



1

2

Siemens AG

3

Product PKI Certificate Management Service –
Certification Practice Statement for Siemens
Product PKI Infrastructure Certificates

4

5

6

7 Document History

Version	Date	Author	Change Comment
1.0	26.01.2022	Michael Munzert, Antonio Vaira; T CST	First released version

8

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

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

13 Scope and Applicability

14 This document constitutes the Certification Practice Statement (CPS) for the PKI service providing
15 infrastructure certificates to Siemens Product PKI Tenant. The Product PKI is responsible for the
16 operation of the Root CAs as well as for the Issuing CAs. Together with the Central CPS, this document
17 discloses to interested parties the business policies and practices under which the Product PKI operates.

18 The Central PMA ensures that the certification practices established to meet the applicable
19 requirements specified in the present document are properly implemented in accordance with
20 Siemens' Information Security Policy.

21 Document Status

22 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.Gaus, Norbert	Head of Siemens T RPD1	Jan, 2022

23

24	Content	
25	Document History	2
26	Scope and Applicability	Error! Bookmark not defined.
27	Document Status	Error! Bookmark not defined.
28	Content.....	3
29	1 Introduction.....	12
30	1.1 Overview.....	12
31	1.1.1 PKI hierarchy.....	13
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	15
43	1.5.1 Organization Administering the Document.....	15
44	1.5.2 Contact Person	15
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	31
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	32
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.....	37
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.....	38
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 39

301 9.16.2 Assignment 39

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.

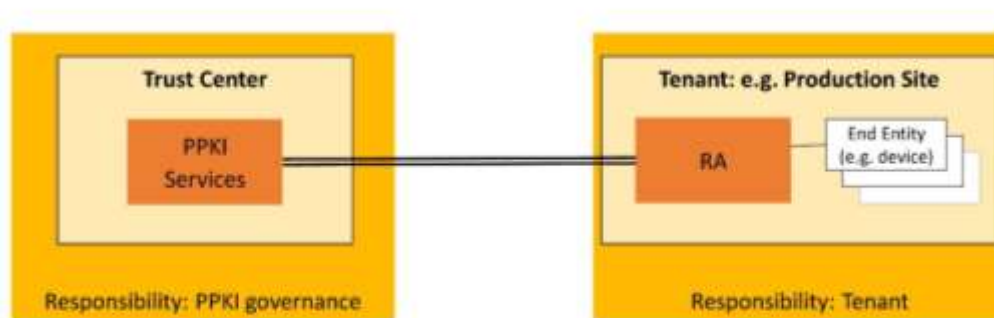
325 Moreover - together with the CPSs – the CPs also define the certification process as well as the cooperation, duties
326 and rights of the Product PKI participants.

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:

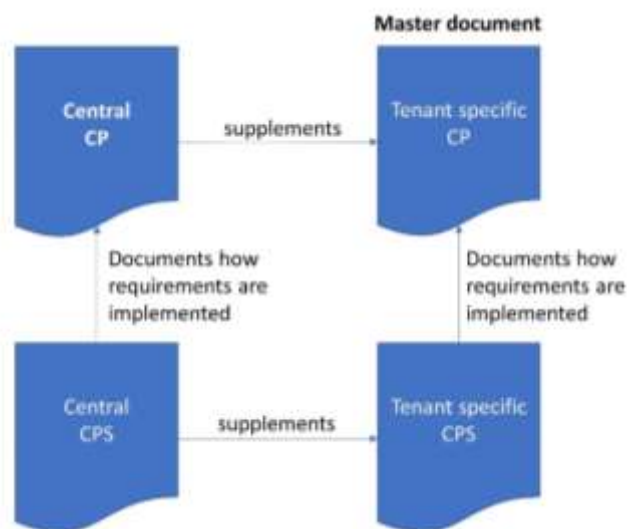
- 334 • **Product PKI Governance:** responsible for the Product PKI service is the organization listed in section 1.5
335 Policy Administration.
- 336 • **IT Services:** The central Product PKI service is hosted in the Siemens Trust Center that is operated and
337 managed by Siemens IT department.
- 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

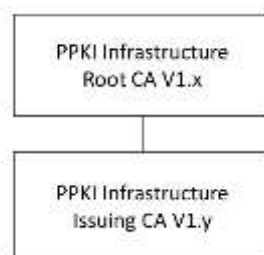
358

Figure 2: Document structure (CP and CPS)

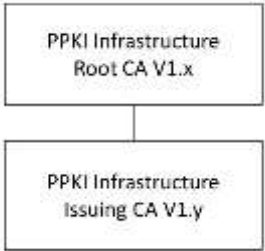
359 In addition to the requirements defined in this CP and the corresponding CPSs, Siemens IT systems are operated
 360 according to the Siemens internal information security rules and respective execution guidelines, which define
 361 how IT systems must be operated securely. The corresponding documents 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 CP is referred to as Certificate Policy 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: 1.3.6.1.4.1.4329.99.1.2.1000.1

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

379 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.

