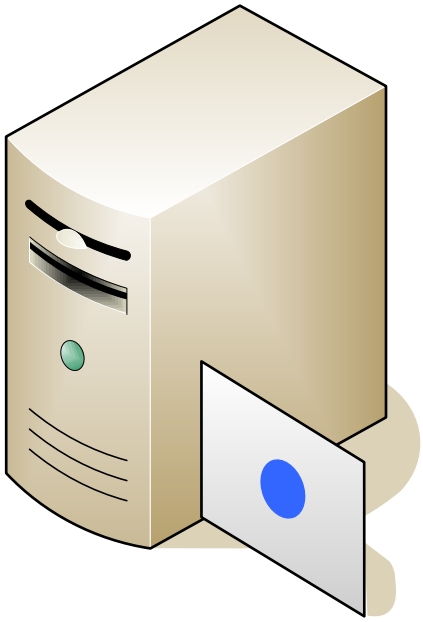
LSU PKI Architecture

LOUISIANA STATE UNIVERSITY



6 July 2006
Version 36

Prepared by
John Morello, CISSP
Deputy Information Security Officer
morello@lsu.edu

Table of Contents

1 Executive Summary

LSU A&M in Baton Rouge is faced with many of the same IT security challenges as other peer institutions in higher education. For example, concerns about safeguarding student information, protecting against malicious users, and providing a safe campus computing environment must be balanced against the concept of academic openness and having a diverse set of users and needs on campus. There are many IT security tools that can assist institutions like LSU in achieving their goals and one of them is the use of Public Key Infrastructure (PKI). A PKI provides LSU with a flexible, extensible foundation that it can leverage to solve many IT security problems. In April of 2006 LSU A&M in Baton Rouge began evaluating technical architectures for its PKI. The model that we chose uses a certificate authority (CA) running locally in our computing center, but one that issues certificates that are globally trusted across the internet. This global trust comes from a newly entered-into contract with Cybertrust, which certifies our CA and allows it to chain through their globally trusted root. This document describes the overall technical architecture designed for LSU. A companion document, the LSU PKI Deployment and Operations Guide, describes the processes used to commission and manage the PKI.

1.1 What is a PKI?

A Public Key Infrastructure is an enabling, foundational technology that allows organizations to build security solutions that leverage a common trust. The PKI provides an organization with the facility to create, distribute, and manage keys used by computers and users. These keys can be used for business functions such as sending secure email, encrypting data on disks to protect against loss or theft, and securing communications, such as with virtual private networks (VPNs). The PKI approach separates the management of the keys from their use, allowing an organization to leverage the infrastructure for a variety of different uses that would otherwise require separate infrastructure components. Because of this, the PKI can help organizations operate more securely and at lower costs over the long term.

1.2 What is a PKI not?

A PKI is not an all encompassing solution to an organization's security challenges. For example, deploying a PKI will not solve patch management problems, nor correct poor passwords, nor cure virus infections. A PKI may be leveraged to assist in each of these areas but it is not, in and of itself, a solution to any of them. Rather, think of a PKI as a reusable framework that can help free an organization from having to implement point security solutions that are difficult to manage and integrate. For example, today LSU purchases certificates for use on its various websites in an isolated fashion. While these certificates enable secure web browsing to its web properties, they are isolated in the sense that they require their own key generation, distribution, and revocation facilities. With an LSU PKI present, that common framework for key management could be leveraged for not only SSL, but also for disk encryption, application security, secure email, and other uses. This commonality allows LSU to leverage an efficiency of scale; by using a PKI, the organization can use a single management and technical methodology to satisfy many business needs.

1.3 What does this document describe?

This document outlines the overall architecture and technical approach used to implement PKI within the LSU environment. This design is based on industry, LSU, Cybertrust, and Microsoft standard best practices for securely deploying and managing certificate services.

2 Introduction

2.1 Document Purpose

This document describes the design of LSU's certificate issuance and management systems. It is intended to assist application developers and systems administrators that wish to leverage LSU's PKI.

The intended audience of this document is:

- LSU A&M Information Technology Services (ITS) technical staff
- LSU System technical staff
- Any vendor or third party that LSU requests to integrate with the system

2.2 Document Scope

- Physical infrastructure
- Logical infrastructure
- Technologies used
- High level configuration

2.3 Exclusions

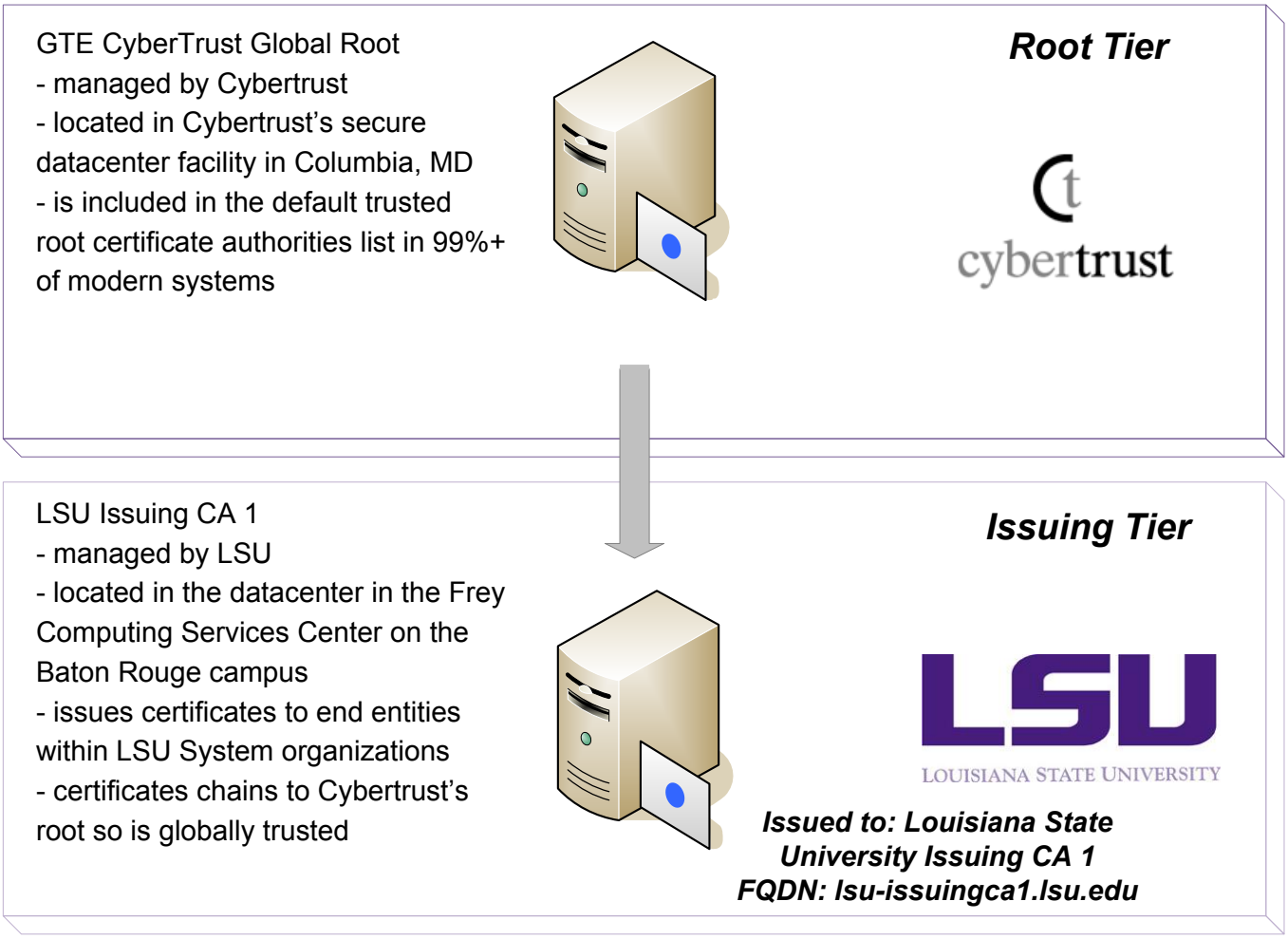
This document specifically excludes the following:

