



UniCERT

Version 5.2.1

Installation Guide for Windows

The information in this document is subject to change without notice and does not represent a commitment on the part of Betrusted. Betrusted does not accept any responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used only in accordance with the terms of such license. The documentation is issued in confidence for the purposes only for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under an agreement or with the consent in writing of Betrusted, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Betrusted.

UniCERT is a trademark of Betrusted. Oracle is a registered trademark of Oracle Corporation. Other trademarks used throughout this publication are the property of their respective owners.

All URLs given were active at the time of going to press. Betrusted makes no guarantee of their continued validity and takes no responsibility for their content.

Written and published by Betrusted.

Copyright © Betrusted 2004

All Rights Reserved.

License and credits

Betrusted licenses UniCERT. By installing and/or using this software product, you accept the terms and conditions of the current standard Betrusted license agreement. If you do not have a current copy of this agreement and would like to see it, please contact the Betrusted contracts department. If you have a signed license agreement with Betrusted for this software product, the terms and conditions of that signed license agreement take precedence over the standard terms and conditions.

Third-party licenses and credits

UniCERT uses the following third-party libraries:

- XMLSec, copyright © 2002 Aleksey Sanin.
- LibXML, copyright © 1998-2002 Daniel Veillard.
- LibEAY, copyright © 1995-1998 Eric Young (eay@cryptsoft.com)
- XML4c, copyright © 1999-2000 The Apache Software Foundation.

For more information on the licensing for these libraries, see the `<install directory>\docs\thirdpartylicense.txt` file supplied with UniCERT v5.2.1.

Contents

License and credits	iii
Chapter 1: About the distributed UniCERT CDs	1
What does UniCERT Core contain?	1
Which documents are provided?	2
Who is it for?	3
What does it assume you already know?	4
How the UniCERT product is distributed	4
Using the Web components CD	5
Using the WebRAO Client CD	5
Using the Key Archiver CD	5
Using the ARM CD	5
Using the UPI CD	5
Conventions used in the documentation	6
Related references	7
About Betrusted	7
Contacting Global Support Services	7
Chapter 2: Installation prerequisites	9
Compatibility with previous versions	9
Environments supported	10
Minimum hardware requirements	11
Software and optional hardware requirements	12
Supported Oracle version	12
Supported PKCS#11 devices	13
Supported directory servers	16
Supported OCSP responders	17
Supported VPN products	17
Supported Timestamp servers	17
Supported J2SE	17
Supported Web servers	17
Using Tomcat	17
Supported browsers	19
Supported email servers	19
Supported email clients	19
Conformance to standards	19
Unicode	19
Certificates	19
CRLs	19
Chapter 3: Getting ready for your PKI deployment	21
Deciding how to install the UniCERT components	21
Setting up a demo PKI	22
Setting up an enterprise PKI to secure a VPN	23
Setting up a hosted PKI	25
Outsourcing the CA	26
Example 1	26
Outsourcing the RA	27
Example 2	28

Chapter 4: Installing UniCERT Core	31
Preparing the information you require	31
Sample information	32
Installing third-party products	32
Considerations for test or demo core installations	33
Considerations when installing UniCERT components on different computers	34
Installing components for a hierarchical PKI	34
Installing components and their clones	35
Installing UniCERT Core	35
Installing optional UniCERT components	38
Installing the Key Archiver	38
Installing ARM	38
Installing UPI	38
Upgrading from v5.1	39
Uninstalling UniCERT Core	40
Uninstalling permanently	40
Uninstalling before upgrading	41
Upgrading the Publisher	42
Upgrading from Oracle 8.1.7	42
Modifying the Publisher 5.2.1 configuration	42
 Chapter 5: Installing the UniCERT Web components	 45
Overview of the installation process	45
Setting up the UniCERT components you require	46
Preparing the information you require	46
Installing the Web components	47
Adding, configuring, and deleting instances	48
Adding or configuring a Web Handler instance	49
Adding or configuring a WebRAO instance	50
Deleting an instance	50
Testing your WebRAO servlet installation	51
Using servlet managers with the WebRAO	51
Intranet deployment	52
Deployment options	52
Troubleshooting	53
Uninstalling the UniCERT Web Components	54
Uninstalling permanently	54
Uninstalling before upgrading or reinstalling	54
 Appendix A: Using UniCERT in its evaluated configuration	 55
Putting UniCERT in its evaluated configuration	55
Designing your PKI	56
How many UniCERT components?	56
How is your PKI distributed?	57
Planned hierarchy	57
Separate database accounts	57
Access to tokens	57
Splitting PSE files	57
Testing your PKI installation	57
Assumptions about administrators	58
Keeping UniCERT secure	58
Configuring components to work with UniCERT	59
Best practice guidelines	60
Backing up your PKI	60

Passwords and PINs 60
 Authorization groups 61
 Defining separate roles 61
 Auditing your system 62
 Defining an audit policy 62
 Deleting unauthorized users from the PKI 62
 Logical and physical protection of your PKI 63
 CA, RA, and KAS 63
 Other PKI entities 64
 Security enforcing UniCERT components 65
 Example of an evaluated configuration of UniCERT 65

Index 69

About the distributed UniCERT CDs

This guide provides the installation guidelines for the entire UniCERT v5.2.1 product. Although some components are available on different CDs, this guide accompanies the 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 components.

It also describes typical deployment examples 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 v5.2.1 components. It also details the documentation set provided with the UniCERT Core v5.2.1 CD, which you need to manage the entire UniCERT v5.2.1 product.

What does UniCERT Core contain?

The UniCERT Core v5.2.1 CD set provides the following UniCERT core components:

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

It also includes the UniCERT utilities: Database Wizard, Service Manager, Key Generator, and Token Manager. For definitions of the component acronyms, see the *UniCERT v5.2.1 Product Overview*.

For your convenience, the WebRAO servlets and the Web Handler, and the WebRAO Client are provided on separate CDs.



You must install and run the CAO on a computer with a Windows operating system. As of v5.2, you download the WebRAO Client from the WebRAO servlet using a browser.

Which documents are provided?

The UniCERT Core v5.2.1 CD provides the following documents:

- This guide, *UniCERT Core v5.2.1 Installation Guide*
- The *UniCERT v5.2.1 Release Notes*
- The *UniCERT v5.2.1 Product Overview*
- The *UniCERT v5.2.1 Administrator's Guide*
- The *UniCERT v5.2.1 Configuration Guide*
- The *UniCERT v5.2.1 Extensions Guide*
- The *UniCERT Publisher v5.2.1 Administrator's Guide*
- The *UniCERT v5.2.1 Database Administrator's Guide*
- The *UniCERT WebRAO v5.2.1 Client User's Guide*
- `readme.html`

Refer to the *UniCERT v5.2.1 Database Administrator's Guide* for information on installing and configuring Oracle. After then reading this guide and installing the UniCERT 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. See the *UniCERT v5.2.1 Release Notes* for information on resolved issues and new features.
2. See the *UniCERT v5.2.1 Product Overview* for a comprehensive introduction to the UniCERT product.
3. See the *UniCERT v5.2.1 Administrator's Guide* for information on setting up user database accounts for the PKI entities and using UniCERT utilities.
4. Read the *UniCERT v5.2.1 Configuration Guide* for instructions on configuring the PKI entities, creating registration policies (RPs), initializing entities, and managing your PKI.
5. See the *UniCERT Publisher v5.2.1 Administrator's Guide* for instructions on configuring and using the Publisher.
6. Read the *UniCERT WebRAO v5.2.1 Client User's Guide* for instructions on installing and using the WebRAO Client and KRO.

If you are fine-tuning your RPs and need additional information about the X.509 certificates and their extensions, see the *UniCERT v5.2.1 Extensions Guide*. For a schematic representation of the topics covered in the UniCERT documentation set, see Figure 1.



Figure 1: Where to find information

Who is it for?

This CD set is intended for administrators and general 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).

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, 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 cipher algorithms and certificate standards.

How the UniCERT product is distributed

In addition to the UniCERT Core v5.2.1 CD set, there are six other CDs containing UniCERT v5.2.1 components (see Table 1). For a detailed description of each UniCERT component, see the *UniCERT v5.2.1 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: UniCERT’s distributed components

CD name	Components	Documentation
Web Components	WebRAO servlets and JSPs Web Handler and JSPs	<i>UniCERT WebRAO v5.2.1 Client User’s Guide</i> webreadme.html webindex.htm
WebRAO Client	WebRAO Client	<i>UniCERT WebRAO v5.2.1 Client User’s Guide</i> webraoreadme.html webraoindex.htm
Key Archiver	KAS KAO	<i>UniCERT Key Archiver v5.2.1 Administrator’s Guide</i> kasreadme.html kasindex.htm
ARM	ARM	<i>UniCERT ARM v5.2.1 Installation Guide</i> <i>UniCERT ARM v5.2.1 Release Notes</i> <i>UniCERT ARM v5.2.1 Developer’s Guide</i> <i>UniCERT ARM v5.2.1 Reference Guide</i> armreadme.html armindex.htm

Table 1: UniCERT's distributed components (Continued)

CD name	Components	Documentation
UPI	UniCERT Programmatic Interface (UPI)	<i>UPI v5.2.1 Installation Guide</i> <i>UPI v5.2.1 Developer's Guide</i> upireadme.html upiindex.htm
CMP SDK	UniCERT CMP SDK	<i>UniCERT CMP v5.2.2 Installation Guide</i> <i>UniCERT CMP v5.2.2 Tutorial</i> readme.html index.htm

Using the Web components CD

The UniCERT Web Components v5.2.1 CD gives 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 CD on your Web server. The CD also contains utilities to assist you in adding and configuring the Web component instances.

Using the WebRAO Client CD

The UniCERT WebRAO Client v5.2.1 CD provides the primary interface for creating or processing certificate requests: the WebRAO Client. Install this CD 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.

Using the Key Archiver CD

The UniCERT Key Archiver v5.2.1 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 components on the UniCERT Key Archiver CD if you want to add the key archival functionality to your UniCERT PKI.

Using the ARM CD

The UniCERT ARM v5.2.1 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 components from the UniCERT ARM CD.

Using the UPI CD




The UPI is a Java developer's toolkit that enables you to create an advanced, Web-based UniCERT application. You can use it to customize the certificate request and authorization processing

functionality required for your applications and devices to interact with UniCERT.

Conventions used in the documentation

Table 2 lists the various conventions used in Betrusted documentation. We follow these conventions to help you quickly and easily identify particular elements, processes, and names that occur frequently in documents.

Table 2: 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 <code>readme.html</code> on the CD. <code>f:\startup\demo</code>
Text the user needs to enter or programming code	<code>printf("Hello\n");</code>
References to chapter and section names	See Chapter 1, <i>About this guide</i> . See <i>What is it about?</i> 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 <i>UniCERT v5.2.1 Administrator's Guide</i> .
Application names	UniCERT KeyTools Pro
Notes and tips	
Cautions	
Warning (indicates possibility of physical harm)	

Related references

ITU-T Recommendation X.509 | ISO/IEC 9594-8: *Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Framework*, Fourth Edition Draft v8, 3 May 2001.

R. Housley, W. Ford, W. Polk, and D. Solo, *Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*, RFC 3280, April 2002, <http://www.rfc-editor.org/rfcsearch.html>.

The Public Key Cryptography Standards (PKCS) are available from [RSA Laboratories](#).

Schneier, Bruce, *Applied Cryptography*, 2nd edition, Wiley, New York, 1997.

About Betrusted

Betrusted is the premier global provider of security and trust services to the world's leading organizations and government agencies. Through its managed security services, Betrusted offers clients a comprehensive package of leading security products coupled with unrivalled expertise to help reduce costs, increase revenues, and comply with government and industry regulations. For more information, visit <http://www.betrusted.com>.

Contacting Global Support Services

If you are having issues with the UniCERT release, contact Global Support Services (globalsupport@betrusted.com). Before doing so, however, make sure you have the information listed in Table 3.

