



SIEMENS

Certificate



1

2

Siemens AG

3 Product PKI Certificate Management Service –
4 Certification Practice Statement for Siemens
5 Product PKI Infrastructure Certificates
6 V2.1
7

8 Document History

Version	Date	Author	Change Comment
1.0	Jan. 26, 2022	Michael Munzert, Antonio Vaira, T CST	First released version
1.1	Oct. 11, 2022	Kai Che, Michael Munzert, T CST	New responsible for document authorization
1.2	Mar. 02, 2023	Kai Che, Michael Munzert, Antonio Vaira T CST	Detailed Chapter 6 key generation
2.0	Oct. 18, 2023	Kai Che, Michael Munzert, Antonio Vaira T CST	Copied parts of the description of the Central CPS to Tenant CPS (this document)
2.0	July 10, 2024	Kai Che	Review performed, no changes.
2.1	Jan. 30, 2025	Kai Che	Updated department from T CST to FT RPD CST due to reorganization.

9

10 This document will be reviewed every year or in the event of an important ad-hoc change according
11 to the Information Security update process for documents. Each new version will be approved by the
12 respective management level before being released.

13 This document is published under www.siemens.com/pki.

14 Scope and Applicability

15 This document constitutes the Certification Practice Statement (CPS) for the PKI service providing
16 infrastructure certificates to Siemens Product PKI Tenant. The Product PKI is responsible for the
17 operation of the Root CAs as well as for the Issuing CAs. Together with the Central CPS, this document
18 discloses to interested parties the business policies and practices under which the Product PKI operates.
19 The Central PMA ensures that the certification practices established to meet the applicable
20 requirements specified in the present document are properly implemented in accordance with
21 Siemens' Information Security Policy.

22 Document Status

23 This document has been classified as "Unrestricted".

	Name	Department	Date
Author	Various authors, detailed information see document history.		
Checked by	Stenger, Meiko	Siemens LC	May, 2020
	Kuechler, Markus	Siemens IT	Feb., 2022
Authorization	Dr. Kind, Andreas	Head of Siemens FT RPD CST	Jan., 2025

Content

24	Content	
25	Document History	2
26	Scope and Applicability	2
27	Document Status	2
28	Content.....	3
29	1 Introduction.....	12
30	1.1 Overview.....	12
31	1.1.1 PKI hierarchy.....	14
32	1.2 Document Name and Identification.....	15
33	1.3 PKI Participants.....	15
34	1.3.1 Certification Authorities	15
35	1.3.2 Registration Authorities	15
36	1.3.3 Subscribers	15
37	1.3.4 Relying Parties	15
38	1.3.5 Other Participants	15
39	1.4 Certificate Usage	15
40	1.4.1 Appropriate Certificate Usage	15
41	1.4.2 Prohibited Certificate Usage	15
42	1.5 Policy Administration	16
43	1.5.1 Organization Administering the Document.....	16
44	1.5.2 Contact Person	16
45	1.5.3 Person Determining CP and CPS Suitability for the Policy	16
46	1.5.4 CPS Approval Procedures	16
47	1.6 Definitions and Acronyms	17
48	1.6.1 Definitions	17
49	1.6.2 Acronyms.....	19
50	2 Publication and Repository Responsibilities	20
51	2.1 Repositories.....	20
52	2.2 Publication of Certification Information.....	20
53	2.3 Time or Frequency of Publication	20
54	2.4 Access Controls on Repositories.....	20
55	3 Identification and Authentication	21
56	3.1 Naming	21
57	3.1.1 Types of Names	21

58	3.1.2	Need of Names to be Meaningful	21
59	3.1.3	Anonymity or Pseudonymity of Subscribers	21
60	3.1.4	Rules for Interpreting Various Name Forms.....	21
61	3.1.5	Uniqueness of Names.....	21
62	3.1.6	Recognition, Authentication, and Roles of Trademarks.....	21
63	3.2	Initial Identity Validation	21
64	3.2.1	Method to Prove Possession of Private Key.....	21
65	3.2.2	Authentication of Organization Identity	21
66	3.2.3	Authentication of Individual Identity	21
67	3.2.4	Non-verified Subscriber Information	21
68	3.2.5	Validation of Authority	22
69	3.2.6	Criteria for Interoperation.....	22
70	3.3	Identification and Authentication for Re-key Requests	22
71	3.3.1	Identification and Authentication for Routine Re-Key.....	22
72	3.3.2	Identification and Authentication for Re-Key After Revocation	22
73	3.4	Identification and Authentication for Revocation Requests	22
74	4	Certificate Lifecycle Operational Requirements	23
75	4.1	Certificate Application.....	23
76	4.1.1	Who can submit a certificate application?.....	23
77	4.1.2	Enrollment Process and Responsibilities.....	23
78	4.2	Certificate Application Processing	23
79	4.2.1	Performing identification and authentication functions.....	23
80	4.2.2	Approval or Rejection of Certificate Applications	23
81	4.2.3	Time to Process Certificate Applications.....	23
82	4.3	Certificate Issuance	23
83	4.3.1	CA Actions during Certificate Issuance	23
84	4.3.2	Notification to Subscriber by the CA of Issuance of Certificate	23
85	4.4	Certificate Acceptance	23
86	4.4.1	Conduct constituting certificate acceptance.....	23
87	4.4.2	Publication of the certificate by the CA.....	24
88	4.4.3	Notification of Certificate issuance by the CA to other entities.....	24
89	4.5	Key Pair and Certificate Usage	24
90	4.5.1	Subject Private Key and Certificate Usage	24
91	4.5.2	Relying Party Public Key and Certificate Usage.....	24
92	4.6	Certificate Renewal	24

93	4.6.1	Circumstance for Certificate Renewal.....	24
94	4.6.2	Who may request renewal?	24
95	4.6.3	Processing Certificate Renewal Request	24
96	4.6.4	Notification of new Certificate Issuance to Subscriber	24
97	4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	24
98	4.6.6	Publication of the Renewal Certificate by the CA	24
99	4.6.7	Notification of Certificate Issuance by the CA to other Entities.....	24
100	4.7	Certificate Re-key	24
101	4.7.1	Circumstances for Certificate Re-key	24
102	4.7.2	Who may request certification of a new Public Key?.....	24
103	4.7.3	Processing Certificate Re-keying Requests.....	25
104	4.7.4	Notification of new Certificate Issuance to Subscriber	25
105	4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	25
106	4.7.6	Publication of the Re-keyed Certificate by the CA	25
107	4.7.7	Notification of Certificate Issuance by the CA to other Entities.....	25
108	4.8	Certificate Modification.....	25
109	4.8.1	Circumstance for Certificate Modification	25
110	4.8.2	Who may request Certificate modification?	25
111	4.8.3	Processing Certificate Modification Requests.....	25
112	4.8.4	Notification of new Certificate Issuance to Subscriber	25
113	4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	25
114	4.8.6	Publication of the Modified Certificate by the CA.....	25
115	4.8.7	Notification of Certificate Issuance by the CA to Other Entities	25
116	4.9	Certificate Revocation and Suspension	25
117	4.9.1	Circumstances for Revocation	25
118	4.9.2	Who can request revocation?	25
119	4.9.3	Procedure for Revocation Request	26
120	4.9.4	Revocation Request Grace Period	26
121	4.9.5	Time within which CA must Process the Revocation Request	26
122	4.9.6	Revocation Checking Requirement for Relying Parties	26
123	4.9.7	CRL Issuance Frequency	26
124	4.9.8	Maximum Latency for CRLs	26
125	4.9.9	On-line Revocation/Status Checking Availability	26
126	4.9.10	On-line Revocation Checking Requirements	26
127	4.9.11	Other Forms of Revocation Advertisements Available	26