- Application design or integration questions, beyond a discussion of the standards and interfaces supported by the PKI
- Deployment or operational details, which are provided in a companion document, the LSU PKI Deployment and Operations Guide
- Development of a Certificate Practices Statement or Certificate Policy; by participating in Cybertrust's OmniRoot program, we are bound by their CPS

3 Architecture

The certificate authority (CA) hierarchy utilizes a two tier design, with a root tier managed by Cybertrust and an online issuing CA run at LSU. This design fulfils all stated goals for the project, provides immediate capability for SSL certificates, and provides significant capacity for future needs LSU may wish to use the system for.

The root tier forms the core trust anchor in the hierarchy. In other words, the trust relationship of all certificates issued by a CA in the hierarchy eventually chain up to the root CA. The root CA forms the common bond between all CAs and certificates in the hierarchy. The root CA issues certificates only to issuing CAs that have demonstrated compliance with its security and certificate policies. Cybertrust manages the root CA in one of its secure hosting facilities.



The issuing CA is online and available on the network. This is an end entity facing system responsible for providing certificates to the LSU's user and machine population. Its certificate is signed by the Cybertrust CA above it in the hierarchy and it issues certificates that chain through itself to the Cybertrust root CA.

From a growth standpoint, LSU can easily add additional capacity to the hierarchy by simply commissioning new enterprise CAs following the same process used in this project. While it is unlikely that LSU will outgrow the hardware capabilities provided by the server in the initial design (at least not within the 3 year lifecycle anticipated for

it), LSU may wish to host a CA offsite for disaster recovery purposes. If this need arises, LSU again need only follow the provisioning process from this design, and can place CAs at any remote datacenter location it desires.

3.1 Qualified Subordination

Qualified subordination allows cross-certification of CA certificates with name constraints and provides for more precise control of certificate trusts. With qualified subordination, LSU can include or exclude certificate purposes or naming suffixes when federating with other entities. This design does not utilize qualified subordination to constrain the types of certificates that can be used within the hierarchy. If, in the future, LSU wishes to federate its PKI with another organization, such as the Higher Education PKI (HEPKI) efforts ongoing at Educause and Internet2, qualified subordination and cross certification could be used to facilitate this integration.

3.2 CA Operating System

There are numerous new capabilities in the Windows Server 2003 Certificate Authority service, including key archival, delta CRLs, and version 2 templates. LSU chose to use Windows Server 2003, Enterprise Edition with Service Pack 1 as the operating system for its issuing CA. Each instance of Windows used as an issuing CA is built according to the standard LSU Windows server build policy and updated with all relevant security updates. It is managed using the standard LSU change management practices and software inventory and update tools. Because this server is available on the production network, it is maintained with all critical updates and service packs.

3.3 CA Server Hardware

Microsoft performance testing has shown that the signing key length of the CA has the most significant impact on the potential enrollment rate of the CA. A larger number of certificates can be signed and enrolled in a given time if a smaller key size is used. If a larger key size is used, more CPU time is required to issue each certificate. The total number of issued certificates should not have a significant influence on either server performance or the rate at which the CA issues certificates; the performance of the issuing CA stays nearly the same whether thousands or millions of certificates have previously been issued. Therefore, the scalability of the CA is considered to be linear, based on the size and performance of the disk arrays that are used to store both the database and log files.
The following table describes hardware resources and the comments on their state in LSU's infrastructure, with significant ceiling provided for future growth. The LSU Internal Issuing CA is built on an IBM xSeries 346 server, with dual 3.2GHz Intel Xeon processors, 4GB of RAM, and at more than 100GB of high performance disk space.

Resource	Notes	Analysis
Number of CPUs	Additional CPUs increase the overall performance of the CA. This is the most critical resource for a Windows Server 2003 CA during certificate creation.	The base LSU server standard meets the CPU needs of a CA. Additionally, since LSU will be using a hardware security module, the CPUs will not likely be a performance factor.
Memory	In general, additional memory does not have a significant role in the enrollment performance of the CA. The CA should meet general recommended system requirements (512 MB), however, the minimum amount of memory is 256 MB.	The base LSU server standard meets the RAM needs of a CA.

Disk size	The capacity of the disk volume that stores the database and log files is the primary limiting factor for the number of certificates that a CA is able to maintain. Each certificate that is issued uses approximately 16 KB of disk space in the database, and an additional 4 KB is required if the private key is archived. The certificate database must contain all of the issued certificates to be able to revoke certificates and provide a record of operations. Because none of the records are ever automatically tombstoned or automatically deleted, the certificate database continuously increases in size when new certificates are issued. Nevertheless a CA administrator can use the certutil.exe command-line utility to delete expired records from the CA database. The Windows Server 2003 CA has been tested to issue more than 35 million certificates on a single four-processor, Intel-based computer. The maximum database size was not reached in the test scenarios.	The base LSU server standard meets the disk space needs of a CA. If, over time, the CAs require greater disk capacity than present at install time, their capacity can be increased by adding more disks to the system. LSU Issuing CA 1 is configured with 5 146GB 15000 RPM SCSI attached disks. They are split into 2 RAID1 arrays, with a shared hot spare. Each array is formatted as a single NTFS partition. Array 0 is represented in Windows as the C: drive and contains the operating system binaries and the CA database. Array 1 is the D: drive and contains the CA database log files.
Key length	The larger the signature key length, the greater the CPU utilization. Larger keys degrade CA performance. To be CPU-independent, organizations may consider hardware acceleration to provide a large number of both key generation and signing operations.	LSU will be using hardware security modules for all CAs.
Bandwidth	A 100 megabit network connection is suitable to enroll a large number of certificates and causes no performance bottleneck, assuming that the server is running the CA exclusively with no additional applications or network services.	The current LSU network is capable of servicing certificate request network demand.