Table 3: Product information

UniCERT support information	
Version:	
Patch versions (if applicable):	
Operating system (include version and service packs):	
System path:	
Compiler version:	
Hardware platform:	

Table 3: Product information (Continued)

UniCERT support information		
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



You can copy this text and email or print it from the pdf and fax it to Global Support Services.

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 v5.2.1 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.

Compatibility with previous versions

UniCERT v5.0 was restructured architecturally and was essentially a new product. Therefore, if you have an earlier version of UniCERT, contact Global Support Services for the *Migrating from UniCERT v3.x to v5.2.1 Administrator's Guide*.

If you have UniCERT v5.1 or v5.2, you can upgrade to UniCERT v5.2.1; however, upgrading also requires:

1. (UniCERT v5.1 only) Backing up the old registry settings; see *Upgrading from v5.1* on page 39
2. Uninstalling the old version (see *Uninstalling before upgrading* on page 41)
3. Running the UniCERT Database Upgrade Utility after installing UniCERT v5.2.1



The UniCERT Programmatic Interface (UPI) v5.2 is fully compatible with UniCERT v5.2.1; you do not need to upgrade it.

As there were also significant changes in the v5.x versions, compatibility with earlier v5.x components is not supported. The UniCERT Publisher is the only exception to the version incompatibility rule: If you are running the Publisher separately from the rest of UniCERT, you can also upgrade to v5.2.1 from

Publisher v5.0.1 patch 3. See *Upgrading the Publisher* on page 42 for more information.

Environments supported

UniCERT v5.2.1 supports the operating systems listed in Table 4.

Table 4: Supported operating systems

User	Supported systems
Client	<ul style="list-style-type: none"> • Microsoft Windows 2000 Professional Service Pack 4 • Microsoft Windows XP Professional Service Pack 2
Server	<ul style="list-style-type: none"> • Microsoft Windows 2000 Server Service Pack 4 • Microsoft Windows 2003 Enterprise Edition



Although we have only fully tested with the Windows 2000 Server and 2003 Enterprise Edition, you can also use the Windows 2000 Advanced Server or Data Center Server, or the Windows 2003 Standard Edition or Data Center Edition, respectively; these products are simply differently licensed versions of the Windows servers.

For a complete listing of the UniCERT v5.2.1 components, see Table 5. All of the components listed in this table except the advanced components are provided in the UniCERT Core v5.2.1 CD installation set.

Table 5: UniCERT v5.2.1 components

Components
Core components
Certification Authority (CA)
Certification Authority Operator (CAO)
Publisher
Certificate Status Server (CSS)
Registration Authority (RA)
RA eXchange
Web Handler
CMP Handler
email Handler

Table 5: UniCERT v5.2.1 components (Continued)

Components
SCEP Handler
WebRAO
Advanced components
Advanced Registration Module (ARM)
Key Archiver, which consists of three components: <ul style="list-style-type: none"> • Key Archive Server (KAS) • Key Archive Operator (KAO) • Key Recovery Operator (KRO)
UniCERT Programmatic Interface (UPI)
UniCERT CMP SDK
Utilities
Database Wizard
Key Generator
RA Auditor
Token Manager
Service Manager



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

Minimum hardware requirements

Depending on which UniCERT v5.2.1 components you are installing on a computer, the minimum hardware requirements can differ.

Table 6 lists the minimum system requirements for Windows operating systems.

Table 6: Minimum system requirements

Component	Requirement
RAM	512 MB if installing Oracle to the computer; without Oracle, 256 MB
Hard drive space	4 GB for the Oracle installation and database, 400 MB of swap space, and 52 MB for data and index files on the Oracle server computer
Processor	Pentium IV, single or multiprocessor computer
Clock speed	1.8 GHz
Other drives	CD-ROM drive for installation

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.

Software and optional hardware requirements

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

- All core components except the protocol handlers and the WebRAO require Oracle.
- The Key Archiver and ARM, which are advanced components, also require Oracle.

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 clients.

Supported Oracle version

Table 7 describes the supported Oracle versions and any additional requirements:

- For details on the Oracle security patch, see *Installing the Oracle security patch* on page 13.

- If you have a previous version of Oracle, see *Previous Oracle versions*.
- For information on installing and configuring Oracle, see the *UniCERT v5.2.1 Database Administrator's Guide*.

Table 7: Supported Oracle versions

User	Supported version	Requirements
Server	Oracle v9.2.0.5 (9i) and security patch	<ul style="list-style-type: none"> • If you have an earlier version of Oracle 9i, upgrade to the 9.2.0.5 patch. • Apply the security patch available from Oracle Metalink (see <i>Installing the Oracle security patch</i>).
	Oracle v8.1.7.4 and security patch	<ul style="list-style-type: none"> • You require the Oracle 9i client for distributed UniCERT components. • You have to add replication capabilities to your Oracle 8.1.7.4 database (see the <i>UniCERT v5.2.1 Database Administrator's Guide</i>). • If you have the Oracle v8.1.7 server, ensure that you upgrade to version 8.1.7.4; there are memory leaks with 8.1.7. • Apply the security patch available from Oracle Metalink (see <i>Installing the Oracle security patch</i>).
Client	Oracle v9.2.0.1 (9i)	If you have an earlier version of Oracle 9i, upgrade to the 9.2.0.1 patch.

Installing the Oracle security patch

The security patch is available from Oracle Metalink: http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1.

For more information on the security patch, see Oracle's FAQ on Security Alert 68 (<http://metalink.oracle.com/metalink/plsql/showdoc?db=Not&id=282108.1>).

Previous Oracle versions

UniCERT v5.2.1 does not work with Oracle 8.0.5 or 8.1.6 databases. If you have pre-v5.0 UniCERT and an earlier version of Oracle, request the UniCERT v3.x to 5.2.1 Migration CD from Global Support Services.

Supported PKCS#11 devices

There are a variety of hardware security modules (HSMs) and smart card products that UniCERT supports. Typically, HSMs are only used

for securing the most sensitive entities in your PKI, the CAs, and to a lesser extent the RAs. You can use smart cards to secure other PKI entities' keys, such as the CAO or the WebRAO Client. End users 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.

Choosing the device driver

It is important that you use the correct device driver for your PKCS#11 devices. Table 8 lists the supported HSMs' specifications, and Table 9 provides the same information for the supported smart cards. Alternate drivers that the vendors provide may not function correctly with UniCERT.

Table 8: Supported HSM versions and DLLs

Vendor	Product	Software version	DLLs
AEP Systems	SureWare Keyper	v2.4 (adapter v3.9)	bp201w32hsm.dll
AEP Systems	Sureware Keyper Enterprise	v1.2 (adapter v3.9)	bp201w32hsm.dll
SafeNet	Luna 2, Luna CA3 (LunaDoc reader)	v8.2 (v3.9 firmware)	cryst201.dll
SafeNet	Luna SA Client	v2.2.1	cryptoki.dll
nCipher	nForce, nShield	v8.32	cknfast.dll


 Chrysalis-ITS, which produced the Luna HSMs, was acquired by SafeNet.

Table 9: Supported smart card versions and DLLs

Vendor	Product	Readers	Smart cards	Software version	DLLs
SafeNet	SignaSure	SR10 DKR610 serial DKR630 USB DKR710 serial DKR730 USB	DK330	CIP v4.7	dkck201.dll
SafeNet	iKey	USB port	iKey 2032	CIP v4.7	dkck201.dll
Gemplus	GemSAFE	GemPC400 GemPC410 GemPC430 (Windows 2000 only) The Datakey DKR610 and DKR710 readers listed above	GPK16K (v2)	v4.1	gc1lib.dll
Oberthur Card Systems	Authentic Web Pack	Omnikey 1010 Omnikey 2020 (same as DKR610 and DKR730) OCR 136 serial OCR 150 USB	CosmopolIC	AWP 3.0.1	OCScryptolib_p11.dll



Both Datakey, which produced SignaSure, and Rainbow, which produced iKey, were acquired by SafeNet.

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 v5.2.1 enables you to generate up to 4096-bit RSA keys or 1024-bit DSA keys. However:

- SureWare Keyper v2.4 supports up to 2048-bit RSA keys.
- nCipher supports up to 4096-bit RSA keys, as do the Luna CA3 and Luna SA products.
- Smart cards – with the exception of DK330 and CosmopolIC – do not support DSA keys, only RSA.
- Gemplus and iKey smart cards are restricted to a maximum key size of 1024 bits.
- Depending on the card’s mapping, a GemSAFE GPK16K card can hold four 1024-bit and two 512-bit RSA keys, but not five 1024-bit keys.
- If you use the DK330 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.

FIPS-140 accreditation of supported devices

The PKCS#11 devices that UniCERT v5.2.1 supports have the following accreditation:

- Luna CA3 has FIPS 140-1 level 3.
- SureWare Keyper has FIPS-140 level 4.
- nShield has FIPS-140 level 3, and nForce has FIPS-140 level 2.
- The Oberthur CosmopolIC smart cards have FIPS-140 level 2.

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

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. UniCERT v5.2.1 has been fully tested with the following LDAP v3 compliant directory servers:

- Sun Java System Directory Server v5.2 (previously called iPlanet)
- Microsoft’s Active Directory (Window 2000 and Windows 2003)

- Critical Path's CP Directory Server v4.1
- Siemen's DirX v6.0

Supported OCSF responders

When you use the UniCERT Publisher, you can publish to Tumbleweed Validation Authority (VA) v4.6; previously, this product was called Valicert Enterprise Validation Authority. No other OCSF responders have been tested with UniCERT v5.2.1.

Supported VPN products

The UniCERT SCEP Handler v5.2.1 supports the latest Cisco IOS version for routers, which is v12.2.23. It has also been tested with the following:

- Cisco VPN client v4.0.5
- Cisco VPN 3000 Concentrator v4.1.5
- Cisco IOS Router v12.3.10
- Checkpoint FireWall-1/VPN-1 R55
- Nortel Connectivity Switch v4.75

Supported Timestamp servers

The UniCERT Publisher has been tested with the UniCERT Timestamp Server v2.0.2 patch 2 and 2.0.3.

Supported J2SE

The Java 2 Platform, Standard Edition (J2SE) included in the UniCERT installer is 1.4.2_03 (which is also referred to as Java Runtime Environment, JRE).

Supported Web servers

To provide the necessary HTTP support for the UniCERT Web Handler and WebRAO components, use one of the tested Web server and servlet manager pairs:

- Microsoft IIS (Internet Information Server) v5.0, with ServletExec v4.2 patch 19.
- Sun Java System Web Server v6.0 Service Pack 2 (previously called Sun ONE Web Server and prior to that, iPlanet). No servlet manager is required.
- Apache v1.3 or v2.0, with Tomcat v4.1.27.

For more information on using servlet managers, see *Using servlet managers with the WebRAO* on page 51.

Using Tomcat

UniCERT is deployed with a default Tomcat servlet container. Typically, you need to integrate this servlet container with your Web server by bridging the Web server (IIS or Apache) with Tomcat.

Integrating Tomcat with other Web servers

To integrate Tomcat with Apache Web servers, use the plug-in provided by Tomcat and Apache (`mod_jk`). For more information, see <http://jakarta.apache.org/tomcat/tomcat-4.1-doc/jk2/jk/aphowto.html>.

If you have IIS, be aware that it does not execute servlets and Java Server Pages (JSPs) by default. Therefore, you need to configure IIS to use the Tomcat redirector plug-in, `isapi_redirect.dll`, which allows IIS to send servlet and JSP requests to Tomcat. For information, see <http://jakarta.apache.org/tomcat/tomcat-4.1-doc/jk2/jk/iishowto.html>.