380 1.3 PKI Participants

381 See Central CP.

382 1.3.1 Certification Authorities

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

384 1.3.1.1 Root CA

385 See Central CP.

386 1.3.1.2 Intermediate CA

387 See Central CP.

388 1.3.1.3 Issuing CAs

389 See Central CP.

390 1.3.2 Registration Authorities

391 See Central CP.

392 1.3.3 Subscribers

393 See Central CP.

394 1.3.4 Relying Parties

395 See Central CP.

396 1.3.5 Other Participants

397 1.3.5.1 Subject (End-Entity)

398 See Central CP.

399 1.4 Certificate Usage

400 1.4.1 Appropriate Certificate Usage

401 See Central CP.

402 1.4.2 Prohibited Certificate Usage

403 See Central CP.

404 1.5 Policy Administration

405 1.5.1 Organization Administering the Document

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

407 Siemens Aktiengesellschaft ("Siemens AG")

408 Technology ("T") Research & Predevelopment 1 ("RPD1")
 409 Otto-Hahn-Ring 6, 81739 Munich, GERMANY
 410 E-mail: [contact.pki \(at\) siemens.com](mailto:contact.pki@siemens.com)
 411 Website: <https://www.siemens.com/pki>

412 **1.5.2 Contact Person**

413 Questions about this CP may be sent to:

414 Siemens AG
 415 T RDA CST
 416 Attn: Product PKI
 417 Otto-Hahn-Ring 6, 81739 Munich, GERMANY
 418 E-mail: [contact.pki \(at\) siemens.com](mailto:contact.pki@siemens.com)

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

420 **1.5.3 Person Determining CP and CPS Suitability for the Policy**

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

423 **1.5.4 CPS Approval Procedures**

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

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

432 1.6 Definitions and Acronyms

433 1.6.1 Definitions

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

480	Registration Authority (RA)	PKI-incorporated facility for participant-authentication.
481		See also section 1.3.2.
482	Relying Party	Individual or legal entity that uses certificates;
483		see also section 1.3.5.
484	Root CA	Entity that issues and manages certificates of Intermediate or Issuing
485		CAs (in case there do not exist Intermediate CAs). The certificate of
486		the Root CA is self-signed.
487	Root CA System	Technical components (hardware and software) hosting Root and
488		(optionally) Intermediate CAs.
489	Secure Device	A component (such as a Smart Card or HSM) that substantiated to
490		protect the private key stored in that device. All cryptographic
491		operations using the private key are performed inside this Secure
492		Device.
493	Siemens Product PKI Certificate Management Service	
494		Siemens internal organization that issues and manages certificates.
495		This organization operates the Root CA System as well as the Issuing
496		CA systems.
497	Smart Card	Integrated circuit card including a micro-processor that can be used
498		for random number generation and generation and storage of secret
499		keys. A Smart Card can use the keys for the generation of digital
500		signatures and for other PKI-applications
501	Subject	End-Entity that uses the private End-Entity key (EE key). The End-
502		Entity may differ from the Subscriber.
503	Subscriber	Subscriber for all certificates issued by the Product PKI is the
504		respective Tenant as legal entity.
505		See also section 1.3.3.
506	Tenant	Tenant can be every Siemens AG organizational unit or any other legal
507		entity that has a contract in place that covers Product PKI services.
508		The Tenants typically operate and maintain the Registration
509		Authorities (e.g. within their production facilities or data center). In
510		such a case the Tenants are responsible for RA operation and End-
511		Entity authentication.
512	Tenant PMA	PMA that is responsible for the management and operation of the
513		local Product PKI Certificate Management components such as RA
514		and/or LRA as well as for identification of End-Entities.
515	Token	Transport-medium for certificates and keys
516	Trust Center	The term "Trust Center" refers to assets and components that are
517		centrally operated and maintained at the Trust Center location as well
518		to the respective processes.
519	Trusted Operator	Product PKI has the overall responsibility of issuing certificates to
520		Subjects and managing and revoking certificates. Tenants delegate
521		may delegate parts or these functions to the Central Product PKI
522		Certificate Management Service or to other internal Service Providers
523		of Siemens, which are called Trusted Operators

524	1.6.2	Acronyms
525	ARL	Authority Revocation List
526	CA	Certification Authority
527	CISO	Chief Information Security Officer
528	CMP	Certificate Management Protocol (RFC 4210)
529	CN	Common Name
530	CP	Certificate Policy
531	CPS	Certification Practice Statement
532	CRL	Certificate Revocation List
533	DN	Distinguished Name
534	EE	End-Entity
535	FIPS	Federal Information Processing Standard
536	FQDN	Fully qualified domain name
537	HSM	Hardware Security Module
538	IEEE	Institute of Electrical and Electronics Engineers
539	IETF	Internet Engineering Task Force
540	IDeVID	Initial Device Identifier (IEEE 802.1AR)
541	ISO	International Organization for Standardization
542	ISMS	Information Security Management System
543	LDeVID	Locally significant Device Identifier (IEEE 802.1AR)
544	OCSP	Online Certificate Status Protocol
545	OID	Object Identifier
546	PIN	Personal Identification Number
547	PKI	Public Key Infrastructure
548	PPKI	Product PKI
549	PMA	Policy Management Authority
550	RA	Registration Authority
551	RFC	Request for Comment
552	SLA	Service Level Agreement
553	URL	Uniform Resource Locator
554	UTF8	Unicode Transformation Format-8