128	4.9.12	Special Requirements for Private Key Compromise.....	26
129	4.9.13	Circumstances for Suspension.....	26
130	4.9.14	Who can request suspension?	26
131	4.9.15	Procedure for suspension request	26
132	4.9.16	Limits on suspension period	26
133	4.10	Certificate Status Services	26
134	4.10.1	Operational Characteristics.....	26
135	4.10.2	Service Availability.....	27
136	4.10.3	Optional Features	27
137	4.11	End of Subscription.....	27
138	4.12	Key Escrow and Recovery	27
139	4.12.1	Key Escrow and Recovery Policy and Practices	27
140	4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	27
141	5	Management, Operational, and Physical Controls.....	28
142	5.1	Physical Security Controls.....	28
143	5.1.1	Site Location and Construction	28
144	5.1.2	Physical Access	28
145	5.1.3	Power and Air Conditioning.....	28
146	5.1.4	Water Exposure	28
147	5.1.5	Fire Prevention and Protection	28
148	5.1.6	Media Storage	28
149	5.1.7	Waste Disposal	28
150	5.1.8	Off-site Backup	28
151	5.2	Procedural Controls.....	28
152	5.2.1	Trusted Roles.....	28
153	5.2.2	Numbers of Persons Required per Task	28
154	5.2.3	Identification and Authentication for Each Role	28
155	5.2.4	Roles Requiring Separation of Duties.....	28
156	5.3	Personnel Controls	28
157	5.3.1	Qualifications, Experience and Clearance Requirements	28
158	5.3.2	Background Check Procedures.....	28
159	5.3.3	Training Requirements	29
160	5.3.4	Retraining Frequency and Requirements.....	29
161	5.3.5	Job Rotation Frequency and Sequence	29
162	5.3.6	Sanctions for Unauthorized Actions.....	29

163	5.3.7	Independent Contractor Requirements	29
164	5.3.8	Documents Supplied to Personnel	29
165	5.4	Audit Logging Procedures.....	29
166	5.4.1	Types of Events Recorded	29
167	5.4.2	Frequency of Processing Log	29
168	5.4.3	Retention Period for Audit Log.....	29
169	5.4.4	Protection of Audit Log.....	29
170	5.4.5	Audit Log Backup Procedures.....	29
171	5.4.6	Audit Collection System (Internal vs. External)	29
172	5.4.7	Notification to Event-Causing Subject.....	29
173	5.4.8	Vulnerability Assessments.....	29
174	5.5	Records Archival	29
175	5.5.1	Types of Records Archived	29
176	5.5.2	Retention Period for Archived Audit Logging Information.....	29
177	5.5.3	Protection of Archive.....	29
178	5.5.4	Archive Backup Procedures.....	30
179	5.5.5	Requirements for Time-Stamping of Record.....	30
180	5.5.6	Archive Collection System (internal or external).....	30
181	5.5.7	Procedures to Obtain and Verify Archived Information.....	30
182	5.6	Key Changeover.....	30
183	5.7	Compromise and Disaster Recovery	30
184	5.7.1	Incident and Compromise Handling Procedures.....	30
185	5.7.2	Corruption of Computing Resources, Software, and/or Data	30
186	5.7.3	Entity Private Key Compromise Procedures.....	30
187	5.7.4	Business Continuity Capabilities After a Disaster.....	30
188	5.8	CA or RA Termination	30
189	6	Technical Security Controls	31
190	6.1	Key Pair Generation and Installation.....	31
191	6.1.1	Key Pair Generation.....	31
192	6.1.2	Private Key Delivery to Subscriber	31
193	6.1.3	Public Key Delivery to Certificate Issuer.....	31
194	6.1.4	CA Public Key Delivery to Relying Parties	31
195	6.1.5	Key Sizes	31
196	6.1.6	Public Key Parameters Generation and Quality Checking.....	31
197	6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	31

198	6.2	Private Key Protection and Cryptographic Module Engineering Controls	31
199	6.2.1	Cryptographic Module Standards and Controls	31
200	6.2.2	Private Key (n out of m) Multi-person Control.....	31
201	6.2.3	Private Key Escrow	31
202	6.2.4	Private Key Backup	31
203	6.2.5	Private Key Archival.....	31
204	6.2.6	Private Key Transfer into or from a Cryptographic Module.....	32
205	6.2.7	Private Key Storage on Cryptographic Module	32
206	6.2.8	Method of Activating Private Key.....	32
207	6.2.9	Method of Deactivating Private Key.....	32
208	6.2.10	Method of Destroying Private Key	32
209	6.2.11	Cryptographic Module Rating	32
210	6.3	Other Aspects of Key Pair Management	32
211	6.3.1	Public key archival	32
212	6.3.2	Certificate operational periods and key pair usage periods	32
213	6.4	Activation Data	32
214	6.4.1	Activation Data Generation and Installation.....	32
215	6.4.2	Activation Data Protection	32
216	6.4.3	Other Aspects of Activation Data	33
217	6.5	Computer Security Controls	33
218	6.5.1	Specific Computer Security Technical Requirements.....	33
219	6.5.2	Computer Security Rating.....	33
220	6.6	Life Cycle Security Controls	33
221	6.6.1	System Development Controls.....	33
222	6.6.2	Security Management Controls.....	33
223	6.6.3	Life Cycle Security Controls	33
224	6.7	Network Security Controls	33
225	6.8	Time Stamp Process	33
226	7	Certificate, CRL, and OCSP Profiles.....	34
227	7.1	Certificate Profile.....	34
228	7.1.1	Version Number(s)	34
229	7.1.2	Certificate Extensions	34
230	7.1.3	Algorithm Object Identifiers	34
231	7.1.4	Name Forms	34
232	7.1.5	Name Constraints	34

233	7.1.6	Certificate Policy Object Identifier	34
234	7.1.7	Usage of Policy Constraints Extension.....	34
235	7.1.8	Policy Qualifiers Syntax and Semantics	34
236	7.1.9	Processing Semantics for the Critical Certificate Policies Extension	34
237	7.2	CRL Profile	34
238	7.2.1	Version number(s).....	34
239	7.2.2	CRL and CRL entry extensions	34
240	7.3	OCSP Profile.....	34
241	7.3.1	Version Number(s)	34
242	7.3.2	OCPS Extension.....	34
243	8	Compliance Audit and Other Assessment.....	35
244	8.1	Frequency or Circumstances of Assessment.....	35
245	8.2	Identity / Qualifications of Assessor.....	35
246	8.3	Assessor's Relationship to Assessed Entity	35
247	8.4	Topics Covered by Assessment	35
248	8.5	Actions Taken as a Result of Deficiency	35
249	8.6	Communication of Results	35
250	9	Other Business and Legal Matters.....	36
251	9.1	Fees.....	36
252	9.1.1	Certificate Issuance or Renewal fees.....	36
253	9.1.2	Certificate Access fees.....	36
254	9.1.3	Revocation or Status Information Access fees	36
255	9.1.4	Fees for other Services	36
256	9.1.5	Refund Policy.....	36
257	9.2	Financial Responsibility	36
258	9.2.1	Insurance Coverage	36
259	9.2.2	Other Assets	36
260	9.2.3	Insurance or Warranty Coverage for End-Entities	36
261	9.3	Confidentiality of Business Information.....	36
262	9.3.1	Scope of Confidential Information	36
263	9.3.2	Information not within the Scope of Confidential Information	36
264	9.3.3	Responsibility to Protect Confidential Information.....	36
265	9.4	Privacy of Personal Information	36
266	9.4.1	Privacy plan	36
267	9.4.2	Information treated as private	36

268	9.4.3	Information not deemed private.....	36
269	9.4.4	Responsibility to protect private information.....	37
270	9.4.5	Notice and consent to use private information	37
271	9.4.6	Disclosure pursuant to judicial or administrative process	37
272	9.4.7	Other information disclosure circumstances	37
273	9.5	Intellectual Property Rights.....	37
274	9.5.1	Intellectual Property Rights in Certificates and Revocation Information	37
275	9.5.2	Intellectual Property Rights in CP	37
276	9.5.3	Intellectual Property Rights in Names.....	37
277	9.5.4	Property rights of Certificate Owners	37
278	9.6	Representations and Warranties	37
279	9.6.1	CA representations and warranties.....	37
280	9.6.2	RA representations and warranties.....	37
281	9.6.3	Subscriber representations and warranties	37
282	9.6.4	Relying party representations and warranties	37
283	9.6.5	Representations and warranties of other participants	37
284	9.7	Disclaimers of Warranties	37
285	9.8	Limitations of Liability	37
286	9.9	Indemnities.....	37
287	9.10	Term and Termination.....	38
288	9.10.1	Term	38
289	9.10.2	Termination	38
290	9.10.3	Effect of Termination and Survival	38
291	9.11	Individual Notices and Communication with Participants	38
292	9.12	Amendments	38
293	9.12.1	Procedure for Amendment	38
294	9.12.2	Notification Mechanism and Period.....	38
295	9.12.3	Circumstances under which OID must be changed.....	38
296	9.13	Dispute Resolution Provisions	38
297	9.14	Governing Law	38
298	9.15	Compliance with Applicable Law.....	38
299	9.16	Miscellaneous Provisions	38
300	9.16.1	Entire Agreement	38
301	9.16.2	Assignment	38
302	9.16.3	Severability	39

303	9.16.4	Enforcement (attorneys' fees and waiver of rights).....	39
304	9.16.5	Force Majeure	39
305	9.17	Other Provisions	39
306	9.17.1	Order of Precedence of CP	39
307	10.	References.....	40
308			
309			

310 1 Introduction

311 This document is structured according to RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy
312 and Certification Practices Framework" [RFC3647].