Configuring SSL support

If you are using Tomcat as a standalone Web server, you need to configure Tomcat to work securely with SSL. This secures the data exchange between the WebRAO client and servlet and requires:

- A server certificate and corresponding private RSA key for Tomcat
- A key store

UniCERT only supports SSL server-side authentication. For instructions on setting up standalone Tomcat to work securely with SSL, see <http://jakarta.apache.org/tomcat/tomcat-4.1-doc/ssl-howto.html>.



For background information on the SSL protocol, see <http://www.freesoft.org/CIE/Topics/121.htm>.

When running Tomcat primarily as a Servlet/JSP container behind another Web server, such as Apache or Microsoft IIS, configure the primary Web server to handle the SSL connections from users. For Apache, see <http://jakarta.apache.org/tomcat/tomcat-3.3-doc/tomcat-ssl-howto.html#s5>; for IIS, see <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q142849>.



Due to a limitation in Java, do not issue keys larger than 2048 bits for SSL server or client certificates; otherwise, the keys in the SSL certificate's chain will not load when you are using the WebRAO over SSL.

Typically, this server negotiates all SSL-related functionality and then passes on any requests destined for the Tomcat container only after decrypting those requests.

Supported browsers Certificate applicants using the Web Handler can run one of the following browsers to communicate with UniCERT:

- Internet Explorer v5.5 Service Pack 2 or v6.0
- Netscape Communicator v4.7 or v7.x

WebRAO Client users can use one of the supported Internet Explorer versions or Netscape Communicator v7.2.

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 the tested email server, Microsoft Exchange Server v5.5 or 2000. SMTP servers are also supported.

Supported email clients

UniCERT has been tested with the email clients outlined in Table 10.

Table 10: Supported email clients

Windows 2000	Windows 2003	Windows XP	Solaris 8
Outlook XP	Outlook 2003	Outlook XP	Netscape Messenger v4.77

Conformance to standards

UniCERT v5.2.1 supports the following standards and formats.

Unicode

UniCERT v5.2.1 supports extended ASCII and Unicode character sets used in:

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

Certificates

UniCERT v5.2.1 issues and works with DER encoded X.509 v3 and v1 certificates.

CRLs

UniCERT v5.2.1 supports DER encoded X.509 v2 certificate revocation lists (CRLs).

Getting ready for your PKI deployment

How you install the UniCERT 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 for secure communications.



If you are not familiar with PKI concepts and terminology, see the *UniCERT v5.2.1 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 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 Betrusted's professional services.



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

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

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

In UniCERT v5.2.1, 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 18, *Cloning*, in the *UniCERT v5.2.1 Configuration Guide*.

Setting up a demo PKI

For demonstration or testing purposes, install all of the UniCERT components except the WebRAO applet on one Windows computer (see Figure 2). You can also install the Oracle 9i server on the same computer, although its performance may be affected when you run Oracle and multiple UniCERT components together.

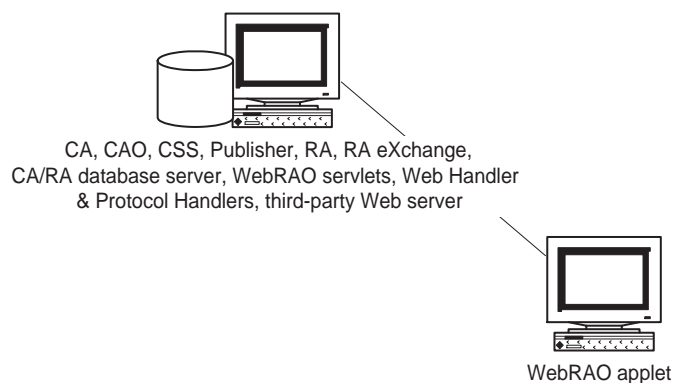


Figure 2: Installing a test PKI

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

- Installing the Oracle 9i server and the UniCERT core v5.2.1 components (see *Installing UniCERT Core* on page 35)
- 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, we recommend that you install the WebRAO servlets and Web Handler there. However, you can also install them with the other UniCERT components.

-
- Defining your demo PKI entities (see the *UniCERT v5.2.1 Configuration Guide*)
 - Creating a demo registration policy (RP) and authorization group for remote certificate applicants (see the *UniCERT v5.2.1 Configuration Guide*)



You can 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 applet and submitting a request via a Web browser

The test scenario shown in Figure 2 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: CMP Handler, Web Handler, email 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 and retrieve the certificate successfully, the demo PKI is functioning correctly.

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 expired certificates



To create a PKI-enabled VPN, perform the same installation and configuration tasks that the demo PKI required (see *Deciding how to install the UniCERT components* on page 21).

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 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. Alternatively, you can use additional RAs and RA eXchanges, implementing one pair for each division.

Although Figure 3 shows only one WebRAO Client (applet) per WebRAO server, you can have multiple WebRAO Clients per server, and you can have multiple WebRAO servers per RA.

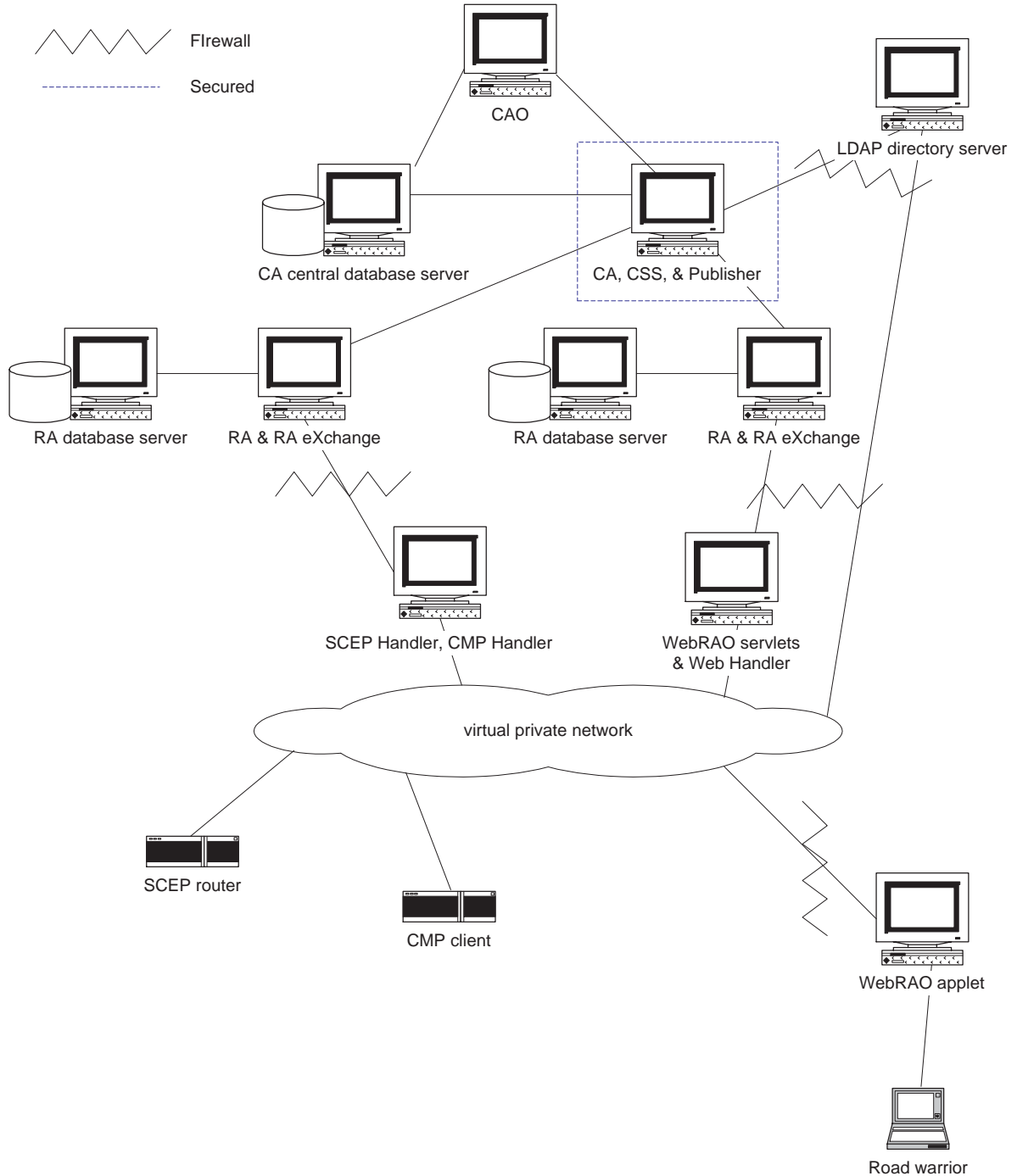


Figure 3: Setting up a PKI for your corporate VPN

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 *Setting up a demo PKI* on page 22), a hosted PKI typically performs the tasks listed in *Setting up an enterprise PKI to secure a VPN* on page 23.

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. Your LDAP server does not normally get outsourced.

Example 1

The example in Figure 4 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 Publisher, you can install multiple instances as needed. For more information on clones, see *Installing components and their clones* on page 35.

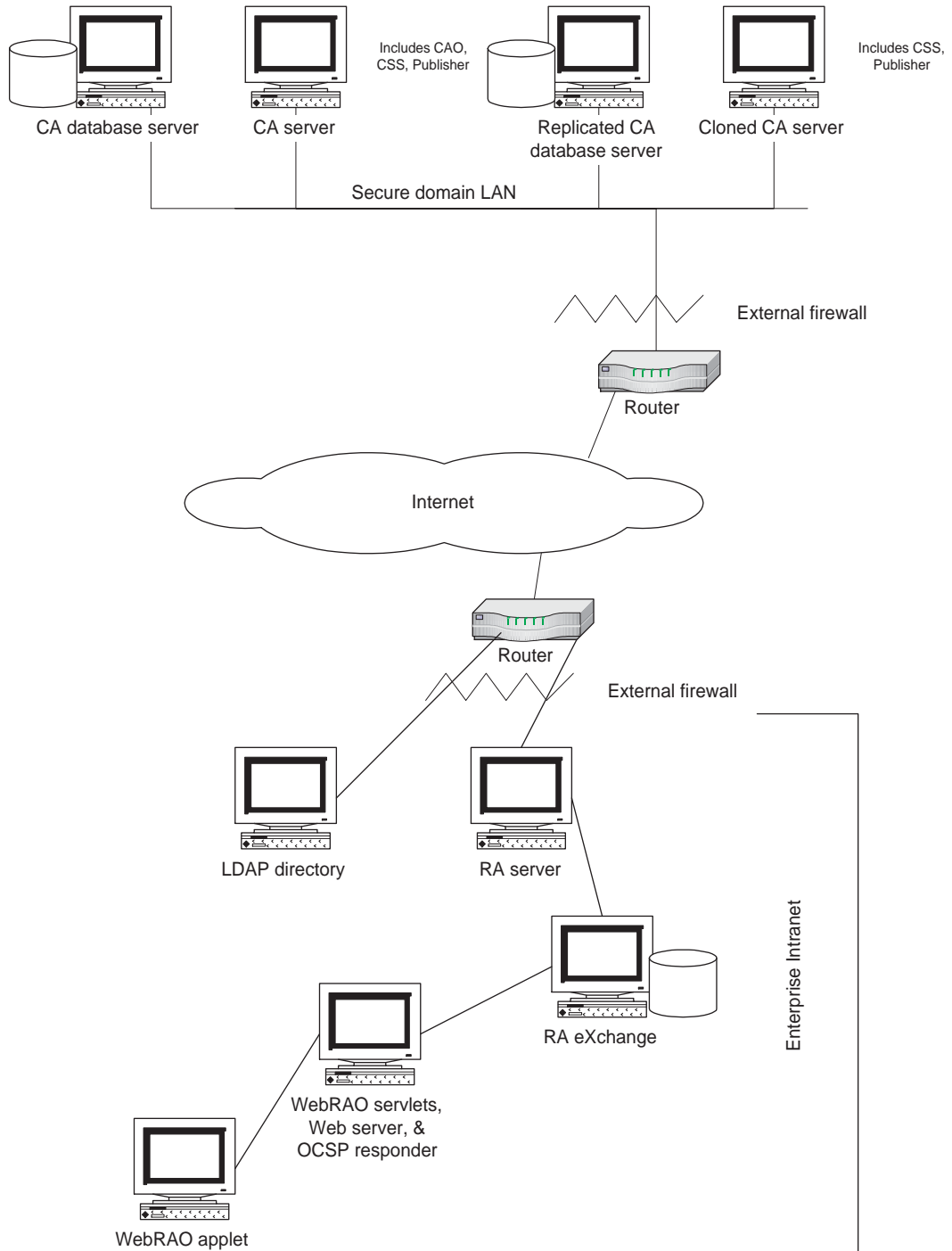


Figure 4: Outsourcing the CA and related components

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, 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.

