Airbus Public Key Infrastructure

Certificate Policy

Version 5.5

SIGNATURE PAGE

Signed by:Olivier Pujol - SIG
Signed at:2022-06-10 16:08:49 +02:00
Reason:I approve this document

Olivier Pujol AIRBUS

_____ _____

Airbus Policy Management Authority DATE

DOCUMENT VERSION CONTROL

Version	Date	Authors	Description	Reason for Change
5.5	2022-04-29	Carillon	Revision	Updated CA structure New OIDs Split Audit Administrator role in two
5.4	2022-02-14	ADTS	Revision	Update new PMA chair identity
5.3	2020-10-09	ADTS	Revision	Creation of new level of assurance EADS-INFRA-USER. Certificate Policy changes to introduce this new level of assurance.
5.2	2018-07-17	ADTS	Revision	Creation of New CA for Digital Workplace in section 1.1.4 Scope Inclusion of Remote ID Proofing in section 1.6, 3.2.3, 3.2.3.1, 3.2.3.2 Creation of new certificate template for specific use cases at infrastructure-256 level of assurance in section 6.1.7, 10, 10.2
5.1	2017-11-17	ADTS	Revision	Creation of 2 new issuing CA for GP NAC Update section 1.1.4 Scope
5.0	2017-09-13	ADTS	Revision	Airbus Rebranding: whole document Various update to comply with UK, DE, SP, FR and US law Section 1.6 ;3.2.3.1 ;5.3.2 ;5.5.2 ;9.4 ;9.5.1 ;9.6 ;9.7 ;9.8 ;9.10.2 ;9.10.3 ;9.12.2 ;9.13.2 ;9.14 ;9.15 ;9.16.2 Revocation of psc CA: section 1.1.4
4.9	2017-07-18	ADTS	Revision	Creation of 2 new Issuing CAs from EADS S2 Root CA1 for National restricted needs.
4.8	2016-12-08	AGTC	Revision	Airbus Group Trust Centre generates two new issuing CAs at EADS Infrastructure 256 level of assurance to deliver certificates to mobile devices. Add content in section 1.1.4 Scope

4.7	2016-09-02	Carillon	Revision	Creation of new intermediate and signing certificate authorities under both the "EADS Root CA 2" and "EADS S2 Root CA 1" root certificate authorities, for use exclusively by Airbus ICT. Add a new extension in CRL profile. Indicate new PMA chair identity. Update references to Cassidian Communications CA and to IceCAP levels of assurance. Minor editorial changes. Add content in section: 4.9.7, 5.6, 10.1, 10.3.1 Modify content in sections: 1.0, 1.1.4, 1.2, 1.3.1.10, 1.5.2, 5.2.2, 6.1.1, 6.1.5, 6.2.2, 9.4, 9.12.2, 10.1.1, 10.1.2, 10.1.3, 10.1.7, 10.2.16, 10.2.17. Remove content in sections: 1, 1.1.4, 1.2, 1.3.1.6, 1.3.1.8, 1.3.7, 1.4, 1.6.1, 2.4, 3.1.1, 3.2.3, 3.2.3.1, 3.2.3.2, 3.3.1, 4.9.1, 4.9.5, 4.9.10, 5.2.3, 5.3.1, 5.6, 6.1.1, 6.1.5, 6.1.7, 6.2.4.4, 6.2.8, 6.4.3, 7.1.6, 9.14, 10.7, 11.
4.6	2015-03-18	Carillon	Revision	Introduction of two new sub CAs: Airbus Group CA2 (cross-certified) and pscCA2 and minor editorial cleanup: Replace "organization" by Organisation" when required. Add information about new sub CAs Airbus Group CA2 and pscCA2 in section 1.1.4, figure 1. Replace "EADS" by "Airbus" when required.

4.5	2014-09-25	Carillon	Revision	Alignment on CertiPath CP (to satisfy mapping v20 - September 22, 2014): Replace EADS by Airbus when appropriate. Add content in sections 2.4, 3.1.1, 3.2.3.3.2, 4.9.1, 5.2.3, 5.2.4, 5.5.1, 6.2.2, 6.2.4.2, 6.2.4.3, 10.2.9, 10.2.14 and 10.7. Modify content in sections 5.2.2, 5.6, 6.1.1, 6.1.7 and 10.2.12. Remove content in sections 6.2.5, 9.1.1, 9.1.3 and 10.2.3. section 5.6 (Key Changeover) change the TSS
4.4	2014-05-05	CCG	Revision	Addition of Time Stamping Services in 5.6 "Key Changeover" and corresponding Certificate Profile Airbus Group rebranding
4.3	2014-02-11	Carillon	Revision	Remove acknowledgement from Basic Assurance Levels; Adjust language to permit use of CMS for non PIV-I smartcard management; Permit the use of SCEP as part of component authentication for all Assurance Levels applicable to Device Certificates; Update definition and acronym list.
4.2	2013-12-05	Carillon	Revision	Additional language to CP to address TA requirements for PIV-I and differentiate from other Group PKI TA requirements. Replace language "For Basic Assurance Level Certificates" with "for certificates asserting the Basic Assurance Level"; Replace instances of "EADS PKI" with "EADS Group PKI". Update to Privacy Policy URLs. Specify that UPN shall be unique per subscriber or role; Specify requirements for nextUpdate field in CRLs.

4.1	2013-06-27	Carillon	Revision	Addition of requirements to address CertiPath CP Mapping; Addition of new assurance levels: EADS-INFRASTRUCTURE-256, basic-hardware, basic-hardware-256 Addition to existing requirements for Role Code Signing Certificates to address those used for Aircraft and Spacecraft code signing; Formatting and other general changes; Specify who may perform in-person proofing for human Subscribers for Certificates of Assurance Levels other than Basic.
4.0	2013-03-26	EADS Corporate Trust Centre	Revision	Introduction of a new SHA2 Root and Sub-CA New key-length 4096 for the new Root CA Insertion of a new key lifetime for the SHA2 Root and Signing CA in chapter 5.6 Key Changeover Changes to requirements for code signing certificates Clarification for Trusted Agent and role requirements Minor editorial clean up
3.7	2013-01-31	Carillon	Revision	Remove SHA1-only restriction from the code signing certificate profile
3.6	2012-11-08	Carillon	Revision	Clarification for device certificate usage. Clarification for which types of certificates may be modified and which may be renewed.
3.5	2012-05-04	Carillon	Revision	Liability language update.

3.4	2012-04-24	Carillon	Revision	Inclusion of statement that the EADS Enterprise architecture and the Cassidian Communications architecture shall not cross-certify with one another. Inclusion of official time source for US. Update to governing law to include provisions for US. Addition of Extended Key Usage Requirements. Split of EADS Group PKI Sub CA Certificate Profile section: one section for EADS Enterprise and another for Cassidian Communications.
3.3	2012-02-07	Carillon	Revision	Renaming EADS North America CAs to Cassidian Communications CAs. Updated the subject distinguished name field in Cassidian Communications PCA -> CBCA Certificate profile. Correction to CRLDP and AIA extensions in the IceCAP-cardAuth Certificate profile.
3.2	2011-11-30	Carillon	Revision	Inclusion of Certificate Profile for EADS North America PCA -> CBCA; Addition of missing requirement for appropriate uses of digital Certificates issued by the EADS North America CAs; and Modification to an incorrect section reference. Modification as a result of DGME comment

3.1	2011-11-17	Carillon	Revision	Addition of key size requirements effective 12/31/2030. Addition of requirement for HTTP pointers to appear before LDAP pointers (if present) in the AIA extension and CRL DP. Addition of PKCS 10 Request profile. Addition of Aircraft Equipment as devices and corresponding modification to Aircraft and Aircraft Equipment Certificate Profiles. Specification of where key recovery policies and practises are found, when any. Addition of restrictions preventing the use of SHA-1 and SHA-256 on the same CA. Renaming Cassidian Communications CAs to EADS North America CAs and specifying cross-certification of this CA architecture at the Root.
3.0	2011-09-23	Carillon	Revision	Addition of IceCAP Assurance Levels and other PIV-I related information Addition of "-256" Assurance Levels Addition of the EADS-INFRASTRUCTURE Assurance Level Addition of role-based certificates Addition of signature and encryption certificate profiles for devices Addition of guidance rules and certificate profiles for devices that are aircraft
2.18	2011-05-11	EADS	Revision	Align EADS identity proofing requirement to CertiPath identity proofing requirements.
2.17	2011-03-18	EADS	Revision	Change to comply with European Legislation (especially with regard to Labor Law)

2.16	2011-01-11	Carillon	Revision	The CertiPath Bridge is creating new "variant" policy OIDs for member PKIs who need to continue issuing certificates with the SHA-1 hash. Therefore, this update changes the Policy Mappings in the cross-certificate to map these new OIDs, and allows SHA-1 to continue being used. We also include a 3rd policy mapping, allowing an EADS relying party requiring medium-software assurance to understand technologically that a CertiPath variant-medium-hardware assurance certificate is acceptable.
2.15	2010-12-14	Carillon	Revision	The EADS Referent concept has been replaced with the Customer Requestor concept of the provisioning system. RFC 5280 has superseded RFC 3280.
2.14	2010-10-08	Patrick Patterson	Revision	Final adjustments to bring EADS CP into full alignment with CertiPath CP 3.12.
2.12	2010-09-08	Patrick Patterson	Revision	As a result of an updated mapping exercise, several minor discrepancies between the EADS and CertiPath CP were found.
2.11	2010-07-13	Patrick Patterson Patrick Turcotte	Revision	Allow employees to have Basic Assurance Level Certificates Allow non-employees to have Medium Assurance Level Certificates Various adjustments (ToC modifications, use "EADS Group", SSCD) Adjust TA and antecedent relationship requirements to reflect changes in the CertiPath CP
2.10	2009-05-06	Patrick Patterson Patrick Turcotte	Revision	Cleanup review: internal consistency adjustments, syntax and typos, etc. Allow for basic Assurance Level encryption Certificates for EADS employees

2.9	2009-03-13	Patrick Patterson Patrick Turcotte	Revision	Add qualified certificate statement extension to signature profile Allow certificate renewal Correct UPN extension implementation
2.8	2009-02-20	Patrick Patterson	Revision	Updated Diagram Added Basic Encryption capability for EADS Employees and Contractors. Modified PMA address
2.7	2009-01-29	Patrick Patterson Patrick Turcotte	Revision	Add smartcard logon extension Modified PMA address Formatting update
2.6	2008-11-28	Patrick Patterson Patrick Turcotte	Revision	Add UPN in Subscriber Identity Certificate profile
2.5	2008-10-6	Patrick Patterson Patrick Turcotte	Revision	Additional options for TA security clearance requirements
2.4	2008-04-25	Patrick Patterson Dave Coombs	Revision	Changes to registration procedure.
2.3	2008-04-22	Patrick Patterson Dave Coombs	Revision	Remove references to cert renewal, fix OCSP profile
2.2	2008-04-11	Patrick Patterson Dave Coombs	Revision	Final cleanup per PMA Change Requests for approval by CertiPath

2.1	2008-02-15	Dave Coombs Patrick Patterson	Revision	Final cleanup for submission to CertiPath
2.0	2008-01-15	Dave Coombs Patrick Patterson Jérôme Carrère	Revision	CertiPath and DSWG compliance
1.4.6	2007-03-27	Nicolas LOIR	Revision	Update following Certipath CP pre-mapping

DOCUMENT REFERENCES

Document Title	Version	Date of Issuance
Airbus PMA Charter	V 1.0	November 27, 2007
CertiPath Certificate Policy	V 3.25	March 17, 2014
Airbus GroupPKI Naming Policy	V 1.0	January 22, 2008

Table of Content

1.INTRODUCTION

This Certificate Policy defines several policies applicable to the use of digital Certificates for authentication, integrity (through digital signatures) and encryption in order to provide electronic identification of End-Entities as required for conducting electronic Business (eBusiness) with and within Airbus, its Business Units, partners, suppliers and customers, and the Aerospace & Defence community; and to facilitate interoperability among Aerospace industry Public Key Infrastructure domains.

The twenty policies represent the:

- EADS-INFRA-USER,
- EADS-INFRASTRUCTURE,
- EADS-INFRASTRUCTURE-256,
- basic-software,
- basic-software-256,
- basic-hardware,
- basic-hardware-256,
- medium-software-CBP (DEPRECATED),
- medium-software,
- medium-software-256,
- medium-software-org-256,
- medium-hardware-CBP (DEPRECATED),
- medium-hardware,
- medium-hardware-256,
- medium-hardware-org-CBP (DEPRECATED),
- medium-hardware-org,
- medium-hardware-org-256,
- IceCAP-cardAuth (DEPRECATED),
- IceCAP-hardware (DEPRECATED),
- IceCAP-contentSigning (DEPRECATED)

Assurance Levels for Public Key Certificates.

The "org" Assurance Levels represent Certificates issued to an entire organisation or corporation, rather than to an individual person or device.

The word "assurance" used in this CP means how well a Relying Party (RP) can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was

used to produce the Certificate and (if appropriate) deliver the Private Key to the Subscriber performs its task.

The Airbus PKI will be required to comply with the Certification Policy of other PKI domains CAs or Bridge CAs to which it is cross-certified through the use of policy mapping or direct policy assertion.

This policy covers the Airbus PKI Root CAs (Airbus Enterprise Root CA, and Airbus Enterprise SHA2 Root CAs) and the certified subordinated Airbus PKI Sub CAs (Airbus Enterprise Sub CAs, and Airbus Enterprise SHA2 Sub CAs). The Airbus Enterprise Sub CAs and the Airbus Enterprise SHA2 Sub CAs may cross certify with other PKI domains in order to allow interoperation with other Enterprises required for the business of Airbus and its Business Units.

Any use of or reference to this CP outside the purview of the Airbus PKI is completely at the using party's risk. Only the Airbus PKI Root CAs and Sub CAs of those roots shall assert the OIDs listed in section 1.2 of this document in any Certificates issued by the Airbus PKI, except in the policyMappings extension of Certificates issued by the CAs cross-certified with an Airbus PKI PCA for the establishment of equivalency between the Airbus and external PKI domains Assurance Levels.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet *X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework*.

1.1.OVERVIEW

1.1.1.Certificate Policy (CP)

Certificates contain one or more Airbus registered Certificate Policy object identifiers (OIDs), as per section 7.1.6, matching certain Assurance Levels. This may be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. The party that registers the OIDs (in this case, the Airbus Policy Management Authority) also publishes the CP for examination by Relying Parties.

Cross-certificates issued by an Airbus PKI PCA shall, in the *policyMappings* extension and in whatever other fashion is determined by the Airbus Policy Management Authority (Airbus PMA, cf. section 1.3.1) to be necessary for interoperability, reflect what mappings exist between this CP and the cross certified PKI domains' CPs.

1.1.2.Relationship between this CP and the Airbus CPS

This CP states what assurance can be placed in a Certificate issued under this policy. The Airbus Certification Practice Statements (Airbus CPSs) state how the Airbus PKI CAs establish that assurance.

1.1.3.Relationship between this CP, the other PKI domains' CPs

The levels of assurance of the Certificates issued under this CP are mapped by the Airbus Policy Management Authority (Airbus PMA) to the levels of assurance of the Certificates issued by other PKI domains which cross certify with an Airbus PKI PCA. The policy mappings information is placed into the Certificates issued by an Airbus PKI PCA, or otherwise published or used by

the Airbus PKI Operational Authority (described in section 1.3.1.2) so as to facilitate interoperability.

1.1.4.Scope

Figure 1 illustrates the scope of this CP.

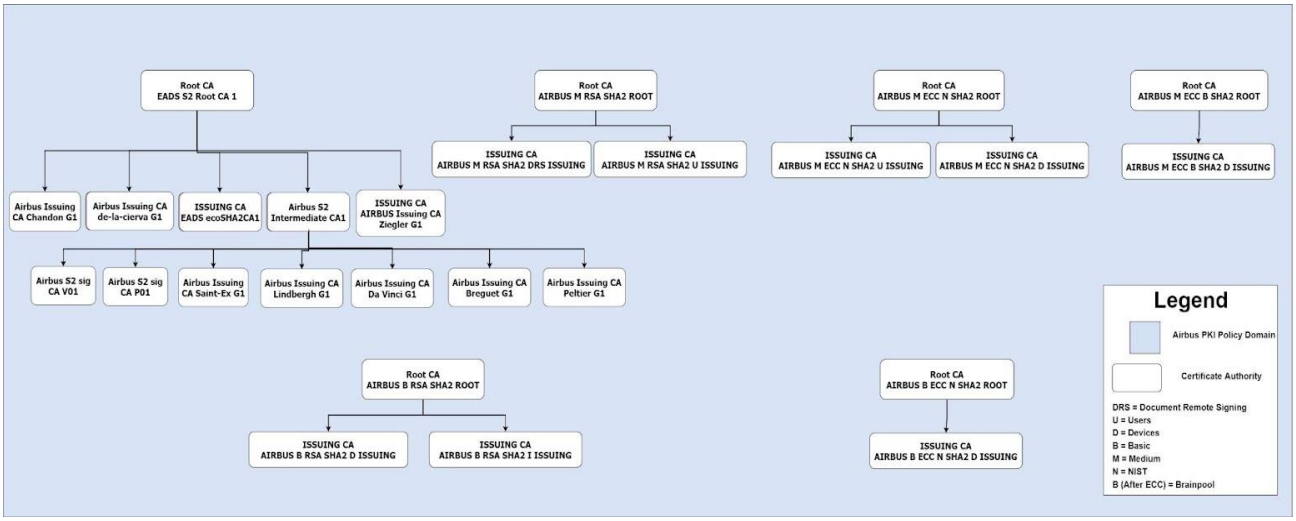

Figure 1 – Scope and Domain of Airbus PKI CAs

This CP imposes requirements on all the Airbus PKI CAs and other PKI domains involved in issuing Certificates. These include the following:

- the Airbus Enterprise Root Certification Authority (Airbus Enterprise Root CA);
- all Airbus Enterprise SHA2 Root Certification Authorities (Airbus Enterprise SHA2 Root CAs);
- all subordinated Airbus Enterprise Certification Authorities (Airbus Enterprise Sub CAs);
- all subordinated Airbus Enterprise SHA2 Certification Authority (Airbus Enterprise SHA2 Sub CAs); and
- other PKI domains' CAs.

The Airbus PKI Root CAs shall issue CA Certificates only to Airbus PKI Sub CAs approved by the Airbus PMA.

The Airbus PKI Root CAs may also issue Certificates to individuals who operate the Airbus PKI Root CAs or devices necessary for the operation of the Airbus PKI Root CAs.

The Airbus PKI Sub CAs shall issue CA Certificates only to Airbus PKI Sub CAs approved by the Airbus PMA.

The Airbus PKI PCAs (i.e.: the Airbus Enterprise Sub CAs and the Airbus Enterprise SHA2 Sub CAs) shall issue CA Certificates only to other PKI domains' CAs approved for cross-certification by the Airbus PMA.

Airbus PKI Sub CAs may issue Certificates to individuals, devices, or organisations at any Assurance Level consistent with the Assurance Level and type delegated to that Sub CA by its issuing CA.

The Airbus PKI Root CAs and Airbus PKI Sub CAs exist to facilitate trusted communications within the Airbus Domain and with Airbus partners, customers, and regulatory authorities either directly or through cross-certification with other PKI domains.

Within this document, the term CA, when used without qualifier, shall refer to any certification authority subject to the requirements of this Certificate Policy, including the Airbus PKI Root CAs and Airbus PKI Sub CAs.

The term Airbus Enterprise CAs shall be used for requirements that pertain to the Airbus Enterprise Root CAs and the Airbus Enterprise Sub CAs.

The term Airbus Enterprise SHA2 CAs shall be used for requirements that pertain to the Airbus Enterprise SHA2 Root CAs and the Airbus Enterprise SHA2 Sub CAs.

The term Airbus PKI CAs shall be used for requirements that pertain to the Airbus Enterprise CAs and the Airbus Enterprise SHA2 CAs.

Requirements that apply to a specific CA type will be denoted by specifying the CA type, e.g., Airbus PKI Root CAs, Airbus PKI Sub CAs, other PKI domains' CAs, etc.

The scope of this CP in terms of Subscriber (i.e., End Entity) Certificate types is limited to those listed in section 10.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is called the Airbus PKI Certificate Policy (CP).

There are several levels of assurance in this Certificate Policy, which are defined in subsequent sections.

Each Assurance Level is uniquely represented by an "object identifier" (OID), which is asserted in each Certificate issued by the Airbus PKI Sub CAs that complies with the policy stipulations under this CP.