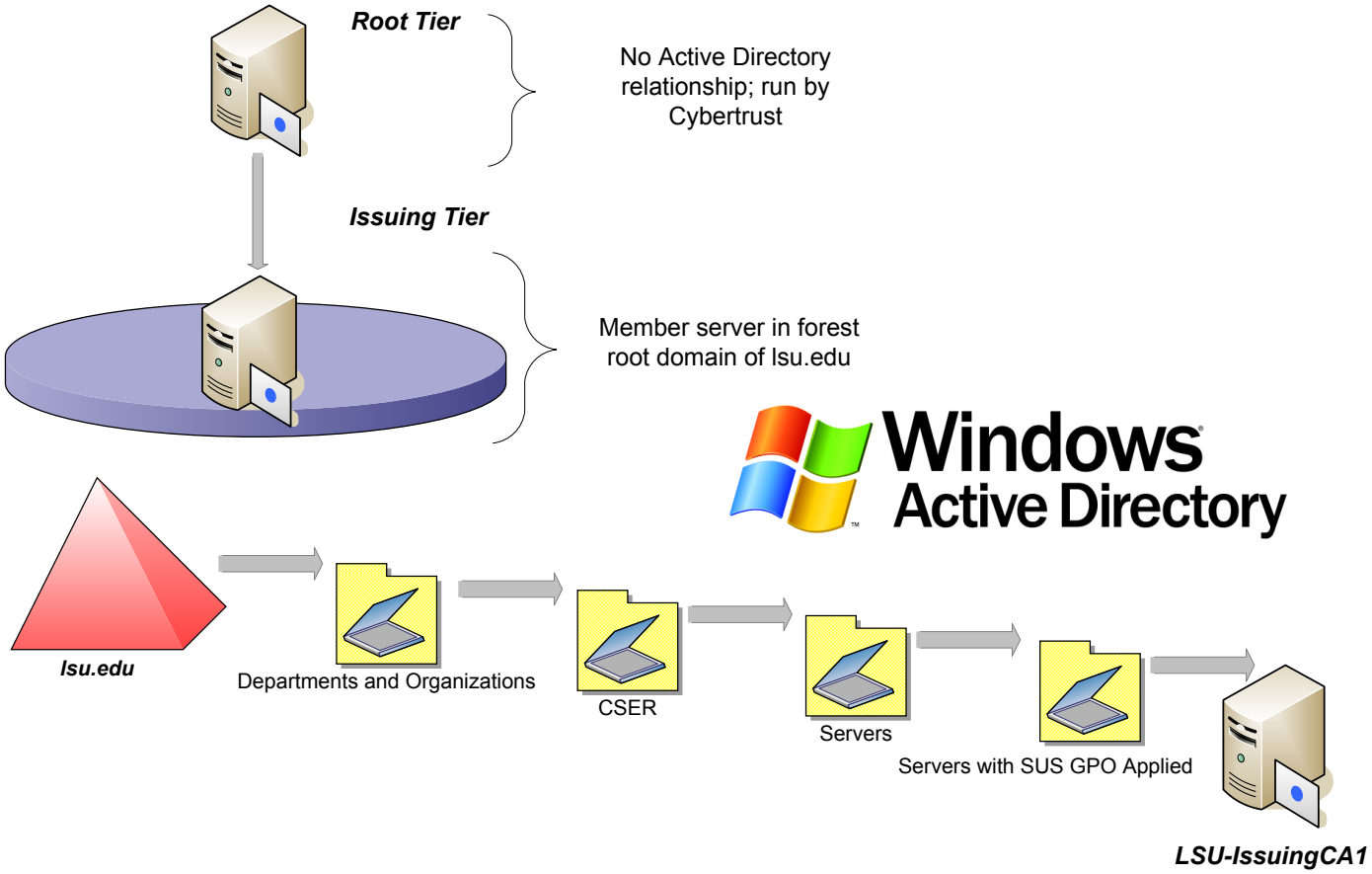
3.4 CA Availability

When considering redundancy within the PKI, it is important to keep in mind that clients will only need to communicate with a CA during certificate issuance and certificate renewal. Certificate users do not contact the CA on an ongoing basis and do not require its availability to utilize certificates it has issued. As such, even in a worst case scenario where LSU's CA was completely offline, the user impact should be minimal (assuming service is restored prior to the end of the CRLs' validity lifetime), as the only failures from this scenario would be users or computers that need to have certificates created or renewed. Existing users or machines with currently valid certificates would likely not even be aware of the outage.

That said, to a large extent, the Windows PKI is automatically redundant. Information about certificate templates, the names of CA, authentication against those CAs, and CRL distribution points are all provided by Active Directory. In the initial LSU design, there is a single issuing CA online. If LSU requires additional capacity over time, or wishes to host CA services in other datacenters, we simply need to follow the process outlined in the deployment guide to provision an additional issuing CA.

3.5 Active Directory Considerations

Organizations can operate a Windows Server 2003 enterprise CA if all domain controllers in the Active Directory are running Windows 2000 SP3 or later. Windows 2000 SP3 domain controllers are the minimum version required to support the schema upgrade for Windows Server 2003 PKI capabilities. The schema upgrade is required to add additional template information, key archival information, cross-certificate objects, and object identifier (also known as OID) objects in the directory. LSU's Active Directory environment was already prepared to integrate with a Windows Server 2003 enterprise CA because its schema was already running the Windows Server 2003 schema and all domain controllers were already running at least Windows 2000 SP3.



3.6 Operational Management

LSU's CA, being hosted in a Windows Active Directory environment, will utilize the existing support resources for server management. However, role-separation controls will be in effect between server management and certificate management functions. The Networking, Infrastructure, and Research (NIR) back office team will be responsible for managing the server hardware, network connectivity, and base operating system. The IT Security and Policy team will have exclusive management responsibility to the hardware security module and the Certificate

Authority operations. The IT Security and Policy Office will be responsible for:

- Certificate Authority and HSM operation
- Validation and approval for all digital certificate requests
- Revocation of digital certificates based on authorized request or proven incident
- Certificate Authority alert management
- Interaction with the server management team in “cross-over” support cases for the server (e.g. patching, OS upgrades, hardware replacement)

3.7 Certificate Practice Statement

A certificate practice statement (CPS) is commonly defined as a statement about the way that a CA issues certificates. A CPS might include the following types of information:

- Positive identification of the CA, including the CA name, server name, and Domain Name System (DNS) address
- Certificate policies that are implemented by the CA and the certificate types that are issued
- Policies, procedures, and processes for issuing, renewing, and recovering certificates
- Cryptographic algorithms, cryptographic service providers (CSPs), and the key length that is used for the CA certificate

As part of the OmniRoot program, LSU operates its CA in accordance with the Cybertrust CPS. The Issuer Statement field in each certificate LSU issues will be pointed to the www.lsu.edu/pki web site, which can add any additional relevant information prior to pointing to Cybertrust’s CPS.