Example 2

The example in Figure 5 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.



If you want to use Oracle replication or cluster support, you must purchase the full ASFU license from Oracle.

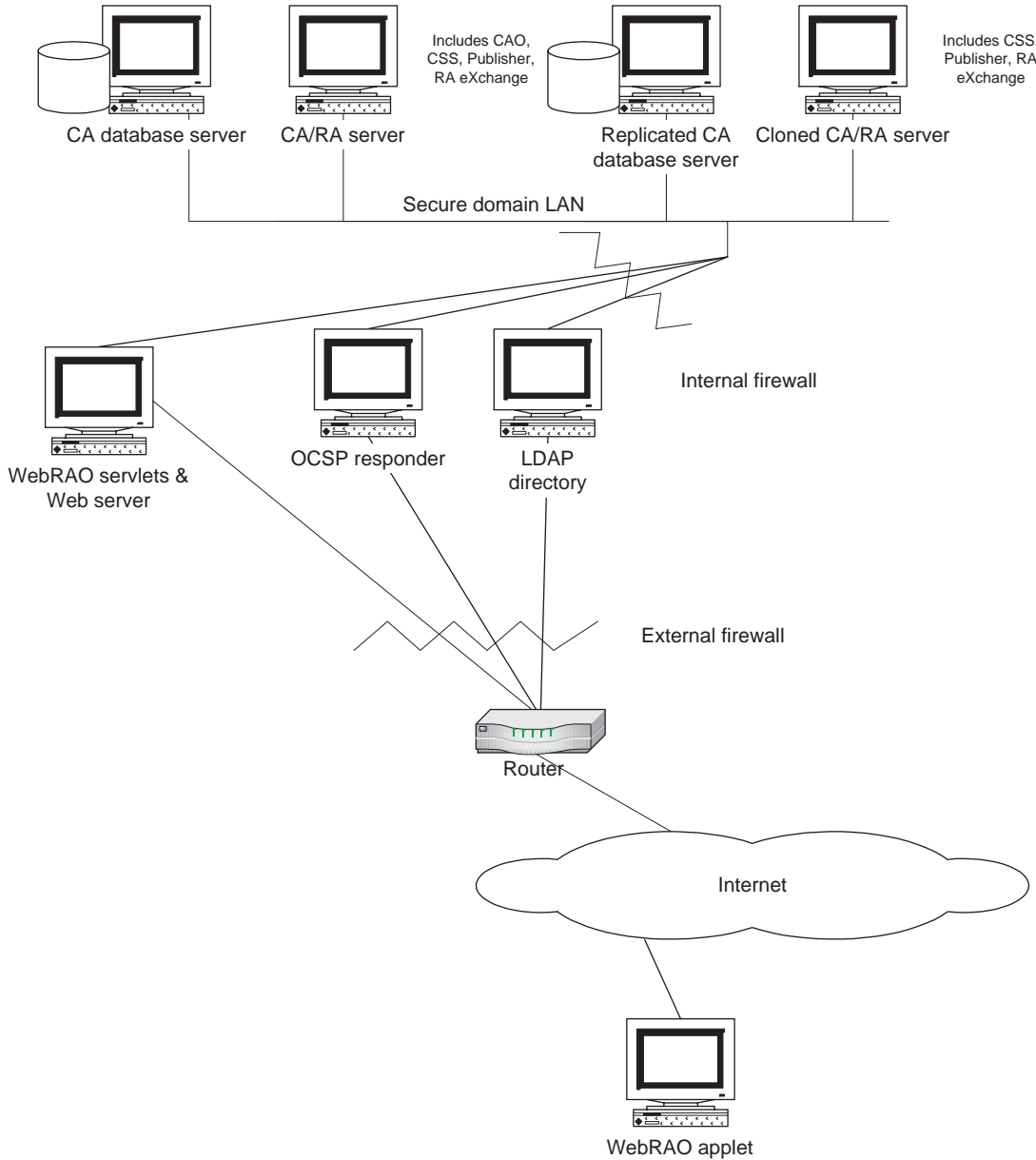


Figure 5: Outsourcing the CA and RA

Once you have verified that you meet the necessary hardware and software requirements (Chapter 2, *Installation prerequisites*) and determined how you are deploying UniCERT PKI (Chapter 3, *Getting ready for your PKI deployment*), you can install the UniCERT core v5.2.1 components.

The UniCERT Core v5.2.1 CD set provides the majority of the UniCERT core components and utilities. For ease of distributed installation, the UniCERT Web Components v5.2.1 CD provides the WebRAO servlets and the Web Handler. Depending on your PKI requirements, you may also need one or more of the other UniCERT CDs. See *How the UniCERT product is distributed* on page 4 for more information on the CDs available.



Ensure there is enough space on your system before installing UniCERT v5.2.1, especially if you are installing the Oracle database on the same computer. Otherwise, you may have problems with your installation (see *Minimum hardware requirements* on page 11).

If you have a previous UniCERT 5.x version installed, see *Compatibility with previous versions* on page 9.

Preparing the information you require

Before installing UniCERT Core v5.2.1, prepare the following information. For your Oracle database accounts you require:

- A system identifier (SID) for your database instance
- A database name for your database instance
- Account usernames and passwords for your UniCERT components

For your UniCERT components you require:

- Distinguished name (DN) elements.
- DN aliases.

- Personal secure environment (PSE) or PKCS#12 filenames and passwords.
- 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

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

- SID: AcmeCA
- Database name: AcmeDB
- 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.acme.com`
- IP address: 255.255.255.255

Installing third-party products

We recommend that you install third-party products destined for use with UniCERT before you install UniCERT Core v5.2.1. 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.

Oracle also adheres to this installation order. You install Oracle before installing UniCERT as UniCERT requires a customized database installation; you cannot run UniCERT without it. See the *UniCERT v5.2.1 Database Administrator's Guide* for instructions on

installing and configuring Oracle. See *Supported Oracle version* on page 12 for details of the supported Oracle versions.



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

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, following the instructions in the *UniCERT v5.2.1 Database Administrator's Guide*.
4. Install the Oracle 9.2.0.5 client for all PKI computers. 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. Make the registry setting changes to upgrade each computer's Oracle installation to support UTF8.
6. Set up mail accounts and/or a Web server for the RA eXchange, email Handler, and WebRAO, as needed for your PKI.

Considerations for test or demo core installations

In these instructions, we assume that you are installing the UniCERT core components to one Windows computer. For test systems and any PKIs destined to have only one CA, you need:

- One installation of the core CD set.
- The WebRAO servlets from the UniCERT Web Components v5.2.1 CD. See Chapter 5, *Installing the UniCERT Web components*.

Whether you install the optional UniCERT components on this same computer depends on your requirements. If you are setting up a distributed PKI, see *Considerations when installing UniCERT components on different computers*.

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

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 core documentation, utilities, and core components, including one or more protocol handlers as needed, from the UniCERT Core v5.2.1 CD
- The WebRAO servlets and Web Handler from the UniCERT Web Components v5.2.1 CD, as required
- The WebRAO Client, downloaded via your browser from the UniCERT WebRAO servlet



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 v5.2.1 Administrator's Guide*. For information on configuring them, see Chapter 1, *Introduction*, in the *UniCERT v5.2.1 Configuration Guide*.

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 either on the same computer as each CA instance or 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.

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 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. This is also true for the CMP Handler, email Handler, and SCEP Handler. However, unlike the WebRAO and Web Handler, they can communicate with another RA eXchange, provided it is connected to a different RA.

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.
- 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 the same computer, they use the same crypto profile.
- 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. You follow a similar procedure to cloning from software; however, the process for copying the PSE to the clone's computer depends on the HSM you are using.

For example, if you are using a SafeNet LunaCA3 token, you can clone the token using the LunaCA3 device and transfer it to the other computer, which requires its own HSM. For other HSMs, refer to the documentation that came with your HSM.

- 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.

Installing UniCERT Core

To install the UniCERT Core v5.2.1 components, follow these steps:

1. If you have a previous version of UniCERT installed:
 - UniCERT v5.1: See *Upgrading from v5.1* on page 39.
 - UniCERT v5.2: See *Uninstalling before upgrading* on page 41.
2. Put the UniCERT Core v5.2.1 for Windows CD in your computer's CD drive. The installation wizard automatically starts. The screen shown in Figure 6 is the first screen you see.



Figure 6: Beginning the installation of UniCERT Core v5.2.1

3. Select the language you would like to work in and click **OK**.
4. Click **Next** on the **Introduction** screen. The **License Agreement** screen is displayed.
5. Accept the license agreement and click **Next**.
6. Accept the default installation directory, `C:\Program Files\Betruusted\UniCERT`, on the **Choose Install Folder** screen and click **Next**. Alternatively, specify another directory and click **Next**.



If you choose to install any UniCERT component to a directory other than the default, ensure the “)” character is not included in the directory path. Otherwise, the UniCERT component will not be able to connect to Oracle when you start it, as Oracle does not support all the characters that Windows supports in its filenames or paths.

7. Specify the Windows desktop or menu access to UniCERT on the **Choose Shortcut Folder** screen. By default, the installer creates a program group named **Betruusted UniCERT v5.2.1**. Click **Next**.

8. Leave **Full Install** as the **Install Set** value to choose all components, utilities, and documentation. Alternatively, choose **Custom** for **Install Set** and select the components you wish to install. These instructions assume you are installing all components from the CD. Click **Next**.
9. (Windows XP only) Leave the default values, **Yes**, selected to add the UniCERT and Oracle services to your network configuration and click **Next** (see Figure 7). If you are not using the Windows firewall, select **No** and click **Next**.