The OIDs are registered under the Airbus arc as follows:

EADS OBJECT IDENTIFIER	::= 1.3.6.1.4.1.16304
EADSCAObjects	::= EADS 3
EADSCACorporate	::= EADSCAObjects 6
EADSCorporateCAPolicies	::= EADSCACorporate 2
id-EADSINFRASTRUCTURE	::= EADSCorporateCAPolicies 1
id-EADSINFRASTRUCTURE-256	::= EADSCorporateCAPolicies 2
id-BasicSoftware	::= EADSCorporateCAPolicies 3
id-MediumSoftwareCBP (DEPRECATED)	::= EADSCorporateCAPolicies 4
id-MediumHardwareCBP (DEPRECATED)	::= EADSCorporateCAPolicies 5
id-MediumHardwareOrgCBP (DEPRECATED)	::= EADSCorporateCAPolicies 6
id-MediumSoftware	::= EADSCorporateCAPolicies 7
id-MediumHardware	::= EADSCorporateCAPolicies 8
id-MediumHardwareOrg	::= EADSCorporateCAPolicies 9
id-BasicSoftware-256	::= EADSCorporateCAPolicies 10
id-MediumSoftware-256	::= EADSCorporateCAPolicies 11
id-MediumHardware-256	::= EADSCorporateCAPolicies 12
id-MediumSoftwareOrg-256	::= EADSCorporateCAPolicies 13
id-MediumHardwareOrg-256	::= EADSCorporateCAPolicies 14
id-IceCAPHardware (DEPRECATED)	::= EADSCorporateCAPolicies 20

id-IceCAPCardAuth (DEPRECATED)	::= EADSCorporateCAPolicies 21
id-IceCAPContentSigning (DEPRECATED)	::= EADSCorporateCAPolicies 22
id-BasicHardware	::= EADSCorporateCAPolicies 30
id-BasicHardware-256	::= EADSCorporateCAPolicies 31
id-EADSINFRA-USER-256	::= EADSCorporateCAPolicies 32

The Airbus PMA shall not request any 'pass-through' policy OIDs to be asserted in any cross-certificates issued to them by an external PKI domain.

Unless otherwise stated, a requirement stated in this CP applies to all Assurance Levels. Moreover, unless otherwise stated, all of the requirements for "-256" Assurance Levels are the same as those for the corresponding Assurance Level without "-256" in it, except that the CAs

asserting "-256" must use SHA-256 for generation of PKI objects such as Certificates, Certificate Revocation Lists (CRLs) and Onlin[1]e Certificate Status Protocol (OCSP) responses.

The relationships between these assurance levels, and which OIDs may be asserted at which assurance level, are fully detailed in section 7.1.6.

1.3.PKI PARTICIPANTS

This section contains a description of the roles relevant to the administration and operation of the Airbus PKI CAs.

1.3.1.Airbus PKI Authorities

1.3.1.1.Airbus Policy Management Authority (Airbus PMA)

The Airbus PMA is responsible for:

- Commissioning, drafting and approving the Airbus PKI CP (this document);
- Commissioning compliance analysis, acting on recommendations resulting from analysis, and approving the Airbus PKI CPSs;
- Accepting and approving applications from entities desiring to cross-certify with an Airbus PKI PCA;
- Ensuring continued conformance of the Airbus PKI CPSs with applicable requirements as a condition for continued securing of the Assurance Levels as stipulated in this CP;
- Managing the interoperation with other PKI domains' CAs;
- Ensuring continued conformance of the Airbus PKI and other domains' PKI with applicable requirements as a condition for allowing continued interoperability with cross-certified CAs.

Airbus shall enter a contractual relationship through a Memorandum Of Agreement (MOA) with the PMAs of other PKI domains setting forth the respective responsibilities and obligations of both parties, and the mappings between the Certificate levels of assurance contained in this CP and those in the respective CP of the other PKI domains' CA subject to cross-certification. The term "MOA" as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

A complete description of Airbus PMA roles and responsibilities is provided in the Airbus PKI Policy Management Authority Charter [Airbus PMA CHARTER].

1.3.1.2.Airbus PKI Operational Authority (OA)

The Airbus PKI Operational Authority consists of the organisations that are responsible for the operation of the Airbus PKI CAs, including issuing Certificates when directed by the Airbus PMA or any authorised Airbus Registration Authority (RA) operating under this CP, posting those Certificates and Certificate Revocation Lists (CRLs) into the repositories of the Airbus PKI,

1

and ensuring the continued availability of these repositories to all users in accordance with section 2 of this document.

1.3.1.3.Airbus PKI Operational Authority Administrator

The Administrator is the individual within the Operational Authority who has principal responsibility for overseeing the proper operation of the Airbus PKI infrastructure components, and who appoints individuals to the positions of Operational Authority Officers.

The Administrator is selected by and reports to the Airbus PMA.

The Administrator approves the issuance of Certificates to the other trusted roles operating the Airbus PKI CAs.

1.3.1.4.Airbus PKI Operational Authority Officers

These officers are the individuals within the Operational Authority, selected by the Administrator, who operate the Airbus PKI infrastructure components, including executing the

Airbus PMA direction to issue Certificates to CAs or taking other action to enable interoperability between the Airbus PKI CAs and external domain PKIs.

The Airbus PKI Operational Authority Officers cover the Operational Authority Officer, the Internal Auditor, the Audit Operator, and the Operator activities, all described in section 5.2.1 of this CP.

1.3.1.5. Entity Principal Certification Authority (PCA)

A Principal CA is a CA within a PKI that has been designated by the PMA to interoperate directly with an external domain CA (e.g., through the exchange of Cross-Certificates).

As operated by the Operational Authority, an Airbus PKI PCA is responsible for all aspects of the issuance and management of a Cross-Certificate issued to an external domain CA, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Cross-Certificate manufacturing process,
- The publication of Cross-Certificates,
- The revocation of Cross-Certificates,
- Ensuring that all aspects of the services, operations and infrastructure related to Cross-Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

The Airbus PKI PCA(s) shall not issue Cross-Certificates to another Airbus PKI PCA.

1.3.1.6. The Airbus PKI Root CAs

The Airbus PKI Root CAs are the Root CAs of the Airbus PKI. Each Airbus PKI Root CA is a trust anchor for Relying Parties trying to establish the validity of a Certificate issued by an Airbus PKI Sub CA, whose chain of trust can be traced back to that specific Root CA.

The Airbus PKI Root CAs issue and revoke Certificates to Airbus PKI Sub CAs upon authorisation by the Airbus PMA. As operated by the Operational Authority, the Airbus PKI

Root CAs are responsible for all aspects of the issuance and management of those Sub CA Certificates, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Certificate manufacturing process,
- The publication of Certificates,
- The revocation of Certificates, and
- Ensuring that all aspects of the services, operations and infrastructure related to Sub CA Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7. The Airbus PKI Subordinate CAs

The Airbus PKI Sub CAs are all of the Airbus PKI Intermediate and/or Airbus PKI Signing CAs subordinate to the Airbus PKI Root CAs as defined below.

An Airbus Enterprise Sub CA and an Airbus Enterprise SHA2 Sub CA may function as a PCA.

1.3.1.7.1. Airbus PKI Intermediate CAs

An Intermediate CA is a CA that is not a Root CA and whose primary function is to issue Certificates to other CAs. Intermediate CAs may or may not issue some End-Entity Certificates.

The Airbus PKI Intermediate CAs issue and revoke Certificates to other Airbus PKI Sub CAs upon authorisation by the Airbus PMA. The Airbus PKI Intermediate CAs are responsible for all

aspects of the issuance and management of those Sub CA Certificate, as detailed in this CP, including:

- The control over the registration process;
- The identification and authentication process;
- The Certificate manufacturing process;
- The publication of Certificates;
- The revocation of Certificates; and
- Ensuring that all aspects of the services, operations and infrastructure related to Sub CA Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.7.2. Airbus PKI Signing CAs

A Signing CA is a CA whose primary function is to issue Certificates to End-Entities. A Signing CA does not issue Certificates to other CAs.

As operated by the Operational Authority, an Airbus PKI Signing CA is responsible for all aspects of the issuance and management of an End-Entity Certificate, as detailed in this CP, including:

- The control over the registration process;
- The identification and authentication process;
- The Certificate manufacturing process;
- The publication of Certificates;
- The revocation of Certificates; and
- Ensuring that all aspects of the services, operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.8. Certificate Status Authority (CSA)

A CSA is an authority that provides status of Certificates or certification paths. A CSA can be operated in conjunction with the CAs or independent of the CAs. Examples of a CSA are:

- Online Certificate Status Protocol (OCSP) Responders that provide revocation status of Certificates.
- Server-based Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services.

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide Certificate validation services adhere to the same security requirements as repositories.

1.3.1.9. Time-Stamp Authority (TSA)

A TSA is an authority that issues and validates trusted timestamps. A TSA can be operated in conjunction with a CA or independent of a CA.

1.3.1.10. Card Management System (CMS)

The Card Management System is responsible for managing smart card token content.

In the context of this CP, CMS is recommended for smart card management for all Assurance Levels. CAs shall be responsible for ensuring that their CMSs meet the requirements described in this document, as pertains to the Assurance Levels of smart card credentials managed by the CMS.

1.3.2. Registration Authorities

An RA is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her Public Key Certificate. An RA interacts with the CA to enter and approve the Subscriber Certificate request information. The Airbus Operational Authority acts as the RA for the Airbus PKI Root CAs, and for Airbus PKI PCAs when dealing with cross certification. It performs its function in accordance with the concerned Airbus CPS approved by the Airbus PMA.

An RA shall possess a Certificate of assurance equal to or greater than that of the Certificate being issued, protected as described in sections 6.1.1 and 6.2.1.

1.3.3. Subscribers

A Subscriber is the entity whose name appears as the subject in a Certificate, who asserts that it uses its key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and who does not itself issue Certificates. This entity has the duty to protect the Certificate that is provided to him/her as expressed in the General Terms and Conditions related to this CP. Airbus PKI Root CA Subscribers include only Airbus PKI CA Operational Authority personnel and, when determined by the Airbus PMA, possibly certain network or hardware devices such as firewalls and routers when needed for PKI-infrastructure protection.

Airbus PKI Sub CA Subscribers include Airbus employees (employees of Airbus Business Units), subcontractor personnel, suppliers, partners or customers, and hardware devices such as firewalls, routers, servers, or aircraft and/or aircraft equipment operated by or in the name of Airbus and its Business Units.

CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who are issued Certificates for uses other than signing and issuing Certificates or Certificate status information.

1.3.4. Affiliated Organisation

Subscriber Certificates may be issued in conjunction with an organisation that has a relationship with the Subscriber; this is termed affiliation. The organisational affiliation shall be indicated in a relative distinguished name in the subject field in the Certificate, and the Certificate shall be revoked in accordance with section 4.9.1 when affiliation is terminated.

1.3.5. Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a Public Key. The Relying Party is responsible for deciding how to check the validity of the

Certificate by checking the appropriate Certificate status information. The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the creator of a message or document, or to establish confidential communications with the holder of the Certificate. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.6. Other participants

1.3.6.1. Related Authorities

The Airbus PKI CAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The Airbus CPSs shall identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.6.2. Trusted Agent

A Trusted Agent is appointed by the OA and may collect and verify Subscriber identity and information on behalf of an RA. Information shall be verified in accordance with section 3.2 and communicated to the RA in a secure manner.

A Trusted Agent shall not have direct access to the CA to enter or approve Subscriber information.

1.3.7. Applicability

The sensitivity of the information processed or protected using Certificates issued by Airbus PKI CAs will vary significantly. Entities must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on

the sensitivity or significance of the information. This evaluation is done by each Entity for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at various levels of assurance as listed in section 1.2.

The Certificate levels of assurance contained in this CP are set forth below, as well as a brief and non-binding description of the applicability for applications suited to each level.

Assurance Level	Applicability
EADS-INFRASTRUCTURE, EADS-INFRASTRUCTURE-256	This level is used for the issuance of digital credentials to devices and other components for use only within Airbus. Certificates shall only be issued at this Assurance Level to non-human Subscribers, i.e.: hardware devices and components operated by or in the name of Airbus and/or an Airbus Business Unit.
EADS-INFRA-USER	This level is used for the issuance of digital credentials to mobile device users within Airbus. Certificates shall only be issued at this Assurance Level to mobile device users. e.: email.address@airbus.com Any other usage for certificates issued with this level of assurance is prohibited.
basic-software, basic-software-256	This level is relevant to environments where risks and consequences of data compromise are low. Subscriber Private Keys shall be stored in software at this Assurance Level.
basic-hardware, basic-hardware-256	This level is relevant to environments where risks and consequences of data compromise are low. Subscriber Private Keys shall be stored in hardware at this Assurance Level.
medium-software, medium-software-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in software at this Assurance Level. Certificates of this Assurance Level issued to Subscribers for signing purposes may be used for Qualified Signatures, as specified in ETSI TS 101456.

medium-hardware, medium-hardware-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Subscriber Private Keys shall be stored in hardware at this Assurance Level. Certificates of this Assurance Level issued to Subscribers for signing purposes may be used for Qualified Signatures with SSCD, as specified in ETSI TS 101456
medium-software-org-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial, or where it is desirable to ensure the integrity of a document or software has not been compromised once it has left the control of the signing organisation or corporation. Subscriber Private Keys shall be stored in software at this Assurance Level. These digital Certificates shall only be issued to organisations and corporations. All transactions utilising Certificates at this Assurance Level shall be performed using the timestamp protocol outlined in IETF RFC 3161 and IETF RFC 5816 .
medium-hardware-org, medium-hardware-org-256	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial, or where it is desirable to ensure the integrity of a document or software has not been compromised once it has left the control of the signing organisation or corporation. Subscriber Private Keys shall be stored in hardware at this Assurance Level. These digital Certificates shall only be issued to organisations and corporations. All transactions utilising Certificates at this Assurance Level shall be performed using the timestamp protocol outlined in IETF RFC 3161 and IETF RFC 5816.

1.3.7.1. Factors in Determining Usage

The Relying Party must first determine the level of assurance required for an application, and then select the Certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the Airbus PMA or the

Airbus Operational Authority. Nonetheless, this CP contains some helpful guidance, set forth herein, which Relying Parties may consider in making their decisions.

1.3.7.2.Obtaining Certificates

Relying Parties see section 2.

All other entities see section 3.

1.4.CERTIFICATE USAGE

The Airbus PKI CAs shall issue digital Certificates for various uses in the context of conducting eBusiness within or with Airbus Business Units, or for extended Airbus Enterprise (e.g. to customers, suppliers, etc.).

1.4.1.Appropriate Certificate uses

No stipulation.

1.4.2.Prohibited Certificate uses

No stipulation.

1.5.POLICY ADMINISTRATION

1.5.1.Organisation administering the document

The Airbus PMA is responsible for all aspects of this CP.

1.5.2.Contact person

Questions regarding this CP shall be directed to the Airbus PMA represented by:

Olivier Pujol

Chair of the Airbus PKI PMA

Airbus S.A.S.

2, Rond-Point Emilie Dewoitine

31703 BLAGNAC Cedex - France

1.5.3.Person determining CPS suitability for the policy

The Airbus PMA shall approve the Airbus PKI CPSs and commission an analysis to determine whether the Airbus PKI CPSs conform to the Airbus PKI CP.

When such a compliance analysis shall be performed:

- The determination of suitability shall be based on an independent compliance analyst's results and recommendations; and
- The compliance analysis shall be from a firm, which is independent from the entity being audited. The compliance analyst may not be the author of the CP or the CPS; and

- The entity PMA shall determine whether a compliance analyst meets these requirements.

When entering into a MOA:

- Each entity shall be responsible for determining whether their CPS(s) conform to their CP(s).
- Entities shall be obliged to properly adhere to the policy mapping between the Airbus PKI CP and external PKI domain CPs.
- The entity shall be obliged to attest to such compliance periodically.

1.5.4.CPS approval procedures

The CPS shall be more detailed than the corresponding Certificate Policy described in this document. The Airbus PKI CPSs shall specify how this CP shall be implemented to ensure

compliance with the provisions of this CP. The approval procedures for the CPSs shall be outlined in the Airbus PMA Charter and by-laws.

1.5.5.Waivers

There shall be no waivers to this CP.

1.6.DEFINITIONS AND ACRONYMS

1.6.1.Definitions

Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code) that is used to perform cryptographic operations using a Private Key.
Airbus Directory	Repository accessible only to Airbus internal End-Entities and Relying Parties.
Assurance Level	A representation of how well a Relying Party can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the End-Entity whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was used to produce the Certificate and (if appropriate) deliver the Private Key to the End-Entity performs its task.
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Card Management System (CMS)	The Card Management System is responsible for managing smart card token content.

Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: • The identity of the Certification Authority issuing it. • The identity of the certified End-Entity. • A Public Key that corresponds to a Private Key under the control of the certified End-Entity. • The Operational Period. • A serial number. The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certification Authority (CA)	A Certification Authority is an entity that is responsible for authorising and causing the issuance or revocation of a Certificate. By extension, the term "CA" can also be used to designate the infrastructure component that technically signs the Certificates and the revocation lists it issues. A Certification Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this function to separate entities. A Certification Authority performs three essential functions. First, it is responsible for identifying and authenticating the intended Authorised Subscriber to be named in a Certificate, and verifying that such Authorised Subscriber possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate. Second, the Certification Authority actually creates and digitally signs the Authorised Subscriber's Certificate. The Certificate issued by the Certification Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private Key Pair. Third, the Certification Authority creates and digitally signs the Certificate Revocation Lists and/or Authority Revocation Lists.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorised Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.

CertiPath	CertiPath is a corporation whose purpose is to design, implement, maintain and market a secure Public Key infrastructure communications bridge, initially focused on the aerospace and defence industry.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. Within this document, the term CP, when used without qualifier, refers to the Airbus CP, as defined in section 1.
Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Certificate Request	A message sent from an applicant to a CA in order to apply for a digital certificate. The certificate request contains information identifying the applicant and the Public Key chosen by the applicant. The corresponding Private Key is not included in the request, but is used to digitally sign the entire request. If the request is successful, the CA will send back a certificate that has been digitally signed with the CA's Private Key.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When an End-Entity chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Status Authority (CSA)	A CSA is an authority that provides status of Certificates or certification paths.

Cross-certificate (CC)	A Certificate used to establish a trust relationship between two Certification Authorities. A cross-certificate is a Certificate issued by one CA to another CA which contains the subject CA Public Key associated with the private CA signature key used by the subject CA for issuing Certificates. Typically a cross-certificate is used to allow End-Entities in one CA domain to communicate securely with End-Entities in another CA domain. A cross-certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1 domain, to accept a Certificate used by Entity #b, who has a Certificate issued to Entity #b by CA#2.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. Whether the message has been altered since the transformation was made.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End-Entity within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
End-Entity (EE)	A person, device or application that is issued a certificate by a CA.
Airbus PKI Directory	Publicly-accessible Repository.
Entity	Any autonomous element within the PKI, including CAs, RAs and End-Entities.
Employee	An employee is any person employed in or by the Airbus.

Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorisation. Smartcards and USB tokens are examples of hardware tokens.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (End-Entities).
Incident	Misuse relating to a single credential regardless of the relying parties involved
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Intermediate CA	A CA that is not a Root CA and whose primary function is to issue Certificates to other CAs. An Intermediate CA is a Subordinate CA.
Issuing CA	In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the Certificate.
Key Generation	The process of creating a Private Key and Public Key pair.
Key Pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Local Registration Authority (LRA)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).

Memorandum of Agreement	As used in the context of this CP, between Airbus or an Airbus Business Unit and external PKI Domains legal Representation allowing interoperation between the respective Airbus PKI CAs and an external PKI domains CA. Airbus consults the Airbus PMA through the Airbus PMA Chair on the MOA
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognised standards organisation.
Operational Authority (OA)	An agent of an Airbus PKI CA. The Operational Authority is responsible to the Policy Management Authority for: Interpreting the *Certificate Policies* that were selected or defined by the Policy Management Authority. Developing a *Certification Practice Statement (CPS)*, in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647)*, to document the CA's compliance with the Certificate Policies and other requirements. Maintaining the CPS to ensure that it is updated as required. Operating the Certification Authority in accordance with the CPS.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organisation	Department, agency, partnership, trust, joint venture or other association.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.
PIN	Personal Identification Number. See activation data for definition

PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS."
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Policy	This Certificate Policy.
Policy Management Authority (PMA)	An agent of the Certification Authority. The Policy Management Authority is responsible for: Dispute resolution. Selecting and/or defining *Certificate Policies*, in accordance with the *Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 3647)*, for use in the Certification Authority PKI or organisational enterprise. Approving of any interoperability agreements with external Certification Authorities. Approving practices, which the Certification Authority must follow by reviewing the *Certification Practice Statement* to ensure consistency with the *Certificate Policies*. Providing Policy direction to the CA and the Operational Authority.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key certificates.
Principal CA (PCA)	CA within a PKI that has been designated to interoperate directly with another PKI (e.g., through the exchange of cross-certificates with a PCA in another PKI domain).
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.

Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.
Public/Private Key Pair	See Key Pair.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A Relying Party is a recipient of a Certificate signed by an Airbus PKI CA who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS. The term "Relying Party" designates the legal entity responsible for the recipient's actions.
Relying Party Agreement	An agreement, entered into by a Relying Party, that provides for the respective liabilities of Airbus or its Business Units and of the Relying Party. Such agreement is a prerequisite in order to be able to rely on the Certificate.
Remote Proofing	An identity proofing process that employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.

RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
Role Certificate	A Role Certificate is a Certificate which identifies a specific role on behalf of which the human Subscriber is authorized to act.
Root CA	A CA that is the trust anchor for a set of relying parties.
SCVP	Protocol that allows a client to delegate Certificate path construction and Certificate path validation to a server.
Secure Signature-Creation Devices (SSCD)	A set of hardware and software elements designed for and allowing the creation of a digital signature in a secure manner. This is used in the context of the CEN CWA 14169 standard
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Signing CA	A CA whose primary function is to issue Certificates to End-Entities. A Signing CA is a Subordinate CA.
Software-based Certificate	A digital Certificate (and associated Private Keys) that are created and stored in software – either on a local workstation or on a server.
Sponsoring Organisation	An organisation with which an Authorised Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).
Subordinate CA	A CA that is not a Root CA. It is subordinate to either a Root CA or other Subordinate CA.
Subscriber	An entity that is the subject of a Certificate and which is capable of using, and is authorised to use, the Private Key, that corresponds to the Public Key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the *Certificate Policy* and *the General Terms and Conditions*.