4 Security Design

4.1 Hardware Security Modules

An HSM (Hardware Security Module) is a dedicated hardware device that is managed separately from the operating system. These modules work with servers to provide a secure hardware store for CA keys. From an operating system view through the CryptoAPI interfaces, the HSM is seen as a cryptographic service provider (CSP) device. The HSM provides highly secure operational management that is protected by multilayered hardware and software tokens, as well as a number of other key features, including:

- Hardware-based, cryptographic operations, such as random number generation, key generation, and digital signatures, as well as key archival and recovery.
- Hardware protection of valuable private keys that are used to secure asymmetric cryptographic operations.
- Secure management of private keys.
- Acceleration of cryptographic operations, which relieves the host server of having to perform processor-intensive, cryptographic calculations.

In the LSU design, an nCipher nShield (500 Transactions Per Second model) is used as a directly attached HSM. The HSM is a FIPS 140-2 level 3 device and support K of N protection of the keying material. The HSM provides significant protection against compromise of the private keys, as an attacker would need to possess both the HSM storage as well as a defined number of access tokens and their PINs (the 'K' in 'K of N') to access the key. It is critical to note that HSMs are designed to prevent malicious parties from tampering with their contents. Thus, they strictly enforce a limit on consecutive failed logon attempts. In LSU's design, after 10 consecutive failed attempts, the storage is irrevocably erased.

4.2 Physical Security

As with any sensitive information asset, the certificate authorities should be kept in a physically secure datacenter. The designed LSU architecture fulfils this requirement by keeping the online issuing CA in the existing LSU datacenter at the Frey Computing Services Center on the Baton Rouge campus and utilizing the strong physical controls already present there. These controls include card key access and video surveillance.

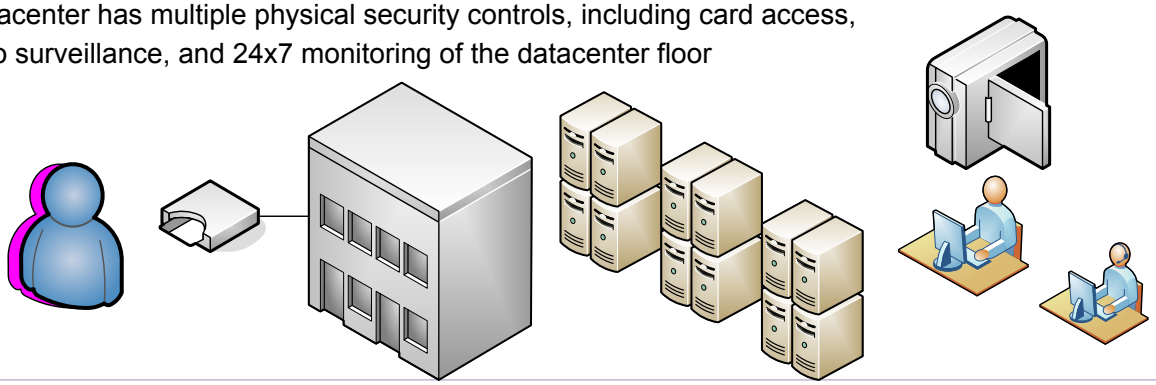
Root Tier

GTE CyberTrust Global Root
- managed by Cybertrust
- physical design has no impact to LSU's implementation

Issuing Tier

LSU Issuing CA 1
- run on IBM x346 2U server in Frey datacenter
- uses nCipher nShield 500TPS HSM
- runs Windows Server 2003 EE SP1

- datacenter has multiple physical security controls, including card access, video surveillance, and 24x7 monitoring of the datacenter floor



4.3 Installation User Rights

On a server that is a domain member, such as the issuing CAs, the user who installs an enterprise CA must be a member of the Active Directory root Domain Admins and Enterprise Admins security groups. This set of permissions is required for any enterprise CA installation, and it assumes that the Enterprise Admins group or Domain Admins group also is a member of the local server Administrators group. Forest wide administrative privileges are required because CA information is stored in the Sites and Services container in the directory; a forest wide container. The Active Directory team in LSU's Networking, Infrastructure, and Research IT Enablement group will perform the initial installation of the CA.