555 2 Publication and Repository Responsibilities

556 2.1 Repositories

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

558 The repository responsibilities include:

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

564 Subjects and Relying Parties have access to:

- 565 • Certificate Revocation List (CRL)
- 566 • and OCSP responder

567 via: ppki-va.siemens.com .

568 2.2 Publication of Certification Information

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

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

571 2.3 Time or Frequency of Publication

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

574 2.4 Access Controls on Repositories

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

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

578 **3 Identification and Authentication**

579 **3.1 Naming**

580 **3.1.1 Types of Names**

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

583 **3.1.2 Need of Names to be Meaningful**

584 **3.1.2.1 CA Names**

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

586 **3.1.2.2 End-Entity Names**

587 For details see Certificate Profile Documentation [PROF].

588 **3.1.3 Anonymity or Pseudonymity of Subscribers**

589 **3.1.3.1 CA Names**

590 See Central CP.

591 **3.1.3.2 End-Entity Names**

592 See Central CP.

593 **3.1.4 Rules for Interpreting Various Name Forms**

594 See Central CP.

595 **3.1.5 Uniqueness of Names**

596 **3.1.5.1 CA Names**

597 See Central CP.

598 **3.1.5.2 End-Entity Names**

599 See Central CP.

600 **3.1.6 Recognition, Authentication, and Roles of Trademarks**

601 See Central CP.

602 **3.2 Initial Identity Validation**

603 See also Central CP.

604 **3.2.1 Method to Prove Possession of Private Key**

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

608 **3.2.2 Authentication of Organization Identity**

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

610 **3.2.3 Authentication of Individual Identity**

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

612 **3.2.4 Non-verified Subscriber Information**

613 See Central CP.

614 **3.2.5 Validation of Authority**

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

616 **3.2.6 Criteria for Interoperation**

617 No stipulation.

618 **3.3 Identification and Authentication for Re-key Requests**

619 **3.3.1 Identification and Authentication for Routine Re-Key**

620 See central CP.

621 **3.3.2 Identification and Authentication for Re-Key After Revocation**

622 Not supported.

623 **3.4 Identification and Authentication for Revocation Requests**

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

627 4 Certificate Lifecycle Operational Requirements

628 4.1 Certificate Application

629 4.1.1 Who can submit a certificate application?

630 4.1.1.1 Root and Intermediate CA

631 See Central CP.

632 4.1.1.2 Issuing CAs

633 See Central CP.

634 4.1.1.3 End-Entity Certificates

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

637 4.1.2 Enrollment Process and Responsibilities

638 4.1.2.1 CA Certificates

639 See Central CP.

640 4.1.2.2 End-Entity Certificate

641 The End-Entity certificate and the corresponding private key is generated by the central service. The private
642 key material is securely transported via a PKCS#12 container.

643 4.2 Certificate Application Processing

644 4.2.1 Performing identification and authentication functions

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

646 4.2.2 Approval or Rejection of Certificate Applications

647 See Central CP and section 4.2.1.

648 4.2.3 Time to Process Certificate Applications

649 See Central CP.

650 4.3 Certificate Issuance

651 4.3.1 CA Actions during Certificate Issuance

652 See Central CP.

653 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

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

659 4.4 Certificate Acceptance

660 4.4.1 Conduct constituting certificate acceptance

661 See Central CP.

- 662 **4.4.2 Publication of the certificate by the CA**
- 663 Relying parties of the Infrastructure CA are the BUs. Terms and conditions are made available to the relying parties
664 as part of the ordering process.
- 665 **4.4.3 Notification of Certificate issuance by the CA to other entities**
- 666 No stipulation.
- 667 **4.5 Key Pair and Certificate Usage**
- 668 See Central CP.
- 669 **4.5.1 Subject Private Key and Certificate Usage**
- 670 See Central CP.
- 671 **4.5.2 Relying Party Public Key and Certificate Usage**
- 672 See Central CP.
- 673 **4.6 Certificate Renewal**
- 674 Certificate renewal is the issuance of a new certificate to an entity without changing the public key or any other
675 information in the certificate.
- 676 Not supported.
- 677 **4.6.1 Circumstance for Certificate Renewal**
- 678 No stipulation.
- 679 **4.6.2 Who may request renewal?**
- 680 No stipulation.
- 681 **4.6.3 Processing Certificate Renewal Request**
- 682 No stipulation.
- 683 **4.6.4 Notification of new Certificate Issuance to Subscriber**
- 684 No stipulation.
- 685 **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**
- 686 No stipulation.
- 687 **4.6.6 Publication of the Renewal Certificate by the CA**
- 688 No stipulation.
- 689 **4.6.7 Notification of Certificate Issuance by the CA to other Entities**
- 690 No stipulation.
- 691 **4.7 Certificate Re-key**
- 692 "Re-key" addresses the generating of a new Key Pair and applying for the issuance of a new certificate and
693 replacing the existing Key Pair.
- 694 **4.7.1 Circumstances for Certificate Re-key**
- 695 See Central CP.
- 696 **4.7.2 Who may request certification of a new Public Key?**
- 697 **4.7.2.1 Re-keying of an Issuing CA certificate**
- 698 See Central CP.