General Terms and Conditions	An agreement, entered into by a Subscriber, that provides the responsibilities and obligations of the Subscribers when using Certificates. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.
Token	A hardware security device containing an End-Entity's Private Key(s) and Certificate. (see "Hardware Token")
Transaction	Any use of a single credential. Multiple transactions associated with misuse of a single credential constitute an incident.
Trusted Agent	An agent who a Registration Authority relies on to verify that an applicant fulfils part of or all of the necessary prerequisites to obtain a certificate for an End-Entity.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not "valid" until it is both issued by a CA and has been accepted by the Subscriber.

1.6.2.

1.6.3.Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
C	Country
CA	Certification Authority
CBCA	CertiPath Bridge Certification Authority
CBP	Commercial Best Practices (DEPRECATED)
CHUID	Cardholder Unique Identifier CMS
CMS	Card Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DC	Domain Component
DN	Distinguished Name
DNS	Domain Name Service
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	End-Entity
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority

FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
GUID	Globally Unique Identifier
HR	Human Resources
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
KAPIS	Konzernabschluss, Planungs und Information-System (Enterprise financial statement, plan and Information System)
KRP	Key Recovery Policy
KRPS	Key Recovery Practices Statement
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
O	Organisation
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisational Unit

PCA	Principal Certification Authority
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification - Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SCEP	Simple Certificate Enrolment Protocol
SCVP	Server-based Certificate Validation Protocol
SHA-1	Secure Hash Algorithm, Version 1
SSCD	Secure Signature-Creation Devices
SSL	Secure Sockets Layer
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier

URL	Uniform Resource Locator
UUID	Universally Unique Identifier

2.PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1.REPOSITORIES

The Airbus PKI operates Repositories containing all information necessary to provide lookup and validation services for issued Certificates.

The mechanisms used by the Airbus PKI to post information to its respective repositories, as required by this CP, shall include:

- Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP) or the Hypertext Transport Protocol (HTTP),
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP, and
- Access control mechanisms when needed to protect repository information as described in later sections.

The PKI Repositories containing Certificates and Certificate status information shall be deployed so as to provide high levels of reliability (24/24h & 7/7d at a rate of 99% availability or better).

2.2.PUBLICATION OF CERTIFICATE INFORMATION

2.2.1.Publication of CA Information

The Airbus PKI CP shall be published electronically on the Airbus Enterprise PKI web site.

All encryption Public Key Certificates issued by the Airbus PKI CAs to digital Certificate users shall be published to the respective applicable Repositories, as set forth in the applicable CPSs.

All CRLs, ARLs, CA certificates, and CA Cross-Certificates issued by Airbus PKI CAs shall be published to the respective and applicable Repositories as set forth in the applicable CPSs.

Even if CP shall be published electronically on the Airbus Enterprise PKI web site, applicable CPSs must be kept Airbus Confidential.

All publication made by Airbus PKI CAs shall be performed as soon as an internal event that may require publication (revocation, issuance or modification of certificate) is validated by the CA.

2.2.2.Interoperability

Where Certificates and CRLs are published in the Airbus Directory or the Airbus Enterprise PKI Directory, standards-based schemas for directory objects and attributes shall be implemented. Airbus Repositories as defined above shall be interoperable as required with all repositories operated by CAs with which the Airbus PKI is cross-certified.

The following interoperability profile is defined:

- **Protocol**: access to Certificates and CRLs stored in the Airbus Directory and Airbus PKI Directory shall be provided using the following protocols: LDAP and HTTP.
- **Naming**: CA Certificates shall be stored in the Airbus Directory and Airbus PKI Directory in the entry that appears in the Certificate subject name. The issuedByThisCA

element of crossCertificatePair shall contain the Certificate(s) issued by a CA whose name the entry represents. CRLs shall be stored in the Airbus PKI Directory in the entry that appears in the CRL issuer name.

- **Object Class**: Entries that define CAs shall be members of pkiCA cpCPS auxiliary object classes. Entries that describe end-users shall be defined by the inetOrgPerson class, which inherits from other classes: person, and organisationalPerson. These entries shall also be a member of pkiUser auxiliary object class.
- **Attributes**: CA entries shall be populated with the cACertificate, crossCertificatePair, and certificateRevocationList, cPCPS attributes, as applicable. User entries shall be populated with userCertificate attribute containing encryption Certificate.
- **Authentication**: for read access to the information in the Internet, "none" authentication shall be sufficient. Any write, update, add entry, delete entry, add attribute, delete attribute, change schema etc., shall require password over SSL or stronger authentication mechanism.

2.3.TIME OR FREQUENCY OF PUBLICATION

Airbus PKI CA public information identified in section 2.2.1 shall be published prior to the first Certificate being issued in accordance with this CP by that CA. Certificates and Certificate status information shall be published as specified in section 4 of this CP.

2.4.ACCESS CONTROLS ON REPOSITORIES

Any PKI Repository information not intended for public dissemination or modification shall be protected.

Encryption Certificates and status information for all Certificates in the Airbus PKI Directory shall be publicly available through the Internet.

This CP shall be publicly available through the Internet.

Access to information in Airbus Directory shall be limited to the Airbus intranet.

3.IDENTIFICATION AND AUTHENTICATION

3.1.NAMING

3.1.1.Types of Names

The Airbus PKI CAs shall generate and sign Certificates containing an X.501 Distinguished Name (DN) in the Issuer and Subject fields. Such DNs shall be assigned in accordance with section 3.1.4 Subject Alternative Name may be used, if marked non-critical; section 10 lists the accepted contents (email address, UPN, FQDN, etc.) and their specific formats.

For Certificates issued to human Subscribers, the subject DN shall either contain the value "Unaffiliated" in the last organisational unit (ou) attribute or shall contain the affiliated

organisation name in an appropriate relative distinguished name attribute (e.g., organisation (o), organisational unit (ou), or domain component (dc) attribute).

3.1.2. Need for names to be meaningful

The Certificates issued pursuant to this CP are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates shall identify the person or object to which they are assigned in a meaningful way.

DNs shall be used, wherein the Common Name represents the Subscriber in a way that is easily understandable for humans.

For people, this will typically be:

- **Given-Name[space]** [2] **MI** [3] **[space]** [4] **Surname**, and subject to the uniqueness requirements of section 3.1.5.

For equipment, this may be an IP address, a Fully-Qualified Domain Name (FQDN) or a URL.

For CAs, organisations, or corporations, this must be the officially recognised legal name or registration number of the organisation or corporation.

All DNs shall be unique and shall satisfy asserted namespace constraints.

Subject DNs shall accurately reflect the organisation with which the Subject is affiliated.

When UPN is used, it shall accurately reflect organisational structure, and shall be unique per subscriber or role.

3.1.3. Anonymity or pseudonymity of Subscribers

CA certificates shall not contain anonymous or pseudonymous identities.

Certificates issued by Airbus PKI CAs shall not contain anonymous or pseudonymous identities, only names as defined in section 7 are applicable for issuance of a Certificate.

3.1.4. Rules for interpreting various name forms

Rules for interpreting name forms shall be contained in the [Airbus PKI Naming Policy], and in the applicable Certificate profile.

The authority responsible for the Airbus name space is the Airbus Corporate Communication Department.

3.1.5. Uniqueness of names

Name uniqueness across the Airbus domains shall be enforced. The Airbus PKI CAs and RAs shall enforce name uniqueness within their authorised X.500 name space.

The applicable CPSs shall describe how names shall be allocated within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if "Joe Q

[2] "[space]" refers to a space character and not the individual characters.

Smith" leaves a CA's community of Subscribers, and a new, different "Joe Q Smith" enters the community of Subscribers, how will these two people be provided unique names).

The Airbus PMA shall be responsible for ensuring name uniqueness in Certificates issued by the Airbus PKI CAs.

3.1.6. Recognition, authentication, and role of trademarks

The use of trademarks will be reserved to registered trademark holders and to the CAs in strict proportion to that required for the performance of this CP.

3.1.7. Name Claim Dispute Resolution Procedure

The Airbus PMA shall resolve or cause to be resolved any name collision brought to its attention that may affect interoperability.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to prove possession of Private Key

In all cases where the party named in a Certificate generates its own keys that party shall be required to prove possession of the Private Key, which corresponds to the Public Key in the Certificate request. For signature keys, this may be done by the entity using its Private Key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature

[3] MI represent the middle initial(s). They are optional, and are to be used if necessary to ensure name uniqueness. If used, the middle initial(s) have a maximum length of two characters.

[4] "[space]" refers to a space character and not the individual characters. This space is not to be included if no middle initials are used (i.e. the Common Name does not include two consecutive spaces).

using the party's Public Key. The Airbus PMA may allow other mechanisms that are at least as secure as those cited here.

3.2.2. Authentication of organisation identity

Requests for medium-hardware-org, medium-software-org-256, or medium-hardware-org-256 Certificates in the name of an organisation shall include the following:

- full company name, legal name, or internal KAPIS code;
- address of its head office;
- documentation of the existence of the organisation (such as articles of incorporation);
- its Dun and Bradstreet identifier if doing business within, but not limited to, the United States of America;
- a letter from its authorised representative officially requesting said Certificate;
- any device proving the right to create and publish software within the community if the Certificate to be issued shall be used for code-signing;
- a declaration by the organisation that they shall not publish viruses or other harmful code signed with a code-signing Certificate; and
- a face-to-face meeting with the RA or CA and an authorised representative of the organisation carrying the appropriate power of attorney.

In all cases, the existence of an affiliated organisation shall be verified prior to issuing any end user Certificates on its behalf. The RA shall verify the authenticity of the requesting representative and the representative's authorisation to act in the name of the organisation. Moreover, requests for end-user Certificates other than unaffiliated Subscribers shall include the name of the organisation and shall be verified with the identified affiliated organisation.

3.2.3. Authentication of individual identity

For all Assurance Levels applicable to human Subscribers other than Basic, identity shall be established by in-person or remote proofing before the RA, Trusted Agent, or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. For remote identity proofing, the accepted process shall be compliant with "DSWG Spec 42 §2-3-2.1 - Identity Proofing and Vetting Requirement".

The Airbus PKI CAs shall ensure that the applicant's identity information is verified and checked in accordance with this CP and the applicable CPSs. The CA or an RA shall ensure that the applicant's identity information and Public Key are properly bound. Additionally, the CA or the RA shall record the process that was followed for issuance of each Certificate. Process

information shall depend upon the Certificate level of assurance and shall be addressed in the applicable CPS.

3.2.3.1. Authentication of Individuals, who are Airbus employees or employees of an Airbus Business Unit

CAs and RAs are responsible for ensuring that they are in compliance with all applicable laws when collecting personally identifiable information. If a jurisdiction prohibits the collection, distribution or storage of any of the information specified in this section, an alternate, equivalent proofing mechanism may be used that assures the identity of the applicant to an equivalent level, subject to approval of the Airbus PMA. If the data is used to proof an identity for medium-software or medium-hardware Assurance Level, this alternate procedure shall be

communicated to external domain PKIs prior to implementation, or as outlined in the MOA with that external domain PKI.

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification; and
- A signed declaration by that person that he or she verified the identity of the applicant as required by this CP which may be met by establishing how the applicant is known to the verifier as required by this CP.

For Basic Assurance Levels, the following information shall be recorded:

1. the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
2. the full name and legal status of the applicant's Employer;
3. an email address for the applicant;
4. a declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4;
5. the date and time of the verification.

For all Assurance Levels applicable to human Subscribers other than Basic, the following information shall be recorded:

1. the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
2. the date and place of birth or other attribute(s) which may be used to uniquely identify the applicant;
3. the full name and legal status of the Subscriber's Employer;
4. a physical address or other suitable method of contact;
5. a declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4;
6. the date and time of the verification; and
7. a declaration of identity signed by the applicant using a handwritten signature. This shall be performed in the presence of the person performing the identity authentication.

For Certificates asserting the Medium Assurance Levels, the applicant shall:

1. present one (1) valid National Government-issued photo ID or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License); and
2. present evidence that he or she is an Airbus employee or an employee of an Airbus

Business Unit.

For Certificates asserting the Basic Assurance Levels, the applicant's identity can be determined based on existing corporate data.

Identity for other Assurance Levels applicable to human Subscribers shall be established by in-person or remote proofing before the RA or Trusted Agent; information provided shall be verified to ensure legitimacy.

Requirements for authentication of individual identity using an in-person antecedent are listed in section 3.2.3.4.

3.2.3.2. Authentication of Individuals, who are not Airbus employees

Airbus may issue digital Certificates to individuals who are not employees of Airbus or of an Airbus Business Unit. In such cases, Airbus shall establish a contractual relationship with the external company employing such an individual, whereby a representative of said company shall be nominated to act as Customer Requestor for that company. The Customer Requestor shall provide authorisation for applicants at that company to receive certificates, and shall provide identifying information of applicants to be used during the identity-proofing process.

CAs and RAs are responsible for ensuring that they are in compliance with all applicable laws when collecting personally identifiable information. If a jurisdiction prohibits the collection, distribution or storage of any of the information specified in this section, an alternate, equivalent proofing mechanism may be used that assures the identity of the applicant to an equivalent level, subject to approval of the Airbus PMA. If the data is used to proof an identity for medium-software or medium-hardware Assurance Level, this alternate procedure shall be

communicated to external domain PKIs prior to implementation, or as outlined in the MOA with that external domain PKI.

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification; and
- A signed declaration by that person that he or she verified the identity of the applicant as required by this CP which may be met by establishing how the applicant is known to the verifier as required by this CP.

For Basic Assurance Levels, the following information shall be recorded:

1. the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
2. the full name and legal status of the applicant's Employer;
3. an email address for the applicant;
4. a declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4;
5. the date and time of the verification;
6. a declaration signed by the Customer Requestor, authorising the non- Airbus applicant to obtain an Airbus Certificate.

For all Assurance Levels applicable to human Subscribers other than Basic, the following information shall be recorded:

1. the full name, including surname and given name(s) of the applicant, and maiden name, if applicable;
2. the date and place of birth or other attribute(s) which may be used to uniquely identify the applicant;
3. the full name and legal status of the applicant's Employer;
4. a physical address or other suitable method of contact for the applicant;
5. a declaration signed by the applicant indicating his acceptance of the privacy policy outlined in section 9.4;
6. the date and time of the verification;
7. a declaration signed by the Customer Requestor, authorising the non- Airbus applicant to obtain an Airbus Certificate.

For Certificates asserting the Medium Assurance Levels, the applicant shall:

1. present one (1) valid National Government-issued photo ID or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver's License);

2. have recorded as with the above information for all Assurance Levels, unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant; and

3. sign a declaration of identity using a handwritten signature. This shall be performed in the presence of the person performing the identity authentication.

For Certificates asserting Basic Assurance Levels, the applicant's identity can be determined based on a previously established business relationship.

Identity for other Assurance Levels applicable to human Subscribers shall be established by in-person or remote proofing before the RA or Trusted Agent; information provided shall be verified to ensure legitimacy.

Requirements for authentication of individual identity using an in-person antecedent are listed in section 3.2.3.4.

3.2.3.3. Authentication of Component Identities

In the event a human sponsor is changed, the new sponsor shall review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

3.2.3.3.1. For Infrastructure LoAs

For computing and communications components issued Certificates at the Airbus-INFRASTRUCTURE Assurance Level, a standardized mechanism (such as SCEP, or Microsoft AutoEnrollment) may be used to automatically provide Equipment Identification and the Equipment public keys to the CA. All registration information must be traceable to a unique device or component, and be able to be positively associated with the key pair generated by that device, using a suitable proof of possession mechanism.

3.2.3.3.2. For all other Assurance Levels

Some computing and communications components (routers, firewalls, servers, etc.) and other non-human Subscribers (aircraft and/or aircraft equipment or systems, etc.) will be named as Certificate subjects. In such cases, the component (usually referred to as a "device") shall have

a human sponsor (the "Device Sponsor"). The Device Sponsor shall be responsible for providing the following registration information:

- Equipment identification (e.g., serial number, aircraft registration number, equipment part number) or service name (e.g., DNS name) sufficient to unique identify the Subject;
- Equipment Public Keys;
- Equipment authorisations and attributes (if any are to be included in the Certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the Device Sponsor (using Certificates of equivalent or greater assurance than that being requested); or
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of section 3.2.3.1 or 3.2.3.2.

Once this information has recorded by the Device Sponsor, the device may use a standardized mechanism (such as SCEP) to automatically provide the Equipment public keys to the CA, and to allow the CA to provision the issued Certificate to the device. Where SCEP is used, the strength of the challenge password shall meet the requirements for activation data for keys corresponding to the assurance level of the Certificate being issued, and shall be communicated between the Device Sponsor and the CA using a method that provides authentication, integrity and confidentiality commensurate with the Assurance Level of the Certificate being requested. Furthermore, the SCEP server shall implement a mechanism to limit passphrase guessing attacks.

3.2.3.4.Human Subscriber Initial Identity Proofing Via Antecedent Relationship

The following requirements shall apply when human subscriber identity is verified using antecedent relationship with the sponsoring organisation:

1. The applicant shall personally appear before a verifier (usually a Trusted Agent);
2. The applicant and the verifier shall have an established working[5] relationship with the sponsoring organisation. The relationship shall be sufficient to enable the verifier to, with a high degree of certainty, verify that the applicant is the same person that was identity proofed. An example to meet this requirement is when the applicant and Trusted Agents are employed by the same company and the company badge forms the basis for the applicant authentication;
3. The applicant shall present a valid sponsoring organisation-issued photo ID. This photo ID shall have been issued on the basis of in-person identity proofing using one valid

[5] An example of "established working relationship" is the person is employed by the sponsoring organisation. Another example of "established working relationship" is the person is consultant to the sponsoring organisation or is employed by a contractor of the sponsoring organisation.

National Government-issued Picture ID, or two valid non-National Government IDs, one of which shall be a recent photo ID (e.g., Drivers License);

4. The verifier shall record the following:

    a. His/her own identity;

    b. Unique identifying number from the Identifier (ID) of the verifier;

    c. Unique identifying number from the applicant's sponsoring organisation-issued photo ID;

    d. Date and time of the identity verification; and

    e. Date and time of sponsoring organisation-issued photo ID, if applicable.

5. The verifier shall sign a declaration that he or she verified the identity of the applicant as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy; and

6. The applicant shall sign a declaration of identity using a handwritten signature. This declaration shall be signed in the presence of the verifier.

3.2.3.5.Authentication of Human Subscriber for Role Certificates

Human Subscribers may be issued Role Certificates. In addition to the stipulations below, authentication of individuals for Role Certificates shall follow the stipulations of sections 3.2.3.1 or 3.2.3.2 of this CP for Airbus employees or non- Airbus employees, respectively.

A Role Certificate shall identify a specific role on behalf of which the Subscriber is authorized to act rather than the Subscriber's name. A Role Certificate can be used in situations where non-repudiation is desired. A Role Certificate shall not be a substitute for an individual Subscriber Certificate. Each role for which a Role Certificate is to exist shall have a Role Sponsor.

Multiple Subscribers can be assigned to a role at the same time, however, the signature key pair shall be unique to each Role Signature Certificate issued to each individual; the encryption key pair and Role Encryption Certificate may be shared by the individuals assigned the role.

The CA or the RA shall record the information identified in Section 3.2.3 for a Role Sponsor associated with the role before issuing a Role Certificate. The CA or the RA shall validate

from the Role Sponsor that the individual Subscriber has been approved for the Role Certificate.

Subscribers issued Role Certificates shall protect the corresponding role credentials in the same manner as individual credentials.

The procedures for issuing Role Certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organisation affiliation, key generation, private key protection, and Subscriber obligations).

For the Role Signature Certificate:

The individual assigned the role or the Role Sponsor may act on behalf of the Certificate subject for Certificate management activities such as:

- Issuance;
- Renewal;
- Re-key; and
- Revocation.

Issuance of Role Signature Certificates shall require the approval of the Role Sponsor. Renewal and re-key shall require the approval of the Role Sponsor if the validity period is extended beyond that already approved by the Role Sponsor.

For the Role Encryption Certificate:

Only the Role Sponsor may act on behalf of the Certificate subject for Certificate management activities such as:

- Issuance;
- Renewal;
- Re-key; and
- Revocation.

3.2.3.6. Authentication of Human Subscriber for Code Signing Certificates

The registration information shall be verified to an Assurance Level commensurate with the Certificate Assurance Level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the Subscriber (using Certificates of equivalent or greater assurance than that being requested); or
- In person registration by the Subscriber, with the identity of the Subscriber confirmed in accordance with the requirements of section 3.2.3.1 or 3.2.3.2.

3.2.4. Non-verified Subscriber information

Information that is not verified shall not be included in Certificates.

3.2.5. Validation of authority

Prior to issuing cross-certificates, the Airbus PKI PCA shall validate the external PKI domain CA Certificate requestor's authorisation to act in the name of the external PKI domain CA. In addition, the Airbus PKI PCA shall obtain Airbus PMA approval prior to issuing CA Certificates.

Certificates that contain explicit or implicit organisational affiliation shall be issued only after ascertaining the applicant has the authorisation to act on behalf of the organisation in the asserted capacity.