313 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
314 "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14
315 [RFC2119] [RFC8174] even in case the keywords are not capitalized.

316 1.1 Overview

317 This document describes the Certification Practice Statement of the Siemens Product PKI Certificate Management
318 Service (in the following called "Product PKI") of the Tenant providing Infrastructure Certificates for all other
319 Product PKI Tenants.

320 Together with the central CPS [CCPS] it describes the services provided by the Product PKI as well as binding
321 requirements that must be fulfilled by Product PKI participants. In case there are no additional requirements defined
322 by the tenant (in this document, i.e. Tenant CPS), the respective section will refer to the Central CP. In case specific
323 requirements are listed they will apply in addition to the requirements set forth in the Central CP. Under no
324 circumstances, provisions set forth in this document can weaken the requirements set forth in the Central CP.

325 Moreover - together with the CPSs – the CPs also define the certification process as well as the cooperation, duties
326 and rights of the Product PKI participants.

327 The Product PKI is a PKI that provides and manages certificates (e.g. "IDevID certificates" or "Manufacturer Device
328 certificates") that are stored on and used by Siemens products and solutions. The private key might be used in
329 bootstrapping scenarios for authentication purposes. Or the certificate might be used to proof that the device is
330 a genuine Siemens device.

331 Unless otherwise stated, the term "Product PKI" or any of its entities, refer to "Siemens Product PKI Certificate
332 Management Service", or any of its respective entities, for the rest of this Certificate Policy.

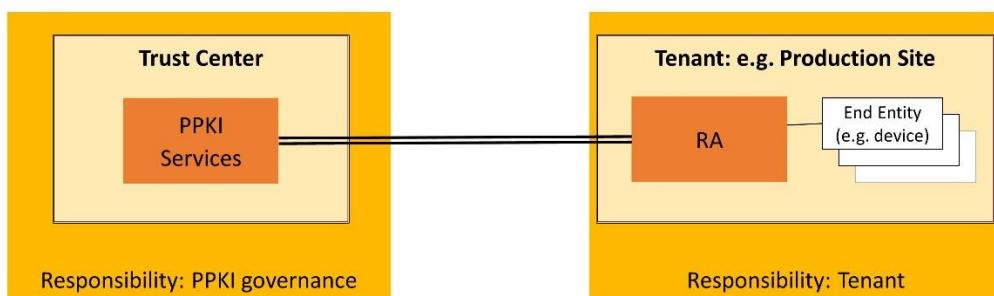
333 Since different stakeholders are involved, also responsibilities are distributed between these stakeholders:

- 334 • **Product PKI Governance:** responsible for the Product PKI service is the organization listed in section 0

335 • Policy Administration.

336 • **IT Services:** The central Product PKI service is hosted in the Siemens Trust Center that is operated and
337 managed by Siemens IT department.

338 • **Tenant:** Tenant can be every Siemens AG organizational unit or any other legal entity that has a contract in
339 place that covers Product PKI services. The Tenants typically operate and maintain the registrations authorities
340 (e.g. within their production facilities or data center). Therefore, the Tenants are responsible for RA operation
341 and End-Entity authentication.



342

343 **Figure 1: Stakeholders and typical responsibility split**

344 In accordance with this responsibility split, there are two Certificate Policies, one for the central part of the Product
345 PKI (Central CP) and additional ones for the Tenant specific aspects (this document).

346 The same holds for the corresponding Certification Practice Statements (CPSs).

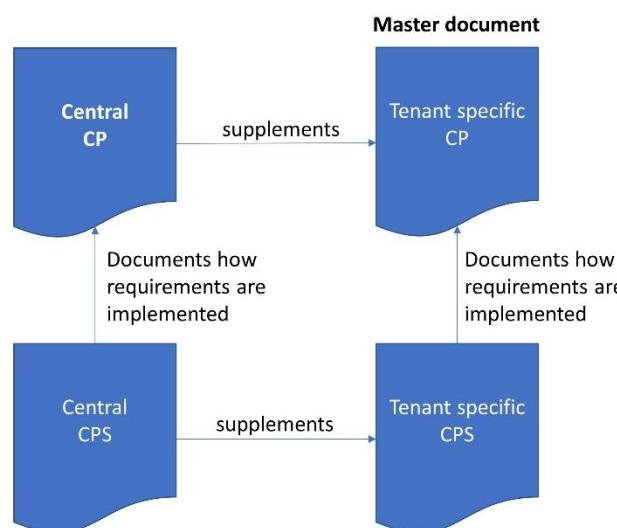
347 The Tenant specific CP is always the master document. It defines all requirements for which the Tenant is
348 responsible for. In particular, it comprises the management and operation of the RAs and/or LRAs, of publicly
349 accessible repositories. Where appropriate, the Tenant specific CP will also refer to requirements valid for the
350 operation of the central service. In that case the phrase "See also Central CP for central service aspects". In those
351 sections that are not relevant for the Tenant, it is referred to the central CP by using the phrase "See central CP".

352 The Tenant specific CP is supplemented with the Central CP. In particular, the Central CP comprises all
353 requirements for the management and operation of the Central PKI System including Root CA and Issuing CAs.

354 The Tenant CPS describes how the requirements defined in the Tenant CP are implemented.

355 In addition, the Central CPS supplements how the requirements defined in the Central CP are implemented.

356 The different documents and their interrelation are depicted in the following figure:

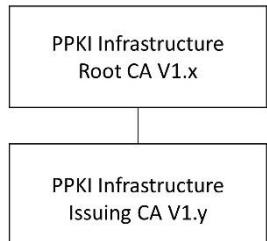


357

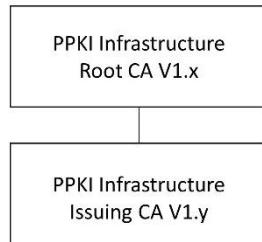
358 **Figure 2: Document structure (CP and CPS)**

359 In addition to the requirements defined in this CP and the corresponding CPSs, Siemens IT systems are operated
360 according to the Siemens internal information security rules and respective execution guidelines, which define
361 how IT systems must be operated securely. The corresponding documents can be retrieved on request.
362 These rules are part of a Siemens ISMS [ISMS], which is defined and implemented according to ISO 27001.

363 **1.1.1 PKI hierarchy**



364 The specific PKI hierarchy is shown in
365 Figure 3.



366
367 **Figure 3: PPKI hierarchy for Infrastructure Certificates**

368 The Issuing CA for Siemens Product PKI Infrastructure Certificates issues certificates that are used (together with
369 the corresponding private keys) to identify and authenticate the different Tenants to provide the right, Tenant
370 specific services (e.g. issuing CAs). These certificates are typically deployed on Local RAs, managed by the Tenants,
371 but also on PPKI core components to correctly identify them and guarantee authenticated and integrity protected
372 connections between the Tenants and the PPKI component, e.g. CMP gateway, or any generic PPKI servers.