- 699 **4.7.2.2 Re-keying of End-Entity certificates**
- 700 The End-Entity, prior to the expiration of its certificate, will authenticate against the CA with its still valid certificate
701 and initiate the issuance of a new certificate.
- 702 **4.7.3 Processing Certificate Re-keying Requests**
- 703 See section 4.3.1
- 704 **4.7.4 Notification of new Certificate Issuance to Subscriber**
- 705 See section 4.3.2
- 706 **4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**
- 707 See section 4.4.1
- 708 **4.7.6 Publication of the Re-keyed Certificate by the CA**
- 709 See section 4.4.2
- 710 **4.7.7 Notification of Certificate Issuance by the CA to other Entities**
- 711 See section 4.4.3
- 712 **4.8 Certificate Modification**
- 713 Certificate modification means that the keys of a certificate remain unchanged, but more certificate information
714 than for a certificate renewal is changed.
- 715 Not supported.
- 716 **4.8.1 Circumstance for Certificate Modification**
- 717 No stipulation.
- 718 **4.8.2 Who may request Certificate modification?**
- 719 No stipulation.
- 720 **4.8.3 Processing Certificate Modification Requests**
- 721 No stipulation.
- 722 **4.8.4 Notification of new Certificate Issuance to Subscriber**
- 723 No stipulation.
- 724 **4.8.5 Conduct Constituting Acceptance of Modified Certificate**
- 725 No stipulation.
- 726 **4.8.6 Publication of the Modified Certificate by the CA**
- 727 No stipulation.
- 728 **4.8.7 Notification of Certificate Issuance by the CA to Other Entities**
- 729 No stipulation.
- 730 **4.9 Certificate Revocation and Suspension**
- 731 **4.9.1 Circumstances for Revocation**
- 732 See Central CP.
- 733 **4.9.2 Who can request revocation?**
- 734 RA owners can request revocation of the EE certificates that have been issued for their RA.