Prior to issuing code signing certificates, the RA shall verify that the Subscriber has authorization to perform code signing.

3.2.6. Criteria for interoperation

Airbus PKI Sub CAs and Airbus PKI PCAs implementing this CP shall certify other CAs (including Cross-Certification) only as authorised by the Airbus PMA. Such an external PKI

domain CA shall adhere to the following requirements before being approved by the Airbus PMA for Cross-Certification:

- Have a CP mapped to and determined by the Airbus PMA to be in conformance with this CP;
- Operate a PKI that has undergone a successful compliance audit pursuant to section 8 of this CP and as set forth in the Subject CA CP;
- Issue Certificates compliant with the profiles described in this CP, and make Certificate status information available in compliance with this CP;
- Provide CA Certificate and Certificate status information to the Relying Parties in compliance with this CP.

3.3.IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1.Identification and authentication for routine re-key

External PKI domain CAs and Subscribers shall be authenticated through use of their current public key Certificates or by using the initial identity-proofing process as described in section 3.2.

Re-key of CAs other than External PKI domain CAs is not permitted.

Further identification and authentication requirements apply according to the Assurance Level, as set forth in the table below.

Assurance level	Further requirements
EADS-INFRASTRUCTURE EADS-INFRASTRUCTURE-256 EADS-INFRA-USER basic-software basic-software-256 basic-hardware basic-hardware-256	No further requirements
medium-software medium-software-256 medium-software-org-256 medium-hardware medium-hardware-256 medium-hardware-org medium-hardware-org-256	The initial identity-proofing process must be carried out at least once every nine (9) years

For external PKI domain CAs, identity shall be re-established through the initial registration process at least once every three (3) years as required by section 3.2.2.

When a current public key Certificate is used for identification and authentication purposes, the expiration date of the new Certificate shall not cause the Certificate Subject to exceed the initial identity-proofing time frames specified in the table and paragraph above, and the assurance level of the new certificate shall not exceed the assurance level of the Certificate being used for identification and authentication purposes.

3.3.2.Identification and authentication for re-key after revocation

After a Certificate has been revoked other than during an update action, the subject (i.e., a CA or an End-Entity) is required to go through the initial registration process described in section 3.2 to obtain a new Certificate.

For Basic (or lower) Assurance Level Certificates, in case of loss, theft or malfunction the new registration process could consider some of the previously provided subscriber information, as still valid (e.g. General Terms and Conditions). Nevertheless the registration authority shall perform the same controls as during the initial registration process.

3.4.IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests shall always be authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's associated Public Key, regardless of whether the Private Key has been compromised.

4.CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

It is the intent of this CP to identify the minimum requirements and procedures that are necessary to support trust in the PKI, and to minimise imposition of specific implementation requirements on the OA, Subscribers, and Relying Parties.

Communication among the CA, RA, Trusted Agent, other parties confirming identities, and subscriber shall have requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the Assurance Level of the Certificate being managed. When cryptography is used, the mechanism shall be at least as strong as the certificates being managed. For example, a web site secured using SSL Certificate issued under medium-software policy and set up with appropriate algorithms and key sizes

satisfies integrity and confidentiality requirements for medium-software Certificate management.

The content of communication shall dictate if some, all, or none of the security services are required.

4.1.CERTIFICATE APPLICATION

4.1.1.Who can submit a Certificate application

4.1.1.1.Application for Organisational Certificates

An RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.2.Application for End-Entity Certificates by an individual

The Subscriber, or an RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.3.Application for End-Entity Certificates on behalf of a device

For EADS-INFRASTRUCTURE and EADS-INFRA-USER Assurance Levels, the Certificate application may be automatically sent to the CA using a standardized mechanism (such as SCEP, or Microsoft AutoEnrollment).

For all other Assurance Levels applicable to non-human Subscribers, the Device Sponsor, who needs to be a Subscriber, or an RA acting on behalf of the Subscriber shall submit a Certificate application to the CA.

4.1.1.4.Application for CA Certificates

For CA-Certificate applications to an Airbus PKI CA, an authorised representative of the Subject CA shall submit the application to the Airbus PMA.

4.1.2.Enrolment process and responsibilities

Applicants for Public Key Certificates shall be responsible for providing accurate information in their applications for certification.

Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties, and shall be described in the applicable CPS.

For CA certificates, the Airbus PMA shall verify all authorisations and other attribute information received from an applicant CA.

4.1.2.1.End-Entity Certificates

The applicant and the RA must perform the following steps when an applicant applies for a Certificate:

- establish and record identity of Subscriber (per section 3.2);
- obtain a public/private Key Pair for each Certificate required; and

- establish that the Public Key forms a functioning Key Pair with the Private Key held by the Subscriber (per section 3.2.1).

For Assurance Levels other than EADS-INFRASTRUCTURE and EADS-INFRA-USER, the applicant and RA must also:

- provide a point of contact for verification of any roles or authorisations requested; and
- verify the authority of the applicant.

These steps may be performed in any order that is convenient for the RA and Subscribers, and that do not defeat security; but all must be completed prior to Certificate issuance.

Any electronic transmission of shared secrets shall be protected (e.g., encrypted, or using a split secret scheme where the parts of the shared secret are sent using multiple, separate channels) using means commensurate with the requirements of the data to be protected by the Certificates being issued.

4.1.2.2.CA Certificates

The Airbus PMA shall make the procedures and application form available to entities requesting issuance of a CA Certificate from an Airbus PKI Sub CA.

An Airbus PKI Root CA shall certify Airbus PKI Sub CAs implementing this CP only as authorised by the Airbus PMA. A CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647], shall accompany the applications of the requesting Airbus PKI Sub CA.

Requests by external PKI domain CAs for CA Certificates from an Airbus PKI PCA shall be submitted to the Airbus PMA using the contact provided in section 1.5.

The Airbus PMA shall evaluate the submitted application in accordance with procedures that it shall develop and publish, and make a determination regarding whether to issue the requested Certificate(s), and what policy mapping to express in the Certificate(s), if applicable[6].

The Airbus PMA shall commission a CPS compliance analysis prior to authorising the OA to issue and manage CA Certificates asserting this CP.

Airbus PKI CAs shall only issue Certificates asserting the OIDs outlined in this CP upon receipt of written authorisation from the Airbus PMA, and then may only do so within the constraints imposed by the Airbus PMA or its designated representatives.

4.2.CERTIFICATE APPLICATION PROCESSING

It is the responsibility of the RA, or, in the case of a CA Certificate, the Airbus PMA, to verify that the information in a Certificate Application is accurate.

This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber's sponsoring organisation. If databases are used to confirm Subscriber information, then these databases must be protected from unauthorized

[6] Note that subordinated CAs (Airbus Group PKI Sub CAs) inheriting this CP do not require policy mapping.

modification to a level commensurate with the level of assurance of the Certificate being sought.

Specifically, the databases shall be protected using physical security controls, personnel security controls, cryptographic security controls, computer security controls, and network security controls specified for the RA elsewhere in this CP.

The applicable CPS shall specify procedures to verify information in Certificate Applications.

4.2.1.Performing identification and authentication functions

Prior to Certificate issuance, a Subscriber shall be required to sign a General Terms and Conditions containing the requirements that the Subscriber shall protect the Private Key and use the Certificate and Private Key for authorised purposes only.

4.2.2.Approval or rejection of Certificate applications

The Airbus PKI CAs, respective RAs, or the Airbus PMA may approve or reject a Certificate application.

For CAs the Airbus PMA may approve or reject a Certificate application.

4.2.3.Time to process Certificate applications

The Certificate application processing from the time the request/application is posted on the CA or RA system to Certificate issuance shall take no more than 30 days.

4.3.CERTIFICATE ISSUANCE

Upon receiving a request to issue a Certificate, the CA shall ensure that there is no deviation in the requested attributes from the information validated as per section 4.2.

The Certificate request may contain an already built ("to-be-signed") Certificate. This Certificate will not be signed until the process set forth in this CP and the respective CPS has been met.

4.3.1.CA actions during Certificate issuance

The CA verifies the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.

The CA shall authenticate a Certificate Request, ensure that the Public Key is bound to the correct Subscriber, obtain a proof of possession of the Private Key, then generate a Certificate, and provide the Certificate to the Subscriber. The CA shall publish the Certificate to a repository

in accordance with this CP and the applicable CPS. This shall be done in a timely manner, which is detailed in section 2.

4.3.2.Notification to Subscriber by the CA of issuance of Certificate

The CA shall notify Subscribers of successful Certificate issuance in accordance with procedures set forth in the applicable CPS.

The Airbus OA shall inform the Airbus PMA of any Certificate issuance to a CA by an Airbus PKI CA. The Airbus PMA shall inform the authorised instance of such applicant CA of the successful Certificate issuance.

Notification of Certificate issuance shall be provided to the Airbus PKI CAs and to cross-certified PKI domains PMAs according to the contractual obligations established through the respective MOA by the Airbus PMA.

4.4.CERTIFICATE ACCEPTANCE

Airbus shall enter into a Memorandum Of Agreement (MOA) with external PKI domains' legal representatives setting forth the respective responsibilities and obligations of both parties. The acceptance procedure for the respective CA Certificates shall be defined in the MOA.

4.4.1.Conduct constituting Certificate acceptance

As part of the Certificate issuance process for Certificates asserting Assurance Levels higher than Basic, a Subscriber shall explicitly indicate acceptance or rejection of the Certificates to the CA as set forth in the respective CPS.

For the issuance of CA Certificates to Airbus PKI Sub CAs the Airbus PMA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

4.4.2.Publication of the Certificate by the CA

Certificates shall be published according to section 2 as soon as they are issued.

4.4.3.Notification of Certificate issuance by the CA to other entities

The Airbus OA shall inform the Airbus PMA of any cross Certificate issuance to an external PKI domain CA by an Airbus PKI PCA.

The Airbus PMA shall inform the authorised representative of such applicant external PKI domain CA of the successful cross Certificate issuance.

Notification of such cross Certificate issuance shall be provided to the Airbus PKI CAs and to cross-certified PKI domains' PMAs according to the contractual obligations established through the respective MOA by the Airbus PMA.

4.5.KEY PAIR AND CERTIFICATE USAGE

4.5.1.Subscriber Private Key and Certificate usage

Subscribers and CAs shall protect their Private Keys from access by any other party, as specified in section 6.2. Use of the Private Key corresponding to the Public Key in the Certificate, aside

from initial proof-of-possession transaction with the CA, shall only be permitted once the Subscriber has agreed to the General Terms and Conditions and accepted the Certificate.

Subscribers shall use the Private Key for Airbus business only, unless other use is explicitly permitted in the applicable General Terms and Conditions.

Subscribers and CAs shall use their Private Keys for the purposes as constrained by the extensions (such as key usage, extended key usage, Certificate Policies, etc.) in the Certificates issued to them. For example, the OCSP Responder Private Key shall be used only for signing OCSP responses.

Subscribers and CAs shall discontinue use of the Private Key following expiration or revocation of the Certificate.

4.5.2.Relying Party Public Key and Certificate usage

Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess the following:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by section 1.4.1 or 1.4.2. CAs and RAs are not responsible for assessing the appropriateness of the use of a Certificate;

- that the Certificate is being used in accordance with the keyUsage, extendedKeyUsage, and certificatePolicies field extensions included in the Certificate; and

- the status of the Certificate and all Certificates in the chain of trust, including revocation status according to section 4.9.6.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilise appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate chain and verifying the digital signatures on all Certificates in the Certificate chain.

In circumstances where a Time Stamping service is used, applications verifying software packages signed with either an organisational (medium-hardware-org, medium-software-org-256, or medium-hardware-org-256) or Role code-signing Certificate used for Aircraft and Spacecraft Software Signature, shall check the timestamp, and shall reject any software package which either does not have a timestamp issued by a recognized Time Stamp Authority, or whose timestamp shows a time later than the time of the check, or whose timestamp shows a time before the 'Valid before' date of the Certificate signing the software package.

4.6.CERTIFICATE RENEWAL

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to reduce the size of CRLs. A Certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. After Certificate renewal, the old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Certificate renewal is only supported by this CP for OCSP, and Cross-Certificates.

4.6.1.Circumstance for Certificate renewal

A Certificate may be renewed if the Public Key has not reached the end of its validity period, the associated Private Key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the Certificate must not exceed

the remaining lifetime of the Private Key, as specified in Section 0. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2.Who may request renewal

A Subject may request the renewal of its Certificate.

A Device Sponsor may request renewal of an OCSP Certificate it has sponsored.

The PMA may request renewal of a PCA's Certificate.

4.6.3.Processing Certificate renewal requests

A Certificate renewal shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.

For Cross-Certificates issued by an Airbus PKI PCA, Certificate renewal also requires that a valid MOA exists between the Airbus PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new Certificate.

4.6.4.Notification of new Certificate issuance to Subscriber

See Section 4.3.2.

4.6.5.Conduct constituting acceptance of a renewal Certificate

See Section 4.4.1.

4.6.6.Publication of the renewal Certificate by the CA

See Section 4.4.2.

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

See Section 4.4.3.

4.7.CERTIFICATE RE-KEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a Certificate means that a new Certificate is created that has the same characteristics and Assurance Level as the old one, except that the new Certificate has a new, different Public Key (corresponding to a new, different Private Key) and a different serial

number, and it may be assigned a different validity period. After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1.Circumstance for Certificate re-key

A CA may issue a new Certificate to the Subject when the Subject has generated a new Key Pair and is entitled to a Certificate.

4.7.2.Who may request certification of a new Public Key

A Subject may request the re-key of its Certificate.

A Role Sponsor may request re-key of Role Signature and Role Encryption Certificates for which he/she is the sponsor.

The individual identified in a Role Signature Certificate may request re-key of his/her Role Signature Certificate.

A Device Sponsor may request re-key of a component Certificate it has sponsored.

An external PKI domain's PMA may request re-key of its cross Certificate.

4.7.3.Processing Certificate re-keying requests

A Certificate re-key shall be achieved using one of the following processes:

- Initial registration process as described in section 3.2; or
- Identification & Authentication for Re-key as described in section 3.3.

For CA Certificates issued to other PKI domains' CAs, Certificate re-keying also requires that a valid MOA exists between Airbus and the PMA of the respective other PKI domain CA, and the term of the MOA is beyond the expiry period for the new Certificate.

For Role Signature Certificates, re-key shall require the approval of the Role Sponsor if the validity period is extended beyond that already approved by the Role Sponsor.

4.7.4.Notification of new Certificate issuance to Subscriber

See section 4.3.2.

4.7.5.Conduct constituting acceptance of a re-keyed Certificate

See section 4.4.1.

4.7.6.Publication of the re-keyed Certificate by the CA

See section 4.4.2.

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

See section 4.4.3.

4.8.CERTIFICATE MODIFICATION

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old

Certificate. For example, an Airbus PKI Sub CA may choose to update a Certificate of a Subscriber whose characteristics have changed (e.g., has been assigned a new email address).

The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or the Trusted Agent in order for an updated Certificate having the new name to be issued, such as by the method described in section 3.2 of this CP.

Certificate modification is only supported by this CP for CA Certificates.

4.8.1. Circumstance for Certificate modification

An Airbus PKI Root CA may issue a new certificate to a Subject CA when some of the Subject information has changed, e.g., change in subject attributes, etc., and the Subject continues to be entitled to a certificate.

4.8.2. Who may request Certificate modification

The Airbus PMA may request modification to an Airbus PKI CA Certificate.

4.8.3. Processing Certificate modification requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2; or
- Identification & Authentication for Re-key as described in Section 3.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2.

For Cross-Certificates issued by an Airbus PKI PCA, Certificate modification also requires that a valid MOA exists between the Airbus PMA and the Subject CA, and the term of the MOA is beyond the expiry period for the new Certificate.

4.8.4. Notification of new Certificate issuance to Subscriber

See Section 4.3.2.

4.8.5. Conduct constituting acceptance of modified Certificate

See Section 4.4.1.

4.8.6. Publication of the modified Certificate by the CA

See Section 4.4.2.

4.8.7. Notification of Certificate issuance by the CA to other entities

See Section 4.4.3.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for revocation

A Certificate shall be revoked when the binding between the subject and the subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the Certificate become invalid;
- An organisation terminates its relationship with the CA such that it no longer provides affiliation information;
- Privilege attributes asserted in the Subject's Certificate are reduced;
- The Subject can be shown to have violated the stipulations of its agreement;
- The Private Key, or the media holding the Private Key, is suspected of compromise; or
- The Subject or other authorised party (as defined in this CP or the respective CPS) asks for his/her Certificate to be revoked.

Whenever any of the above circumstances occur, the associated Certificate shall be revoked and placed on the CRL. Revoked Certificates shall be included on all new publications of the Certificate status information until the Certificates expire.

In addition, if it is determined subsequent to issuance of new Certificates that a private key used to sign requests for one or more additional Certificates may have been compromised at the time the requests for additional Certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked.

4.9.2.Who can request revocation

A Certificate subject, human supervisor of a human subject, Human Resources (HR) person for the human subject, Device Sponsor for a component it has sponsored, issuing CA, or RA may request revocation of a Certificate.

For Role Signature Certificates, revocation may be requested by the individual identified in the Certificate or by the Role Sponsor. Role Encryption Certificate revocation may only be requested by the Role Sponsor.

For a medium-hardware-org, medium-software-org-256, or medium-hardware-org-256 Certificate issued to a Corporation or other Organisation as a whole, revocation may be requested by an authorized representative of the Subject Organisation carrying the appropriate power of attorney, the issuing CA, or RA.

In the case of CA Certificates issued to another PKI domain by an Airbus PKI PCA, the external PKI domain PMA or the Airbus PMA may request revocation of a Certificate.

For CA Certificates, authorised individuals representing the CA Operational Authority may request revocation of Certificates.

Notwithstanding the above, an Airbus PKI CA may, at its sole discretion, revoke any Subscriber or Device Certificate it has issued for reasons outlined in section 4.9.1.

4.9.3.Procedure for revocation request

A request to revoke a Certificate shall identify the Certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

Any CA may unilaterally revoke a CA Certificate it has issued. However, the Operational Authority for Airbus PKI CAs shall revoke a Subject CA Certificate only in the case of an

emergency. Generally, the Certificate will be revoked based on the subject request, authorised representative of subject request, or PMA request.

Upon receipt of a revocation request, a CA shall authenticate the request and then revoke the Certificate. In the case of a CA Certificate issued by the Airbus PKI CAs, the Operational Authority shall seek guidance from the Airbus PMA before revocation of the Certificate except when the Airbus PMA is not available and there is an emergency situation such as:

- Request from the Subject CA for reason of key compromise;
- Determination by the Operational Authority that a Subject CA key is compromised; or
- Determination by the Operational Authority that a Subject CA is in violation of this CP, an applicable CPS, or a contractual obligation to a degree that threatens the integrity of the Airbus PKI.

For Certificates issued by an Airbus PKI Sub CA whose operation involves the use of a cryptographic hardware token, a Subscriber ceasing its relationship with an Airbus organisation (Airbus Business Unit) that sponsored the Certificate shall, prior to departure, surrender to the organisation (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organisation. The token shall be disposed of in

accordance with section 6.2.10 promptly upon surrender and shall be protected from malicious use between surrender and such disposition.

If a Subscriber leaves an organisation (an Airbus Business Unit) and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber Certificates associated with the unretrieved tokens shall be immediately revoked for the reason of key compromise.

4.9.4.Revocation request grace period

There is no revocation grace period. The parties identified in section 4.9.2 must request revocation as soon as they identify the need for revocation.

4.9.5.Time within which CA must process the revocation request

Airbus PKI CAs shall process all revocation requests for CA Certificates within six (6) hours of receipt of request.

For Airbus PKI Sub CAs, processing time for Subscriber Certificate revocation requests shall be as specified below:

Assurance Level	**Processing Time for Revocation Requests**
EADS-INFRASTRUCTURE, EADS-INFRASTRUCTURE-256, EADS-INFRA-USER, basic-software, basic-software-256, basic-hardware, basic-hardware-256	Within thirty-six (36) hours of receipt of request
medium-software, medium-software-256, medium-software-org-256, medium-hardware, medium-hardware-256, medium-hardware-org, medium-hardware-org-256	Before next CRL is generated unless request is received within 2 hours of CRL generation

4.9.6.Revocation checking requirement for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences

for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7.CRL issuance frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

A CA shall ensure that superseded Certificate status information is removed from the PKI Repository upon posting of the latest Certificate status information.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of Certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

The following table provides CRL issuance frequency requirements.

	CRL Issuance Frequency

Routine	At least once every thirty (30) days for off-line roots. At least once every thirty (30) days for off-line Airbus Business Units Intermediate CAs operating at the Infrastructure level of assurance. At least once every twenty-four (24) hours for all others.
Loss or Compromise of Private Key	Within eighteen (18) hours of request for revocation.
CA Compromise	Immediately, but no later than eighteen (18) hours after notification of such compromise.

CAs that issue routine CRLs less frequently than the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs.

Such CAs shall also be required to notify the other cross-certified PKI domains' Operational Authorities upon Emergency CRL issuance. This requirement shall be included in the respective MOA between Airbus and other respective PKI domains' responsible organisations.

For Offline Root CAs that do not issue end-entity Certificates except for internal operations, the nextUpdate field of the CRL shall be less than or equal to thisUpdate plus 45 days.

