techem

Zertifikatsrichtlinie der Techem PKI

für die ECC-PKI und RSA-PKI

Version 1.0

Verteiler	Alle Teilnehmer der Techem-PKI	
Version	**Datum**	**Was wurde wo geändert?**
0.1		Ersterstellung
1.0	10.05.2019	Erste finale Version

techem

1 Einleitung 9
1.1 Überblick 9
1.2 Name und Kennzeichnung des Dokuments 9
1.3 PKI-Teilnehmer 10
1.3.1 Zertifizierungsstellen 10
1.3.2 Registrierungsstellen 10
1.3.3 Zertifikatsnehmer 11
1.3.3.1 Zertifikatsnehmer RSA-PKI 11
1.3.3.2 Zertifikatsnehmer ECC-PKI 11
1.3.4 Zertifikatsnutzer 11
1.3.5 Andere Teilnehmer 12
1.4 Verwendung von Zertifikaten 12
1.4.1 Erlaubte Verwendungen von Zertifikaten 12
1.4.2 Verbotene Verwendungen von Zertifikaten 12
1.5 Pflege des Policy-Dokuments 12
1.5.1 Zuständigkeit für das Dokument 12
1.5.2 Ansprechpartner/Kontaktpersonen 12
1.5.3 Zuständiger für die Anerkennung einer CP in Hinblick auf diese Mindestanforderungen 13
1.5.4 Annahmeverfahren für Teilnehmer-CP 13
1.6 Definitionen und Abkürzungen 13
2 Veröffentlichungen und Verzeichnisdienst 13
2.1 Informationsdienste 13
2.2 Veröffentlichung von Informationen zur Zertifikatserstellung 13
2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen 14
2.4 Zugriff auf Informationsdienste 14
3 Identifizierung und Authentifizierung 14
3.1 Namensregeln 14
3.1.1 Namensformen 14
3.1.2 Notwendigkeit aussagefähiger Namen 15
3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern 16
3.1.4 Regeln für die Interpretation verschiedener Namensformen 16
3.1.5 Eindeutigkeit von Namen 17
3.1.6 Verwendung von Markennamen 17
3.2 Erstmalige Überprüfung der Identität 17
3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels 17
3.2.2 Authentifizierung von Organisationszugehörigkeiten 17
3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers 17
3.2.4 Ungeprüfte Zertifikatsnehmerangaben 18
3.2.5 Prüfung der Berechtigung zur Antragstellung 18
3.2.6 Kriterien zur Zusammenarbeit 18

3.3 Identifizierung und Authentifizierung von Anträgen auf Zertifizierung nach Schlüsselerneuerung 18
3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Zertifizierung nach Schlüsselerneuerung 18
3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen 18
3.4 Identifizierung und Authentifizierung von Sperranträgen 19
4 Betriebsanforderungen 19
4.1 Zertifikatsantrag 19
4.1.1 Wer kann einen Zertifikatsantrag stellen? 19
4.1.2 Registrierungsprozess und Zuständigkeiten 19
4.2 Verarbeitung des Zertifikatsantrags 19
4.2.1 Durchführung der Identifizierung und Authentifizierung 20
4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen 20
4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen 20
4.3 Zertifikatsausgabe 20
4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten 20
4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA 21
4.4 Zertifikatsannahme 21
4.4.1 Verhalten für eine Zertifikatsannahme 21
4.4.2 Veröffentlichung des Zertifikats durch die CA 21
4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats 21
4.5 Verwendung des Schlüsselpaares und des Zertifikats 21
4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer 21
4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer . 22
4.6 Zertifikatserneuerung ohne Schlüsselwechsel 22
4.6.1 Bedingungen für eine Zertifikatserneuerung 22
4.6.2 Wer darf eine Zertifikatserneuerung beantragen? 22
4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung 22
4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats .. 23
4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung 23
4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA 23
4.6.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Erneuerung des Zertifikats 23
4.7 Zertifikatserneuerung mit Schlüsselwechsel 23
4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung 23
4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen? 23
4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen 23
4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats 24
4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen 24
4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA 24
4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats 24

4.8 Zertifikatsänderung 24
4.8.1 Bedingungen für eine Zertifikatsänderung 24
4.8.2 Wer darf eine Zertifikatsänderung beantragen? 24
4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung 25
4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats .. 25
4.8.5 Verhalten für die Annahme einer Zertifikatsänderung 25
4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA 25
4.8.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats. 25
4.9 Sperrung und Suspendierung von Zertifikaten 25
4.9.1 Bedingungen für eine Sperrung 26
4.9.2 Wer kann eine Sperrung beantragen? 26
4.9.3 Verfahren für einen Sperrantrag 26
4.9.4 Fristen für einen Sperrantrag 26
4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die Techem CA 26
4.9.6 Nutzung der verfügbaren Methoden zum Prüfen von Sperrinformationen 27
4.9.7 Frequenz der Veröffentlichung von Sperrlisten 27
4.9.8 Maximale Latenzzeit für Sperrlisten 27
4.9.9 Verfügbarkeit von Online-Sperrinformationen 27
4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen 27
4.9.11 Andere Formen zur Anzeige von Sperrinformationen 28
4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels 28
4.9.13 Bedingungen für eine Suspendierung 28
4.9.14 Wer kann eine Suspendierung beantragen? 28
4.9.15 Verfahren für Anträge auf Suspendierung 28
4.9.16 Begrenzungen für die Dauer von Suspendierungen 28
4.10 Statusabfragedienst für Zertifikate 28
4.10.1 Funktionsweise des Statusabfragedienstes 28
4.10.2 Verfügbarkeit des Statusabfragedienstes 28
4.10.3 Optionale Leistungen 29
4.11 Kündigung durch den Zertifikatsnehmer 29
4.12 Schlüsselhinterlegung und Wiederherstellung 29
4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel 29
4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln 29
5 Physische, organisatorische und personelle Sicherheitsmaßnahmen 29
5.1 Physische Sicherheitsmaßnahmen 30
5.1.1 Lage und Gebäude 30
5.1.2 Zugang 30
5.1.3 Strom, Heizung und Klimaanlage 30
5.1.4 Gefährdung durch Wasser 30
5.1.5 Brandschutz 30
5.1.6 Aufbewahrung von Datenträgern 30
5.1.7 Datenvernichtung 31
5.1.8 Desaster Backup 31

5.2 Verfahrensvorschriften 31
5.2.1 Rollenkonzept 31
5.2.2 Mehraugenprinzip 31
5.2.3 Identifizierung und Authentifizierung jeder Rolle 31
5.2.4 Rollentrennung 32
5.3 Personelle Sicherheitsmaßnahme 32
5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit 32
5.3.2 Sicherheitsüberprüfung der Mitarbeiter 32
5.3.3 Anforderungen an Schulungen 32
5.3.4 Häufigkeit von Schulungen und Belehrungen 32
5.3.5 Häufigkeit und Folge von Job-Rotation 32
5.3.6 Maßnahmen bei unerlaubten Handlungen 32
5.3.7 Anforderungen an freie Mitarbeiter 33
5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen 33
5.4 Überwachungsmaßnahmen 33
5.4.1 Arten von aufgezeichneten Ereignissen 33
5.4.2 Häufigkeit der Analyse von Aufzeichnungen 33
5.4.3 Aufbewahrungszeit von Aufzeichnungen 33
5.4.4 Schutz der Aufzeichnungen 33
5.4.5 Datensicherung der Aufzeichnungen 33
5.4.6 Speicherung der Aufzeichnungen (intern / extern) 34
5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen 34
5.4.8 Schwachstellenanalyse 34
5.5 Archivierung von Aufzeichnungen 34
5.5.1 Arten von archivierten Aufzeichnungen 34
5.5.2 Aufbewahrungsfristen für archivierte Daten 34
5.5.3 Schutz des Archivs 34
5.5.4 Datensicherung des Archivs 34
5.5.5 Anforderungen an Zeitstempel 34
5.5.6 Archivierung (intern / extern) 34
5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen 35
5.6 Schlüsselwechsel der CA 35
5.7 Kompromittierung und Geschäftswiederherstellung 35
5.7.1 Behandlung von Vorfällen und Kompromittierungen 35
5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung 35
5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der CA 35
5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einem Katastrophenfall 36
5.8 Schließung einer CA oder einer Registrierungsstelle 36
6 Technische Sicherheitsmaßnahmen 36
6.1 Erzeugung und Installation von Schlüsselpaaren 37
6.1.1 Erzeugung von Schlüsselpaaren 37
6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer 37
6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber 37
6.1.4 Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer 37
6.1.5 Schlüssellängen 38

6.1.5.1 Schlüssellängen RSA-PKI 38
6.1.5.2 Schlüssellängen ECC-PKI 38
6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle 38
6.1.6.1 Parameter RSA-PKI 38
6.1.6.2 Parameter ECC-PKI 38
6.1.7 Schlüsselverwendungen 39
6.2 Schutz des privaten Schlüssels und Anforderungen an kryptographische Module 39
6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module 39
6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) 39
6.2.3 Hinterlegung privater Schlüssel 39
6.2.4 Backup privater Schlüssel 39
6.2.5 Archivierung privater Schlüssel 39
6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen 39
6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen 40
6.2.8 Aktivierung privater Schlüssel 40
6.2.9 Deaktivierung privater Schlüssel 40
6.2.10 Zerstörung privater Schlüssel 40
6.2.11 Beurteilung kryptographischer Module 40
6.3 Andere Aspekte des Managements von Schlüsselpaaren 40
6.3.1 Archivierung öffentlicher Schlüssel 40
6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren 41
6.4 Aktivierungsdaten 41
6.4.1 Vergabe von Aktivierungsdaten 41
6.4.2 Schutz von Aktivierungsdaten 41
6.4.3 Andere Aspekte 41
6.5 Sicherheitsmaßnahmen in den Rechneranlagen 41
6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen 41
6.5.2 Beurteilung von Computersicherheit 41
6.6 Technische Maßnahmen während des Lebenszyklus 42
6.6.1 Sicherheitsmaßnahmen bei der Entwicklung 42
6.6.2 Sicherheitsmaßnahmen beim Computermanagement 42
6.6.3 Sicherheitsmaßnahmen während des Lebenszyklus 42
6.7 Sicherheitsmaßnahmen für Netze 42
6.8 Zeitstempel 42
7 Profile von Zertifikaten, Sperrlisten und OCSP 42
7.1 Zertifikatsprofile 42
7.1.1 Versionsnummern 43
7.1.2 Zertifikatserweiterungen 43
7.1.3 Algorithmen OIDs 44
7.1.4 Namensformate 44
7.1.5 Namensbeschränkungen 44
7.1.6 OIDs der Zertifikatsrichtlinien 44
7.1.6.1 RSA-PKI OIDs 44
7.1.6.2 ECC-PKI OIDs 44
7.1.7 Nutzung der Erweiterung "Policy Constraints" 45

