Vista	successful with limitations
3.	S3-1	XP / RDC v6	Server 2003	failed
4.	S3-1	XP / RDC v6	Vista	successful with limitations
5.	S3-1	Vista	Server 2003	failed
6.	S3-1	Vista	Vista	failed
7.	S3-2	Vista	Server 2003	successful

8.	S3-2	Vista	Vista	failed

Table 4: Options for Scenario 3B

In option 1 through 4 the COE Windows XP client with S3-1 card connects to the WBP terminal server. Both Windows Server 2003 as well as Vista were tested, and both with the original RDC v5 client software as well as with the newer RDC v6 (originated from Vista).

With Windows Server 2003 as WBP terminal server logon was not successful in option 1 and 3, due to the inability to select the proper certificate on the card for the RDP session. Installing RDC v6 on Windows XP (option 3 and 4) did not bring any improvement due the inability of RDC v6 for XP to select other certificates than in slot 0 on the card. This in contrast to scenario 1 with multiple cards each with one certificate.

Here, Vista as remote desktop saved the day however. Where RDC client from XP is unable to select a certificate, Vista presents a screen after an unsuccessful attempt as if you logon interactively. After selecting the correct certificate for the user, you can logon.

In option 5 through 8 the COE workstation was replaced with Vista. Again the WBP terminal server was either Server 2003 or Vista based. But instead of two different versions of RDC (Vista uses RDC v6 natively) now both smart cards – SC3-1 and SC3-2 – were used, again resulting in four different options. As observed in scenario 3A Windows Vista is able to select the proper certificate on a smart card during interactive logon and is successful to logon interactively with both cards.

An important observation for options 5 through 8 is that RDC v6 of Vista is able to present and identify both certificates on the card. The user can select the certificate for authentication and present the PIN for the card. This raises expectations for successful logon to the remote desktop or terminal server.

The options presented when attempting to logon in this scenario can be seen in Figure 9.

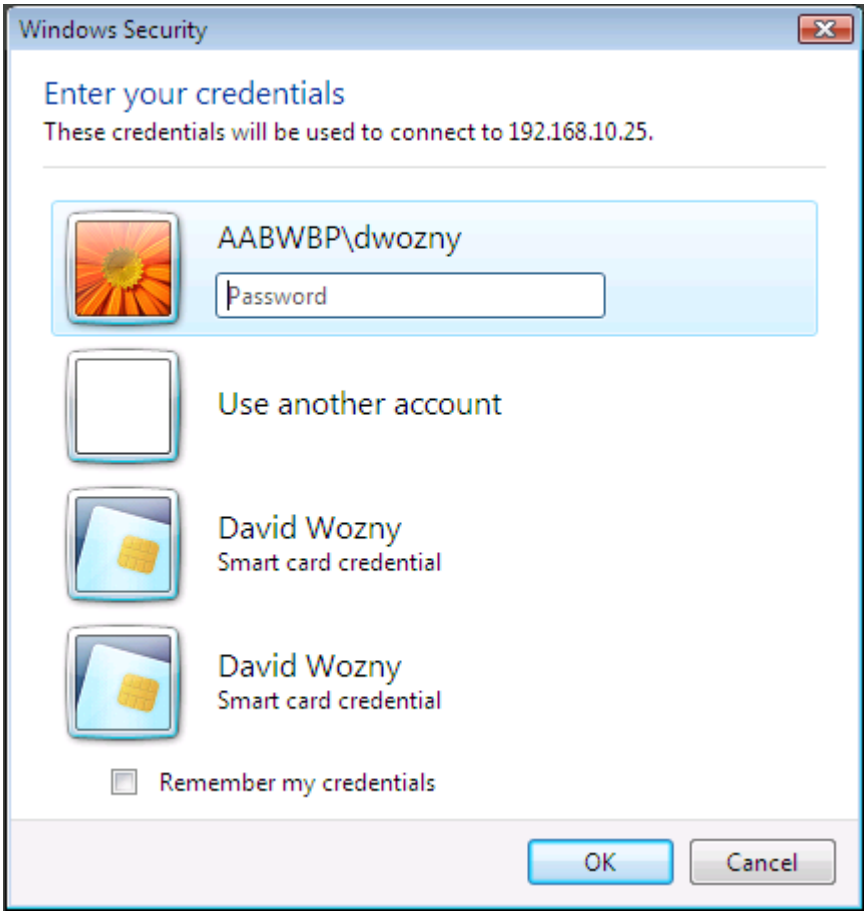

Figure 9: RDC Dual Certificate Selection

With Windows Server 2003 as WBP terminal server logon with SC3-1 (option 5) however failed for the same reason as option 1 and 3: unable to select another certificate on the card. For the same reason option 7 was successful. Card SC3-2 used here, with the WBP certificate in slot 0, circumvent the limitation of Server 2003 terminal server. This leads to the conclusion that although RDC/Vista allows for certificate selection, Windows Server 2003 terminal service can only read the certificate in slot 0 of the card.

Options 6 and 8, with card SC3-1 and SC3-2 respectively, failed against expectation. Again, the Remote Desktop Connection client allows you to select the proper certificate on the card. However logon efforts ended in an error stating that the specified user name does not exist. Where the Vista terminal service from XP (with both RDC v5 and v6) allowed for a successful logon, leads the Vista-to-Vista scenario to confusion and failure.

4.6. Conclusions

Initially this scenario proved to be the most problematic because Vista did not accept smart card logon with the Giesecke & Devrient SmartCafe Expert 64K card using the AET SafeSign middleware. After switching to the Gemalto .NET card using the Base Smart Card CSP hotfix on XP/2003 for enrolment and logon, this limitation disappeared. Note that when Vista or Windows Server 2008 is not used, the G&D card can still be used in this scenario. One conclusion is that Vista/Server 2008 currently limits card selection for unknown reasons.

A Windows XP (COE) workstation limits the flexibility of the solution regarding the order of certificate enrolment and successful interactive logon. The same limitation affects Windows Server 2003 terminal server (WBP). If the terminal server is replaced by Vista you can successful logon to the RDP session, although a bit cumbersome.

With a Vista (COE) workstation the future looks bright since it can logon interactively with both cards. The order of enrolment has become irrelevant. Next, logon to a Server 2003 terminal server shows the same limitation of this operating system: it can only read certificates in slot 0. A Vista terminal server should overcome this, but the Vista-to-Vista combination gets completely lost in the dark.

As stated in the introduction, card management systems are expected to be the most important limitation for a potential implementation.