373 **1.2 Document Name and Identification**

374 This CPS is referred to as Certificate Practice Statement for the 'Siemens Product PKI Infrastructure Certificates'.

375 Title: Product PKI Certificate Management Service – Certification Practice Statement for Siemens
376 Product PKI Infrastructure Certificates

377 OIDs: See Product PKI Certificate Management Service – Certificate Policy for Siemens Product PKI
378 Infrastructure Certificates [ICP]

379 Expiration: This version of the document is the most current one until a subsequent release.

380 The set of all documents describing the Siemens Product PKI is referred to under the OID 1.3.6.1.4.1.4329.99.1.2.

381 **1.3 PKI Participants**

382 See Central CP.

383 **1.3.1 Certification Authorities**

384 A graphical overview of the CA hierarchy is depicted in Figure 3: PPKI hierarchy for Infrastructure Certificates.

385 1.3.1.1 Root CA

386 See Central CP.

387 1.3.1.2 Intermediate CA

388 See Central CP.

389 1.3.1.3 Issuing CAs

390 See Central CP.

391 **1.3.2 Registration Authorities**

392 See Central CP.

393 **1.3.3 Subscribers**

394 See Central CP.

395 **1.3.4 Relying Parties**

396 See Central CP.

397 **1.3.5 Other Participants**

398 1.3.5.1 Subject (End-Entity)

399 See Central CP.

400 **1.4 Certificate Usage**

401 **1.4.1 Appropriate Certificate Usage**

402 See Central CP.

403 **1.4.2 Prohibited Certificate Usage**

404 See Central CP.

405

406 **1.5 Policy Administration**

407 **1.5.1 Organization Administering the Document**

408 The organization responsible for drafting, maintaining, and updating this CP is:

409 Siemens Aktiengesellschaft ("Siemens AG")

410 Technology ("T") Research & Predevelopment 1 ("RPD1")

411 Otto-Hahn-Ring 6, 81739 Munich, GERMANY

412 E-mail: [contact.pki \(at\) siemens.com](mailto:contact.pki(at)siemens.com)

413 Website: <https://www.siemens.com/pki>

414 **1.5.2 Contact Person**

415 Questions about this CP may be sent to:

416 Siemens AG

417 FT RPD CST

418 Attn: Product PKI

419 Otto-Hahn-Ring 6, 81739 Munich, GERMANY

420 E-mail: [contact.pki \(at\) siemens.com](mailto:contact.pki(at)siemens.com)

421 Certificate Problem Reports shall be sent to: [contact.pki \(at\) siemens.com](mailto:contact.pki(at)siemens.com)

422 **1.5.3 Person Determining CP and CPS Suitability for the Policy**

423 The Policy Management Authority (Tenant PMA) in section 1.5.1 determines suitability of this document and the
424 respective CPS.

425 **1.5.4 CPS Approval Procedures**

426 An annual risk assessment is carried out to evaluate business requirements and determine the security
427 requirements to be included in the certificate policy for the stated community and applicability. In addition, the CP
428 as well as the CPS will be reviewed every year regarding consistency with the actual PKI processes and services (see
429 also section 8).

430 This document is accepted and approved by the Central PMA. Acceptance of the Siemens ACP process (which is
431 part of the Siemens ISMS) constitutes acceptance of this document which therefore will not be explicitly signed.
432 However, in case minor changes of this document will be necessary (see also 9.12.3), a new version will be
433 published after release and official approval will be part of the next Siemens ACP process review.

434 1.6 Definitions and Acronyms

435 1.6.1 Definitions

436	Authority Revocation List	Certificate Revocation List containing CA certificates.
437	CA certificate	Certificate for a Certification Authority's public key.
438	Central PMA	PMA that is responsible for the management and operation of the Central Product PKI Certificate Management service.
439	Central Product PKI System	Technical components of the Product PKI Certificate Management System that are managed and operated in the Siemens Trust Center facility.
440	Certificate Policy (CP)	Compare section 1.1.
441	Certification Authority (CA)	Authority, that is entitled to certify public keys; compare section 1.3.1.
442	Distinguished Name	Sequence of data-fields uniquely identifying e.g. the issuer and the Subject within a certificate or a CRL. The format of a Distinguished Name is defined in the [X.520] standard.
443	EE certificate	See "End-Entity certificate".
444	End-Entity	Equivalent to Subject; the identity of the End-Entity is connected to the certificate and the related key-pair. See also section 1.3.3.
445	End-Entity certificate	A digital certificate is used to prove ownership of a public key and the corresponding private key. It must not be used for certifying and issuing CRLs or other certificates.
446	End-User certificate	See "End-Entity certificate".
447	HSM	Hardware Security Modul that can be used for random number generation and generation and storage of secret keys. The HSM can use the keys for digital signatures and for other PKI-applications.
448	Intermediate CA	Entity that issues and manages certificates of further Intermediate CAs or Issuing CAs and has a certificate signed by either a Root CA or by an Intermediate CA.
449	Issuing CA	Entity that issues and manages certificates of End Entities and has a certificate signed by either a Root CA or by an Intermediate CA.
450	Issuing CA System	Technical components (hardware and software) hosting Issuing and Intermediate CAs.
451	Multi-person Control	Sensitive activities typically are carried out by more than one person holding a trusted role. This is called Multi-person control.
452	Policy Management Authority	A body (of Siemens) that is responsible for setting, implementing and administering policy decisions regarding this CP and related documents and agreements in the Product PKI
453	Product PKI	Term used in this document for the Siemens Product PKI Certificate Management Service (due to ease of readability).
454	Product PKI System	Technical components (central and local) that are necessary to manage and operate the Product PKI Certificate Management System.
455	Qualified Auditor	Auditor who has appropriate knowledge in order to evaluate and assess and confirm the requirements and corresponding implementation of measures defined in the Certificate Policy documents and the Certification Practice Statements, respectively.
456	Registration Authority (RA)	PKI-incorporated facility for participant-authentication. See also section 1.3.2.
457		

484	Relying Party	Individual or legal entity that uses certificates; see also section 1.3.5.
485		
486	Root CA	Entity that issues and manages certificates of Intermediate or Issuing CAs (in case there do not exist Intermediate CAs). The certificate of the Root CA is self-signed.
487		
488		
489	Root CA System	Technical components (hardware and software) hosting Root and (optionally) Intermediate CAs.
490		
491	Secure Device	A component (such as a Smart Card or HSM) that substantiated to protect the private key stored in that device. All cryptographic operations using the private key are performed inside this Secure Device.
492		
493		
494		
495	Siemens Product PKI Certificate Management Service	Siemens internal organization that issues and manages certificates. This organization operates the Root CA System as well as the Issuing CA systems.
496		
497		
498		
499	Smart Card	Integrated circuit card including a micro-processor that can be used for random number generation and generation and storage of secret keys. A Smart Card can use the keys for the generation of digital signatures and for other PKI-applications
500		
501		
502		
503	Subject	End-Entity that uses the private End-Entity key (EE key). The End-Entity may differ from the Subscriber.
504		
505	Subscriber	Subscriber for all certificates issued by the Product PKI is the respective Tenant as legal entity. See also section 1.3.3.
506		
507		
508	Tenant	Tenant can be every Siemens AG organizational unit or any other legal entity that has a contract in place that covers Product PKI services. The Tenants typically operate and maintain the Registration Authorities (e.g. within their production facilities or data center). In such a case the Tenants are responsible for RA operation and End-Entity authentication.
509		
510		
511		
512		
513		
514	Tenant PMA	PMA that is responsible for the management and operation of the local Product PKI Certificate Management components such as RA and/or LRA as well as for identification of End-Entities.
515		
516		
517	Token	Transport-medium for certificates and keys
518	Trust Center	The term "Trust Center" refers to assets and components that are centrally operated and maintained at the Trust Center location as well to the respective processes.
519		
520		
521	Trusted Operator	Product PKI has the overall responsibility of issuing certificates to Subjects and managing and revoking certificates. Tenants delegate may delegate parts or these functions to the Central Product PKI Certificate Management Service or to other internal Service Providers of Siemens, which are called Trusted Operators
522		
523		
524		
525		

526	1.6.2	Acronyms
527	ARL	Authority Revocation List
528	CA	Certification Authority
529	CISO	Chief Information Security Officer
530	CMP	Certificate Management Protocol (RFC 4210)
531	CN	Common Name
532	CP	Certificate Policy
533	CPS	Certification Practice Statement
534	CRL	Certificate Revocation List
535	DN	Distinguished Name
536	EE	End-Entity
537	FIPS	Federal Information Processing Standard
538	FQDN	Fully qualified domain name
539	HSM	Hardware Security Module
540	IEEE	Institute of Electrical and Electronics Engineers
541	IETF	Internet Engineering Task Force
542	IDevID	Initial Device Identifier (IEEE 802.1AR)
543	ISO	International Organization for Standardization
544	ISMS	Information Security Management System
545	LDevID	Locally significant Device Identifier (IEEE 802.1AR)
546	OCSP	Online Certificate Status Protocol
547	OID	Object Identifier
548	PIN	Personal Identification Number
549	PKI	Public Key Infrastructure
550	PPKI	Product PKI
551	PMA	Policy Management Authority
552	RA	Registration Authority
553	RFC	Request for Comment
554	SLA	Service Level Agreement
555	URL	Uniform Resource Locator
556	UTF8	Unicode Transformation Format-8

557 **2 Publication and Repository Responsibilities**

558 **2.1 Repositories**

559 Tenant specific Product PKI Repositories are operated by trusted service provider(s).

560 The repository responsibilities include:

- 561 1. accurately publishing information;
- 562 2. archiving certificates;
- 563 3. publishing the status of certificates;
- 564 4. promptness or frequency of publication; and
- 565 5. security of the repository and controlling access to information published on the repository to prevent unauthorized access and tampering.