7.1.8 Syntax und Semantik von "Policy Qualifiers" 45
7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikatsrichtlinie 45
7.2 Sperrlistenprofile 45
7.2.1 Versionsnummern 45
7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen 45
7.3 Profile des Statusabfragedienstes (OCSP) 45
7.3.1 Versionsnummern 46
7.3.2 OCSP Erweiterungen 46
8 Überprüfungen der CA und andere Bewertungen 46
8.1 Häufigkeit und Bedingungen für Überprüfungen 46
8.2 Identität/Qualifikation des Prüfers 46
8.3 Stellung des Prüfers zum Bewertungsgegenstand 46
8.4 Durch Überprüfungen abgedeckte Themen 46
8.5 Reaktionen auf Unzulänglichkeiten 46
8.6 Information über Bewertungsergebnisse 46
9 Andere finanzielle und rechtliche Angelegenheiten 47
9.1 Gebühren 47
9.2 Finanzielle Zuständigkeiten 47
9.3 Vertraulichkeitsgrad von Geschäftsdaten 47
9.3.1 Definition von vertraulichen Informationen 47
9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören 47
9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen 47
9.4 Schutz personenbezogener Daten 47
9.4.1 Datenschutzkonzept 47
9.4.2 Als persönlich behandelte Daten 48
9.4.3 Daten, die nicht als persönlich behandelt werden 48
9.4.4 Zuständigkeiten für den Datenschutz 48
9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten 48
9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften 48
9.4.7 Andere Bedingungen für Auskünfte 48
9.5 Geistiges Eigentumsrecht 48
9.6 Zusicherungen und Garantien 49
9.6.1 Zusicherungen und Garantien der CA 49
9.6.2 Zusicherungen und Garantien der RA 49
9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer 49
9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer 49
9.6.5 Zusicherungen und Garantien anderer PKI-Teilnehmer 49
9.7 Gewährleistungen 49
9.8 Haftungsbeschränkungen 50
9.9 Schadensersatz 50
9.10 Inkrafttreten und Beendigung 50
9.10.1 Inkrafttreten 50
9.10.2 Beendigung 50
9.10.3 Auswirkung der Beendigung und Weiterbestehen 50
9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern 50

9.12 Ergänzungen 50
9.12.1 Verfahren für Ergänzungen 51
9.12.2 Benachrichtigungsmechanismen und -fristen 51
9.12.3 Bedingungen für OID Änderungen 51
9.13 Verfahren zur Schlichtung von Streitfällen 51
9.14 Zugrunde liegendes Recht 51
9.15 Einhaltung geltenden Rechts 51
9.16 Sonstige Bestimmungen 51
9.16.1 Vollständigkeitserklärung 51
9.16.2 Abgrenzungen 52
9.16.3 Salvatorische Klausel 52
9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) 52
9.16.5 Höhere Gewalt 52
9.17 Andere Bestimmungen 52

0

1 Einleitung

Dieses Dokument ist die Zertifizierungsrichtlinie (CP) der Techem PKI für das Sicherheitsniveau
Produktion. Sie regelt die Abläufe und legt dabei insbesondere die Rahmenbedingungen für die
Ausstellung von Zertifikaten entsprechend der internationalen Norm X.509 fest.

1.1 Überblick

Diese CP ist nach RFC 3647 gestaltet.

In diesem Dokument werden alle wesentlichen Vorgänge und Verfahren zur Nutzung und zum Betreib der Techem PKI beschrieben.

Alle in dieser CP angegebenen Regelungen sind für alle Beteiligten der Techem PKI verbindlich und können nicht abgeschwächt werden.

Im Rahmen der Techem PKI betreibt die Techem Energy Services GmbH für das Sicherheitsniveau Produktion die oberste Zertifizierungsstellen (Root-CAs) und alle nachgeordneten Zertifizierungsstellen (Sub-CAs) für die beiden PKI-Stränge ECC-PKI und RSA-PKI.

Diese CP umfasst alle PKI Stränge der Techem PKI, sowohl den RSA als auch den ECC Strang. In Kapiteln in denen die beschriebenen Prozesse aufgrund der unterschiedlichen Anwendungen in den Strängen von einander Abweichen werden Unterpunkte aufgenommen.
Diese sind analog der Techem OID bezeichnet im Falle von Kapitel x, Unterkapitel y:

- x.y.1 für die RSA-PKI
- x.y.2 für die ECC-PKI

1.2 Name und Kennzeichnung des Dokuments

Diese CP ist eine übergreifende CP und enthält sowohl die CP für die RSA PKI als auch für die ECC PKI und ist folgendermaßen identifiziert:

- Titel: Zertifizierungsrichtlinie der Techem PKI - Sicherheitsniveau Produktion -

- Version: 1.0
- Object Identifier (OID): 1.3.6.1.4.1.14721.100.0.1.1.1.10 (RSA-PKI)
- Object Identifier (OID): 1.3.6.1.4.1.14721.100.0.2.1.1.10 (ECC-PKI)

Die OIDs sind wie folgt zusammengesetzt:

RSA PKI
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) techem (14721) pki(100) production(0) rsa(1) internal(1) version(1) cp(10)}

ECC PKI
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) Techem (14721) pki(100) production(0) ecc(2) internal(1) version(1) cp(10)}

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Den Zertifizierungsstellen (CAs) obliegt die Ausstellung von Zertifikaten innerhalb der Techem PKI.

Die Techem PKI besteht aus zwei getrennten Strängen, einem ECC-Strang und einem RSA-Strang. Beide Stränge sind in sich abgeschlossen und verfügen jeweils über eine eigene RootCA.
So gibt es zwei RootCAs in der Techem PKI, eine ECC-RootCA und eine RSA-RootCA.

Die obersten CAs der Techem PKI (Techem RootCAs) zertifizieren ausschließlich Zertifikate von unmittelbar nachgeordneten CAs entsprechend dieser CP und dem CPs der Techem PKI. Der Betrieb der Techem RootCAs und aller nachgeordneten CAs in der Techem PKI erfolgt durch die Techem Energy Services GmbH.
Die öffentlichen Schlüssel der Techem -RootCAs sind in selbstsignierten Zertifikaten enthalten (Techem ECCRootCA 01 G1 und Techem RSARootCA 01 G1). Zertifikate für nachgeordnete CAs können in der Techem PKI ausschließlich durch die Techem RootCAs ausgestellt werden.

1.3.2 Registrierungsstellen

Einer Registrierungsstelle (RA) obliegt die Überprüfung der Identität und Authentizität von Teilnehmern und Zertifikatsinhabern.
Sie überprüft auch die Berechtigung des Antragstellers eines Zertifkats auf Zertifikatsausstellung gemäß den Techem Vorgaben.

Diese Aufgaben werden von den betreuenden Fachabteilungen der jeweiligen CA übernommen.

1.3.3 Zertifikatsnehmer

Ein Zertifikatsnehmer besitzt den Privaten-Schlüssel, der zum Öffentlichen-Schlüssel im Zertifikat der Techem PKI gehört. Er ist verpflichtet, die Sicherheitsrichtlinien der Techem Energy Services GmbH einzuhalten.

Mögliche Verwendungszwecke in den End-Entitäten können je nach PKI Strang (RSA/ECC) variieren. Für die verschiedenen Stränge gelten folgende Regeln:

1.3.3.1 Zertifikatsnehmer RSA-PKI

Zertifikate ausgestellt von der RSA SubCA 01

- Kunden
- Mitarbeiter
- Geschäftspartner

Zertifikate ausgestellt von der RSA SubCA 02

- Computer
- Netzwerkdevices

1.3.3.2 Zertifikatsnehmer ECC-PKI

- Computer
- Netzwerkdevices
- IoT Geräte

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer von Zertifikaten der Techem PKI müssen in einer Geschäftsverbindung zur Techem Energy Services GmbH stehen, die Ihnen erlaubt Techem- Zertifikate zu nutzen. Indem sie die Techem PKI nutzen, erklären sie sich implizit damit einverstanden, die Techem Sicherheitsrichtlinien und diese CP einzuhalten.

1.3.5 Andere Teilnehmer

Bei Dienstleistern, die als Zertifikatsnehmer tätig werden, um Dienste für die Techem Energy Services GmbH zu erbringen, liegt die Verantwortung für die Einhaltung der CP beim beauftragenden Dienstleister.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Die im Rahmen der Techem PKI ausgestellten Zertifikate dürfen für alle Verfahren genutzt werden, die von dem im Zertifikat enthaltenen Schlüsselverwendungszwecken ermöglicht werden.

Je nach Profil des Zertifikats sind dies unter anderem:

- Authentisierung von Servern mit TLS
- Authentisierung von Nutzern (TLS-Client-Authentisierung)
- Authentisierung von IoT Geräten (TLS-Client-Authentisierung)
- Verschlüsselung von Daten

Teilnehmer bzw. Zertifikatsinhaber sind selbst für die Nutzung in den Anwendungsprogrammen
zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen deren Sicherheitsanforderungen genügen.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die Nutzung des Zertifikats darf nicht im Widerspruch zu den im Zertifikat enthaltenen Schlüsselverwendungszwecken erfolgen, insbesondere ist die Ausstellung von Zertifikaten und Sperrlisten ausschließlich CAs vorbehalten.

1.5 Pflege des Policy-Dokuments

1.5.1 Zuständigkeit für das Dokument

Die Verwaltung dieses Dokuments erfolgt durch die Abteilung IT-Architecture & Governance der Techem Energy Services GmbH.

