PKI Design

Author: David Wozny
Department: Enterprise Architecture (via IT Security Solutions)

Version: 0.99
Last update: 31st December 1999
Filename: PKI Design
Project: 70EETRC10151 – PKI Implementation

CONTENTS

1. DOCUMENT CONTROL

1.1. Document History

Version	Date	Reason for Change
0.1	31/12/1999	First draft

1.2. Document Owners

Name	Position	Organisation
AN Other 1	Enterprise Architecture Manager	ABC

1.3. Document Distribution

Name	Position	Organisation
AN Other 2	Project Manager	ABC

2. INTRODUCTION

2.1. Management Summary

A Public Key Infrastructure (PKI) is being implemented into the "ABC IT estate" to provide a capability such that a number of initiatives (which rely upon certificates) presently being considered can successfully be delivered, such as 802.1x authentication of wireless devices.

The implementation of PKI in ABC provides a platform for the uptake of many more services to be delivered "on top of it" in the middle and long term; the PKI for ABC is designed in such a way as to be as flexible as reasonably possible without impacting its principle raison d'être as a security enforcement enabler.

The scope of the ABC PKI is solely for internal use, i.e. within the enterprise boundary and not extending to citizens or external third parties. Some of the more *onerous PKI practices*, such as Certification Practice Statements and Certificate Policies are not implemented in the ABC PKI as there is to be no assertion of non-repudiation or any commercial liability agreements with subscribing parties (i.e. users and computers which request certificates).

2.2. Objective

This document articulates the design of the main components which constitute the PKI capability for ABC and identifies critical impact areas of the ABC PKI on existing systems in the ABC estate.

2.3. Scope Statements

The following elements are within the scope of this document:

- PKI system architecture
- Certification Authority (CA) server design and specification
- Active directory integration
- Revocation status design and publication
- Availability, monitoring and disaster recovery
- Security aspects of the design

The following elements are outside the scope of this document:

- Hardware Security Module (HSM) design and specification
- Design of solutions "leveraging the PKI", such as IEE 802.1x, etc.

3. PKI INTRODUCTION

3.1. Overview

The PKI provides the capability for the issuance x.509 digital certificates to subscribing entities. A digital certificate issued by a trusted Certification Authority (CA) asserts a logical binding between a subject (typically a user or device) and a public key in a cryptographically secure envelope.

A simple two-tier approach has been taken for the ABC PKI, comprising:

- Tier One: Root CA (offline - nominally)
- Tier Two: Issuing CA (online, Active Directory integrated)

This trust model is illustrated in Figure 1.

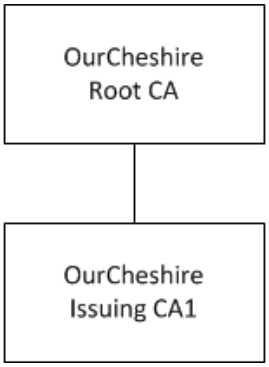

Figure 1: ABC PKI Trust Model

Whilst ensuring that a secure, available, robust and flexible PKI is implemented for ABC, a prime design goal was to not engineer in complexity anywhere that it is not strictly necessary. This design philosophy is reflected in much of the design documented herewith.

Figure 2 illustrates the ABC PKI components and their relationship with infrastructure elements.