735 **4.9.3 Procedure for Revocation Request**

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

738 See also section 3.4.

739 **4.9.4 Revocation Request Grace Period**

740 See Central CP.

741 **4.9.5 Time within which CA must Process the Revocation Request**

742 See Central CP.

743 **4.9.6 Revocation Checking Requirement for Relying Parties**

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

746 **4.9.7 CRL Issuance Frequency**

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

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

749 **4.9.8 Maximum Latency for CRLs**

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

751 **4.9.9 On-line Revocation/Status Checking Availability**

752 Not supported.

753 **4.9.10 On-line Revocation Checking Requirements**

754 No stipulation.

755 **4.9.11 Other Forms of Revocation Advertisements Available**

756 No stipulation.

757 **4.9.12 Special Requirements for Private Key Compromise**

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

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

761 See also central CP for central service aspects.

762 **4.9.13 Circumstances for Suspension**

763 Not supported.

764 **4.9.14 Who can request suspension?**

765 No stipulation.

766 **4.9.15 Procedure for suspension request**

767 No stipulation.

768 **4.9.16 Limits on suspension period**

769 No stipulation.

770 **4.10 Certificate Status Services**

771 **4.10.1 Operational Characteristics**

772 See section 4.9.

773 **4.10.2 Service Availability**

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

776 **4.10.3 Optional Features**

777 No stipulation.

778 **4.11 End of Subscription**

779 See Central CP.

780 **4.12 Key Escrow and Recovery**

781 Not supported.

782 **4.12.1 Key Escrow and Recovery Policy and Practices**

783 No stipulation.

784 **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

785 No stipulation.

786 5 Management, Operational, and Physical Controls

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

790 5.1 Physical Security Controls

791 5.1.1 Site Location and Construction

792 See Central CPS [CCPS]

793 5.1.2 Physical Access

794 See Central CPS [CCPS].

795 5.1.3 Power and Air Conditioning

796 See Central CPS [CCPS].

797 5.1.4 Water Exposure

798 See Central CPS [CCPS].

799 5.1.5 Fire Prevention and Protection

800 See Central CPS [CCPS].

801 5.1.6 Media Storage

802 See Central CPS [CCPS].

803 5.1.7 Waste Disposal

804 See Central CPS [CCPS].

805 5.1.8 Off-site Backup

806 See Central CPS [CCPS].

807 5.2 Procedural Controls

808 5.2.1 Trusted Roles

809 See Central CPS [CCPS].

810 5.2.2 Numbers of Persons Required per Task

811 See Central CPS [CCPS].

812 5.2.3 Identification and Authentication for Each Role

813 See Central CPS [CCPS].

814 5.2.4 Roles Requiring Separation of Duties

815 See Central CPS [CCPS].

816 5.3 Personnel Controls

817 5.3.1 Qualifications, Experience and Clearance Requirements

818 See Central CPS [CCPS].

819 5.3.2 Background Check Procedures

820 See Central CPS [CCPS].

821	5.3.3 Training Requirements
822	See Central CPS [CCPS].
823	5.3.4 Retraining Frequency and Requirements
824	See Central CPS [CCPS].
825	5.3.5 Job Rotation Frequency and Sequence
826	See Central CPS [CCPS].
827	5.3.6 Sanctions for Unauthorized Actions
828	See Central CP.
829	5.3.7 Independent Contractor Requirements
830	See Central CP.
831	5.3.8 Documents Supplied to Personnel
832	See Central CP.
833	5.4 Audit Logging Procedures
834	5.4.1 Types of Events Recorded
835	See Central CPS [CCPS].
836	5.4.2 Frequency of Processing Log
837	See Central CP.
838	5.4.3 Retention Period for Audit Log
839	See Central CPS [CCPS].
840	5.4.4 Protection of Audit Log
841	See Central CPS [CCPS].
842	5.4.5 Audit Log Backup Procedures
843	See Central CPS [CCPS].
844	5.4.6 Audit Collection System (Internal vs. External)
845	See Central CPS [CCPS].
846	5.4.7 Notification to Event-Causing Subject
847	See Central CP.
848	5.4.8 Vulnerability Assessments
849	See Central CPS [CCPS].
850	5.5 Records Archival
851	5.5.1 Types of Records Archived
852	CPS: See Central CPS [CCPS].
853	5.5.2 Retention Period for Archived Audit Logging Information
854	See Central CPS [CCPS].
855	5.5.3 Protection of Archive
856	See central CP.

857 See Central CPS [CCPS].

858 **5.5.4 Archive Backup Procedures**

859 See Central CPS [CCPS].

860 **5.5.5 Requirements for Time-Stamping of Record**

861 See Central CP.

862 **5.5.6 Archive Collection System (internal or external)**

863 See Central CPS [CCPS].

864 **5.5.7 Procedures to Obtain and Verify Archived Information**

865 See Central CP.

866 **5.6 Key Changeover**

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

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

873 **5.7 Compromise and Disaster Recovery**

874 **5.7.1 Incident and Compromise Handling Procedures**

875 See Central CP.

876 **5.7.2 Corruption of Computing Resources, Software, and/or Data**

877 See Central CP.

878 **5.7.3 Entity Private Key Compromise Procedures**

879 See Central CP.

880 **5.7.4 Business Continuity Capabilities After a Disaster**

881 See Central CP.

882 **5.8 CA or RA Termination**

883 See central CP.

884 6 Technical Security Controls

885 6.1 Key Pair Generation and Installation

886 6.1.1 Key Pair Generation

887 Private keys for infrastructure certificates are created by used PKI software. In case of automated re-keying the
888 private key is created by the End-Entity starting from the first re-key.

889 6.1.2 Private Key Delivery to Subscriber

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

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

895 6.1.3 Public Key Delivery to Certificate Issuer

896 See Tenant specific CP [TCP].

897 6.1.4 CA Public Key Delivery to Relying Parties

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

900 See also Central CP [CCP].

901 6.1.5 Key Sizes

902 See Central CP.

903 6.1.6 Public Key Parameters Generation and Quality Checking

904 See Central CP.

905 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

906 See Central CP.

907 6.2 Private Key Protection and Cryptographic Module Engineering Controls

908 6.2.1 Cryptographic Module Standards and Controls

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

910 See also central CP for central service aspects.

911 6.2.2 Private Key (n out of m) Multi-person Control

912 4 eyes principle is applied for private keys of end entities (see 6.1.2 Private Key Delivery to Subscriber).

913 See also central CP for central service aspects.

914 6.2.3 Private Key Escrow

915 No supported.

916 6.2.4 Private Key Backup

917 See Central CP.

918 6.2.5 Private Key Archival

919 No stipulation.

920 6.2.6 Private Key Transfer into or from a Cryptographic Module

921 Not supported for End-Entity keys.

922 See also central CP for central service aspects.

923 **6.2.7 Private Key Storage on Cryptographic Module**

924 End-Entity keys shall be stored in a security module if technically feasible.

925 See also central CP for central service aspects.

926 **6.2.8 Method of Activating Private Key**

927 End-Entity private keys are automatically active after generation.

928 See also central CP for central service aspects.

929 **6.2.9 Method of Deactivating Private Key**

930 Deactivating Private Keys is not supported.

931 **6.2.10 Method of Destroying Private Key**

932 In case of resetting an End-Entity, the administrator in control of the End-Entity executes adequate measures to
 933 securely delete the formerly used private keys if possible.