For all other CAs, the nextUpdate shall be less than or equal to thisUpdate plus 48 hours.

4.9.8.Maximum latency for CRLs

The maximum delay between the time a Subscriber Certificate revocation request is received by a CA and the time that this revocation information is available to Relying Parties shall be no greater than twenty-four (24) hours.

The CRL shall be subject to the repository availability requirements in section 2.1. Care shall be taken by the CA to ensure that the public copy is replaced atomically when it is being updated.

4.9.9.On-line revocation/status checking availability

In addition to CRLs, CAs and Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

If a CA supports on-line revocation/status checking, the latency of Certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.

The OCSP availability requirements shall be specified in the relevant Relying Party Agreement.

4.9.10.On-line revocation checking requirements

The Airbus PKI CAs are not required to operate an OCSP Responder covering the Certificates they issue.

The Airbus PKI Repository shall contain and publish a list of all OCSP Responders operated by the Airbus PKI CAs.

If OCSP is implemented, the service shall comply with the Internet Engineering Task Force (IETF) RFC 2560 to meet security and interoperability requirements.

4.9.11.Other forms of revocation advertisements available

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

Any alternative method must meet the following requirements:

- the alternative method must be described in the applicable approved CPS;
- the alternative method must provide authentication and integrity services commensurate with the Assurance Level of the Certificate being verified.

4.9.12.Special requirements related to key compromise

None beyond those stipulated in section 4.9.7.

4.9.13.Circumstances for suspension

Certificate suspension is not supported by this CP.

4.9.14.Who can request suspension

Not supported.

4.9.15.Procedure for suspension request

Not supported.

4.9.16.Limits on suspension period

Not supported.

4.10.CERTIFICATE STATUS SERVICES

The Airbus PKI is not required to support Server-based Certificate Validation Protocol (SCVP).

4.10.1.Operational characteristics

No stipulation.

4.10.2.Service availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate status service.

4.10.3. Optional features

No stipulation.

4.11. END OF SUBSCRIPTION

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

Unexpired CA Certificates shall always be revoked at the end of subscription.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key escrow and recovery policy and practices

Under no circumstances shall a CA or End-Entity signature key be escrowed by a third-party.

For Airbus PKI CAs that issue encryption certificates, the Airbus PKI key escrow recovery policy and practices shall be described in the Airbus Key Recovery Policy (KRP), compliant with the CertiPath KRP, and its related Key Recovery Practices Statement (KRPS).

4.12.2. Session key encapsulation and recovery policy and practices

This CP neither requires nor prohibits the Airbus PKI to have the capability of recovering session keys. If session keys are recoverable, then the associated policy and practices shall be described in the Airbus Key Recovery Policy (KRP), compliant with the CertiPath KRP, and its related Key Recovery Practices Statement (KRPS).

5.FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1.PHYSICAL CONTROLS

5.1.1.Site location and construction

The location and construction of the facility housing CA and CMS equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorised access to the CA equipment and records.

5.1.2.Physical access

5.1.2.1.CA Physical Access

CA, CSA, and CMS equipment shall always be protected from unauthorised access. The physical security requirements pertaining to CA, CSA, and CMS equipment are:

- Ensure no unauthorised access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers
- Ensure manual or electronic monitoring for unauthorised intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Provide at least three (3) layers of increasing security such as perimeter, building, and CA room
- For CAs asserting:
    - Only Basic and/or lower Assurance Levels: Require controls to physical access and cryptographic modules consistent with those used for commercially sensitive systems.
    - All other Assurance Levels: Require two (2) person physical access control to both the cryptographic module and computer system.
- If a CA shares physical location with a CA of a higher Assurance Level, the CA's physical controls must be as if it were operating at that higher Assurance Level.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be

memorised, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA, CSA, or CMS equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed");
- For off-line CAs and CSA, all equipment other than the PKI Repository is shut down;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorised access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2.RA Equipment Physical Access

RA equipment shall be protected from unauthorised access while the RA cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.3.Power and air conditioning

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a

minimum of six (6) hours operation in the absence of commercial power, to support continuity of operations.

5.1.4.Water exposures

Protection against water exposures shall be in conformance with the Airbus standard data centre procedures.

5.1.5.Fire prevention and protection

Fire prevention and protection means shall be in conformance with the Airbus standard data centre procedures.

5.1.6.Media storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media containing audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7.Waste disposal

Sensitive waste material shall be disposed of in a secure fashion.

5.1.8.Off-site backup

Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored offsite not less than once every seven (7) days. At least one (1) full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup data shall be protected with physical and procedural controls commensurate to that of the operational CA.

5.2.PROCEDURAL CONTROLS

For Airbus PKI CAs operating at EADS-INFRASTRUCTURE or EADS-INFRA-USER Assurance Levels, CA personnel selection, management, discipline and operations shall reflect the commercial best practises for IT management and governance. For Airbus PKI CAs operating at Assurance Levels other than EADS-INFRASTRUCTURE or EADS-INFRA-USER, the stipulations in the remainder of this section apply.

5.2.1.Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that

the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of five roles (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile):

- CA System Administrator – authorised to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
- Officer – authorised to request or to approve Certificates or Certificate revocations.
- Internal Auditor – authorised to view and maintain audit logs.
- Operator – authorised to perform system backup and recovery.
- Audit Operator – authorised to perform technical maintenance operations on audit systems.

The following sections define these and other trusted roles.

5.2.1.1.CA System Administrator

The CA System Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring Certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

CA System Administrators shall not issue Certificates to Subscribers.

5.2.1.2.Officer

The Officer shall be responsible for issuing Certificates; that is:

- Registering new applicants and requesting the issuance of Certificates;
- Verifying the identity of applicants and accuracy of information included in Certificates;
- Approving and executing the issuance of Certificates, and;
- Requesting, approving and executing the revocation of Certificates.

An Officer can be either an Operational Authority Officer when dealing with CA Certificates, or an RA. A Trusted Agent must not act as an Officer.

5.2.1.3.Internal Auditor and Audit Operator

The Internal Auditor shall be responsible for:

- Reviewing and maintaining, audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with the applicable CPSs.

The Audit Operator shall be responsible for:

- The routine operation of the audit and archive equipment and operations such as system backups and recovery or changing recording media in such equipment.
- Performing archiving tasks of audit logs.

5.2.1.4.Operator

The operator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5.Registration Authority

An RA's responsibilities are:

- Verifying identity, pursuant to section 3.2;
- Entering Subscriber information, and verifying correctness;
- Securely communicating requests to and responses from the CA;
- Receiving and distributing Subscriber Certificates.

The RA role is highly dependent on Public Key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.6.CSA Roles

A CSA shall have at least the following roles.

The CSA administrator shall be responsible for:

- Installation, configuration, and maintenance of the CSA;
- Establishing and maintaining CSA system accounts;
- Configuring CSA application and audit parameters, and;
- Generating and backing up CSA keys.

The CSA Internal Auditor shall be responsible for:

- Reviewing and maintaining CSA audit logs;
- Performing or overseeing internal compliance audits to ensure that the CSA is operating in accordance with its CPS;

The operator shall be responsible for the routine operation of the CSA equipment and operations such as system backups and recovery or changing recording media.

The CSA Audit Operator shall be responsible for:

- The routine operation of the audit and archive equipment and operations such as system backups and recovery or changing recording media in such equipment.
- Performing archiving tasks of audit logs.

5.2.1.7.CMS Roles

A CMS shall have at least the following roles which correspond to those listed in section 5.2.1 and are submitted to the same requirements:

1. The CMS Administrators shall be responsible for:
    - Installation, configuration, and maintenance of the CMS;
    - Establishing and maintaining CMS system accounts;
    - Configuring CMS application and audit parameters; and
    - Generating and backing up CMS keys.
2. The CMS Internal Auditor shall be responsible for:
    - Reviewing and maintaining audit logs; and
    - Performing or overseeing internal compliance audits to ensure that the CMS is operating in accordance with the applicable CPSes.
3. The CMS Operators shall be responsible for:
    - The routine operation of the CMS equipment; and
    - Operations such as system backups and recovery or changing recording media.
4. The CMS Audit Operators shall be responsible for:
    - The routine operation of the CMS audit and archive equipment; and
    - Operations such as system backups and recovery or changing recording media in such equipment.
    - Performing archiving tasks of audit logs.

5.2.1.8.Device Sponsor

A Device Sponsor fills the role of a Subscriber for non-human system components that are named as Public Key Certificate subjects for Certificates of Assurance Levels other than EADS-INFRASTRUCTURE. The Device Sponsor works with the RAs to register components (routers,

firewalls, etc.) in accordance with section 3.2.3.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

A Device Sponsor need **not** be a Trusted role, but should have been issued a credential that is equal to or higher Assurance Level than the credential that they are sponsoring.

5.2.1.9.Trusted Agent

A Trusted Agent is responsible for:

- Verifying identity, pursuant to section 3.2; and
- Securely communicating Subscriber information to the RA.

A Trusted Agent is NOT a trusted role.

5.2.1.10. Role Sponsor

A Role Sponsor is a Subscriber responsible for the management activities pertaining to the Role Certificates for which he/she is the sponsor. The Role Sponsor shall hold an individual Certificate in his/her own name issued by the same CA at the same or higher assurance level as

the Role Certificate being requested for Subscribers. The Role Sponsor need not hold a Role Certificate.

In addition, the Role Sponsor shall be responsible for:

- Authorizing individuals for a Role Certificate;
- Recovery of private decryption keys associated with Role Encryption Certificates;
- Revocation of individual Role Certificates;
- Always maintaining a current up-to-date list of individuals who have been issued Role Certificates; and
- Always maintaining a current up-to-date list of individuals who have been provided decryption private keys associated with Role Encryption Certificates.

A Role Sponsor is NOT a trusted role.

5.2.2.Number of persons required per task

Two (2) or more persons shall be required to perform the following tasks:

- CA and CSA key generation;
- CA and CSA key activation;
- CA and CSA key backup.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1.

Multiparty control shall not be achieved using personnel that serve in an Internal Auditor or Audit Operator role.

It is recommended that multiple persons are assigned to all roles in order to support continuity of operations.

5.2.3.Identification and authentication for each role

An individual in a trusted role shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role.

An individual in a trusted role shall authenticate to remote components of the PKI using a method commensurate with the strength of the PKI.

All Trusted Roles who operate a CMS which manages certificates issued by the AIRBUS Enterprise SHA2 CAs shall be allowed access only when authenticated using a method commensurate with at least medium-hardware requirements.

5.2.4.Roles requiring separation of duties

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Individual CA, CSA and CMS personnel shall be specifically designated to the five roles defined in section 5.2.1 above. Individuals may assume more than one role, except:

- Individuals who assume an Officer role may not assume an Administrator role;
- Individuals who assume an Internal Auditor or Audit Operator role shall not assume any other role; and
- Under no circumstances shall any of the five roles perform its own compliance auditor function.

An individual fulfilling the role of Trusted Agent shall not hold any other role within the same CA, and shall not perform its own compliance auditor function.

No individual fulfilling any of the roles outlined in section 5.2.1 shall be assigned more than one identity.

5.3.PERSONNEL CONTROLS

For Airbus PKI CAs operating at EADS-INFRASTRUCTURE or EADS-INFRA-USER Assurance Levels, CA personnel selection, management, discipline, and operations shall reflect the commercial best practises for IT management and governance.

For Airbus PKI CAs operating at Assurance Levels other than EADS-INFRASTRUCTURE or EADS-INFRA-USER the stipulations in the remainder of this section apply.

5.3.1.Qualifications, experience, and clearance requirements

A group of individuals responsible and accountable for the operation of each CA, CSA and CMS shall be identified. The trusted roles of these individuals per section 5.2.1 shall be identified.

All persons filling trusted roles and the Trusted Agent role shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation to the extent allowed by law. Personnel appointed to trusted roles or the Trusted Agent role shall:

- Have successfully completed an appropriate training program;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere or conflict with their duties for the role;
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance, or had a security clearance revoked for cause;
- Have not been convicted of a serious crime or other offence which affects his/her suitability for the position; and
- Be appointed in writing by an approving authority.

For CAs issuing Certificates at Medium or higher Assurance Levels, each person filling a trusted role shall satisfy the following two requirements:

- One of:
    - The person shall be a citizen of the country where the CA is located; or

    - For CAs located within the European Union, the person shall be a citizen of one of the member states of the European Union;

- For jurisdictions where obtaining a suitable criminality check or financial verification is not possible, CA/CSA/CMS System Administrators, Internal Auditors, Audit Operators, CA/CSA/CMS Operators, and RA Trusted Roles shall have a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) - 22 CFR 120.32.

Trusted Agents participating in the issuance process for Certificates at Medium or higher Assurance Levels must pass a background check consistent with that outlined in section 5.3.2.

For RAs, Trusted Agents, and personnel appointed to the trusted roles for the CSAs, in addition to the above, the person may be a citizen of the country where the function is located.

If a given CA shall only be operating at a Basic Assurance Level (or only at any lower Assurance Level), it is permissible for the trusted roles for that CA not to have any specific clearance or qualification beyond those normally applied to hiring employees of Airbus, or of those normally stipulated for Airbus contractors, providing that any such trusted roles do not have any access, privilege or permission on any CA operating at any other Assurance Level higher than the given Basic Assurance Level (or the given lower Assurance Level), and that any component of the Basic (or lower) Assurance Level CA does not share a physical or logical location with a CA of any other Assurance Level higher than itself.

5.3.2. Background check procedures

All persons filling CA trusted roles, CSA trusted roles, CMS trusted roles, and RA roles shall have completed a background investigation as allowed by applicable national law or regulation.

The scope of the background check shall include the following areas covering the past five (5) years and should be refreshed every five (5) years:

- Employment;
- Education (Regardless of the date of award, the highest educational degree shall be verified);
- Place of residence;
- Law Enforcement in accordance with applicable law; and
- References

Adjudication of the background investigation shall be performed in accordance with the requirements of the appropriate national adjudication authority.

The results of these checks shall not be released except as required in sections 9.3 and 9.4.

Background check procedures shall be described in the CPS.

5.3.3.Training requirements

All personnel performing duties with respect to the operation of a CA, CSA, CMS, or an RA shall receive comprehensive training.

Training shall be conducted in the following areas:

- CA/CSA/CMS/RA security principles and mechanisms
- All PKI software versions in use on the CA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4.Retraining frequency and requirements

Individuals responsible for trusted roles shall be aware of changes in the CA, CSA, CMS, or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such

changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5.Job rotation frequency and sequence

No stipulation.

5.3.6.Sanctions for unauthorised actions

The responsible PMA shall ensure appropriate administrative and disciplinary actions are taken against personnel who violate this policy in accordance with the local labour laws.

5.3.7.Independent contractor requirements

Sub-Contractor personnel employed to perform functions pertaining to CA, CSA, CMS, or RA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of section 5.3).

5.3.8.Documentation supplied to personnel

The CA, CSA, and CMS shall make available to its personnel the Certificate Policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

5.4.AUDIT LOGGING PROCEDURES

No stipulations for Airbus PKI CAs operating only at the EADS-INFRASTRUCTURE Assurance Level.

For Airbus PKI CAs operating at Assurance Levels other than only EADS-INFRASTRUCTURE, the stipulations in the remainder of this section apply.

Audit log files shall be generated for all events relating to the security of the CAs, CSAs, CMSes, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during

compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.5.2.

5.4.1.Types of events recorded

All security auditing capabilities of the CA, CSA, CMS, and RA operating system and the CA, CSA, CMS, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded.

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- A message from any source requesting an action by a CA is an auditable event. The message must include message date and time, source, destination and contents.

The following events shall be audited:

Auditable Event	CA	CSA	RA	CMS
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	X
Any attempt to delete or modify the Audit logs	X	X	X	X
Obtaining a third-party time-stamp	X	X	X	X
IDENTITY-PROOFING				
Successful and unsuccessful attempts to assume a role	X	X	X	X
The value of maximum number of authentication attempts is changed	X	X	X	X
The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	X
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	X
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	X	X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	X	X	X	X
DATA EXPORT AND OUTPUT				

Auditable Event	CA	CSA	RA	CMS
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	X
KEY GENERATION				
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component Private Keys	X	X	X	X
All access to Certificate subject Private Keys retained within the CA for key recovery purposes	X	N/A	N/A	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication	X	X	X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION				
All Certificate requests	X	N/A	X	X
CERTIFICATE REVOCATION				
All Certificate revocation requests	X	N/A	X	X
CERTIFICATE STATUS CHANGE APPROVAL				

Auditable Event	CA	CSA	RA	CMS
The approval or rejection of a Certificate status change request	X	N/A	N/A	X
CA CONFIGURATION				
Any security-relevant changes to the configuration of the Component	X	X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	-	-	X
The access control privileges of a user account or a role are modified	X	-	-	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the Certificate profile	X	N/A	N/A	X
CERTIFICATE STATUS AUTHORITY MANAGEMENT				
All changes to the CSA profile (e.g. OCSP profile)	N/A	X	N/A	N/A
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	X	N/A	N/A	N/A
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the Certificate revocation list profile	X	N/A	N/A	N/A
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	X	X	X	X
Designation of personnel for multiparty control	X	-	N/A	X
Installation of the Operating System	X	X	X	X

Auditable Event	CA	CSA	RA	CMS
Installation of the PKI Application	X	X	X	X
Installation of hardware cryptographic modules	X	X	X	X
Removal of hardware cryptographic modules	X	X	X	X
Destruction of cryptographic modules	X	X	X	X
System Start-up	X	X	X	X
Logon attempts to PKI Application	X	X	X	X
Receipt of hardware / software	X	X	X	X
Attempts to set passwords	X	X	X	X
Attempts to modify passwords	X	X	X	X
Back up of the internal CA database	X	-	-	X
Restoration from back up of the internal CA database	X	-	-	X
File manipulation (e.g., creation, renaming, moving)	X	-	-	-
Posting of any material to a PKI Repository	X	-	-	-
Access to the internal CA database	X	X	-	-
All Certificate compromise notification requests	X	N/A	X	X
Loading tokens with Certificates	X	N/A	X	X
Shipment of Tokens	X	N/A	X	X
Zeroising Tokens	X	N/A	X	X
Re-key of the Component	X	X	X	X

Auditable Event	CA	CSA	RA	CMS
CONFIGURATION CHANGES				
Hardware	X	X	-	X
Software	X	X	X	X
Operating System	X	X	X	X
Patches	X	X	-	X
Security Profiles	X	X	X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing Component	X	-	-	X
Access to the Component	X	X	-	X
Known or suspected violations of physical security	X	X	X	X
ANOMALIES				
Software error conditions	X	X	X	X
Software check integrity failures	X	X	X	X
Receipt of improper messages	X	X	X	X
Misrouted messages	X	X	X	X
Network attacks (suspected or confirmed)	X	X	X	X
Equipment failure	X	-	-	X
Electrical power outages	X	-	-	X
Uninterruptible Power Supply (UPS) failure	X	-	-	X

Auditable Event	CA	CSA	RA	CMS
Obvious and significant network service or access failures	X	-	-	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operating System clock	X	X	X	X

5.4.2.Frequency of processing log

Audit logs shall be reviewed at least once every thirty (30) days.

Statistically significant sample of security audit data generated by the CA, CSA, CMS, or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. The Internal Auditor shall explain all significant events in an audit log summary.

Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Actions taken as a result of these reviews shall be documented.

5.4.3.Retention period for audit log

Audit logs shall be retained onsite for at least sixty (60) days as well as being retained in the manner described in section 5.5. For the CA, CSA, and CMS, the Internal Auditor shall be the only role responsible to review the audit log, while the Audit Operator shall be the only role responsible to manage the audit log (e.g., backup, archive, rotate, delete, etc.). For RA, a System Administrator other than the RA shall be responsible for managing the audit log.

5.4.4.Protection of audit log

System configuration and procedures shall be implemented together to ensure that:

- Only authorised people have read access to the logs. For the CA, CMS, and CSA, the authorised individual shall be the Internal Auditor (for review) or Audit Operator (for

backup and other management). For an RA, the authorised individual shall be a system administrator other than the RA;

- Only authorised people may archive audit logs; and,
- Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

Audit logs shall be moved to a safe, secure storage location separate from the CA equipment.

It is acceptable for the system to over-write audit logs after they have been backed up and archived.

5.4.5.Audit log backup procedures

Audit logs and audit summaries shall be backed up at least once every thirty (30) days. A copy of the audit log shall be sent off-site in accordance with the CPS every thirty (30) days.

5.4.6.Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the CA, CSA, CMS, or RA. Audit processes shall be invoked at system start-up, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or

confidentiality of the information protected by the system is at risk, then the CA shall determine whether to suspend CA operation until the problem is remedied.

5.4.7. Notification to event-causing subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organisation, device, or application that caused the event.

5.4.8. Vulnerability assessments

No stipulation beyond section 5.4.2.

5.5. RECORDS ARCHIVAL

No stipulations for Airbus PKI CAs operating at EADS-INFRASTRUCTURE or EADS-INFRA-USER Assurance Levels.

For Airbus PKI CAs operating at Assurance Levels other than EADS-INFRASTRUCTURE or EADS-INFRA-USER, the stipulations in the remainder of this section apply.

5.5.1. Types of records archived

CA, CSA, CMS, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any Certificate (including those revoked or expired) issued by the CA.