1.5.2 Ansprechpartner/Kontaktpersonen

Für Fragen zum Betrieb und zur Verwendung von Zertifikaten der Techem PKI ist folgende Email-Adresse zu verwenden:

it-sicherheit@techem .de

1.5.3 Zuständiger für die Anerkennung einer CP in Hinblick auf diese Mindestanforderungen

Die in Abschnitt 1.5.2 benannten Personen sind für die jährliche Prüfung der CP in der Techem PKI
verantwortlich.

1.5.4 Annahmeverfahren für Teilnehmer-CP

Die Genehmigung der CP erfolgt durch den Informationssicherheitsbeauftragten der Techem Energy Services GmbH.

1.6 Definitionen und Abkürzungen

PKIX	Public Key Infrastrukturen nach X.509 [RFC 5280]
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
DN	Distinguished Name nach X.500
CSR	Certificate Signing Request (PKCS#10)

2 Veröffentlichungen und Verzeichnisdienst

2.1 Informationsdienste

Für jede CA der Techem PKI werden die in Abschnitt 2.2 genannten Informationen gemäß Abschnitt
2.3 und Abschnitt 2.4 vorgehalten.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die folgenden Informationen werden veröffentlicht:

- CP der Techem PKI – Sicherheitsniveau Produktion–

- Zertifikate der techm Root-CAs und deren Sub-CAs, sowohl ECC als auch RSA, mit ihren Fingerabdrücken
- Kontaktinformationen, unter denen eine Sperrung beantragt werden kann
- Sperrinformationen der Techem Root-CAs und ihrer Sub-CAs
- Verweis auf den Verzeichnisdienst der Techem PKI
- Pflichten der Teilnehmer
- Informationen für Zertifikatsinhaber

Diese Informationen werden online auf den Seiten:

- ca-rsa.techem.de – für Belange der RSA-PKI
- ca-ecc.techem.de – für Belange der ECC-PKI

veröffentlicht und stehen dort ständig (24 Stunden am Tag, 7 Tage die Woche) zur Verfügung. Es wird sichergestellt, dass ungeplante Ausfallzeiten und Wartungen minimiert und der Betrieb schnellstmöglich wiederhergestellt wird.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Für die Aktualisierung der in Abschnitt 2.2 genannten Informationen gelten folgende Fristen:

- Zertifikate: spätestens drei Werktage nach der Ausstellung
- CP: zum Inkrafttreten einer neuen Version (nach Ankündigung, s. Abschnitt 9.10.1)
- Sperrinformationen:
  CRLs: Siehe Abschnitt 4.9.7

  OCSP: analog zu CRLs (siehe Abschnitt 4.9.7)

2.4 Zugriff auf Informationsdienste

Der lesende Zugriff auf alle in Abschnitt 2.2 aufgeführten Informationen ist ohne Zugriffskontrolle
möglich. Schreibender Zugriff auf diese Informationen wird nur berechtigten
Personen gewährt.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Namensformen

In der Techem PKI wird eine einheitliche Namenshierarchie verwendet.
Alle innerhalb der Techem PKI ausgestellten Zertifikate beinhalten eindeutige Namen (DN) gemäß der Normenserie X.500. Ein DN enthält eine Folge von kennzeichnenden Attributen, durch die jeder Zertifikatsinhaber eindeutig referenziert wird.

Ein DN entspricht grundsätzlich folgendem Schema, dabei sind optionale Attribute in eckige Klammern gesetzt, Attributwerte in spitzen Klammern müssen durch die jeweiligen Werte ersetzt werden. Die Reihenfolge dieser Attribute muss eingehalten werden. Die Bedeutung der Attribute wird in Abschnitt 3.1.2 beschrieben.

C=<Staat>
O=<Organisation>
CN=<Eindeutiger Name>

Die Attribute „C“ und „O“ müssen genau einmal angegeben werden und sind innerhalb der Techem PKI festgelegt. C=“DE“, O=“techem” als Synonym für Techem Energy Services GmbH.
Die Attribute „OU“, „CN“ und „emailAddress“ dürfen auch mehrfach angegeben werden.
Weitere Attribute (z. B. „SER“ oder „UID“) können verwendet werden, soweit sie die in der Techem PKI verwendeten Standards nicht verletzen.
Obwohl die Angabe von E-Mail-Adressen im DN möglich ist, sollten diese bevorzugt in der Zertifikaterweiterung „subjectAlternativeName“ aufgenommen werden.
In Zertifikate für Datenverarbeitungssysteme werden keine E-Mail-Adressen aufgenommen, weder im DN noch im „subjectAlternativeName“.

3.1.2 Notwendigkeit aussagefähiger Namen

Der DN muss den Zertifikatsinhaber eindeutig identifizieren und er muss aussagekräftig sein.

Bei der Namensvergabe gelten die folgenden Regelungen:
Das Pflichtattribut „C“ muss das 2-Zeichen-Staaten-Kürzel (festgelegt im ISO Standard 3166-1 [ISO-3166-1]) des Staates enthalten, in dem die im Pflichtattribut „O“ genannte Organisation ihren Standort hat.
Das Pflichtattribut „O“ muss den Namen des Teilnehmers enthalten. Die Authentizität des Namens wird nach Abschnitt 3.2.2 überprüft. Namen einer organisatorischen Untereinheit der im Pflichtattribut „O“ genannten Organisation
enthalten. Falls mehrere Attribute „OU“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden und die Reihenfolge der benannten organisatorischen
Untereinheiten sollte von größeren zu kleineren Untereinheiten absteigen.
Der DN enthält mindestens ein Attribut „CN“.

Jedes Attribut „CN“ muss eine angemessene Darstellung des Namens des Zertifikatsinhabers enthalten, es muss folgendes gelten:

a. Ein Attribut „CN“ in einem Zertifikat für ein Datenverarbeitungssystem enthält alternativ:
   - einen voll-qualifizierten Domain-Namen

- eine IP-Adresse
- eine eindeutige Geräte ID

b. Ein Attribut “CN” in einem Zertifikat für Personen oder Mandanten enthält den Namen der Person oder der juristische Person

c. Ein Attribut „CN“ in einem Zertifikat für eine Zertifizierungsstelle enthält den Namen der CA bzw. einen eindeutigen Hinweis auf die CA-Funktion.

Falls mehrere Attribute „CN“ angegeben werden, müssen diese im DN jeweils direkt hintereinander aufgeführt werden.

In Zertifikaten für Datenverarbeitungssysteme werden keine E-Mail-Adressen aufgenommen, weder im DN noch im „subjectAlternativeName“.
In Zertifikaten für Personen oder Mandanten sollte im “subjectAlternativeName” eine E-Mail-Adresse aufgenommen werden, unter der die Person oder der Mandant erreichbar ist.

Für E-Mail-Adressen, IP-Adressen und Domain-Namen, die in die Zertifikaterweiterung für alternative Zertifikatnamen („subjectAlternativeName“) unter den Typen „rfc822Name“, „iPAddress“ bzw. „dNSName“ aufgenommen werden, gelten obige Regelungen analog.

Ist ein Attributwert länger als durch den jeweiligen Standard erlaubt, so muss stattdessen eine angemessene, wenn möglich wohlbekannte und eingeführte Abkürzung verwendet werden.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Entfällt

3.1.4 Regeln für die Interpretation verschiedener Namensformen

In den DN-Attributen „L“, „O“, „OU“ und „CN“ dürfen ausschließlich
die folgenden Zeichen verwendet werden:

a-z A-Z 0-9 ' ( ) , - . / : Leerzeichen

Im CN darf für besondere Zertifikattypen zusätzlich ein „*“ verwendet werden.
Für die Ersetzung deutscher Sonderzeichen gelten folgende Substitutionsregeln:

Ä -> Ae, Ö ->Oe, Ü -> Ue, ä -> ae, ö -> oe, ü -> ue, ß -> ss

Sonderzeichen mit Akzenten verlieren diese. Ansonsten wird eine für das betreffende Zeichen
gemeinhin verwendete Schreibweise aus den Zeichen a-z und A-Z so zusammengesetzt,

dass der entsprechende Laut entsteht.

3.1.5 Eindeutigkeit von Namen

Vor der Zertifizierung muss die Korrektheit und Eindeutigkeit des angegebenen Namens von der Techem PKI RA überprüft werden. Der DN eines Zertifikatsinhabers muss eindeutig sein und
darf nicht an unterschiedliche Zertifikatsinhaber vergeben werden.
Bei Namensgleichheit gilt grundsätzlich das Prinzip: „Wer zuerst kommt, wird zuerst bedient".
In Streitfällen entscheidet die Techem PKI. Die Eindeutigkeit des DN kann durch die Verwendung von „OU", „UID" oder „SER" Attributen oder durch die Verwendung von Pseudonymen
im Attribut „CN" wie z. B. „PN: Max Mustermann 2" erreicht werden

3.1.6 Verwendung von Markennamen

Entfällt.

3.2 Erstmalige Überprüfung der Identität

3.2.1 Methoden zur Überprüfung des Besitzes des privaten Schlüssels

Bei Antragsstellung mittels Certificate Signing Request (CSR) muss nachgewiesen werden, dass der zukünftige Zertifikatsinhaber im Besitz des privaten Schlüssels ist. Dies geschieht, indem der im Zertifikatantrag enthaltene CSR mit dem privaten Schlüssel signiert und an die CA übermittelt
wird. Die CA muss die Gültigkeit der Signatur überprüfen.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Wenn sich der Zertifikatsnutzer außerhalb der Techem Energy Services GmbH befindet, muß durch den Fachbereich sichergestellt sein, dass der Externe-Teilnehmer über eine vertragliche Beziehung zur Techem Energy Services GmbH verfügt, die ihn zur Nutzung von Zertifikaten der Techem PKI berechtigt.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsnehmers

Es muß ein von dem nutzenden Fachbereich erarbeiteten und von der Techem PKI abgenommenen Prozess zur Identifizierung und Authentifizierung des Zertifikatsnehmers geben.

Der Prozess muss sicherstellen, dass nur der vorgesehene Nutzerkreis an Zertifikate der Techem PKI gelangt und Missbrauch unterbunden ist.

