verizon

UniCERT Core v5.4

Installation Guide

for Linux

1. About the distributed UniCERT Core product

This guide provides the installation guidelines for the entire UniCERT product. Although some UniCERT components are available on different CDs, this guide accompanies the UniCERT Core software and as such presents information to help you to determine which CDs you need, the prerequisites for those components, and where to install the UniCERT Core components. It also provides instructions for upgrading your components.

In addition, this guide describes typical deployments of public-key infrastructures (PKIs). Depending on your PKI requirements, one of these examples may provide a starting point for developing your own deployment strategy. Detailed information on installing UniCERT in a configuration that meets requirements for Common Criteria EAL 4+ validation is provided in Appendix A, *Using UniCERT in its evaluated configuration*.

This chapter explains the relation of the UniCERT Core components to the other UniCERT components. It also details the documentation set provided with the UniCERT Core, which you need to manage the entire UniCERT product.

1.1 What does UniCERT Core contain?

The UniCERT Core CD set provides the following UniCERT components:

- The CA, CAO, CSS, and Publisher
- The RA and RA eXchange
- The CMP Handler, email Handler, and SCEP Handler

It also includes the UniCERT utilities: Database Upgrade Utility, Database Wizard, RA Auditor, Service Manager, Key Generator, and Token Manager. For definitions of the component acronyms, see the *UniCERT Product Overview*.

The UniCERT Web Components, although part of UniCERT, are provided separately for ease of installation. Major releases of the UniCERT Web Components, the WebRAO servlets, and

the Web Handler are provided on their own CD so that you can install them separately on your web server. Minor releases are made available via Global Support Services.

You must install and run the CAO and RA Auditor on a computer with a Windows operating system. You can download the WebRAO Client from the WebRAO servlet using a browser or install it from the WebRAO Client CD for Windows.

1.1.1 Which documents are provided?

The main UniCERT Core installation provides the following documents:

- This guide, *UniCERT Core Installation Guide*
- The *UniCERT Core Release Notes*
- The *UniCERT Product Overview*
- The *UniCERT Administrator's Guide*
- The *UniCERT Configuration Guide*
- The *UniCERT Extensions Guide*
- The *UniCERT Publisher Administrator's Guide*
- The *UniCERT Database Administrator's Guide for Redhat Linux*
- UniCERT Error Messages
- UniCERT Event Codes
- `readme.html`

Refer to the *UniCERT Database Administrator's Guide* for information on installing and configuring Oracle. After reading this guide and installing the UniCERT Core components as explained in Chapter 4, *Installing UniCERT Core*, check the `readme.html` for any known issues.

If you are installing UniCERT for the first time, we recommend that you then refer to the other documents in the following order:

1. Run the demonstrations for first-time users (see Getting Started Demos for UniCERT).
2. See the *UniCERT Core Release Notes* for information on resolved issues and new features.
3. See the *UniCERT Product Overview* for a comprehensive introduction to the UniCERT product.
4. See the *UniCERT Administrator's Guide* for information on setting up user database accounts for the PKI entities and using UniCERT utilities.
5. Read the *UniCERT Configuration Guide* for instructions on creating and managing your PKI, configuring the PKI entities, creating registration policies (RPs), and initializing entities.
6. See the *UniCERT Publisher Administrator's Guide* for instructions on configuring and using the Publisher.

1. About the distributed UniCERT Core product

If you are fine-tuning your RPs and need additional information about the X.509 certificates and their extensions, see the *UniCERT Extensions Guide*. For a schematic representation of the topics covered in the UniCERT Core documentation set, see Figure 1.1.

Figure 1.1: Where to find information

1.1.2 Who is it for?

This documentation set is intended for administrators and users of the UniCERT product and for managers of an organization's or company's information security system. As the manager or security officer, you define your company's PKI, deciding where the individual UniCERT components are to be installed and defining your company's Certification Practices Statement (CPS).

1.1.3 What does it assume you already know?

As a manager or administrator of information security systems, you are computer literate, with extensive knowledge about networks, operating systems, Oracle databases, and the internet. We assume that you have a basic, not thorough, understanding of cryptosystems and their purposes. It is not necessary that you have a comprehensive knowledge of the various cryptographic algorithms and certificate standards.

1.2 How the UniCERT product is distributed

For summary information on the UniCERT Core CD set, see Table 1.1. For the advanced or optional UniCERT components, see the CD sets listed in Table 1.2.

For a detailed description of each UniCERT component, see the *UniCERT Product Overview*. For recommendations on the components to use in a highly secure PKI, see Appendix A, *Using UniCERT in its evaluated configuration*.

Table 1.1: UniCERT Core CDs

CD name	Components	Documentation
UniCERT Core	UniCERT Core components and utilities for Windows: • CAO and RA Auditor • Database Wizard, Database Upgrade Utility, Key Generator, Token Manager UniCERT Core components and utilities for Linux: • CA, CSS, Publisher, RA, RA eXchange, SCEP Handler, email Handler, and CMP Handler • Service Manager, Database Wizard, Database Upgrade Utility, Key Generator, and Token Manager The Web Components, and WebRAO Client come on their own CD as outlined below.	The UniCERT Core documentation set; see Section 1.1.1, *Which documents are provided?*.

Web Components	WebRAO Servlet
	Web Handler
	RA eXchange Proxy Servlet
		UniCERT Web Components Administrator's Guide
		UniCERT Web Components Release Notes
		UniCERT WebRAO Client User's Guide (made accessible to the client via the web)
		`webreadme.html`
		`index.html`

Table 1.1: UniCERT Core CDs (Continued)

CD name	Components	Documentation

WebRAO Client	WebRAO Client for Windows	*UniCERT WebRAO Client User's Guide*
		`webraoreadme.html`
		`webraoindex.html`

Table 1.2: UniCERT's advanced components

CD name	Components	Documentation

Key Archiver	KAO for Windows
	KAS for Linux
		UniCERT Key Archiver Administrator's Guide
		UniCERT Key Archiver Release Notes
		`kasreadme.html`
		`kasindex.htm`

ARM	ARM	*UniCERT ARM Installation Guide*
		UniCERT ARM Developer's Guide
		UniCERT ARM Reference Guide
		UniCERT ARM Release Notes
		`armreadme.html`
		`armindex.htm`

UPI	UniCERT Programmatic Interface (UPI)	*UPI Installation Guide*
		UPI Developer's Guide
		UPI Servlet Reference Guide
		UPI Client Reference Guide
		UPI Release Notes
		`upireadme.html`
		`upiindex.htm`

Autoenroll	Autoenroll Handler for Windows
	Autoenroll Publisher for Windows
		UniCERT Autoenroll Administrator's Guide
		UniCERT Autoenroll Release Notes
		`readme.html`
		`index.htm`

The CAO, KAO, WebRAO Client, RA Auditor, and Autoenroll components are only available on Windows.

1.2.1 Using the Web Components

The UniCERT Web Components give you both the WebRAO servlets and the Web Handler, which is one of the UniCERT protocol handlers. If you plan to have certificate applicants submit their requests remotely via the web, install this on your web server. There are also some utilities to assist you in adding and configuring the web component instances.

1.2.2 Using the WebRAO Client

The UniCERT WebRAO Client provides the primary interface for creating or processing certificate requests. Install this on each computer to be used for processing certificate requests. These are typically distributed computers across the internet, contact points for external customers, or internal road warriors.

1.2.3 Using the Key Archiver

The UniCERT Key Archiver provides you with the capabilities to archive and securely store private encryption keys, enabling you to recover them if they are lost or become corrupt. Key recovery is strictly controlled and an audit trail is used to track when the keys were recovered and by whom. Purchase and install the optional UniCERT Key Archiver components if you want to add the key archival functionality to your UniCERT PKI.

1.2.4 Using the ARM

The UniCERT ARM is an advanced component for automating request processing. It is a highly customizable service that comes with a default set of plug-ins to perform normal UniCERT operations, and a developer's toolkit for you to write your own plug-ins. If you require a more powerful alternative to the WebRAO that allows for the extensibility of the request process, purchase and install the optional ARM component.

1.2.5 Using the UPI

The UPI is a Java developer's toolkit that enables you to create advanced, web-based registration and authorization applications. You can use it to customize the certificate request and authorization processing functionality required for your applications and devices to interact with UniCERT.

1.2.6 Using the Autoenroll

The UniCERT Autoenroll is an advanced component for automating the process of certificate requests in Microsoft Windows environments.

The UniCERT Autoenroll Handler enables you to issue certificates from your UniCERT CA to Windows users and server components, such as domain controllers. Windows 7, Windows 2008 R2, Vista, XP, and 2003 clients can automatically request a certificate for the user when the user logs onto a Windows domain. The Windows clients can also request renewal of users' certificates as they are about to expire (again, with virtually no user interaction).

1.3 Conventions used in the documentation

Table 1.3 lists the various conventions used in the documentation. We follow these conventions to help you quickly and easily identify particular elements, processes, and names that occur frequently in documents.

Table 1.3: Conventions

Element	Sample formatting
All GUI items, including menu options, buttons, icons, fields, and window titles	File menu Select File>New>Folder. Save As dialog OK
Keystrokes	Tab Enter F1 Ctrl+Alt+1
Filenames and directory paths	Locate `readme.html` on the CD. `f:\startup\demo`
Text the user needs to enter or programming code	`printf("Hello\n");`
References to chapter and section names	See Chapter 1, *About this guide*. See *What is it about?* on page 1.
References to figures, tables, and code examples.	See Table 1. See Figure 1. See Code example 1.
References to other documents	See the *UniCERT Administrator's Guide.*
Application names	UniCERT KeyTools Pro
Notes and tips	
Cautions	
Warning (indicates possibility of physical harm)	

1.4 Related references

[1] See Section 1.5, *References*, in the *UniCERT Extensions Guide*.

[2] UniCERT Product Overview, 2013

[3] The Public Key Cryptography Standards (PKCS) are available from RSA Laboratories (http://www.rsa.com/rsalabs/node.asp?id=2124).

[4] UniCERT Web Components v5.4 Documentation set, 2013.

[5] UniCERT WebRAO Client v5.4 Documentation set, 2013.

[6] UniCERT Key Archiver v5.4 Documentation set, 2013.

[7] UniCERT ARM v5.4 Documentation set, 2013.

[8] UniCERT UPI v5.4 Documentation set, 2013.

[9] UniCERT Autoenroll v5.4 Documentation set, 2013.

[10] Schneier, Bruce, *Applied Cryptography*, 2nd edition, Wiley, New York, 1996.

[11] Shirey, R. , Internet Security Glossary, The Internet Society, 2000 http://www.ietf.org/rfc/rfc2828.txt

1.5 About Verizon

Verizon, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonenterprise.com.

1.6 Contacting Global Support Services

If you are having issues with the UniCERT Core release, contact Global Support Services (iam-support@verizon.com). Before doing so, however, make sure you have the information

listed in Table 1.4. You can either copy this text and email or print it from the PDF and fax it to Global Support Services.

Table 1.4: Product information

UniCERT Core support information		
Version:		
Patch versions (if applicable):		
Operating system (include version and service packs):		
System path:		
Compiler version:		
Hardware platform:		
Network details (PKI layout):		
Nature of problem:	Issue report	Documentation issue
	Feature missing	Query
	Other	
Is the problem reproducible? If yes, how? (attached/forwarded)	Yes	No
Third-party tool and its version:		
Error number (if applicable) and complete exception error message:		
Copy of other files, for example, your certificate, PSE, or P12 file (where applicable). Note: Ensure you send your password for these files separately.	Yes	No

2. Installation prerequisites

Once you have determined your PKI strategy, make sure that the computers to be included in your PKI meet the following requirements before you begin the installation process.

If you are not familiar with PKI concepts or public-key cryptography, read the *UniCERT Product Overview* before planning your PKI deployment or installing UniCERT. The information in Appendix A, *Using UniCERT in its evaluated configuration*, also helps you understand how best to design and deploy your PKI.

2.1 Environments supported

UniCERT supports the operating systems listed in Table 2.1. Not all the supported operating systems have been tested with this release; refer to Table 2.1 for details.

For recommendations on which UniCERT PKI components meet common criteria requirements, see Appendix A, *Using UniCERT in its evaluated configuration*.

UniCERT v5.4 is provided for Linux systems (CentOS and Red Hat); however, some components are Windows only. In addition, the UPI and certain UniCERT utilities are supported on both Linux and Windows. Table 2.1 details which operating systems the components are supported on.

You can run the UniCERT components on physical systems or virtual machines (VMs); however, you need to evaluate how any HSMs or tokens that are connected to physical

interfaces, such as PCI or USB, are dependent on the underlying hardware and virtualization environments.

Table 2.1: Supported operating systems

Components	Supported systems	Tested
• CA, CSS, Publisher, RA, RA eXchange • WebRAO servlets, Web Handler, RA eXchange Proxy servlet • SCEP Handler, email Handler, CMP Handler • KAS • ARM • UPI • Service Manager • Database Wizard, Database Upgrade Utility, Key Generator, Token Manager	CentOS 6.4 x64	Yes
	Red Hat Enterprise Linux 6.4 x64	Yes
• CAO • KAO • WebRAO Client • UPI • RA Auditor • Database Wizard, Database Upgrade Utility, Key Generator, Token Manager	Microsoft Windows XP Professional Service Pack 3	No
	Microsoft Windows 7 Ultimate Edition	Yes
	Microsoft Windows 8 (for Web Components only)	Yes
	Microsoft Windows 2008 R2	Yes
	Microsoft Windows 2003 R2 Service Pack 2	No

Although Windows Server 2008 R2 is 64-bit, it supports 32-bit applications. UniCERT is a 32-bit application and also requires the 32-bit version of the Oracle client on Windows.