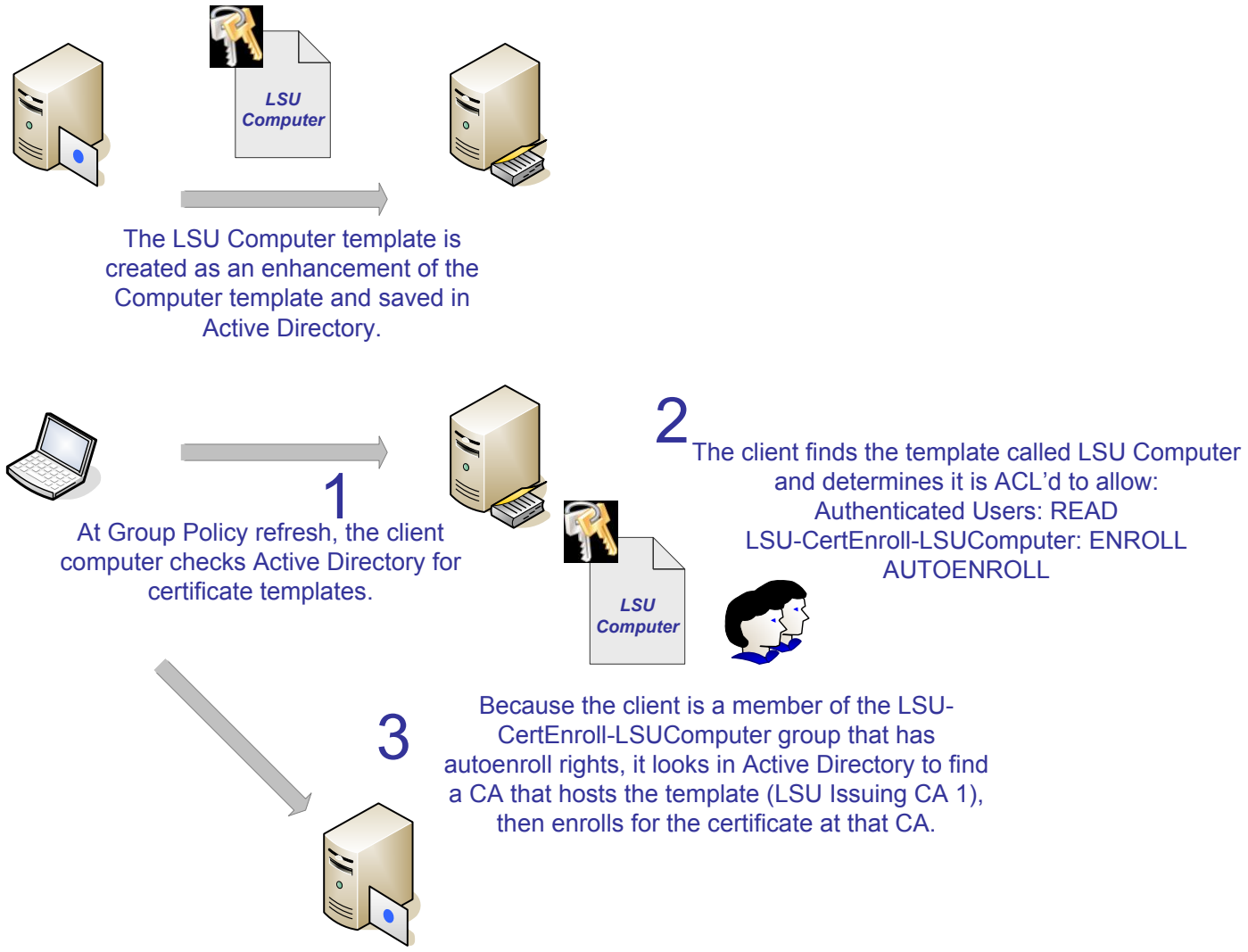
4.4 Authentication and Authorization

A CA running Windows Server 2003, Enterprise Edition uses DCOM and Kerberos impersonation for authenticating requesters. It compares the client token against an access control list (ACL) set on the certificate template, as well as the DCOM enrollment interface on the CA itself, when a certificate is requested. This allows LSU to create

templates that only certain users or computers, based on normal Windows group membership, have access to.

All systems or users that enroll for certificates via autoenrollment must be members of LSU's Active Directory (lsu.edu). All requests for certificates for users or computers that are not part of LSU's Active Directory will be made through an SSL encrypted web portal. This portal will authenticate users against their Active Directory accounts and provide a self service mechanism for requesting and obtaining certificates. For users from other LSU System organizations, LSU A&M will create a 'sponsored' account for them within the Active Directory expressly for certificate management functionality. These accounts will be created, maintained, and subject to the same requirements as existing sponsored accounts.

The following diagram illustrates how autoenrollment occurs within LSU's PKI.



4.5 Auditing

LSU's certificate authority will log important events as they occur within the environment. Specifically:

- Backup and restores of any key data
- CA configuration changes

- CA security or rights changes
- The actions of issuing, managing or revoking certificates
- Key storage and key retrieval
- Server/service start and stop

The IT Security and Policy Office will be the primary recipient of these logs and will act on them as necessary. These logs will be kept for 30 days, except in cases where the Office determines greater retention lengths are necessary. As part of the OmniRoot program, Cybertrust may request an audit of the LSU Issuing CA in rare cases, such as if a system compromised is suspected. Cybertrust has agreed that if such an event should ever occur, LSU could utilize the IT auditing group from the LSU System office to perform the assessment.

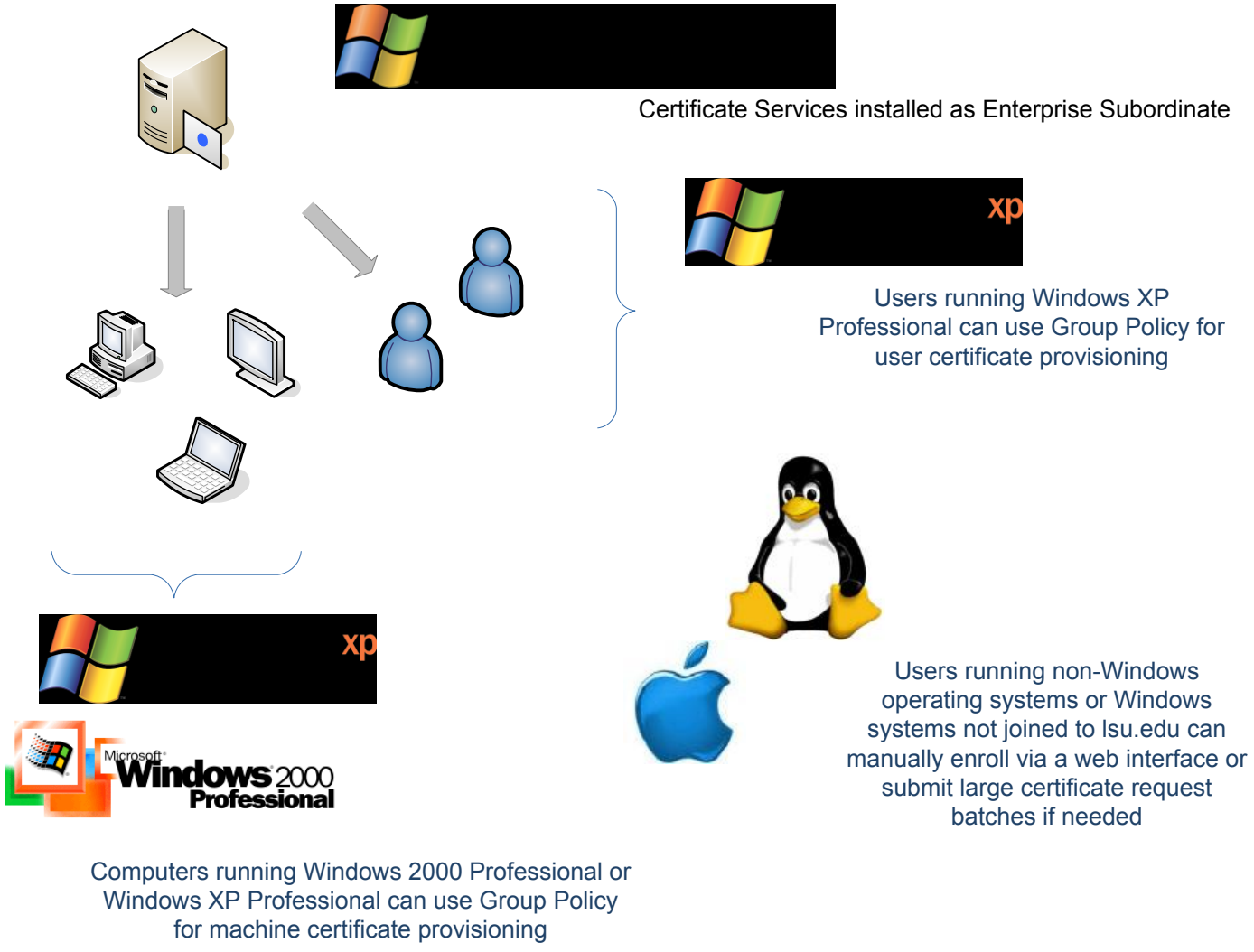
4.6 CA Key Lengths and Lifetimes

The following table describes key lifetimes and private key renewal strategies in LSU's environment.