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

Außer den Angaben in Abschnitt 3.2.2 und Abschnitt 3.2.3 werden keine weiteren Informationen
überprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Es muß ein, von dem nutzenden Fachbereich, erarbeiteten und von der Techem PKI abgenommenen Prozess zur Überprüfung für die Berechtigung zur initial Zulassung eines Teilnehmers geben. Dieser muß sicherstellen, das nur berechtigte Anträge von der Techem PKI bearbeitet wird.

3.2.6 Kriterien zur Zusammenarbeit

Über eine Zusammenarbeit mit den PKIs anderer Institutionen entscheidet ausschließlich die Techem PKI.

3.3 Identifizierung und Authentifizierung von Anträgen auf Zertifizierung nach Schlüsselerneuerung

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Zertifizierung nach Schlüsselerneuerung

Bei der routinemäßigen Zertifikaterneuerung ist neben den Methoden aus Abschnitt 3.2.3 zusätzlich die Authentifizierung der Identität eines Zertifikatsnutzers durch ein gültiges persönliches Zertifikat aus der Techem PKI zulässig, wenn die zugrundeliegende Identifizierung
innerhalb der Befristung aus Abschnitt 4.2.1 durchgeführt wurde.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Nach dem Sperren eines Zertifikats kann eine Authentifizierung nicht mehr mit dem gesperrten
Zertifikat durchgeführt werden.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Authentifizierung einer Sperrung (siehe Abschnitt 4.9) kann auf die folgenden Arten erfolgen:

- Übermittlung einer vorher vereinbarten Authentisierungsinformation (schriftlich, per Telefon, oder elektronisch)
- Übergabe eines Sperrantrags mit einer geeigneten elektronischen Signatur, die den Teilnehmer bzw. Zertifikatsinhaber authentifiziert
- Übergabe eines Sperrantrags mit einer handschriftlichen Unterschrift

4 Betriebsanforderungen

4.1 Zertifikatsantrag

Das Stellen eines Zertifikatsantrages bedeutet nicht, dass die Techem PKI verpflichtet ist, ein Zertifikat gemäß des Zertifikatsantrages auszustellen. Er stellt lediglich die Anforderung eines Zertifikates dar.

Zertifikatsanträge können grundsätzlich nur für bereits eingeführte Verfahren angenommen werden. Die Zuordnung eines Zertifikatsantrags zu einem Verfahren und damit einem Fachbereich ist zwingend notwendig.

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Eine Zertifikatsantrag wird grundsätzlich durch den nutzenden Fachbereich oder einen von diesem ermächtigten Teilnehmer beantragt.

Zertifikate die von PKI Komponenten benötigt werden, wie dem OCSP Responder Zertifikat, werden automatisch beantragt und ausgestellt.

4.1.2 Registrierungsprozess und Zuständigkeiten

Es muss einen von dem nutzenden Fachbereich erarbeiteten und von der Techem PKI abgenommenen Registrierungsprozess geben. Dieser stellt sicher, dass nur der vorgesehene Nutzerkreis an Zertifikate der Techem PKI gelangt und Missbrauch unterbunden wird.

4.2 Verarbeitung des Zertifikatsantrags

Zertifikatsanträge können einzeln oder als Massenanfrage an die Techem PKI gestellt werden.
Es sind dabei die jeweiligen vereinbarten Verfahren und Protokolle einzuhalten.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Durch geeignete Maßnahmen zur Identifizierung und Authentifizierung ist sicherzustellen, dass Techem PKI Schlüsselmaterial und Zertifikate nicht in die Hände von unberechtigten Dritten gelangt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Für die Annahme oder Ablehnung von Zertifikatsanträgen, wenn diese den geforderten technischen Anforderungen der Techem PKI entsprechen, ist der Fachbereich des nutzenden Verfahrens zuständig.

Wenn die technischen Anforderungen der Techem PKI nicht eingehalten werden, werden diese seitens der Techem PKI abgelehnt, unabhängig von der Annahme durch den Fachbereich.

Grundsätzlich sind Teilnehmer von einer Ablehnung Ihres Zertifikatsantrages in Kenntnis zu setzen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die konkreten Fristen und Bearbeitungszeiten für Zertifikatsanträge werden jeweils mit dem Fachbereich verfahrensindividuell geregelt.

4.3 Zertifikatsausgabe

Die Art der Zertifikatsausgabe durch die Techem PKI wird jeweils mit dem Fachbereich verfahrensindividuell geregelt.

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten

Die formalen Voraussetzungen für die Ausstellung eines Zertifikats werden durch die CA in angemessener Weise überprüft. Insbesondere überprüft die CA die Gültigkeit der Signatur des CSR.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch die CA

Nach der Ausstellung des Zertifikates durch die CA, wird dem Zertifikatsnehmer auf dem für die Nutzung vorgesehenen Weg das Zertifikat übermittelt oder er wird durch die CA über die Möglichkeit zum Download informiert.

Insbesondere kommen hierbei auch vereinbarte automatisierte Verfahren zum Einsatz, die ohne das manuelles Eingreifen des Zertifikatsnehmers auskommen.

4.4 Zertifikatsannahme

Der Zertifikatsinhaber ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der ausstellenden CA nach Erhalt zu verifizieren.

4.4.1 Verhalten für eine Zertifikatsannahme

Ein Zertifikat wird angenommen, wenn es verwendet wird oder wenn innerhalb von 5 Tagen nach Erhalt kein Widerspruch erfolgt.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Eine Veröffentlichung der Zertifikate in Verzeichnisdiensten seitens der CA findet nicht statt.

4.4.3 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe des Zertifikats

Entfällt

4.5 Verwendung des Schlüsselpaares und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Private Schlüssel müssen angemessen geschützt werden. Zertifikate dürfen ausschließlich in Übereinstimmung mit diesem CP eingesetzt werden.
Eine von der im Zertifikat vorhandenen KeyUsage abweichenden Nutzung ist nicht erlaubt.

Insbesondere ist es End-Entitäts-Zertifikaten nicht erlaubt als CA aufzutreten und andere Zertifikate oder CRL zu signieren.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Wenn Zertifikatsprüfer Zertifikate aus der Techem PKI verwenden, müssen sie sicherstellen, dass diese ein im Anwendungskontext angemessenes Sicherheitsniveau haben. Darüber hinaus sind Zertifikatsprüfer verpflichtet sicherzustellen, dass ein geprüftes Zertifikat korrekt
und gültig ist. Dies schließt die Prüfung der Signatur des Zertifikats durch die ausstellende CA sowie die Prüfung des Zertifikats auf Sperrung ein.

4.6 Zertifikatserneuerung ohne Schlüsselwechsel

Bei einer Zertifikatserneuerung ohne Schlüsselwechsel wird ein neues Zertifikat unter Beibehaltung
des alten Schlüsselpaars ausgestellt, sofern das Schlüsselpaar den kryptographischen Mindestanforderungen der CP genügt, die im Zertifikat enthaltenen Informationen unverändert bleiben und kein Verdacht auf Kompromittierung des privaten Schlüssels vorliegt.

4.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung kann beantragt werden, wenn die Gültigkeit eines Zertifikats abläuft.

Grundsätzlich ist von einem Rezertifizieren des alten Schlüssels abzusehen und mit einem neuen Zertifikat auch ein neuer Schlüssel zu generieren.

Wenn technische Aspekte es erforderlich machen ist auch eine Zertifikatserneuerung mit Rezertifizierung des alten Schlüssels erlaubt.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Eine Zertifikatserneuerung wird grundsätzlich durch den nutzenden Fachbereich oder den Teilnehmer beantragt.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Der Ablauf der Zertifikatserneuerung entspricht den Regelungen für Erstanträge unter Abschnitt
4.3, für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.3.1.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die Regelungen gemäß Abschnitt 4.3.2.

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Es gelten die Regelungen gemäß Abschnitt 4.4.1.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA

Es gelten die Regelungen gemäß Abschnitt 4.4.2.

4.6.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Erneuerung des Zertifikats

Entfällt.

4.7 Zertifikatserneuerung mit Schlüsselwechsel

Bei einer Zertifikatserneuerung mit Schlüsselwechsel wird ein neues Zertifikat für ein neues Schlüsselpaar ausgestellt, sofern die im bereits bestehenden Zertifikat enthaltenen Informationen
unverändert bleiben. Es wird analog zu Abschnitt 4.6 vorgegangen.

4.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Eine Zertifikatserneuerung kann beantragt werden, wenn die Gültigkeit eines Zertifikats abläuft.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Eine Zertifikatserneuerung wird grundsätzlich durch den nutzenden Fachbereich oder den Teilnehmer beantragt.

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Der Ablauf der Zertifikatserneuerung mit Generierung von neuen Schlüsseln entspricht den Regelungen für Erstanträge unter Abschnitt 4.3, für die Identifizierung und Authentifizierung gelten die Regelungen gemäß Abschnitt 3.3.1.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Es gelten die Regelungen gemäß Abschnitt 4.3.2.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Es gelten die Regelungen gemäß Abschnitt 4.4.1.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Eine Veröffentlichung der Zertifikate in Verzeichnisdiensten seitens der CA findet nicht statt.

4.7.7 Benachrichtigung anderer Zertifikatsinfrastruktur-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Entfällt

4.8 Zertifikatsänderung

Eine Zertifikatsänderung kann notwendig werden, wenn sich Attribute des Zertifikates ändern. Dies könnte die KeyUsage oder Zertifikatserweiterungen sein.

4.8.1 Bedingungen für eine Zertifikatsänderung

Es muss sichergestellt sein, dass ein zu änderndes Zertifikat noch über eine ausreichend lange Gültigkeitsdauer verfügt.

Sobald ein neues geändertes Zertifikat von der CA ausgegeben wurde, wird automatisch und unmittelbar das alte Zertifikat zurückgezogen.

4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Eine Zertifikatsänderung wird grundsätzlich durch den Teilnehmer beantragt.

4.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Der Ablauf bei der Zertifikatsänderung entspricht den Regelungen für Erstanträge unter Abschnitt 4.3.

4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Es gelten die Regelungen gemäß Abschnitt 4.3.2.

4.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Es gelten die Regelungen gemäß Abschnitt 4.4.1.

4.8.6 Veröffentlichung der Zertifikatsänderung durch die CA

Eine Veröffentlichung der Zertifikate in Verzeichnisdiensten seitens der CA findet nicht statt.