567 Subjects and Relying Parties have access to:

- 568 • Certificate Revocation List (CRL)

- 569 • and OCSP responder

570 via: ppki-va.siemens.com .

571 **2.2 Publication of Certification Information**

572 The Tenant publishes certificate status information at ppki-va.siemens.com .

573 The CP is published on the website specified in section 1.5.1 Organization Administering the Document.

574 **2.3 Time or Frequency of Publication**

575 Updates to this CPS and the Central CPS are published in accordance with the definitions in section 9.12 of this document.

577 **2.4 Access Controls on Repositories**

578 Information published in the repository can be accessed with read-only access.

579 Administration of the published information shall be carried out only by trusted roles with adequate access control restrictions.

581 **3 Identification and Authentication**

582 **3.1 Naming**

583 **3.1.1 Types of Names**

584 The complete policy of specifying names and CA certificate profiles is documented for each certificate type in the
585 respective Certificate Profile Documentation [PROF], which can be retrieved on request.

586 **3.1.2 Need of Names to be Meaningful**

587 **3.1.2.1 CA Names**

588 The CN must be stated as the full name of the CA.

589 **3.1.2.2 End-Entity Names**

590 For details see Certificate Profile Documentation [PROF].

591 **3.1.3 Anonymity or Pseudonymity of Subscribers**

592 **3.1.3.1 CA Names**

593 See Infrastructure Tenant CP.

594 **3.1.3.2 End-Entity Names**

595 See Infrastructure Tenant CP.

596 **3.1.4 Rules for Interpreting Various Name Forms**

597 See Central CP.

598 **3.1.5 Uniqueness of Names**

599 **3.1.5.1 CA Names**

600 See Central CP.

601 **3.1.5.2 End-Entity Names**

602 See Infrastructure Tenant CP.

603 **3.1.6 Recognition, Authentication, and Roles of Trademarks**

604 See Central CP.

605 **3.2 Initial Identity Validation**

606 See also Infrastructure Tenant CP.

607 **3.2.1 Method to Prove Possession of Private Key**

608 The key pairs are either generated by the corresponding issuing CA or by the End-Entity in case of automatic
609 certificate update. In the latter case proof of private key possession is realized via state-of-the-art certificate
610 management protocol, e.g. CMP.

611 **3.2.2 Authentication of Organization Identity**

612 The identity of the requesting organization is checked as part of the onboarding process.

613 **3.2.3 Authentication of Individual Identity**

614 The individual identity of the corresponding (L)RA, or End-Entity, is determined within the onboarding process.

615 **3.2.4 Non-verified Subscriber Information**

616 See Infrastructure Tenant CP.

617 **3.2.5 Validation of Authority**

618 The authority of the requester is checked as part of the onboarding process.

619 **3.2.6 Criteria for Interoperation**

620 See Infrastructure Tenant CP.

621 **3.3 Identification and Authentication for Re-key Requests**

622 **3.3.1 Identification and Authentication for Routine Re-Key**

623 See central CP.

624 **3.3.2 Identification and Authentication for Re-Key After Revocation**

625 Not supported.

626 **3.4 Identification and Authentication for Revocation Requests**

627 Revocation requests can be initialized either manually via MyIT portal or by the (L)RA. In the first case only requests
628 from such persons listed in the onboarding checklist will be accepted. In the second case only revocation requests
629 from a specific RA for its own keys are accepted.

630 4 Certificate Lifecycle Operational Requirements

631 4.1 Certificate Application

632 4.1.1 Who can submit a certificate application?

633 4.1.1.1 Root and Intermediate CA

634 See Central CP.

635 4.1.1.2 Issuing CAs

636 See Central CP.

637 4.1.1.3 End-Entity Certificates

638 EE certificates (for examples, certificates used by RAs or by PPKI service internal components to authenticate
639 against the central services) are generated as part of the onboarding process.

640 4.1.2 Enrollment Process and Responsibilities

641 4.1.2.1 CA Certificates

642 See Infrastructure Tenant CP.

643 4.1.2.2 End-Entity Certificate

644 The End-Entity certificate and the corresponding private key is generated by the central service. The private key
645 material is securely transported via a PKCS#12 container. Certificate application is carried out by the Trust Center
646 personnel.

647 4.2 Certificate Application Processing

648 4.2.1 Performing identification and authentication functions

649 Identity information is checked as part of the onboarding process.

650 4.2.2 Approval or Rejection of Certificate Applications

651 See Infrastructure Tenant CP and section 4.2.1.

652 4.2.3 Time to Process Certificate Applications

653 See Central CP.

654 4.3 Certificate Issuance

655 4.3.1 CA Actions during Certificate Issuance

656 See Infrastructure Tenant CP.

657 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

658 The End-Entity (e.g., the operator of a RA), for which the subscriber has requested a certificate, is notified via
659 email w.r.t. the status of certificate issuance. The initial key material as PKCS#12 container is securely sent via
660 encrypted and signed email to the first technical contact listed in the onboarding check list. The passphrase for
661 the PKCS12 container is sent via signed and encrypted email to the second technical contact listed in the
662 onboarding checklist.

663 4.4 Certificate Acceptance

664 4.4.1 Conduct constituting certificate acceptance

665 See Infrastructure Tenant CP.

666 **4.4.2 Publication of the certificate by the CA**
667 Relying parties of the Infrastructure CA are the BUs. Terms and conditions are made available to the relying parties
668 as part of the ordering process.

669 **4.4.3 Notification of Certificate issuance by the CA to other entities**
670 No stipulation.

671 **4.5 Key Pair and Certificate Usage**
672 See Infrastructure Tenant CP

673 **4.5.1 Subject Private Key and Certificate Usage**
674 See Central CP.

675 **4.5.2 Relying Party Public Key and Certificate Usage**
676 See Central CP.

677 **4.6 Certificate Renewal**
678 Certificate renewal is the issuance of a new certificate to an entity without changing the public key or any other
679 information in the certificate.
680 Not supported.

681 **4.6.1 Circumstance for Certificate Renewal**
682 No stipulation.

683 **4.6.2 Who may request renewal?**
684 No stipulation.

685 **4.6.3 Processing Certificate Renewal Request**
686 No stipulation.

687 **4.6.4 Notification of new Certificate Issuance to Subscriber**
688 No stipulation.

689 **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**
690 No stipulation.

691 **4.6.6 Publication of the Renewal Certificate by the CA**
692 No stipulation.

693 **4.6.7 Notification of Certificate Issuance by the CA to other Entities**
694 No stipulation.

695 **4.7 Certificate Re-key**
696 "Re-key" addresses the generating of a new Key Pair and applying for the issuance of a new certificate and
697 replacing the existing Key Pair.

698 **4.7.1 Circumstances for Certificate Re-key**
699 See Central CP.

700 **4.7.2 Who may request certification of a new Public Key?**
701 4.7.2.1 Re-keying of an Issuing CA certificate
702 See Central CP.

703 4.7.2.2 Re-keying of End-Entity certificates
704 The End-Entity, prior to the expiration of its certificate, will authenticate against the CA with its still valid certificate
705 and initiate the issuance of a new certificate.

706 **4.7.3 Processing Certificate Re-keying Requests**

707 See section 4.3.1

708 **4.7.4 Notification of new Certificate Issuance to Subscriber**

709 See section 4.3.2

710 **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

711 See section 4.4.1

712 **4.7.6 Publication of the Re-keyed Certificate by the CA**

713 See section 4.4.2

714 **4.7.7 Notification of Certificate Issuance by the CA to other Entities**

715 See section 4.4.3

716 **4.8 Certificate Modification**

717 Certificate modification means that the keys of a certificate remain unchanged, but more certificate information
718 than for a certificate renewal is changed.