The operating systems supported for UniCERT Autoenroll differ from those supported for the other UniCERT components. See the *UniCERT Autoenroll Administrator's Guide*.

2.2 User account requirements

The user account requirements depend on which UniCERT component you are using, as outlined in Table 2.2. In addition, the administrator privileges on Windows XP work differently

to the other supported Windows operating systems, that is, Windows Vista, Windows 2008, Windows 7, or Windows 8 (see Table 2.3).

Only the UniCERT Web Components are currently supported on Windows 8.

Table 2.2: User account requirements

UniCERT component	Type of user account
CA Operator	User level privileges; however, if creating crypto profiles from within the CAO, you are prompted to log on as an administrator, as this task requires administrator privileges.
RA Event Viewer	User level privileges; however, if creating crypto profiles from within the CAO, you are prompted to log on as an administrator, as this task requires administrator privileges.
Service Manager	Administrator privileges
Token Manager	Administrator privileges
Database Wizard	User level privileges
Key Generator	User level privileges; however, if creating crypto profiles from within the Key Generator, you are prompted to log on as an administrator, as this task requires administrator privileges.
Publisher Configuration utility	Administrator privileges
Web Handler Configuration utility	Administrator privileges; as the Web Handler configuration tool requires write access to the configuration files installed with the Web Handler, you need to be an administrator to access these files and therefore run this tool.
WebRAO Configuration utility	Administrator privileges; as the WebRAO configuration tool requires write access to the configuration files installed with the WebRAO, you need to be an administrator to access these files and therefore run this tool.
Key Archive Operator	User level privileges; however, if creating crypto profiles from within the KAO, you are prompted to log on as an administrator, as this task requires administrator privileges.

Table 2.3 outlines the differences in the administrator account privileges on the different operating systems.

Table 2.3: Administrator accounts on Windows operating systems

Operating system	Administrator account functionality
Windows XP	You must be logged on as an administrator for any components requiring administrator privileges. If you are logged on with user level privileges, you cannot run any component requiring administrator privileges. For example, if you are running the CAO with user level privileges, the Edit Crypto Profiles button is grayed out. You must either log back on as an administrator or request that an administrator create the required crypto profiles in the Token Manager.
Windows Vista, Windows 2008, Windows 7 and Windows 8	As part of the user account control functionality, when a user with administrative privileges attempts to start an application requiring administrative privileges, Windows displays the User Account Control dialog, prompting you to confirm that you want to use your full administrator privileges. If you are not an administrator, Windows displays the User Account Control dialog, but in this case it prompts you to provide administrator's credentials to run the program. Without User Account Control (UAC), when a user is logged on as an administrator, that user is automatically granted full access to all system resources. We recommend you do not disable UAC for security reasons.

2.3 Minimum hardware requirements

Depending on which UniCERT components you are installing on a computer, the minimum hardware requirements can differ.

Table 2.4 lists the minimum system requirements for the Linux operating system if there are only a few UniCERT services on it.

Table 2.4: Minimum system requirements

Component	Requirement
RAM	2 GB (64-bit only) if not installing Oracle; with the Oracle server database, 3 GB
Hard drive space	• 5 GB for the Oracle server installation and database, 400 MB of swap space, and 72 MB for data and index files on the Oracle server computer • 1500 MB if you install all UniCERT components on the same computer
Processor	x86-64

Table 2.4: Minimum system requirements (Continued)

Component	Requirement
Clock speed	1 GHz
Other drives	CD-ROM drive for installation

During installation, you will also require a significant amount of temporary space. To make sure that you have adequate space, set a `tmp` variable for a directory that has 450 MB free.

If you are running a large number of service instances, for example for a managed services environment, we recommend that you meet at least the specifications listed in Table 2.5. It assumes you have a separate Oracle server.

Table 2.5: Requirements for managed UniCERT services

Component	Requirement
RAM	1 MB L2 Cache per Processor 2 GB Memory per Processor
Hard drive space	2 x 73 GB 10000 rpm SAS Disk Drives
Processors	Two x86-64 processors
Clock speed	1.5 GHz
Other drives/ communications	2 PCI-X Slots 2 PCIe Slots 4 x 10/100/1000 Mbps Ethernet Ports Secure Socketed Configuration Chip

Table 2.6 lists the minimum system requirements for the supported Windows operating systems, which you need for the CAO, RA Auditor, and KAO.

Table 2.6: Minimum system requirements

Component	Requirement
RAM	1 GB (32-bit) or 2 GB (64-bit)
Hard drive space	300 MB for the UniCERT components and documentation
Processor	1.8 GHz or faster 32-bit (x86) or 64-bit (x64) processor
Clock speed	1.8 GHz
Other drives	CD-ROM drive for installation

The WebRAO Client on its own functions on a computer with lower specifications. For it, you can use a 1.6 GHz or faster processor that has 1 GB of RAM. As the WebRAO Client is browser based, you need minimal hard drive space.

You may wish to exceed these minimum hardware requirements, particularly for the server components. The amount of hard drive space required depends on the number of certificates you intend to process.

2.4 Software and optional hardware requirements

This section provides information on all the supported third-party software and hardware versions for UniCERT Core components and certificate applicants. Which third-party software is mandatory depends on the UniCERT Core components your PKI includes. Oracle is the most common requirement:

- Most of the UniCERT Core components, including the Core Publisher, require Oracle. However, none of the protocol handlers, including the optional Autoenroll Handler, the WebRAO, and the Autoenroll Publisher, use Oracle.
- The Key Archiver and ARM, which are advanced components, also require Oracle. However, the advanced component UPI does not.

Individual components also necessitate specific software. For example, the Publisher interoperates with an LDAP server or OCSP responder; the email Handler requires a supported email server and client.

2.4.1 Supported Oracle versions

Table 2.7 describes the supported Oracle versions and any additional requirements:

- If you have Oracle support and have not already patched your Oracle version, see http://www.oracle.com/technetwork/topics/security/alerts-086861.html for details on Oracle's critical patch updates. Otherwise, contact Global Support Services for assistance.

- Most Oracle critical patch updates apply to both the client and the server.
- For information on installing and configuring Oracle, see the *UniCERT Database Administrator's Guide*.

Table 2.7: Supported Oracle versions

User	Supported version	Requirements
Server	**On Red Hat:** • Oracle v11.2.0.4 (patch number 13390677) • Oracle v11.2.0.3.4 (patch number 14275605) **On Windows:** • Oracle v11.2.0.3 (x64) (patch number 13413168)	We recommend that you also install the specified critical patch as this critical patch revision was applied to Oracle when tested with this release of UniCERT. **Note:** If you are using the Oracle v11.2.0.4 server, the `sys` user must explicitly grant the `DBMS_REPUTILS` execute permission to the Oracle database administrator who will use the UniCERT Database Wizard, for example, `system` (see Section 2.2.5, *Granting the DBMS_REPUTILS execute permission*, in the *UniCERT Database Administrator's Guide*).
Client	**On CentOS and Red Hat:** • Oracle 11.2.0.3.7 (patch number 16619892) **On Windows:** • Oracle v11.2.0.3 (patch number 17163633)	As UniCERT Core is built against the Oracle client libraries, if you have an earlier version of the Oracle client, you must install the critical patch.

2.4.2 Installing xterm

Some of the UniCERT components require access to xterm, a terminal emulator. Before installing UniCERT, ensure that xterm is installed by running the following command:

Code example 2.1: Installing xterm

```
yum install xterm
```

2.4.3 Configuring the firewall

If you have a firewall running on a system hosting a UniCERT service, add rules to allow TCP packets to be routed between the relevant UniCERT service port numbers.

2.4.4 Supported PKCS#11 devices

UniCERT supports a variety of hardware security modules (HSMs) and smart card products. Typically, HSMs are only used for securing the most sensitive entities in your PKI—the CAs, as well as other services such as the RA or RA eXchange. You can use smart cards to secure other PKI users' keys, for example:

- CAO or KAO users

- The WebRAO Client users, that is, the Registration Authority Operator (RAO), Key Recovery Operator (KRO), and Registration and Recovery Operator (RRO)
- The CMP Handler, email Handler, or SCEP Handler

End users also typically use smart cards.

All of the PKCS#11 HSMs and smart card products that you can use with UniCERT conform to the 2.01 version of the PKCS#11 standard.

We recommend that you do not use smart cards for the primary UniCERT services; use them for storing PKI user and end user credentials only.

Given that card management systems interoperate with the smart cards, we do not list supported card management systems for UniCERT. If you wish to integrate a card management system into your PKI, contact Global Support Services.

2.4.4.1 Choosing the HSM device driver

It is important that you use the correct device driver for your PKCS#11 devices. Not all the supported HSMs have been tested with this release of UniCERT; refer to Table 2.8 for details on the supported HSMs and which HSMs were tested with this release. Alternate drivers and HSMs that the vendors provide have not been tested and may not function with UniCERT.

Table 2.8: Supported HSM versions and libraries

Vendor	Product	Version	Shared objects	Tested
AEP Networks	Keyper Enterprise	v5.01 (firmware v2.0)	`pkcs11.Linux-_i64.so.4.09`	Yes
	Keyper Enterprise	v4.09 (firmware v1.8)	`pkcs11.Linux-_i64.so.4.09`	Yes
	Keyper Plus (No ECC support)	v5.01 (firmware v2.1)	`pkcs11.linux_gc-c_4_1_2_glibc_2_5_x86_64.so.5.01`	Yes
nCipher	nShield Connect	v11.50 (firmware v2.50.16)	`libcknfast-64.so`	Yes
	netHSM 500	v11.50 (firmware v2.50.16)	`libcknfast-64.so`	Yes

Table 2.8: Supported HSM versions and libraries (Continued)

Vendor	Product	Version	Shared objects	Tested
SafeNet	Luna SA K6	v5.2.1 (v6.2.1 firmware) Appliance Software v5.2.1 PED v2.0.2	`libCryptoki2_64.so`	Yes
	Luna SA K5	v4.4.1 (v4.6.8 firmware) Appliance Software v4.4.1-5 PED v2.0.2	`libCryptoki2_64.so`	Yes
	Luna CA4 (LDK-02-0101)	v2.5 (firmware v4.6.1) PED v2.0.2)	`libCryptoki2_64.so`	Yes

If you are using an nCipher HSM and you want to use K of N functionality, you must use the nCipher preload utility. For details on this preload utility, refer to your vendor documentation.

If you are using a Luna SA K5 HSM to store keys and you are generating keys at a CAO that is running on Microsoft Windows Server 2008 R2, set the Network Trust Links (NTLS) timer to 180 seconds to avoid issues with key generation. Log into your Luna SA K5 HSM with administrator credentials from PuTTY (SSH) and run `ntls timer show` from the Luna shell to show your current timer settings. If it shows anything less than 180 seconds, run `ntls timer set -timeout 180` to change it to 180 seconds.

2.4.4.2 Choosing the smart card device driver

It is important that you use the correct device driver for your PKCS#11 devices. Table 2.9 provides information for the smart cards that certificate applicants and CAO, KAO, and

WebRAO Client users can use. Alternate drivers that the vendors provide may not function correctly with UniCERT.

For information on the readers that the smart cards support, check with their vendors.

Table 2.9: Supported smart card versions and DLLs

Vendor	Product	Version	DLLs	Tested
SafeNet	SafeNet Authentication Client v8.1	iKey 2032 (driver v4.1.0.6) iKey 4000 (driver v4.1.0.6)	`dkck201.dll`	Yes
		Model 330 Model 400	`dkck201.dll`	No
		eToken Pro 72K	`etpkcs11.dll`	Yes
		Aladdin eToken	`etpkcs11.dll`	No
Gemalto	Classic Client	v6.1 Patch 3	`gclib.dll`	No

2.4.4.3 Memory, mapping, and algorithm constraints

Depending on the memory or mapping constraints, as well as the functions of the PKCS#11 device, you may be restricted as to the size of key you can generate, the number of keys, or the type of keys. UniCERT enables you to generate up to 8192-bit RSA keys or 1024-bit DSA keys. However:

- AEP Keyper Professional, nCipher, and the Luna SA products support up to 4096-bit RSA keys.
- Some smart cards do not support DSA keys, only RSA.
- iKey smart cards are restricted to a maximum key size of 2048 bits.
- If you use the Model 330 or 400 smart card with the SR10 reader or DKR7xx readers (Cardman), you can generate 2048-bit RSA keys. You cannot generate 2048-bit RSA keys using the DKR630 USB port.

Remember that the size of certificates and other objects stored on a PKCS#11 device also affect the number and size of keys that you can generate on the device.

For additional information on your PKCS#11 device's mapping constraints or technical specifications, see your vendor documentation.

2.4.4.4 Accreditation of supported devices

The PKCS#11 devices that UniCERT supports have the following accreditation:

- Luna SA has FIPS 140-2 level 3 and Common Criteria EAL 4+ validation (see http://www.safenet-inc.com/hardware_security_modules/lunasa.aspx).

- AEP Keyper Professional has FIPS 140-1 level 4, and AEP Keyper Enterprise has FIPS 140-2 level 4 (see http://www.aepnetworks.com/index.php/products/series-k).
- The SafeNet iKey 2032 smart cards have FIPS 140-1 level 2 and the SafeNet iKey 4000 smart cards have FIPS 140-2 Level 3 (see http://www.safenet-inc.com/products/data_protection/multi-factor_authentication/certificate-based_pki_usb_authenticators.aspx).
- netHSM has FIPS 140-2 level 3 and Common Criteria EAL 4+ validation (see http://www.thales-esecurity.com/Products/Approvals/FIPS%20140-2.aspx).

