MIELE PKI

Certificate Policy (CP)

Table of contents

Document control 6
Basic Description 6
Version History 6
Document Review and Signoff 6
Related Documents 7
1. Introduction 8
1.1. Overview 9
1.2. Document Name and Identification 11
1.3. PKI Participants 12
1.3.1. Certification Authorities 12
1.3.2. Registration Authorities 12
1.3.3. Subscribers 12
1.3.4. Relying parties 12
1.3.5. Other participants 12
1.4. Certificate Usage 13
1.4.1. Appropriate certificate uses 14
1.4.2. Restricted certificate uses 14
1.4.3. Prohibited certificate uses 14
1.5. Policy Administration 15
1.5.1. Organization administering the document 15
1.5.2. Contact person 15
1.5.3. Person determining CPS suitability for the policy 15
1.5.4. CPS approval procedures 15
1.6. Definitions and Acronyms 16
2. Publication and Repository Responsibilities 17
2.1. Repositories 17
2.2. Publication of Certification Information 17
2.3. Time or Frequency of Publication 17
2.4. Access Controls on Repositories 17
3. Identification and Authentication 18
3.1. Naming 18
3.1.1. Types of names 18
3.1.2. Need for names to be meaningful 20
3.1.3. Anonymity or pseudonymity of subscribers 20

3.1.4. Rules for interpreting various name forms 20
3.1.5. Uniqueness of names 20
3.1.6. Recognition, authentication, and role of trademarks 20
3.2. Initial Identity Validation 21
3.2.1. Method to prove possession of private key 21
3.2.2. Authentication of organization identity 21
3.2.3. Authentication of individual identity 21
3.2.4. Non-verified subscriber information 21
3.2.5. Validation of authority 21
3.2.6. Criteria for interoperation 21
3.3. Identification and Authentication for Re-key Requests 22
3.3.1. Identification and authentication for routine re-key 22
3.3.2. Identification and authentication for re-key after revocation 22
3.4. Identification and Authentication for Revocation Requests 22
4. Certificate Life-Cycle Operational Requirements 23
4.1. Certificate Application 23
4.1.1. Who can submit a certificate application 23
4.1.2. Enrolment process and responsibilities 23
4.2. Certificate application processing 24
4.2.1. Performing identification and authentication functions 24
4.2.2. Approval or rejection of certificate applications 24
4.2.3. Time to process certificate applications 24
4.3. Certificate Issuance 25
4.3.1. CA actions during certificate issuance 25
4.3.2. Notification to subscriber by the CA of issuance of certificate 25
4.3.3. Certificate Acceptance 25
4.3.4. Conduct constituting certificate acceptance 25
4.3.5. Publication of the certificate by the CA 26
4.3.6. Notification of certificate issuance by the CA to other entities 26
4.4. Key Pair and Certificate Usage 26
4.4.1. Subscriber private key and certificate usage 26
4.4.2. Relying party public key and certificate usage 27
4.5. Certificate Renewal 27
4.5.1. Circumstance for certificate renewal 27
4.5.2. Who may request renewal 27
4.5.3. Processing certificate renewal requests 27
4.5.4. Notification of new certificate issuance to subscriber 27

4.5.5. Conduct constituting acceptance of a renewal certificate....27
4.5.6. Publication of the renewal certificate by the CA....28
4.5.7. Notification of certificate issuance by the CA to other entities....28
4.6. Certificate Re-key....28
4.6.1. Circumstance for certificate re-key....28
4.6.2. Who may request certification of a new public key....28
4.6.3. Processing certificate re-keying requests....28
4.6.4. Notification of new certificate issuance to subscriber....28
4.6.5. Conduct constituting acceptance of a re-keyed certificate....28
4.6.6. Publication of the re-keyed certificate by the CA....28
4.6.7. Notification of certificate issuance by the CA to other entities....28
4.7. Certificate Modification....28
4.7.1. Circumstance for Certificate Modification....29
4.7.2. Who may request certificate modification....29
4.7.3. Processing certificate modification requests....29
4.7.4. Notification of new certificate issuance to subscriber....29
4.7.5. Conduct constituting acceptance of modified certificate....29
4.7.6. Publication of the modified certificate by the CA....29
4.7.7. Notification of certificate issuance by the CA to other entities....29
4.8. Certificate Revocation and Suspension....30
4.8.1. Circumstances for revocation....30
4.8.2. Who can request revocation....30
4.8.3. Procedure for revocation request....30
4.8.4. Revocation request grace period....30
4.8.5. Time within which CA must process the revocation request....30
4.8.6. Revocation checking requirement for relying parties....31
4.8.7. CRL issuance frequency....31
4.8.8. Maximum latency for CRLs....31
4.8.9. On-line revocation/status checking availability....32
4.8.10. On-line revocation checking requirements....32
4.8.11. Other forms of revocation advertisements available....32
4.8.12. Special requirements key compromise....32
4.8.13. Circumstances for suspension....32
4.8.14. Who can request suspension....32
4.8.15. Procedure for suspension request....32
4.8.16. Effect of a suspension....32
4.8.17. Limits on suspension period....32

4.9. Certificate Status Services....33
4.9.1. Operational characteristics....33
4.9.2. Service availability....33
4.9.3. Optional features....33
4.10. End of Subscription....33
4.11. Key Escrow and Recovery (Optional)....33
4.11.1. Key escrow and recovery policy and practices....33
4.11.2. Session key encapsulation and recovery policy and practices....33

Document control

Basic Description

Document title	Miele PKI Certificate Policy (CP)
Topic	Certificate Policy for the Miele PKI Service based on RFC 3647
Version	1.0
Status	Final draft for discussion
Document OID	1.3.6.1.4.1.44739.509.1.20.20.1
Supersedes Document	-
Author	Dr. Dieter Krug
Miele responsible contact	Dr. Dieter Krug

Version History

Version	Version Date	Comment
0.1	15.04.2015	Initial Draft
0.2	21.04.2015	Extensions in section 2 and 3
0.3	28.04.2015	Extensions in section 4
0.4	06.05.2015	Review and extensions in section 4
0.9	29.05.2015	Final Draft
1.0	22.06.2015	Final Version after minor changes