719 Not supported.

720 **4.8.1 Circumstance for Certificate Modification**

721 No stipulation.

722 **4.8.2 Who may request Certificate modification?**

723 No stipulation.

724 **4.8.3 Processing Certificate Modification Requests**

725 No stipulation.

726 **4.8.4 Notification of new Certificate Issuance to Subscriber**

727 No stipulation.

728 **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

729 No stipulation.

730 **4.8.6 Publication of the Modified Certificate by the CA**

731 No stipulation.

732 **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

733 No stipulation.

734 **4.9 Certificate Revocation and Suspension**

735 **4.9.1 Circumstances for Revocation**

736 See Central CP.

737 **4.9.2 Who can request revocation?**

738 RA owners can request revocation of the EE certificates that have been issued for their RA.

739 **4.9.3 Procedure for Revocation Request**

740 RA owners can request revocation of their EE certificates either manually by generating a ticket in MyIT or via the
741 RA using CMP.

742 See also section 3.4.

743 **4.9.4 Revocation Request Grace Period**

744 See Central CP.

745 **4.9.5 Time within which CA must Process the Revocation Request**

746 See Central CP.

747 **4.9.6 Revocation Checking Requirement for Relying Parties**

748 Relying Parties shall check the status of certificates on which they wish to rely by consulting the most recent CRL or
749 using another applicable method.

750 **4.9.7 CRL Issuance Frequency**

751 ARLs are regularly issued every 6 month or in exceptional cases when a specific CA certificate needs to be revoked.

752 CRLs are regularly issued once per day or in exceptional cases when a specific EE certificate needs to be revoked.

753 **4.9.8 Maximum Latency for CRLs**

754 CRLs shall be posted to the repository within a reasonable time after generation.

755 **4.9.9 On-line Revocation/Status Checking Availability**

756 Not supported.

757 **4.9.10 On-line Revocation Checking Requirements**

758 No stipulation.

759 **4.9.11 Other Forms of Revocation Advertisements Available**

760 No stipulation.

761 **4.9.12 Special Requirements for Private Key Compromise**

762 Beside issuing a new ARL the RA owners will be informed via signed email.

763 If the RA operator has a reason to believe that there has been a compromise of an EE private key, then it shall
764 notify the respective Issuing CA to take appropriate action, including request for revocation.

765 See also central CP for central service aspects.

766 **4.9.13 Circumstances for Suspension**

767 Not supported.

768 **4.9.14 Who can request suspension?**

769 No stipulation.

770 **4.9.15 Procedure for suspension request**

771 No stipulation.

772 **4.9.16 Limits on suspension period**

773 No stipulation.

774 **4.10 Certificate Status Services**

775 **4.10.1 Operational Characteristics**

776 See section 4.9.

777 **4.10.2 Service Availability**

778 The service to retrieve CRLs shall be available twenty-four (24) hours a day, seven (7) days a week, except in case
779 of Force Majeure Events (CP section 9.16.5).

780 **4.10.3 Optional Features**

781 No stipulation.

782 **4.11 End of Subscription**

783 See Central CP.

784 **4.12 Key Escrow and Recovery**

785 Not supported.

786 **4.12.1 Key Escrow and Recovery Policy and Practices**

787 No stipulation.

788 **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

789 No stipulation.

790 5 Management, Operational, and Physical Controls

791 As this tenant for providing key material and certificates to securely connect RAs with the Central Product PKI
792 service is operated as part of the Central PPKI service, all relevant requirements are set forth in the Central CP
793 [CP].

794 5.1 Physical Security Controls

795 5.1.1 Site Location and Construction

796 See Central CPS [CCPS]

797 5.1.2 Physical Access

798 See Central CPS [CCPS].

799 5.1.3 Power and Air Conditioning

800 See Central CPS [CCPS].

801 5.1.4 Water Exposure

802 See Central CPS [CCPS].

803 5.1.5 Fire Prevention and Protection

804 See Central CPS [CCPS].

805 5.1.6 Media Storage

806 See Central CPS [CCPS].

807 5.1.7 Waste Disposal

808 See Central CPS [CCPS].

809 5.1.8 Off-site Backup

810 See Central CPS [CCPS].

811 5.2 Procedural Controls

812 5.2.1 Trusted Roles

813 See Central CPS [CCPS].

814 5.2.2 Numbers of Persons Required per Task

815 See Central CPS [CCPS].

816 5.2.3 Identification and Authentication for Each Role

817 See Central CPS [CCPS].

818 5.2.4 Roles Requiring Separation of Duties

819 See Central CPS [CCPS].

820 5.3 Personnel Controls

821 5.3.1 Qualifications, Experience and Clearance Requirements

822 See Central CPS [CCPS].

823 5.3.2 Background Check Procedures

824 See Central CPS [CCPS].

825 **5.3.3 Training Requirements**
826 See Central CPS [CCPS].

827 **5.3.4 Retraining Frequency and Requirements**
828 See Central CPS [CCPS].

829 **5.3.5 Job Rotation Frequency and Sequence**
830 See Central CPS [CCPS].

831 **5.3.6 Sanctions for Unauthorized Actions**
832 See Central CP.

833 **5.3.7 Independent Contractor Requirements**
834 See Central CP.

835 **5.3.8 Documents Supplied to Personnel**
836 See Central CP.

837 **5.4 Audit Logging Procedures**

838 **5.4.1 Types of Events Recorded**
839 See Central CPS [CCPS].

840 **5.4.2 Frequency of Processing Log**
841 See Central CP.

842 **5.4.3 Retention Period for Audit Log**
843 See Central CPS [CCPS].

844 **5.4.4 Protection of Audit Log**
845 See Central CPS [CCPS].

846 **5.4.5 Audit Log Backup Procedures**
847 See Central CPS [CCPS].

848 **5.4.6 Audit Collection System (Internal vs. External)**
849 See Central CPS [CCPS].

850 **5.4.7 Notification to Event-Causing Subject**
851 See Central CP.

852 **5.4.8 Vulnerability Assessments**
853 See Central CPS [CCPS].

854 **5.5 Records Archival**

855 **5.5.1 Types of Records Archived**
856 CPS: See Central CPS [CCPS].

857 **5.5.2 Retention Period for Archived Audit Logging Information**
858 See Central CPS [CCPS].

859 **5.5.3 Protection of Archive**
860 See central CP.

861 See Central CPS [CCPS].

862 **5.5.4 Archive Backup Procedures**

863 See Central CPS [CCPS].

864 **5.5.5 Requirements for Time-Stamping of Record**

865 See Central CP.

866 **5.5.6 Archive Collection System (internal or external)**

867 See Central CPS [CCPS].

868 **5.5.7 Procedures to Obtain and Verify Archived Information**

869 See Central CP.

870 **5.6 Key Changeover**

871 In the event of a CA key changeover, the new CA public key should be published early enough to allow the timely distribution of the new public key.

873 For example, if a EE certificate is valid for 1 year, the issuing CA certificate for 5 years and the root CA certificate is valid for 20 years then the issuing CA should be renewed not later than 15 months before the expiration of its certificate. The root CA certificate should be renewed not later than 5.25 years before the expiration of its certificate.

877 **5.7 Compromise and Disaster Recovery**

878 **5.7.1 Incident and Compromise Handling Procedures**

879 See Central CP.

880 **5.7.2 Corruption of Computing Resources, Software, and/or Data**

881 See Central CP.

882 **5.7.3 Entity Private Key Compromise Procedures**

883 See Central CP.

884 **5.7.4 Business Continuity Capabilities After a Disaster**

885 See Central CP.

886 **5.8 CA or RA Termination**

887 See central CP.

888 6 Technical Security Controls

889 6.1 Key Pair Generation and Installation

890 6.1.1 Key Pair Generation

891 Private keys for infrastructure certificates are centrally created by used PKI software.

892 In case of automated re-keying the private key is created by the End-Entity starting from the first re-key.

893 6.1.2 Private Key Delivery to Subscriber

894 The centrally generated private keys are securely distributed via signed and encrypted email within PKCS#12
895 containers to the first technical contact listed in the onboarding checklist. The corresponding passphrase for the
896 PKCS#12 container is sent via signed and encrypted email to the second technical contact listed in the onboarding
897 checklist.