4.8.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines neuen Zertifikats

Entfällt

4.9 Sperrung und Suspendierung von Zertifikaten

Kontaktinformationen für Sperranträge werden Online unter den Adressen ca-rsa.techem.de und ca-ecc.techem.de Informationen veröffentlicht. Innerhalb der üblichen Geschäftszeiten, nach Eingang, wird mit der Behandlung der Meldung begonnen.

Notfälle, bei denen Zertifikate aus der Techem PKI missbräuchlich oder betrügerisch verwendet werden, können gemäß 4.9.3. gesperrt werden.

Bereits abgelaufene Zertifikate können nicht gesperrt werden.

Die Sperrung eines Zertifikats kann nicht rückgängig gemacht werden.

4.9.1 Bedingungen für eine Sperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe vorliegt:

- Das Zertifikat enthält Angaben, die nicht gültig sind.
- Der private Schlüssel wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert
  1. bzw. missbraucht.
- Der Zertifikatsinhaber ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Das Zertifikat verletzt Warenzeichen o. ä. nach Abschnitt 3.1.6
- Die Nutzung des Zertifikats verstößt gegen die CP.
- Die ausstellende CA stellt den Zertifizierungsbetrieb ein.
- Der Zertifikatsinhaber bzw. Teilnehmer stellt einen Sperrantrag.

4.9.2 Wer kann eine Sperrung beantragen?

Zertifikatsinhaber bzw. Teilnehmer können einen Sperrantrag ohne Angabe von Gründen stellen.
Dritte können einen Sperrantrag stellen, wenn sie Hinweise vorlegen, dass einer der unter Abschnitt 4.9.1 genannten Gründe für eine Sperrung vorliegt.

4.9.3 Verfahren für einen Sperrantrag

Stellen Zertifikatsinhaber bzw. Teilnehmer einen Sperrantrag, so müssen sie sich gegenüber der ausstellenden CA authentifizieren. Die möglichen Verfahren sind in Abschnitt 3.4 dargestellt.
Nach erfolgreicher Authentifizierung führt die ausstellende CA die Sperrung durch.
Stellt ein Dritter einen Sperrantrag, so führt die ausstellende CA eine Prüfung der angegebenen
Gründe durch. Liegt einer der in 4.9.1 genannten Gründe vor, führt sie die Sperrung durch.
Nach erfolgter Sperrung werden Teilnehmer und ggf. Zertifikatsinhaber darüber elektronisch informiert. Die Sperrinformation wird mindestens bis zum Ablaufdatum des gesperrten Zertifikats über die Sperrdienste verfügbar gemacht.

4.9.4 Fristen für einen Sperrantrag

Wenn Gründe (siehe Abschnitt 4.9.1) für eine Sperrung vorliegen, muss unverzüglich ein Sperrantrag gestellt werden.

4.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die Techem CA

Eine CA muss eine Zertifikatssperrung unverzüglich vornehmen, wenn die Voraussetzungen dafür gegeben sind (siehe Abschnitt 4.9.3).

4.9.6 Nutzung der verfügbaren Methoden zum Prüfen von Sperrinformationen

Die gesamte Zertifikatskette muss auf Sperrung der einzelnen Zertifikate überprüft werden. Gemäß Abschnitt 4.9.9 ist eine Prüfung von Sperrinformation durch die Techem CA jederzeit gewährleistet.

4.9.7 Frequenz der Veröffentlichung von Sperrlisten

CAs, die nicht ausschließlich CA-Zertifikate ausstellen, müssen mindestens alle 10 Tage eine neue CRL erstellen und veröffentlichen. Andere CAs müssen mindestens alle 90 Tage eine CRL erstellen und veröffentlichen. Wird ein Zertifikat gesperrt, so muss die sperrende CA umgehend eine neue CRL erstellen und veröffentlichen.

4.9.8 Maximale Latenzzeit für Sperrlisten

Nach Erzeugung neuer CRLs müssen diese umgehend, spätestens jedoch nach 24 Stunden, veröffentlicht werden.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

CAs können OCSP als Online-Sperr- und -Statusüberprüfungsverfahren anbieten (siehe Abschnitt 4.10).
Das Bereitstellen einer CRL ist hingegen für alle CAs verpflichtend.
Sperrinformationen werden ständig (24 Stunden am Tag, 7 Tage die Woche) bereitgestellt. Es wird sichergestellt, dass ungeplante Ausfallzeiten und Wartungen minimiert und der Betrieb schnellstmöglich wiederhergestellt werden.

4.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Es gelten die Anforderungen zum Schutz des privaten Schlüssels gemäß Abschnitt 6.2.
Die Korrektheit der durch die CA bereitgestellten Sperr- bzw. Statusinformationen über Zertifikate wird durch die allgemeinen Sicherheitsmechanismen der Techem RootCA (siehe Kapitel
5 und 6) sichergestellt. Auf dem Transportweg sind die Sperr- bzw. Statusinformationen durch elektronische Signaturen gegen Manipulation geschützt (siehe Abschnitte 7.2 und 7.3).

Einträge zu gesperrten Zertifikaten werden nicht vor Ablauf des betroffenen Zertifikats aus der CRL oder dem OCSP-Dienst entfernt.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine Angaben.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Bei einer Kompromittierung des privaten Schlüssels ist das entsprechende Zertifikat unverzüglich
zu sperren. Bei einer Kompromittierung des privaten Schlüssels einer CA werden
alle von ihr ausgestellten Zertifikate gesperrt.

4.9.13 Bedingungen für eine Suspendierung

Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten ist nicht erlaubt.

4.9.14 Wer kann eine Suspendierung beantragen?

Entfällt.

4.9.15 Verfahren für Anträge auf Suspendierung

Entfällt.

4.9.16 Begrenzungen für die Dauer von Suspendierungen

Entfällt.

4.10 Statusabfragedienst für Zertifikate

Für alle von der Techem PKI ausgestellten Zertifikate ist eine Prüfung auf den Sperr-Status des Zertifikates gegeben.

Die Pflicht zur Bereitstellung von CRLs ist in Kapitel 2 geregelt.

4.10.1 Funktionsweise des Statusabfragedienstes

Zertifikate, für die ein Online-Sperr- und -Statusüberprüfungsverfahren (OCSP) angeboten wird, beinhalten einen Verweis auf diesen Dienst.
Der OCSP-Dienst gibt für nicht ausgestellte Zertifikate eine negative Auskunft.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Statusabfragedienste werden ständig (24 Stunden am Tag, 7 Tage die Woche) bereitgestellt.

Es wird sichergestellt, dass ungeplante Ausfallzeiten und Wartungen minimiert und der Betrieb schnellstmöglich wiederhergestellt werden.

4.10.3 Optionale Leistungen

OCSP steht nicht zwingend für alle von der Techem PKI ausgestellten Zertifikate zur Verfügung und ist somit eine optionale Leistung.

4.11 Kündigung durch den Zertifikatsnehmer

Eine Beendigung der Zertifikatnutzung erfolgt entweder durch eine Sperrung oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Die CAs in der Techem PKI bieten keine Schlüsselhinterlegung und -Wiederherstellung für Teilnehmer
oder Zertifikatsinhaber an.

Teilnehmer, die eine interne Schlüsselhinterlegung einsetzen, müssen die Sicherheitsvorgaben für derartige Verfahren der Techem Energy Services GmbH einhalten.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Entfällt.

5 Physische, organisatorische und personelle Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI.

Die Sicherheitsmaßnahmen sind grundsätzlich an die Maßnahmenkataloge des IT-Grundschutzhandbuchs angelehnt.

Die Infrastruktur, auf der die Techem PKI betrieben wird, wird in redundanten Rechenzentren von einem IT-Infrastruktur Provider zur Verfügung gestellt.

5.1 Physische Sicherheitsmaßnahmen

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und erfüllt alle technischen und organisatorischen Standards für einen sicheren Rechenzentrumsbetrieb.

5.1.1 Lage und Gebäude

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und erfüllt alle Voraussetzungen der baulichen Anforderungen an für den Betreib von Rechenzentren.

5.1.2 Zugang

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und hat den erforderlichen Zugangsschutz umgesetzt.

5.1.3 Strom, Heizung und Klimaanlage

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und gewährleistet alle diesbezüglichen Anforderungen.

5.1.4 Gefährdung durch Wasser

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und verfügt über entsprechende Schutzmaßnahmen vor Wasser.

5.1.5 Brandschutz

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und verfügt über Brandschutzvorrichtungen.

5.1.6 Aufbewahrung von Datenträgern

Datenträger werden von dem ISO 27001 zertifizierten IT-Infrastruktur Provider den Sicherheitsanforderungen entsprechend aufbewahrt.

5.1.7 Datenvernichtung

Datenträger und Daten werden von dem ISO 27001 zertifizierten IT-Infrastruktur Provider den Vorgaben entsprechend vernichtet.

5.1.8 Desaster Backup

Der IT-Infrastruktur Provider ist ISO 27001 zertifiziert und hat ein Desaster Recovery Konzept etabliert.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Der Betrieb der Techem PKI findet gemäß eines Rollenkonzeptes statt, bei dem alle notwendigen Rollen des Betriebteams definiert sind und das gemäß dem Rollentrennungskonzept aufgebaut ist.
Bei sicherheitsrelevanten Tätigkeiten kommt immer das 4-Augen-Prinzip zur Anwendung.

5.2.2 Mehraugenprinzip

Sicherheitsrelevante Tätigkeiten bei dem Betreib der Techem PKI werden durch Rollen abgedeckt, bei denen das Vier-Augen-Prinzip realisiert ist.

Alle anderen Tätigkeiten können von einer Person durchgeführt werden.

Es wird sichergestellt, dass jede Rolle mit ausreichend vielen Mitarbeitern besetzt ist, um einen kontinuierlichen Betrieb zu gewährleisten.

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Die Identifizierung und Authentifizierung der Rollen muss auf Grundlage des in Abschnitt 5.2.1 und Abschnitt 5.2.2 beschriebenen Rollenmodells erfolgen.
Der technische Zugang zu den IT-Systemen wird durch Nutzerkennung und Passwort oder ein stärkeres Verfahren realisiert. Es sind die geltenden Passwort-Richtlinien der Techem GmbH einzuhalten.
Der physikalische Zugang zu den IT-Systemen muss durch Zutrittskontrollmaßnahmen reglementiert werden.