Purpose of Certificate	Key Length	Certificate Life	Private Key Renewal Strategy
Root CA (top tier managed by Cybertrust in LSU's PKI)	4096 bits	Managed by Cybertrust, no efforts required by LSU.	
Issuing CAs (bottom tier in LSU's PKI)	2048 bits	7 years	Renew every 5 years.
End entities	1024-2048 bits	1 month – 1 year	Renewal at half the certificate lifetime

5 Enrollment Strategy

One of the primary benefits of a Windows based PKI is the fact that certificate provisioning is accomplished without the need to install additional software on entities that participate in the PKI. Rather, through a combination of autoenrollment and Group Policy, all certificate provisioning is managed autonomously and invisibly to the end user. LSU will utilize this technology to automatically distribute machine certificates to computers that are members of its Active Directory (the forest named lsu.edu). The following diagram illustrates the enrollment capabilities of various operating systems.



5.1 Certificate Template Design

LSU will initially only make a few certificate templates available on its issuing CAs. One is a computer certificate template that will enable machine enrollment for certificates to enable IPSec, 802.1x and other computer authentication and encryption capabilities. Others include templates for SSL and for IPSec on non-Windows systems. By default, the first enterprise CA added to a forest loads a number of pre-defined certificate templates. This default behavior is reversed in the LSU deployment such that all certificate templates are removed from the

issuing CAs after deployment. Instead, LSU will manually create and add the needed templates, ensuring that at no point during the deployment can a user or machine enroll for a certificate other than those expressly approved by LSU. The LSU Computer certificate template is based on the default Windows "Computer" template and has the following attributes:

Attribute	Description	Value
distinguishedName	The DN of the template.	LSUComputer
dsiplayName	The name displayed in the MMC.	LSU Computer
pkiExpirationPeriod	The validity lifetime of the cert.	6 Months
pkiOverlapPeriod	The renewal period of the cert.	3 Months
pkiDefaultCSPs	The default CSP used by clients during enrollment.	Microsoft RSA SChannel Cryptographic Provider
msPKI-RA-Signature	Number of RA signatures required on a request referencing this template.	0
msPKI-Minimal-Key-Size	Minimal key size required.	1024
msPKI-Template-Cert-Template-OID	OID of this template.	Deployment dependent
msPKI-Supersede-Templates	Name of the template that this template supersedes.	N/A
msPKI-RA-Policies	RA issuer policy OIDs required.	N/A
msPKI-RA-Application-Policies	RA application policy OIDs required.	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
msPKI- Certificate Policy	The Certificate issuer policy OIDs are placed in the OID_CERT_POLICIES extension by the policy module.	N/A
msPKI- Certificate -Application-Policy	Certificate application policy OIDs.	N/A

The OmniRoot program distinguishes between certificates whose uses are public and those whose uses are internal. Certificates are considered public if they are utilized by systems and users that are not part of the LSU organization, such as a prospective student submitting their application through an SSL secured website. Other certificates, which are used within the LSU organization, such as those used to encrypt data on LSU's servers or for IPSec, are considered internal.

Because the cost of the OmniRoot program is based on the number of publicly facing certificates, it's important that we be able to easily track how many public certificates are issued and to whom. Thus, for any certificate whose purpose is public, the distinguished name of the template will begin with *PublicCertificate* and the display name will begin with *(Public Certificate)*. For example, the publicly facing LSU SSL certificate template is based on the default Windows "Web Server" template and will have the following attributes.

Attribute	Description	Value

distinguishedName	The DN of the template.	PublicCertificateLSUWebServer
dsiplayName	The name displayed in the MMC.	(Public Certificate) LSU Web Server
pkiExpirationPeriod	The validity lifetime of the cert.	1 Year
pkiOverlapPeriod	The renewal period of the cert.	3 Months
pkiDefaultCSPs	The default CSP used by clients during enrollment.	Microsoft RSA SChannel Cryptographic Provider
msPKI-RA-Signature	Number of RA signatures required on a request referencing this template.	0
msPKI-Minimal-Key-Size	Minimal key size required.	2048
msPKI-Template-Cert-Template-OID	OID of this template.	Deployment dependent
msPKI-Supersede-Templates	Name of the template that this template supersedes.	N/A
msPKI-RA-Policies	RA issuer policy OIDs required.	N/A
msPKI-RA-Application-Policies	RA application policy OIDs required.	Server Authentication (1.3.6.1.5.5.7.3.1)
msPKI- Certificate Policy	The Certificate issuer policy OIDs are placed in the OID_CERT_POLICIES extension by the policy module.	N/A
msPKI- Certificate -Application-Policy	Certificate application policy OIDs.	N/A

The other templates made available on the CAs will have the default Windows attributes and will be the following: Domain Controller, Domain Controller Authentication, IPSec, IPSec (Offline request).

For other LSU System campuses and organizations that utilize the CA, specific templates will be created for each group. For example, if the LSU Health Sciences center uses a web server certificate, a separate certificate template will be created for them, as a clone of the (Public Certificate) LSU Web Server template. This new template would be called (Public Certificate) LSU Health Sciences Web Server template. This process allows the IT Security and Policy Office to more easily monitor the number of public and internal certificates issued to each organization.

5.2 Certificate Request Approval

When a certificate request reaches a CA that is running a member of the Windows Server 2003 family, the CA can immediately issue the certificate or put it into a pending state. It is the responsibility of the CA administrator to configure the enrollment method either globally for a CA or on a per-template basis. For a Windows Server 2003, Enterprise Edition enterprise CA the enrollment method can be set individually for a V2 template.

In LSU's environment, this option is set on a per template basis, with most templates likely being issued automatically. Since access to the template in the first place is controlled by the ACL on it, only those users or computers that LSU specifies will have access to make the request. There may be some templates, for example (Public Certificate) LSU Web Server, where LSU desires an additional layer of control on certificate creation. In these cases, the templates can be set to require administrative approval, and LSU will have a workflow process for regularly reviewing and acting on submitted requests. The Windows SMTP exit module will be configured to automatically

send email to the IT Security and Policy Office when a certificate request that requires approval is submitted. The Office will establish and communicate a Service Level Agreement for acting upon these requests, likely within 24 hours.