898 The PKCS#12 container, together with its password, are deleted upon sending them to the tenants.

899 6.1.3 Public Key Delivery to Certificate Issuer

900 In case of centrally generated key pairs no public key needs to be delivered to the CA.

901 In case of automatic rekeying the certification request (incl. the public key) is securely transmitted via CMP over
902 TLS (using the still valid keys that will be updated via this request).

903 6.1.4 CA Public Key Delivery to Relying Parties

904 Relying party is only the central PPKI service. The delivery of CA public keys is performed as part of the initial key
905 event (set-up of issuing CA).

906 See also Central CP [CCP].

907 6.1.5 Key Sizes

908 See Infrastructure Tenant CP.

909 6.1.6 Public Key Parameters Generation and Quality Checking

910 Centrally generated Key Pairs are generated in Hardware Security Modules certified according to FIPS 140-2 level
911 3.

912 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

913 See Central CP.

914 6.2 Private Key Protection and Cryptographic Module Engineering Controls

915 6.2.1 Cryptographic Module Standards and Controls

916 It is strongly recommended that end-entities securely store the private key (e.g. within a TPM if possible).

917 See also central CP for central service aspects.

918 6.2.2 Private Key (n out of m) Multi-person Control

919 4 eyes principle is applied for private keys of end entities (see 6.1.2 Private Key Delivery to Subscriber).

920 See also central CP for central service aspects.

921 6.2.3 Private Key Escrow

922 No supported.

923 6.2.4 Private Key Backup

924 See Central CP.

925 6.2.5 Private Key Archival

926 No stipulation.

927 **6.2.6 Private Key Transfer into or from a Cryptographic Module**
 928 Not supported for End-Entity keys.
 929 See also central CP for central service aspects.

930 **6.2.7 Private Key Storage on Cryptographic Module**
 931 End-Entity keys shall be stored in a security module if technically feasible.
 932 See also central CP for central service aspects.

933 **6.2.8 Method of Activating Private Key**
 934 End-Entity private keys are automatically active after generation.
 935 See also central CP for central service aspects.

936 **6.2.9 Method of Deactivating Private Key**
 937 Deactivating Private Keys is not supported.

938 **6.2.10 Method of Destroying Private Key**
 939 In case of resetting an End-Entity, the administrator in control of the End-Entity executes adequate measures to
 940 securely delete the formerly used private keys if possible.
 941 See also central CP for central service aspects.

942 **6.2.11 Cryptographic Module Rating**
 943 See section 6.2.1.

944 **6.3 Other Aspects of Key Pair Management**

945 **6.3.1 Public key archival**
 946 Public key and related certificate shall be archived in accordance with Section 5.5.

947 **6.3.2 Certificate operational periods and key pair usage periods**
 948 The respective maximum validity periods for keys are:
 949

Certified Entity	Validity Period
PPKI Infrastructure Root CA	Up to two years
PPKI Infrastructure Issuing CA	Up to two years
CMP certificate	Up to one year
TLS certificate	Up to one year

950 **Table 1: Maximum validity periods**

951 See also central CP.

952 **6.4 Activation Data**

953 **6.4.1 Activation Data Generation and Installation**
 954 Passphrase for PKCS#12 container is defined during the onboarding and securely delivered to the Tenant.
 955 See also central CP for central service aspects.

956 **6.4.2 Activation Data Protection**
 957 See Central CP.

958 **6.4.3 Other Aspects of Activation Data**
959 See Central CP.

960 **6.5 Computer Security Controls**

961 **6.5.1 Specific Computer Security Technical Requirements**
962 Specific computer security requirements for RAs are defined in [ISMS].
963 See also central CP for central service aspects.

964 **6.5.2 Computer Security Rating**
965 No stipulation.

966 **6.6 Life Cycle Security Controls**

967 **6.6.1 System Development Controls**
968 See Central CP.

969 **6.6.2 Security Management Controls**
970 RA security management controls shall follow regulations equivalent to Siemens ISMS [ISMS].
971 See also central CP for central service aspects.

972 **6.6.3 Life Cycle Security Controls**
973 See Central CP.

974 **6.7 Network Security Controls**

975 The (L)RA network security controls shall follow regulations equivalent to Siemens ISMS [ISMS].
976 See also central CP for central service aspects.

977 **6.8 Time Stamp Process** 978 See Central CP.

979 7 Certificate, CRL, and OCSP Profiles

980 7.1 Certificate Profile

981 Details of the tenant specific certificate profile can be found in [PROF].

982 See also central CP.

983 7.1.1 Version Number(s)

984 See Central CP.

985 7.1.2 Certificate Extensions

986 See Central CP.

987 7.1.3 Algorithm Object Identifiers

988 See section 6.1.5.

989 7.1.4 Name Forms

990 Consistency checks are performed as part of the acceptance procedure of the checklist(s).

991 7.1.5 Name Constraints

992 No stipulation.

993 7.1.6 Certificate Policy Object Identifier

994 The Issuing CA certificates contain the anyPolicy OID (2.5.29.32.0).

995 Following OIDs are included in the Subject certificates:

996 1.3.6.1.4.1.4329.38.1000.3.2

997 1.3.6.1.4.1.4329.99.1.2.1000.2

998 7.1.7 Usage of Policy Constraints Extension

999 No stipulation.

1000 7.1.8 Policy Qualifiers Syntax and Semantics

1001 No stipulation.

1002 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

1003 Critical Certificate Policy extension shall conform to IETF RFC 5280 [RFC5280].

1004 7.2 CRL Profile

1005 7.2.1 Version number(s)

1006 See Central CP.

1007 7.2.2 CRL and CRL entry extensions

1008 See Central CP.

1009 7.3 OCSP Profile

1010 7.3.1 Version Number(s)

1011 See Central CP.

1012 7.3.2 OCPS Extension

1013 See Central CP.

1014 8 Compliance Audit and Other Assessment

1015 8.1 Frequency or Circumstances of Assessment

1016 Compliance to this CP and the relevant CPSs shall be checked on a yearly basis. In addition, an bi-annual asset
1017 classification of the PKI components takes place. The asset classification is performed in accordance with the
1018 Siemens Enterprise Risk Management Process [ERM]. A possible outcome of either the audit or the asset
1019 classification is the adaption of the implemented security mechanisms and controls, which may result in changes
1020 in CP and CPSs.

1021 8.2 Identity / Qualifications of Assessor

1022 Compliance audits shall be performed by a qualified auditor.

1023 See also central CP for central service aspects.

1024 8.3 Assessor's Relationship to Assessed Entity

1025 The assessor shall be organizationally independent from the assessed entity's operational authority.

1026 See also central CP for central service aspects.

1027 8.4 Topics Covered by Assessment

1028 See Central CP.

1029 8.5 Actions Taken as a Result of Deficiency

1030 If a compliance audit or other assessments show deficiencies of the assessed entity, a determination of actions to
1031 be taken shall be made. This determination is made by Tenant PMA with input from the auditor/assessor. Tenant
1032 PMA is responsible for developing and implementing a corrective action plan.

1033 If Tenant PMA determines that such deficiencies pose an immediate threat to the security or integrity of the
1034 Product PKI or the respective Tenant, a corrective action plan shall be developed in accordance with the incident
1035 response procedures described in section 5.7.1 within thirty (30) days and implemented within a commercially
1036 reasonable period of time, and a re-assessment is to be performed within thirty (30) days after completion of the
1037 corrective action. For less serious deficiencies, Tenant PMA shall evaluate the significance of such issues and
1038 determine the appropriate response.

1039 Possible actions taken include but are not limited to:

- 1040 temporary suspension of operations until deficiencies are corrected
- 1041 revocation of certificates issued to the assessed entity
- 1042 changes in personnel
- 1043 triggering special investigations or more frequent subsequent compliance assessments, and
- 1044 claims for damages against the assessed entity

1045 8.6 Communication of Results

1046 An Audit Compliance Report, including identification of corrective measures taken or being taken by the
1047 component, shall be provided to the Tenant PMA.