Document Review and Signoff

Version	Version Date	Reviewer Name	Signoff Date
1.0	22.06.2015	Dr. Dieter Krug	

Related Documents

Document title	**Miele PKI Certification Practice Statement (CPS)**
Document Name	Miele PKI CPS v1.0.pdf
Description	Certification Practice Statement for the Miele PKI Service
Document OID	1.3.6.1.4.1.44739.509.1.20.20.2
Latest available version	v1.0
Last changed	22.06.2015

Document title	**Miele PKI Certificate Profiles**
Document Name	Miele PKI Certificate Profiles RFC 5280 v1.0.pdf
Description	RFC5280 Certificate Profiles for Miele PKI
Latest available version	v1.0
Last changed	14.04.2015

Document title	**Miele PKI Trust Chain Overview**
Document Name	Miele PKI Trust Chain Overview v1.0.pdf
Description	Trust Chain Overview for Miele PKI Hierarchy
Latest available version	v1.0
Last changed	15.04.2015

Document title	**Miele PKI IANA PEN Namespace**
Document Name	Miele PKI IANA PEN Namespace v1.0.pdf
Description	Overview of the Miele PKI related IANA PEN Namespace
Latest available version	v1.0
Last changed	15.04.2015

1. Introduction

The X.509 standard defines a **Certificate Policy (CP)** as "a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements". An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

This certificate policy document describes the policies of the Certification Authorities (CAs) operated by Miele & Cie. KG. It is applicable to all entities that have relationships with the Miele PKI CAs by consuming respective certificates, including end users-, cross-certified CAs, and Registration Authorities (RAs). This Certificate Policy document provides those entities with a clear statement of the policies and responsibilities of the Miele PKI and its CAs, as well as the responsibilities of each entity in dealing with Miele PKI CAs.

The Certificate Policy (CP) helps the user of certification services to determine the level of trust that he can put in the certificates that are issued by the Miele PKI CAs. The existence of policies is critical when dealing with a reliable PKI or certification services.

The Miele PKI certification service is only as trustworthy as the procedures contained and operated in it. The Miele PKI Certificate Policy therefore covers all relevant preconditions, regulations, processes and measures within the Miele PKI certification service as a compact information source for current and potential participants.

This document will rely on other parts of the general Miele PKI certification service documentation and will sum up that information that is of importance for the participating PKI users. Other related documentation is referenced in this Certificate Policy document where relevant while an overview of other documents is listed in the document control section.

It should be provided for free and publicly accessible to any Miele PKI user.

1.1. Overview

The Miele & Cie. KG PKI (Miele PKI) in general consists of a two-tier CA hierarchy trust chain, terminating in a trusted Root Authority ("Miele Root CA 01"). The Root CA and two subordinate CAs define the CA hierarchy, while the subordinate certification authorities are implemented to issue different types of end-entity certificates. While the first subordinate CA ("Miele Sub CA 01") is intended to issue machine oriented certificates, the second subordinate CA ("Miele Sub CA 02") is planned to issue user based certificates. The current level of implementation is focused on machine certificates only, while "Miele Sub CA 02" was already built for future use.

All CA certificates and respective keys are protected using Hardware Security Modules to implement an additional layer of security and to protect the CA's keys. In addition, the Root CA is implemented using a physical isolated and offline server in combination with a multi-eye principle based key authorization mechanism from the HSM requiring k/n authorization for key access.

All installed components, especially the CAs are reduced to a minimal level of installed components to provide additional security while different components and roles are installed on separate servers in the infrastructure as required from a functional perspective.

The whole trust chain is built for a corporate Miele use-case implementing up to date key length and algorithms. This includes deprecation of older algorithms like "SHA-1" and intentionally implementing large key sizes and up to date hashing algorithms while security was decided to be more important than backward compatibility with older cryptographic implementations. This may lead to certain issues with older cryptographic implementations and application consuming certificates from the Miele PKI which once discovered in turn need to be resolved on the application side by upgrading consuming applications and operating systems.

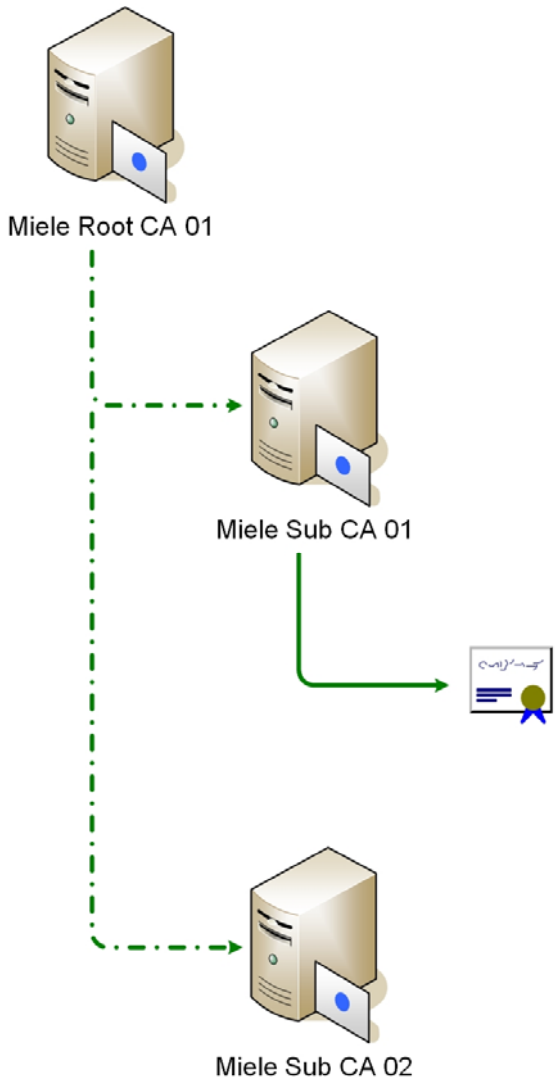
As the primary information source for Miele PKI is hosted on a load balancer enabled web server infrastructure, CRLs, CA certificates and the current versions of the CP and CPS documents are also located on these web servers while the main references to revocation and authority information are implemented using HTTP based location information and URLs. In addition to the CRL based revocation information Miele PKI is also supporting the OCSP protocol (RFC 5019, a profile of the Online Certificate Status Protocol (OCSP) outlined in RFC 2560) based on the current CRL information from authoritative subordinate CAs for OCSP aware PKI clients.