5.3 Key Archival

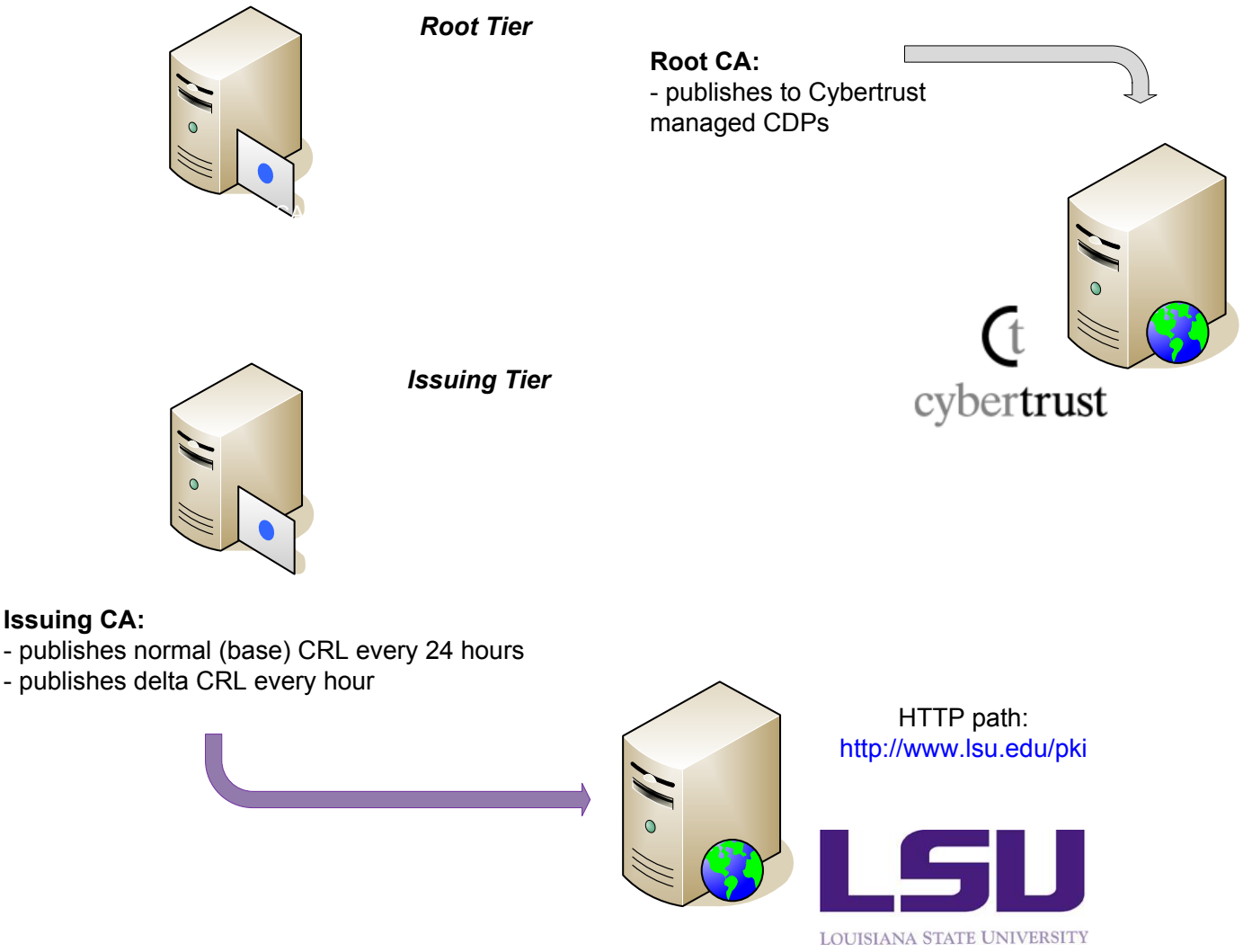
Key recovery implies that the private key portion of a public-private key pair may be archived and recovered. Private key recovery does not recover any data or messages, it merely enables a user to retrieve lost or damaged keys or for an administrator to assume the role of a user for data access or data recovery purposes. In many applications, data recovery cannot occur without first performing key recovery. Windows Server 2003 supports key archival, a process where the CA can store a copy of private keys that are on end entities within the CA database. This can be particularly useful to LSU for scenarios such as disk encryption and email encryption, as it allows users to readily recover their own data in cases of a lost or damaged key. LSU can choose what certificates should use archival on a per template, or even a per CA basis. Given the types of certificates used in the initial design, key archival is not required and is not enabled. However, as LSU implements new services that leverage the PKI, key archival will be enabled on specific certificate templates as necessary. The IT Security and Policy Office will be solely responsible for acting as the Key Recovery Agent (KRA).

6 Revocation Strategy

Each certificate created will have a validity lifetime associated with it. From time to time, though, LSU will need to invalidate certain certificates prior to the end of their validity period. For example, if an employee is given a certificate with a validity period that expires in December 2006, but that employee leaves the organization in August 2006, LSU would want to mark that certificate as invalid. This type of revocation is commonly accomplished with the use of Certificate Revocation Lists (CRLs), which are simple files containing a list of certificate serial numbers that are signed by a CA. The serial numbers contained on this CRL list those certificates for which the validity lifetime is still valid, but which LSU no longer considers trustworthy. Clients can then download this CRL and check against it to determine the validity of certificates.

Any X.509 V3 certificate (except the root CA certificate itself) should have a pointer to a valid CRL. The CRL distribution point is included in the certificate's extension and cannot be modified after a certificate is enrolled. The CRL is essential to ensure the quality (status) of certificates that are published by the CA. As such, an important part of the LSU PKI is having CRLs that are physically redundant, highly available, and accessible by external parties. An online CA, like LSU Issuing CA 1, that is joined to an Active Directory domain automatically publishes the CRL to Active Directory so that it can be accessible through LDAP. The CRL can also be made available through an HTTP URL that points to a location on a Web server.

In the LSU design, there are many non-Windows and / or non-Active Directory joined computers that will be utilizing the PKI. Thus, the advantages of publishing to Active Directory are minimal. Instead, LSU will publish its CRL only to an HTTP path, www.lsu.edu/pki. Using an HTTP path allows us to more easily build a redundant hosting platform and also removes the potential complexities associated with enabling client LDAP lookups. The root CA will publish a CRL on a basis determined by Cybertrust. LSU's issuing CA will publish a complete CRL every 24 hours.



6.1 Delta CRLs

In a production environment, the number of certificates that are revoked in relation to the total number of certificates issued is often quite low. However, over time the CRL may include hundreds or even thousands of certificate serial numbers. Though these serial numbers will be removed from the CRL as the original certificates they represent reach the end of their validity lifespan, the CRL itself is traditionally a single flat file that grows more or less linearly as additional certificates are revoked.

RFC 2459 and RFC 3280 define a method that can be used to reduce base CRL sizes by using delta CRLs. Delta CRLs maintain a list of certificates that have been revoked since the last base CRL publication. Base CRLs and delta CRLs are cached by Windows XP and Windows Server 2003. To ensure the validity of a certificate, the client uses the locally-cached base and delta CRL until the CRL's validity period expires. If a base CRL expires, the client retrieves a new base CRL from the distribution point that is specified in the certificate. If the base CRL is valid but the cached delta CRL is expired, a Windows client retrieves only the delta CRL. Typically, a delta CRL is much smaller in size than a base CRL because it saves only the certificates that have been revoked after the last base CRL update. Previous versions of Windows, such as Windows 2000, are not aware of delta CRLs and must continue to rely on normal CRLs. In the LSU environment, the standard desktop operating system is a mix of Windows 2000 and Windows XP. As such, many LSU systems will be able to take advantage of delta CRLs; those that cannot will continue to utilize normal

CRLs with no negative impact. The end result of this approach is that Windows XP and Windows Server 2003 systems are able to take advantage of hourly CRLs with minimal impact to network utilization, while other operating systems use a daily CRL. LSU Issuing CAs will publish delta CRLs every hour, and a base CRL every 24 hours. LSU will adhere to the following best practices regarding management and usage of delta CRLs:

- If a large number of certificates are revoked and if the number of revoked certificates exceeds the number of revoked certificates that are already part of the base CRL, the size of a delta CRL is larger than the size of a base CRL. Note that this scenario is very unlikely to occur and is not considered to be typical. However, if it does occur, a new base should be published, rather than a new delta.
- Do not use delta CRLs with offline CAs
- Use delta CRLs with all issuing CAs (the bottom tier of the LSU hierarchy).
- Do not publish frequent delta CRLs to Active Directory if replication takes longer than the time the delta CRL is valid.

The approach of publishing delta CRLs every 12 hours is well within the global convergence time for LSU's Active Directory

7 Detailed Configuration of LSU's CAs

Registry references follow the syntax that is used by the certutil tool.

7.1 LSU Issuing CA 1 Configuration Parameters

CSP (CA Certificate)

Description

The CSP is responsible for generating the certificate's key material and certificate generation.

Value

nCipher Enhanced Cryptographic Provider

Defined at

CA Installation Wizard

Stored at

HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CSP\Provider

Impacts

CA certificate

Hash Algorithm

Description

Defines the hash algorithm that is used for hashing and signing certificate contents.

Value

SHA-1

Defined at

CA Installation Wizard

Stored at

HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CSP\HashAlgorithm

Impacts

CA certificate

Key Length (CA Certificate)

Description

Defines the complexity of the key material that is assigned to the CA certificate.

Value

2048

Defined at
CA Installation Wizard

Stored at
Certificate request and is only used temporarily

Impacts
CA key material stored on HSM.

Common Name
Description
Name displayed in the Issued To field on the certificate. The common name must not exceed 64 characters in length.

Value
Louisiana State University Issuing CA 1

Defined at
CA Installation Wizard

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CommonName

Impacts
The common name becomes part of the certificate issuer name and is also part of the CRL and AIA.

CA Database Path
Description
Defines where the CA's database is located in the CA's file system.

Value
C:\CertDB

Defined at
CA Installation Wizard

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\DBDirectory

Impacts
The CA must be able to obtain the appropriate path name from the registry when the CA starts.

CA Log File Path
Description
Defines where the CA's transaction log files are located in the root CA's file system.

Value
D:\CertLog
Defined at
CA Installation Wizard

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\DBLogDirectory

Impacts
The CA must be able to obtain the appropriate path name from the registry when the CA starts.

Shared folder
Description
Defines where the CA's transaction log files are located in the root CA's file system.

Value
None… no shared folder used.

Defined at
CA Installation Wizard

Stored at
User-defined location during installation

Impacts
Clients that cannot receive the CA certificate through group policies and need to manually import the certificate.

Distinguished Name Suffix
Description
The name space is automatically mapped to the Active Directory namespace. The ***Value*** is predefined because of the domain membership of the CA.

Value
CN=Configuration, DC=lsu,DC=edu

Defined at
Automatically defined

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\DSConfigDN

Impacts
The distinguished name becomes part of the certificate issuer name and is also part of the CRL and AIA.

CRL Distribution Point

Description
Defines the URLs where the client can locate the certificate revocation list that is related to the certificate.

Value
http://www.lsu.edu/pki/LouisianaStateUniversityIssuingCA1.crl

Defined at
Certification Authority MMC

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CRLPublicationURLs

Impacts
Any user, computer, service, or program that verifies the root certificate

Authority Information Access (AIA)
Description
Defines the URLs where the client can find the certificate's issuer certificate.

Value
http://www.lsu.edu/pki/LouisianaStateUniversityIssuingCA1.crt

Defined at
Certification Authority MMC

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CACertPublicationURLs

Impacts
Any user, computer, service, or program that verifies the root certificate

CRL Publication Interval
Description
Also controls the CRL validity time

Value
1 day

Defined at
Certification Authority MMC

Stored at
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CRLPeriod
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CRLPeriodUnits

Impacts
CA CRL publication algorithm and any user, computer, service, or computer that verifies the CRL.

Delta CRL publication interval

Description

Defines similar to the CRL publication interval and the publication interval of the delta CRL.

Value

1 hour

Defined at

Certification Authority MMC

Stored at

HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CRLDeltaPeriod
HKLM\System\CurrentControlSet\Services\CertSvc\Configuration\CAName\CRLDeltaPeriodUnits

Impacts

Any client that can verify the certificate validity through delta CRLs

8 References

Microsoft Corporation. (n.d.). *Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.* Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.msp.

Microsoft Corporation. (n.d.). *Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003.* Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx.

Microsoft Corporation. (n.d.). *Public Key Infrastructure for Windows Server 2003 Technology Center.* Retrieved from http://microsoft.com/pki.

Microsoft Corporation. (n.d.). *Windows Server 2003 PKI Operations Guide.* Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03pkog.mspx.

Microsoft Corporation. (2003, March 28). *Designing a Public Key Infrastructure.* Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b.mspx.

Microsoft Corporation. (2003, May 21). *PKI Enhancements in Windows XP Professional and Windows Server 2003.* Retrieved from http://www.microsoft.com/technet/prodtechnol/winxppro/Plan/PKIEnh.asp.

Microsoft Corporation. (2003, April 23). *Windows Server 2003 Security Guide.* Retrieved from http://www.microsoft.com/technet/security/prodtech/windowsserver2003/W2003HG/SGCH00.mspx.

Microsoft Corporation. (2004, May 17). *Windows Server 2003 Advanced Certificate Enrollment and Management.* Retrieved from http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.mspx.

Morello, J. (2006). *LSU PKI Deployment and Operations Guide.* Baton Rouge.

The Internet Engineering Task Force. (2003, November). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* Retrieved from http://www.ietf.org/rfc/rfc3647.txt.

The Internet Engineering Task Force. (2005, September 20). *Public-Key Infrastructure (X.509) (pkix) Charter.* Retrieved from http://www.ietf.org/html.charters/pkix-charter.html .