5.2.4 Rollentrennung

Es muß durch Rollentrennung und das Vier-Augen-Prinzip gewährleistet sein, dass eine Person alleine kein Schaden anrichten oder den Betrieb der Techem PKI stören kann.

So sollten technische Administratoren nicht gleichzeitig über eine Rolle im PKI Betreib verfügen.

5.3 Personelle Sicherheitsmaßnahme

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Es kommen beim Betrieb der Techem PKI nur Mitarbeiter zum Einsatz, die über die benötigte Befähigung verfügen.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Entfällt.

5.3.3 Anforderungen an Schulungen

Alle Mitarbeiter, die beim Betrieb der Techem PKI zum Einsatz kommen werden, vorher an der CA-Software geschult. Darüber hinaus werden bei neuen Versionen der CA-Software die neuen Feature ebenfalls durch Schulungen den Mitarbeitern bekannt gemacht.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Schulungen werden nach Bedarf angesetzt.

5.3.5 Häufigkeit und Folge von Job-Rotation

Entfällt.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Bei unerlaubten Handlungen an der Techem CA durch bestimmte Mitarbeiter werden diese aus dem PKI Betriebsteam entfernt und eventuell disziplinarische Maßnahmen ergriffen.

5.3.7 Anforderungen an freie Mitarbeiter

Es gelten an freie Mitarbeiter dieselben Anforderungen wie an interne Mitarbeiter.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen

Alle zur Einhaltung der Sicherheitsmaßnahmen und des Betreib nötigen Dokumente werden dem PKI Betriebsteam der Techem zur Verfügung gestellt.

5.4 Überwachungsmaßnahmen

Es kommen die Maßnahmen der Techem Energy Services GmbH zum Einsatz, die für den Betrieb von SW-Komponenten gelten.

5.4.1 Arten von aufgezeichneten Ereignissen

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.2 Häufigkeit der Analyse von Aufzeichnungen

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.3 Aufbewahrungszeit von Aufzeichnungen

Es gelten die allgemeinen Anforderungen der Techem Energy Services GmbH.

5.4.4 Schutz der Aufzeichnungen

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.5 Datensicherung der Aufzeichnungen

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.6 Speicherung der Aufzeichnungen (intern / extern)

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.4.8 Schwachstellenanalyse

Es gelten die Richtlinien der Techem Energy Services GmbH.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Die gesetzlichen Pflichten zur Archivierung von Aufzeichnungen werden erfüllt.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Es gelten die gesetzlichen Regelungen für Aufbewahrungsfristen.

5.5.3 Schutz des Archivs

Archivierte Aufzeichnungen werden gemäß den gesetzlichen Vorgaben geschützt.

5.5.4 Datensicherung des Archivs

Es gelten die gesetzlichen Regelungen zur Datensicherung.

5.5.5 Anforderungen an Zeitstempel

Entfällt.

5.5.6 Archivierung (intern / extern)

Es gelten die internen Regelungen der Techem Energy Services GmbH.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Es gelten die internen Regelungen der Techem Energy Services GmbH.

5.6 Schlüsselwechsel der CA

Die Gültigkeitsdauer von Schlüsseln ist in Abschnitt 6.3.2 festgelegt. Falls der Schlüssel einer CA kompromittiert wurde, gelten die in Abschnitt 5.7 aufgeführten Regelungen. Nach Erzeugung eines neuen CA-Schlüssels muss dieser gemäß Kapitel 2 veröffentlicht werden.

5.7 Kompromittierung und Geschäftswiederherstellung

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Die Prozeduren zur Behandlung von Sicherheitsvorfällen und bei der Kompromittierung von privaten Schlüsseln einer CA müssen schriftlich dokumentiert und an alle Mitarbeiter ausgehändigt werden. Die Grundzüge der Prozeduren sind in den folgenden Unterkapiteln aufgeführt.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Werden innerhalb einer CA fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der CA haben, muss der Betrieb des entsprechenden
IT-Systems unverzüglich eingestellt werden.
Das IT-System muss auf einer Ersatz-Hardware unter Wiederherstellung der Software und der Daten aus der Datensicherung neu aufgesetzt, überprüft und in einem sicheren Zustand in Betrieb genommen werden. Anschließend muss das fehlerhafte oder modifizierte IT-System
analysiert werden. Bei Verdacht einer vorsätzlichen Handlung müssen gegebenenfalls rechtliche Schritte eingeleitet werden. Darüber hinaus müssen eine Bewertung der Sicherheit und eine Revision zur Aufdeckung von Schwachstellen erfolgen.
Gegebenenfalls müssen zusätzliche Abwehrmaßnahmen zur Vermeidung ähnlicher Vorfälle ergriffen werden. Die Mitarbeiter der Techem PKI arbeiten in diesen Fällen mit den Experten des Computer-
Notfallteams in der Techem Energy Services GmbH zusammen.

5.7.3 Verhalten bei Kompromittierung des privaten Schlüssels der CA

Wurde ein privater Schlüssel kompromittiert, so muss das dazugehörige Zertifikat gesperrt werden (siehe Abschnitt 4.9.1).

Wurde der private Schlüssel einer CA kompromittiert, so müssen das Zertifikat der CA und alle damit ausgestellten Zertifikate gesperrt werden. Außerdem müssen alle betroffenen Teilnehmer bzw. Zertifikatsinhaber informiert werden.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einem Katastrophenfall

Eine Wiederaufnahme des Zertifizierungsbetriebs nach einer Katastrophe muss Bestandteil der Notfallplanung sein und innerhalb kurzer Zeit erfolgen können, sofern die Sicherheit der Zertifizierungsdienstleistung gegeben ist.
Die Bewertung der Sicherheitslage obliegt dem Sicherheitsbeauftragten.

5.8 Schließung einer CA oder einer Registrierungsstelle

Wird der Betrieb einer CA eingestellt, müssen folgende Maßnahmen ergriffen werden:

- Information des Teilnehmers bzw. der Zertifikatsinhaber sowie der Zertifikatprüfer
- Sperrung aller von der CA ausgestellten Zertifikate, somit auch aller Zertifikate von Teilnehmerservice-Mitarbeitern
- sichere Zerstörung der privaten Schlüssel der CA
- Widerrufung aller an Auftragnehmer vergebenen Autorisierungen, im Namen der CA zu handeln

Die Techem PKI muss den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen
Sperrliste für den zugesicherten Aufbewahrungszeitraum (siehe Abschnitt 5.4.3) sicherstellen.

6 Technische Sicherheitsmaßnahmen

Die Gewährleistung geeigneter technischer Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI.
Detaillierte Informationen sind in einem Sicherheitskonzept festgeschrieben. Im Folgenden werden die Maßnahmen für die technische Sicherheit beschrieben.

Sofern dabei einzelne Sicherheitsmaßnahmen nicht spezifiziert werden, sind diese grundsätzlich an die Maßnahmenkataloge des IT-Grundschutzhandbuchs angelehnt.

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Die Schlüsselpaare aller CAs müssen in einer gesicherten Umgebung, die den Anforderungen aus Abschnitt 6.2.1 genügt, im Vier-Augen-Prinzip, erzeugt werden (siehe Abschnitt 5.2.2). Die Anzahl der hierzu autorisierten Mitarbeiter wird auf das betrieblich notwendige Maß beschränkt.

Für End-Entity Zertifikate können, je nach Verwendungszweck und unter Einhaltung geeigneter kryptographischer Maßnahmen, folgende Methoden zum Einsatz kommen:

- Das Schlüsselpaar wird zentral von der PKI erstellt und dem Konsumenten zur Verfügung gestellt
- Das Schlüsselpaar wird von der konsumierenden Instanz selbst erstellt und der Public Key mittels eines Certifcate Signing Requests (CSR) der PKI zum Ausstellen eines Zertifikates zur Verfügung gestellt

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Von der CA erstellte Private Keys werden kryptographisch geschützt dem Zertifikatsnehmer zur Verfügung gestellt.

Bei maschineller Verarbeitung des Schlüsselmaterials kann dies in einem speziellen sicheren Format erfolgen, das von der Techem PKI zugelassen ist.
Bei manueller Verarbeitung des Schlüsselmaterials sollen existierende Standardformate wie PKCS#12 genutzt werden.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Der Certificate Signing Request (CSR) des Teilnehmers wird per E-Mail, HTTPS oder auf einem Datenträger an die CA übermittelt. Die Zugehörigkeit des CSR zu einem bestimmten Zertifikatantrag wird durch Unterschrift oder elektronische Signatur bestätigt.

6.1.4 Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer

Die öffentlichen Schlüssel aller CAs der Techem PKI können über einen Informationsdienst gemäß Kapitel 2 abgerufen werden.

6.1.5 Schlüssellängen

Andere Algorithmen als die Aufgeführten werden nicht unterstützt.

6.1.5.1 Schlüssellängen RSA-PKI

Für den RSA-Algorithmus müssen alle von der Techem RSA-PKI ausgestellten Zertifikate eine Schlüssellänge von mindestens 2048 Bit haben. Andere Schlüssellängen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

Die verwendeten Schlüssel für die RootCA und die SubCAs müssen eine Mindestlänge von 4096 Bit haben. Andere Schlüssellängen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

6.1.5.2 Schlüssellängen ECC-PKI

Für den ECC-Algorithmus, es gelten die Kurvenparameter gemäß NIST-256, müssen alle von der Techem ECC-PKI ausgestellten Zertifikate eine Schlüssellänge von mindestens 256 Bit haben. Andere Schlüssellängen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

Die verwendeten Schlüssel für die RootCA und die SubCAs müssen eine Mindestlänge von 256 Bit haben. Andere Schlüssellängen dürfen verwendet werden, wenn ihre Sicherheit mindestens äquivalent ist.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

CA-Schlüssel dürfen nicht über den aufgrund der Algorithmen erlaubten Gültigkeitszeitraum hinaus verwendet werden.

6.1.6.1 Parameter RSA-PKI

Als kryptographische Algorithmen sind in der RSA-PKI RSA mit SHA256 gültig.

6.1.6.2 Parameter ECC-PKI

Als kryptographische Algorithmen sind in der ECC-PKI ECC mit Kurvenparametern gemäß NIST-256 mit SHA256 gültig.

6.1.7 Schlüsselverwendungen

Die privaten Schlüssel der CAs dürfen ausschließlich für die Ausstellung von Zertifikaten und für die Signatur von Sperrinformationen verwendet werden.

6.2 Schutz des privaten Schlüssels und Anforderungen an kryptographische Module

Der private Schlüssel jeder CA muss durch geeignete technische und organisatorische Maßnahmen geschützt werden.

Schlüsselmaterial muss manipulationssicher transportiert und gelagert werden.

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Wenn kryptographische Module zum Einsatz kommen, müssen sie gemäß 6.2 gesichert sein.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Der Zugriff auf den privaten Schlüssel der RootCAs muss gemäß Abschnitt 6.2.8 immer im Vier-Augen-Prinzip (2 aus 2) gemeinsam stattfinden.

6.2.3 Hinterlegung privater Schlüssel

Hinterlegung privater Schlüssel einer CA im Sinne eines Key Escrow findet nicht statt.

6.2.4 Backup privater Schlüssel

Backup privater Schlüssel einer CA in verschlüsselter Form, an einem sicheren, nur nach Autorisierung zugänglichen Ort ist zum Zweck des Notfall Recovery zulässig.

Hierzu dienen Prozesse, die den besonderen Sicherheitsanforderungen angepasst sind.

6.2.5 Archivierung privater Schlüssel

Für die Archivierung privater Schlüssel gelten die Regelungen aus Abschnitt 6.2.4.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Entfällt.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Entfällt.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten Schlüssels einer CA geschieht durch entsperren mittels PIN. Für die PIN gelten die Regelungen gemäß 6.4.1.

6.2.9 Deaktivierung privater Schlüssel

Die Deaktivierung der privaten Schlüssel einer RootCA muss automatisch nach Beendigung des
Zertifizierungsprozesses erfolgen.

Dies gilt ebenfalls für aktive SubCAs, nach Beendigung des Zertifizierungsprozesses muss eine Deaktivierung der privaten Schlüssel erfolgen.
Hiervon ausgenommen sind aktive SubCAs, die durch eine maschinelle Schnittstelle angesprochen werden und hochverfügbar sein müssen. Sofern entsprechende Sicherheitsmaßnahmen zum unbefugten Zugriff auf die CA getroffen wurden und diese in einer geschützten Umgebung betrieben wird, dürfen die privaten Schlüssel dieser CA innerhalb der geschützten Umgebung der CA persistiert werden.

6.2.10 Zerstörung privater Schlüssel

Vor Außerdienststellung eine Computers mit Schlüsselmaterial müssen alle darauf gespeicherten privaten Schlüssel vernichtet werden. Alle Kopien des privaten Schlüssels einer CA müssen mit Beendigung ihres Lebenszyklus vernichtet werden.
Bei der Vernichtung der privaten Schlüssel einer CA muss nach dem Vier-Augen-Prinzip verfahren werden.

6.2.11 Beurteilung kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Siehe Abschnitt 5.5.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die in der Techem PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Zertifikate für die Root CA: 15 Jahre
- Zertifikate für Sub CAs: 7,5 Jahre
- End-Entity Zertifikate für Systeme oder Nutzer: maximal 2,5 Jahre
- Zertifikate können nicht länger gültig sein als das ausstellende CA-Zertifikat.

Für die Nutzungsdauer von Schlüsselpaaren gelten die Regelungen aus Abschnitt 6.1.6. Bevor der Schlüssel einer CA ungültig wird, wird rechtzeitig ein neues Schlüsselpaar erzeugt und an den notwendigen Stellen bekannt gegeben.

6.4 Aktivierungsdaten

6.4.1 Vergabe von Aktivierungsdaten

Die PIN für die CA-Schlüssel besteht aus numerischen Zeichen mit einer Länge von mindestens 16 Stellen und muß konform mit der Techem Passwort-Richtlinie gewählt werden.

6.4.2 Schutz von Aktivierungsdaten

Aktivierungsdaten müssen geheim gehalten werden und dürfen nur den Mitarbeitern bekannt
sein, die diese nach Abschnitt 5.2.1 für die Durchführung einer spezifischen Funktion benötigen.

6.4.3 Andere Aspekte

Entfällt.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Alle CAs dürfen ausschließlich auf Basis von gehärteten Betriebssystemen betrieben werden. Darüber hinaus müssen Zugriffskontrolle und Nutzerauthentifizierung als Sicherheitsmaßnahmen
umgesetzt werden.

6.5.2 Beurteilung von Computersicherheit

Die in Abschnitt 6.5.1 genannten Sicherheitsmaßnahmen müssen dem aktuellen Stand der

Technik entsprechen.

6.6 Technische Maßnahmen während des Lebenszyklus

Während des gesamten Lebenszyklus ist durch den IT-Provider und den CA-Software Hersteller gewährleistet, dass gefundene technische Sicherheitsschwachstellen behoben werden.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Die Sicherheit der Software ist durch geeignete Qualitätssicherungsmaßnahmen seitens des IT-Providers und des CA-Software Herstellers gewährleistet.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Die Sicherheit des Betriebs wird durch den Einsatz geeigneter Monitoring und Auditmaßnahmen gewährleistet.

6.6.3 Sicherheitsmaßnahmen während des Lebenszyklus

Die unter 6.6.1 und 6.6.2 aufgeführten Maßnahmen werden über die gesamten Lebenszyklus der Techem PKI aufrecht erhalten.

6.7 Sicherheitsmaßnahmen für Netze

Die Netze werden von einem ISO 27001 zertifizierten IT-Provider gemanagte und verfügen über die erforderlichen Kontroll- und Schutzmechanismen.

6.8 Zeitstempel

Entfällt.

7 Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Jedem Zertifikat muss durch die ausstellende CA eine eindeutige Seriennummer zugeordnet werden.

7.1.1 Versionsnummern

Zertifikate werden nach X.509 Version 3 ausgestellt.

Alle Zertifikate enthalten folgende Inhalte:

- Identifizierung der ausstellenden CA, der Organisation und des Landes, in dem sie angesiedelt ist
- Der Name des Zertifikatsinhabers oder eine IP Adresse/Host Name oder die Geräte ID
- Der öffentliche Schlüssel, der mit dem privaten Schlüssel unter der Kontrolle des Zertifikatsinhabers korrespondiert
- Das Anfangs- und Enddatum der Gültigkeitsperiode des Zertifikats
- Die Seriennummer des Zertifikats
- Die elektronische Signatur der ausstellenden CA
- ggf. Einschränkungen der Einsatzmöglichkeiten des Zertifikats

7.1.2 Zertifikatserweiterungen

Grundsätzlich sind alle Zertifikatserweiterungen nach X.509 oder herstellerspezifische Erweiterungen zulässig.

Zertifikate für CAs
In Zertifikaten für CAs müssen die Erweiterung keyUsage mit den Werten „keyCertSign“ und „cRLSign“ sowie die Erweiterung basicConstraints mit dem Wert „cA=True“ aufgenommen werden.

Des weiteren beinhalten Zertifikate für SubCAs eine Erweiterung cRLDistributionPoint mit einem Verweis auf die zugehörige Sperrliste und eine Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat und den zugehörigen OCSPDienst.

End-Entity-Zertifikate
Zertifikate für alle anderen Verwendungszwecke werden optional mit der Erweiterung basicConstraints mit dem Wert „CA=False“ als Nicht-CA-Zertifikat markiert und tragen keine CA-spezifische keyUsage-Erweiterung, d. h. die Erweiterung keyUsage darf nicht die Werte „keyCertSign“ oder „cRLSign“ beinhalten.

End-Entity-Zertifikate enthalten immer die Erweiterung cRLDistributionPoint mit einem Verweis auf die zugehörige Sperrliste und die Erweiterung authorityInfoAccess mit einem Verweis auf das signierende CA-Zertifikat.

Optional können Zertifikate für Datenverarbeitungssysteme sowie Zertifikate für natürliche Personen und Gruppen zusätzlich die Erweiterung authorityInfoAccess mit einem Verweis auf den zugehörigen OCSP-Dienst enthalten.

7.1.3 Algorithmen OIDs

Objekt Identifikatoren für Algorithmen werden nach PKIX verwendet.

7.1.4 Namensformate

Siehe Abschnitt 3.1.
Domainnamen und IP-Adressen, die im Subject-DN enthalten sind, werden immer auch in den alternativen Zertifikatnamen („subjectAlternativeName“) unter den Typen „dNSName“ bzw. „iPAddress“ aufgeführt.

7.1.5 Namensbeschränkungen

Siehe Abschnitt 3.1.

7.1.6 OIDs der Zertifikatsrichtlinien

In jedem von der Techem PKI Sicherheitsniveau Produktion ausgestelltem Zertifikat werden folgende OIDs nach Abschnitt 1.2 referenziert:.

7.1.6.1 RSA-PKI OIDs

- 1.3.6.1.4.1.14721.100.0.1 : Techem RSA-PKI Sicherheitsniveau Produktion
- 1.3.6.1.4.1.14721.100.0.1.1 : Generationen-Identifikation der PKI, aktuell erste Generation
- 1.3.6.1.4.1.14721.100.0.1.1.1 : Version, aktuell Version eins der zugrundeliegenden CP
- 1.3.6.1.4.1.14721.100.0.1.1.1.21 : Ausstellungs-Richtlinie für die Zertifikatsnutzung, als Zertifikatsidentifier.
- Identifiziert End Entity und SubCA Zertifikate, der RSA SubCA 01
- 1.3.6.1.4.1.14721.100.0.1.1.1.22 : Ausstellungs-Richtlinie für die Zertifikatsnutzung, als Zertifikatsidentifier. Identifiziert End Entity und SubCA Zertifikate, der RSA SubCA 02
- 1.3.6.1.4.1.14721.100.0.1.1.1.10 : diese CP

7.1.6.2 ECC-PKI OIDs

- 1.3.6.1.4.1.14721.100.0.2 : Techem ECC-PKI Sicherheitsniveau Produktion
- 1.3.6.1.4.1.14721.100.0.2.1 : Generationen-Identifikation der PKI, aktuell erste Generation
- 1.3.6.1.4.1.14721.100.0.2.1.1 : Version, aktuell Version eins der zugrundeliegenden CP
- 1.3.6.1.4.1.14721.100.0.2.1.1.20 : Ausstellungs-Richtlinie, als Zertifikatsidentifier
- 1.3.6.1.4.1.14721.100.0.2.1.1.10 : diese CP

7.1.7 Nutzung der Erweiterung "Policy Constraints"

Keine.