Besides several additional infrastructure components four high-available web site clusters using load balancer infrastructure exist as part of the Miele PKI for all related HTTP based locations and references including the OCSP responder service. Two high-available web clusters (one for CRL, one for OCSP) are implemented to support internal network Miele clients and servers, while two web clusters are dedicated to external traffic providing identical services as the two internal facing web clusters. The external facing web clusters are protected by an application layer gateway infrastructure to provide additional security measures and to enforce protocol compliance of incoming requests.

Miele PKI implementation

The following section is a brief overview of the implemented Miele PKI trust chain model and the CA hierarchy for the Miele trust chain including the Miele PKI certification services provided by this architecture.

Overview of the Miele PKI trust chain:



CA Name	: Miele Root CA 01, O=Miele, C=DE
CA Role	: Certification of Miele PKI Sub CAs
Keylength	: 4096 Bit RSA, SHA-256
Lifetime	: 20 Years
CRL Lifetime	: 3 Months, 1 Months Overlap
CRL Publishing	: offline / manual CRL Publishing
Key Security	: Network HSM, multi-eye principle authorization
Instance type	: physical
Status	: offline
Availability	: cold standby

CA Name	: Miele Sub CA 01, O=Miele, C=DE
CA Role	: Issuance of Machine based End Entity Certificates
Keylength	: 4096 Bit RSA, SHA-256
Lifetime	: 10 Years
CRL Lifetime	: 5 Days, 3 Days Overlap
CRL+ Lifetime	: 8 Hours, 4 Hours Overlap
CRL Publishing	: Online CRL Publishing
Key Security	: Network HSM, Module Protection
Instance type	: VM
Status	: online
Availability	: Hyper-V Replica with Microsoft DPM backup

Keylength	: 2048 Bit RSA, SHA-256
Lifetime	: 2 Years (Max.)
Key Security	: Software protected storage for machine based certificates

CA Name	: Miele Sub CA 02, O=Miele, C=DE
CA Role	: Issuance of User based End Entity Certificates
Keylength	: 4096 Bit RSA, SHA-256
Lifetime	: 10 Years
CRL Lifetime	: 5 Days, 3 Days Overlap
CRL+ Lifetime	: 8 Hours, 4 Hours Overlap
CRL Publishing	: Online CRL Publishing
Key Security	: Network HSM, Module Protection
Instance type	: VM
Status	: online
Availability	: Hyper-V Replica with Microsoft DPM backup

1.2. Document Name and Identification

This CP is called "**Miele PKI Certificate Policy**" and has its own Object Identifier. For details please refer to the Miele PKI IANA PEN namespace document outlined in the related documents section.

X.509 OID – Miele PKI

1.3.6.1.4.1.44739.**509** Base of the Miele PKI Namespace

X.509 OID – Miele PKI Class identifier

1.3.6.1.4.1.44739.509.**1** Base of the Miele PKI trust chain namespace

X.509 OID –Environment

1.3.6.1.4.1.44739.509.1.**20** Base of the Miele PKI production environment

X.509 OID – Issuance Policy namespace

1.3.6.1.4.1.44739.509.1.20.**10** Base of the Miele PKI issuance policy reference

X.509 OID – Issuance Policy identifiers

1.3.6.1.4.1.44739.509.1.20.10.**1** MielePKI issuance policy reference

X.509 OID – PKI Policy:

1.3.6.1.4.1.44739.509.1.20.**20** Base of the Miele PKI documents namespace

X.509 OID – Current CP documentation:

1.3.6.1.4.1.44739.509.1.20.20.**1** Miele PKI Certificate Policy v1.0

X.509 OID – Current CPS documentation:

1.3.6.1.4.1.44739.509.1.20.20.**2** Miele PKI Certification Practice Statement v1.0

Along with other documentation CP and CPS document locations are accessible to Miele PKI certification service participants at http://www.pki.miele.com

1.3. PKI Participants

1.3.1. Certification Authorities

Miele & Cie. KG operates a two-tier CA hierarchy which issues machine in its current mode of operation and user certificates in the future to Miele employees and Miele partners.

The two-tier CA hierarchy is built upon:

- an offline “Miele Root CA 01”
- two subordinate issuing CAs with functional differentiation for user and machine-based certificates: “Miele Sub CA 01”, “Miele Sub CA 02”

The certificate services hierarchy is implemented in the Miele LDAP directory hierarchy in the root domain. Physically, the offline Root and the respective two issuing CAs and all other PKI related infrastructure services are located in the Miele Data Centers at Gütersloh, Germany.

1.3.2. Registration Authorities

Miele PKI Registration Authority (RA) is an integral function of Miele PKI with online access to the Certificate Authority. The Miele PKI RA allows initiating a certificate request to the CA. For online requests only Miele LDAP directory authorized objects are allowed to request for issuance of certificates. Offline requests for manually enrolled certificates following different subject naming schemes or enrollment requests for LDAP directory integrated systems are issued with manual validation by authorized personal before issuance. User authorization is granted by Miele identity and access management process, the Registration Authority console is the interface which is provided by the Miele PKI certificate management solution based on the existing Miele identity management processes.

Machine authorization is granted by the Miele hardware / software deployment process while automated machine based certificate enrolment is controlled by LDAP directory service and respective permissions.

1.3.3. Subscribers

Possible end-entities in this PKI include Miele employees, computers, network devices and respective identities and machines of approved Miele partners. All end-entities are certified by the Miele PKI certification authorities and as such are certificate subscribers. In the current mode of operation only machine based certificates using automated or manual enrollment mechanisms are issued.

The subscriber holds a private key that corresponds to the public key listed in that certificate. Subscribers of the Miele PKI are internal machines, users and approved partners with their respective machines and users according to Miele identity management and security policy.

1.3.4. Relying parties

A relying party is any entity who relies upon a certificate that is issued by an Issuing CA or Root CA and that is used in a manner consistent with this CP. A relying party could be within or outside the organization of Miele & Cie. KG. For instance a Web Client that checks the validity of a Web Server certificate within the Miele organization or in terms of secure email, using the recipient certificate for encrypting emails to the recipient. Relying parties implicitly agree to the terms of this CP documentation, the CPS documentation and referenced general Miele security policies in their respective latest version.