Data To Be Archived	RootCA/CA	CSA	RA	CMS
Certification Practice Statement	X/X	X	X	X
Contractual obligations	X/X	X	X	X
System and equipment configuration	X/X	X	-	X
Modifications and updates to system or configuration	X/X	X	-	X
Certificate requests	X/X	-	-	X
Revocation requests	X/X	-	-	X
Subscriber identity authentication data as per section 3.2.3	N/A / X	N/A	X	X
Documentation of receipt and acceptance of Certificates, including Subscriber Agreements	X/X	N/A	X	X
Documentation of receipt of Tokens	N/A / X	N/A	X	X
All Certificates issued or published	X/X	N/A	N/A	X
Certificate Policy	X	X	X	X
Record of Component CA Re-key	N/A / N/A	X	X	X
All CRLs and CRLs issued and/or published	X/X	N/A	N/A	N/A
All Audit Logs	X/X	X	X	X
Other data or applications to verify archive contents	X/X	X	X	X
Documentation required by compliance auditors	X/X	X	X	X
Compliance Audit Reports	X	X	X	X

5.5.2.Retention period for archive

The retention period for archive data shall depend on the legal and business requirements and is set forth in the respective CPS. However, the archive data must be kept for a minimum retention period of fifteen (15) years. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications required processing the archive data shall also be maintained for the minimum retention period specified above.

5.5.3.Protection of archive

No unauthorised user shall be permitted to write to, modify, or delete the archive. For the CA, CSA, and CMS, the authorised individuals are Internal Auditors and Audit Operators. For the RA digital archives, authorised individuals are someone other than the RA. The contents of the archive shall not be released except as determined by the Airbus PMA for the Airbus PKI CAs, or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognised agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSA, CMS, or RA) with physical and procedural security controls equivalent or better than those for the component. The archive shall also be adequately protected from environmental threats such as temperature, humidity, radiation, and magnetism.

5.5.4.Archive backup procedures

Adequate and regular backup procedures shall be in place so that in the event of loss or destruction of the primary archives, a complete set of backup copies held in a separate location will be available. The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5.Requirements for time-stamping of records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6.Archive collection system (internal or external)

No stipulation.

5.5.7.Procedures to obtain and verify archive information

Procedures detailing how to create, verify, package, transmit and store archive information shall be published in the applicable CPS.

5.6.KEY CHANGEOVER

To minimise risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates

signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

The following table provides the life times for Certificates and associated Private Keys.

Key	2048 Bit Keys		4096 Bit Keys	
	Private Key	Certificate	Private Key	Certificate
Airbus PKI Root CAs	20 years	20 years	20 years	20 years
Airbus PKI Sub CAs	5 years	10 years	10 years	13 years
Airbus PKI BU Intermediate CAs	5 years	10 years	10 years	13 years
Subscriber Identity or Signature	3 years	≤ 3 years	3 years	≤ 3 years
Subscriber Encryption	n/a	≤ 3 years	n/a	≤ 3 years
Role Signature	3 years	≤ 3 years	3 years	≤ 3 years
Role Encryption	n/a	≤ 3 years	n/a	≤ 3 years
Organisational Subscriber Signature	3 years	≤ 3 years	3 years	≤ 3 years
Code Signer	3 years	≤ 8 years	3 years	≤ 8 years
Organisational Code Signer	3 years	≤ 8 years	3 years	≤ 8 years
Time Stamping Services Signed by root CA	3 years	≤ 20 years	3 years	≤ 20 years
Time Stamping Services signed by signing CA	3 years	≤ 10 years	3 years	≤ 13 years
Server, Device or Aircraft Component Identity or Signature	3 years	≤ 3 years	3 years	≤ 3 years
Server, Device or Aircraft Component Encryption	n/a	≤ 3 years	n/a	≤ 3 years

OCSP Responders	3 years	1 month	3 years	1 month

A CA cannot generate a Certificate for a Subscriber whose validity period would be longer than the CA Certificate validity period. As a consequence, the CA Key Pair shall be changed at the latest at the time of CA Certificate expiration minus Subscriber Certificate validity duration.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and compromise handling procedures

If a CA or CSA detects a potential cracking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA or CSA key is suspected of compromise, the procedures outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA or CSA needs to be rebuilt, only some Certificates need to be revoked, and/or the CA or CSA key needs to be declared compromised.

The Airbus PMA members shall be notified if any of the following cases occur:

- suspected or detected compromise of an Airbus PKI CA system;
- physical or electronic attempts to penetrate an Airbus PKI CA system;
- denial of service attacks on an Airbus PKI CA component;
- any incident preventing an Airbus PKI CA from issuing a CRL within twenty-four (24) hours of the time specified in the next update field of its currently valid CRL.

The Airbus PMA members and other domain PKI (who entered a MOA with the Airbus) PMA members shall be notified if any of the following cases occur:

- Revocation of a relevant CA certificate, such as for a CA cross-certified with the other domain's PKI, is planned;
- any incident preventing such a relevant CA from issuing a CRL within twenty-four (24) hours of the time specified in the next update field of its currently valid CRL.

This will allow the other PKI domains to protect their interests as Relying Parties.

The CA Operational Authority shall re-establish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The CMS shall have documented incident-handling procedures that are approved by the head of the organisation responsible for operating the CMS. If the CMS or CMS keys are compromised, all Certificates issued to the CMS shall be revoked, if applicable. The damage caused by the CMS compromise shall be assessed and all Subscriber Certificates that may have been compromised shall be revoked, and Subscribers shall be notified of such revocation. The CMS shall be re-established.

5.7.2.Computing resources, software, and/or data are corrupted

If a CA or CSA equipment is damaged or rendered inoperative, but the signature keys are not destroyed; the operation shall be re-established as quickly as possible, giving priority to the ability to generate Certificate status information. Before returning to operation, ensure that the system's integrity has been restored.

If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA shall be securely[7] notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties.

If the ability to revoke Certificates is inoperative or damaged, the CA shall re-establish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's revocation capability cannot be established in a reasonable time-frame, the CA shall determine whether to request revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all Subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3.Entity Private Key compromise procedures

If a CA's signature keys are compromised, lost, or suspected to be compromised:

- All cross certified CAs shall be securely notified at the earliest feasible time (so that entities may issue CRLs revoking any cross-certificates issued to the CA);
- A new CA Key Pair shall be generated by the CA in accordance with procedures set forth in the applicable CPS;
- New CA Certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
- The CA shall request all subscribers to re-key using the procedures outlined in section 3.3.2; and
- If the CA is an Airbus PKI Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The Airbus PMA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a CSA key is compromised, all Certificates issued to the CSA shall be revoked, if applicable. The CSA will generate a new Key Pair and request new Certificate(s), if applicable. As a CSA

[7] With confidentiality, source authentication, and integrity security services applied.

operated by the Airbus PKI may not be a trust anchor, there are no specific requirements regarding trust anchor propagation.

If a CMS key is compromised, incident handling procedures as per section 5.7.1 apply.

If an RA signature keys are compromised, lost, or suspected to be compromised:

- The RA Certificate shall be immediately revoked;
- A new RA Key Pair shall be generated in accordance with procedures set forth in the applicable CPS;
- A new RA Certificate shall be requested in accordance with the initial registration process set elsewhere in this CP;
- All Certificate registration requests approved by the RA since the date of the suspected compromise shall be reviewed to determine which ones are legitimate; and
- For those Certificate requests or approvals that cannot be ascertained as legitimate, the resultant Certificates shall be revoked and their subjects (i.e., Subscribers) shall be notified of revocation.

5.7.4.Business continuity capabilities after a disaster

In the case of a disaster whereby all of a CA's installations are physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its Certificates be revoked. The CA shall follow steps 2 through 5 in section 5.7.3 above.

5.8.CA, CMS, CSA, OR RA TERMINATION

In the event of termination of a CA, the CA shall request all Certificates issued to it be revoked.

In the event of a CA termination, the Airbus PMA shall provide notice to all cross certified CAs prior to the termination. Additionally, in the case of an Airbus PKI Root CA or Airbus PKI Sub CA termination, cross-certified PKIs will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

A CA, CMS, CSA, and RA shall archive all audit logs and other records prior to termination.

A CA, CMS, CSA, and RA shall destroy all its Private Keys upon termination.

CA, CMS, CSA, and RA archive records shall be transferred to an appropriate authority such as the PMA responsible for the entity.

If an Airbus PKI Root CA is terminated, the Airbus PKI Root CA shall use secure means to notify the Subscribers to delete all trust anchors representing the terminated Airbus PKI Root CA.

6.TECHNICAL SECURITY CONTROLS

6.1.KEY PAIR GENERATION AND INSTALLATION

Subject Public Keys shall meet the following requirements:

- RSA keys
    - Algorithm OID: rsaEncryption {1 2 840 113549 1 1 1}
    - Parameters: NULL
    - Modulus *n* and Public Exponent *e* where:
        - *n* is 2048, 3072, or 4096 bits; and
        - $2^{16} < e < 2^{256}$
- ECC keys
    - Algorithm OID: ecPublicKey {1 2 840 10045 2 1}
    - Parameters:
        - namedCurve NIST-P256 {1 2 840 10045 3 1 7}; or
        - namedCurve NIST-P384 {1 3 132 0 34}; or
        - namedCurve BrainpoolP384r1 {1 3 36 3 3 2 8 1 1 11}
    - Subject public key: uncompressed EC point

6.1.1.Key pair generation

The following table provides the requirements for Key Pair generation for the various entities.

Entity	FIPS 140-2 Level	Hardware or Software	Key Storage Restricted to the Module on which the Key Was Generated
CA	3	Hardware	Yes
CMS	2	Hardware	Yes
RA	2	Hardware	Yes
OCSP Responder	2	Hardware	Yes
Code Signing (basic-software, basic-software-256)	No requirements	Software	No Requirement
Code Signing (medium-software, medium-software-256)	1	Software	No Requirement
Code Signing (medium-hardware, medium-hardware-256)	2	Hardware	Yes
EADS-INFRASTRUCTURE, EADS-INFRASTRUCTURE-256 EADS-INFRA-USER	No requirements	Software / hardware	No Requirement
basic-software, basic-software-256	No requirements	Software	No Requirement
basic-hardware, basic-hardware-256	No requirements	Hardware	No Requirement
medium-software, medium-software-256, medium-software-org-256	1	Software	No Requirement
medium-hardware, medium-hardware-256, medium-hardware-org, medium-hardware-org-256	Aircraft Signature, Authentication or Encryption: No Requirement Others: 2	Hardware	Device or Aircraft Encryption: No Requirement Others: Yes

EADS-INFRA-USER	No requirements	Software / hardware	No Requirement

Random numbers for medium-hardware, medium-hardware-256, medium-hardware-org, and medium-hardware-org-256 Assurance Level keys shall be generated in FIPS 140-2 Level 2 validated hardware cryptographic modules.

When Private Keys are not generated on the token to be used, originally generated Private Keys shall be destroyed after they have been transferred to the token. This does not prohibit the key generating modules to further act as the key escrow module.

Multiparty control shall be used for CA Key Pair generation, as specified in section 5.2.2.

The CA Key Pair generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

Activation of the CMS Master Key shall require strong authentication of Trusted Roles. Key diversification operations by the CMS shall also occur on the CMS hardware cryptographic module. For CMSs, the diversification master keys shall be stored in hardware cryptographic modules that support the highest Assurance Level of smartcards managed by that CMS. CMS Master Key and diversification master keys shall be protected from unauthorized disclosure and distribution. Card management shall be configured such that only the authorized CMS can manage issued cards.

6.1.2.Private key delivery to Subscriber

CAs shall generate their own Key Pair and therefore do not need Private Key delivery.

If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the Private Key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or may be

delivered on a hardware cryptographic module. In all cases, the following requirements shall be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber.
- The Private Key shall be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the Private Key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module shall be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of Private Keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the Private Key. Activation data shall be delivered using a separate secure channel.

The CA or the RA shall maintain a record of the Subscriber acknowledgement of receipt of the token.

6.1.3.Public key delivery to Certificate issuer

Where the Subscriber or RA generates Key Pairs, the Public Key and the Subscriber's identity shall be delivered securely to the CA for Certificate issuance. The delivery mechanism shall

bind the Subscriber's verified identity to the Public Key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the Certificate.

6.1.4.CA Public Key delivery to Relying Parties

The Public Key of a trust anchor shall be provided to the Subscribers acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

- The CA loading a trust anchor onto tokens delivered to Subscribers via secure mechanisms;
- Secure distribution of a trust anchor through secure out-of-band mechanisms;
- Comparison of Certificate hash (fingerprint) against trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); or
- Loading trust anchor from web sites secured with a currently valid Certificate of equal or greater Assurance Level than the Certificate being downloaded and the trust anchor is not in the certification chain for the Web site Certificate.

6.1.5.Key sizes

If the Airbus PMA determines that the security of a particular algorithm may be compromised**,** it may require the CAs to revoke the affected Certificates. External PKI domains PMA may require Airbus PKI CAs to revoke the affected Certificates, according to the applicable MOA.

All Certificates, CRLs and protocols used by the PKI (e.g., Transport Layer Security (TLS)) shall use the following algorithm suites for the time periods indicated (following NIST SP800-57):

Cryptographic Function	Expire on or before 12/31/2010	Expire after 12/31/2010 but before 12/31/2030	Expire after 12/31/2030
Signature	1024 bit RSA per FIPS 186-3 For ECDSA, per FIPS 186-3, 193 bit prime field or 163 bit binary field	2048, 3072, or 4096 bit RSA per FIPS 186-3 For ECDSA, per FIPS 186-3, 224, 256, or 384 bit prime field or 233 or 283 bit binary field	3072 or 4096 bit RSA per FIPS 186-3 For ECDSA, per FIPS 186-3, 256 or 384 bit ECDSA prime field, or 283 bit ECDSA binary field
Hashing	SHA-1	SHA-1 for certificates issued before 1/1/2011; SHA-1 or SHA-256 for certificates issued on or after 1/1/2011 but before 1/1/2014; SHA-256 for all certificates asserting the "-256" policy OIDs; SHA-256 for all certificates and CRLs issued on or after 1/1/2014 (i.e. only certificates asserting the "-256" policy OIDs will be issued)	SHA-256 or SHA-384

Public Key Encryption	1024 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 193 bit prime field or 163 bit binary field	2048, 3072, or 4096 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 224, 256, or 384 bit prime field or 233 or 283 bit binary field	3072 or 4096 bit RSA per PKCS 1 For ECDH, per SP 800-56A, 256 or 384 bit ECDSA prime field, or 283 bit ECDSA binary field
Symmetric Encryption	3 Key TDES or AES	3 Key TDES or AES	AES

Regardless, all CAs shall use 2048 bit RSA, or 256 bit prime field or 283 bit binary field, or stronger.

A CA or OCSP responder whose certificate is signed using SHA-256 or SHA-384 shall not use SHA-1 in its signatures, or rely on signatures using SHA-1.

6.1.6.CSAs shall use the same signature algorithms, key sizes, and hash algorithms as used by the relevant CA to sign its CRL.Public key parameters generation and quality checking

RSA keys shall be gnerated in accordance with FIPS 186-3 (except for certificates at the Basic or lower Assurance Levels).

ECDSA and ECDH keys shall be generated in accordance with FIPS 186-3. Only curves from FIPS 186-3 and Brainpool curves shall be used.

6.1.7.Key usage purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage extension in the X.509 Certificate. The Certificate Profiles in section 10 specify the allowable values for this extension for different types of Certificates issued by the Airbus PKI CAs. This rule excludes certificates issued under Infrastructure or INFRA-USER levels of assurance. A specific document will be kept up to date by the OAA to keep track of the different certificate profiles created at infrastructure or INFRA-USER levels of assurance. Organisational or Code-Signing Certificates asserting the nonrepudiation keyUsage must only be used in conjunction with an RFC 3161 compliant TSA.

CA Certificates shall set the cRLSign and certSign bits.

Public keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure Sockets

Layer) that provide authenticated connections using key management Certificates and require setting both digitalSignature and keyEncipherment bits to be set.

For End Entity certificates, the Extended Key Usage extension shall always be present and shall not contain anyExtendedKeyUsage {2.5.29.37.0}.

The extended key usage shall meet the requirements stated in section 10.7. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

6.2.PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1.Cryptographic module standards and controls

The relevant standards for cryptographic modules are FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*. The Airbus PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards shall be published by the Airbus PMA. Cryptographic modules shall be validated to the FIPS 140-2 level identified in section 6.1, or validated, certified, or verified to requirements published by the Airbus PMA; when a Private Key is used in a Qualified Certificate with SSCD context, it must also comply with CEN CWA 14169. Additionally, the Airbus PMA reserves the right to review technical

documentation associated with any cryptographic modules under consideration for use by the CAs.

The table in section 6.1.1 summarises the minimum requirements for cryptographic modules; higher levels may be used. In addition, Private Keys shall not exist outside the Cryptographic Module in plaintext form.

6.2.2.Private key (n out of m) multi-person control

Use of a CA private signing key and CSA private signing key shall require action by at least two (2) persons.

6.2.3.Private key escrow

Under no circumstances shall a third party escrow any signature key.

End-Entity Private Keys used solely for decryption shall be escrowed prior to the generation of the corresponding Certificates, with the exception of decryption Private Keys associated with aircraft and/or aircraft equipment encryption Certificates which do not need to be escrowed.

6.2.4.Private key backup

6.2.4.1.Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multi-person control as used to generate and protect the original signature key. A single backup copy of the signature key shall be stored at or near the CA location.

A second backup copy shall be kept at the CA backup location.

Procedures for CA private signature key backup shall be included in the appropriate CPS and shall meet the multiparty control requirement of section 5.2.2.

6.2.4.2.Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting the basic-software, basic-software-256, medium-software, or medium-software-256 may be backed up or copied, but must be held in the Subscriber's control. Storage must ensure security controls consistent with the protection provided by the subscriber's Cryptographic Module.

Subscriber private signature keys whose corresponding Public Key is contained in a Certificate asserting an Assurance Level other than those listed above shall not be backed up or copied.

6.2.4.3.CSA Private Key Backup

If backed up, the CSA private signature keys shall be backed up under the same single or multi-person control as used to generate the CSA private signature key, and shall be accounted for and protected in the same manner as the original. A single backup copy of the CSA private signature key may be stored at or near the CSA location. A second backup copy may be kept at

the CSA backup location. Procedures for CSA private signature key backup shall be included in the appropriate CPS.

6.2.5.Private key archival

Private signature keys shall not be archived.

6.2.6.Private key transfer into or from a cryptographic module

CA, CSA, and CMS Private Keys shall be generated by and remain in an approved cryptographic module.

The CA, CSA, and CMS Private Keys may be backed up in accordance with section 6.2.4.1.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7.Private key storage on cryptographic module

The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module. Private Keys must be stored on a cryptographic module at least as strong as that referenced in section 6.1.1 for that key's generation.

6.2.8.Method of activating Private Key

The user of a cryptographic module must be authenticated to the cryptographic module before the activation of any Private Key(s), except as indicated below. Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9.Method of deactivating Private Key

The cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorised access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. CA, CSA, and CMS hardware cryptographic modules shall be removed and stored in a secure container when not in use. Hardware cryptographic modules used by RAs shall be removed and either stored in a secure container or kept on the person of the RA when not in use.

6.2.10.Method of destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be done by overwriting the data. For hardware cryptographic modules, this

usually requires executing a "zeroise" command. Physical destruction of hardware is generally not required.

6.2.11. Cryptographic Module Rating

See section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

The Public Key is archived as part of the Certificate archival.

6.3.2. Certificate operational periods and Key Pair usage periods

See section 5.6.

6.3.3. Corporate/Organisational or Role-Based Aircraft and Spacecraft Code Signing Certificate Keys

If this Certificate is issued to a Corporation or Organisation as a whole, the Subscribers and/or Subscriber's Employers must keep a log stating possession of the Private Key, including the name of the individual to whom the Private Key was entrusted, and the time and date it was entrusted to them.

For Role based Code Signing Certificates where the Keys are used to sign Aircraft and Spacecraft software parts, the Role sponsor, or the Role Sponsor's employer, shall keep a log stating to whom such role Certificates were issued[8].

This log must be kept for a minimum of thirty (30) years, or as further required by Industry Regulation. The Subscriber and/or Subscriber's Employer are responsible to ensure that the individual in possession of the Private Key corresponding to a Certificate of either type complies with this CP. Moreover, log information maintained by the Subscriber and Subscriber's Employer may be audited by the CA or RA at any time.

6.4. ACTIVATION DATA

6.4.1. Activation data generation and installation

The activation data used to unlock Private Keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the crypto module used to store the keys. Subscriber activation data may be user selected. For CAs, it shall either entail the use of biometric data or satisfy the policy-enforced at/by the cryptographic module. If the activation

[8] Since the individual is issued a distinct Certificate, tracking the Certificate lifetime is sufficient to know when that Individual had the capability to sign software parts.

data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

6.4.2. Activation data protection

Data used to unlock Private Keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorised, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

6.4.3. Other aspects of activation data

CAs, CMSes, CSAs, and RAs shall change the activation data whenever the token is re-keyed or returned from maintenance.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific computer security technical requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSA, CMS, and RA shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Prohibit object re-use
- Require use of cryptography for session communication and database security
- Require a trusted path for identification and authentication
- Provide domain isolation for process
- Provide self-protection for the operating system
- Require self-test security related CA services (e.g., check the integrity of the audit logs)

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when

possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The CA-computer system shall be configured with minimum of the required accounts, network services, and, for CAs operating at Medium or higher Assurance Levels, no remote login functionality.

The Airbus PKI Root CAs shall be operated offline with no network connections installed.

6.5.2.Computer security rating

No stipulation.

6.6.LIFE CYCLE TECHNICAL CONTROLS

6.6.1.System development controls

The System Development Controls for the CA and CSA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Hardware and software developed shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not parts of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Applications required to perform the PKI operations shall be obtained from

sources authorised by local policy. CA, CMS, CSA, and RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2.Security management controls

The configuration of the CA, CSA, and CMS systems as well as any modifications and upgrades shall be documented and controlled.

There shall be a mechanism for detecting unauthorised modification to the CA, CSA, and CMS software or configuration.

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA and CMS systems. The CA and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

In addition, only applications required to perform the organisation's mission shall be loaded on the RA workstation, and all such software shall be obtained from sources authorized by local policy.

6.6.3.Life cycle security controls

No stipulation.

6.7.NETWORK SECURITY CONTROLS

The Airbus PKI Root CAs and their internal PKI Repositories shall be off-line.

Information shall be transported from the Internal PKI Repository to the Airbus Directory and the Airbus PKI Repositories using manual mechanisms at the Airbus PKI Root CAs.

Airbus PKI Sub CAs, CSAs, CMSes, and RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8.TIME-STAMPING

All CA, CSA, and CMS components shall regularly synchronise with a time service such as that provided by the Physikalisch-Technische Bundesanstalt (PTB), (which provides the "legal" German time), or a source that is synchronised with the National Institute of Standards and Technology (NIST) and U. S. Naval Observatory (USNO), (which provide the "legal" US time) such as time provided by the US Global Positioning System. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSA responses

Asserted times shall be accurate to within three (3) minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4.1.

7.CERTIFICATE, CRL, AND OCSP PROFILES

7.1.CERTIFICATE PROFILE

7.1.1.Version number(s)

The CAs shall issue X.509 v3 Certificates (populate version field with integer "2").

7.1.2.Certificate extensions

Airbus PKI CAs' critical private extensions shall be interoperable in their intended community of use.

Airbus PKI Sub CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains the Certificate formats.

All medium Assurance Level Certificates issued to Subscribers for signing purposes must include the necessary extensions as per RFC 3739 and ETSI TS 101862.

7.1.3.Algorithm object identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha256(2)}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) sha384(3)}

Certificates under this CP shall use the following OID for identifying the subject Public Key information:

rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) public-key-type(2) 1}

7.1.4.Name forms

The subject and issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC3280. Subject and issuer fields shall include attributes as detailed in

the tables below. Certificates issued for use as ETSI-qualified-signature Certificates must use name form option 1.

Subject Name Form for CAs

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0...1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Certification Authorities" or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc"
	Required	C	1	Country name, e.g., "C=US"
2	Recommended	CN	0...1	Descriptive name for CA, e.g., "CN=XYZ Inc CA"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Certification Authorities" or similar text
	Optional	O	0...1	Issuer name, e.g., "O=XYZ Inc"
	Optional	C	0...1	Country name, e.g., "C=US"
	Required	DC	1	Domain name, e.g., "DC=xyzinc"
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc.

Subject Name Form for Organisations

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Recommended	CN	0...1	Descriptive name for organisation, e.g., "CN=ABC Inc"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Corporations", "Organisations", or similar text
	Required	O	1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	C	1	Country name, e.g., "C=US" exactly as it appears in the CA Certificate(s)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
2	Recommended	CN	0...1	Descriptive name for organisation, e.g., "CN=ABC Inc"
	Optional	OU	0...N	As needed
	Recommended	OU	0...1	"Corporations", "Organisations", or similar text
	Optional	O	0...1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	DC	1	Domain name, e.g., "DC=xyzinc" exactly as it appears in the CA Certificate(s)
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as it appears in the CA Certificate(s)

Subject Name Form (Other Subscribers)

OPTION	USAGE	ATTRIBUTE	REQUIRED COUNT	CONTENT
1	Required	See Content description	1...N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0...N	As needed
	Required	O	1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	C	1	Country name, e.g., "C=US" exactly as it appears in the CA Certificate(s)
2	Required	See Content description	1...N	Additional naming attributes for uniquely identifying the subject including common name, serialNumber, email, etc.
	Optional	OU	0...N	As needed
	Optional	O	0...1	Issuer name, e.g., "O=XYZ Inc" exactly as it appears in the CA Certificate(s)
	Required	DC	1	Domain name, e.g., "DC=xyzinc" exactly as it appears in the CA Certificate(s)
	Required	DC	1...N	Domain root label(s), e.g., "DC=com" or, "DC=com, DC=au", etc. exactly as it appears in the CA Certificate(s)

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

Aircraft Identification is an identifier registered in an aerospace industry-recognized registry and verifiable by the CA (e.g.: aircraft registration / tail number).

Aircraft Equipment Identification shall be an identifier registered in an aerospace industry-recognized registry and verifiable by the CA (e.g.: equipment registration number).

7.1.5.Name constraints

The CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats in section 10 subject to the requirements above.

In the case where an Airbus PKI CA certifies another CA within the Airbus PKI, the certifying Airbus PKI CA shall impose restrictions on the name space authorised in the subordinate Airbus PKI CA, which are at least as restrictive as its own name constraints.

The Airbus PKI CAs shall not obscure a Subscriber Subject name. Issuer names shall not be obscured. Airbus PKI CAs may assert critical or non-critical name constraints beyond those specified in the Certificate Formats.

7.1.6.Certificate Policy object identifier

CA and Subscriber Certificates issued under this CP shall assert one or more of the Certificate Policy OIDs listed in section 1.2 of this document.

A CA Certificate shall contain the policy OIDs of all policies under which it issues Certificates.

For non-CA Certificates, the Certificate asserting a policy OID shall also assert all lower assurance policy OIDs, within the restrictions outlined below. (Refer to Figure 2 in section 1.2 for the Assurance Level hierarchy.)

The following rules govern which OIDs may be asserted together:

- EADS-INFRASTRUCTURE and EADS-INFRASTRUCTURE-256 shall only be asserted for Certificates issued to Devices;
- An "org" OID shall only be asserted in Organisational Certificates;
- Organisational Certificates shall assert only "org" OIDs;
- Role-based Code Signing Certificates used for Aircraft and Spacecraft Code Signing shall assert only the medium-hardware-256 policy OID;
- A non-"-256" Certificate shall not assert a "-256" policy OID;

Thus, for example, a CA issuing Certificates at all Assurance Levels shall assert the following OIDs in Certificates it issues:

Assurance Level	**OIDs Asserted**
EADS-INFRASTRUCTURE	id-EADSINFRASTRUCTURE
EADS-INFRASTRUCTURE-256	id-EADSINFRASTRUCTURE-256 id-EADSINFRASTRUCTURE
EADS-INFRA-USER	id-EADSINFRA-USER-256
basic-software	id-BasicSoftware id-EADSINFRASTRUCTURE
basic-software-256	id-BasicSoftware-256 id-BasicSoftware id-EADSINFRASTRUCTURE-256 id-EADSINFRASTRUCTURE
basic-hardware	id-BasicHardware id-BasicSoftware id-EADSINFRASTRUCTURE
basic-hardware-256	id-BasicHardware-256 id-BasicHardware id-BasicSoftware-256 id-BasicSoftware id-EADSINFRASTRUCTURE-256 id-EADSINFRASTRUCTURE
medium-software	id-MediumSoftware id-BasicHardware id-BasicSoftware id-EADSINFRASTRUCTURE

medium-software-256	id-MediumSoftware-256 id-MediumSoftware id-BasicHardware-256 id-BasicHardware id-BasicSoftware-256 id-BasicSoftware id-EADSINFRASTRUCTURE-256 id-EADSINFRASTRUCTURE
medium-hardware	id-MediumHardware id-MediumSoftware id-BasicHardware id-BasicSoftware id-EADSINFRASTRUCTURE
medium-hardware-256	id-MediumHardware-256 id-MediumHardware id-MediumSoftware-256 id-MediumSoftware id-BasicHardware-256 id-BasicHardware id-BasicSoftware-256 id-BasicSoftware id-EADSINFRASTRUCTURE-256 id-EADSINFRASTRUCTURE
medium-hardware-org	id-MediumHardwareOrg
medium-software-org-256	id-MediumSoftwareOrg-256
medium-hardware-org-256	id-MediumHardwareOrg-256 id-MediumHardwareOrg id-MediumSoftwareOrg-256

7.1.7.Usage of Policy Constraints extension

The Airbus PKI policy domain shall follow the Certificate formats described in this CP, since inhibiting policy mapping may limit interoperability.

7.1.8.Policy qualifiers syntax and semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers.

7.1.9.Processing semantics for the critical Certificate Policies extension

Processing semantics for the critical Certificate Policy extension shall conform to X.509 certification path processing rules. Where such rules conflict with IETF RFC 3280, RFC 5280 shall be followed.

7.2.CRL PROFILE

7.2.1.Version number(s)

CAs shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2.CRL and CRL entry extensions

Critical private extensions shall be interoperable in their intended community of use.

Section 10 contains the CRL formats.

7.3.OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 2560. Section 10 contains the OCSP request and response formats.

7.3.1.Version number(s)

The version number for requests and responses shall be v1.

7.3.2.OCSP extensions

Responses shall support the nonce extension.

8.COMPLIANCE AUDIT AND OTHER ASSESSMENTS

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS and the provisions of the contracts (including MOA) with cross-certified CAs are being implemented and enforced.

8.1.FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The CAs operating at Assurance Levels other than only EADS-INFRASTRUCTURE, EADS-INFRA-USER, CSAs, CMSs, and RAs shall be subject to a periodic compliance audit, which is not less frequent than once per year.

The OA has the right to require unscheduled compliance inspections of subordinate CA, CSA, CMS, or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS.

The Airbus PMA has the right to require unscheduled compliance audits of all entities in the Airbus PKI. The Airbus PMA shall state the reason for any unscheduled compliance audit. This compliance audit allows the Airbus PMA to authorise or not (regarding the audit results) the Airbus PKI CAs to operate under this CP.

In the context of cross-certification, audits shall be requested as stated in the respective contracts and/or MOA.

8.2.IDENTITY AND QUALIFICATIONS OF ASSESSOR

8.2.1.CAs operating only at the EADS-INFRASTRUCTURE or EADS-INFRA-USER Assurance Level

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with the requirements of this CP.

8.2.2.CAs operating at other Assurance Levels

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with the requirements of this CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

8.3.ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

8.3.1.CAs operating only at the EADS-INFRASTRUCTURE or EADS-INFRA-USER Assurance Level

The compliance auditor may be internal or external to the Business Unit operating the CA undergoing audit.

8.3.2.CAs operating at other Assurance Levels

The compliance auditor shall be a firm, which is independent from Airbus N.V. and its affiliated companies, as well as sub-contractors operating the Airbus PKI. The Airbus PMA shall determine whether a compliance auditor meets this requirement.

8.4.TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP, the applicable CPSs, and the applicable MOAs.

The compliance audit must include an assessment of the applicable CPS against this CP, to determine that the CPS adequately addresses and implements the requirements of the CP.

8.5.ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The Airbus PMA or cross certified PKI PMAs may determine that a CA is not complying with its obligations set forth in this CP or the respective contracts (including MOAs) with cross-certified PKIs.

When such a determination is made, the PMA may suspend operation, may revoke the CA, or take other actions as appropriate. The respective CPS shall provide the appropriate procedures.

When the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, any contract with cross-certified PKIs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the Airbus PMA of the discrepancy.
- The Airbus PMA shall notify any affected cross-certified external PKI domains' PMAs promptly;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the respective contracts, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to halt temporarily operation of the CA, to revoke a Certificate issued by the CA, or take other actions it deems appropriate. The PMA shall develop procedures for making and implementing such determinations.

8.6. COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, shall be provided to the PMA as set forth in section 8.1. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

9.OTHER BUSINESS AND LEGAL MATTERS

9.1.FEES

9.1.1.Certificate issuance or renewal fees

Airbus is entitled to charge end-user Subscribers for the issuance, management, and renewal of certificates provided by the Airbus PKI.

9.1.2.Certificate access fees

Airbus decides on any fees related to the Airbus PKI services.

There shall be no fee associated with Relying Party access to Certificates in the Airbus PKI Directory.

9.1.3.Revocation or status information access fees

Airbus decides on any fees related to the Airbus PKI services.

There shall be no fee associated with Relying Party access to revocation or status information.

9.1.4.Fees for other services

Airbus decides on any fees related to the Airbus PKI services.

9.1.5.Refund policy

No stipulation.

9.2.FINANCIAL RESPONSIBILITY

9.2.1.Insurance coverage

Airbus shall maintain reasonable levels of insurance coverage as required by applicable laws.

9.2.2.Other assets

Airbus shall maintain sufficient financial resources to maintain operations and fulfil duties.

9.2.3.Insurance or warranty coverage for End-Entities

No stipulation.

9.3.CONFIDENTIALITY OF BUSINESS INFORMATION

Subscribers acknowledge that any information made public in a Certificate is deemed not private. In that respect, Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or confidential.

Personal and corporate information, which does not appear in certificates and in public directories, held by a CA or an RA is considered confidential and shall not be disclosed by the

CA or RA. Unless required by law or court order, any disclosure of such information requires Subscriber's written prior consent.

The treatment of confidential business information provided to external PKIs in the context of submitting an application for cross certification will be in accordance with the terms of the agreements entered into between the applicable entity and Airbus.

Each CA shall maintain the confidentiality of confidential business information that is clearly marked or labelled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.4.PRIVACY OF PERSONAL INFORMATION

For the purposes of the PKI related services, the Airbus PKI collects, stores, processes and discloses personally identifiable information in accordance with applicable laws and regulations, meaning Directive 95/46/EC, as transposed into domestic legislation of each Member State of the European Economic Area and in each case as amended, replaced or superseded from time to time, including without limitation by the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union, and/or other applicable data protection or national/federal or state/provincial/emirate privacy legislation in force, including where applicable, statues, decisions, guidelines, guidance notes, codes of practice, codes of conduct and data protection certification mechanisms issued from time to time by courts, any Supervisory Authority and other applicable authorities. Details of Airbus Data Protection Policy are published at:

http://publication.certificateservices.eads.com

Subscribers and End Entities must be given access and the ability to correct or modify their personal or organisation information upon appropriate request to the issuing CA. Such information must be provided only after taking proper steps to authenticate the identity of the requesting party.

9.5.INTELLECTUAL PROPERTY RIGHTS

The Airbus PKI owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

The Airbus PKI Operational Authority shall not violate intellectual property rights held by others.

9.5.1.Property Rights in Certificates and Revocation Information

Airbus PKI CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

Airbus grants permission to reproduce and distribute its Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to a Relying Party Agreement with the relevant CA. Airbus shall grant permission to use revocation

information to perform Relying Party functions, subject to applicable contractual agreements.

The subscriber, who has a certificate delivered by the Airbus PKI, retains all intellectual rights on the information it has provided and contained in the certificate delivered by an Airbus PKI CA (subject name). An external CA, which cross-certifies with the Airbus PKI, retains all intellectual rights it owns on the information contained in the CA certificate delivered by Airbus PKI PCAs (CA distinguished name, Public Key, policy OID ...)

9.5.2.Property Rights in this CP and related CPSs

Airbus asserts that it owns and/or has licensed the Intellectual Property Rights to this CP and related CPS. Furthermore, Airbus reserves all Intellectual Property Rights in this CP and related CPSs to be granted to Licensors at its discretion in conjunction with all applicable agreements and licenses.

9.5.3.Property Rights in Names

The Certificates may contain copyright material, trade marks and other proprietary information, and no commercial exploitation or unauthorised use of the material or information in or via the Certificates is permitted, except as may be provided in this CP or in any applicable agreement. In the event of any permitted use or copying of trade marks and/or copyright material, no deletions or changes in proprietary notices shall be made without written authorisation from the owner.

9.5.4.Property Rights in Keys

Key pairs corresponding to Certificates of cross-certified CAs and Subscribers are the property of the cross-certified CAs and Subscribers that are the respective subjects of these Certificates, subject to the rights of Subscribers regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these Key Pairs. Notwithstanding the foregoing, Airbus PKI Root CAs' root Public Keys and the root

Certificates containing them, including all PCA Public Keys and self-signed Certificates, are the property of Airbus.

9.6.REPRESENTATIONS AND WARRANTIES

Additional representations and warranties of the Airbus PKI and contractual partners are contained in contractual agreements between the parties. This includes agreement on responsibility for export compliance.

9.6.1.CA representations and warranties

9.6.1.1.The Airbus PKI Root CAs

The Airbus OA represents that, to its knowledge:

- Their Certificates meet all material requirements of this CP, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

The applicable agreements may include additional representations and warranties.

9.6.1.2.The Airbus PKI Subordinate or Cross-Certified CAs

Subordinate and Cross-Certified CAs represent and warrant that:

- There are no material misrepresentations of fact in the cross-certificates known to or originating from the entity approving the Cross Certification Applications or issuing the cross-certificates,
- There are no errors in the information in the cross-certificate that were introduced by the entity approving the Cross Certification Application or issuing the cross-certificate

as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,

- Their CA signing key is protected and that no unauthorised person has ever had access to the Private Key,
- All representations made by the Subordinate CA or Cross-Certified CA in the applicable agreements are true and accurate,
- All information supplied by the Subscriber in connection with, and/or contained in the Certificate has been duly verified, and
- The Certificate is being used exclusively for authorised purposes, consistent with this and any other applicable CP or CPS.

9.6.2. Subscriber representations and warranties

An Airbus PKI CA shall require the Subscribers to sign a document containing the requirements the Subscriber shall meet respecting protection of the Private Key and use of the Certificate before being issued the Certificate. Subscribers shall agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their Private Keys at all times and prevent them from unauthorised access in accordance with this policy, as stipulated in their General Terms and Conditions.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their Private Keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CP.
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates, as set forth in this CP and the General Terms and Conditions.
- Use Certificates provided by the Airbus PKI CAs only for authorised and legal purposes in accordance with this CP.
- Comply with all export laws and regulations for dual usage goods as may be applicable, as relates to the usage and transport of keys, certificates and algorithms mandated by this CP.
- Cease to use Airbus certificates if they become invalid and remove them from any applications and/or devices they have been installed on.

Device Sponsors (as described in section 5.2.1.4) shall assume the obligations of Subscribers for the Certificates associated with their components.

9.6.3. Relying Party representations and warranties

Parties who rely upon the Certificates issued under a policy defined in this document shall:

- use the Certificate for the purpose for which it was issued, as indicated in the Certificate information (e.g., the key usage extension);
- check each Certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- establish trust in the CA who issued a Certificate by verifying the Certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment;

- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

9.6.4.Representations and warranties of other participants

See section 2 for Repository obligations.

The Airbus PMA shall ensure that Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the Certificate information posting and retrieval stipulations of this CP;
- provide access control mechanisms sufficient to protect repository information as described in section 2.4.

An OCSP Responder that has been issued an Airbus PKI CA Certificate shall conform to the stipulations of this document including operating under a CPS that has been approved by the Airbus PMA. Such OCSP Responders which are found to have acted in a manner inconsistent with these obligations are subject to action as described in section 8.5.

9.7.DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, Policy Mapping Agreements, Cross-Certificates Agreements, Memorandums of Agreement, and any other related agreements may contain disclaimers of all warranties (other than any express warranties contained in such agreements or set forth in this CP).

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS CP OR THOSE BETWEEN AIRBUS AND ITS CUSTOMERS UNDER SEPARATE AGREEMENTS AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, (A) CERTIFICATES ISSUED BY AIRBUS AND THE AIRBUS PKI ARE PROVIDED "AS IS", AND AIRBUS, ITS EMPLOYEES, OFFICERS, AGENTS, REPRESENTATIVES, AND DIRECTORS DISCLAIM ALL OTHER WARRANTIES, REPRESENTATIONS, TERMS, CONDITIONS AND OBLIGATIONS OF EVERY TYPE, WHETHER EXPRESSED, IMPLIED OR STATUTORY (INCLUDING, WITHOUT LIMITATION, ANY REPRESENTATIONS AND WARRANTIES OF SUITABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE, SECURITY, OR ACCURACY OF INFORMATION PROVIDED), AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN and/OR LACK OF REASONABLE CARE AND (B) THE ENTIRE RISK OF THE USE OF ANY AIRBUS CERTIFICATES, ANY SERVICES

PROVIDED BY AIRBUS, OR THE VALIDATION OF ANY DIGITAL SIGNATURES LIES WITH THE APPLICABLE PARTICIPANT.

THIS CLAUSE IS SUBJECT ALWAYS TO SECTION 9.8 (LIMITATIONS OF LIABILITY)

9.8.LIMITATIONS OF LIABILITY

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable General Terms and Conditions, subject to the applicable law governing the relationship between the parties.

The liability (and/or limitation thereof) of Airbus to other PKI domains' CAs to which Airbus PKI CAs issue Certificates shall be set forth in the applicable agreements.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements between the applicable CA and the Relying Party.

OTHER THAN THE ABOVE DESCRIBED LIMITATIONS OF LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL AIRBUS BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, ANY COSTS, EXPENSES, OR LOSS OF PROFITS, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL AIRBUS BE LIABLE FOR ANY USAGE OF CERTIFICATE THAT EXCEEDS THE LIMITATIONS OF USAGE STATED UNDER THIS CP OR THAT IS NOT IN COMPLIANCE WITH THIS CP AND ASSOCIATED CPS.