7.1.8 Syntax und Semantik von "Policy Qualifiers"

Siehe Abschnitt 1.2.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung Zertifikats-richtlinie

Keine.

7.2 Sperrlistenprofile

Für jede CA in der Techem PKI wird eine CRL bereitgestellt. Diese enthält die gesperrten Zertifikate
der jeweiligen CA. Jede CRL enthält folgende Informationen:

- Versionsnummer (siehe Abschnitt 7.2.1)
- Signaturalgorithmus
- Identifizierung der ausstellenden CA
- Zeitpunkt der Ausstellung
- Spätester Zeitpunkt des nächsten Updates (bei Sperrung eines Zertifikats wird sofort eine neue CRL generiert)
- Seriennummern und Sperrungsdaten der gesperrten Zertifikate
- Die elektronische Signatur der ausstellenden CA

7.2.1 Versionsnummern

Sperrlisten müssen X.509 Version 2 konform erstellt werden.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Keine.

7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP-Dienst wird konform zu RFC6960 betrieben.

OCSP-Antworten werden mit einem Zertifikat signiert, das von der CA des zu prüfenden Zertifikats ausgestellt wurde.

7.3.1 Versionsnummern

OCSP wird in Version 1 unterstützt.

7.3.2 OCSP Erweiterungen

Keine.

8 Überprüfungen der CA und andere Bewertungen

Die Abläufe für alle CAs der Techem PKI sind so gestaltet, dass sie diesem CP entsprechen.

Sie werden in regelmäßigen Abständen angepasst um dem jeweiligen Stand der Technik zu entsprechen.

8.1 Häufigkeit und Bedingungen für Überprüfungen

Eine externe Zertifizierung für die Techem PKI ist aktuell nicht vorgesehen.

8.2 Identität/Qualifikation des Prüfers

Entfällt.

8.3 Stellung des Prüfers zum Bewertungsgegenstand

Entfällt.

8.4 Durch Überprüfungen abgedeckte Themen

Entfällt.

8.5 Reaktionen auf Unzulänglichkeiten

Bekanntgewordene Sicherheitsprobleme werden von der Techem PKI beseitigt.

8.6 Information über Bewertungsergebnisse

Entfällt.

9 Andere finanzielle und rechtliche Angelegenheiten

9.1 Gebühren

Entfällt.

9.2 Finanzielle Zuständigkeiten

Entfällt.

9.3 Vertraulichkeitsgrad von Geschäftsdaten

9.3.1 Definition von vertraulichen Informationen

Alle Informationen über Teilnehmer der Techem PKI bzw. Zertifikatsinhaber, die nicht unter Abschnitt 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.
Zertifikatsinhaber haben das Recht, Einsicht in die Daten zu erhalten, die bei der Ausstellung ihrer Zertifikate archiviert wurden.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen, die in den veröffentlichten Zertifikaten und Sperrlisten explizit (z. B. E-Mail-Adresse) oder implizit (z. B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Die Techem PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.
Daten dürfen im Rahmen der Diensterbringung nur weitergegeben werden, wenn
zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten
Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

9.4 Schutz personenbezogener Daten

9.4.1 Datenschutzkonzept

Die Techem PKI muss zur Leistungserbringung personenbezogene Daten elektronisch speichern
und verarbeiten. Dies geschieht in Übereinstimmung mit der DSVGO dem BDSG.

9.4.2 Als persönlich behandelte Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

9.4.3 Daten, die nicht als persönlich behandelt werden

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

9.4.4 Zuständigkeiten für den Datenschutz

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.3 analog.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Die Techem PKI nutzt personenbezogene Daten, soweit dies zur Leistungserbringung erforderlich
ist.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Die Techem Energy Services GmbH unterliegt dem Recht der Bundesrepublik Deutschland und muss vertrauliche
und personenbezogene Informationen bei Vorliegen entsprechender gesetzlicher Auskunftspflichten
oder bei gerichtlicher Anordnung freigeben.

9.4.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Geistiges Eigentumsrecht

Die Techem Energy Services GmbH ist Urheber dieser CP. Die genannten Dokumente können unverändert an Dritte weitergegeben werden. Weitergehende Rechte werden nicht eingeräumt.

Insbesondere ist die Weitergabe veränderter Fassungen der CP der Techem PKI,
die Überführung in maschinenlesbare oder andere veränderbare Formen der elektronischen Speicherung, auch auszugsweise, ohne Zustimmung der Techem Energy Services GmbH nicht zulässig.

9.6 Zusicherungen und Garantien

9.6.1 Zusicherungen und Garantien der CA

Die Techem PKI verpflichtet sich, alle im Rahmen dieser CP beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

Wenn weitere Auftragnehmer Aufgaben in der Techem PKI wahrnehmen, so wird durch geeignete
Verfahren und Prüfungen sichergestellt, dass die durchgeführten Aufgaben den sich
aus CP der Techem PKI ergebenden Anforderungen entsprechen.
Die Verantwortung für den Betrieb der CAs der Techem PKI verbleibt bei der Techem Energy Services GmbH.

Die Teile der Techem PKI, die die Ausstellung und Sperrung von Zertifikaten durchführen, verfügen über eine dokumentierte Struktur welche die unbefangene Durchführung der Tätigkeiten gewährleistet.

9.6.2 Zusicherungen und Garantien der RA

Die Techem PKI verpflichtet sich, alle in dieser CP beschriebenen Aufgaben nach bestem Wissen und Gewissen durchzuführen.

9.6.3 Zusicherungen und Garantien der Zertifikatsnehmer

Jeder Zertifikatsnehmer ist verpflichtet, die ihn betreffende Aspekte dieser CP einzuhalten.

9.6.4 Zusicherungen und Garantien der Zertifikatsnutzer

Es gelten die Bestimmungen aus Abschnitt 4.5.2.

9.6.5 Zusicherungen und Garantien anderer PKI-Teilnehmer

Sofern weitere Beteiligte alsDienstleister in den Zertifizierungsprozess eingebunden werden, ist die Techem PKI in der Verantwortung, den Dienstleister zur Einhaltung der CP der Techem PKI zu verpflichten.

9.7 Gewährleistungen

Gewährleistung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.8 Haftungsbeschränkungen

Haftungsbeschränkung wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.9 Schadensersatz

Schadensersatz wird in den Verträgen zwischen den beteiligten Parteien geregelt.

9.10 Inkrafttreten und Beendigung

9.10.1 Inkrafttreten

Die CP der Techem PKI tritt an dem in ihnen angegebenen Datum in Kraft.

Sie wird über den entsprechenden Informationsdienst (siehe Kapitel 2) veröffentlicht. Eine Änderung von CP der Techem PKI wird von der Techem Energy Services GmbH eine dem Umfang der Änderungenangemessene Zeit, mindestens jedoch zwei Wochen, vorab angekündigt.

Die Geschäftsführung der Techem Energy Services GmbH ist verantwortlich für die Implementierung undEinhaltung dieses CP der Techem PKI.

9.10.2 Beendigung

Dieses Dokument ist solange gültig, bis es durch eine neue Version ersetzt wird (siehe Abschnitt 9.10.1) oder der Betrieb der Techem PKI eingestellt wird.

9.10.3 Auswirkung der Beendigung und Weiterbestehen

Von einer Aufhebung der CP unberührt bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten.

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Andere als die in diesem CP festgelegten Benachrichtigungen bleiben der Techem PKI freigestellt.

9.12 Ergänzungen

Eine Änderung der CP kann nur durch die Geschäftsführung der Techem Energy Services GmbH erfolgen.

Werden Änderungen vorgenommen, die sicherheitsrelevante Aspekte betreffen oder die Abläufe seitens der Teilnehmer erforderlich machen, ist eine Änderung der OID der CP erforderlich (siehe Abschnitt 1.2).

9.12.1 Verfahren für Ergänzungen

Siehe Abschnitt 9.12.1.

9.12.2 Benachrichtigungsmechanismen und -fristen

Siehe Abschnitt 9.12.1.

9.12.3 Bedingungen für OID Änderungen

Für alle Belange die Techem OIDs betreffend ist die Abteilung IT-Architecture & Governance der Ansprechpartner.

9.13 Verfahren zur Schlichtung von Streitfällen

Grundsätzlich ist die in Abschnitt 1.5.2 genannte Stelle für die Konfliktbeilegung zuständig. Kann ein Konflikt von dieser Stelle nicht befriedet werden, kann die Geschäftsführung der Techem Energy Services GmbH angerufen werden.

9.14 Zugrunde liegendes Recht

Der Betrieb der Techem PKI unterliegt den Gesetzen der Bundesrepublik Deutschland.

9.15 Einhaltung geltenden Rechts

Abgesehen von Abschnitt 9.16.1 sind dies Belange der Rechtsabteilung der Techem Energy Services GmbH und werden hier nicht explizit behandelt.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitserklärung

Alle in diesem CP der Techem PKI enthaltenen Regelungen gelten zwischen der

Techem Energy Services GmbH und den Beteiligten. Die Ausgabe einer neuen Version ersetzt alle vorherigenVersionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abgrenzungen

Entfällt.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP der Techem PKI unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmungen gilt diejenige wirksame Bestimmung als vereinbart, welche dem Sinn und Zweck der unwirksamen Bestimmung weitgehend entspricht. Im Falle von Lücken gilt dasjenige als vereinbart, was nach Sinn und Zweck dieser CP vernünftigerweise vereinbart worden wäre, hätte man die Angelegenheit von vornherein bedacht.

9.16.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb einer innerhalb der Techem PKI operierenden CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand sind Sitz der Techem Energy Services GmbH.

9.16.5 Höhere Gewalt

Entfällt.

9.17 Andere Bestimmungen

Entfällt.