1.3.5. Other participants

Not applicable

1.4. Certificate Usage

The use and protection of keys and certificates will be on the sole responsibility of each subscriber and relying party.

Miele Trust Chain

Certificates issued by Miele Root CA 01

Certificate Name Type	Purpose of issued certificate
Subordinate Certification Authority	Issue certificates for Miele PKI subordinate certification authorities.

Certificates issued by Miele Sub CA 01

Certificate Name Type	Purpose of issued certificate
Miele Server Authentication	Server Authentication
Miele Webserver Authentication	Webserver Authentication
Miele Domain Controller Authentication	Domain Controller Authentication
Miele Client Authentication	Client Authentication
Miele SCOM Gateway Authentication	Mutual Gateway Authentication
Miele OCSP Response Signing	OCSP Response Signing

Certificates issued by Miele Sub CA 02

Certificate Name Type	Purpose of issued certificate
Miele OCSP Response Signing	OCSP Response Signing

For further details please refer to the RFC5280 certificate profile document outlined in the related documents section which is available upon request.

1.4.1. Appropriate certificate uses

All certificates issued by the Miele PKI are used for Miele internal business purposes by Miele internal employees and approved Miele partners only.

Miele PKI machine certificates may only be used for authentication purposes and to ensure the confidentiality of communication channels.

In addition Miele has defined certificate trust levels for different trust and security categories of issued end-entity certificates. These levels are defined and based upon security and technical requirements for the use and trust of different certificates. Further details are outlined in the Miele Certification Practice Statement referenced in the related documents section.

1.4.2. Restricted certificate uses

The Miele PKI is primarily for internal use and trust is not validated by any mutual third-party. Partners and other external entities should not assume any higher level of trust than assigned internally within Miele & Cie. KG.

1.4.3. Prohibited certificate uses

Generally, any usage not covered in sections 1.4. Certificate Usage, 1.4.1 “Appropriate certificate uses” and 1.4.2 “Restricted certificate uses”. The following use is explicitly prohibited:

- use of subscriber end entity certificates as CA certificates
- use of subscriber end-entity certificates for different purposes other than outlined in the certification request.
- use of subscriber end-entity certificates outside of their given validity period
- use of subscriber end-entity certificates after revocation by the Miele PKI
- use of machine certificates on non-Miele and on non-certified partner machines and devices
- use of certificates for non-Miele internal and partner purposes

1.5. Policy Administration

1.5.1. Organization administering the document

This Certificate Policy is administered by the Miele PKI Security Governance Team represented by the named contact outlined in section 1.5.2.

1.5.2. Contact person

Miele & Cie. KG
Dr. Dieter Krug
Carl-Miele-Straße 29
33325 Gütersloh
Germany

Voice: +49 52 41-89-28 28
Fax: +49 52 41-89-28 28
Email: hotline@miele.com
Web: http://www.pki.miele.com

1.5.3. Person determining CPS suitability for the policy

see 1.5.2 Contact person.

1.5.4. CPS approval procedures

Miele & Cie. KG Director Compliance/Security approved this document prior to publication. This document is regularly re - evaluated.

1.6. Definitions and Acronyms

Certificate (public key certificate)

A data structure containing the public key of an electronic identity and additional information. A certificate is digitally signed using the private key of the issuing CA binding the subject's identity to the respective public key.

Certificate Policy (CP)

A document containing the rules that indicate the applicability and use of certificates issued to Miele PKI subscribers

Certification Practices Statement (CPS)

A document containing the practices that Miele PKI certification authority employs in issuing certificates and maintaining PKI related operational status.

Certification Authority (CA)

The unit within Miele PKI to create, assign and revoke public key certificates.

Directory

A database containing information and data related to identities, certificates and CAs.

End-Entity

An entity that is a subscriber, a relying party, or both.

Public Key Infrastructure (PKI)

Framework of technical components and related organizational processes for the distribution and management of private keys, public keys and corresponding certificates.

Registration Authority (RA)

An entity that is responsible for the identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is the delegate of certain tasks on behalf of a CA).

A Registration Authority (RA) could provide the following functions:

- proving identity of certificate applicants
- approve or reject certificate applications
- process subscriber requests to revoke their certificates

Relying Party

A recipient of a certificate issued by an Miele PKI CA who relies on the certificate, the respective Miele PKI trust chain and its corresponding policies.

Subscriber

A person or a machine that is the subject named or identified in a certificate and holds the private key that corresponds to the associated certificate. In particular and besides several other use cases, LDAP directory member machines are the most common Miele PKI subscribers.

2. Publication and Repository Responsibilities

2.1. Repositories

The central repository for the Miele PKI CAs is provided by an LDAP directory. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 3, as specified in Internet RFC 4510.

For availability reasons and to ease access to specific information, such as CP / CPS documentation and certificate based references, an alternate repository is provided (Miele PKI Web site located at http://www.pki.miele.com . The protocol used to access the Miele PKI site and certificate based references is HTTP.

2.2. Publication of Certification Information

The Miele PKI publishes information regarding its PKI services (CRLs and CA certificates) except CP and CPS to both locations listed in 2.1. CP and CPS documentation is published to the Miele PKI web site only.

Miele PKI end-entity certificates may be published in the central repositories depending on appropriate end-entity certificate purposes according to certificate profiles in their most current version.

2.3. Time or Frequency of Publication

Minor updates of the Miele PKI CP and CPS documents may be published once a year. Critical changes of Miele PKI CP and CPS documents are published immediately.

CRLs and CA certificates are published using a defined schedule. For details please refer to chapter “CRL issuance frequency” regarding CRLs and chapter “Circumstance for certificate modification” for CA certificates.

2.4. Access Controls on Repositories

All information published on the Miele PKI web site is read-accessible Miele internally and anonymously from the Internet (CRTs, CRLs, CP and CPS). Additionally an OCSP service is accessible Miele internally and anonymously from the Internet. Miele has set logical and physical security controls to restrict modifying (including adding and deleting) repository entries to authorized staff only. The Miele LDAP directory repository is limited to Miele internal certificate subscribers and trusted relying parties who have a valid Miele LDAP directory account. Access to this repository is controlled by appropriate LDAP directory permissions and is based on the Miele identity and access management policies.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

Miele Trust Chain

CA certificate naming of the **Miele Root CA 01**

Attribute	Value
Subject Name	CN = Miele Root CA 01 O = Miele C = DE
Subject Alternative Name	None

CA certificate naming of the **Miele Sub CA 01**

Attribute	Value
Subject Name	CN = Miele Sub CA 01 O = Miele C = DE
Subject Alternative Name	None

CA certificate naming of the **Miele Sub CA 02**

Attribute	Value
Subject Name	CN = Miele Sub CA 02 O = Miele C = DE
Subject Alternative Name	None

Subscriber certificate naming of **Miele Domain Controller Authentication**

Attribute	Value	
Subject Name	CN =	<Domain Controller FQDN>
Subject Alternative Name (DNS)		<Domain Controller FQDN> <Domain DNS Name> <Domain NetBios Shortname>

Subscriber certificate naming of **Miele Server Authentication**

Attribute	Value	
Subject Name	CN =	<Server FQDN / HTTP Host Header>
Subject Alternative Name (DNS)		<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **Miele Webserver Authentication**

Attribute	Value	
Subject Name	CN =	<Server FQDN / HTTP Host Header>
Subject Alternative Name (DNS)		<Multiple Server FQDN / HTTP Host Header / Domain Names>

Subscriber certificate naming of **Miele Client Authentication**

Attribute	Value	
Subject Name	CN =	<Client FQDN>
Subject Alternative Name (DNS)		<Client FQDN>

Subscriber certificate naming of **Miele SCOM Gateway Authentication**

Attribute	Value	
Subject Name	CN =	<Gateway Server FQDN>
Subject Alternative Name (DNS)		<Gateway Server FQDN>

Subscriber certificate naming of **Miele OCSP Response Signing**

Attribute	Value	
Subject Name	CN =	<OCSP Responder FQDN>
Subject Alternative Name (DNS)		<OCSP Responder FQDN>

3.1.2. Need for names to be meaningful

The semantics of the names used is commonly understood; therefore the identity of the subjects can be determined. User names and all machine names must exactly match the entries in the forms supplied at the time of the subscriber's registration and certificate enrolment.

3.1.3. Anonymity or pseudonymity of subscribers

Certificate subscribers cannot be anonymous, but are allowed to use pseudonymous unique names and aliases as long as these names are unique throughout the whole Miele internal namespace / network while pseudonym and alternative names need to be matched to a responsible administrative contact / person during the registration process.

3.1.4. Rules for interpreting various name forms

- Distinguished Names follow the X.500 naming context as well as RFC 2247
- Distinguished Names represent the LDAP naming context referring to RFC 2247

3.1.5. Uniqueness of names

The subject name and subject alternative names of certificates must be unique except for environments with technical requirements to have multiple certificates issued with the same name due to high availability implementations.

3.1.6. Recognition, authentication, and role of trademarks

No trademarks will be knowingly used. An explicit check of any name will not be conducted, as all names will only be used by Miele internally and approved business partners and not published on any open sources.

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

The certificate applicant's possession of a private key is proved through the use of a digitally signed PKCS#10 or CMC certificate request. This request is signed with the corresponding private key of the certificate subscriber.

3.2.2. Authentication of organization identity

Not applicable.

3.2.3. Authentication of individual identity

Depending on the corresponding certificate type, certificates may be requested automatically via auto-enrollment or manual enrollment (online or offline) via Miele PKI certificate enrollment process implemented by the certificate management portal. For details please refer to chapter "Certificate Application"

Certificate requests are restricted to Miele PKI and approved Miele partner subscribers with a valid machine or user account in the Miele LDAP directory or to IT staff enrolling on behalf of registered corporate or approved partner hardware and devices. Certificates for machine subscribers requested online or offline via Miele PKI certificate enrollment process can only be requested by users with a valid LDAP directory user account.

Authentication is performed by

(1) a successful logon to the Miele LDAP directory

or

(2) a valid corporate Miele email address and additional information to verify the requestor during the enrolment and approval process.

or

(3) on behalf of an approved partner user or devices by authorized Miele internal staff

3.2.4. Non-verified subscriber information

Any enrollment request that holds non verifiable information and / or information that cannot be validated as a valid Miele contact responsible for enrollment of the corresponding end-entity certificate is discarded without any further notice.

3.2.5. Validation of authority

Enrollment requests containing alias names or pseudonyms need to be validated to a responsible administrative contact in charge for the end-entity machine or device that requests certification during the enrollment process. Change of responsibility or role of the respective administrative contact while the Miele PKI end-entity certificate is still in use need to be communicated without prior notice to the responsible Miele PKI certificate and enrollment authority. Unless the machine or device is considered "End of Life" and is to be decommissioned a new administrative contact taking up the responsibilities of the former administrative contact is mandatory. This especially applies to virtual machines and is not limited to physical hardware.

3.2.6. Criteria for interoperation

Not applicable

3.3. Identification and Authentication for Re-key Requests

It is necessary for a subscriber to obtain a new certificate before his certificate expires. Otherwise the continued use of certificates may be disrupted and a new initial enrolment request needs to be created. Miele PKI in the current state of implementation and offered end-entity certificates always requires that a new key pair is generated for the subscriber to replace the expiring key pair.

3.3.1. Identification and authentication for routine re-key

Certificates issued via auto enrollment

Routine re-keying for auto-enrolled certificates is performed automatically, prior certificate expiration within the certificate renewal period. Subscribers are identified and authenticated for the automatic re-keying process by the LDAP directory and corresponding permissions. A re-key request contains the new key is signed using the current valid key.

Certificates requested manually online or offline via Miele PKI certificate management process

Routine re-keying for certificates requested online or offline via Miele PKI certificate management process is performed manually prior to certificate expiration within the certificate renewal period.

Users are identified and authenticated for the controlled re-keying process by

(1) a successful logon to the Miele LDAP directory

or

(2) a valid corporate Miele email address and additional information verifying the requestor.

A re-key request must contain the new key and is signed using the current valid key. Failure to conduct a routine re-keying process before expiration of the existing certificate requires a new initial enrolment request to be created.

3.3.2. Identification and authentication for re-key after revocation

A re-key request after revocation is performed by using the same process as the initial enrollment and identity validation procedures which is basically an initial certificate enrollment request.

3.4. Identification and Authentication for Revocation Requests

In order to avoid delay in disabling compromised credentials, temporary revocation requests can be raised by any Miele employee with minimal validation requirements (e.g. known telephone number, known email address or personal knowledge). Any temporary revocation request will trigger a process to either permanently invoke or cancel the revocation which includes appropriate identification and authentication mechanisms.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

Certificates are requested manually via the Miele PKI built-in operating system mechanisms and respective Miele PKI processes. These end-entity certificates require an initial application form for every device or machine including administrative contact information and proof of authorization that the requesting administrative contact maintains and manages the system the requested end-entity certificate is to be enrolled for on administrative behalf.

Certificate requests in an automatic enrollment scenario are managed based on the existing Miele identity and access management processes and requires prior machine or device registration and appropriate permissions in the Miele LDAP directory.

This procedure especially applies to requests for

- Miele Domain Controller Authentication
- Miele Server Authentication
- Miele Client Authentication
- Miele OCSP Response Signing

certificates.

4.1.1. Who can submit a certificate application

Miele employees and approved partners of Miele can submit a certificate application. A valid Miele LDAP directory user account and appropriate authorization according to the applicants' role is required.

For every system or device within Miele a named administrative contact is appointed and authorized to request an appropriate certificate. The respective administrative contact role and authorization for administrative request on behalf is validated during the enrollment and validation process.

In an automatic enrollment scenario only an initial administrative contact initiated enrollment request using the Miele standard device registration processes of the corresponding device or machine is required. Certificates of this type are controlled by the Miele PKI operations staff in combination with automatic enrollment mechanisms; therefore no dedicated request is required for single certificates.

4.1.2. Enrolment process and responsibilities

<u>Enrollment process</u>

- Domain Controller Authentication certificates to machine subscribers are enrolled automatically via Active Directory Group Policies.
- OCSP Responder certificates to machine subscribers are enrolled automatically via OCSP responder machine and OCSP responder array configuration.
- Server Authentication certificates to machine subscribers are enrolled automatically via Active Directory Group Policies.
- Client Authentication certificates to machine subscribers are enrolled automatically via Active Directory Group Policies.

- Webserver Authentication certificates to machine subscribers are enrolled manually according Miele PKI certificate enrollment processes and procedures in combination with the administrative contact that generates a certificate signing request for a Miele internal machine
- Gateway Authentication certificates to machine subscribers are enrolled manually according Miele PKI certificate enrollment processes and procedures in combination with the administrative contact that generates a certificate signing request for a Miele internal machine

Responsibilities

Miele PKI operations staff is responsible for successful enrollment of all auto-enrolled certificates. The administrative contact of each system is responsible for correct and appropriate use of the enrolled certificate based on the Miele PKI certificate policies.

For manually enrolled certificate types the administrative contact as the certificate requestor on behalf is responsible for successful enrollment and use after successful issuance of the respective certificate according to the existing Miele PKI certificate policies.

4.2. Certificate application processing

Applications for certificates are part of the standard Miele IT change management process while respective Miele change management policies and regulations apply.

4.2.1. Performing identification and authentication functions

Identification and authentication is performed by the Miele LDAP directory. All requesting entities require a valid LDAP directory account for authentication or an appropriate administrative contact LDAP directory account is required for enrollment on behalf of non-LDAP directory integrated devices.

4.2.2. Approval or rejection of certificate applications

For every system within Miele a named administrative contact is appointed and authorized to approve or reject a certification application.

For auto-enrolled certificates only initial administrative contact approval of the corresponding device or machine is required. Certificates of this type are controlled and approved by the Miele PKI operations staff, therefore no dedicated approval or rejection is required for single certificates.

For manually enrolled certificate types the administrative contact as the certificate requestor is responsible for successful enrollment and use after successful issuance of the respective certificate according to the existing Miele PKI certificate policies. The Miele PKI operations team is responsible for enrollment requests to match to existing certificate policies and that certificate enrollment for machines is conducted by authorized administrative contact only.

4.2.3. Time to process certificate applications

Certificate requests for existing certificate templates including a defined enrollment process will be processed according to the respective Miele IT change management service level agreement.

Requests for new certificate types will be processed on a best effort basis.

4.3. Certificate Issuance

Certificates requested manually (online or offline) in an administrative contact based "enroll on behalf" scenario are issued by the certificate management portal (see 4.1.2 Enrolment process and responsibilities for details). In all other cases, certificate issuance is performed automatically based on the configuration settings in the Miele LDAP directory.

A certificate which is requested manually (online or offline) is created and issued following the approval of a certificate application. Miele PKI creates and issues a certificate based on the information given in the approved certificate application in connection with Miele internal repositories to validate authorization and administrative responsibility for the desired system.

4.3.1. CA actions during certificate issuance

Before issuing certificates to Miele PKI subscribers, the following procedures are performed by the Miele PKI Issuing CAs or Miele PKI operations staff:

- Check the certificate request for alignment to Miele PKI CP and CPS
- Check the requestors permissions and role to request a certificate for the desired end- entity certificate template
- For manual requests check the requestor to match to the administrative contact role for the desired system
- Store subscribers' certificate request in the CA database
- Issuance of subscriber certificates
- Store subscribers' certificate in the CA database

4.3.2. Notification to subscriber by the CA of issuance of certificate

The certificate subscriber is notified for successful issuance. In case of an administrative contact based "enroll on behalf" scenario and machine based certificate subscribers, the related administrative contact responsible for the service or application is notified. Notification does not apply to automatically enrolled certificate subscribers.

4.3.3. Certificate Acceptance

4.3.4. Conduct constituting certificate acceptance

Based on the current mode of operation of the Miele PKI, certificate requests and certificate acceptance is only constituted for machine based certificates in automatic enrollment or manual "enroll on behalf" scenarios only.

Manual enrolled machine certificates

After receiving the certificate, the administrative contact responsible for the service or application the certificate was requested on behalf has to verify the certificates. If the certificate contains invalid information or if the key or the certificate is faulty, the administrative contact has to notify the Miele PKI operations staff immediately. In case of proper keys and certificates, a certificate acceptance is constituted implicitly.

All auto-enrolled machine certificates

After successful automatic certificate enrollment on the requesting machine a certificate acceptance is constituted.

4.3.5. Publication of the certificate by the CA

The certificates of Miele PKI certification authorities are published in the Miele LDAP directory and on the Miele PKI website:

- Miele Root CA 01 certificates (current and renewed CA certificate)
- Miele Sub CA 01 certificates (current and renewed CA certificate)
- Miele Sub CA 02 certificates (current and renewed CA certificate)

Miele PKI end-entity certificates may be published in the central repositories depending on appropriate end-entity purposes according to certificate profiles in their most current version and / or technical requirements depending on the desired use case.

4.3.6. Notification of certificate issuance by the CA to other entities

Notification of other entities is not supported.

4.4. Key Pair and Certificate Usage

4.4.1. Subscriber private key and certificate usage

The Miele *"Information Security Policies"* (cf. directives 1186, 1187 and 1188) contain the general security obligations which apply to all users. These guidelines can be found on the Miele intranet website "Miele-Veröffentlichungen".

Furthermore, subscribers are required

- to provide complete and accurate information on their certificate applications
- to use the issued certificate in accordance with "1.4. Certificate Usage"
- to protect the respective private key material according to Miele Information Security Policies in combination with technical requirements for the respective certificate type
- to discontinue using the private key material at the end of the key usage period
- not intentionally compromise the Miele PKI security measures and neither disrupt or interfere with the Miele PKI certification services and / or bypass existing policies or security measures
- not to duplicate or transmit key material unauthorized
- to enforce revocation checking, certificate lifetime and chain validation wherever possible and appropriate according to the respective certificate type.

In case of a discovered or believed private key compromise or violation of any other requirements mentioned above and connected Miele security policies, the subscriber must immediately notify Miele IT Helpdesk, request certificate revocation, discontinue any further use and take appropriate measures in connection with Miele PKI and IT Security processes to mitigate any security risk arising from key compromise.

4.4.2. Relying party public key and certificate usage

Relying parties must assess if a given certificate is appropriate for the specific purpose. In particular they must verify that a certificate is used in accordance with "1.4. Certificate Usage".

Certificates may only be relied upon if the following verification steps are successful

- Identifying a certificate chain up to the trusted Miele Root CA 01 including its' subordinate CAs
- Verifying the certificate chain and end-entity certificates, including
    - validation of each digital signature
    - all certificate extensions including key usage and extended key usage extension matching to the appropriate and approved purposes
    - validation of validity period
    - conduct certificate revocation checking either by CRL or OCSP while systems supporting OCSP should prefer OCSP as the primary method for revocation checking and may fall back to CRL if the OCSP responder service is unavailable. This fall back method does not apply to an OCSP responder stating the certificate as invalid.

Relying parties may not compromise the Miele PKI security measures, policies and verification steps and neither disrupt or interfere with Miele PKI certification services. In case of any security violation the relying parties must discontinue any further usage and notify Miele helpdesk immediately and apply countermeasures as advised by Miele PKI operations team without question or delay.

4.5. Certificate Renewal

Certificate renewal is the process whereby a new Certificate with an updated validity period is created for an existing Key Pair.

As a general matter, Miele PKI does not support Certificate renewal. Whenever a Miele PKI Certificate expires, the Subscriber is required to generate a new Key Pair and request a new Certificate (i.e.,) in accordance with the Miele CP / CPS requirements.

4.5.1. Circumstance for certificate renewal

Not applicable.

4.5.2. Who may request renewal

Not applicable.

4.5.3. Processing certificate renewal requests

Not applicable.

4.5.4. Notification of new certificate issuance to subscriber

Not applicable.

4.5.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.5.6. Publication of the renewal certificate by the CA

Not applicable.

4.5.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.6. Certificate Re-key

Certificate re-key means to extend the certificate lifetime including generation of a new key pair. Certificate re-key with a new generated key pair is recommended from a security perspective because the key pair will change for each certificate renewal, but certificate re-keying does not support modification in certificate information such as key-length, hash- and signature algorithm. For future PKI operation this would be a limiting factor to adopt new algorithm requirements. Therefore Miele PKI does not support Certificate re-key and any re-key request is treated as a new certificate issuance request. All sub sections of 4.6 are not applicable to Miele PKI.

4.6.1. Circumstance for certificate re-key

Not applicable.

4.6.2. Who may request certification of a new public key

Not applicable.

4.6.3. Processing certificate re-keying requests

Not applicable.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.6.6. Publication of the re-keyed certificate by the CA

Not applicable.

4.6.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.7. Certificate Modification

Miele PKI does support certificate modification to the subscriber with changing information in the certificate and Re-Key. If modification of subscriber information is required a new certificate needs to be requested following revocation of the old certificates upon issuance of the new certificate. See also 4.6 Certificate Re-key.

4.7.1. Circumstance for Certificate Modification

CA and end-entity certificate modification with re-key takes place when the certificate lifetime is in the defined renewal period or operational and / or security measures require certificate modification with re-key due to possible security countermeasures.

CA certificate modification with re-key scheme

Certificate Type	Validity Period	Renewal Period
Miele Root CA 01	20 years	16 years
Miele Sub CA 01	10 years	8 years
Miele Sub CA 02	10 years	8 years

Furthermore, certificate modification with re-key can or must take place under following circumstances:

- After a subscriber's certificate has expired
- After a subscriber's certificate is revoked
- After a subscriber's certificate is lost by accident and any recovery procedure if applicable is not successful
- After a subscriber's certificate is deleted or the subscribing end-entity system is marked "end of life", retired and decommissioned. This also applies to system re-installation procedures.

4.7.2. Who may request certificate modification

- Auto-enrollment certificates are automatically requested by the subscriber machine for certificate modification with re-key

- For manually enrolled machine certificates, the responsible Miele administrative contact must request a new certificate in the validity period of the existing certificate following revocation of the existing certificate

4.7.3. Processing certificate modification requests

The renewal process with re-keying for auto-enrolled computer certificates will take place automatically, therefore there is no specific process needed.

The renewal process with re-keying for initial manually enrolled end-entity certificates is the same as the initial enrollment process.

4.7.4. Notification of new certificate issuance to subscriber

See section 4.3 Certificate Issuance.

4.7.5. Conduct constituting acceptance of modified certificate

See section 4.3.4 Conduct constituting certificate acceptance.

4.7.6. Publication of the modified certificate by the CA

See section 4.3.5 Publication of the certificate by the CA

4.7.7. Notification of certificate issuance by the CA to other entities

Notification of other entities is not supported.

4.8. Certificate Revocation and Suspension

4.8.1. Circumstances for revocation

A certificate revocation must be performed when

- the respective Miele PKI Certification Authority ceases operations for any reason
- the private key associated with the public key listed in the certificate or the media holding such private key is suspected or known to have been stolen, disclosed in an unauthorized manner or otherwise compromised
- the key and/ or device is stolen / lost / retired and the certificate is still in its validity period
- violation by the subscriber of any of its material and essential obligations under the Miele PKI CP and CPS or the subscriber agreement
- a given determination, in the Miele PKI Authority's sole discretion, that the certificate was not issued in accordance with the terms and conditions of the Miele CP and CPS
- a determination by the Miele PKI authority that continued use of the certificate is inappropriate or injurious to the proper functioning or intent of the Miele PKI
- the subscriber is no longer authorized to have a Miele PKI Certificate
- Devices and/ or Machines are reinstalled and the respective end-entity certificate is still in its validity period

4.8.2. Who can request revocation

The following persons or roles can request a revocation for certificates

- Administrative contact or security officer for the respective certificate
- Line Manager for certificates in the sphere of his or her responsibility
- Authorized service administrators
- Miele PKI certificate subscribers
- Any authorized member of Miele & Cie. KG's Information Security Team

4.8.3. Procedure for revocation request

A revocation request can be raised by

- calling Miele IT Helpdesk
- sending an email to the Miele IT Helpdesk
- using another written or electronic form, for instance via Miele IT Helpdesk Portal
- Miele IT change request tools

4.8.4. Revocation request grace period

There is no revocation request grace period. All revocation requests are considered effective with the request reaching the Miele PKI operations staff and appropriate measures are started to be applied immediately according to the Miele PKI service level agreement.

4.8.5. Time within which CA must process the revocation request

Revocation requests will be processed according to the respective incident management service level agreement in combination with the respective certificate type of the desired certificate.

4.8.6. Revocation checking requirement for relying parties

Miele PKI relying parties must have revocation checking and full chain validation capabilities wherever possible and technically applicable.

4.8.7. CRL issuance frequency

Miele PKI base CRL issuance frequency

Certificate Authority	Publication	Overlap	Lifetime
Miele Root CA 01	3 Months	1 Months	4 Months
Miele Sub CA 01	5 Days	3 Days	8 Days
Miele Sub CA 02	5 Days	3 Days	8 Days

Delta CRLs are not directly exposed / reference to the certificate subscriber but are used as a technical vehicle to enhance OCSP responder accuracy relying on CRL / delta CRL revocation information. There the following information is considered for documentation purposes only.

Miele PKI delta CRL issuance frequency

Certificate Authority	Publication	Overlap	Lifetime
Miele Sub CA 01	8 Hours	4 Hours	12 Hours
Miele Sub CA 02	8 Hours	4 Hours	12 Hours

4.8.8. Maximum latency for CRLs

Miele PKI CRLs published on Miele PKI validation services web location

CRLs are immediately available after CRL publication to the internal and external web site locations.

Miele PKI CRLs published in Miele LDAP directory

CRL availability depends on the maximum LDAP directory replication latency and site topology with a maximum delay of 60 minutes under normal operational conditions

4.8.9. On-line revocation/status checking availability

OCSP (Online Certificate Status Protocol) is available to all Miele PKI participants and implemented to support revocation checking of end-entity certificates. The OCSP service, as an alternative to CRL download, is provided by the OCSP responders within the Miele PKI environment supporting both internal and external clients using different installations / machines to mitigate security risks.

The OCSP Responders are authorized by Miele issuing CAs using respective OCSP response signing certificates issued by each Sub CA.

The Miele PKI OCSP Responders rely on up to date CRL and / or delta CRL information that is retrieved automatically on a regular basis.

Miele PKI OCSP responder accuracy in immediate revocation scenarios when CRLs are published manually by the Miele PKI operations staff after revocation of important certificates is due to caching mechanisms in combination with regular CRL and / or delta CRL retrieval interval expected not to exceed 60 minutes under normal operational conditions.

4.8.10. On-line revocation checking requirements

Windows 7, Windows Server 2008 or higher machines and other devices with OCSP client capabilities are able to check certificate revocation status via OCSP. Windows XP or Windows Server 2003 machines check certificate status by CRLs and ignore any available OCSP extension.

4.8.11. Other forms of revocation advertisements available

Not applicable.

4.8.12. Special requirements key compromise

Not applicable.

4.8.13. Circumstances for suspension

Certificate suspension is supported in general in Miele PKI trust chain.

Circumstances for suspension requests are all applicable reasons that require temporarily revoked certificates.

Certificate suspension is not considered in the current implemented Miele PKI and its respective use cases but may be considered in later phases.

4.8.14. Who can request suspension

See 4.8.2

4.8.15. Procedure for suspension request

See 4.8.3

4.8.16. Effect of a suspension

The certificate will be flagged as “revoked”. The revocation reason code for this certificate will be set to “Certificate Hold”. This will disable all associated functions related to the certificate while enabling future final revocation or un-revocation during the certificate’s validity period if required.

4.8.17. Limits on suspension period

The suspension period cannot exceed 1 year or exceed the lifetime of the revoked certificate.

4.9. Certificate Status Services

Not applicable.

4.9.1. Operational characteristics

Not applicable

4.9.2. Service availability

Not applicable

4.9.3. Optional features

Not applicable

4.10. End of Subscription

CRL and OCSP subscription ends when the Miele PKI CA certificate is expired or the Miele PKI CA and connected PKI service is terminated.

- All CRL and OCSP subscription ends, when the Miele Root CA 01 certificate is expired or the respective Root CA service is terminated.

- CRL and OCSP of the Miele Sub CA 01 subscription ends, when the Miele Sub CA 01 certificate is expired or the Miele Sub CA 01 service is terminated.

- CRL and OCSP of the Miele Sub CA 02 subscription ends, when the Miele Sub CA 02 certificate is expired or the Miele Sub CA 02 service is terminated.

4.11. Key Escrow and Recovery (Optional)

Not applicable and not implemented in the current level of implementation.

4.11.1. Key escrow and recovery policy and practices

Not applicable and not implemented in the current level of implementation.

4.11.2. Session key encapsulation and recovery policy and practices

Not applicable and not implemented in the current level of implementation.