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

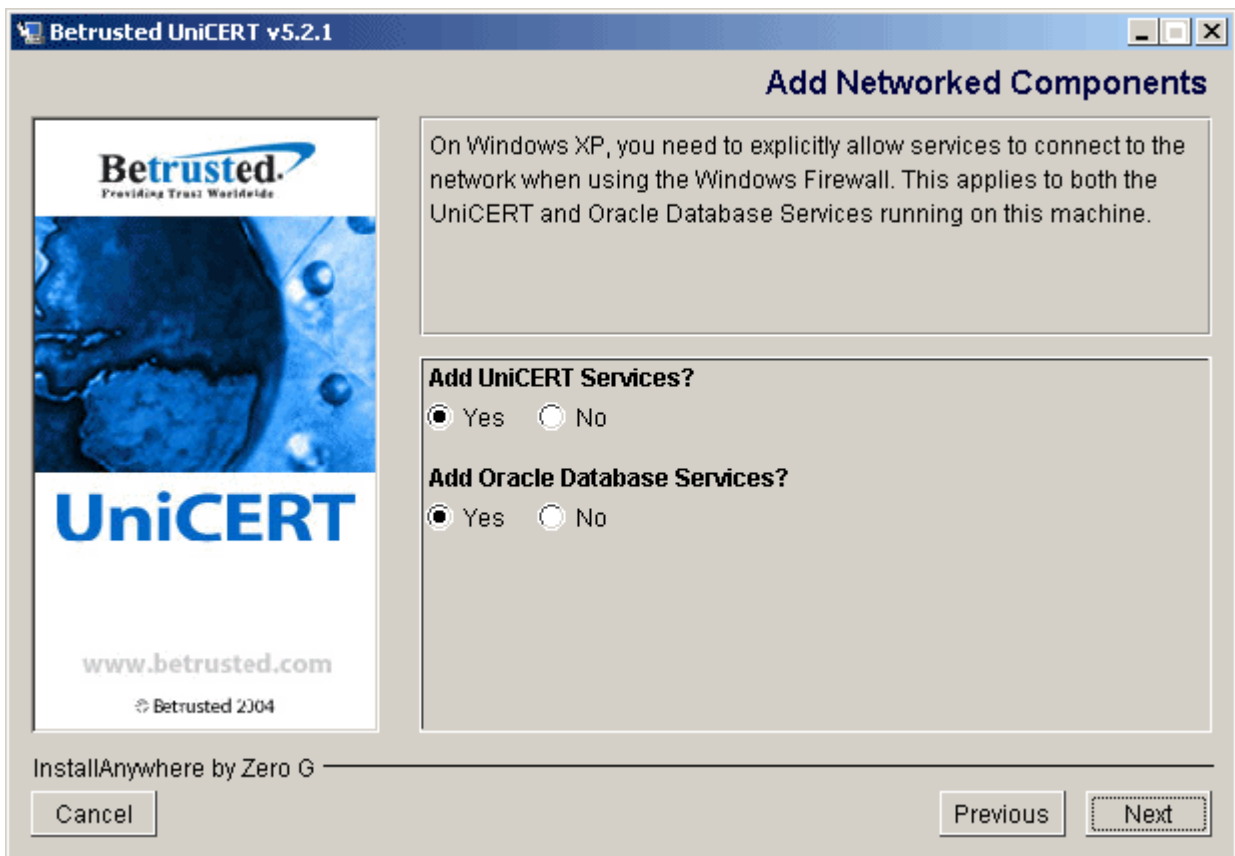


Figure 7: Enabling your services on XP

10. Review the preinstallation summary information that the installer lists. If the details are correct, click **Install**.
11. We recommend that you read the `readme.html` as prompted.

12. Click **Done**.
13. If the CAO is one of the components you are installing, reboot the computer to ensure that the CAO is correctly updated with the system information.

If you require the core UniCERT Web components, see Chapter 5, *Installing the UniCERT Web components*.

Installing optional UniCERT components

The UniCERT components available on other CDs are advanced, optional components. For a description of these components and their CDs, see *How the UniCERT product is distributed* on page 4.

Installing the Key Archiver

To install the UniCERT Key Archiver, follow these steps:

1. Load the UniCERT Key Archiver v5.2.1 CD. The installation wizard automatically starts.
2. Click **Next** on the **Introduction** screen.
3. Follow the installation wizard's instructions and install the Key Archiver to the same program group and installation directory as the other UniCERT components. You may want to install the KAS and the KAO components to different computers.
4. We recommend that you read the `kasreadme.html` as prompted by the installation wizard.
5. Eject the UniCERT Key Archiver v5.2.1 CD.

Installing ARM

To install the UniCERT ARM, follow these steps:


1. Load the UniCERT ARM v5.2.1 CD. The installation wizard automatically starts.
2. Click **Next** on the **Introduction** screen.
3. Follow the installation wizard's instructions and install the ARM to the same program group and installation directory as the other UniCERT components.
4. We recommend that you read the `armreadme.html` as prompted by the installation wizard.
5. Eject the UniCERT ARM v5.2.1 CD.

Installing UPI

To install the UniCERT Programmatic Interface(UPI), follow these steps:


1. Load the UniCERT UPI v5.2.1 CD. The installation wizard automatically starts.
2. Click **Next** on the **Introduction** screen.

3. Follow the installation wizard's instructions and install the UPI to the same program group and installation directory as the other UniCERT components.
4. We recommend that you read the `upireadme.html` as prompted by the installation wizard.
5. Eject the UniCERT UPI v5.2.1 CD.

 UniCERT v5.2.1 is also compatible with the UPI v5.2.

Upgrading from v5.1

Because UniCERT v5.2.1 has changed the registry settings it creates on installation, you need to modify your existing UniCERT registry settings to reuse your defined crypto profiles and service instances. You also need to modify the service instances' executable paths post-installation, as Windows tracks services independently from the registry. Alternatively, you can uninstall UniCERT v5.1, install v5.2.1, and re-create all your PKI entities.

 Modifying your registry manually is a risky procedure. Be sure to back up your registry before following the steps below so that you can restore it to working order should any errors occur.

If you have a distributed UniCERT v5.1 installation, follow these steps to back up and restore the registry entries before removing your v5.1 on each UniCERT computer:

1. Start the Registry Editor (`regedit.exe`) application.
2. Select the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Baltimore-Technologies\CryptoEngine\CryptoProfiles`

3. Right-click this registry key and click **Export**; then save the registry settings to a file, for example, `v51crypto.reg`.
4. Repeat steps 2-3 for this registry key, saving the exported registry keys to another `.reg` file:

`HKEY_LOCAL_MACHINE\SOFTWARE\Baltimore-Technologies\UniCERT`

5. Remove the installed UniCERT v5.1 components; see *Uninstalling before upgrading* on page 41.
6. Install the necessary UniCERT v5.2.1 components; see *Installing UniCERT Core* on page 35 and *Installing the Web components* on page 47.

