COMODO
Creating Trust Online®

Comodo
Certificate Manager

Comodo Certificate Authority Proxy Server Architectural Overview

Comodo CA Limited
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Table of Contents

Legal Information

1.Preface

This manual provides an architectural overview of Comodo Certificate Authority Proxy Server (Comodo CAPS). Basically, it describes how the Comodo CAPS functions. It lays an important conceptual foundation for much of the practical information contained in other manuals. Information in this manual applies to the Comodo CAPS running on all operating systems.

2.Overview

Comodo CAPS is an integral part of Comodo Active Directory Agent (Comodo ADA), which is designed as a service of operation system. It is intended to replace the original Certificate Authority (CA) component of Active Directory Certificate Services (AD CS). It acts like the original component, but uses Comodo Certificate Manager (CCM) for certificate enrollment instead of functioning in independent CA mode. The implementation of Comodo CAPS is highly compatible with the native Microsoft CA. This brings many key advantages, such as:

- Usage without additional client software at workstations
- Support of invisible to end-user Microsoft automatic enrollment and renewal
- Support of all versions of certificate templates from Win2000 to Win2008R2 functional level.
- Full integration into the Microsoft User Interface. PKI administrator can manage Comodo CAPS using Server Manager utility, other standard system tools, command line and scripts. Existing skills and knowledge of PKI administrator are applicable.
- Compatible with Web-based enrollment role and other sub-roles of Active Directory Certificate Services.

3.Environment Description

3.1.The Working Environment

Comodo CAPS is not the only integral part of CCM. From another side, it is the subsystem of Microsoft Certificate Authority Services. Figure 1 depicts the working environment of Comodo CAPS.

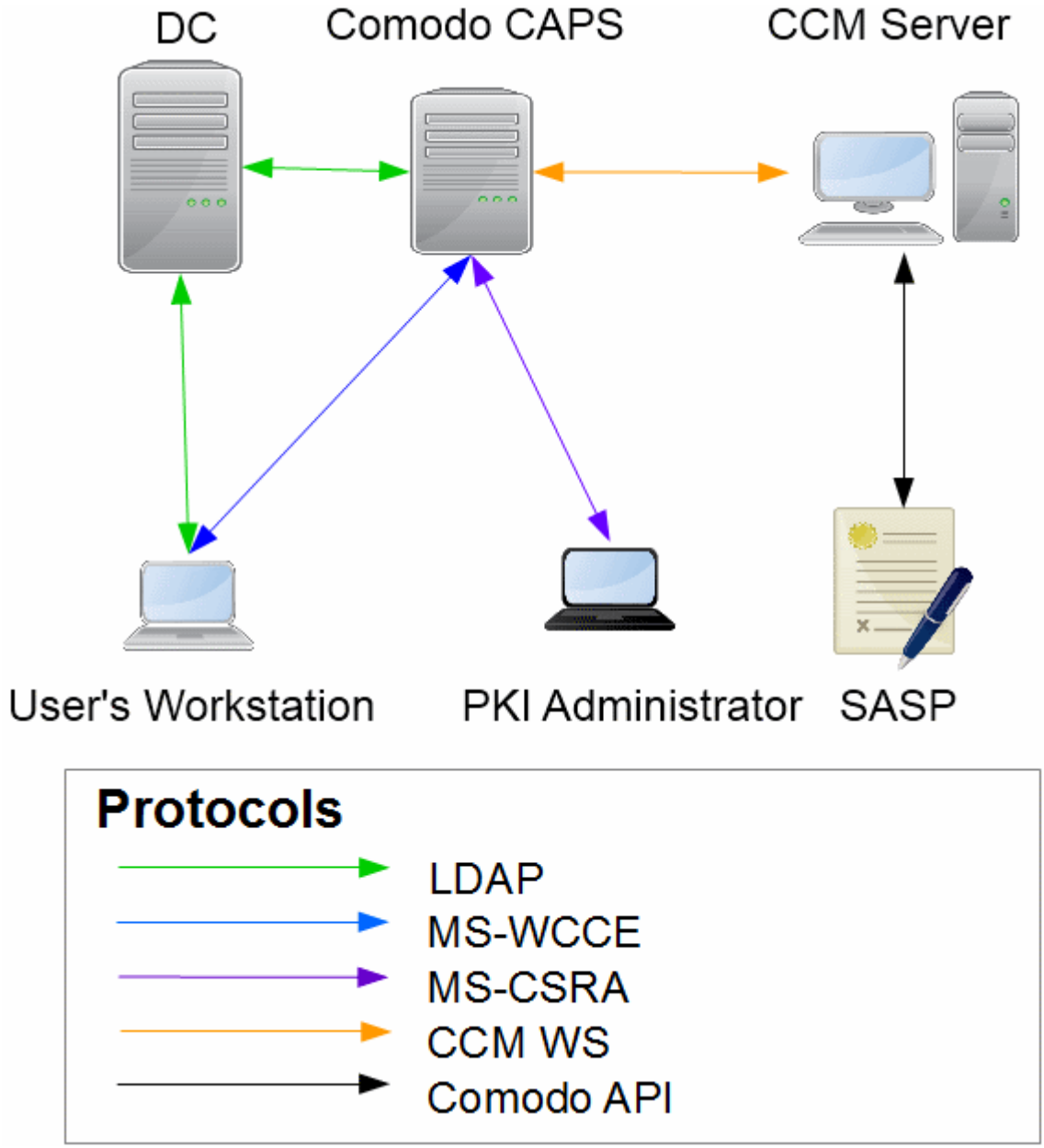

Figure 1. Working environment of Comodo CAPS

This figure shows the auto-enrollment process. Please refer to time diagrams for interactions details.

3.2. Protocols Usage Explanation

3.2.1. LDAP Usage

LDAP - Lightweight Directory Access Protocol, provided by Active Directory for accessing information services over network. It is a well-known protocol, so details related to it are omitted in this document. It is used by:

- Client's Workstation for retrieving information about templates and available certification authorities (CA's).
- Comodo CAPS for retrieving attributes of AD user according to template settings

3.2.2. MS-WCCE Usage

WCCE – Windows Client Certificate Enrollment Protocol is a set of DCOM (Distributed Component Object Model) interfaces. It is used for interactions between clients and Comodo CAPS to perform enrollment, revocation and property retrieval.