AIRBUS SHALL NOT BE LIABLE FOR ANY DAMAGE ARISING FROM THE COMPROMISE OF A SUBSCRIBER'S PRIVATE KEY OR ANY LOSS OF DATA.

SAVE FOR LIABILITY WHICH IS NOT PERMISSIBLE AT LAW, THE TOTAL, AGGREGATE LIABILITY OF EACH AIRBUS CA ARISING OUT OF OR RELATED TO IMPROPER ACTIONS BY THE AIRBUS CA SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD) PER TRANSACTION AND ONE MILLION DOLLARS ($1 MILLION USD) PER INCIDENT.

9.9.INDEMNITIES

9.9.1.Indemnification by Customer CAs

To the extent permitted by applicable law, other PKI domains CAs issued Certificates by Airbus agree to indemnify and hold Airbus harmless from any acts or omissions resulting in liability,

any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Airbus may incur as a result of:

- Falsehood or misrepresentation of fact by the other PKI domains CA in the applicable contractual agreements,
- Failure by the other PKI domains CA to disclose a material fact in any applicable contractual agreement, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The other PKI domains CA's failure to protect the other PKI domains CA Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the other PKI domains CA Private Key, or
- The other PKI domains CA's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Any applicable agreement may include additional indemnity obligations.

9.9.2.Indemnification by Relying Parties

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold Airbus harmless from any acts or omissions resulting in

liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Airbus may incur as a result of:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

Any applicable contractual agreement with Airbus may include additional indemnity obligations.

9.9.3.Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold Airbus harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Airbus may incur as a result of:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Fraudulent or negligent use of certificates by the Subscriber,
- Unauthorised use of the certificates by Subscribers including use of certificates beyond the prescribed use defined by this CP,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's Private Key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable General Terms and Conditions may include additional indemnity obligations.

This indemnification clause shall not be applicable for the Airbus employees.

9.10.TERM AND TERMINATION

9.10.1.Term

This CP becomes effective upon its execution by the Airbus PMA and publication in the appropriate directory (as defined in section 2). Amendments to this CP shall become effective

upon execution by the Airbus PMA and publication in the appropriate Repository (as defined in section 2).

9.10.2.Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version.

Airbus may decide to terminate this CP as of right, at any time for convenience. All Entities shall be notified 6 (six) months prior to the effective termination of this CP.

9.10.3.Effect of termination and survival

Upon termination of this CP, CAs cross-certified with or subordinate to Airbus PKI CAs are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. Termination or expiration shall not affect any provision of this CP which is expressly or by implication intended to come into or remain in effect on or after termination or expiration, including the following sections of this CP: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

9.11.INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Unless otherwise specified by agreement between the parties, the Airbus PKI OA shall use commercially reasonable methods to communicate with cross certified CAs, taking into account the criticality and subject matter of the communication.

9.12.AMENDMENTS

9.12.1.Procedure for amendment

The Airbus PMA shall review this CP and the respective CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the Airbus PMA.

If the Airbus PMA wishes to recommend amendments or corrections to the CP or CPS, such modifications shall be circulated to appropriate parties identified by the Airbus PMA. Comments from such parties will be collected and considered by the AIRBUS PMA in a fashion prescribed by the Airbus PMA.

Following approval by the Airbus PMA, public notification of amendments shall be made.

Notwithstanding the foregoing, if the Airbus PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of Airbus, the Airbus PMA shall be entitled to make such amendments effective immediately upon publication in the Repository without having to circulate the amendments prior to their adoption.

9.12.2.Notification mechanism and period

Errors, updates and anticipated changes to the CP and CPS resulting from reviews are provided to the Airbus PMA by the OA Administrator. In addition, the OA Administrator shall communicate changes to every affected entity, including cross-certified PKIs, via a designated point of contact, including a description of the change.

This CP and any subsequent changes shall be made publicly available within seven (7) days of approval by the Airbus PMA. The Subscriber shall be bound by the most up to date version of

the CP from its date of publication whose modifications shall not be substantially detrimental to the Subscribers.

The most up to date copy of this CP can be found at:

http://publication.certificateservices.eads.com/

9.12.3.Circumstances under which OID must be changed

Certificate Policy OIDs shall be changed if the Airbus PMA determines that a change in the CP reduces the level of assurance provided.

9.13.DISPUTE RESOLUTION PROVISIONS

9.13.1.Disputes among the AIRBUS PMA/OA and Third Parties

Provisions for resolving disputes between the Airbus PKI PMA/OA and contractually linked entities shall be set forth in the applicable agreements between the parties.

9.13.2.Alternate Dispute Resolution Provisions

In case of any dispute or disagreement between two or more participants arising out of or related to this CP, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one disputing party to the other. If the dispute is not successfully resolved by negotiation between the entities or the parties within sixty (60) days following the date of such notice, it shall be settled by final and binding arbitration before a single arbitrator knowledgeable in the information technology industry in accordance with the then existing Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC). The place of arbitration shall be defined in the relevant agreement between contracting parties. In the absence of such agreement, the place of arbitration shall be Munich, Germany.

9.14.GOVERNING LAW

The Airbus Enterprise PKI and the AIRBUS Enterprise SHA2 PKI:

The law governing the enforceability, construction, interpretation, and validity of this CP shall be defined in the relevant agreement between contracting parties. In the absence of such agreement, subject to any limits appearing in applicable law, the laws of the Federal Republic of Germany, shall govern the enforceability, construction, interpretation, and validity of this CP,

irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the Federal Republic of Germany.

9.15.COMPLIANCE WITH APPLICABLE LAW

This CP may be subject to applicable mandatory national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

Parties agree to conform to applicable laws and regulations.

9.16.MISCELLANEOUS PROVISIONS

9.16.1.Entire agreement

No stipulations.

9.16.2.Assignment

Except as otherwise provided under the applicable agreements and to the extent permitted by law, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party, except that Airbus may assign and delegate this CP, at any time, to any successor (i) in case of any merger, consolidation, re-organisation, voluntary sale or transfer of Airbus or, (ii) the voluntary sale or transfer of all or substantially all of Airbus' assets.

9.16.3.Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4.Enforcement (attorneys' fees and waiver of rights)

Failure or delay at any time to enforce any right hereunder shall not constitute a waiver of such right or affect the validity of the CP or any part thereof, nor shall it prejudice the rights to enforce such right at a subsequent time.

9.16.5.Force Majeure

Airbus shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

AIRBUS HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO AIRBUS.

9.17.OTHER PROVISIONS

No stipulation.

10.CERTIFICATE, CRL, AND OCSP FORMATS

This section contains the formats for the various PKI objects such as Certificates, CRLs, and OCSP requests and responses. For algorithm identifiers, parameter encoding, Public Key encoding, and signature encoding for ECDSA and ECDH, IETF RFC 3279 shall be used.

Certificates and CRLs issued under a policy OID of this CP shall not include any critical extensions not listed in the profiles in this section. Certificates and CRLs issued under a policy OID of this CP may contain non-critical extensions not listed in the profiles in this section only upon Airbus PMA approval. No stipulation for Infrastructure level of assurance.

First entries in the caIssuers field of the AIA extension and CRL DP shall point to a resource that is publicly available using HTTP. If LDAP pointers are used, they shall appear only after the HTTP pointers.

For attribute values other than dc and e-mail address: All CA Distinguished Names (in various fields such as Issuer, Subject, Subject Alternative Name, Name constraints, etc.) shall be encoded as printable string. All Subscriber DN portions that name constraints apply to, shall be encoded as printable string. Other portions of the Subscriber DN shall be encoded as printable string if possible. If a portion cannot be encoded as printable string, then and only then shall it be encoded using a different format and that format shall be UTF8.

All dc and email address attribute values shall be encoded as IA5 string.

If the Entity PKI provides OCSP services for a CA, that CA must also issue a full and complete CRL (i.e., a CRL without Issuing Distribution Point extension) for use by the OCSP Responder.

The CRL distribution point extension shall only populate the distributionPoint field. The distributionPoint field shall contain HTTP (i.e., of the form http://...) URI and may be followed by LDAP (i.e., of the form ldap://...) URI. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL or a Distribution Point based partitioned CRL. The Distribution Point field shall contain a full name (i.e., the Distribution Point field shall not contain nameRelativetoCRLIssuer).

Global Unique Identifier (GUID) used in Certificates shall conform to [RFC 4122] requirement. Since GUID is associated with a card, the same GUID shall be asserted as UUID in all applicable Certificates and in all applicable other signed objects on the card.

10.1.PKI COMPONENT CERTIFICATES

10.1.1.EADS Enterprise PCA → CBCA Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	cn=CertiPath Bridge CA, ou=Certification Authorities, o=CertiPath LLC, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; {id-MediumSoftware}, {id-MediumHardware}
Policy Mapping	c=no; [{id-MediumSoftware} {id-variant-mediumSoftware}], [{id-MediumSoftware} {id-variant-mediumHardware}], [{id-MediumHardware} {id-variant-mediumHardware}]
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Name forms as per Airbus PKI Naming Policy
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for p7c file containing Certificates issued to PCA, may be followed by LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry; id-ad-ocsp access method entry contains HTTP URL for the PCA OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

10.1.2. EADS Enterprise SHA2 PCA → CBCA G2 Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	cn=CertiPath Bridge CA - G2, ou=Certification Authorities, o=CertiPath LLC, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; {id-MediumSoftware-256}, {id-MediumHardware-256}
Policy Mapping	c=no; [{id-MediumSoftware-256} {id-mediumSoftware}], [{id-MediumSoftware-256} {id-mediumHardware}], [{id-MediumHardware-256} {id-mediumHardware}]
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Name forms as per Airbus PKI Naming Policy
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for p7c file containing Certificates issued to PCA, may be followed by LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry; id-ad-ocsp access method entry contains HTTP URL for the PCA OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

10.1.3.Cassidian Communications PCA → CBCA G2 Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	cn=CertiPath Bridge CA - G2, ou=Certification Authorities, o=CertiPath LLC, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as in PCA PKCS-10 request to the CBCA)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the CBCA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; {id-MediumSoftware-256}, {id-MediumHardware-256}, {id-IceCAPHardware}, {id-IceCAPCardAuth}, {id-IceCAPContentSigning}
Policy Mapping	c=no; [{id-MediumSoftware-256} {id-mediumSoftware}], [{id-MediumSoftware-256} {id-mediumHardware}], [{id-MediumSoftware-256} {id-IceCAP-hardware}], [{id-MediumHardware-256} {id-mediumHardware}], [{id-MediumHardware-256} {id-IceCAP-hardware}], [{id-IceCAPHardware} {id-IceCAP-hardware}], [{id-IceCAPCardAuth} {id-IceCAP-cardAuth}], [{id-IceCAPContentSigning} {id-IceCAP-contentSigning}]
Basic Constraints	c=yes; cA=True; path length constraint absent
Name Constraints	c=yes; optional, excluded subtrees: Name forms as per Airbus PKI Naming Policy
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for p7c file containing Certificates issued to PCA, may be followed by LDAP URL pointer to the caCertificate attribute of the PCA PKI Repository entry; id-ad-ocsp access method entry contains HTTP URL for the PCA OCSP Responder
CRL Distribution Points	c = no;
Inhibit anyPolicy	c=no; skipCerts = 0

10.1.4.Airbus PKI Self-Signed Root Certificate (also called Trust Anchor)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonRepudiation (optional)
Basic Constraints	c=yes; cA=True; path length constraint absent

10.1.5.AIRBUS Enterprise and AIRBUS Enterprise SHA2 Subordinate CA Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonRepudiation (optional)
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints	c=yes; cA=True; path length constraint absent
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA
CRL Distribution Points	c = no;

10.1.6.Airbus Business Units Intermediate CA and Airbus Business Units SHA2 Intermediate CA Certificates

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
PIssuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet string (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet string (same as in PKCS-10 request from the subject CA)
Key Usage	C=yes; keyCertSign, cRLSign, DigitalSignature (optional), nonRepudiation (optional)
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints	c=yes; cA=True; path length = 1
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA
CRL Distribution Points	c=no;

10.1.7.Cassidian Communications Subordinate CA Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request from the subject CA)
Key Usage	c=yes; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Certificate Policies	c=no; As per section 7.1.6
Basic Constraints	c=yes; cA=True; pathLength=0;
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate and crossCertificatePair attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA
CRL Distribution Points	c = no;

10.1.8.Time Stamp Authority Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuer CA DN conforming to section 7.1.4 of this CP
Validity Period	Expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 Subject CA DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate and crossCertificatePair attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA
CRL Distribution Points	c = no;

10.1.9.OCSP Responder Certificate

The following table contains the OCSP Responder Certificate profile assuming that the same CA using the same key as the Subscriber Certificate issues the OCSP Responder Certificate.

Field	**Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than one month from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 OCSP Responder (subject) DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended Key Usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	HTTP URL for the OCSP Responder
No Check id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}	c=no; Null
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA

10.2.END-ENTITY CERTIFICATES

This section describes the values that populate each field of the Certificates issued by the Airbus PKI CAs excluding infrastructure level of assurance. The OAA shall be able at any time to

provide the templates of the issued certificates upon request of the PMA as stipulated in 6.1.7.Key usage purposes.

10.2.1.Subscriber Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 5280 method 1 or other method)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; URI (mandatory for IceCAP-hardware, otherwise optional), otherName::principalName(1.3.6.1.4.1.311.20.2.3, optional, ASN1-encoded UTF-8 string); RFC822 email address (optional); others optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.2.Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; RFC822 email address (required); URI (optional); others optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no
Qualified Certificate Statements	optional, c=no; id-etsi-qcs-QcCompliance, id-etsi-qcs-QcRetentionPeriod=11 (for software certificates) optional, c=no; id-etsi-qcs-QcCompliance, id-etsi-qcs-QcRetentionPeriod=11; id-etsi-qcs-QcSSCD (for hardware certificates)

10.2.3.Subscriber Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; RFC822 email address (required); URI (optional), others optional
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.4.Organisational Subscriber Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 (Organisational) of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature, nonRepudiation
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.5.Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; as per section 7.1.6
Subject Alternative Name	c=no; DN of the person controlling the code signing Private Key
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.6.Organisational Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 (Organisational) of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.7.Device or Server Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (required), keyEncipherment (optional)
Extended key usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.8.Device or Server Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.9.Device or Server Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Host URL | Host IP Address | Host Name }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.10.Aircraft or Aircraft Equipment Identity Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (required), keyEncipherment (optional)
Extended key usage	optional; c=no;
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed byLDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.11. Aircraft or Aircraft Equipment Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended key usage	optional; c=no;
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-caIssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.12. Aircraft or Aircraft Equipment Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN conforming to section 7.1.4 of this CP cn={ Aircraft Identification | Aircraft Equipment Identification (see 7.1.4) }
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; keyEncipherment (required), dataEncipherment (optional)
Extended key usage	c=no; as per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c=no; always present, Aircraft Identification | Aircraft Equipment Identification (see 7.1.4)
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed byLDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder
CRL Distribution Points	c = no

10.2.13.Role Signature Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN for role conforming to Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c = no; DN of the person controlling the role signing private key; RFC822 email address of role (Optional)
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.14.Role Encryption Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN for role conforming to Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; ; keyEncipherment
Extended Key Usage	c=no; As per section 10.7
Certificate Policies	c=no; As per section 7.1.6
Subject Alternative Name	c = no; RFC822 email address of role (required); others optional
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.15.Role Code Signing Certificate

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	3 years from date of issue expressed in UTCTime until 2049
Subject Distinguished Name	Unique X.500 subject DN for role conforming to Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Refer to section 7.1.3
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA Certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature (always present), nonRepudiation (optional)
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; as per section 7.1.6
Subject Alternative Name	c = no; DN of the person controlling the role code signing private key; RFC822 email address of role (Optional)
CRL Distribution Points	c = no
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing Certificates issued to Issuing CA, may be followed by LDAP URL pointer to the caCertificate attribute of the Issuing CA; id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.16.IceCAP Card Authentication Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} per Section 6.1.5
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	No longer than 3 years from date of issue; Expressed in UTCTime for dates until end of 2049
Subject Distinguished Name	serialNumber=<GUID> with applicable DN prefix.
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA per RFC 3280 method 1 or other method)
Key Usage	c=yes; digitalSignature
Extended Key Usage	c-yes; As per section 10.7
Certificate Policies	c=no; id-IceCAPCardAuth as per section 7.1.6
Subject Alternative Name	c=no; URI urn:uuid:<32 character hex representing 128 bit GUID>
CRL Distribution Points	c=no;
Authority Information Access	c = no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.2.17.IceCAP Content Signer Certificate (DEPRECATED)

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	WithRSAEncryption {1 2 840 113549 1 1 11} per Section 6.1.5
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
Validity Period	10 years from date of issue expressed in UTCTime for dates until end of 2049
Subject Distinguished Name	Unique X.500 subject DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	2048 bit modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extension	**Value**
Authority Key Identifier	c=no; Octet String (same as subject key identifier in Issuing CA certificate)
Subject Key Identifier	c=no; Octet String (same as in PKCS-10 request or calculated by the Issuing CA)
Key Usage	c=yes; digitalSignature
Extended key usage	c=yes; As per section 10.7
Certificate Policies	c=no; id-IceCAPContentSigning as per section 7.1.6
Subject Alternative Name	optional; c=no
CRL Distribution Points	c = no;
Authority Information Access	c=no; id-ad-calssuers access method entry contains HTTP URL for .p7c file containing certificates issued to Issuing CA id-ad-ocsp access method entry contains HTTP URL for the Issuing CA OCSP Responder

10.3 CRL FORMAT

10.3.1 Full and Complete CRL

If the CA provides OCSP Responder Services, the CA shall make a full and complete CRL available to the OCSP Responders as specified below. This CRL may also be provided to the relying parties.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	Refer to section 7.1.3
Issuer Distinguished Name	Unique X.500 Issuing CA DN conforming to section 7.1.4 of this CP
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked Certificates list	0 or more 2-tuple of Certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	Refer to section 7.1.3
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in Certificates issued by the CA)
nextPublish (1.3.6.1.4.1.311.21.4)	c=no; optional, Next CRL expected issuance date in UTC Time
CRL Entry Extension	**Value**
Reason Code	c=no; optional, must be included when reason code = key compromise or CA compromise

10.3.2 Distribution Point Based Partitioned CRL

Not supported.

10.3.OCSP REQUEST FORMAT

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of Certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

10.5 OCSP RESPONSE FORMAT

See RFC 2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	**Value**
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder Certificate)
Produced At	Generalized Time
List of Responses	Each response will contain Certificate id; Certificate status, thisUpdate, nextUpdate,
Responder Signature	Refer to section 7.1.3
Certificates	Applicable Certificates issued to the OCSP Responder
Response Extension	**Value**
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**

Field	Value
None	None

10.6 PKCS 10 REQUEST FORMAT

The following table contains the format for PKCS 10 requests.

Field	**Value**
Version	V1 (0)
Subject Distinguished Name	Unique X.500 CA DN as specified in Section 7.1.4 of this CP
Subject Public Key Information	Refer to section 6.1
Subject's Signature	Refer to section 7.1.3
Extension (encoded in extension request attribute)	**Value**
Subject Key Identifier	c=no; Octet String
Key Usage	c=yes; optional; keyCertSign, cRLSign, DigitalSignature, nonRepudiation
Basic Constraints	c=yes; optional; cA=True; path length constraint (absent or 0 as appropriate)
Name Constraints	c=yes; optional; permitted subtrees for DN, RFC-822, and DNS name forms

10.7 EXTENDED KEY USAGE

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
CA	None	None	All
OCSP Responder	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}	None	All Others
Subscriber, Role: Authentication	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}; id-pkinit-KPClientAuth {1 3 6 1 5 2 3 4}	None	All Others
Subscriber, Role, and Organisation Subscriber: Signature	id-kp-emailProtection {1.3.6.1.5.5.7.3.4}; MSFT Document Signing {1.3.6.1.4.1.311.10.3.12}; Adobe Certified Document Signing {1.2.840.113583.1.1.5}	None	All Others
Subscriber, Role: Encryption	id-kp-emailProtection {1.3.6.1.5.5.7.3.4};	Any EKU that is consistent with Key Usage, e.g., Encrypting File System {1.3.6.1.4.1.311.10.3.4}	Any EKU that is not consistent with Key Usage anyExtendedKeyUsage {2.5.29.37.0}
Code Signing, Role Code Signing	id-kp-codesigning {1 3 6 1 5 5 7 3 3}	Life-time Signing {1.3.6.1.4.1.311.10.3.13}	All Others
Device Authentication, Web Server	id-kp-serverAuth {1 3 6 1 5 5 7 3 1} id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Device Signature	None	None	All
Device Encryption	None	None	All
Domain Controller	id-kp-serverAuth {1 3 6 1 5 5 7 3 1}; id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; id-pkinit-KPKdc {1 3 6 1 5 2 3 5}; smartCardLogon {1.3.6.1.4.1.311.20.2.2}	None	All Others
Time Stamp Authority	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	None	All Others

Certificate Type	Required EKU	Optional EKU	Prohibited EKU
Web Client	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}	None	All Others
Workstation	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}; iKEIntermediate {1.3.6.1.5.5.8.2.2}; id-kp-ipsecIKE {1 3 6 1 5 5 7 3 17}	None	All Others