7. For the registry files that you created in steps 2-4:
 - a. Open the file in a text editor and replace all instances of `SOFTWARE\Baltimore-Technologies` with `SOFTWARE\Betrusted`.
 - b. Save the file.
 - c. Locate the modified file in Windows Explorer and double-click it. The Registry Editor prompts you to confirm the registry update action. Click **Yes**.
8. Start the Registry Editor if it is not running already, locate the following registry keys, and delete them:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Betrusted\UniCERT\InstalledComponents\5.1
HKEY_LOCAL_MACHINE\SOFTWARE\Betrusted\UniCERT\version\5.1
```

9. Run the UniCERT Database Upgrade Utility; select **Start>Programs>Betrusted UniCERT v5.2.1>Database Upgrade Utility** and log onto your database.
10. Upgrade all your accounts, following the instructions from the Database Upgrade Utility wizard.
11. Run the configuration utility for the WebRAO and Web Handler on their respective computers to update the instances (see *Adding, configuring, and deleting instances* on page 48).
12. (Publisher only) Update the Publisher's configuration; see *Modifying the Publisher 5.2.1 configuration* on page 42.
13. Run the Service Manager and update your instances to reflect their new executable path.

Uninstalling UniCERT Core

You must uninstall UniCERT Core v5.2.1 before reinstalling it. Similarly, if you have v5.2 installed, remove it before upgrading to v5.2.1 (see *Uninstalling before upgrading* on page 41). If you have UniCERT Core v5.1 installed, you need to upgrade its registry settings before following the uninstall instructions here (see *Upgrading from v5.1* on page 39).

You use the Control Panel's **Add/Remove Programs** option when uninstalling the UniCERT Core v5.2.1 components. However, the process for uninstalling UniCERT Core differs slightly if you are completely removing UniCERT from your system or simply upgrading.

Uninstalling permanently

Follow these steps to completely remove UniCERT, including your crypto profiles, PSEs, and registration policies:

1. Stop the UniCERT services by selecting **Start>Programs>Betrusted UniCERT v5.2.1>Service Manager** and then stopping each service.

2. (UniCERT v5.2 only) Save a copy of your system path information to a text file, as uninstalling v5.2 erroneously removes it. To do this, access the path variable by using **Start>Settings>Control Panel>System**, clicking **Environment Variables** on the **Advanced** tab, and then copying the value set for **Path**.
3. Remove each service. To do this, select the service and then **Service Instance>Delete**.
4. Exit the Service Manager.
5. Select **Start>Programs>Betrusted UniCERT v5.2.1>Token Manager** and delete all of your crypto profiles. This deletes them from the registry.
6. Select **Start>Settings>Control Panel>Add/Remove Programs**.
7. Remove each component individually. The installed UniCERT components are listed in the **Add/Remove Programs** screen.
8. Manually delete the UniCERT installation directory, which may contain PSEs or registration policies that you created. It also contains Web component directories if you installed them; remove these as well.

Uninstalling before upgrading

Follow these steps to uninstall the entire UniCERT Core product:

1. Make sure the UniCERT services are not running, so the Windows registry is updated correctly. To stop the services, select **Start>Programs>Betrusted UniCERT v5.x>Service Manager** and then stop all services.
2. (UniCERT v5.2 only) Save a copy of your system path information to a text file, as uninstalling v5.2 erroneously removes it. To do this, access the path variable by using **Start>Settings>Control Panel>System**, clicking **Environment Variables** on the **Advanced** tab, and then copying the value set for **Path**.
3. Back up any PSEs and RPs as a precaution.
4. Select **Start>Settings>Control Panel>Add/Remove Programs**.
5. Remove each component individually. The installed UniCERT components are listed in the **Add/Remove Programs** screen.



Uninstalling the UniCERT Core v5.2.1 components does not affect any PSEs or registration policies you may have created. Therefore, if you have stored these in the UniCERT installation directories, the uninstaller does not remove these directories.

6. Remove Web component directories from the UniCERT installation directory if you installed them.
7. Install the core components you require (see *Installing UniCERT Core* on page 35 and *Installing the Web components* on page 47).

Upgrading the Publisher

If you have Publisher v5.0.1 patch 3 or later installed, upgrade to v5.2.1. You can continue to use your existing PKI database information, although you must back it up and uninstall the older Publisher software.



Previously, the UniCERT Publisher was available on a separate CD.

If you have APM v2.1, which interoperated with UniCERT v3.x, there is a multi-version upgrade to perform as part of the migration from UniCERT v3.x to UniCERT v5.2.1. See the *Migrating from UniCERT v3.x to v5.2.1 Administrator's Guide*.

Upgrading from Oracle 8.1.7

To upgrade to UniCERT Publisher v5.2.1 if you are using Publisher v5.0.1 and Oracle 8.1.7:

1. Back up your `pub.conf` file, source directories, and your certificate store.
2. Uninstall the older Publisher version (see *Uninstalling UniCERT Core* on page 40).
3. Uninstall the Oracle 8.1.x client.



Normally, the Oracle client is in a different directory than the Oracle server when it is on the same computer. Do not remove the server software. If you are also upgrading the Oracle server to 9.2.0.5, see the *UniCERT v5.2.1 Database Administrator's Guide* for more information.

4. Install the Oracle 9.2 client.
5. Install the Publisher from the core CD (see *Installing UniCERT Core* on page 35).
6. Run the UniCERT Database Upgrade Utility; select **Start>Programs>Betrusted UniCERT v5.2.1>Database Upgrade Utility** and log onto your database.
7. Follow the instructions from the Database Upgrade Utility wizard.

Modifying the Publisher 5.2.1 configuration

Once you have restored your registry settings, installed the UniCERT Publisher v5.2.1, and updated its database, you also need to update its configuration to reflect your new installation directory structure.



If you are upgrading from UniCERT v5.2, you do not need to perform these steps; the installation directory structure is the same in v5.2.1.

To update the Publisher configuration:

1. Modify both the CA's and Publisher's configuration to point to the new directory where certificates and CRLs are stored:
 - a. In the CAO's PKI Editor, open the CA's properties and specify the new directory in the **Cache directory** field on the **Publications** tab.
 - b. In the Publisher Configuration, specify the same source directory on the **CA Source Directory and Publication Retries** screen.



For more information on configuring the CA and Publisher to post certificates, CRLs, and ARLs, see the *UniCERT Publisher v5.2.1 Administrator's Guide*.

2. Copy the CA certificate, ARL, and CRL from the old (or backed up) certificate store to the new certificate store; the new default location is C:\Program Files\Betrusted\UniCERT\Publisher\Config\CACertStore.
3. Copy your backed up to the new <install directory>\Publisher.

You can now start and use the Publisher services.

Installing the UniCERT Web components

For your convenience, the UniCERT Web components and WebRAO Client are provided on separate CDs from the rest of UniCERT Core:

- The UniCERT v5.2.1 Web Components CD provides the WebRAO servlets and JSPs, and the Web Handler and JSPs. This chapter describes how you install them.
- The UniCERT WebRAO v5.2.1 Client CD provides the WebRAO Client. For information on installing it, see Chapter 3, *Installing the UniCERT WebRAO Client*, in the *UniCERT WebRAO v5.2.1 Client User's Guide*.

Overview of the installation process

Follow these steps to install the WebRAO servlets and the Web Handler:

1. Verify that the computer you are installing on meets the necessary hardware and software requirements (see Chapter 2, *Installation prerequisites*).
2. Ensure that the components you require from the UniCERT v5.2.1 Core CD are installed (see Chapter 4, *Installing UniCERT Core*).
3. Prepare the information you require during the installation process (see *Preparing the information you require* on page 46).
4. Install the WebRAO servlets and the Web Handler as required (see *Installing the Web components* on page 47).
5. Create and configure the WebRAO and Web Handler instances you need (see *Adding, configuring, and deleting instances* on page 48).
6. Test that the WebRAO servlets are working correctly (see *Testing your WebRAO servlet installation* on page 51).

7. Set up the Web Handler (see Chapter 13, *Creating and using a Web Handler entity*, of the *UniCERT v5.2.1 Configuration Guide*).
8. Customize the Web Handler and the WebRAO (see Appendix B, *Customizing the WebRAO and Web Handler*, of the *UniCERT v5.2.1 Configuration Guide*).

Setting up the UniCERT components you require

Once you have installed UniCERT Core v5.2.1, set up your PKI to include the components you require for the WebRAO and the Web Handler. Specifically, this involves:

- Creating your PKI and setting up your CA and CAO
- Adding an RA to the PKI
- Adding an RA eXchange to the PKI
- Registering the WebRAO and/or Web Handler

See the *UniCERT v5.2.1 Configuration Guide* for instructions on creating and setting up your PKI.

Preparing the information you require

Before installing the UniCERT v5.2.1 Web components and creating instances for them, ensure that you have the following information for the Web Handler and the WebRAO:

- A name for your instance. If you are creating multiple instances, ensure each one has a unique name.
- The component's DN.
- The host name and port number of the RA eXchange it will connect to.
- The DN of the RA it will communicate through.

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

- DN: cn=Acme WebRAO, ou=California Branch, o=Acme, c=US
- Instance name: Acme WebRAO1
- RA eXchange host name: `hand.acme.com`
- RA eXchange port number: 6049
- RA DN: cn=Acme RA1, ou=California Branch, o=Acme, c=US

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

- DN: cn=Acme Web Handler, ou=California Branch, o=Acme, c=US

- Instance name: Acme Web Handler1
- RA eXchange host name: `knee.acme.com`
- RA eXchange port number: 6089
- RA DN: `cn=Acme RA2, ou=New York Branch, o=Acme, c=US`

Installing the Web components

To install the UniCERT v5.2.1 Web components, follow these steps:

1. Put the UniCERT v5.2.1 Web Components for Windows CD in your computer's CD drive. The installation wizard automatically starts. The screen shown in Figure 8 is the first screen you see.



Figure 8: Beginning the installation of UniCERT Core v5.2.1

2. Select the language you would like to work in and click **OK**.
3. Click **Next** on the **Introduction** screen. The **License Agreement** screen is displayed.
4. Accept the license agreement and click **Next**.

5. Accept the default installation directory, `C:\Program Files\Betrusted\UniCERT`, on the **Choose Install Folder** screen and click **Next**. Alternatively, specify another directory and click **Next**.



If you choose to install any UniCERT component to a directory other than the default, ensure the “)” character is not included in the directory path. Otherwise, the UniCERT component will not be able to connect to Oracle when you start it, as Oracle does not support all the characters that Windows supports in its filenames or paths.

6. Specify the Windows desktop or menu access to UniCERT on the **Choose Shortcut Folder** screen. By default, the installer creates a program group named **Betrusted UniCERT v5.2.1**. The installer does not prompt you for a shortcut folder if you already have the UniCERT Core v5.2.1 installed on your computer. Click **Next**.
7. Leave **Full Install** as the **Install Set** value to install both the WebRAO servlets and the Web Handler. Alternatively, choose **Custom** for **Install Set** and select the component you wish to install. Click **Next**.
8. Install the Java servlet engine, Tomcat, if you do not already have an equivalent engine installed. The installer only prompts you to install it if it detects that Tomcat is not installed. Click **Next**.



The installer installs the J2SE v1.2.4_03 even if you select not to install Tomcat.

9. Review the preinstallation summary information that the installer lists. If the details are correct, click **Install**.
10. We recommend that you read the `readme.html` as prompted.
11. Click **Done**.

Once you have installed the Web components, you need to create and configure the component instances. See *Adding, configuring, and deleting instances*.

Adding, configuring, and deleting instances

The UniCERT Web Components v5.2.1 CD provides a utility for adding, configuring, and deleting Web Handler and WebRAO instances. See *Adding or configuring a Web Handler instance*, *Adding or configuring a WebRAO instance* on page 50, or *Deleting an instance* on page 50 as appropriate.



The utility only accepts characters that you can enter at the command line.

If you have purchased and installed the UPI, an advanced UniCERT component, you can also use the utility to add, configure or delete a UPI instance. The utility works the same way for the UPI as for the Web Handler; however, if you are using the UPI v5.2, the required template file will not have been installed and the utility will create one.



Ensure that the UPI is installed to the same directory level as the WebRAO and Web Handler, for example, `<install directory>\UPI`.

Adding or configuring a Web Handler instance

Follow these steps to add a new Web Handler instance or configure an existing one:

1. Select **Start>Programs>Betrusted UniCERT v5.2.1>Web Components>Configure Web Handler**.
2. Enter an instance name as prompted.
If an instance under the name you provided exists, proceed to step 4. If no instance with that name exists, the utility prompts you to create one.
3. Type `y` to create a new instance. The utility creates a new instance and prompts you to configure it.
4. Configure the instance. The utility specifies the RA eXchange connection information. By default this is `localhost:6049`.
5. Type `y` to change this or `n` to leave it as it is.
If you did not modify the RA eXchange address, proceed to step 7.
If you chose to change it, continue from step 6.
6. Enter the new RA eXchange address. If you are running multiple RA eXchange clones and you want to include additional addresses, enter them in a comma separated list, for example, `localhost:6049,localhost:8976`.
7. The utility specifies the RA DN or `RAID`. Type `y` to change it or `n` to leave it as it is. If you chose to change it, type the new RA DN as prompted, for example, `cn=Acme RA,o=Acme,c=US`.
8. The utility specifies the Web Handler DN or `WebEEID`. Type `y` to change it or `n` to leave it as it is. If you chose to change it, enter the new Web Handler DN as prompted, for example, `cn=Acme Web Handler1,o=Acme,c=US`.
9. Close the command prompt. The Web Handler is updated with the configuration details you specified:
 - If you added a new instance, the utility creates a folder with the instance name you provided under `<install directory>\`

WebHandler/. It also adds the Web Handler context to `<install directory>\tomcat\jakarta-tomcat-4.1.27\conf\server.xml`.

- The utility configures the RA eXchange address, the RA DN (RAID parameter), and the Web Handler DN (WebEEID parameter) in `<install directory>\WebHandler\<instance name>\WEB-INF\web.xml`.

Adding or configuring a WebRAO instance

Follow these steps to add a new WebRAO instance or configure an existing one:

1. Select **Start>Programs>Betrusted UniCERT v5.2.1>Web Components>Configure WebRAO**.

2. Enter an instance name as prompted.

If an instance under the name you provided exists, proceed to step 4. If no instance with that name exists, the utility prompts you to create one.

3. Type `y` to create a new instance. The utility creates a new instance and prompts you to configure it.

4. Configure the instance. The utility specifies the RA eXchange connection information.

5. Type `y` to change this or `n` to leave it as it is.

If you chose not to modify the RA eXchange address, proceed to step 7.

If you chose to change it, continue from step 6.

6. Enter the new RA eXchange address, for example, `localhost:6049`. If you are running multiple RA eXchange clones and you want to specify another address, type `y` and enter the address. Otherwise, type `n`.

7. The utility specifies the RA DN or RAID. Type `y` to change it or `n` to leave it as it is. If you chose to change it, type the new RA DN as prompted, for example, `cn=Acme RA,o=Acme,c=US`.

8. Close the command prompt. The WebRAO is updated with the configuration details you specified:

- If you added a new instance, the utility creates a folder with the instance name you provided under `<install directory>\WebRAO`. It also adds the Web Handler context to `<install directory>\tomcat\jakarta-tomcat-4.1.27\conf\server.xml`.

- The utility configures the RA eXchange address and the RA DN (RAID parameter) in `<install directory>\WebRAO\<instance name>\WEB-INF\web.xml`.

Deleting an instance

You can also use the Web Components utility to delete an instance:

1. Open the command prompt and enter the following command:

```
java -jar config.jar <install directory> <component to configure> <instance name> -delete
```

For example:

```
java -jar config.jar "C:\Program Files\Betrusted\UniCERT\"
WebRAO WebRAO1 -delete
```

The Web Components utility removes the instance you specified.

2. Type `exit` to close the command prompt.

Testing your WebRAO servlet installation

To test that the WebRAO servlet components are working correctly, you can use Tomcat, the standalone server installed with UniCERT. The UniCERT installer adds the WebRAO context to `<install directory>\tomcat\jakarta-tomcat-4.1.27\conf\server.xml`, and configures the RA eXchange and the RA ID in `<install directory>\WebRAO\<WebRAO_instance>\WEB-INF\web.xml`.



Make sure you have an internet connection to the WebRAO servlets before testing the WebRAO Client.

After installing Tomcat and the WebRAO on the Web server:

1. Start Tomcat by running `<install directory>\tomcat\jakarta-tomcat-4.1.27\bin\startup.bat`.
2. Access the URL <http://localhost:8080/>. It loads the Tomcat default homepage in your Web browser.
3. Check that the WebRAO Client Web pages are installed correctly by accessing the WebRAO **Login** page in your Web browser. The default URL is http://localhost:8080/<WebRAO_instance>/.

If you or your Web server administrator has enabled SSL for secure connections, a browser dialog appears asking you to trust the SSL certificate when the WebRAO **Login** page loads. If an SSL warning message appears, SSL is not working. For information on using SSL with Tomcat, see *Configuring SSL support* on page 18.



The first time you load the WebRAO Client, it prompts you to trust content from Betrusted.

Using servlet managers with the WebRAO

As an alternative to testing the WebRAO servlet components with Tomcat, you can use your Web server and/or servlet managers. We do not provide full instructions for doing so, but instead give setup guidelines for ensuring that you can run the WebRAO.

Using ServletExec with Netscape

If you are using ServletExec as your servlet manager and your WebRAO clients are going to be using Netscape, remove the section

shown in Code example 1 from the `<InstanceName>\WEB-INF\web.xml` file.

Code example 1: Deleting code from the WebRAO's web.xml file

```
<error-page>
  <error-code>404</error-code>
  <location>/pages/unknown.jsp</location>
</error-page>
```

Using Sun Java System Web Server

If you are using the Sun Java System Web Server for the WebRAO or the Web Handler, add the section shown in Code example 2 to the `<install directory>\<component>\<InstanceName>\WEB-INF\web.xml` file.

Code example 2: Adding code to the WebRAO's or Web Handler's web.xml file