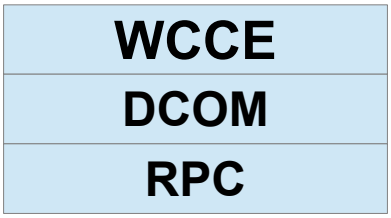

Figure 2. WCCE Protocol Stack

3.2.3. MS-CSRA Usage

CSRA - Certificate Services Remote Administration Protocol is a set of DCOM interfaces, which is used for interactions between administrative tools and Comodo CAPS. It allows configuring the state and policy of Comodo CAPS by native Windows Server Manager as well as by third party utilities. It is also used for management of requests and certificates, stored in the Comodo CAPS database.

4. Process View

4.1. About Process View

This section explains the behavior of Comodo CAPS environment during operations of enrollment and revocation. It deals with the dynamic aspect of each participant in the environment, as shown in the Process Diagrams.

4.2. Understanding Process Diagrams

Both Enrollment and Revocation operations are described by a set of time diagrams, which shows the sequence of interactions between all participants of a corresponding operation. The list of participants varies for different operations. Each participant has a separate time axis on the diagram, but a time scale is common for all axes. Each interaction phase changes a state of two participants, so it is displayed as an arrow between them, directed from initiator. A variety of communication protocols are used for different interactions. Each arrow is marked by special color that depends on a protocol used for corresponding interaction. A beginning and ending of interaction phases are interpreted as pair of events for the pair of participants. Each event is named with letter, which indicates event type (A – start of operation, Z – successful, T – middle event, E – failure) and digital order number, which is unique for a diagram. Please, see Figure 4 for details. This legend is common for all Process Diagrams.

4.3. Enrollment Process View

Enrollment Process Diagram is represented in Figure 3.

4.3.1. List of Participants

- Client's Workstation (Client)
- CA Administrator's Workstation
- Domain Controller (DC)
- Comodo CA Proxy Server (CA)
- CCM Server
- SASP