934 See also central CP for central service aspects.

935 **6.2.11 Cryptographic Module Rating**

936 See section 6.2.1.

937 **6.3 Other Aspects of Key Pair Management**

938 **6.3.1 Public key archival**

939 Public key and related certificate shall be archived in accordance with Section 5.5.

940 **6.3.2 Certificate operational periods and key pair usage periods**

941 The respective maximum validity periods for keys are:

942

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

Table 1: Maximum validity periods

943

944 See also central CP.

945 **6.4 Activation Data**

946 **6.4.1 Activation Data Generation and Installation**

947 Passphrase for PKCS#12 container is defined during the onboarding and securely delivered to the Tenant.

948 See also central CP for central service aspects.

949 **6.4.2 Activation Data Protection**

950 See Central CP.

951 **6.4.3 Other Aspects of Activation Data**

952 See Central CP.

953 6.5 Computer Security Controls

954 6.5.1 Specific Computer Security Technical Requirements

955 Specific computer security requirements for RAs are defined in [ISMS].

956 See also central CP for central service aspects.

957 6.5.2 Computer Security Rating

958 No stipulation.

959 6.6 Life Cycle Security Controls

960 6.6.1 System Development Controls

961 See Central CP.

962 6.6.2 Security Management Controls

963 RA security management controls shall follow regulations equivalent to Siemens ISMS [ISMS].

964 See also central CP for central service aspects.

965 6.6.3 Life Cycle Security Controls

966 See Central CP.

967 6.7 Network Security Controls

968 The (L)RA network security controls shall follow regulations equivalent to Siemens ISMS [ISMS].

969 See also central CP for central service aspects.

970 6.8 Time Stamp Process

971 See Central CP.

972 7 Certificate, CRL, and OCSP Profiles

973 7.1 Certificate Profile

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

975 See also central CP.

976 7.1.1 Version Number(s)

977 See Central CP.

978 7.1.2 Certificate Extensions

979 See Central CP.

980 7.1.3 Algorithm Object Identifiers

981 See Central CP.

982 7.1.4 Name Forms

983 See Central CP.

984 7.1.5 Name Constraints

985 No stipulation.

986 7.1.6 Certificate Policy Object Identifier

987 The Issuing CA certificates contain the "any policy" OID.

988 Following OIDs are included in the Subject certificates:

989 1.3.6.1.4.1.4329.38.1000.3.2

990 1.3.6.1.4.1.4329.99.1.2.0.1

991 7.1.7 Usage of Policy Constraints Extension

992 No stipulation.

993 7.1.8 Policy Qualifiers Syntax and Semantics

994 No stipulation.

995 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

997 7.2 CRL Profile

998 7.2.1 Version number(s)

999 See Central CP.

1000 7.2.2 CRL and CRL entry extensions

1001 See Central CP.

1002 7.3 OCSP Profile

1003 7.3.1 Version Number(s)

1004 See Central CP.

1005 7.3.2 OCPS Extension

1006 See Central CP.

1007 8 Compliance Audit and Other Assessment

1008 8.1 Frequency or Circumstances of Assessment

1009 Compliance to this CP and the relevant CPSs shall be checked on a yearly basis. In addition, an bi-annual asset
 1010 classification of the PKI components takes place. The asset classification is performed in accordance with the
 1011 Siemens Enterprise Risk Management Process [ERM]. A possible outcome of either the audit or the asset
 1012 classification is the adaption of the implemented security mechanisms and controls, which may result in changes
 1013 in CP and CPSs.

1014 8.2 Identity / Qualifications of Assessor

1015 Compliance audits shall be performed by a qualified auditor.

1016 See also central CP for central service aspects.

1017 8.3 Assessor's Relationship to Assessed Entity

1018 The assessor shall be organizationally independent from the assessed entity's operational authority.

1019 See also central CP for central service aspects.

1020 8.4 Topics Covered by Assessment

1021 See Central CP.

1022 8.5 Actions Taken as a Result of Deficiency

1023 If a compliance audit or other assessments show deficiencies of the assessed entity, a determination of actions to
 1024 be taken shall be made. This determination is made by Tenant PMA with input from the auditor/assessor. Tenant
 1025 PMA is responsible for developing and implementing a corrective action plan.

1026 If Tenant PMA determines that such deficiencies pose an immediate threat to the security or integrity of the
 1027 Product PKI or the respective Tenant, a corrective action plan shall be developed in accordance with the incident
 1028 response procedures described in section 5.7.1 within thirty (30) days and implemented within a commercially
 1029 reasonable period of time, and a re-assessment is to be performed within thirty (30) days after completion of the
 1030 corrective action. For less serious deficiencies, Tenant PMA shall evaluate the significance of such issues and
 1031 determine the appropriate response.

1032 Possible actions taken include but are not limited to:

- 1033 temporary suspension of operations until deficiencies are corrected
- 1034 revocation of certificates issued to the assessed entity
- 1035 changes in personnel
- 1036 triggering special investigations or more frequent subsequent compliance assessments, and
- 1037 claims for damages against the assessed entity

1038 8.6 Communication of Results

1039 An Audit Compliance Report, including identification of corrective measures taken or being taken by the
 1040 component, shall be provided to the Tenant PMA.

1041 9 Other Business and Legal Matters

1042 All business and legal matters will be regulated within specific contracts if necessary.

1043 9.1 Fees

1044 9.1.1 Certificate Issuance or Renewal fees

1045 No stipulation.

1046 9.1.2 Certificate Access fees

1047 No stipulation.

1048 9.1.3 Revocation or Status Information Access fees

1049 No stipulation.

1050 9.1.4 Fees for other Services

1051 No stipulation.

1052 9.1.5 Refund Policy

1053 No stipulation.

1054 9.2 Financial Responsibility

1055 No stipulation.

1056 9.2.1 Insurance Coverage

1057 No stipulation.

1058 9.2.2 Other Assets

1059 No stipulation.

1060 9.2.3 Insurance or Warranty Coverage for End-Entities

1061 No stipulation.

1062 9.3 Confidentiality of Business Information

1063 9.3.1 Scope of Confidential Information

1064 No stipulation.

1065 9.3.2 Information not within the Scope of Confidential Information

1066 No stipulation.

1067 9.3.3 Responsibility to Protect Confidential Information

1068 No stipulation.

1069 9.4 Privacy of Personal Information

1070 9.4.1 Privacy plan

1071 No stipulation.

1072 9.4.2 Information treated as private

1073 No stipulation.

1074	9.4.3 Information not deemed private
1075	No stipulation.
1076	9.4.4 Responsibility to protect private information
1077	No stipulation.
1078	9.4.5 Notice and consent to use private information
1079	No stipulation.
1080	9.4.6 Disclosure pursuant to judicial or administrative process
1081	No stipulation.
1082	9.4.7 Other information disclosure circumstances
1083	No stipulation.
1084	9.5 Intellectual Property Rights
1085	No stipulation.
1086	9.5.1 Intellectual Property Rights in Certificates and Revocation Information
1087	No stipulation.
1088	9.5.2 Intellectual Property Rights in CP
1089	No stipulation.
1090	9.5.3 Intellectual Property Rights in Names
1091	No stipulation.
1092	9.5.4 Property rights of Certificate Owners
1093	No stipulation.
1094	9.6 Representations and Warranties
1095	9.6.1 CA representations and warranties
1096	No stipulation.
1097	9.6.2 RA representations and warranties
1098	No stipulation.
1099	9.6.3 Subscriber representations and warranties
1100	No stipulation.
1101	9.6.4 Relying party representations and warranties
1102	No stipulation.
1103	9.6.5 Representations and warranties of other participants
1104	No stipulation.
1105	9.7 Disclaimers of Warranties
1106	No stipulation.
1107	9.8 Limitations of Liability
1108	No stipulation.

1109 **9.9 Indemnities**

1110 No stipulation.

1111 **9.10 Term and Termination**

1112 **9.10.1 Term**

1113 No stipulation.

1114 **9.10.2 Termination**

1115 No stipulation.

1116 **9.10.3 Effect of Termination and Survival**

1117 No stipulation.

1118 **9.11 Individual Notices and Communication with Participants**

1119 No stipulation.

1120 **9.12 Amendments**

1121 **9.12.1 Procedure for Amendment**

1122 In the case of CP amendments, change procedures may include:

- 1123 a notification mechanism to provide notice of proposed amendments to affected Product PKI Participants
- 1124 a comment period; a mechanism by which comments are received, reviewed and incorporated into the
- 1125 document and
- 1126 a mechanism by which amendments become final and effective

1127 **9.12.2 Notification Mechanism and Period**

1128 A modification or amendment of the CP/CPS leads to a new version of the CP/CPS.

1129 The new version of the CP/CPS will be published after its release on the website stated in section 1.5.1.

1130 **9.12.3 Circumstances under which OID must be changed**

1131 Changes, which will not materially reduce the assurance that the CP or its implementation provides and will be
 1132 judged by the Policy Management Authority (CP section 1.5) to have an insignificant effect on the acceptability of
 1133 certificates, do not require a change in the CP OID.

1134 Changes, which will materially change the acceptability of certificates for specific purposes, may require
 1135 corresponding changes to the CP OID.

1136 **9.13 Dispute Resolution Provisions**

1137 No stipulation.

1138 **9.14 Governing Law**

1139 No stipulation.

1140 **9.15 Compliance with Applicable Law**

1141 No stipulation.

1142 **9.16 Miscellaneous Provisions**

1143 No stipulation.

1144 **9.16.1 Entire Agreement**

1145 No stipulation.

1146 **9.16.2 Assignment**

1147 No stipulation.

1148 **9.16.3 Severability**

1149 No stipulation.

1150 **9.16.4 Enforcement (attorneys' fees and waiver of rights)**

1151 No stipulation.

1152 **9.16.5 Force Majeure**

1153 Siemens shall be not held liable for violations of this CP due to causes that are reasonably beyond its control,
 1154 including but not limited to, an event of Force Majeure, act of the authority, failure of equipment, failure of
 1155 telecommunications lines, failure of internet access or any unforeseeable events.

1156 **9.17 Other Provisions**

1157 **9.17.1 Order of Precedence of CP**

1158 This CP provides baseline requirements that are applicable to all CAs operated in the name of the Tenant. In the
 1159 event of a conflict between this CP and any other documents, the following documents shall be given precedence
 1160 with the same order of the list:

1161 For the scope of applicability for the Product PKI as defined in section 1.1:

1162 1. Product PKI Central CP

1163 2. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1164 3. Documentation executed or expressly authorized by respective PMA

1165 For the scope of applicability for the Tenant specific parts (in particular (L)RA operation and End-Entity
 1166 authentication) as defined in section 1.1:

1167 1. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1168 2. Product PKI Central CP

1169 3. Documentation executed or expressly authorized by respective PMA

1170 **10. References**

- 1171 In case of legitimate interest, Siemens internal regulations and guidelines as well as other internal documents can
1172 be retrieved on request.
- 1173 [ACP] Asset Classification & Protection; <https://intranet.siemens.com/acp>
- 1174 [CCP] Siemens Product PKI Certificate Management Service – Central Certificate Policy; Jan. 14, 2022,
1175 Version 1.8, www.siemens.com/pki.
- 1176 [CCPS] Siemens Product PKI Certificate Management Service – Central Certification Practice Statement;
1177 Jan. 14, 2022, Version 1.2, www.siemens.com/pki.
- 1178 [ECRYPT] ECRYPT-CSA; Algorithms, Key Size and Protocols Report; February 2018;
1179 <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>
- 1180 [ERM] Siemens Enterprise Risk Management; “Enterprise Risk Management – Integrated Framework”;
1181 <https://intranet.for.siemens.com/cms/054/en/about/org/Pages/cf-a-erm-org.aspx>
1182 and <https://intranet.for.siemens.com/cms/080/de/processes/office/Pages/ric-ch-erm.aspx>
- 1183 [ETSI 401] ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for
1184 Trust Service Providers; August 2017
- 1185 [ETSI 411] ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements
1186 for Trust Service Providers issuing certificates; Part 1: General requirements; August 2017
- 1187 [FIPS] National Institute of Standards and Technology; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC
1188 MODULES; May 2001; <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- 1189 [IEEE802.1AR] IEEE 802.1AR; IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity;
1190 June 2018; https://standards.ieee.org/standard/802_1AR-2018.html
- 1191 [IHP] The Siemens Incident Handling process as part of the ISMS; <https://www.cert.siemens.com/incident-response/process/>
- 1192
- 1193 [ISMS] SFeRA - Security Framework and Regulations Application; <https://webapps.siemens.com/sfera>
- 1194 [ISO27001] ISO/IEC 27001; Information technology — Security techniques — Information security management
1195 systems — Requirements; October 2013
- 1196 [NIST] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5 (Draft), NIST,
1197 10/2019; <https://www.nist.gov/news-events/news/2019/10/recommendation-key-management-part-1-general-draft-nist-sp-800-57-part-1>
- 1198
- 1199 [PROF] Certificate Profile Naming Convention for Infrastructure Certificates,
1200 <https://wiki.ct.siemens.de/display/ProductPKI/PPKI+Naming+Conventions>
- 1201 [RFC2119] IETF; RFC 2119; Key words for use in RFCs to Indicate Requirement Levels; March 1997.
- 1202 [RFC3647] IETF; RFC 3647; Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices
1203 Framework; November 2003.
- 1204 [RFC5280] IETF; RFC 3647; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List
1205 (CRL) Profile; May 2008; <https://tools.ietf.org/html/rfc5280>
- 1206 [TCP] Tenant CP, IT_Infrastructure_Certificates__CP_v1.0
- 1207 [TÜV] TÜV IT; Sichere Infrastrukturen für IT-Systeme – Trusted Site Infrastructure; Version 4.0;
1208 https://www.tuvit.de/fileadmin/user_upload/TUEViT_TSI_V4_0.pdf
- 1209 [X.520] ITU-T; X520 Information technology – Open Systems Interconnection – The Directory: Selected
1210 attribute type