```
<servlet-mapping>
  <servlet-name>
    invoker
  </servlet-name>
  <url-pattern>
    /servlet/*
  </url-pattern>
</servlet-mapping>
```

Intranet deployment

When you download the WebRAO Client, the Java plug-in is installed. This requires an Internet connection to download the plug-in's installer from java.sun.com. You can modify the WebRAO's `applet.jsp` to point at an intranet location if a local connection is preferred.

See <http://java.sun.com/j2se/1.4.2/docs/guide/deployment/deployment-guide/upgrade-guide/deployment.html> for deployment details.



When modifying the WebRAO pages, ensure that the applet's name is not changed.

Deployment options To disable an optional WebRAO Client component, either rename the file on the server or move it out of the `<instance>/client` folder.

The component download is triggered by `KeyToolsProJava5220Signed.jar`; if it does not exist on the computer accessing the WebRAO Client URL, the WebRAO Client components are downloaded.

Troubleshooting

Provided the WebRAO **Login** page appears when you access the WebRAO Client URL, your WebRAO installation is successful. If the **Login** page did not display:

- Verify that you correctly specified the WebRAO instance name in the URL, including its capitalization.
- Double-check that the WebRAO context in `server.xml` matches your installation (see Code example 3).
- Double-check that the RA eXchange and the RA ID configuration in `web.xml` matches your installation (see Code example 4).

Code example 3: Redefining the WebRAO context

```
<Context path="/WebRAO" docBase="<install_dir>\WebRAO\<WebRAO_instance>" debug="0"
reloadable="true"/>
```

Code example 4: Redefining the RA eXchange and RA ID configuration

```
<param-name>RAeXchanges</param-name>
<param-value>localhost:6049</param-value>
...
<param-name>RAID</param-name>
<param-value>cn=Acme RA1,o=Acme,c=US</param-value>
```

If problems persist, we recommend removing and reinstalling the WebRAO. See *Uninstalling the UniCERT Web Components* on page 54.

You are now ready to test your PKI installation. Use the WebRAO Client to send a certificate request to your CA. If you receive the certificate once it is issued, your installation is working. See *Testing the WebRAO Client* in the *UniCERT WebRAO v5.2.1 Client User's Guide*.



The default URL for the WebRAO Client is http://<host name:port>/<WebRAO_instance>/. The default index page is located in `<install directory>\WebRAO\<WebRAO_instance>\sample-index.html`.

If your installation is still not working, contact Betrustrusted Global Support Services (globalsupport@betrustrusted.com). Supply as much of the following information as possible:

- A copy of `web.xml` from the WebRAO servlet's `<instance>/WEB-INF/` folder.
- Any output from the WebRAO Client's Java console window. To view the Java console, right-click the Java icon in the system tray and select **Show Console**.
- Any output from the servlet manager logs or console.

Uninstalling the UniCERT Web Components

You must uninstall the UniCERT WebRAO v5.2.1 and the UniCERT Web Handler v5.2.1 before reinstalling or upgrading them. You uninstall the WebRAO and the Web Handler separately. For simplicity, we refer to them as Web components in these instructions. The process for uninstalling differs according to whether you are uninstalling permanently or uninstalling before reinstalling or upgrading.

Uninstalling permanently

Remove a Web component from your computer before upgrading or reinstalling as follows:

1. Stop your Web server or servlet manager, for example, Tomcat.
2. Use the Web Components utility to delete any instances you have added. See *Deleting an instance* on page 50.
3. Use the Control Panel's Add/Remove Programs option to uninstall the Web component, selecting **Betrusted UniCERT v5.2.1 WebRAO** or **Betrusted UniCERT v5.2.1 Web Handler** as appropriate. Folders and files created after installation are not removed.
4. Manually delete the Web component's installation directory to remove any files that were not removed by the uninstall process. Ensure that files such as saved certificates or keys are deleted securely to prevent unauthorized people from accessing them.

Uninstalling before upgrading or reinstalling

To uninstall a Web component before upgrading or reinstalling, follow these steps:

1. If you have localized/customized your Web pages, make a backup copy of the servlet and applet `.properties` files before uninstalling the Web Server components.
2. Stop your Web server or servlet manager, for example, Tomcat.
3. Use the Control Panel's Add/Remove Programs option to uninstall the Web component, selecting **Betrusted UniCERT v5.2.1 WebRAO** or **Betrusted UniCERT v5.2.1 Web Handler** as appropriate. Folders and files created after installation, including WebRAO instances, are not removed.

Appendix A

Using UniCERT in its evaluated configuration

A

This appendix provides guidance on how to configure UniCERT v5.2.1 in its mandatory Common Criteria EAL4+ evaluated state, as well as best practice guidelines for designing and managing your PKI. Where appropriate, we indicate additional security measures you can implement when setting up your UniCERT PKI.

Read this appendix in conjunction with *Additional Guidance for Users and Administrators of the Common Criteria Evaluated Version of Betruusted UniCERT v5.2.1*. The *Additional Guidance* document forms part of the Common Criteria specific documentation for users and administrators. See also the *Security Target for Betruusted UniCERT v5.2.1* for further information on the evaluated UniCERT v5.2.1 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 v5.2.1 documentation set on the CD. Contact Global Support Services (globalsupport@betruusted.com) if you require them.

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 9).

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 the Luna CA3 HSM from SafeNet or the CosmopolIC smart card from Oberthur Card Systems in conjunction with UniCERT v5.2.1 for storing root keys, as they have Common Criteria EAL 4+ accreditation and provide tamper detection. See *Configuring components to work with UniCERT* on page 59 for the accredited versions of smart cards and HSMs.
- Do not use the UniCERT components ARM, CMP Handler, or UPI with the UniCERT core components, as they have not been evaluated for their security enforcing functions.
- 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.
- Implement security-related patches as soon as you receive them. For more information on patches, see Betrusted's One | Web secure server (<http://www.betrusted.com/support/oneweb.asp>).

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.

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 *Security enforcing UniCERT components* on page 65.



The CAO and WebRAO Client components are only available for the Windows platform.

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.

Planned hierarchy

Will there be one single security officer/system administrator to manage the entire PKI? If possible, use several administrators with responsibility for different components. See *Defining separate roles* on page 61.

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 *Deleting unauthorized users from the PKI* on page 62, and *Deleting a user account or database* in the *UniCERT v5.2.1 Administrator's Guide*.

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.

Splitting PSE files

In software, implementing split PSEs offers an additional means of protecting access to the keys and certificates contained on them. For more information on splitting PSEs, see Chapter 3, *Using the UniCERT Token Manager*, in the *UniCERT v5.2.1 Administrator's Guide*.



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

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 details on testing the WebRAO Client, see *Testing the WebRAO Client* in the *UniCERT WebRAO v5.2.1 Client User's Guide*.

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 UniCERT v5.2.1, 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 *Formulating a Certification Practices Statement* in the *UniCERT v5.2.1 Product Overview*, and Chapter 2, *Defining registration policies for certification*, in the *UniCERT v5.2.1 Configuration Guide*.

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.
- Do not share out the directories in which the component executables/shared libraries components 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.
- Use the native security options available for Windows platforms.
- 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.
- 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 and RA's database on a daily basis (see Appendix D, *Backing up and recovering databases*, in the *UniCERT v5.2.1 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.

You can choose to have the CA's PSE file split into parts and protected by more than one user's passphrase. In this way, the responsibility for creating or running the CAs is shared among two or more trusted security officers; one person cannot load the PSE if he knows only his passphrase and the PSE has been saved as multiple parts, each protected by a different person's passphrase.

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 core installation of UniCERT v5.2.1 in its evaluated configuration:

- Ensure you use HSMs with sufficient cryptographic hardware validation. For example, the Luna CA3 version 3.97, software versions 8.0 and 8.1 HSM from SafeNet has Common Criteria EAL 4+ assurance as well as FIPS 140-1 level 3 accreditation.
- Ensure any smart cards you use have sufficient cryptographic validation. For example, the CosmopolIC 2.1 v4 smart card from Oberthur Card Systems has Common Criteria EAL 4+ and FIPS 140-1 level 2 accreditation.
- The Luna CA3 version 3.97 HSM from SafeNet is the only HSM device with both Common Criteria EAL 4+ and FIPS 140-1 level 3 accreditation, supported by UniCERT v5.2.1, that also provides passive detection of physical tampering, such as tamper-detection seals, locks, and zeroization switches.

Best practice guidelines

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

Backing up your PKI

Back up the CA and RA 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 floppy disks, optical media, or magnetic tape, store them securely under lock and key or in a fire-proof safe.

Passwords and PINs

Create strong passwords for user accounts on CA and RA 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.



Remember to 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, 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. Delete the old smart card from your PKI using the Token Manager and issue the first WebRAO Client user with a new certificate and keys on a new smart card.

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 v5.2.1 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.

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 v5.2.1 in its Common Criteria EAL4+ evaluated state, ensure you set up three CAO users.

Auditing your system

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

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 v5.2.1 offers individual accountability for all transactions carried out in the PKI.

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 them 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 22, *Administering certificates*, in the *UniCERT v5.2.1 Configuration Guide*, as well as *Deleting a user account or database* in the *UniCERT v5.2.1 Administrator's Guide*.

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

CAO users

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

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

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

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.

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.

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.

CA, RA, and KAS

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.



The Luna CA3 software v8.2 HSM from SafeNet supports M of N authorization on its tokens and has Common Criteria EAL 4+ accreditation. We recommend you use the Luna CA3 HSM 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, or the RA:

- Disable all communication ports that are not in use by the CA, CAO, and RA, especially Telnet ports.
- Change user passwords and PINs regularly.

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 RA eXchange and the CSS computers 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 the 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* in the *UniCERT WebRAO v5.2.1 Client User's Guide*.
- Change the passwords on user accounts regularly.

Security enforcing UniCERT components

The PKI configuration suggested in *Example of an evaluated configuration of UniCERT* is based on the following assumptions about the security enforcing functions of UniCERT v5.2.1 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:

- CA
- CAO
- RA
- RA Auditor
- RA eXchange
- CSS
- email Handler
- SCEP Handler
- Web Handler
- WebRAO

The following components have not been evaluated for their security enforcing functions, but they interoperate using secure interfaces with the UniCERT core components. Therefore, we consider them as part of this secure configuration:

- Database Wizard
- Key Archiver
- Publisher

Do not include the following components in an evaluated configuration of UniCERT 5.2.1, as their interfaces with core UniCERT components have not been evaluated for security enforcing functions:

- ARM
- UPI
- CMP Handler

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 9i database is installed. These are issues that affect the performance of your PKI, but they do not directly affect its secure functioning.

Ordinarily, if you clone the CA or RA it does not present a security risk. However, if you store the CA or RA PSEs on tokens, you must also clone the token, presuming your hardware device permits cloning. If you do this, ensure you restrict access to the cloned token to trusted administrators. See Chapter 18, *Cloning*, in the *UniCERT v5.2.1 Configuration Guide*.

The sample PKI illustrated in Figure 9 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 *Betrusted Security Target* document.

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 protected by the M of N feature of the Luna CA3 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 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 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 receives requests from the POP server or listens for communications from the RA eXchange.



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

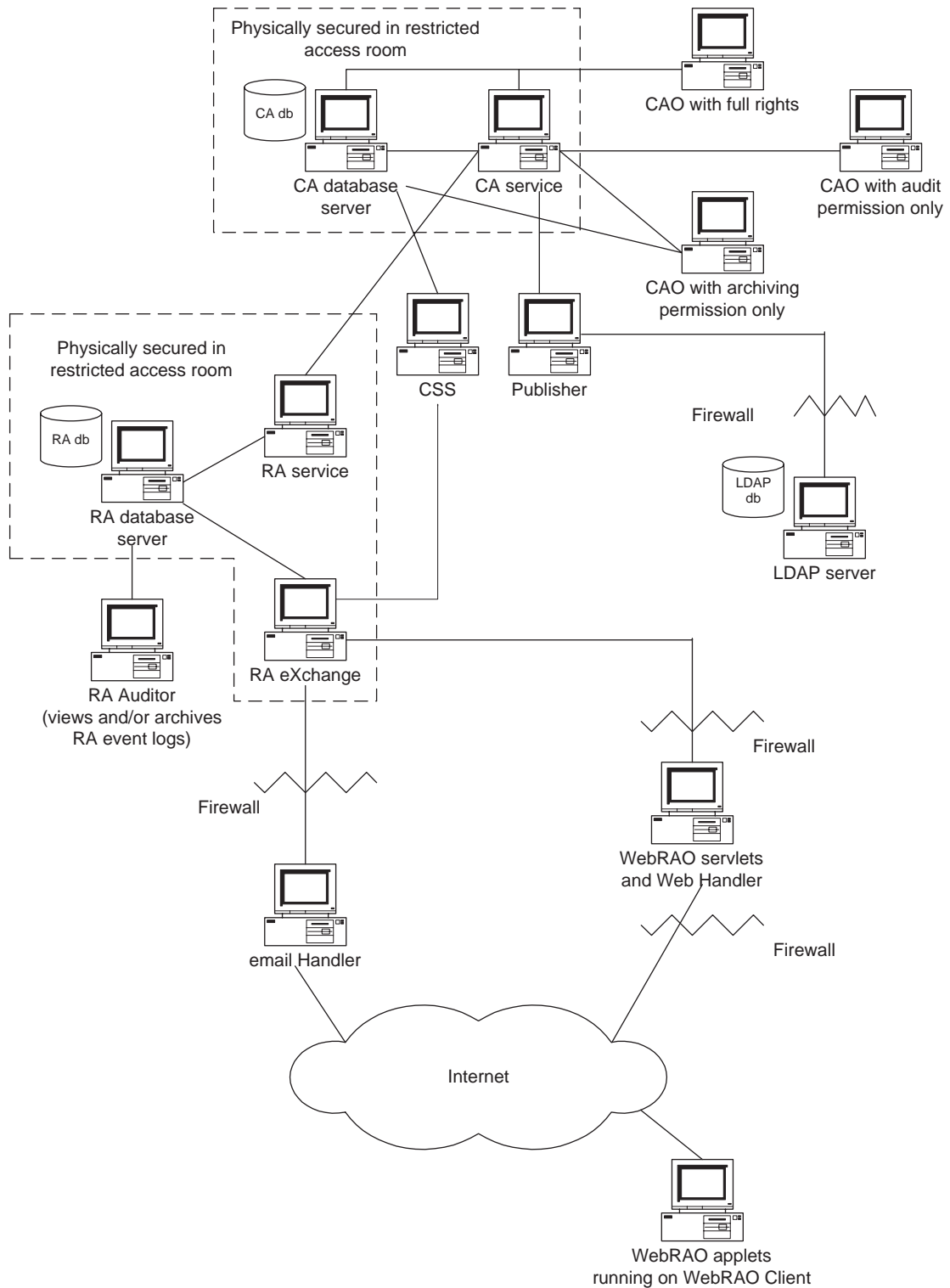


Figure 9: A secure PKI configuration

Index

A

- Access
 - preventing unauthorized, 58, 62
- Active Directory, 16
- AEP Systems, 14
- Apache, 17
- applet.jsp, 52
- Archiving
 - and auditing role, 61
 - keys, 5
- ARM
 - description, 5
 - installing, 38
- Audience, 3
- Auditing
 - archiving role, 61
 - CAO rights, 61
 - defining audit policies, 62
 - event logs, 61, 62
 - reviewing logs, 62

B

- Backing up
 - databases, 59
 - on hardware, 60
 - PSEs, 59
- Betrusted, 7
- Browsers
 - supported, 19

C

- CA
 - cloning, 22
 - hierarchy, 24
 - outsourcing, 27
 - securing, 26
 - security, 56
- CAO
 - deleting user, 62
 - deployment, 26
 - managing clones, 35
 - revoking user, 62
 - users, 61
- Certificate applicants
 - generating own keys, 23

requirements, 19

- Certificate revocation lists
 - See CRLs
- Certificates
 - for Web server, 18
 - standard, 7, 19
- Certification Policy, 58
- Certification Practices Statement
 - See CPS
- Chrysalis-ITS, 14
- Cisco
 - requirements, 17
- Cloning
 - failover facility, 22
 - installation, 35
 - load balancing, 22
- CMP standard, 21
- Common Criteria, 55
 - evaluated components, 65
 - sample configuration, 66
- Configuring
 - evaluated components, 66
 - SSL, 18
 - UniCERT components, 55
- Connecting
 - RA eXchange to other entities, 34
- Conventions, 6
- CP Directory Server, 16, 17
- CPS, 3, 58
- CRLs
 - reference, 7
 - support, 19
- Crypto profiles
 - for clones, 35
 - removing, 41

D

- Databases
 - upgrading, 9
 - upgrading 8.1.x clients, 42
- Datakey, 15
- Deleting
 - registry keys, 40
 - services, 41

| Index

- unauthorized users, 62
- Web components, 50
- Demo PKI
 - configuration, 22
 - testing, 23
- Deploying a PKI
 - considerations, 56
 - demo example, 21, 22
 - hosting example, 21, 25
 - installing components, 21, 22
 - outsourcing, 26, 27
 - PKI design, 21
 - VPN example, 21, 23
- Directory servers
 - installing, 33
 - supported, 16
- DirX, 17
- Distinguished names
 - See DNs
- DNs
 - configuring for Web Handler, 49
 - configuring for WebRAO, 50
 - determining for components, 31, 46
- Documentation
 - on non-core CDs, 4
 - set for core components, 2

E

- EAL4, 55
- Email
 - supported clients, 19
 - supported servers, 19
- Enterprise Validation Authority
 - See Validation Authority
- Environments supported, 10

F

- Firewalls, 37

H

- Hardware requirements, 11
- Hosted PKI, 25
 - privacy concerns, 27
 - requirements, 26
 - sample deployment, 26, 28
- HSMs
 - definition, 13
 - supported, 14

I

- IIS, 17
- Installation
 - characters supported in paths, 36, 48
 - clones, 35
 - default directory, 36, 48
 - distributed, 34
 - example deployments, 21, 22, 23, 25
 - on one computer, 33
 - PKI design, 21
 - preinstallation information, 31
 - reinstalling UniCERT, 40
 - reinstalling WebRAO, 54
 - required parameters, 31
 - tasks, 23
 - testing, 53
 - testing UniCERT, 33
 - third-party products, 32
 - Tomcat, 17, 48
 - upgrading, 40, 54
- Instances
 - deleting, 50
 - updating their path, 40
- Internet Explorer
 - supported versions, 19
- iPlanet, 16
 - See Java System Web Server

J

- Java plug-in, 52
- Java System Directory Server, 16
- Java System Web Server
 - setup, 52
 - supported version, 17
- JRE, 17

K

- Key Archiver
 - CD, 5
 - installing, 38
- Keys
 - for Web server, 18
 - sizes, 15, 18

L

- Licensing
 - UniCERT, 57
- Luna CA3, 14

M

Memory, 15

Microsoft

- Active Directory, 16
- Exchange Server, 19
- Windows versions, 10

N

nCipher, 14

Netscape, 19

O

OCSP

- example of use, 28
- supported responders, 17

Operating systems supported, 10

Oracle

- deployment, 12, 22
- interoperability with UniCERT, 33
- replicated databases, 28
- supported versions, 13

Outsourcing

- CA, 26
- RA, 27

P

Passphrases

- changing, 60
- keeping secure, 59
- multi-authorization, 59

Path environment variable, 41

PINs

- changing, 61

PKCS#11 devices

- accreditation, 16
- changing PINs, 61
- supported drivers, 14

PKI

- administrators, 58
- audit policy, 56
- best practices, 55
- demo, 22
- demo deployment, 22
- deployments, 1, 21
- designing, 21
- guidelines, 60
- hierarchy, 24, 34
- hosted, 25
- installing components, 21, 22

outsourcing, 26, 27

preinstallation information, 31

protecting, 63

security, 59

tasks, 23

testing, 23

VPN deployment, 23

Plug-ins

customized, 5

developing for ARM, 5

Java, 52

Port numbers

avoiding conflicting, 34

clones, 35

Prerequisites

PKI information, 31

reading, 4

Preventing unauthorized access, 58

Privacy concerns, 27

Protocol handlers

not using Oracle, 33

testing, 23

PSEs

backing up, 41, 59

passphrases, 32

removing, 41

splitting, 59

R

RA

cloning, 22

outsourcing, 27

using multiple, 34

RA Auditor

replacing, 63

RA eXchange

using multiple, 34

Rainbow, 15

References, 7

Registration policies

See RPs

Registry, 39, 59

Requirements

browsers, 19

Cisco, 17

directory servers, 16

email clients, 19

email servers, 19

hardware, 11

JRE, 17

| Index

- knowledge, 4
 - Oracle, 13
 - PKCS#11 devices, 14
 - timestamp servers, 17
 - Web server, 17
- Revocation
- unauthorized users' certificates, 62
 - untrustworthy entities, 62
- RPs
- deleting, 41
 - documented, 2
- ## S
- SafeNet, 14
- SCEP Handler
- requirements, 17
 - sample deployment, 24
- Security
- CA, 56
 - components enforcing, 65
 - measures, 58
 - physical and logical, 63
- Security officers
- See SO
- Services
- deleting, 41
 - enabling on Windows XP, 37
 - starting, 55
 - stopping, 41
- Servlet managers
- supported, 17
 - troubleshooting, 53
 - using, 51
- ServletExec, 51
- SIDs
- required information, 31
- Smart cards
- supported, 14
- SO
- defining the CPS, 3
 - managing the PKI, 22
 - replacing, 63
 - using multiple, 57, 59
- SSL
- configuring, 18
 - key size limitation, 18
 - reference, 18
- Standards, 19
- Sub CAs, 34
- Supported versions
- directory servers, 16
 - JRE, 17
 - OCSP responders, 17
 - Oracle, 13
 - smart cards, 14
 - Timestamp servers, 17
 - Web servers, 17
 - Windows, 10
- SureWare Keyper, 14, 16
- ## T
- Testing
- WebRAO setup, 51
 - your PKI, 22, 57
- Third-party products
- installing, 33
- Timestamp servers
- supported, 17
- Tomcat
- installation, 17, 48
 - loading homepage, 51
 - supported version, 17
- Topics in documentation set, 3
- Troubleshooting
- WebRAO installation, 53
- Tumbleweed, 17
- ## U
- UniCERT
- ARM CD, 5
 - compatibility, 9
 - components, 10
 - components requiring Oracle, 12
 - Core CD, 1
 - documentation, 2
 - evaluated components, 65
 - hardware requirements, 11
 - installing to different computers, 34
 - installing to one computer, 33
 - Key Archiver CD, 5
 - licensing, 22, 57
 - non-core components, 4
 - preliminary tasks, 23
 - recommended order of core documents, 2
 - relation of components, 1
 - removing, 40
 - software requirements, 9
 - upgrading, 39, 41
- Unicode, 19
- Uninstalling

- before upgrading, 41
- completely, 40

Upgrading, 39

- core components, 40
- Publisher, 42
- Web Handler, 54
- WebRAO, 54

UPI, 5

- installing, 38

URLs

- Apache, 18
- Betrusted, 7
- PKCS standards, 7

UTF8, 33

V

ValiCert, 17

Validation Authority, 17

Virtual private networks

- See VPNs

VPNs

- client, 17
- requirements, 23
- sample deployment, 25

W

Web Handler

- installing, 47
- using Java System Web Server, 52

Web servers

- integrating tomcat with, 17
- supported, 17
- testing with UniCERT, 23

WebRAO

- installing, 47
- intranet deployment, 52
- sample deployment, 24
- testing, 23, 51
- troubleshooting, 53
- using servlet managers, 51

WebRAO Client

- deploying, 52
- optional deployment, 52
- replacing users, 63

web.xml, 53

Windows

- installing on XP, 37
- systems supported, 10

X

X.509

- certificates, 19
- CRLs, 19