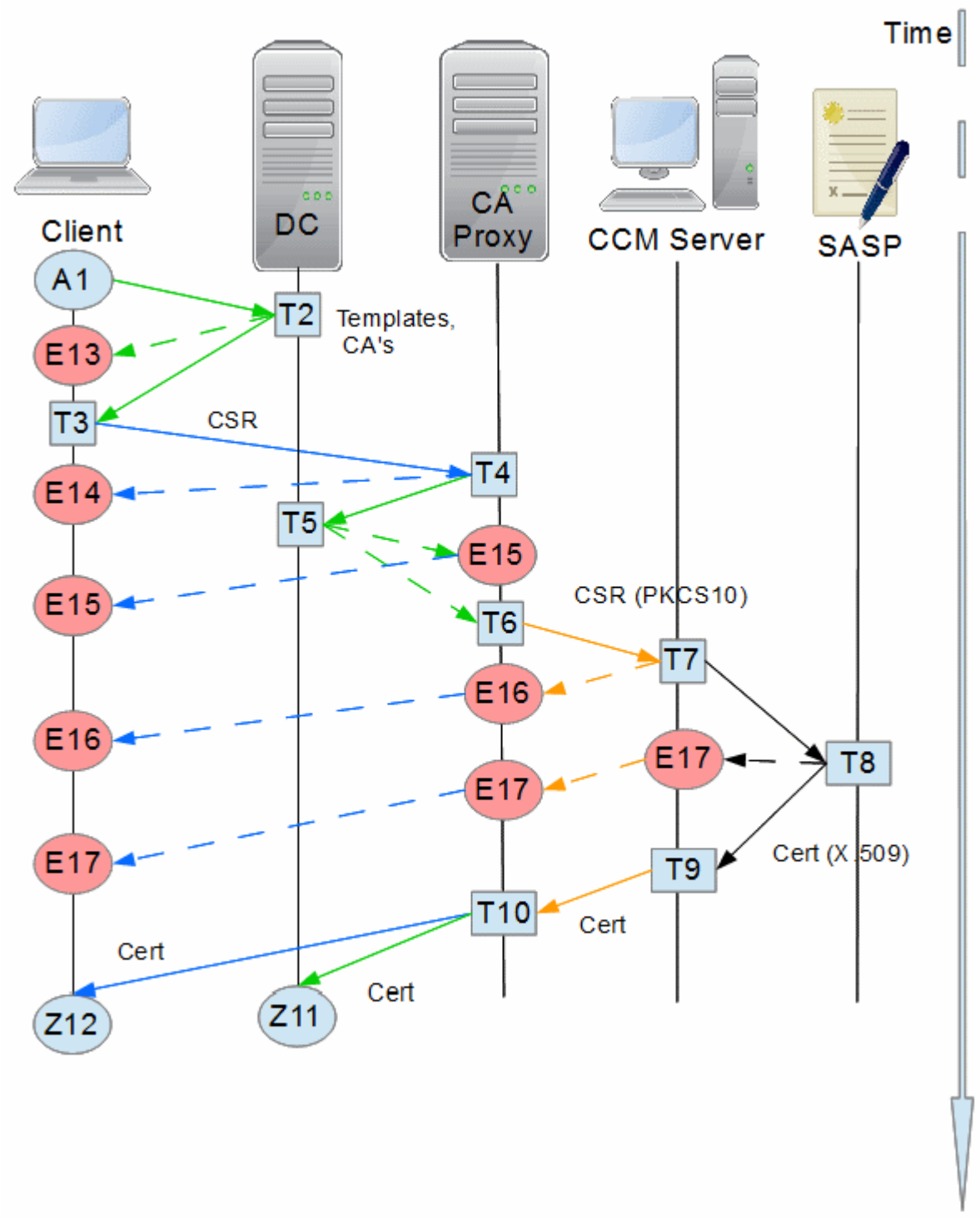

Figure 3. Enrollment process view

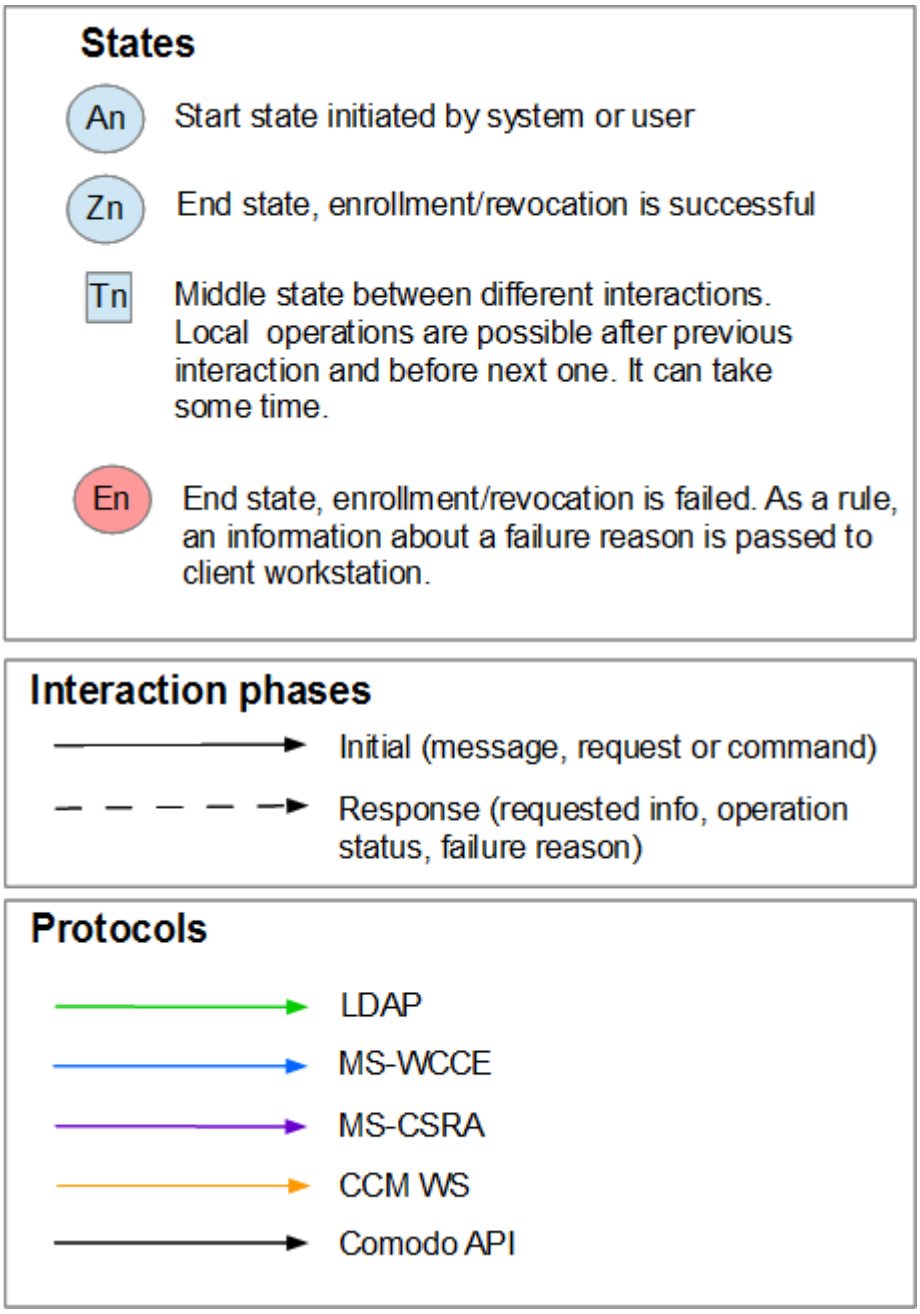

Figure 4. Time Diagrams Legend

4.3.2. Events and Phases Specification

This specification is time-ordered. It describes all events from enrollment triggering to certificate installing.

4.3.2.1. Phase 1

ID	Name	Type	Side
A1	Start event	Initial	Client's Workstation
Description: This is initial event. It starts each enrollment operation. There are several sources, which can cause this event: • An autoenrollment feature			

- A domain user, which uses system tools for interactive-based enrollment
- A third-party software running at computers of a domain

Remarks:

Basically, the autoenrollment process is triggered at logon time (but not at workstation unlocking). It is activated and managed by a domain-based Group Policy. Machine-based Group Policy as well as user-based Group Policy is able to start autoenrollment process. The Group Policy is applied at reboot, or at logon. It is refreshed every eight hours and this interval can be configured. Also autoenrollment can be triggered by an internal timer that activates every eight hours.

4.3.2.2. Phase 2

ID	Type	From	To	Protocol
A1-T2	Initial phase	Client	DC	LDAP

Description: Client requires the list of available templates and CA's. This phase is composite. It includes two independent requests: template request and CA request. In order to make Figure 3 more brief two actions are displayed as one merged action.

Results:

- Successful – next phase is **T2 - T3**.
- Failed - next phase is **T2 - E13**

4.3.2.3. Phase 3

ID	Type	From	To	Protocol
T2-T3	Response phase	DC	Client	LDAP

Description: Client receives the list of available templates and CA's. This phase is composite. It includes two independent responses: template list and CA list.

Local actions at T3 time point: Select the required template according to rules of WCCE (Windows Client Certificate Enrollment Protocol) specification.

Result: Start **T3 - T4**

4.3.2.4. Phase 4

ID	Type	From	To	Protocol
T3-T4	Initial phase	Client	Comodo CAPS	WCCE

Description: Client creates certificate request (CSR) according to one of the certificate templates and submit it to Comodo CAPS.

Remarks: Clients must use one of the following formats of CSR: PKCS #10 (RFC2986), CMC (RFC2797) or CMS (RFC3852). CMC or CMS encapsulates a PKCS #10 structure.

Results:

- CSR transmission successful – next phase is **T4 - T5**.
- CSR transmission is failed - next phase is **T4 - E14**

4.3.2.5. Phase 5

ID	Type	From	To	Protocol

T4-T5	Initial phase	Comodo CAPS	DC	LDAP

Description: Comodo CAPS requests the set of values of the user object attributes in Active Directory by performing a search request against a DC. Please, refer to table in the section '**4.3.3.1 User's attributes that passed to CCM with Certificate Signing Request and revocation** ' for details about requested attributes.

Local actions at T4 time point: Security checking about the requester permissions. The enrollment permission at Comodo CAPS is required, otherwise T4-E14 phase will be initiated.

Results:

- Successful - next phase is **T5 - T6**
- Failed - next phase is **T5 - E15**

Remarks: Template-based CSR does not contain attributes from user's account.

Fully qualified domain name (FQDN) and the distinguished name (DN) of the user is used by Comodo CAPS for the search performing.

4.3.2.6. Phase 6

ID	Type	From	To	Protocol
T5-T6	Response phase	DC	Comodo CAPS	LDAP

Description: Comodo CAPS receives the set of values of the user object attributes from Active Directory by request, initiated at T4-T5 phase. Please, refer to the section 4.3.3.1 for details about requested attributes.

Result: – next phase is **T6 - T7**

4.3.2.7. Phase 7

ID	Type	From	To	Protocol
T6-T7	Initial phase	Comodo CAPS	CCM	CCM WS

Description: Comodo CAPS sends the CSR Package to CCM

Local actions at T6 time point: CSR Package building. It consists with PKCS#10 CSR and user's attributes.

Results:

- Successful – next phase is **T7 - T8**
- Failed - next phase is **T7 - E16**

Remarks: CCM works with PKCS#10 requests only. If CSR has CMC or CMS format, only internal PKCS#10 part will be extracted and included into CSR Package.

4.3.2.8. Phase 8

ID	Type	From	To	Protocol
T7-T8	Initial phase	CCM	SASP	Comodo API

Description: CCM sends the CSR Package to SASP

Local actions at T7 time point: CCM validates user's attributes from CSR Package. If user's e-mail does not exists in the CCM database, an new account for this person will be created and it will be filled with attributes from CSR Package. If such e-mail is already exists, other attributes must match.

Results:

- Successful – certificate is collected, next phase is **T8 - T9**
- Failed - next phase is **T8 - E17** (across all participants)

Remarks: It may take some time to collect certificate by CCM.

4.3.2.9. Phase 9

ID	Type	From	To	Protocol
T8-T9	Response phase	SASP	CCM	Comodo API
Description: CCM collects the certificate from SASP **Local actions at T9 time point**: CCM writes new certificate to the database and make it accessible from corresponding UI form. **Results**: next phase is **T9-T10**				

4.3.2.10. Phase 10

ID	Type	From	To	Protocol
T9-T10	Response phase	CCM	Comodo CAPS	CCM WS
Description: Comodo CAPS receives the certificate from CCM **Results**: next phase is **T10 - T11**				

4.3.2.11. Phase 11

ID	Type	From	To	Protocol
T10-Z11	Response phase	Comodo CAPS	DC	LDAP
T10-Z12	Response phase	Comodo CAPS	Client	WCCE
Description: Comodo CAPS passes the certificate to Client Workstation and to DC. The enrollment process started at Client's workstation installs the certificate into Certificate Store. At the same time Comodo CAPS binds the certificate to the Active Directory user object. **Local actions at T10 time point**: Comodo CAPS makes changes into the CA database. It writes the new certificate and marks corresponding request record as completed. **Results**: Enrollment is complete. The certificate is accessible at the sides of all participants				

4.3.3. CCM Enrollment Specific Details

Comodo CAPS follows some rules and restrictions about enrollment process. This is necessary to keep compatibility with the business rules of CCM. The particulars are listed below.

4.3.3.1. User's Attributes that Passed to CCM with Certificate Signing Request and revocation

	Name of the attribute	Can be	Remarks

		empty	
1	First Name	No	
2	Last Name	No	
3	E-mail	No	Identifies the person at CCM side
4	Company	No	RDN=O (Organization Name)
5	Department	Yes	RDN=OU (Organization Unit Name)

Remark: When CCM receives new CSR with the attributes package, which includes new e-mail, a new person will be created.

4.3.3.2. Key Usage of Active Directory Certificate Template Restriction

Key Usage of Active Directory template MUST be set according to KU bindings in corresponding CCM template.

4.3.3.3. Application policies of Active Directory certificate template restriction

Application policies list in Active Directory template and EKU bindings list in CCM template MUST be equal by used aggregate of OIDs. Each Application policy in AD template MUST have corresponding EKU binding in CCM template.

4.4. Revocation Process View

Comodo CA Proxy supports two revocation methods:

- Manual revocation, which can be started using Server Manager tool as well as any third-party software, that support MS-CSRA protocol for interaction with Windows Certification Authorities. This method allows to revoke any selected certificate.
- Automatic revocation triggered by deletion of a domain user's account. This is group operation. After deletion of an account it will be applicable to all certificates of corresponding user. Automatic revocation can be online and postponed.
    - Online revocation is real-time and it takes place immediately after deletion of a domain user's account or changing it's attributes.
    - Postponed revocation will useful in the case, when Comodo CAPS does not run during deletion of a domain user's account or changing it's attributes. The mechanism of postponed revocation turns on after Comodo CAPS startup. This is background process and it does not interfere with the certificate enrollment. To make postponed revocation possible, Comodo CAPS stores attributes of existing domain users accounts into special database, which will help to detect all changes caused while Comodo CAPS is stopped.

4.4.1. Manual Revocation Process Overview

Manual revocation process is illustrated in Figure 5. The legend of this diagram is displayed in Figure 4.

4.4.1.1. List of Participants

- CA Administrator's Workstation
- Comodo CA Proxy Server (CA)
- CCM Server

- SASP

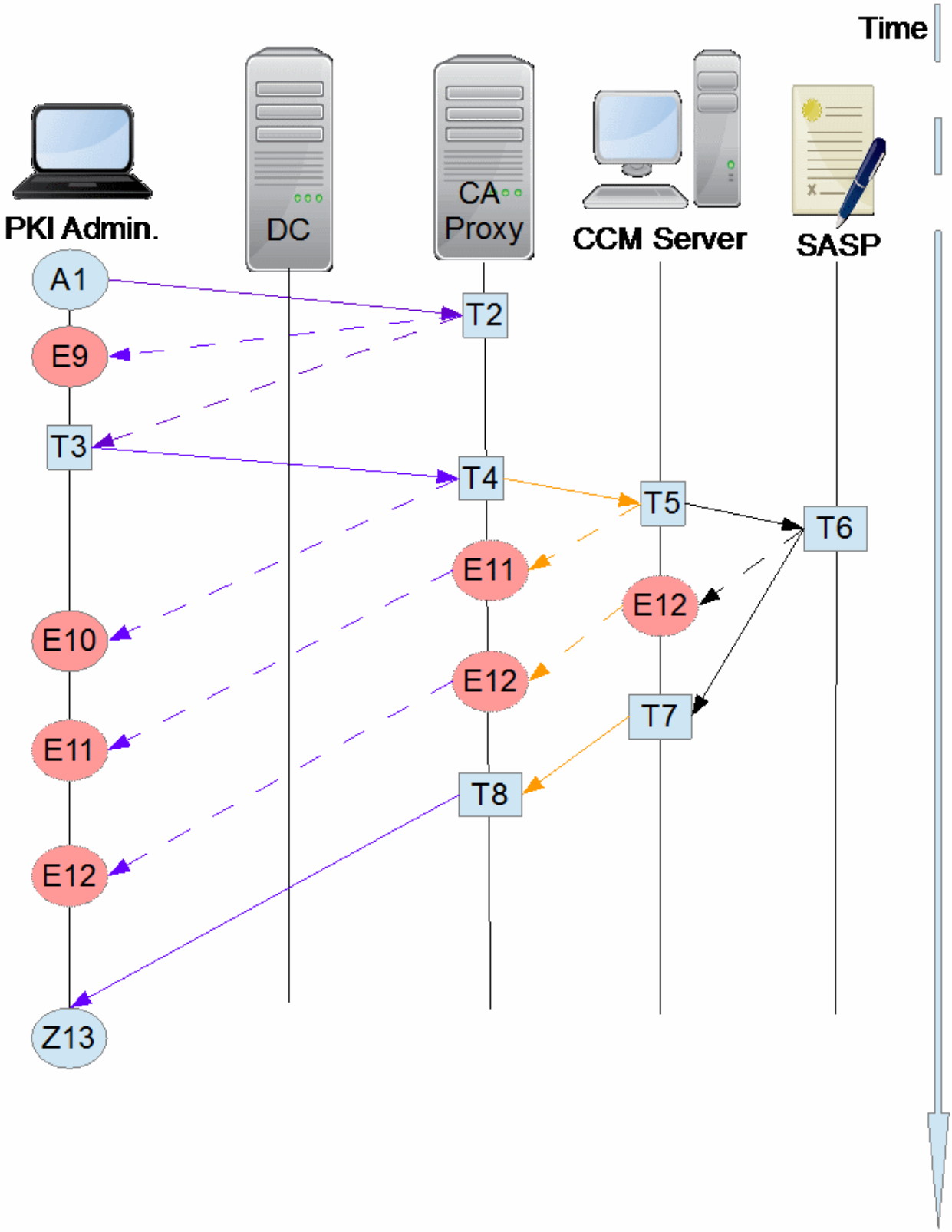

Figure 5. Manual revocation process view

4.4.1.2. Events and Phases Specification

This specification is time-ordered. It begins from issued certificates request and ends with operation response to Administrator's workstation.

4.4.1.2.1. Phase 1

ID	Name	Type	Side
A1	Start event	Initial	Administrator's Workstation
Description: This is initial event. Basically, it is caused by Comodo CAPS Administrator using Server Manager.			

4.4.1.2.2. Phase 2

ID	Type	From	To	Protocol
A1-T2	Initial phase	Administrator	Comodo CAPS	CSRA

Description: Administrator requests the list of issued certificates from Comodo CAPS.

Results:

- Successful – next phase is **T2-T3**.
- Failed - next phase is **T2-E9**

Remarks: This request can be performed before the time point of manual revocation starting. It is depend on implementation of CSRA client role of used administration tool

4.4.1.2.3. Phase 3

ID	Type	From	To	Protocol
T2-T3	Response phase	Comodo CAPS	Administrator	CSRA

Description: Comodo CAPS returns the list of issued certificates to Administrator.

Results: The next phase is **T3-T4**.

Remark: According to CSRA protocol a data set with issued certificates can be transferred by piecemeal. Typically, an administration tool will retrieve next record set when user scrolls down the list. Such behavior helps to optimize the network exchange between CA and Administrator's workstation.

4.4.1.2.4. Phase 4

ID	Type	From	To	Protocol
T3-T4	Initial phase	Administrator	Comodo CAPS	CSRA

Description: An Administration tool sends to Comodo CAPS certificate serial number for revocation.

Results:

- Successful – next phase is **T4-T5**.
- Failed - next phase is **T4-E10**.

Remark: An Administration tool must obtain the certificate ID from the record set, received at **T2-T3** phase. Otherwise, Comodo CAPS will generate an error.

4.4.1.2.5. Phase 5

ID	Type	From	To	Protocol
T4-T5	Initial phase	Comodo CAPS	CCM	CCM WS

Description: Comodo CAPS sends to CCM certificate serial number for revocation.

Results:

- Successful – next phase is **T5-T6**.
- Failed - next phase is **T5-E11**.

Remark: An Administration tool must obtain the certificate serial number from the record set, received at **T2-T3** phase. Otherwise, Comodo CAPS will generate an error.

4.4.1.2.6. Phase 6

ID	Type	From	To	Protocol
T5-T6	Initial phase	CCM	SASP	Comodo API

Description: CCM sends to SASP certificate serial number for revocation.

Results:

- Successful – next phase is **T6-T7**.
- Failed - next phase is **T6-E12**.

4.4.1.2.7. Phase 7

ID	Type	From	To	Protocol
T6-T7	Response phase	SASP	CCM	Comodo API
T7-T8	Response phase	CCM	Comodo CAPS	CCM WS

Description: **T6-T7**: CCM receives revocation response.

T7-T8: Comodo CAPS receives revocation response.

Results: next phase is **T8-Z13**

4.4.1.2.8. Phase 8

ID	Type	From	To	Protocol
T8-Z13	Response phase	Comodo CAPS	Administrator	CSRA

Description: **T8-Z13**: An administration tool receives revocation response. It should refresh the displayed list of issued an revoked certificates.

Local actions at T8 time point: Comodo CAPS updates the status of revoked certificate in it's database.

Results: Revocation is complete

4.4.2. Automatic Revocation Process View

Automatic revocation process is illustrated in Figure 6. The legend of this diagram is displayed in Figure 4.

4.4.2.1. List of participants:

- Comodo CA Proxy Server (CA)
- Domain Controller (DC)
- CCM Server
- SASP

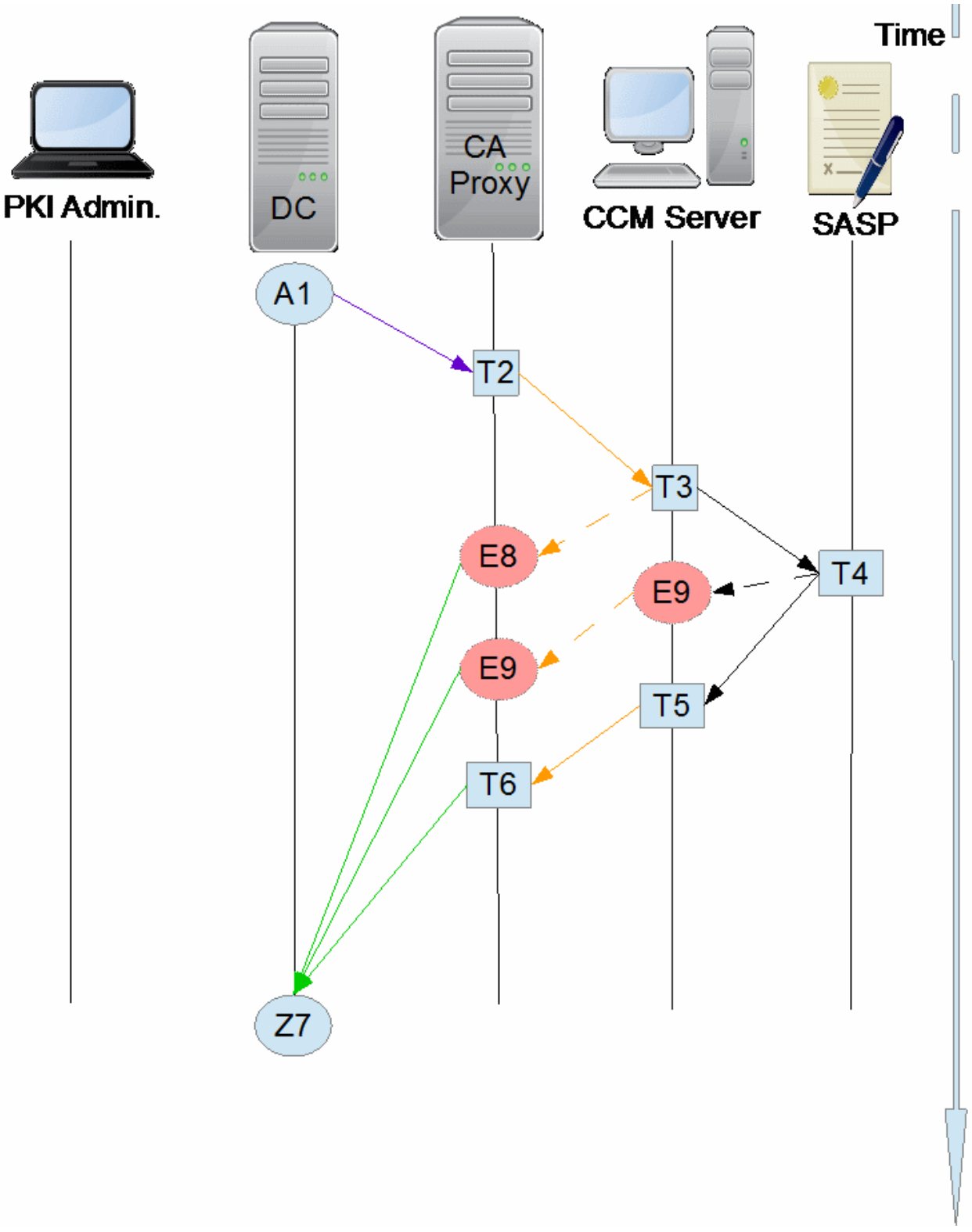

Figure 6. Automatic revocation process view

4.4.2.2. Events and Phases Specification

This specification is time-ordered. It begins from the time point, when the AD user's account is deleted or any attribute is changed. Actually, this event is triggered at DC side by special LDAP search procedure, called by Comodo CAPS. The specification ends with the next session of AD user's account changes lookup.

4.4.2.2.1. Phase 1

ID	Name	Type	Side
A1	Start event	Initial	Administrator's Workstation
Description: This is initial event. It is triggered by DC as a reaction on AD user deletion or user object attributes changing.			

4.4.2.2.2. Phase 2

ID	Type	From	To	Protocol
A1-T2	Initial phase	DC	Comodo CAPS	LDAP
Description: DC picks up a precedent of domain user account deletion or it's attributes changing. After that Comodo CAPS retrieves attributes of corresponding user account from Active Directory. **Local actions at T2 time point**: Comodo CAPS retrieves attributes from local database and compare them with ones from Active Directory. If there are differences or target Active Directory account does not exist then Comodo CAPS will prepare attribute package to revoke all certificates of the user. **Results**: next phase is **T2-T3**. **Remarks**: The person's email change only is not a reason to initiate certificate revocation. This phase does not have Response co-phase (See the section **4.4.3.1.User's attributes that passed to CCM with Certificate revocation data package** for details).				

4.4.2.2.3. Phase 3

ID	Type	From	To	Protocol
T2-T3	Initial phase	Comodo CAPS	CCM	CCM WS
Description: Comodo CAPS sends package with user's account attributes for certificates revocation **Results**: • Successful – next phase is **T2-T3** • Failed - next phase is **T3-E8**				

4.4.2.2.4. Phase 4

ID	Type	From	To	Protocol
T3-T4	Initial phase	CCM	SASP	Comodo API
T4-T5	Response phase	SASP	CCM	Comodo API

Description: CCM interacts with SASP about certificate revocation for corresponding user **Results**: • Successful – next phase is **T5-T6** • Failed - next phase is **T4-E9**				

4.4.2.2.5. Phase 5

ID	Type	From	To	Protocol
T5-T6	Response phase	CCM	Comodo CAPS	CCM WS
Description: CCM returns operation code to Comodo CAPS **Local actions at T6 time point**: If user's account exists in Active Directory, then Comodo CAPS will update account database with new attributes, otherwise corresponding record will be deleted from the database. **Results**: next phase is **T6-Z7**.				

4.4.2.2.6. Phase 6

ID	Type	From	To	Protocol
T6-Z7	Response phase	Comodo CAPS	DC	LDAP
Description: Comodo CAPS set the next lookup session for user's accounts changes at DC **Results**: Revocation is completed. Phases E8-Z7 and E9-Z7 are also initiates the next lookup session. E8 and E9 points can not be interpreted as a reason of automatic revocation process stopping.				

4.4.3. CCM Revocation Specific Details

Specific details related to revocation process are described follow. A manual revocation is performed with a certificate serial number. An automatic revocation is performed with the data from table in the section **4.4.3.1.User's attributes that passed to CCM with Certificate revocation data package**

4.4.3.1. User's Attributes that Passed to CCM with Certificate Revocation Data Package

	Name of the attribute	Can be empty	Remarks
1	First Name	No	The change triggers the revocation
2	Last Name	No	The change triggers the revocation
3	E-mail	No	Identifies the person at CCM side. The change do not triggers the revocation
4	Company	No	RDN=O (Organization Name). The change triggers the revocation
5	Department	Yes	RDN=OU (Organization Unit Name). The change triggers the

			revocation

Remark: When CCM receives new CSR with the attributes package, which includes new e-mail, a new person will be created.

5. Structure of Comodo CAPS

5.1. Comodo CAPS Subsystem Enumeration

Comodo CAPS includes the following subsystems:

- *CA Proxy control system service*
- *Network Interaction subsystem*
  - Certification Enrollment Manager (implements WCCE protocol)
  - Administration Manager (implements CSRA protocol)
- *Revocation Manager*
- *Storage subsystem*
  - CA Proxy Storage Layer (Uses MS Jet Blue Database Engine)
  - Cryptography Layer (Uses MS CryptoAPI)
- *Settings Manager*
- *Java-based Comodo CCM Adaptor*

Figure 7 displays the structure of Comodo CAPS.

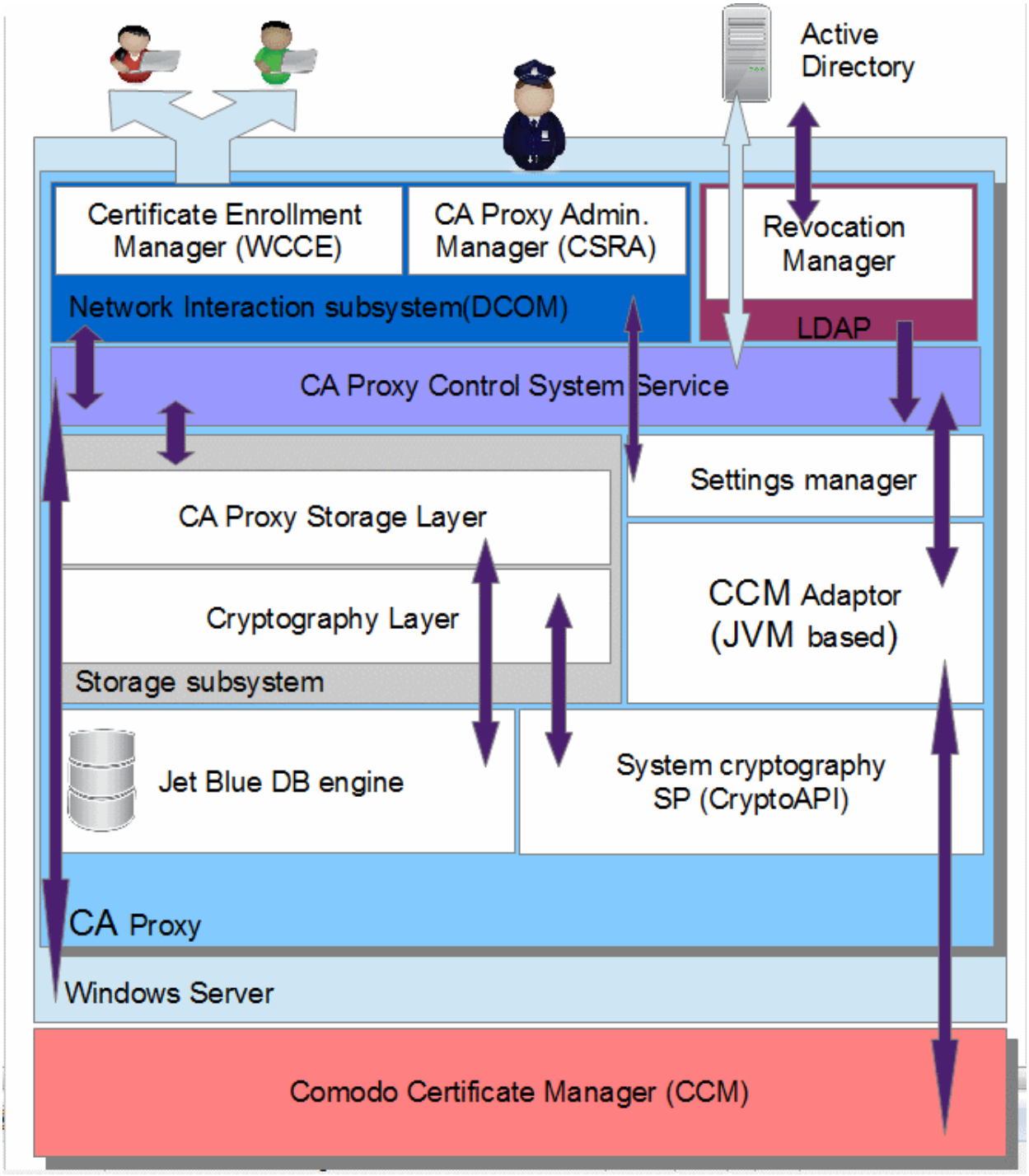

Figure 7. Comodo CAPS structure

5.2. Comodo CAPS Subsystems Description

Actually, Comodo CAPS is a Win32 native program. It runs as Windows Service and managed by Windows Service Control Manager.

5.2.1. CA Proxy Control System Service Description

This subsystem has central role. The Comodo CAPS runtime begins from starting of this subsystem. It is designed to manage other subsystems and provides the following functions:

- *Windows Service Control Manager (SCM) commands handling. SCM is an integral part of Windows. It is started at system boot. It is a remote procedure call (RPC) server. Service configuration and service control programs can start, stop, restart Comodo CAPS locally or remotely using SCM.*

- *Windows Server Manager commands handling (similar to SCM). Server Manager is an administration tool, that eases the task of managing and securing multiple server roles in an enterprise. It is implemented as expanded Microsoft Management Console (MMC).*
- *Management of the following subsystems: Certificate Enrollment Manager, Administration Manager, Revocation Manager, CCM Adaptor. The Java Virtual Machine (JVM) for CCM Adaptor is also managed by this subsystem. This subsystem is also responsible for initiate and properly shutdown the Comodo CAPS certificate database and Windows Certificate*

5.2.2. Network Interaction Subsystem Description

The Network Interaction Subsystem includes Certificate Enrollment Manager and Administration Manager. Both subsystem are developed as implementation of the server role of the corresponding DCOM-based protocol.

5.2.2.1. Certificate Enrollment Manager Description

This subsystem implements the server role of MS-WCCE protocol. It is intended to serve a certification requests of domain forest. Also it manages some Comodo CAPS properties according to MS-WCCE protocol. This subsystem is ready for simultaneous serving of large amount of requests.

5.2.2.2. Administration Manager Description

This subsystem implements the server role of MS-CRSA protocol. It provides functionality of administration to native Windows Server Manager or any third party tools, which can be used for management of Microsoft Certificate Authority role. This functionality includes:

- *Retrieving from the certificate database and transmitting to administration tool information about:*
  - *Pending requests*
  - *Failed requests*
  - *Issued certificates*
  - *Revoked certificates*
  - *Available certificate templates*
- *Retrieving Comodo CAPS properties, which are inherited from native Microsoft CA role*
  - *Setting Comodo CAPS properties*
  - *Manual certificate revocation handling*

5.2.3. Revocation Manager Description

The Revocation Manager runs the separate threads to perform parallel working with Certificate Enrollment Manager and Administration Manager. This subsystem provides the following functionality:

- *Online certificate revocation using AD user objects changes tracking*
- *Postponed certificate revocation using a previously saved accounts information from AD*

Revocation Manager has the special database with information about AD user's accounts. After starting Revocation Manager compares this database content with AD ones. New AD user's accounts are imported. For absent users postponed revocation is performed. To minimize the probability of data loss, the Revocation Manager saves it database in the following cases:

- *Periodically by time*
- *Before Comodo CAPS shutdown*

5.2.4. Storage Subsystem Description

The storage subsystem includes CA Proxy Storage Layer and Cryptography Layer. CA Proxy Storage Layer is abstraction between Comodo CAPS and certificate database. The database usage is not specified by MS-WCCE or MS-CSRA protocols. Microsoft CA implementation uses Extensible Storage Engine, also known as Jet Blue. The runtime code of JET Blue is in ESENT.DLL. This library is present in all versions of operating system since Windows 2000. Currently, Comodo CAPS works with the database of original Microsoft CA. The database contains the following information:

- *Pending, failed and completed certificate requests*
- *Issued and revoked certificates*

Comodo CAPS is able to provide access to existing certificates in the database, issued by Microsoft CA. Also database will be available to Microsoft CA after Comodo CAPS is uninstalled.

5.2.5. CCM Adaptor Description

CCM Adaptor is intended for interaction between CAPS and CCM. It is Java-based part of Comodo CAPS, which implements client role of CCM WS protocol. Comodo CAPS uses Java Native Interface to start internal instance of JVM inside of it's process. Because JVM starts internally, there is no corresponding process of Java executable module (java.exe). CCM Adaptor provides to CAPS the following functions:

- *Certificate enrollment*
- *Certificate revocation*

6. Implementation Details

6.1. Comodo CAPS Binary Module

Currently, Comodo CAPS is designed as **ccm_ca32.exe** Win32 executable module and it runs instead of the original binary module, which located as %SYSTEMROOT%\SYSTEM32\certsrv.exe. The location of **ccm_ca32.exe** is defined by AD Agent home directory (<AD Agent Home>) selected during installation process.

6.2. Revocation Manager Database

The Revocation Manager Database is saved to file <AD Agent Home>\domusr.dat

6.3. Log Files

The log files are saved into <AD Agent Home>\Logs folder. This folder contain the following files:

- *ccm_ca32.log. This log is created by **ccm_ca32.exe** module*
- *agent.log. This log is created by Java-based CCM Adaptor*
- *setup.log. This log is created by AD Agent installer*

The logs *ccm_ca32.log* and *agent.log* can be used for troubleshooting at Active Directory side. To troubleshoot the CCM side, please use *ccm.log, cert.log* and *sasp.log,*located on CCM server.

The log *setup.log* can be used for installation troubleshooting. If Comodo AD Agent is installed properly, this log will be not helpful.

About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767