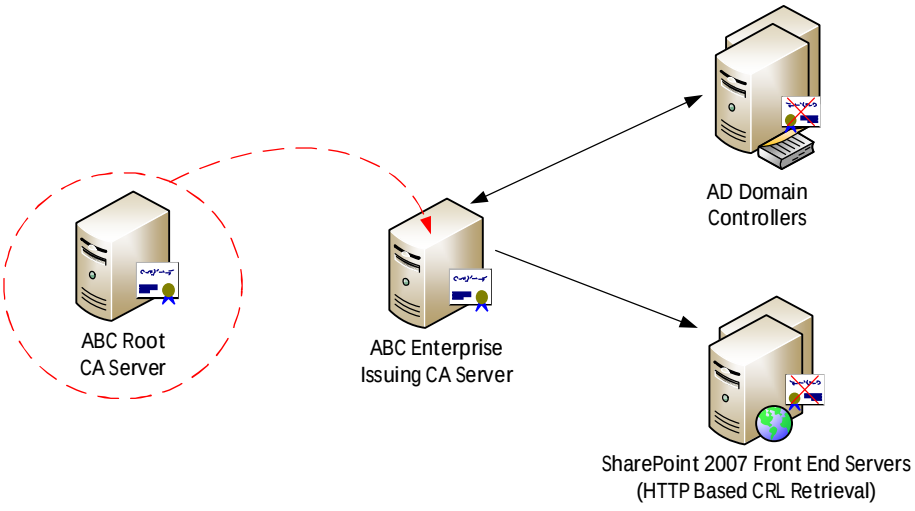

Figure 2: ABC PKI Architectural Overview

The PKI essentially comprises the following principal elements:

- Root CA - trust anchor for the ABC PKI
- Enterprise Issuing CA - issuing the bulk of certificates to end entities
- AD domain controllers - store CA and certificate template definitions, host LDAP CRL distribution points
- SharePoint 2007 Front End Servers - hosting HTTP based Certificate Revocation Lists (CRLs)

3.2. Root CA

A Root CA is deployed as the trust anchor for the ABC PKI; to afford maximum physical security Root CAs are ordinarily deployed offline (physically disconnected from any networks) and located in a secure facility. However, given the medium assurance requirements[1] in scope of the ABC PKI there is not deemed to be justification of extending the complexity and cost to implement dedicated servers or protect sensitive key material (the Root CA's private signing key) with Hardware Security Modules (HSMs).

Further to initial commissioning, the certificates issued by the ABC Root CA (and subordinates) are solely trusted within the ABC IT estate.

The ABC Root CA is implemented on the Windows Server 2008 R2 platform as a standalone CA – i.e. it is not connected to any Active Directory. It is hosted on a VMWare guest which is part of the VMWare ESX 3.5 farm deployed within ABC. The role of the Root CA principally as a trust anchor (it is relatively passive to the on-going operation of the ABC PKI) means that it is ordinarily turned off until such time when it is periodically required to publish a fresh CRL.

3.3. Enterprise Issuing CA

While the Root CA is essentially deployed to establish a trust hierarchy, an enterprise CA implemented on the Active Directory Certificate Services (ADCS) platform is the workhorse of the PKI. Issuing certificates to end entities such as users and devices, the Issuing CAs are deployed subordinate to the Root CA and are fully online. The term enterprise CA and Issuing CA are often used interchangeably in the context of ADCS – the critical emphasis is the distinction of enterprise CAs (which are fully AD integrated, and dependant) and standalone CAs (which have no requirement for AD and typically *sit* on a workgroup joined server).

In ABC, given the potential size of subscriber base there is no justification for any more than a single Enterprise CA to issue certificates to any type of end entity[2] either for performance or availability reasons.

In practical terms, inspection of the certification path of a certificate issued to user entity by the Issuing CA indicates a certificate chain construction as illustrated by the example in Figure 3 (the right hand picture).

The ABC Issuing CA is deployed on the Windows Server 2008 R2 Edition (64-bit) platform.

3.4. Active Directory

Enterprise CAs rely heavily upon (they cannot function without) an Active Directory to store, locate and distribute (using the group policy processing engine) critical supporting PKI elements such as CA certificates and certificate templates. These elements are created in the configuration naming context partition on domain controllers in the forest root domain, and subsequently distributed to all domain controllers within the AD forest. AD is also used by Enterprise CAs to retrieve subscriber subject information, such as User Principal Name (UPN) for injection into user certificates and DNS host name into device certificates.

For clients (servers and workstations) to get maximum value out of Enterprise Signing CAs, it is necessary for them to be domain joined so that material such as certificate templates, CA trust anchors and the like are automatically propagated to them.

<Pictures redacted>

Figure 3: ABC PKI Certificate Chain

[1] The ABC PKI shall not assert non-repudiation or enforce any legal / commercial liability to subscribers / relying parties

[2] Typically users or computers

The AD forest functional level is Windows Server 2003 native, which, whilst being satisfactory to support the principal requirements of the ABC PKI, it does limit extending some of PKI *related* functionality – such as GPO based deployment of wireless 802.1X settings. ABC have updated their AD schema to the latest version (2008 R2) to take advantage of extensions for managing WPA2 settings via group policy and credential roaming in AD (rather than user profiles) for Encrypting File System (EFS) or email encryption (amongst others).

LDAP (AD) is also leveraged as a secondary CDP in the ABC PKI, as described in the following section.

3.5. Revocation Providers

A public key infrastructure must provide a mechanism to enable time valid certificates which are considered untrustworthy (typically due to a lost laptop / stolen smart card, etc.) to be deemed invalid, enabling relying parties to reject them. Revocation status checking is mandatory – if a relying party cannot retrieve revocation status then the certificate presented is deemed untrustworthy.

The ABC PKI solely incorporates Certificate Revocation List (CRL) based revocation providers - Online Certificate Status Protocol (OCSP) is not implemented as there is little justification given the desire to avoid expensive and unessential complexity.

CRLs can be retrieved from both HTTP and LDAP based locations, known as CRL Distribution Points (CDPs).

The primary CDP relates to host-header based web-sites created in Internet Information Services (IIS) on the existing SharePoint 2007 front end servers (Pilar01 and Pilar02); which are accessed via a load balancer.

A secondary CDP based upon LDAP is also available for CRL retrieval in the event that the HTTP CDP is unavailable; it relates to a container in the forest root's configuration naming context which is replicated to all domain controllers in the AD forest.

Whilst Active Directory (LDAP) is a more robust location for a Microsoft Enterprise CA to publish CRLs into (since it is automatic and requires no file transfers), it is preferred to have an HTTP CDP as the primary CDP since it is more universally recognised by relying parties. For example, some relying parties such as firewalls, VPN concentrators, Linux platforms, Oracle applications, may not be able to retrieve CRLs from an Active Directory location.

4. ABC ROOT CA

4.1. Physical Design Overview

The ABC Root CA is deployed on a virtual platform with the specification as detailed in Appendix A: Server Specifications.

During the commissioning of the ABC PKI, the Root CA receives a sub-ordinate CA Certificate Signing Request (CSR) from the ABC Issuing CA.

Once the ABC PKI has been fully commissioned, the Root CA server is powered off until such time as it is required to be operated - ordinarily to publish a CRL which is then published into Active Directory as well as being copied to the HTTP CDP servers on the ABC SharePoint 2007 front end servers. The availability of a fresh (time valid) Root CA CRL is critical for any relying party validating end entity certificates presented to it, as all CA certificates chaining up to the Root CA must be verified.

4.2. Server / Platform Build

4.2.1.Server Hardware

The ABC Root CA is deployed on the ABC VMWare ESX farm as a guest operating system; ESX provides suitable availability such that a failure of the host ordinarily "presenting" the Root CA can easily be presented on another host in the ESX farm.

4.2.2.Disk Storage

The Root CA server has two logical volumes configured:

- (C) hosting the "Windows system"
- (D) hosting the CA database backup, configuration backup and CRLs

4.2.3.Network Connectivity

The Root CA guest operating system has no connectivity to external networks (and all LAN connections are disabled in the guest), transferral of files to / from the Root CA is achieved using VMWare native shared folder type functionality rather than SMB copies over the TCP/IP network.

4.2.4.Operating System Build

The Root CA server is installed on a Windows Server 2008 R2 Standard Edition (64-bit) platform. The server is installed into a workgroup and has non-essential network related services such as Browser, DHCP, DFS, etc. disabled to prevent unnecessary event log noise. "Severe" lockdown measures are not necessary for the Root CA as it is never connected to any network and also it is ordinarily powered down.

There is no requirement for installation of anti-virus software, as the server is not susceptible to viruses due to it never being attached to any networks. Any files / removable media that are introduced to the server are fully virus checked prior to attachment. Generally speaking, the only non-blank media which is introduced to the Root CA server is the certificate signing request of the sub-ordinate Issuing CA.

Prior to installation of the AD CS components the day, time and time-zone is synchronised with a suitable time source. Furthermore, the Windows server is activated with the Microsoft online activation centre using an out-of-band process (via a phone call).

4.2.5.Performance Criteria

The role of a Root CA introduces minimal processor / memory performance criteria for the server; a server which satisfies the "general" specification for Windows Server 2008 R2 is adequate.

Disk storage requirements are also minimal, as it is not expected the CA database will grow by more than say, 10 kilobytes, during its lifetime.

4.3. CA Certificate

4.3.1.Naming

The name of the Root CA deployed in the ABC PKI is:

- OurABC Root CA

Organisational attributes are added to the name such that the full Distinguished Name (DN) is:

- CN=OurABC Root CA, O=ABC, C=GB

4.3.2.CA Signing Key Pair

The Root CA's signing key pair uses an RSA 2,048 bit asymmetric key algorithm – the Root CA's certificate is self-signed (using its own private key). The Root CA's private key is NOT protected by any HSM equipment.

The Windows Server 2008 platform includes a broader suite of cryptographic algorithms than previous Windows Server versions as part of the Cryptography Next Generation (CNG) codebase: such as Elliptic Curve Digital Signing Algorithm (ECDSA) and stronger hashing functions such as SHA-256, etc. Whilst it may sound attractive to select these more advanced crypto suites, they can introduce significant compatibility issues amongst clients such as Windows XP and Windows Server 2003 which don't incorporate CNG. As such, it is deemed sensible to select an algorithm which maintains a practical balance between strength (advanced cryptographic suites) and compatibility / availability; RSA 2,048 with SHA-1 hashing provides this practical balance.

4.3.3.Key Storage Provider

A Key Storage Provider (KSP) is a software module implementing cryptographic functionality, typically including key creation and storage, data hashing and encryption / decryption. A KSP can be implemented entirely in software; alternatively it may act as a wrapper for the cryptographic functionality provided by a hardware cryptographic device such as an HSM. The Windows Server 2008 R2 operating system provides a number of KSPs with the base installation; the KSP employed by the Root CA is the:

- RSA#Microsoft Software Key Storage Provider

4.3.4.Certificate Validity Period

The Root CA certificate has a validity period of twenty years; it is ordinarily renewed at half-life, i.e. every ten years.

The validity period refers to the length of time for which the CA certificate is valid before it expires and needs renewing / rekeying; an organisation deploying a CA certificate must be confident that given present advice it won't be compromised during its lifetime.

The maximum validity period of certificates issued by the Root CA is ten years; this sets the CA certificate validity period of the ABC Issuing CA.

4.4. Revocation

4.4.1.Introduction

All CAs publish CRLs relating to certificates they have issued; the CRL for each CA in a certificate chain must be available for application revocation checking as each certificate in the chain of trust is checked for its revocation status - from end entity certificate all the way to a trusted root.

When a Root CA is installed it is important that its self-signed certificate does not contain any CRL checking references; in practice this is achieved by specifying an empty CRL Distribution Point (CDP). A Root CA certificate is self-signed and therefore does not appear on any CRL issued by a parent CA (there isn't one).

The Root CA does however, need to publish a CRL to support revocation of any certificates it issues, i.e. Issuing CA certificates. Although the Root CA server is disconnected from the ABC IT network, it is still necessary to publish its CRL to locations that are accessible to any relying parties.

Revocation of the Issuing CA certificate would be considered extremely rare (this would only realistically need to be done if the Issuing CA was compromised) and hence it is appropriate to publish the CRL on a relatively infrequent basis.

4.4.2.Validity Period and CRL File Publication

The Root CA CRL is designated a validity period of fifty-two weeks, this period commences at the point of issuance of the CRL. The rationale of a fifty-two week validity period is to allow scheduled re-publication on a yearly basis. An overlap of ten weeks is factored into the CRL validity period to provide some contingency in the event of a problem being apparent when publishing the CRL. The characteristics affecting the CRL validity period are illustrated in Figure 4.

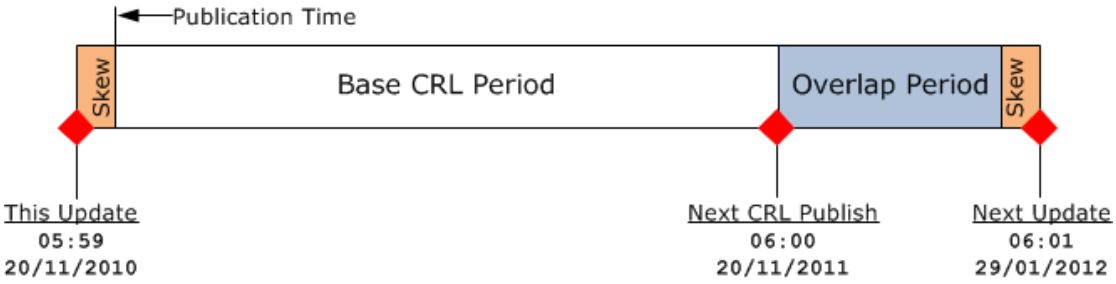

Figure 4: CRL Validity Period Illustration

The "This Update" and "Next Update" extensions effectively form the time boundary around the validity period of a CRL. The overlap extends the validity period of the CRL, such that if the CRL isn't republished prior to its base validity period expiring, it is still valid for a further ten weeks

Microsoft Windows relying parties (such as AD DCs) cache retrieved CRLs for performance reasons. The CRL is cached until the Next CRL Publish threshold is reached; at this point it attempts to retrieve a fresh CRL even though there is still outstanding balance (overlap) remaining on the cached CRL. If a fresh CRL cannot be retrieved, the cached CRL is still valid until the Next Update is reached. Publishing a fresh CRL after a certificate is revoked won't have any immediate impact on the availability of that revocation status to a relying party. Cached CRLs can be a hindrance to effecting rapid certificate revocation status at relying parties and clear understanding of relying party caching is important to ensure that desired revocation behaviour is achieved.

The CRL is published automatically to two file based URLs on the Root CA server, however, these URLs are not included in issued certificates' CDP extensions and hence any relying party does not attempt to retrieve CRLs from these locations when validating certificate chains. The file based URL paths are shown below:

- `C:\Windows\System32\Certsrv\CertEnroll`
- `D:\IDP`

The time characteristics of the Root CA CRL are shown in Table 1.

Characteristic	Value
Base Validity Period	52 Weeks
Base CRL Overlap Period	10 Weeks
Delta CRL Validity Period	0 Minutes (i.e. not applicable)
Clock Skew	1 Minute

Table 1: Root CA CRL Characteristics

4.4.3.CRL Distribution Point Extensions

The CRL published by the Root CA contains two CDP extensions, which are used by relying parties to identify where they can retrieve CRLs from. These CDPs are published into the CDP extension of the CA certificate issued by the Root CA to the Issuing CA.

"Windows" Relying parties attempt to retrieve CRLs from CDPs in order, fifteen seconds is allowed for retrieval of the CRL from the first CDP – if this is not possible, then the second CDP is attempted. Each relying party has a distinct CRL caching policy such that, for example, a Network Policy Server (NPS) server validating WPA2 presented certificates may cache CRLs for their authoritative period whereas other relying parties – such as a firewall, may not cache CRLs at all.

The primary CDP uses an HTTP URL as this protocol is universally recognised by applications and disassociates any reliance on relying parties to "reach into" Active Directory. The secondary CDP uses an LDAP URL related to the ABC AD DNS namespace.

Primary CDP (HTTP)

The primary CDP resolves to an HTTP based entry that is hosted on the ABC SharePoint 2007 front end servers:

- `http://pki.ourABC.abcusers.com/idp/OurABC Root CA.crl`

The IDP path relates to a directory sub-containers configured on the host-header based web-site configured on the two SharePoint 2007 front end servers. The Barracuda network load balancing capability employed in the ABC estate is used, with a new "`PKI`" DNS A record created which corresponds to the virtual TCP/IP address published on the load balancer for the HTTP CDP service.

Secondary CDP (LDAP)

The secondary CDP uses an LDAP URL related to the ABC AD DNS namespace. Whilst using an LDAP URL does not provide the most universal method for retrieving CRLs, it does provide a failback CDP in the event that the HTTP CDP is for whatever reason unavailable.

- `ldap:///CN=OurABC Root CA,CN=ROOTCA,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=ourABC,DC=abcusers, DC=com`

This URL relates to the publication of the CRL into the configuration naming context of the ABC AD in the forest root domain.

The LDAP CDP uses a syntax that enables relying parties to retrieve a CRL from the nearest available LDAP server (AD CS domain controller), rather than explicitly specifying a host – this is often referred to as "serverless binding". By way of explanation…

- `ldap:///CN=…,CN=…`

is interpreted as…

- `ldap://Closest Domain Controller By Site/CN=…,CN=…`

It should be noted that this syntax is generally only resolvable by Microsoft relying parties.

4.4.4.CRL Publication

As previously stated, publication of the Root CA CRL is ordinarily only necessary on an annual basis, after the CRL is manually issued after starting up the Root CA server.