1048 **9 Other Business and Legal Matters**

1049 All business and legal matters will be regulated within specific contracts if necessary.

1050 **9.1 Fees**

1051 **9.1.1 Certificate Issuance or Renewal fees**

1052 No stipulation.

1053 **9.1.2 Certificate Access fees**

1054 No stipulation.

1055 **9.1.3 Revocation or Status Information Access fees**

1056 No stipulation.

1057 **9.1.4 Fees for other Services**

1058 No stipulation.

1059 **9.1.5 Refund Policy**

1060 No stipulation.

1061 **9.2 Financial Responsibility**

1062 No stipulation.

1063 **9.2.1 Insurance Coverage**

1064 No stipulation.

1065 **9.2.2 Other Assets**

1066 No stipulation.

1067 **9.2.3 Insurance or Warranty Coverage for End-Entities**

1068 No stipulation.

1069 **9.3 Confidentiality of Business Information**

1070 **9.3.1 Scope of Confidential Information**

1071 No stipulation.

1072 **9.3.2 Information not within the Scope of Confidential Information**

1073 No stipulation.

1074 **9.3.3 Responsibility to Protect Confidential Information**

1075 No stipulation.

1076 **9.4 Privacy of Personal Information**

1077 **9.4.1 Privacy plan**

1078 No stipulation.

1079 **9.4.2 Information treated as private**

1080 No stipulation.

1081 **9.4.3 Information not deemed private**

1082 No stipulation.

1083 **9.4.4 Responsibility to protect private information**
1084 No stipulation.

1085 **9.4.5 Notice and consent to use private information**
1086 No stipulation.

1087 **9.4.6 Disclosure pursuant to judicial or administrative process**
1088 No stipulation.

1089 **9.4.7 Other information disclosure circumstances**
1090 No stipulation.

1091 9.5 Intellectual Property Rights
1092 No stipulation.

1093 **9.5.1 Intellectual Property Rights in Certificates and Revocation Information**
1094 No stipulation.

1095 **9.5.2 Intellectual Property Rights in CP**
1096 No stipulation.

1097 **9.5.3 Intellectual Property Rights in Names**
1098 No stipulation.

1099 **9.5.4 Property rights of Certificate Owners**
1100 No stipulation.

1101 9.6 Representations and Warranties
1102 **9.6.1 CA representations and warranties**
1103 No stipulation.

1104 **9.6.2 RA representations and warranties**
1105 No stipulation.

1106 **9.6.3 Subscriber representations and warranties**
1107 No stipulation.

1108 **9.6.4 Relying party representations and warranties**
1109 No stipulation.

1110 **9.6.5 Representations and warranties of other participants**
1111 No stipulation.

1112 9.7 Disclaimers of Warranties
1113 No stipulation.

1114 9.8 Limitations of Liability
1115 No stipulation.

1116 9.9 Indemnities
1117 No stipulation.

1118 **9.10 Term and Termination**

1119 **9.10.1 Term**

1120 No stipulation.

1121 **9.10.2 Termination**

1122 No stipulation.

1123 **9.10.3 Effect of Termination and Survival**

1124 No stipulation.

1125 **9.11 Individual Notices and Communication with Participants**

1126 No stipulation.

1127 **9.12 Amendments**

1128 **9.12.1 Procedure for Amendment**

1129 In the case of CP amendments, change procedures may include:

- 1130 a notification mechanism to provide notice of proposed amendments to affected Product PKI Participants
- 1131 a comment period; a mechanism by which comments are received, reviewed and incorporated into the document and
- 1133 a mechanism by which amendments become final and effective

1134 **9.12.2 Notification Mechanism and Period**

1135 A modification or amendment of the CP/CPS leads to a new version of the CP/CPS.

1136 The new version of the CP/CPS will be published after its release on the website stated in section 1.5.1.

1137 **9.12.3 Circumstances under which OID must be changed**

1138 Changes, which will not materially reduce the assurance that the CP or its implementation provides and will be judged by the Policy Management Authority (CP section 1.5) to have an insignificant effect on the acceptability of certificates, do not require a change in the CP OID.

1141 Changes, which will materially change the acceptability of certificates for specific purposes, may require corresponding changes to the CP OID.

1143 **9.13 Dispute Resolution Provisions**

1144 No stipulation.

1145 **9.14 Governing Law**

1146 No stipulation.

1147 **9.15 Compliance with Applicable Law**

1148 No stipulation.

1149 **9.16 Miscellaneous Provisions**

1150 No stipulation.

1151 **9.16.1 Entire Agreement**

1152 No stipulation.

1153 **9.16.2 Assignment**

1154 No stipulation.

1155 **9.16.3 Severability**

1156 No stipulation.

1157 **9.16.4 Enforcement (attorneys' fees and waiver of rights)**

1158 No stipulation.

1159 **9.16.5 Force Majeure**

1160 Siemens shall be not held liable for violations of this CP due to causes that are reasonably beyond its control,
1161 including but not limited to, an event of Force Majeure, act of the authority, failure of equipment, failure of
1162 telecommunications lines, failure of internet access or any unforeseeable events.

1163 **9.17 Other Provisions**

1164 **9.17.1 Order of Precedence of CP**

1165 This CP provides baseline requirements that are applicable to all CAs operated in the name of the Tenant. In the
1166 event of a conflict between this CP and any other documents, the following documents shall be given precedence
1167 with the same order of the list:

1168 For the scope of applicability for the Product PKI as defined in section 1.1:

1169 1. Product PKI Central CP

1170 2. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1171 3. Documentation executed or expressly authorized by respective PMA

1172 For the scope of applicability for the Tenant specific parts (in particular (L)RA operation and End-Entity
1173 authentication) as defined in section 1.1:

1174 1. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1175 2. Product PKI Central CP

1176 3. Documentation executed or expressly authorized by respective PMA

1177 10. References

1178 1179 In case of legitimate interest, Siemens internal regulations and guidelines as well as other internal documents can
be retrieved on request.

1180 [ACP] Asset Classification & Protection; <https://intranet.siemens.com/acp>

1181 [CCP] Siemens Product PKI Certificate Management Service – Central Certificate Policy; latest version, www.siemens.com/pki.

1182 [CCPS] Siemens Product PKI Certificate Management Service – Central Certification Practice Statement; latest version, www.siemens.com/pki.

1183 [ECRYPT] ECRYPT-CSA; Algorithms, Key Size and Protocols Report; February 2018; <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>

1184 [ERM] Siemens Enterprise Risk Management; “Enterprise Risk Management – Integrated Framework”; <https://intranet.for.siemens.com/cms/054/en/about/org/Pages/cf-a-erm-org.aspx> and <https://intranet.for.siemens.com/cms/080/de/processes/office/Pages/ric-ch-erm.aspx>

1185 [ETSI 401] ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers; August 2017

1186 [ETSI 411] ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; August 2017

1187 [FIPS] National Institute of Standards and Technology; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES; May 2001; <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>

1188 [ICP] Product PKI Certificate Management Service – Certificate Policy for Siemens Product PKI Infrastructure Certificates; latest version, www.siemens.com/pki.

1189 [IEEE802.1AR] IEEE 802.1AR; IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity; June 2018; https://standards.ieee.org/standard/802_1AR-2018.html

1190 [IHP] The Siemens Incident Handling process as part of the ISMS; <https://www.cert.siemens.com/incident-response/process/>

1191 [ISMS] SFeRA - Security Framework and Regulations Application; <https://webapps.siemens.com/sfera>

1192 [ISO27001] ISO/IEC 27001; Information technology — Security techniques — Information security management systems — Requirements; October 2013

1193 [NIST] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5 (Draft), NIST, 10/2019; <https://www.nist.gov/news-events/news/2019/10/recommendation-key-management-part-1-general-draft-nist-sp-800-57-part-1>

1194 [PROF] Certificate Profile Naming Convention for Infrastructure Certificates, <https://wiki.ct.siemens.de/display/ProductPKI/PPKI+Naming+Conventions>

1195 [RFC2119] IETF; RFC 2119; Key words for use in RFCs to Indicate Requirement Levels; March 1997.

1196 [RFC3647] IETF; RFC 3647; Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework; November 2003.

1197 [RFC5280] IETF; RFC 3647; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; May 2008; <https://tools.ietf.org/html/rfc5280>

1198 [TCP] Tenant CP, IT_Infrastructure_Certificates__CP_v1.0

1199 [TÜV] TÜV IT; Sichere Infrastrukturen für IT-Systeme – Trusted Site Infrastructure; Version 4.0; https://www.tuvit.de/fileadmin/user_upload/TUEViT_TSI_V4_0.pdf

1200 [X.520] ITU-T; X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute type