



1

2

Siemens AG

3

Product PKI Certificate Management Service –

4

Certificate Policy for Siemens Product PKI

5

Infrastructure Certificates

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](http://www.siemens.com/pki).

## 13 Scope and Applicability

14 This document constitutes the Certificate Policy (CP) for the PKI service providing infrastructure  
15 certificates to Siemens Product PKI Tenant. The Product PKI is responsible for the operation of the Root  
16 CAs as well as for the Issuing CAs. Together with the Central CP, this document discloses to interested  
17 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
<b>Author</b>	Various authors, detailed information see document history.		
<b>Checked by</b>	Stenger, Meiko	Siemens LC	May, 2020
	Kuechler, Markus	Siemens IT	Feb, 2022
<b>Authorization</b>	Dr.Gaus, Norbert	Head of Siemens T RPD1	Jan, 2022

23

24	<b>Content</b>	
25	Document History .....	2
26	Scope and Applicability .....	<b>Error! Bookmark not defined.</b>
27	Document Status .....	<b>Error! Bookmark not defined.</b>
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.....	23
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 .....	25
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.....	26
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 .....	31
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 .....	32
218	6.5.1	Specific Computer Security Technical Requirements.....	32
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 Certificate Policy of the Siemens Product PKI Certificate Management Service (in the  
318 following called "Product PKI") of the Tenant providing Infrastructure Certificates for all other Product PKI Tenants.

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

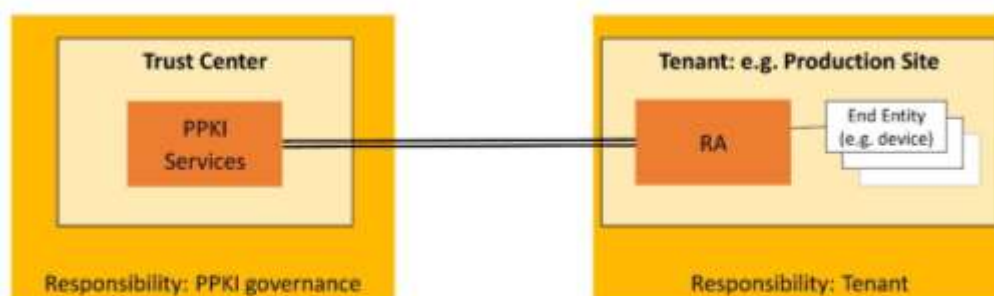
324 Moreover - together with the CPSs – the CPs also define the certification process as well as the cooperation, duties  
325 and rights of the Product PKI participants.

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

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

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

- 333 • **Product PKI Governance:** responsible for the Product PKI service is the organization listed in section 1.5  
334 Policy Administration.
- 335 • **IT Services:** The central Product PKI service is hosted in the Siemens Trust Center that is operated and  
336 managed by Siemens IT department.
- 337 • **Tenant:** Tenant can be every Siemens AG organizational unit or any other legal entity that has a contract in  
338 place that covers Product PKI services. The Tenants typically operate and maintain the registrations authorities  
339 (e.g. within their production facilities or data center). Therefore, the Tenants are responsible for RA operation  
340 and End-Entity authentication.



341  
342 **Figure 1: Stakeholders and typical responsibility split**

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

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

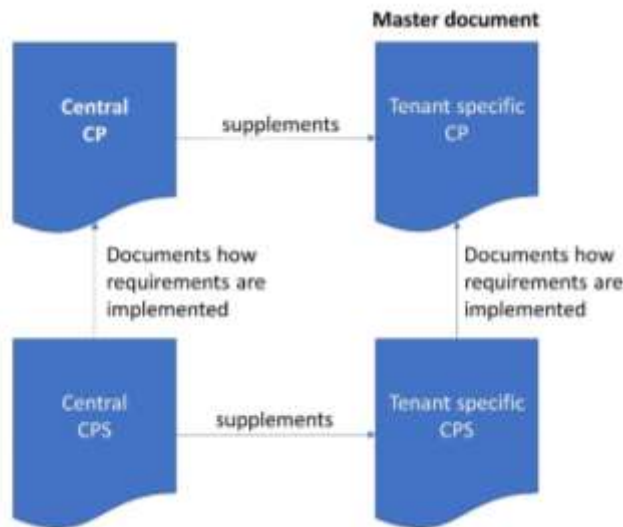
346 The Tenant specific CP is always the master document. It defines all requirements for which the Tenant is  
 347 responsible for. In particular, it comprises the management and operation of the RAs and/or LRAs, of publicly  
 348 accessible repositories. Where appropriate, the Tenant specific CP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

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

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

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

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



356

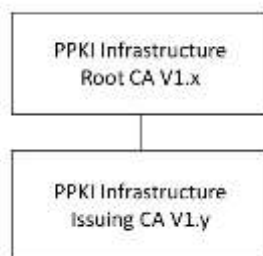
357

Figure 2: Document structure (CP and CPS)

358 In addition to the requirements defined in this CP and the corresponding CPSs, Siemens IT systems are operated  
 359 according to the Siemens internal information security rules and respective execution guidelines, which define  
 360 how IT systems must be operated securely. The corresponding documents can be retrieved on request.

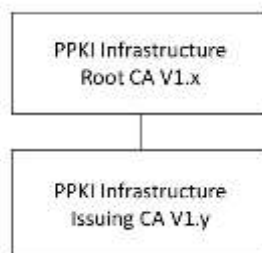
361 These rules are part of a Siemens ISMS [ISMS], which is defined and implemented according to ISO 27001.

362 **1.1.1 PKI hierarchy**



363 The specific PKI hierarchy is shown in

364 Figure 3.



365

366

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

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

## 372 1.2 Document Name and Identification

373 This CP is referred to as Certificate Policy for the 'Siemens Product PKI Infrastructure Certificates'.

374 Title: Product PKI Certificate Management Service – Certificate Policy for Siemens Product PKI  
375 Infrastructure Certificates

376 OIDs: 1.3.6.1.4.1.4329.99.1.2.1000.1

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

378 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.

## 379 1.3 PKI Participants

380 See Central CP.

### 381 1.3.1 Certification Authorities

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

#### 383 1.3.1.1 Root CA

384 See Central CP.

#### 385 1.3.1.2 Intermediate CA

386 See Central CP.

#### 387 1.3.1.3 Issuing CAs

388 See Central CP.

### 389 1.3.2 Registration Authorities

390 See Central CP.

### 391 1.3.3 Subscribers

392 See Central CP.

### 393 1.3.4 Relying Parties

394 See Central CP.

### 395 1.3.5 Other Participants

#### 396 1.3.5.1 Subject (End-Entity)

397 See Central CP.

## 398 1.4 Certificate Usage

### 399 1.4.1 Appropriate Certificate Usage

400 See Central CP.

### 401 1.4.2 Prohibited Certificate Usage

402 See Central CP.

## 403 1.5 Policy Administration

### 404 1.5.1 Organization Administering the Document

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

406 Siemens Aktiengesellschaft ("Siemens AG")

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

## 411 **1.5.2 Contact Person**

412 Questions about this CP may be sent to:

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

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

## 419 **1.5.3 Person Determining CP and CPS Suitability for the Policy**

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

## 422 **1.5.4 CPS Approval Procedures**

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

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



## 431 1.6 Definitions and Acronyms

### 432 1.6.1 Definitions

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

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

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

## 554 2 Publication and Repository Responsibilities

### 555 2.1 Repositories

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

557 The repository responsibilities include:

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

563 Subjects and Relying Parties have access to:

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

566 via: [ppki-va.siemens.com](https://ppki-va.siemens.com) .

### 567 2.2 Publication of Certification Information

568 The Tenant publishes certificate status information at [ppki-va.siemens.com](https://ppki-va.siemens.com).

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

### 570 2.3 Time or Frequency of Publication

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

### 573 2.4 Access Controls on Repositories

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

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

## 577 **3 Identification and Authentication**

### 578 **3.1 Naming**

#### 579 **3.1.1 Types of Names**

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

#### 582 **3.1.2 Need of Names to be Meaningful**

##### 583 **3.1.2.1 CA Names**

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

##### 585 **3.1.2.2 End-Entity Names**

586 For details see Certificate Profile Documentation [PROF].

#### 587 **3.1.3 Anonymity or Pseudonymity of Subscribers**

##### 588 **3.1.3.1 CA Names**

589 See Central CP.

##### 590 **3.1.3.2 End-Entity Names**

591 See Central CP.

#### 592 **3.1.4 Rules for Interpreting Various Name Forms**

593 See Central CP.

#### 594 **3.1.5 Uniqueness of Names**

##### 595 **3.1.5.1 CA Names**

596 See Central CP.

##### 597 **3.1.5.2 End-Entity Names**

598 See Central CP.

#### 599 **3.1.6 Recognition, Authentication, and Roles of Trademarks**

600 See Central CP.

## 601 **3.2 Initial Identity Validation**

602 See also Central CP.

#### 603 **3.2.1 Method to Prove Possession of Private Key**

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

#### 607 **3.2.2 Authentication of Organization Identity**

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

#### 609 **3.2.3 Authentication of Individual Identity**

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

#### 611 **3.2.4 Non-verified Subscriber Information**

612 See Central CP.

613 **3.2.5 Validation of Authority**

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

615 **3.2.6 Criteria for Interoperation**

616 No stipulation.

617 **3.3 Identification and Authentication for Re-key Requests**

618 **3.3.1 Identification and Authentication for Routine Re-Key**

619 See central CP.

620 **3.3.2 Identification and Authentication for Re-Key After Revocation**

621 Not supported.

622 **3.4 Identification and Authentication for Revocation Requests**

623 The validity of revocation request shall be checked before forwarding a revocation request to the Product PKI  
624 service.

625 See also Central CP.

## 626 4 Certificate Lifecycle Operational Requirements

### 627 4.1 Certificate Application

#### 628 4.1.1 Who can submit a certificate application?

##### 629 4.1.1.1 Root and Intermediate CA

630 See Central CP.

##### 631 4.1.1.2 Issuing CAs

632 See Central CP.

##### 633 4.1.1.3 End-Entity Certificates

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

#### 636 4.1.2 Enrollment Process and Responsibilities

##### 637 4.1.2.1 CA Certificates

638 See Central CP.

##### 639 4.1.2.2 End-Entity Certificate

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

## 642 4.2 Certificate Application Processing

#### 643 4.2.1 Performing identification and authentication functions

644 The eligibility of requesters is checked as part of the onboarding process.

#### 645 4.2.2 Approval or Rejection of Certificate Applications

646 See Central CP and section 4.2.1.

#### 647 4.2.3 Time to Process Certificate Applications

648 See Central CP.

## 649 4.3 Certificate Issuance

#### 650 4.3.1 CA Actions during Certificate Issuance

651 See Central CP.

#### 652 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

653 The End-Entity (e.g., the operator of a BU RA), for which the subscriber has requested a certificate, shall be notified  
654 w.r.t. the status of certificate issuance.

## 655 4.4 Certificate Acceptance

#### 656 4.4.1 Conduct constituting certificate acceptance

657 See Central CP.

#### 658 4.4.2 Publication of the certificate by the CA

659 No stipulation.

660 **4.4.3 Notification of Certificate issuance by the CA to other entities**

661 No stipulation.

## 662 4.5 Key Pair and Certificate Usage

663 See Central CP

664 **4.5.1 Subject Private Key and Certificate Usage**

665 See Central CP.

666 **4.5.2 Relying Party Public Key and Certificate Usage**

667 See Central CP.

## 668 4.6 Certificate Renewal

669 Certificate renewal is the issuance of a new certificate to an entity without changing the public key or any other  
670 information in the certificate.

671 Not supported.

672 **4.6.1 Circumstance for Certificate Renewal**

673 No stipulation.

674 **4.6.2 Who may request renewal?**

675 No stipulation.

676 **4.6.3 Processing Certificate Renewal Request**

677 No stipulation.

678 **4.6.4 Notification of new Certificate Issuance to Subscriber**

679 No stipulation.

680 **4.6.5 Conduct Constituting Acceptance of a Renewal Certificate**

681 No stipulation.

682 **4.6.6 Publication of the Renewal Certificate by the CA**

683 No stipulation.

684 **4.6.7 Notification of Certificate Issuance by the CA to other Entities**

685 No stipulation.

## 686 4.7 Certificate Re-key

687 "Re-key" addresses the generating of a new Key Pair and applying for the issuance of a new certificate and  
688 replacing the existing Key Pair.

689 **4.7.1 Circumstances for Certificate Re-key**

690 See Central CP.

691 **4.7.2 Who may request certification of a new Public Key?**

692 **4.7.2.1 Re-keying of an Issuing CA certificate**

693 See Central CP.

694 **4.7.2.2 Re-keying of End-Entity certificates**

695 See Central CP.



696	<b>4.7.3 Processing Certificate Re-keying Requests</b>
697	See section 4.3.1
698	<b>4.7.4 Notification of new Certificate Issuance to Subscriber</b>
699	See section 4.3.2
700	<b>4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate</b>
701	See section 4.4.1
702	<b>4.7.6 Publication of the Re-keyed Certificate by the CA</b>
703	See section 4.4.2
704	<b>4.7.7 Notification of Certificate Issuance by the CA to other Entities</b>
705	See section 4.4.3
706	<b>4.8 Certificate Modification</b>
707	Certificate modification means that the keys of a certificate remain unchanged, but more certificate information
708	than for a certificate renewal is changed.
709	Not supported.
710	<b>4.8.1 Circumstance for Certificate Modification</b>
711	No stipulation.
712	<b>4.8.2 Who may request Certificate modification?</b>
713	No stipulation.
714	<b>4.8.3 Processing Certificate Modification Requests</b>
715	No stipulation.
716	<b>4.8.4 Notification of new Certificate Issuance to Subscriber</b>
717	No stipulation.
718	<b>4.8.5 Conduct Constituting Acceptance of Modified Certificate</b>
719	No stipulation.
720	<b>4.8.6 Publication of the Modified Certificate by the CA</b>
721	No stipulation.
722	<b>4.8.7 Notification of Certificate Issuance by the CA to Other Entities</b>
723	No stipulation.
724	<b>4.9 Certificate Revocation and Suspension</b>
725	<b>4.9.1 Circumstances for Revocation</b>
726	See Central CP.
727	<b>4.9.2 Who can request revocation?</b>
728	RA owners can request revocation of the EE certificates that have been issued for their RA.
729	<b>4.9.3 Procedure for Revocation Request</b>
730	See also central CP.
731	See also section 3.4.

732 **4.9.4 Revocation Request Grace Period**

733 See Central CP.

734 **4.9.5 Time within which CA must Process the Revocation Request**

735 See Central CP.

736 **4.9.6 Revocation Checking Requirement for Relying Parties**

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

739 **4.9.7 CRL Issuance Frequency**

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

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

742 **4.9.8 Maximum Latency for CRLs**

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

744 **4.9.9 On-line Revocation/Status Checking Availability**

745 Not supported.

746 **4.9.10 On-line Revocation Checking Requirements**

747 No stipulation.

748 **4.9.11 Other Forms of Revocation Advertisements Available**

749 No stipulation.

750 **4.9.12 Special Requirements for Private Key Compromise**

751 In case of a CA certificate compromise the RA owners shall be informed.

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

754 See also central CP for central service aspects.

755 **4.9.13 Circumstances for Suspension**

756 Not supported.

757 **4.9.14 Who can request suspension?**

758 No stipulation.

759 **4.9.15 Procedure for suspension request**

760 No stipulation.

761 **4.9.16 Limits on suspension period**

762 No stipulation.

763 **4.10 Certificate Status Services**

764 **4.10.1 Operational Characteristics**

765 See section 4.9.

766 **4.10.2 Service Availability**

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

769 **4.10.3 Optional Features**

770 No stipulation.

771 **4.11 End of Subscription**

772 See Central CP.

773 **4.12 Key Escrow and Recovery**

774 Not supported.

775 **4.12.1 Key Escrow and Recovery Policy and Practices**

776 No stipulation.

777 **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

778 No stipulation.

## 779 5 Management, Operational, and Physical Controls

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

### 783 5.1 Physical Security Controls

#### 784 5.1.1 Site Location and Construction

785 See central CP.

#### 786 5.1.2 Physical Access

787 See central CP.

#### 788 5.1.3 Power and Air Conditioning

789 See central CP.

#### 790 5.1.4 Water Exposure

791 See central CP.

#### 792 5.1.5 Fire Prevention and Protection

793 See central CP.

#### 794 5.1.6 Media Storage

795 See central CP.

#### 796 5.1.7 Waste Disposal

797 See central CP.

#### 798 5.1.8 Off-site Backup

799 See central CP.

### 800 5.2 Procedural Controls

#### 801 5.2.1 Trusted Roles

802 See central CP.

#### 803 5.2.2 Numbers of Persons Required per Task

804 See central CP.

#### 805 5.2.3 Identification and Authentication for Each Role

806 See central CP.

#### 807 5.2.4 Roles Requiring Separation of Duties

808 See central CP.

### 809 5.3 Personnel Controls

#### 810 5.3.1 Qualifications, Experience and Clearance Requirements

811 See central CP.

#### 812 5.3.2 Background Check Procedures

813 See central CP.

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

850 **5.5.4 Archive Backup Procedures**

851 See central CP.

852 **5.5.5 Requirements for Time-Stamping of Record**

853 See Central CP.

854 **5.5.6 Archive Collection System (internal or external)**

855 See central CP.

856 **5.5.7 Procedures to Obtain and Verify Archived Information**

857 See Central CP.

858 **5.6 Key Changeover**

859 In the event of a CA key changeover, the new CA public key shall be published with a suitable interval between  
860 certificate expiry date and the last certificate signed to prevent service interruption.

861 **5.7 Compromise and Disaster Recovery**

862 **5.7.1 Incident and Compromise Handling Procedures**

863 See Central CP.

864 **5.7.2 Corruption of Computing Resources, Software, and/or Data**

865 See Central CP.

866 **5.7.3 Entity Private Key Compromise Procedures**

867 See Central CP.

868 **5.7.4 Business Continuity Capabilities After a Disaster**

869 See Central CP.

870 **5.8 CA or RA Termination**

871 See central CP.

## 872 6 Technical Security Controls

### 873 6.1 Key Pair Generation and Installation

#### 874 6.1.1 Key Pair Generation

875 See Central CP [CCP].

#### 876 6.1.2 Private Key Delivery to Subscriber

877 See Central CP [CCP].

#### 878 6.1.3 Public Key Delivery to Certificate Issuer

879 As the EE public key will be generated together with the private key centrally, no transport to the certificate  
880 issuer is required.

#### 881 6.1.4 CA Public Key Delivery to Relying Parties

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

884 See also Central CP [CCP].

#### 885 6.1.5 Key Sizes

886 See Central CP.

#### 887 6.1.6 Public Key Parameters Generation and Quality Checking

888 See Central CP.

#### 889 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

890 See Central CP.

### 891 6.2 Private Key Protection and Cryptographic Module Engineering Controls

#### 892 6.2.1 Cryptographic Module Standards and Controls

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

894 See also central CP for central service aspects.

#### 895 6.2.2 Private Key (n out of m) Multi-person Control

896 4 eyes principle is applied for private keys of end entities (see 6.1.2 Private Key Delivery to Subscriber).

897 See also central CP for central service aspects.

#### 898 6.2.3 Private Key Escrow

899 No supported.

#### 900 6.2.4 Private Key Backup

901 See Central CP.

#### 902 6.2.5 Private Key Archival

903 No stipulation.

#### 904 6.2.6 Private Key Transfer into or from a Cryptographic Module

905 Not supported for End-Entity keys.

906 See also central CP for central service aspects.

#### 907 6.2.7 Private Key Storage on Cryptographic Module

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

909 See also central CP for central service aspects.

910 **6.2.8 Method of Activating Private Key**

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

912 See also central CP for central service aspects.

913 **6.2.9 Method of Deactivating Private Key**

914 Deactivating Private Keys is not supported.

915 **6.2.10 Method of Destroying Private Key**

916 End-Entity private keys shall be deleted in case of resetting the RA.

917 See also central CP for central service aspects.

918 **6.2.11 Cryptographic Module Rating**

919 See section 6.2.1.

920 **6.3 Other Aspects of Key Pair Management**

921 **6.3.1 Public key archival**

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

923 **6.3.2 Certificate operational periods and key pair usage periods**

924 The respective maximum validity periods for keys are:

925

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

926

**Table 1: Maximum validity periods**

927 See also central CP.

928 **6.4 Activation Data**

929 **6.4.1 Activation Data Generation and Installation**

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

931 See also central CP for central service aspects.

932 **6.4.2 Activation Data Protection**

933 See Central CP.

934 **6.4.3 Other Aspects of Activation Data**

935 See Central CP.

936 **6.5 Computer Security Controls**

937 **6.5.1 Specific Computer Security Technical Requirements**

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



939 See also central CP for central service aspects.

940 **6.5.2 Computer Security Rating**

941 No stipulation.

## 942 **6.6 Life Cycle Security Controls**

943 **6.6.1 System Development Controls**

944 See Central CP.

945 **6.6.2 Security Management Controls**

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

947 See also central CP for central service aspects.

948 **6.6.3 Life Cycle Security Controls**

949 See Central CP.

## 950 **6.7 Network Security Controls**

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

952 See also central CP for central service aspects.

## 953 **6.8 Time Stamp Process**

954 See Central CP.

## 955 7 Certificate, CRL, and OCSP Profiles

### 956 7.1 Certificate Profile

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

958 See also central CP.

#### 959 7.1.1 Version Number(s)

960 See Central CP.

#### 961 7.1.2 Certificate Extensions

962 See Central CP.

#### 963 7.1.3 Algorithm Object Identifiers

964 See Central CP.

#### 965 7.1.4 Name Forms

966 See Central CP.

#### 967 7.1.5 Name Constraints

968 No stipulation.

#### 969 7.1.6 Certificate Policy Object Identifier

970 Subject certificates issued under this CP shall assert one or more of the Certificate Policy OIDs listed in section 1.2  
971 of Certificate Policy. Issuing CA certificate shall contain the policy OIDs of all policies under which it issues  
972 certificates.

#### 973 7.1.7 Usage of Policy Constraints Extension

974 No stipulation.

#### 975 7.1.8 Policy Qualifiers Syntax and Semantics

976 No stipulation.

#### 977 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

### 979 7.2 CRL Profile

#### 980 7.2.1 Version number(s)

981 See Central CP.

#### 982 7.2.2 CRL and CRL entry extensions

983 See Central CP.

### 984 7.3 OCSP Profile

#### 985 7.3.1 Version Number(s)

986 See Central CP.

#### 987 7.3.2 OCPS Extension

988 See Central CP.

## 989 8 Compliance Audit and Other Assessment

### 990 8.1 Frequency or Circumstances of Assessment

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

### 996 8.2 Identity / Qualifications of Assessor

997 Compliance audits shall be performed by a qualified auditor.

998 See also central CP for central service aspects.

### 999 8.3 Assessor's Relationship to Assessed Entity

1000 The assessor shall be organizationally independent from the assessed entity's operational authority.

1001 See also central CP for central service aspects.

### 1002 8.4 Topics Covered by Assessment

1003 See Central CP.

### 1004 8.5 Actions Taken as a Result of Deficiency

1005 If a compliance audit or other assessments show deficiencies of the assessed entity, a determination of actions to  
 1006 be taken shall be made. This determination is made by Tenant PMA with input from the auditor/assessor. Tenant  
 1007 PMA is responsible for developing and implementing a corrective action plan.

1008 If Tenant PMA determines that such deficiencies pose an immediate threat to the security or integrity of the  
 1009 Product PKI or the respective Tenant, a corrective action plan shall be developed in accordance with the incident  
 1010 response procedures described in section 5.7.1 within thirty (30) days and implemented within a commercially  
 1011 reasonable period of time, and a re-assessment is to be performed within thirty (30) days after completion of the  
 1012 corrective action. For less serious deficiencies, Tenant PMA shall evaluate the significance of such issues and  
 1013 determine the appropriate response.

1014 Possible actions taken include but are not limited to:

- 1015  temporary suspension of operations until deficiencies are corrected
- 1016  revocation of certificates issued to the assessed entity
- 1017  changes in personnel
- 1018  triggering special investigations or more frequent subsequent compliance assessments, and
- 1019  claims for damages against the assessed entity

### 1020 8.6 Communication of Results

1021 An Audit Compliance Report, including identification of corrective measures taken or being taken by the  
 1022 component, shall be provided to the Tenant PMA.

## 1023 9 Other Business and Legal Matters

1024 All business and legal matters will be regulated within specific contracts if necessary.

### 1025 9.1 Fees

#### 1026 9.1.1 Certificate Issuance or Renewal fees

1027 No stipulation.

#### 1028 9.1.2 Certificate Access fees

1029 No stipulation.

#### 1030 9.1.3 Revocation or Status Information Access fees

1031 No stipulation.

#### 1032 9.1.4 Fees for other Services

1033 No stipulation.

#### 1034 9.1.5 Refund Policy

1035 No stipulation.

### 1036 9.2 Financial Responsibility

1037 No stipulation.

#### 1038 9.2.1 Insurance Coverage

1039 No stipulation.

#### 1040 9.2.2 Other Assets

1041 No stipulation.

#### 1042 9.2.3 Insurance or Warranty Coverage for End-Entities

1043 No stipulation.

### 1044 9.3 Confidentiality of Business Information

#### 1045 9.3.1 Scope of Confidential Information

1046 No stipulation.

#### 1047 9.3.2 Information not within the Scope of Confidential Information

1048 No stipulation.

#### 1049 9.3.3 Responsibility to Protect Confidential Information

1050 No stipulation.

### 1051 9.4 Privacy of Personal Information

#### 1052 9.4.1 Privacy plan

1053 No stipulation.

#### 1054 9.4.2 Information treated as private

1055 No stipulation.

- 1056 **9.4.3 Information not deemed private**  
1057 No stipulation.
- 1058 **9.4.4 Responsibility to protect private information**  
1059 No stipulation.
- 1060 **9.4.5 Notice and consent to use private information**  
1061 No stipulation.
- 1062 **9.4.6 Disclosure pursuant to judicial or administrative process**  
1063 No stipulation.
- 1064 **9.4.7 Other information disclosure circumstances**  
1065 No stipulation.
- 1066 **9.5 Intellectual Property Rights**  
1067 No stipulation.
- 1068 **9.5.1 Intellectual Property Rights in Certificates and Revocation Information**  
1069 No stipulation.
- 1070 **9.5.2 Intellectual Property Rights in CP**  
1071 No stipulation.
- 1072 **9.5.3 Intellectual Property Rights in Names**  
1073 No stipulation.
- 1074 **9.5.4 Property rights of Certificate Owners**  
1075 No stipulation.
- 1076 **9.6 Representations and Warranties**
- 1077 **9.6.1 CA representations and warranties**  
1078 No stipulation.
- 1079 **9.6.2 RA representations and warranties**  
1080 No stipulation.
- 1081 **9.6.3 Subscriber representations and warranties**  
1082 No stipulation.
- 1083 **9.6.4 Relying party representations and warranties**  
1084 No stipulation.
- 1085 **9.6.5 Representations and warranties of other participants**  
1086 No stipulation.
- 1087 **9.7 Disclaimers of Warranties**  
1088 No stipulation.
- 1089 **9.8 Limitations of Liability**  
1090 No stipulation.

1091 **9.9 Indemnities**

1092 No stipulation.

1093 **9.10 Term and Termination**

1094 **9.10.1 Term**

1095 No stipulation.

1096 **9.10.2 Termination**

1097 See Central CP.

1098 **9.10.3 Effect of Termination and Survival**

1099 No stipulation.

1100 **9.11 Individual Notices and Communication with Participants**

1101 No stipulation.

1102 **9.12 Amendments**

1103 **9.12.1 Procedure for Amendment**

1104 In the case of CP amendments, change procedures may include:

- 1105  a notification mechanism to provide notice of proposed amendments to affected Product PKI Participants
- 1106  a comment period; a mechanism by which comments are received, reviewed and incorporated into the
- 1107 document and
- 1108  a mechanism by which amendments become final and effective

1109 **9.12.2 Notification Mechanism and Period**

1110 A modification or amendment of the CP/CPS leads to a new version of the CP/CPS.

1111 The new version of the CP/CPS will be published after its release on the website stated in section 1.5.1.

1112 **9.12.3 Circumstances under which OID must be changed**

1113 Changes, which will not materially reduce the assurance that the CP or its implementation provides and will be  
 1114 judged by the Policy Management Authority (CP section 1.5) to have an insignificant effect on the acceptability of  
 1115 certificates, do not require a change in the CP OID.

1116 Changes, which will materially change the acceptability of certificates for specific purposes, may require  
 1117 corresponding changes to the CP OID.

1118 **9.13 Dispute Resolution Provisions**

1119 No stipulation.

1120 **9.14 Governing Law**

1121 No stipulation.

1122 **9.15 Compliance with Applicable Law**

1123 No stipulation.

1124 **9.16 Miscellaneous Provisions**

1125 No stipulation.

1126 **9.16.1 Entire Agreement**

1127 No stipulation.

1128 **9.16.2 Assignment**

1129 No stipulation.

1130 **9.16.3 Severability**

1131 No stipulation.

1132 **9.16.4 Enforcement (attorneys' fees and waiver of rights)**

1133 No stipulation.

1134 **9.16.5 Force Majeure**

1135 Siemens shall be not held liable for violations of this CP due to causes that are reasonably beyond its control,  
 1136 including but not limited to, an event of Force Majeure, act of the authority, failure of equipment, failure of  
 1137 telecommunications lines, failure of internet access or any unforeseeable events.

1138 **9.17 Other Provisions**

1139 **9.17.1 Order of Precedence of CP**

1140 This CP provides baseline requirements that are applicable to all CAs operated in the name of the Tenant. In the  
 1141 event of a conflict between this CP and any other documents, the following documents shall be given precedence  
 1142 with the same order of the list:

1143 For the scope of applicability for the Product PKI as defined in section 1.1:

1144 1. Product PKI Central CP

1145 2. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1146 3. Documentation executed or expressly authorized by respective PMA

1147 For the scope of applicability for the Tenant specific parts (in particular (L)RA operation and End-Entity  
 1148 authentication) as defined in section 1.1:

1149 1. Tenant CP that is applicable to a Tenant operated by the Product PKI [this document]

1150 2. Product PKI Central CP

1151 3. Documentation executed or expressly authorized by respective PMA

1152 **10. References**

- 1153 In case of legitimate interest, Siemens internal regulations and guidelines as well as other internal documents can  
1154 be retrieved on request.
- 1155 [ACP] Asset Classification & Protection; <https://intranet.siemens.com/acp>
- 1156 [CCP] Siemens Product PKI Certificate Management Service – Central Certificate Policy; Jan. 14, 2022,  
1157 Version 1.8, [www.siemens.com/pki](http://www.siemens.com/pki).
- 1158 [CCPS] Siemens Product PKI Certificate Management Service – Central Certification Practice Statement;  
1159 Jan. 14, 2022, Version 1.2, [www.siemens.com/pki](http://www.siemens.com/pki).
- 1160 [ECRYPT] ECRYPT-CSA; Algorithms, Key Size and Protocols Report; February 2018;  
1161 <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>
- 1162 [ERM] Siemens Enterprise Risk Management; “Enterprise Risk Management – Integrated Framework”;  
1163 <https://intranet.for.siemens.com/cms/054/en/about/org/Pages/cf-a-erm-org.aspx>  
1164 and <https://intranet.for.siemens.com/cms/080/de/processes/office/Pages/ric-ch-erm.aspx>
- 1165 [ETSI 401] ETSI EN 319 401; Electronic Signatures and Infrastructures (ESI); General Policy Requirements for  
1166 Trust Service Providers; August 2017
- 1167 [ETSI 411] ETSI EN 319 411-1; Electronic Signatures and Infrastructures (ESI); Policy and security requirements  
1168 for Trust Service Providers issuing certificates; Part 1: General requirements; August 2017
- 1169 [FIPS] National Institute of Standards and Technology; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC  
1170 MODULES; May 2001; <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- 1171 [IEEE802.1AR] IEEE 802.1AR; IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity;  
1172 June 2018; [https://standards.ieee.org/standard/802\\_1AR-2018.html](https://standards.ieee.org/standard/802_1AR-2018.html)
- 1173 [IHP] The Siemens Incident Handling process as part of the ISMS; [https://www.cert.siemens.com/incident-  
1174 response/process/](https://www.cert.siemens.com/incident-response/process/)
- 1175 [ISMS] SFeRA - Security Framework and Regulations Application; <https://webapps.siemens.com/sfera>
- 1176 [ISO27001] ISO/IEC 27001; Information technology — Security techniques — Information security management  
1177 systems — Requirements; October 2013
- 1178 [NIST] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5 (Draft), NIST,  
1179 10/2019; [https://www.nist.gov/news-events/news/2019/10/recommendation-key-management-part-  
1180 1-general-draft-nist-sp-800-57-part-1](https://www.nist.gov/news-events/news/2019/10/recommendation-key-management-part-1-general-draft-nist-sp-800-57-part-1)
- 1181 [PROF] Certificate Profile Naming Convention for Infrastructure Certificates,  
1182 <https://wiki.ct.siemens.de/display/ProductPKI/PPKI+Naming+Conventions>
- 1183 [RFC2119] IETF; RFC 2119; Key words for use in RFCs to Indicate Requirement Levels; March 1997.
- 1184 [RFC3647] IETF; RFC 3647; Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices  
1185 Framework; November 2003.
- 1186 [RFC5280] IETF; RFC 3647; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List  
1187 (CRL) Profile; May 2008; <https://tools.ietf.org/html/rfc5280>
- 1188 [TÜV] TÜV IT; Sichere Infrastrukturen für IT-Systeme – Trusted Site Infrastructure; Version 4.0;  
1189 [https://www.tuvit.de/fileadmin/user\\_upload/TUEViT\\_TSI\\_V4\\_0.pdf](https://www.tuvit.de/fileadmin/user_upload/TUEViT_TSI_V4_0.pdf)
- 1190 [X.520] ITU-T; X520 Information technology – Open Systems Interconnection – The Directory: Selected  
1191 attribute type