Contact the other product vendors for information on their FIPS accreditation.

2.4.5 Supported crypto service providers

Table 2.10 lists the crypto service providers (CSPs) that UniCERT supports for certificate applicants. For details on the algorithms and key sizes supported by these CSPs, refer to the Microsoft documentation.

Table 2.10: CSPs supported by UniCERT

Provider supported
Microsoft Base Cryptographic Provider
Microsoft Base DSS Cryptographic Provider
Microsoft Strong Cryptographic Provider
Microsoft Enhanced Cryptographic Provider
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Microsoft RSA SChannel Cryptographic Provider
Microsoft Software Key Storage Provider

If you use the Base DSS CSP at the Web Handler, you can generate DSA keys; however, you cannot import the DSA parameters.

2.4.6 Supported directory servers

If you plan to publish certificates to a directory using the UniCERT Publisher, you need to install one of the supported directory servers shown in the following table. Not all the

supported directory servers have been tested with this release of UniCERT; refer to the following table for details on which directory servers were tested with this release.

Table 2.11: Supported directory servers and testing information

Directory Server	Version supported	Tested
Oracle Directory Server (previously called Sun Java System Directory Server)	v 11.1.1.5.0	Yes
Microsoft's Active Directory Domain Services	Windows 2008 Server R2	No
Critical Path Directory Server	v5.0.0	No
Computer Associates etrust	8.1	No
Open LDAP	2.4.23 (20100719)	No
ViewDS Directory Server	7.2	No
Isode's M-Valut Directory Server	v15.0	No

Any LDAP v3 compliant directory server should work with UniCERT. However, issues encountered when using an unsupported LDAP directory server must be reproduced on one of the supported LDAP directory servers before Verizon can offer technical support on the problem.

2.4.7 Supported OCSP responders

The OCSP interface between UniCERT v5.4 and the Corestreet VA v5.1.5 Patch 10, which obtains the CRLs from LDAP, has been tested in this release. You can also use the Axway Validation Authority (VA, formerly Tumbleweed).

For information on publishing CRLs to LDAP, see the *UniCERT Publisher Administrator's Guide*; see your OCSP vendor's documentation for information on retrieving them.

2.4.8 Supported VPN products

The UniCERT SCEP Handler supports the VPN products listed in Table 2.12. Not all the supported VPN products have been tested with UniCERT; refer to Table 2.12 for details on which VPN products were tested with this release.

Table 2.12: Supported VPN products

VPN product	Version supported	Tested
Cisco IOS router	v12.4	Yes
Cisco VPN Client	v4.8	No

Table 2.12: Supported VPN products

VPN product	Version supported	Tested
Juniper SSG-350M Router with firmware (Firewall+VPN)	v6.1.0.r7.0	No

2.4.9 Supported Timestamp servers

For details on the versions of UniCERT tested with the UniCERT Timestamp Server, see the UniCERT Timestamp Server documentation.

2.4.10 Supported Java SE

Java Platform, Standard Edition 7 (Java SE 7), update 45, which is also referred to as Java Runtime Environment (JRE) v1.7.0_45, is included in the UniCERT installer.

2.4.11 Supported web servers and servlet managers

To provide the necessary HTTP support for the UniCERT Web Handler and WebRAO components, use one of the support web server and servlet manager pairs listed in the following table. Not all the supported web server and servlet manager pairs have been tested with UniCERT; refer to the following table for details on which were tested with this release.

Table 2.13: Supported web servers and servlet managers

Web server and servlet manager	Version supported	Tested
Oracle iPlanet Web Server (previously called Sun Java System Web Server). No servlet manager is required.	v7.0 with Update 12	No
Apache	v2.2.21 with Tomcat v6.0.30 v2.2.21 with Tomcat v7.0.39	No Yes

For more information on using the supported servers/servlet managers, see Chapter 2, *Installing the UniCERT web components*, in the *UniCERT Web Components Administrator's Guide*.

2.4.12 Supported browsers

These are the browsers that certificate applicants can use to communicate with UniCERT. Both the Web Handler and the WebRAO Client support these browser versions. Not all the

supported browsers have been tested with UniCERT; refer to the following table for details on which were tested with this release.

Table 2.14: Supported browsers

Browser	Version supported	Tested
Microsoft Internet Explorer	v6.0	No
	v7.0	No
	v8.0	Yes
	v9.0	No
	v10.0	Yes
Mozilla Firefox	v9.0.x	No
	v10.x	No
	v12.x	No
	v13.x	No
	v21.x	Yes

2.4.13 Supported email servers

To enable certificate applicants to communicate with UniCERT via email and to provide the necessary mail support for the UniCERT email Handler and Publisher components, use one of the following tested email servers

- Microsoft Exchange Server 2007 (version 08.02.0234.001)
- Microsoft Exchange Server 2010
- POP3 Server Version: 5.2.3790.3959

You must configure an email account on Microsoft Exchange Server for each CA. These accounts must be externally secured as the connection between the email handler and the MS exchange server is not secure. We also recommend you use Transport Layer Security (TLS) authentication. For more information, refer to the Microsoft Exchange Server documentation.

2.4.14 Supported email clients

UniCERT has been tested with the following email clients:

- Microsoft Outlook Express v6.0
- Microsoft Outlook 2000
- Microsoft Outlook 2003 SP2

2.5 Conformance to standards

UniCERT supports the following standards and formats.

2.5.1 Unicode

UniCERT supports Unicode character sets used in:

- Email templates
- Email attachments
- End entity and CA certificates

2.5.2 Certificates

UniCERT issues and works with DER encoded X.509 v3 and v1 certificates.

2.5.3 CRLs

UniCERT supports DER encoded X.509 v2 certificate revocation lists (CRLs).

2.6 Using ECC

UniCERT v5.4 includes support for elliptical curve cryptography (ECC). ECC is a form of public-key cryptography based on elliptic curves. The addition of the Elliptic Curve Digital Signature Algorithm (ECDSA) key algorithm offers a substantially greater strength-per-key-bit than traditional algorithms resulting in faster operation and smaller key sizes.

When you select ECDSA as your key algorithm, you must also specify which elliptic curve to use. The elliptic curves supported in UniCERT are those recommended by the National Institute of Standards and Technology (NIST) as outlined in RFC 5480. For more information, see http:///tools.ietf.org/html/rfc5480.

The UniCERT ECC support was developed using open source libraries. The ECC support for the UniCERT C++ components was developed using OpenSSL libraries and the ECC support for the UniCERT Java components was developed using the Bouncy Castle libraries. It is your responsibility to ensure that your use of the ECC algorithms does not infringe any patents or copyrights held by various companies around the world. You should do this by checking the patents and copyrights for the algorithms you plan to use in the country where you are installing the UniCERT component. For more information on OpenSSL and Bouncy Castle licensing, see http://www.openssl.org/ and http://www.bouncycastle.org/ respectively.

Certicom ECDSA support is not included with UniCERT v5.4. Contact Global Support Services for further information.

2.6.1 ECC supported PKCS#11 devices

The devices supported in UniCERT v5.4 are outlined in Section 2.4.4, *Supported PKCS#11 devices*. However, you cannot save ECDSA keys to all of these devices and for some, you can only save ECDSA keys to the devices if you upgrade the software. It is important that you use the correct device driver for your PKCS#11 devices. Alternate drivers that the vendors provide may not function correctly with UniCERT and UniCERT Core.

Currently, Keyper HSM devices do not support ECDSA keys. Only the Luna SA, Luna CA4, and the nCipher netHSM support ECDSA with the recommended software, and only for certain ECDSA curve strengths. For information on ECDSA curve strengths, refer to the relevant HSM device documentation.

2.6.2 ECC restrictions

The following restrictions apply to ECC support in UniCERT v5.4.

2.6.2.1 No archival and recovery of ECDSA keys

As UniCERT v5.4 only archives private keys that are used for encryption purposes, you cannot archive or recover ECDSA keys.

2.6.2.2 Supported curve strenghts

UniCERT v5.4 supports the elliptic curves outlined in Table 2.16:

Table 2.15: Supported elliptic curves

Curve name	NIST curve name	Curve OID	Enabled by default
sect163k1	K-163	1.3.132.0.1	No[Remove this column now?]
sect163r2	B-163	1.3.132.0.15	No
secp192r1	P-192	1.2.840.10045.3.1.1	Yes
secp224r1	P-224	1.3.132.0.33	Yes
sect233k1	K-233	1.3.132.0.26	No
sect233r1	B-233	1.3.132.0.27	No
secp256r1 (default)	P-256	1.2.840.10045.3.1.7	Yes
sect283k1	K-283	1.3.132.0.16	No
sect283r1	B-283	1.3.132.0.17	No
secp384r1	P-384	1.3.132.0.34	Yes
sect409k1	K-409	1.3.132.0.36	No
sect409r1	B-409	1.3.132.0.37	No
secp521r1	P-521	1.3.132.0.35	Yes

Table 2.15: Supported elliptic curves

Curve name	NIST curve name	Curve OID	Enabled by default
sect571k1	K-571	1.3.132.0.38	No
sect571r1	B-571	1.3.132.0.39	No
secp160r1	NA	1.3.132.0.8	No
sect239k1	NA	1.3.132.0.3	No

Limited curve strengths on Windows operating systems

If your CA signing algorithm is ECDSA, be aware that you may have issues installing the certificate on some Windows operating systems. You must ensure that the Windows Operating system supports the ECDSA curves you are using for your CA.

Supported curve strengths at the Web Handler

Key generation at the Web Handler is dependant on the facilities provided by the browser. At present, ECDSA key generation at the Web Handler is supported through the Microsoft Cryptography API Next Generation (CNG) Cryptographic Service Providers (CSP) (first supported in Windows Vista) and is limited to the curve strengths outlined in Table 2.16.

Table 2.16: Supported elliptic curves at the Web Handler

Curve name	NIST curve name	Curve OID	Enabled by default
secp256r1 (default)	P-256	1.2.840.10045.3.1.7	Yes
secp384r1	P-384	1.3.132.0.34	Yes
secp521r1	P-521	1.3.132.0.35	Yes

2.6.2.3 ECDSA browser support

ECDSA is not supported on Mozilla Firefox and if you select ECDSA on the Web Handler registration page, an error message is returned. If you wish to use ECDSA with the Web Handler, you must submit requests using Internet Explorer.

However, as PKCS#10 requests are supported at the Web Handler, you can use Mozilla Firefox to submit PKCS#10 ECDSA requests.

3. Getting ready for your PKI deployment

How you install the components depends on the design of your PKI: it can be distributed across WANs, LANs, or just a few computers in your system (intranet or internet usage). UniCERT uses the PKIX Certificate Management Protocol (CMP) standard, as specified in RFC 4210, for secure communications.

If you are not familiar with PKI concepts and terminology, see the *UniCERT Product Overview*.

This chapter provides three examples of possible PKI deployments:

- A demo testing setup
- A large corporation's virtual private network (VPN)
- A PKI hosted by an outside party

We focus here on the physical installation of UniCERT Core and the required third-party products for these PKI examples; we do not discuss the certification policies that you also need to implement or the detailed design of the PKI. For guidelines on designing a recommended PKI configuration, see Appendix A, *Using UniCERT in its evaluated configuration*, after reading this chapter. If you require additional assistance in setting up certification policies or in designing your PKI, contact Verizon's Professional Services.

We strongly recommend that you install and test a demo version of your PKI before fully implementing it.

3.1 Deciding how to install the UniCERT components

The number of computers and UniCERT component instances you need depends on the volume of certificates to be handled by the system, the geographical coverage required, and the administrative costs involved in managing a distributed PKI.

Part of the decision of how many UniCERT components or instances to install on one computer depends on the processing power of your computer. The decision also necessitates consideration of your PKI requirements and planned hierarchy. For example, if you have different administrators in charge of their own RA and one security officer using the CAO and managing the overall PKI, restrict the RA administrators' physical access to the CAO computer.

As the CAO is not available on Linux, you need at least one computer with a Windows operating system on which the CAO is installed.

If your RAs are not geographically dispersed, a dedicated RA computer with multiple RA clones installed on it and a single RA administrator may be the most efficient setup.

Most UniCERT components are licensed independently, and you must have adequate licenses for your installation. Contact the contracts department if you have any queries on the licensing of the components you have purchased or your Verizon representative if you require additional component licenses.

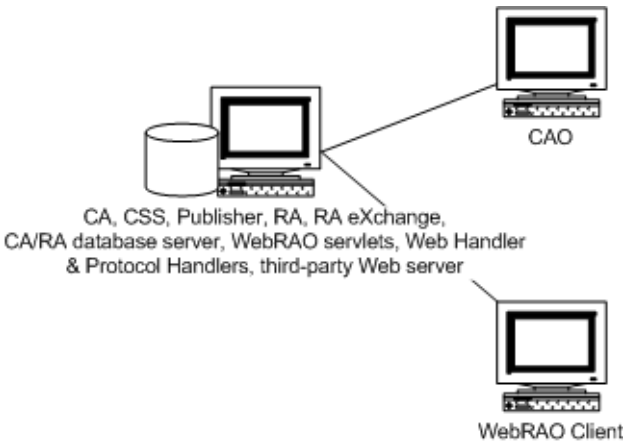
In UniCERT, you implement the failover and load balancing features by cloning the CA, the RA, and the RA eXchange. Cloning the CA on different computers helps to ensure that the CA runs continuously but if the RA is not also cloned and it fails, no requests reach the CA. For more information on the PKI entities you can clone, see Chapter 20, *Cloning*, in the *UniCERT Configuration Guide*.

3.2 Setting up a demo PKI

For demonstration or testing purposes, install the UniCERT CAO on a Windows computer, the WebRAO Client applet on another Windows computer, and the other UniCERT Core components on a Linux computer (see Figure 3.1).

3. Getting ready for your PKI deployment

Figure 3.1: Installing a test PKI



This test setup does not accurately reflect your eventual PKI deployment. However, the demo tests the preliminary installation and configuration tasks:

- Installing the Oracle 11g server and the UniCERT Core components (see Section 4.3, *Installing third-party products*)
- Setting up a web server if it is not already set up (see your third-party web server documentation) and installing the UniCERT WebRAO servlets on it

---

If your web server is on a separate computer on the LAN, typically it is in the DMZ, install the WebRAO servlets and Web Handler there.

- Defining your demo PKI entities (see the *UniCERT Configuration Guide*)
- Creating a demo registration policy (RP) and authorization group for remote certificate applicants (see the *UniCERT Configuration Guide*)

You use the CAO's Registration Policy Wizard to set up RPs for your CA, other PKI entities, and end entities.

- Making the RP available to the WebRAO Client and submitting a request via a web browser

The test scenario shown in Figure 3.1 illustrates the use of the WebRAO, as it is the simplest test. You can also test the submission of certificate requests using one of the protocol handlers: Web Handler, email Handler, CMP Handler, or SCEP Handler. The email Handler requires a mail server. The CMP Handler and SCEP Handler require a CMP enabled client and SCEP router, respectively.

If you are able to submit a certificate request, have the CA issue the certificate, and you can retrieve it, the demo PKI is functioning correctly.

3.3 Setting up an enterprise PKI to secure a VPN

In this example, we are setting up a PKI that issues certificates for VPN end user authentication. The remote certificate applicants generate their own key pairs; the registering entities do not generate keys centrally. Tasks that the UniCERT PKI performs include:

- Registering remote certificate applicants who have been authenticated and have already generated their keys
- Maintaining records of all registered applicants
- Issuing public-key certificates to certify the authenticity of the key holders
- Making the certificates available to the remote applicants who are using web browsers
- Revoking compromised certificates and publishing certificate revocation lists (CRLs)
- Renewing keys and certificates

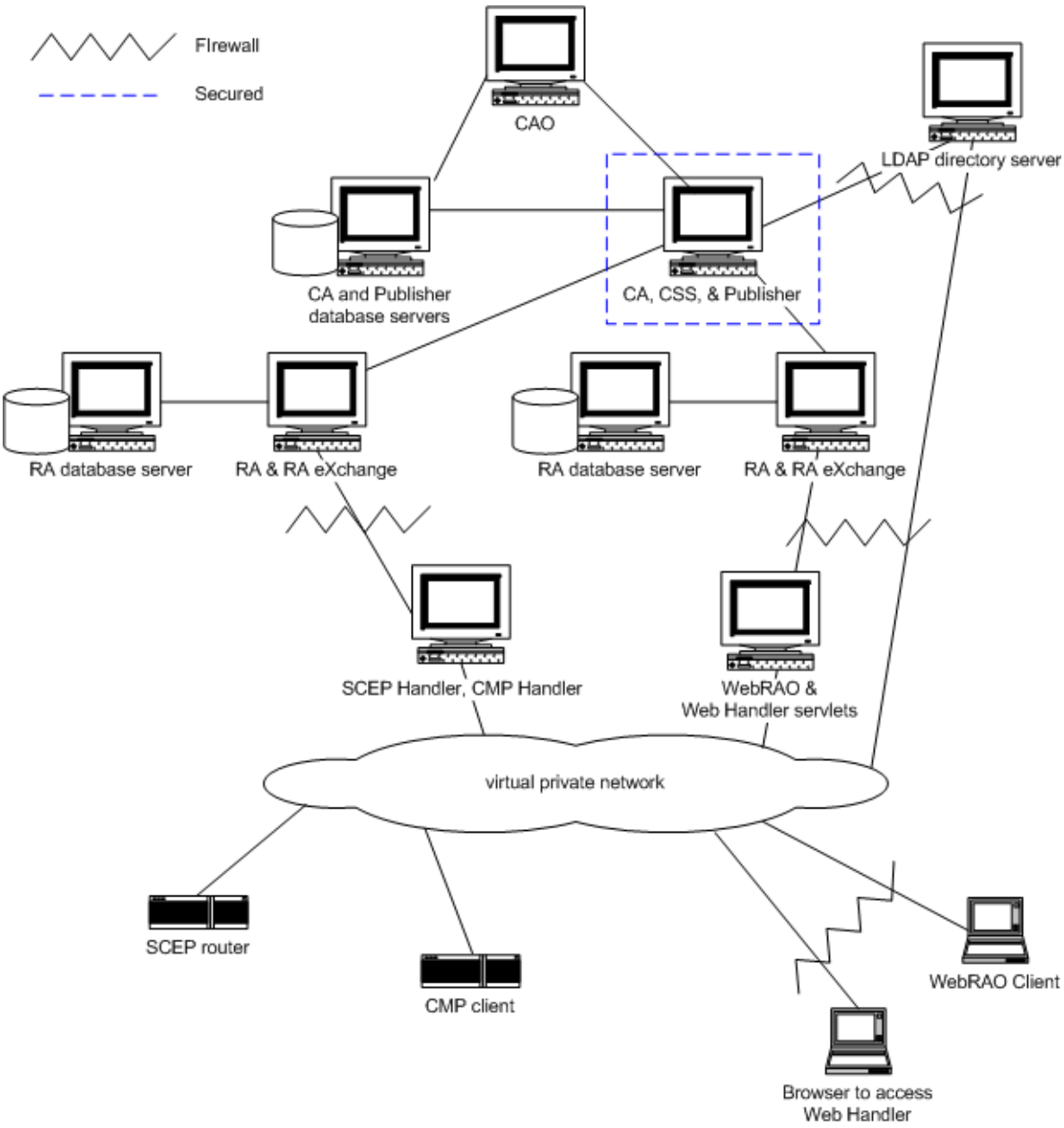
To create a PKI-enabled VPN, perform the same installation and configuration tasks that the demo PKI required (see Section 3.1, *Deciding how to install the UniCERT components*).

As this example is for a large corporation, we assume that the UniCERT CA will issue approximately 250,000 certificates over the next ten years and certificates will be automatically renewed on an annual basis.

Figure 3.2 illustrates one possible deployment that meets these functional requirements, where the CA is kept in a secure location, separate from the other PKI entities. In this example, there is no CA hierarchy; one CA issues certificates for the entire PKI. Depending on the complexity and size of your corporation, you can also implement a CA hierarchy, with one or more subordinate (sub) CA levels for the various divisions in the corporation. With a CA hierarchy, trust chains between the root and sub CAs are important. In addition, you can use additional RAs and RA eXchanges, implementing one pair for each division.

Although Figure 3.2 shows only one WebRAO Client per WebRAO server, you can have multiple WebRAO Clients per server, and you can have multiple WebRAO servers per RA.

Figure 3.2: Setting up a PKI for your corporate VPN



3.4 Setting up a hosted PKI

A hosted PKI meets the same PKI requirements and performs the same tasks as an in-house PKI. The primary difference is that you outsource part of your PKI. Having a service provider

host your PKI entities lets you avail of its security expertise and frees you from the administrative tasks of maintaining your PKI.

In addition to the same installation and configuration tasks completed for the demo PKI (see Section 3.2, *Setting up a demo PKI*), a hosted PKI typically performs the tasks listed in Section 3.3, *Setting up an enterprise PKI to secure a VPN*.

See http://www.verizonenterprise.com/products/security/identity-access/ for information on Verizon's managed hosting services.

3.4.1 Outsourcing the CA

In a hosted PKI, the CA server is always outsourced. The advantages of having a service provider host your CA server are:

- You can rely on the provider's secure facilities, such as a secure bunker, to protect the CA server from unauthorized physical access or damage. Typically, the costs for creating such facilities for your corporation's sole use would be prohibitive.
- The service provider provides key backup management.
- The service provider undergoes physical security audits and is accredited, so you can trust that its security policies and procedures are being implemented correctly.

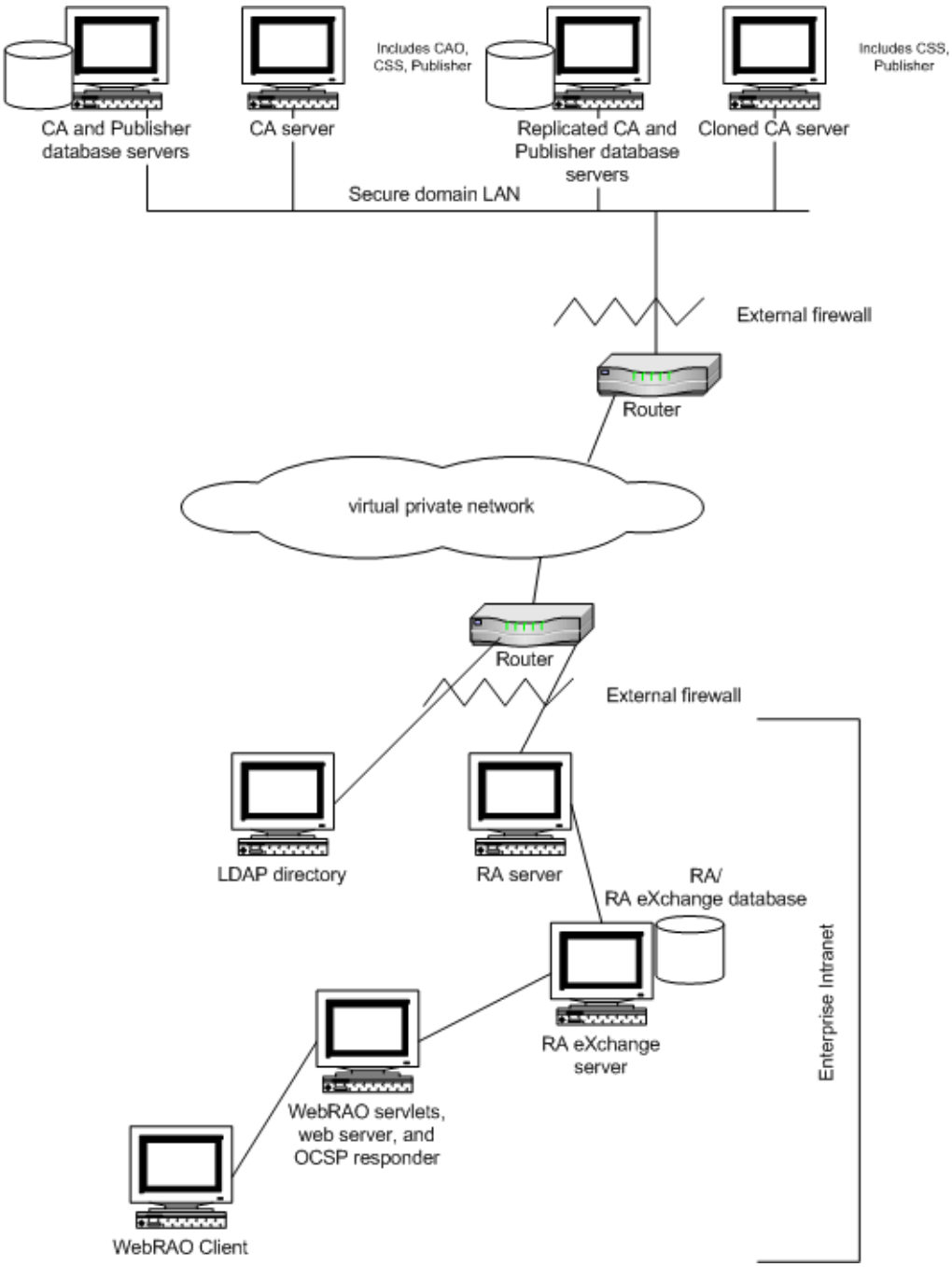
The CA database gets installed on the same computer or in close proximity to its server. Therefore, you outsource both the CA server and its database. Whether you choose to outsource your LDAP server depends on your users' access requirements and your corporate IT policies.

3.4.2 Example 1

The example in Figure 3.3 illustrates a PKI in which a service provider hosts the CA server and its database. Other UniCERT components that need to be in proximity to the CA, such as the CSS, CAO, and Publisher, are also outsourced.

As you only require one CAO for managing the PKI, you do not need a CAO instance for every CA clone. For the UniCERT service components installed on the CA server, such as the UniCERT Publisher, you can install multiple instances as needed. For more information on clones, see Section 4.5.2, *Installing components and their clones*.

Figure 3.3: Outsourcing the CA and related components



3.4.3 Outsourcing the RA

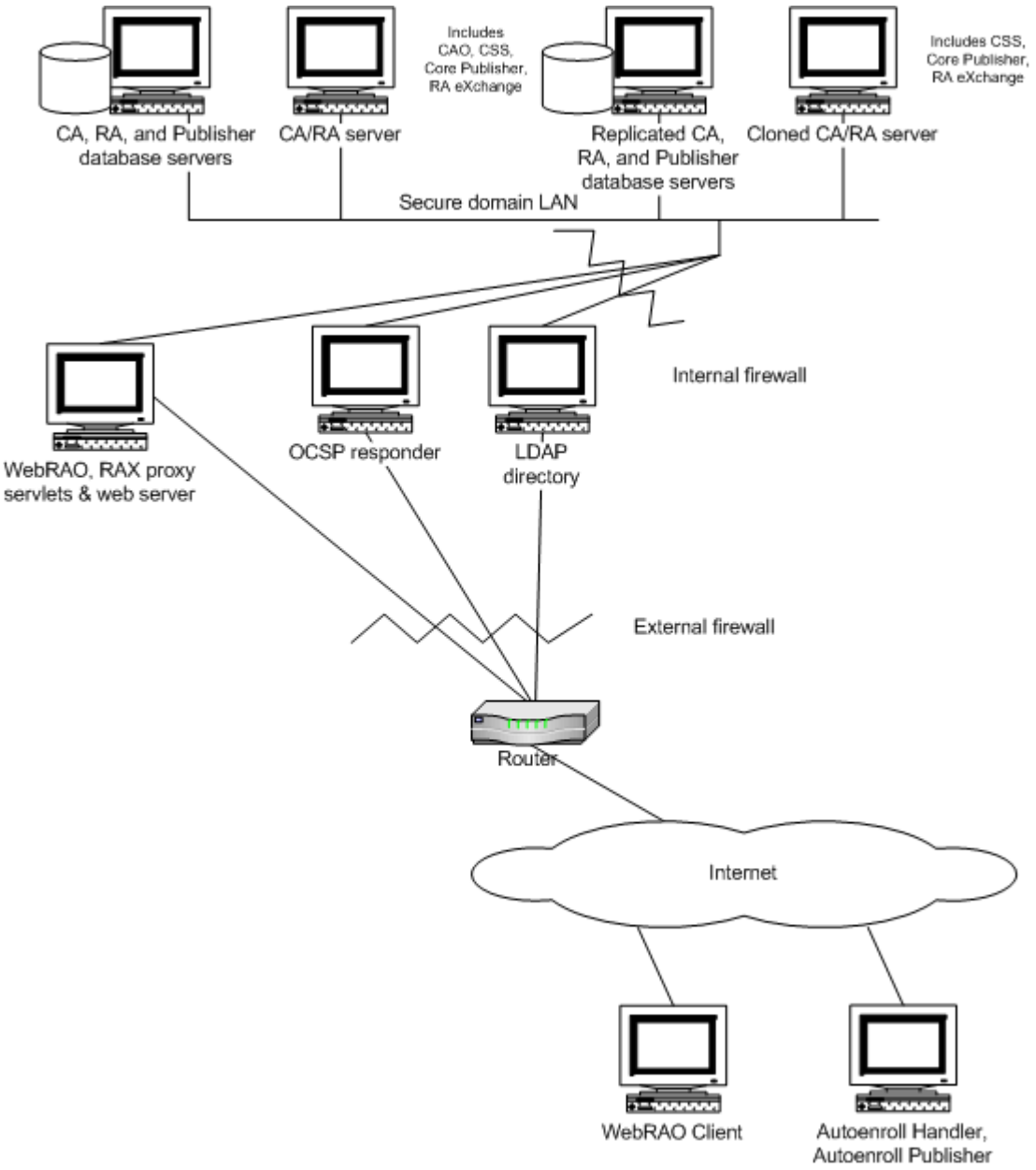
Depending on your legal requirements and the administrative costs of the PKI, you can decide to outsource the RA as well as the CA. UniCERT's architecture, with its separate CA and RA servers, lets you do either:

- If there are privacy constraints about transmitting data externally, you need to keep the RA server within your corporation. For example, within Europe, users' personal data, which forms their digital IDs, cannot cross borders by law. Depending on the location of your corporation and the service provider, you may not have the option of outsourcing the RA.
- You can outsource the RA server and have HR or IT manage corporate data using WebRAOs.
- If the users are local, you may want to manage them locally, as it could be cheaper than the administrative costs of outsourcing the RA server.
- If your corporation does not have an IT department, outsource the RA server.

3.4.4 Example 2

The example in Figure 3.4 illustrates a PKI in which a service provider hosts both the CA and RA servers and a shared database. The Oracle database instance is replicated. This example also assumes that the Publisher in the hosted PKI uses an Online Certificate Status Protocol (OCSP) responder.

Figure 3.4: Outsourcing the CA and RA



4. Installing UniCERT Core

Once you have verified that you meet the necessary hardware and software requirements (Chapter 2, *Installation prerequisites*) and determined how you are deploying your UniCERT PKI (Chapter 3, *Getting ready for your PKI deployment*), you can install the UniCERT Core v5.4 components.

The UniCERT Core v5.4 CD set provides the majority of the UniCERT Core components and utilities. For distributed installations, the UniCERT Web Components v5.4 CD provides the WebRAO servlets and the Web Handler.

Depending on your PKI requirements, you may also need one or more of the other optional UniCERT v5.4 CDs. For more information on the CDs available, see Section 1.2, *How the UniCERT product is distributed*.

⚠ Ensure there is enough space on your system before installing UniCERT v5.4. Otherwise, you may have problems with your installation (see Section 2.3, *Minimum hardware requirements*).

If you have a previous UniCERT version installed, see Section 4.1, *Upgrading from a previous version*.

4.1 Upgrading from a previous version

UniCERT v5.4 now provides the UniCERT service components on Linux. Upgrading to UniCERT v5.4 therefore requires migrating to the supported Linux operating system (see Section 2.1, *Environments supported*). For information and instructions on upgrading and migrating your system, contact Global Support Services (iam-support@verizon.com). Your upgrade path depends on the version you are upgrading from:

- If you have a pre-v5.0 version of UniCERT, be aware that UniCERT v5.4 is not compatible with UniCERT versions prior to v5.0. You cannot migrate directly from UniCERT v3.x to v5.4. You need to migrate to UniCERT v5.2.1 and then to

UniCERT v5.3.8 before you upgrade to UniCERT v5.4. Contact Global Support Services or see the *Migrating from UniCERT v5.x to v5.4 Administrator's Guide*.

- If you are upgrading from UniCERT v5.x to UniCERT v5.4, follow the instructions in the *Migrating from UniCERT v5.x to v5.4 Administrator's Guide*.

If you are upgrading from UniCERT v5.2.1.x, ensure that you do not start the PKI components before you have completed the upgrade to UniCERT v5.4.

4.2 Preparing the information you require

Before installing UniCERT Core v5.4, prepare the following information. For your Oracle database accounts you require:

- A system identifier (SID) for your database instance, which is also its database name
- Account usernames and passwords for your UniCERT components

For your UniCERT components you require:

- Distinguished name (DN) elements
- For software-based components, personal secure environment (PSE) or PKCS#12 filenames and passwords
- For hardware-based components, PINs
- Port numbers if you intend to change them from the UniCERT defaults

---

Ensure that each component instance has a unique port number to prevent possible conflicts.

- A name for the graphical representation of your PKI in the UniCERT CAO.

You also require the following computer information:

- Your computer name
- Your IP address

4.2.1 Sample information

The following demonstrates the information used by a sample CA of Acme Bank:

- SID: AcmeCA
- CA user account: AcmeCA1
- CA account password: AcmeCAUser#1
- DN: cn=Acme Bank Online, ou=New York Branch, o=Acme, c=US
- DN alias: AcmeCA1
- PSE filename: `AcmeCA1.pse`

- PSE password: AcmeCAPassword#1
- Port number: 8764
- PKI name: Online Banking
- Computer name: `foot.example.com`
- IP address: 255.255.255.255

4.3 Installing third-party products

We recommend that you install third-party products destined for use with UniCERT before you install UniCERT Core v5.4. In the case of HSMs and other PKCS#11 devices, install them first so you can generate keys in hardware when you set up the UniCERT components.

You also install Oracle before installing UniCERT, as UniCERT requires a customized database installation; you cannot run UniCERT without it. See the *UniCERT Database Administrator's Guide* for instructions on installing and configuring Oracle. For details of the supported Oracle versions, see Section 2.4.1, *Supported Oracle versions*.

You do not require an Oracle client if you are installing only protocol handlers, the WebRAO, or the optional UPI.

To install any third-party products, do the following:

1. Install any PKCS#11 devices you will be using on the appropriate computers in your PKI if they are not already installed.
2. Install and set up an LDAP directory server if you will be publishing certificates to this type of directory.
3. Install the Oracle database instance or instances on the appropriate server. Follow the instructions in the *UniCERT Database Administrator's Guide*.
4. Install the supported Oracle client for all PKI entities. You need to install the client on any computer on which you are installing one or more UniCERT Core components other than the protocol handlers.
5. Ensure your environment variables are set correctly to include support for UTF8.
6. Set up mail accounts and/or a web server for the RA eXchange, email Handler, and WebRAO, as needed for your PKI.

4.4 Considerations for test or demo core installations

Whether you install components from other UniCERT CDs on the same computer depends on your requirements. For test or demo systems, we assume that you are installing the following on two computers:

- The CAO, RA Auditor, and documentation from the UniCERT Core v5.4 CD on the Windows computer (the necessary utilities are bundled with the CAO).

- The CA, Publisher, CSS, RA, and RA eXchange from the UniCERT Core v5.4 CD on the Linux computer.
- The WebRAO servlets from the UniCERT Web Components v5.4 CD on the Linux computer.

Although you could also access the WebRAO Client in a browser on the Windows computer, we recommend that you access it from a different computer. This enables you to test your PKI setup more accurately.

4.5 Considerations when installing UniCERT components on different computers

The UniCERT components you install, and therefore the CDs you require, vary depending on your PKI requirements. Typically, you install the following components at a minimum:

- The CAO, RA Auditor, and UniCERT documentation from the UniCERT Core v5.4 CD on Windows.
- The utilities and remaining UniCERT components, including one or more protocol handlers as needed, from UniCERT Core v5.4 on Linux.
- The WebRAO servlets and Web Handler from UniCERT Web Components v5.4, as required.
- The WebRAO Client, downloaded via your browser from the WebRAO servlet or installed from the UniCERT WebRAO Client v5.4 CD.

See Chapter 3, *Getting ready for your PKI deployment*, for examples of possible deployments.

As each PKI installation is unique, we focus solely on giving you simple guidelines about installing a distributed PKI. For detailed information on setting up the various UniCERT components once you have installed them, see Chapter 1, *Getting started with UniCERT*, in the *UniCERT Administrator's Guide*. For information on configuring them, see Chapter 1, *Introduction*, in the *UniCERT Configuration Guide*.

4.5.1 Installing components for a hierarchical PKI

If you are building a hierarchical PKI, that is, one with a root CA and subordinate (sub) CAs, install the CA on each computer destined to have the root CA or a sub CA. Install the CAO on a computer in close proximity to each CA instance. For example, your root CA might require additional physical access constraints, and you can install the CAO on another computer that has TCP/IP access to the CA.

We also use the terms single-tier hierarchy, for a PKI that has only the one CA, and multi-tier hierarchy, for PKIs that have one or more levels of subordinate CAs.

Each root or sub CA requires its own database user account. When you install the PKI entities to different computers, remember to specify the correct computer name and, if installing the PKI entities to the same computers, remember to avoid conflicting port numbers during the components' configuration.

You can install and connect multiple RAs to a CA, and you can install more than one RA eXchange for an RA. However, if you have two RA eXchanges connected to one RA, the WebRAOs and Web Handlers can only communicate with one of them. However, the CMP Handler, email Handler, and SCEP Handler, unlike the WebRAO and Web Handler, can communicate with another RA eXchange, provided it is connected to a different RA.

4.5.2 Installing components and their clones

Keep in mind the following considerations when installing UniCERT software for clones:

- The CAO manages both the original CA and its clones, and they all use the same database instance. Similarly, the RA and its clones, the RA eXchange and its clones, and the KAS and its clones share their database instance respectively.
- When an entity is generated in software, the keys, PSE, and user account details for a CA and its clones, an RA and its clones, an RA eXchange and its clones, or a KAS and its clones, are also shared.

  If you have installed a clone on a different computer, you need to transfer a copy of the PSE file, or make the PSE and keys accessible, to that computer as well. You also need to create a crypto profile for the clone if the clone and the original instance are on different computers.
- When implementing clones on different computers, you can generate the original CA's, RA's, RA eXchange's, or KAS's keys in hardware, provided the HSM provides some means of making the keys accessible to another computer. For more information, see Section 20.2, *Cloning from hardware*, in the *UniCERT Configuration Guide*.
- An original instance and each of its clones use a different port number to communicate when you install them to the same computer.
- When installed to different computers, configure the original instance and each clone with the correct computer name.

4.6 Installing UniCERT Core v5.4

The UniCERT Core v5.4 CD for Linux contains the following components:

- The UniCERT CAO and RA Auditor, which are only available on Windows.
- The rest of the UniCERT Core components, which are only available on Linux.

The following sections outline how to install these components on Windows and Linux.

4.6.1 Installing the UniCERT CAO and RA Auditor v5.4 for Windows

If you are upgrading to UniCERT v5.4 from a previous version of UniCERT, see Section 4.1, *Upgrading from a previous version*.

To install the UniCERT CAO and RA Auditor v5.4 on Windows, follow these steps:

1. Log on using an account that has local administrator rights.
2. Install Oracle, including its relevant patches, and any other third-party software you require for UniCERT (see Section 4.3, *Installing third-party products*).
3. Back up your PSEs and RPs, if you have them and have not already done so.
4. Depending on whether you have a previous version of UniCERT installed:
   - Previous version of UniCERT installed: See Section 4.1, *Upgrading from a previous version*.
   - No UniCERT installed: Continue with step 5.
5. Put the UniCERT CAO and RA Auditor v5.4 for Windows CD in your computer's CD drive. The UniCERT CAO and RA Auditor v5.4 installation wizard automatically starts.
6. Select the language you would like to work in and click OK.
7. Click Next on the Introduction screen. The License Agreement screen is displayed.
8. Accept the license agreement and click Next.
9. Specify an installation directory or accept the default, `C:\Program Files\Verizon\UniCERT`, and click Next.
10. Choose the components you wish to install or install all of the components. Click Next.
11. (Windows XP, Vista, and Windows 7 only) To add the UniCERT and Oracle services to your network configuration, leave the default Yes values selected and click Next.

If you do not add these services but are using the default Windows firewall, the services will not run on the more recent Windows clients; you will need to manually update your firewall configuration after the installation to correct this problem.

Vista and XP are intended for the UniCERT client applications and end users.

---

12. If you are not using the Windows firewall, select No and click Next.
13. Review the preinstallation summary information that the installer lists. If the details are correct, click Install.
14. We recommend that you read the `readme.html` as prompted by the installation wizard.
15. Click Done.
16. Eject the UniCERT CAO and RA Auditor v5.4 CD.

17. Reboot the computer to ensure that the components are correctly updated with the system information.
18. Install the remaining UniCERT Core v5.4 components on Linux (see Section 4.6.2, *Installing UniCERT Core v5.4 on Linux*).

4.6.2 Installing UniCERT Core v5.4 on Linux

To install the UniCERT Core v5.4 Linux components, ensure that the `unicert` user account is set up correctly, and complete the preinstallation and installation tasks in this section.

If you require the UniCERT Web components, see Chapter 2, *Installing the UniCERT Web Components*, in the *UniCERT Web Components Administrator's Guide*.

4.6.2.1 Creating a new UniCERT user account

To create a new UniCERT user account, follow these steps:

1. Log in as root.
2. At the shell prompt, use the commands listed in Code example 4.1 to create a UniCERT user account called `unicert`.

Code example 4.1: Defining the user account

```
useradd unicert
```

3. To create a password for this account, use the following command:

```
passwd unicert
```

   Specify a password when prompted and confirm it.
4. Add the sudo package to your system using the following command:

```
yum install sudo
```

5. Add the `unicert` user to the `sudoers` file in the `/etc/sudoers` directory by adding the following entry:

```
unicert ALL=(ALL)ALL
```

If your system administrator requires that more restricted privileges are applied, ensure that the `unicert` user has permission to run RPM installs and can change ownership of files.

4.6.2.2 Completing the preinstallation tasks

Before installing UniCERT, follow these steps:

1. Confirm that you have completed the Oracle preinstallation and install tasks (see the *UniCERT Database Administrator's Guide*).
2. Ensure that Firefox is installed and that the installation directory for your browser is added to the PATH environment variable,
3. If you have a firewall running on a system hosting a UniCERT service, add rules to allow TCP packets to be routed between the relevant UniCERT service port numbers.

4.6.2.3 Installing the UniCERT Core v5.4 Linux components

To install the remaining UniCERT Core v5.4 components on Linux, ensure that the `unicert` user account is set up correctly (see Section 4.6.2.1, *Creating a new UniCERT user account*) before following these steps:

1. Start your computer in an X Windows session and log in as the `unicert` user you defined.
2. Load the UniCERT Core v5.4 CD and change to the `cdrom` device and run the following command:
3. The following RPM installers are provided for UniCERT Core v5.4:
   - `UniCERT_Core-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_CA-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_CSS-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_RA-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_RAX-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_Publisher-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_CMP-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_Email-5.4.0.0-0.x86_64.rpm`
   - `UniCERT_SCEP-5.4.0.0-0.x86_64.rpm`

The RPM installer filenames contain the build number in the format `5.4.0.0-<build number>`. A build number of `0` is used here as an example only; the names of the files provided will contain the final build number.

4. To install an RPM, run the following command:

```
sudo rpm --install <RPM package name>
```

where <RPM package name> is replaced by the name of the RPM installer you are running.

You must install UniCERT_Core-5.4.0.0-0.x86_64.rpm first; the install will fail if you try to install the other components first.

UniCERT Core v5.4 is installed to /usr/local/ by default and the installation creates the directory structure /usr/local/Verizon/UniCERT and /usr/local/apps.

You can change the UniCERT Core RPM's installation location using the relocate command, for example:

```
sudo rpm --install UniCERT_Core-5.4.0.0-0.x86_64.rpm --relocate /usr/
local=/home/unicert
```

5. Install the UniCERT Web Components v5.4 and other, advanced UniCERT components v5.4 on their respective computers. See the guides that are applicable to the components you have purchased:
   - The *UniCERT Web Components Administrator's Guide*
   - *UniCERT Key Archiver Administrator's Guide*
   - *UniCERT ARM v5.3.5 Installation Guide*
   - *UniCERT Autoenroll Administrator's Guide*

4.6.3 Using the main menu

Once you have completed the preinstallation steps and installed UniCERT, you can use its Main Menu to access the UniCERT utilities and documentation on Linux. The UniCERT Main Menu requires access to xterm, a terminal emulator (see Section 2.4.2, *Installing xterm*).

To use the Main Menu, ensure that you started your computer in an X Windows session and log in as the unicert user you defined and used when installing UniCERT. Change to the UniCERT installation directory, <install_location>/Verizon/UniCERT and enter ./MainMenu.sh at the shell prompt. It lists the UniCERT Core utilities and documentation.

For information on using the UniCERT utilities, see the *UniCERT Administrator's Guide*.

4.7 Installing optional UniCERT components

The following UniCERT components are advanced, optional components. For a description of these components and how they are distributed, see Section 1.2, *How the UniCERT product is distributed*.

- Autoenroll: For instructions on installing the UniCERT Autoenroll v5.4, see the *UniCERT Autoenroll Administrator's Guide*.

- Key Archiver: For instructions on installing the UniCERT Key Archiver v5.4, see the *UniCERT Key Archiver Administrator's Guide*.
- Installing ARM: For instructions on installing the UniCERT ARM v5.4, see the *UniCERT ARM v5.3.5 Installation Guide*.
- Installing UPI: For instructions on installing the UniCERT UPI v5.4, see the *UniCERT UPI Installation Guide*.

4.8 Uninstalling UniCERT Core

If you wish to remove your UniCERT v5.4 installation permanently, including your crypto profiles, PSEs, and registration policies:

1. Log in as the UniCERT user.
2. To stop the UniCERT instances, select Main Menu>Service Manager and then use the T (Terminate an instance) option to stop each service.
3. Remove each service. To do this, use the D (Delete an instance) option to delete the instances.
4. Exit the Service Manager.
5. Run the following command to locate your RPM packages:

```
rpm -qa|grep UniCERT
```

6. Remove each UniCERT component using the following command.

Code example 4.2: Removing RPMs

```
sudo rpm -e <RPM package name>
```

where <RPM package name> is replaced by the name of the RPM installer you are removing.

You must uninstall UniCERT_Core-5.4.0.0-222.x86_64.rpm last; the uninstall will fail if you try to remove it first.

7. On your Windows computer, remove the CAO and RA Auditor using Start>Control Panel>Add/Remove Programs.

8. Remove UniCERT Core. The installed UniCERT products are listed in the Add/Remove Programs screen.
9. Manually delete the UniCERT installation directory, which may contain PSEs or registration policies that you created.

The registry directory structure `<install location>/apps` is not deleted. If you want to remove the registry directory before reinstalling UniCERT, delete it manually.

Your organization must perform a threat analysis to identify the level of risk involved if deleted certificate and key files are recovered maliciously or fraudulently. The level of protection needed to ensure that unauthorized people cannot recover the files from the hard disk after deletion may extend to destroying the physical media. We recommend the following as the minimum requirements for secure deletion.

On Linux:

- Rename the file.
- Overwrite the data in the file with zeros using a low level file overwrite utility.
- Delete the link to the file using the `rm` command line option.
- Delete the swap space on the relevant device.

  You can optionally secure the physical media by overwriting the disk using the `format(1MTSOL)` command. You can then degauss and destroy the disk if necessary (as outlined in: http://www.oracle.com/technetwork/server-storage/solaris/overview/purge-135585.html).

On Windows:

- The file deletion bypasses the Windows Recycle bin.
- Zeros are written over the file contents after deletion, for example, by using a secure file or disk deletion utility.
- As an additional precaution, delete the Windows swap file contents.

For additional security, make an independent assessment of the commercially available system utilities that provide secure file deletion.

A. Using UniCERT in its evaluated configuration

This appendix provides guidance on how to configure UniCERT in its mandatory Common Criteria EAL4+ evaluated state.

In addition, this documented configuration serves as an example of a PKI implementation, and this appendix also provides best practice guidelines for designing and managing your PKI. Where appropriate, we indicate additional security measures you can implement when setting up your UniCERT v5.4 PKI.

The *Security Target for Verizon UniCERT v5.3.4* provides further information on the evaluated configuration and on using nonevaluated components, such as the CMP Handler, ARM, and UPI, with it. The *Security Target* supersedes information in this appendix.

The Common Criteria specific documents are not included in the UniCERT v5.4 documentation set provided with the UniCERT Core. Contact Global Support Services (iam-support@verizon.com) if you require them.

A.1 Putting UniCERT in its evaluated configuration

There are several possible evaluated configurations for UniCERT. A model of one particular configuration is provided at the end of this appendix (see Figure A.1).

In brief, for UniCERT to operate in its evaluated configuration:

- Start services manually using the Service Manager. Do not configure services such as the CA, RA, RA eXchange, and CSS to start in automatic mode. Using automatic mode means that the passwords and PINs used to open the private keys of these entities are stored on the computer where the Service Manager is installed.
- Ensure authorization groups are assigned in RPs; do not enable the No Authorization option. For example, set up authorization for the RPs used by the protocol handlers so any requests they pass to the RA are authorized by the WebRAO Client user. Authorization is an important mechanism for you to ensure third party approval for certificate requests.

- Use a Common Criteria EAL 4+ accredited HSM or smart card in conjunction with UniCERT for storing root keys, as they provide tamper detection. See Section A.5, *Configuring components to work with UniCERT*, for the accredited versions of smart cards and HSMs.
- The UniCERT components ARM, CMP Handler, and UPI have not been evaluated as part of the UniCERT v5.4 evaluation; however, they could be included in an evaluated configuration of UniCERT, provided a separate evaluation of each such component (when installed in the PKI environment) is successfully performed.
- Define an audit policy for your PKI that assures independence of the appointed auditor and clearly states the frequency of the audit process, as well as how security-related event logs are dealt with and reported.
- Promptly dispose of all authentication data for an administrator whose access rights have been removed. Revoke the certificate. Destroy the data using the key destruction functions of UniCERT and the HSM or smart card where keys are stored. Remove the associated entity from the PKI.
- Set the clocks on the computers in your PKI from a trusted, accurate, and reliable time source to ensure that an accurate time source is used to timestamp audit records.
- Implement security-related patches as soon as you receive them. For more information, contact Global Support Services (iam-support@verizon.com).

A.2 Designing your PKI

We recommend that you take some time to design your PKI before you implement, test, and deploy it. The cornerstone of any PKI design is the CA. It provides the ultimate point of trust, and it is a primary requirement of good PKI design that the CA is secure at all times. If a CA system is compromised, the entire PKI is compromised.

When designing a PKI, consider the following factors.

A.2.1 How many UniCERT components?

What is the processing power available to you? This determines how many UniCERT components you can install on any one computer and how you distribute them. This in turn affects the way in which you secure each component. For a list of the UniCERT components permitted in evaluated configurations, see Section A.8, *Security enforcing UniCERT components*.

The CAO, KAO, WebRAO Client, and RA Auditor components are only available for the Windows platform.

A.2.2 How is your PKI distributed?

Is your PKI geographically dispersed? If it is, consider how you wish to control access to the various PKI entities, as well as who will manage them.

Most UniCERT components are licensed independently, and you must have adequate licenses for your installation. Contact the Verizon contracts department if you have any queries on the licensing of the components you have purchased, or your Verizon representative if you require additional component licenses.

A.2.3 Planned hierarchy

Will there be one single security officer/system administrator to manage the entire PKI? If possible, use several administrators with responsibility and defined privileges for different components. See Section A.6.4, *Defining separate roles*.

A.2.4 Separate database accounts

Create separate accounts on the CA and RA databases for each PKI entity. This means that in the event of their becoming untrustworthy, revoking the entity from the PKI is relatively straightforward. See Section A.6.7, *Deleting unauthorized users from the PKI*, and Section 2.3.3, *Deleting a user account or database*, in the *UniCERT Administrator's Guide*.

A.2.5 Access to tokens

If the HSM you use to protect access to the CA has an M of N feature, enable M of N when initializing the HSM tokens. This offers added security because more than one person is required to log onto the HSM at CA startup. Consult the HSM vendor's documentation for details on how to enable M of N.

A.2.6 Testing your PKI installation

Test your PKI installation before you deploy it. Suggestions for test activities include:

- Test that the certificate extensions in the policies work as you expect.
- Use the certificates in environments that simulate how they will eventually be used.
- Test that the protocol handler and the WebRAO Client can process an applicant's certificate request, receive a certificate from the CA, and then revoke the certificate. For more information, see *Testing the WebRAO Client* in the *UniCERT WebRAO Client User's Guide*.

A.3 Assumptions about administrators

Using UniCERT in its evaluated configuration is based on the following assumptions about you, the PKI administrator, and your staff:

- You have read the installation and user documentation supplied with the UniCERT release, and you have followed the instructions contained in these documents for setting up and using UniCERT.
- You understand how UniCERT works and how to implement security features for the various entities in your PKI.
- You are sure all operators and administrators working on your PKI are competent and they can implement cryptographic operations correctly.
- Your staff—especially those in charge of the CA, CAO, and RA—are trustworthy.
- You properly dispose of authentication data and associated privileges.
- The authorized auditors regularly review audit logs.

In addition, we assume that you are familiar with, and observe, the security requirements of your organization's Certification Policy (CP) and CPS. This is especially important when you are setting up RPs. See Section 1.4, *Formulating a Certification Practices Statement*, in the *UniCERT Product Overview*, and Chapter 2, *Defining registration policies for certification*, in the *UniCERT Configuration Guide*.

A.4 Keeping UniCERT secure

Given that UniCERT contains confidential information about end users in your PKI, it is essential that you prevent unauthorized people from accessing it. The following guidelines for keeping UniCERT secure underpin the requirements for setting UniCERT up in its Common Criteria evaluated configuration.

To operate UniCERT securely, we recommend the following:

- Secure the computers on which UniCERT components are running by physically restricting who has access to the computer as well as by using the operating system access control features, for example, logon accounts.
- Disable all unnecessary network services (for example, web services) on the computers on which UniCERT components are running.
- Disable remote access to the registry. On Linux, UniCERT creates its own registry for storing component settings in `$HOME/apps`, which is defined during the installation.
- Do not share out the directories in which the component executables/shared libraries reside over the network.
- Do not install or run executables on, or from, a network drive.
- Install all of the UniCERT components behind a firewall.
- Create a backup copy of each component's PSE file and store it securely in case the original file gets corrupted or is accidentally deleted.
- Create and store backups of the file system or RA/CA/KAS databases securely.
- Enforce changing passwords in Oracle for your UniCERT accounts.

- Keep passphrases secure. We recommend that you periodically change the passphrases protecting PSEs, PKCS#12 files, and PKCS#11 devices using the UniCERT Token Manager.
- Revoke an entity's user account on a database, if that entity becomes untrustworthy.
- Back up the CA's, RA's, and KAS's database on a daily basis (see Section 5.1, *Backing up databases*, in the *UniCERT Database Administrator's Guide*). The backup copies of the databases are an important resource when you are investigating security-relevant event logs, for example, if you detect events that do not verify during routine monitoring of audit logs.

A.5 Configuring components to work with UniCERT

The security of your PKI deployment depends on the security enforcing functionality of the components you routinely operate in conjunction with UniCERT.

Protect the CA and RA keys with HSMs. Consider the following when you are configuring components to work with the UniCERT installation in its evaluated configuration:

- Ensure you use a HSM with sufficient cryptographic hardware validation, which is Common Criteria EAL 4+ accredited.
- A HSM that also provides passive detection of physical tampering, such as tamper-detection seals, locks, and zeroization switches.
- Ensure you use a smart card with sufficient cryptographic validation, which is Common Criteria EAL 4+ accredited.

A.6 Best practice guidelines

When managing your PKI, observe the following best practice guidelines.

A.6.1 Backing up your PKI

Back up the CA, RA, and KAS databases on a regular basis, preferably daily. Backup copies of your databases are important when reviewing security-related audit event logs: Individual administrator actions are traceable through the digitally signed event logs.

It is also important to create backup copies of PSE files and tokens for each PKI entity in case the original file becomes corrupted or is deleted. Store the backup copies of your data or PSE files securely. For example, store backup copies of PSEs and tokens on hardware where they cannot easily be accessed. If you store your backup copies of data or files on memory stick, optical media, or magnetic tape, store them securely under lock and key or in a fire-proof safe.

A.6.2 Passwords and PINs

Create strong passwords for system and user accounts on CA, RA, and KAS databases and change them regularly. When using ASCII characters to create passwords, use a mixture of alphanumeric characters and a minimum of eight characters, for example, `Passphrase1!`

The CAO, the Token Manager, and the WebRAO Client software automatically enforce strong passwords when you create passphrases for PSE and PKCS#12 files. If you are using non-ASCII characters, however, this enforcement does not apply. Your non-ASCII passphrase must be eight characters in length.

Depending on the smart card you use, the vendor application may enforce constraints when you create PINs. We recommend that you

- Regularly change the PIN used by administrators to access smart cards and tokens.
- Remove your PKCS#11 token or smart card from the PKCS#11 reader if you log off and leave the computer for any reason.

If you require dual control, for example, at the CAO or KAO, we suggest that you implement separate roles for multiple CAO or KAO users instead (see Section A.6.4, *Defining separate roles*). Otherwise, a possible solution would be to rely on your smart card vendor's dual control system if one exists.

If you, or any other system user, forget your password or PIN or you lose your smart card, we recommend that you do not allow for password or PIN recovery. For example, if one WebRAO Client user loses his smart card, another WebRAO Client user logs onto the WebRAO Client and performs the necessary approvals.

If the WebRAO Client user loses his smart card, you need to revoke the certificates using either the CAO or the WebRAO interface to prevent someone else using the smart card (assuming they have the PIN) and issue new keys, certificates, and smart card to the user. If just the PIN for the smart card has been forgotten, you need to revoke the certificates on the smart card and reinitialize the smart card using the Token Manager (or destroy the smart card).

A.6.3 Authorization groups

Restrict the types of certificates a WebRAO Client user is authorized to work with and the functions she can perform (authorize certificate requests, revocation requests, and renewal requests, or suspend and unsuspend requests) by defining appropriate authorization groups and assigning these to the appropriate RPs. Include two or three authorization groups to make an authorization path for added security. See Chapter 3, *Working with registration policies*, in the *UniCERT Configuration Guide*.

Do not select the No Authorization is required option in RPs for authorizing entities such as the WebRAO Client or the ARM administrator.

A.6.4 Defining separate roles

When you are setting up your PKI, ensure that the CAO user, the audit log user, and the user who archives audit logs are separate, trustworthy people. It makes sense that the person who audits event logs and reports suspected deletions or security-related events is not the same as the person who implements corrective action.

Therefore, we recommend that you set up a minimum of three CAO users:

- The main CAO user with full rights
- A CAO user with rights to audit the event logs
- A CAO user with rights to archive the event logs

The use of three CAO users means that only one accountable user, the main CAO user, can modify the PKI and that the audit logs are tamper-evident. If your organization does not have the resources for three CAO users, you can define two CAO users—one with full rights, the other with permission to both audit and archive the event logs.

To use UniCERT in its Common Criteria EAL4+ evaluated state, ensure that you set up three CAO users.

Similarly, if you are using the optional UniCERT Key Archiver, you can define separate roles for the KAO.

A.6.5 Auditing your system

Regularly review audit logs to identify any tampering or security-related issues that occur while your PKI is running.

A.6.6 Defining an audit policy

Define and implement an audit policy for your PKI. Ensure that the policy specifies when appointed auditors review logs, what constitutes a security-relevant event, and that auditors act promptly on any suspicious audit log entries. The procedure for reporting problems should be explained clearly in your policy.

To assist the auditor role, UniCERT offers individual accountability for all transactions carried out in the PKI. UniCERT also supports the detection of unauthorized deletion of data from its audit logs.

A.6.7 Deleting unauthorized users from the PKI

When an administrator leaves your organization or ceases her role in your PKI for some other reason, revoke that user's certificate, remove the associated entity from the PKI, and remove her user accounts on the CA or RA database immediately. In this way, an unauthorized person cannot access your PKI, even if she still has her keys. For information on deleting and revoking PKI entities, see Chapter 7, *Defining your PKI*, and Chapter 24, *Administering certificates*, in the *UniCERT Configuration Guide*, as well as Section 2.3.3, *Deleting a user account or database*, in the *UniCERT Administrator's Guide*.

The following paragraphs suggest a course of action if the relevant PKI entity user becomes untrustworthy.

A.6.7.1 CAO or KAO users

If the CAO or KAO user becomes untrustworthy, revoke the CAO or KAO user entity in the PKI and remove his user account from the CA or KAS database respectively.

However, if the CAO or KAO user is the CAO or KAO with permission to create other CAOs or KAOs:

1. Create a new CAO or KAO user account and password on the CA database or KAS database respectively.
2. Set the CAO or KAO user permissions to enable him to do everything.
3. Revoke the CAO or KAO user who is no longer trusted.

A.6.7.2 System administrator

If the system administrator in charge of your PKI leaves your organization or becomes untrustworthy:

1. Appoint a new system administrator without delay.
2. Create a new account for the system administrator on the CA database and enter new passwords protecting both the user account and the root keys on all computers where the database and PKI software is installed.
3. Delete the old system administrator user account.

A.6.7.3 RA Auditor and WebRAO Client user

The RA Auditor and WebRAO Client user are the only other entities in your PKI that are associated with people. If the administrator of either becomes untrustworthy for some reason, take the following steps to restore the security of those entities:

1. Appoint a new RA Auditor or WebRAO Client user.
2. Create keys and certificates for the new RA Auditor or WebRAO Client user.
3. Create a new user account for the entity concerned on the RA database.
4. Revoke the entity who is no longer trusted and delete his account on the RA database.

A.7 Logical and physical protection of your PKI

In addition to the secure practices you observe when you set up your PKI, also consider the physical and logical protection of your system once you have deployed it.

Here are some suggestions for protecting the components of your PKI.

A.7.1 CA, KAS, RA, and RA eXchange

The computers on which sensitive entities, such as the CA, CAO, RA, RA eXchange, and KAS, are deployed are the most vulnerable in your PKI. They require the most stringent protection to prevent access by unauthorized users.

Physically protect the CA database server and the CA computer by doing the following:

- Keep the computer in a secure room where access is restricted to authorized users.
- If possible, use an HSM to control secure access to the computer.
- Where your HSM supports it, enforce M of N access at startup.

We recommend you use a HSM that has Common Criteria EAL 4+ accreditation with the evaluated configuration of UniCERT.

Physically protect the RA database server, the RA computer, RA eXchange computer, and the KAS computer by doing the following:

- Keep the computer in a secure room where access is restricted to authorized users.
- Depending on the sensitivity of your data, use either an HSM or a smart card to control secure access to the computer.

Logically protect the computers supporting the CA, CAO, RA, or the RA eXchange:

- Disable all communication ports that are not in use by the CA, CAO, RA, and RA eXchange, especially telnet ports.
- Disallow web browsing from the CA, RA, CAO, RA Event Viewer computers (this includes any computer where the RA Auditor uses the RA Event Viewer), and RA eXchange.
- Change user passwords and PINs regularly.
- Restrict the installation of third-party software.
- Limit access to the Internet or company LAN.

Logically protect any PKI entity that performs an auditing role.

A.7.2 Other PKI entities

Other PKI entities, such as the CSS, Publisher, the protocol handlers, and WebRAO, require less stringent security measures to protect them from unauthorized access. This does not mean that they do not require protection, but rather that you can implement less expensive security measures.

The PKI entities listed here do not require physical protection in secure bunkers. Provide logical protection for these entities as follows:

- Install the CSS computer behind a firewall.
- Install the Publisher, which connects to LDAP directories, on a computer behind a firewall.
- Both the WebRAO and the Web Handler operate across the internet and also on intranets. Install the WebRAO servlet and the Web Handler on a web server behind a firewall.

- Use SSL to encrypt traffic between the Web Handler and WebRAO servlets.
- Enforce regular timeouts for WebRAO Client users to ensure that only an authorized user is working on the computer.
- If you uninstall the WebRAO Client, ensure you securely delete private key files. See *Security issues when uninstalling* in the *UniCERT WebRAO Client User's Guide*.
- Change the passwords on user accounts regularly.

A.8 Security enforcing UniCERT components

The PKI configuration suggested in Section A.9, *Example of an evaluated configuration of UniCERT*, is based on the following assumptions about the security enforcing functions of UniCERT components.

The components listed below have security enforcing functions. Any PKI using UniCERT in its evaluated configuration can include one or more of these components. Table 1 also contains a link to the documentation where you can find additional information on these components.

Table 1: UniCERT components and documentation

UniCERT component	Related documentation
CA	See Chapter 5, *Configuring a CA entity*, in the *UniCERT Configuration Guide*.
CAO	See Chapter 6, *Configuring a CAO entity*, in the *UniCERT Configuration Guide*.
RA	See Chapter 8, *Configuring an RA entity*, in the *UniCERT Configuration Guide*.
RA Event Viewer (RA Auditor provides an auditor role rather than a security enforcing one)	See Chapter 9, *Configuring an RA Auditor entity*, in the *UniCERT Configuration Guide*.
RA eXchange	See Chapter 10, *Configuring an RA eXchange entity*, in the *UniCERT Configuration Guide*.
CSS	See Chapter 11, *Configuring a CSS entity*, in the *UniCERT Configuration Guide*.
email Handler	See Section 12.2, *Configuring an email Handler entity*, in the *UniCERT Configuration Guide*.
SCEP Handler	See Section 12.3, *Configuring a SCEP Handler entity*, in the *UniCERT Configuration Guide*.

A. Using UniCERT in its evaluated configuration

Table 1: UniCERT components and documentation

UniCERT component	Related documentation
Web Handler	See Section 13, *Creating and using a Web Handler entity*, in the *UniCERT Configuration Guide* and the UniCERT Web Components v5.4 documentation set.
WebRAO	See Section 15, *Creating and configuring a WebRAO Client entity*, in the *UniCERT Configuration Guide* and the *UniCERT WebRAO Client User's Guide*.
Database Wizard (this is part of the TOE but does not have any security enforcing functions)	See Section 2, *Using the Database Wizard*, in the *UniCERT Administrator's Guide*.
UniCERT Core Publisher	See Section 1, *Introduction*, in the *UniCERT Publisher Administrator's Guide*.
Key Archiver	See Section 18, *Configuring a KAS entity*, and Section 19, *Configuring a KAO entity*, in the *UniCERT Configuration Guide* and the UniCERT Key Archiver v5.4 documentation set.
Autoenroll Handler	See Section 17, *Configuring an Autoenroll Handler entity*, in the *UniCERT Configuration Guide* and the UniCERT Autoenroll v5.4 documentation set.
Autoenroll Publisher	See the UniCERT Autoenroll v5.4 documentation set.

The following components have not been evaluated as part of the UniCERT v5.4 evaluation; however, they could be included in an evaluated configuration of UniCERT, provided a separate evaluation of each such component (when installed in the PKI environment) is successfully performed:

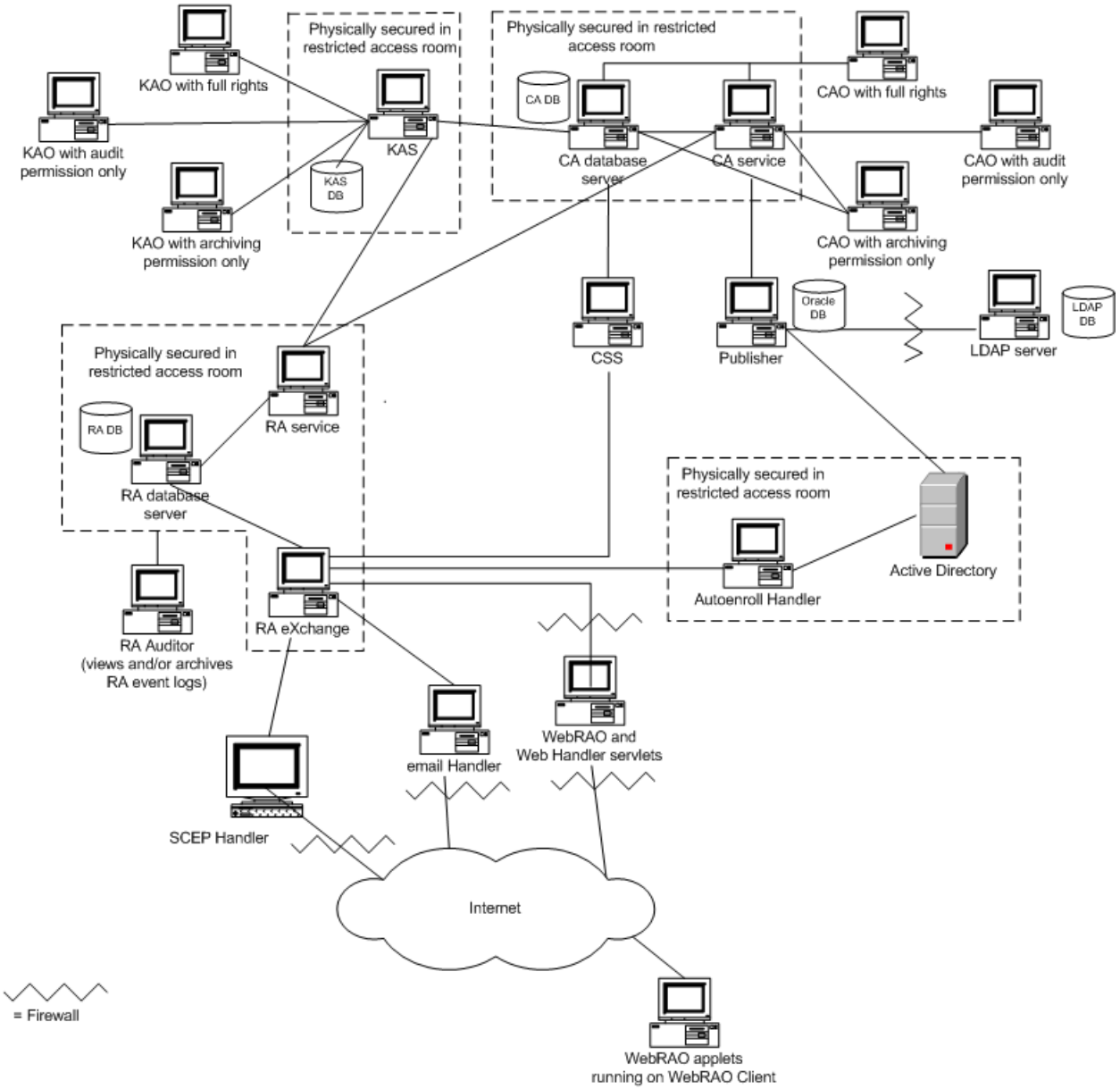
- ARM
- UPI
- CMP Handler

A.9 Example of an evaluated configuration of UniCERT

In this example of an evaluated configuration of UniCERT, we do not consider certain details about the PKI deployment. For example, it is up to you to determine the projected capacity of the PKI, how certificates will be renewed, or where the Oracle database is installed. These are issues that affect the performance of your PKI, but they do not directly affect its secure functioning.

The sample PKI illustrated in Figure A.1 is one of several evaluated configurations possible for UniCERT. Be aware that there are other possible configurations and these are described, but not illustrated, in the Verizon Security Target document.

Figure A.1: A secure PKI configuration with Autoenroll in your enterprise



A. Using UniCERT in its evaluated configuration

This sample evaluated configuration has the following features:

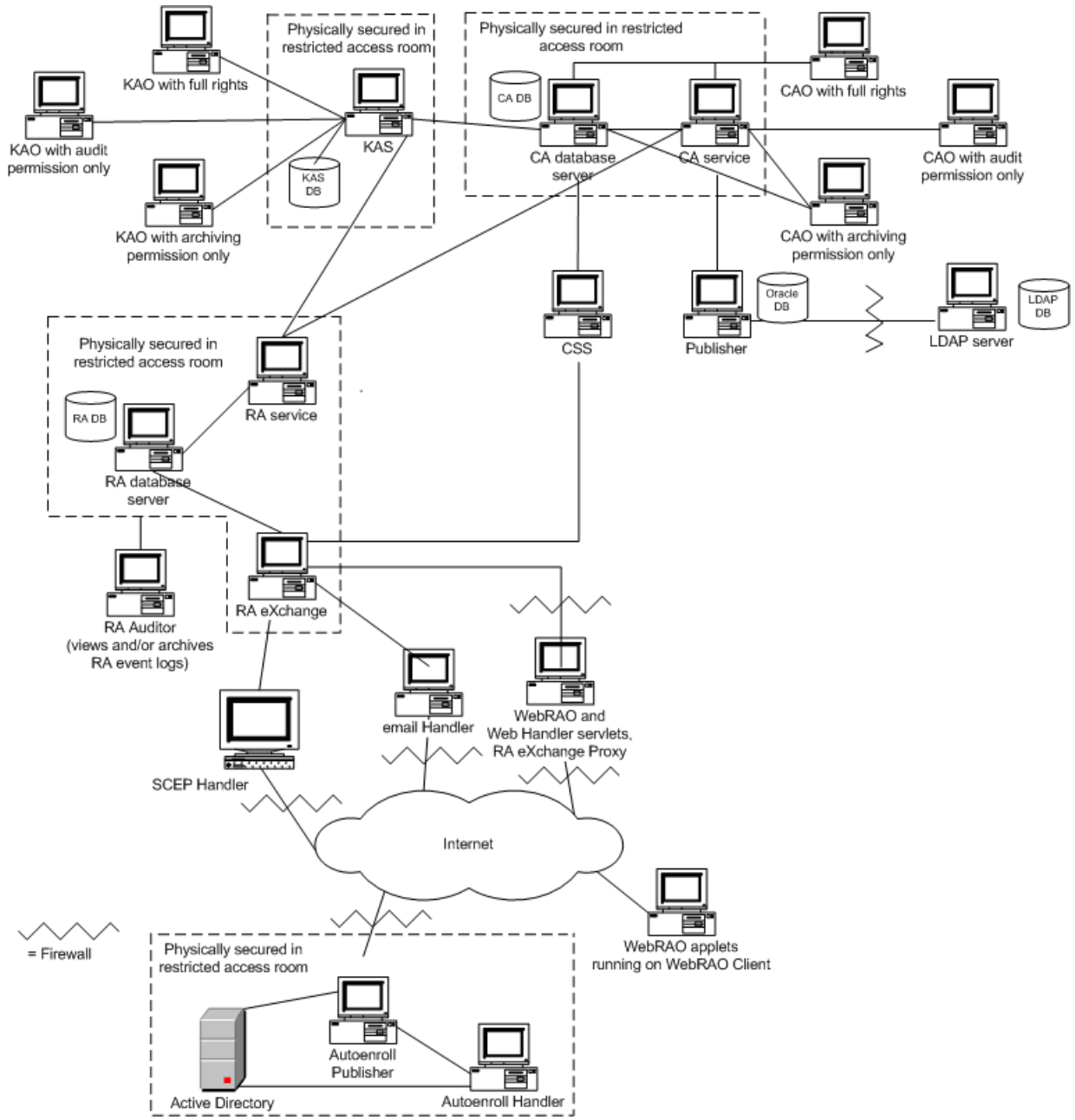
- The CA database server is stored on a computer that is secured in a locked room together with the CA computer. All unnecessary network services are disabled on these computers.
- Access to the CA is restricted to the overall system administrator (or security officer) and where possible protected by the M of N feature of the HSM used to store and manage the root CA keys. The CA service is started manually in the Service Manager.
- The CAO role is split between three CAO administrators. One administrator is in charge of a CAO that has full rights. This person is also the overall system administrator (or security officer). Access to the CAO computer is password controlled. This administrator follows organization policy on auditing event logs, reviews them on a regular basis, and acts upon any suspicious events. This person is trustworthy. There is a second CAO administrator with rights to audit event logs only, and a third CAO administrator with rights to archive audit logs only. This ensures the separation of roles whereby the person who audits event logs and reports suspected deletions or security-related events is not the same as the person who implements corrective action.
- The CSS is connected to the CA database server, and the service is started manually in the Service Manager. It passes on information about the status of a certificate, as OCSP responses, through the RA eXchange, to entities requesting certificate status information. All communication ports not required for connections to the CA and the RA eXchange are disabled.
- The RA database server is physically protected in a secured room together with the RA computer. Access to the RA and the RA service is restricted to the overall system administrator (security officer), and the RA service is started manually in the Service Manager.
- The RA Auditor is a trusted administrator who monitors events, including security-related events, at the RA. She also archives event logs off the RA database.
- The RA eXchange communicates with the RA database server and is physically secured in the same secure room as the RA database server and the RA computer. It is also connected to the CSS, a WebRAO servlet, a Web Handler, as well as an email Handler. In this case, there is a single RA eXchange connected to the RA service but there may be more than one. The RA eXchange is protected behind a firewall.
- The KAS, which securely archives private keys, received via the RA and the KAO components, to the KAS database and is physically secured in a restricted access. The KAO role is split between three KAO administrators. One administrator is in charge of a KAO that has full rights. This person is also the overall system administrator (or security officer). Access to the KAO computer is password controlled. This administrator follows organization policy on auditing event logs, reviews them on a regular basis, and acts upon any suspicious events. This person is trustworthy. There is a second KAO administrator with rights to audit event logs only, and a third KAO administrator with rights to archive audit logs only. This ensures the separation of roles whereby the person who audits event logs and reports suspected deletions or security-related events is not the same as the person who implements corrective action.

- The Autoenroll Handler, communicates with the RA eXchange but unlike other protocol handlers, can he hosted on an external system. The Autoenroll Publisher, which functions in a similar manner to the Core Publisher, but, because it needs to be co-located with the Autoenroll Handler, may be hosted on an external system. Hence, the CA communicates with the Autoenroll Handler, via the RA eXchange rather than with the Autoenroll Publisher directly. Figure A.1 shows the Autoenroll solution deployed with all the UniCERT entities in your enterprise. Figure A.2 shows the Autoenroll solution in a hosted environment, where the Autoenroll Handler and the RA eXchange are communicating via the Internet, and therefore they also require SSL to secure their BRSP messages.
- The computer containing the WebRAO servlets also contains the Web Handler software. They are protected behind a firewall from the requests they receive from end entities, and they use SSL to encrypt the traffic between them. Access to the WebRAO Client is protected using private key timeout, and the user provides an authorization path before she passes any requests she receives, either directly or from the Web Handler, to the RA eXchange.
- The email Handler receives remote email requests from end entities over the internet via the mail server and interfaces with the RA eXchange to pass those requests to the CA. It notifies end users of the status of their request for a certificate, and it is configured to send them their signed certificate when it is ready. The email Handler is started manually in the Service Manager. All communication ports are disabled, except those on which the email Handler gets communications from the RA eXchange or connects to the mail server. As the mail server listens on the POP port, the email Handler requires no ports open to the internet.

We strongly recommend that you install and test a demonstration version of your PKI before you commission it.

A. Using UniCERT in its evaluated configuration

Figure A.2: A secure PKI configuration with Autoenroll in a hosted environment



Index

Index

R

S

T

Index