The mechanism for transferring the CRL to the HTTP CDP locations is by first using native VMWare tools to copy it onto the host server, and then transfer the CRL to a staging area on the Issuing CA server.

An automated promulgation task using RoboCopy (described in Section 5.4.5) transfers the fresh Root CA CRL to the appropriate locations on the ABC SharePoint 2007 front end servers; a manual process of copying the CRL into AD is undertaken by running a suitable AD directory services publication command.

4.5. Authority Information Access

4.5.1.AIA Distribution Points

The Authority Information Access (AIA) extension enables a relying party to obtain a current copy of the CA certificate of the CA which issued the certificate being validated. For example, if an Issuing CA certificate is being inspected the AIA contains the location from where to retrieve the Root CA's certificate.

For the same reasons as specified for the CDP, the AIA employs two URLs, these are shown below:

Primary AIA (HTTP)

- `http://pki.ourABC.abcusers.com/idp/ROOTCA_OurABC Root CA.crt`

Secondary AIA (LDAP)

- `ldap:///CN=OurABC Root CA,CN=AIA,CN=Public Key Services, CN=Services,CN=Configuration,DC=ourABC,DC=abcusers,DC=com`

4.5.2.AIA Certificate Publication

The Root CA's certificate is published to the aforementioned locations during commissioning. There is no requirement for any maintenance to be performed until such time as the Root CA's certificate is due for renewal; at which time the renewed CA certificate is re-published to the above locations.

The AIA path is embedded in the CA certificates issued by the Root CA to the Issuing CA.

4.6. Backup

4.6.1.Introduction

The following components of the Root CA are backed up (or replicas made) to ensure continuity of the system:

- System snapshot
- AD CS CA database
- Root CA private key

4.6.2.System Snapshot

A snapshot of the VMWare image containing the ROOTCA “disk files” is taken after the ROOTCA is operated on an annual basis, the disk files are saved into a secure partition on the DELICIA server in the forest root domain.

4.6.3.AD CS CA Database

Following commissioning, and at every instance when the Root CA is operated to re-publish its CRL a manual process of backing up the CA database is performed.

The database is backed up to the following file system location:

- `D:\CA-Backups\%1`

Where %1 represents the date the backup was taken, e.g. 2010.03.13, 2010.09.13, etc.

4.6.4.CA Private Key

A backup of the Root CA server's private key is stored in a Private Key Exchange File (PFX) located on the AC server’s D-drive.

4.6.5.Combined Backup

The AD CS CA database backup file and the CA private key file are combined into a single backup archive (zip) file on the Root CA and transferred using the VMWare floppy disk image tool onto a secure partition on the DELICIA server in the forest root domain.

4.6.6.Recovery Approach

Rather than attempt to do a "full system" type restore, the recovery approach taken for the Root CA is to do a component by component restore. This approach means that a single process can be employed whatever the disaster circumstance encountered, and is also the same process that will be used to migrate the Root CA onto a different hardware / Windows platform in the future - if and when needed.

A simple overview of the recovery process is described here:

1. Install Windows Server onto the server
2. Copy all the files from the backup CD into corresponding locations on the server
3. Install the CA certificate and private key (using the PFX file)
4. Install ADCS, specifying an existing certificate and private key
5. Run an existing configuration script to set CDP / AIA paths, etc.
6. Perform a CA database restore from the latest backup

4.7. Audit Policy and Availability

4.7.1.Audit Policy

All CA audit categories on the Root CA server are activated.

4.7.2.Availability

There are no high availability requirements as such for the Root CA, given that it is ordinarily offline.

The routine operation of the Root CA (to publish a CRL) is planned to always be executed a minimum of ten weeks prior to a publication failure becoming critical. In practical terms, this means that in the event of a problem becoming apparent at the Root CA, there is a period of ten weeks to remedy the fault by a server restore / rebuild, etc.

4.8. Operator Access and Security

For operator access to the Root CA there is a requirement for two parties (users) to provide different components of the system password which is used to logon. A single user account (administrator) is used which possesses all possible permissions for the CA.

Although best practice generally dictates that user accounts should be directly attributable to persons, the Root CA server is a special case, and the corresponding key ceremony documentation pertaining to its operation will record the names of the persons participating in the logon.