Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ... .

Inhalt

Seite

Nationales Vorwort ... 6

Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Normen ... 7

1 Anwendungsbereich und Zweck ... 8

2 Normative Verweisungen ... 8

3 Begriffe ... 9

4 Abkürzungen und Akronyme ... 12

5 Kryptografische Anwendungen für die praktische Umsetzung von Systemen der Energietechnik (informativ) ... 13

5.1 Kryptografie, kryptografische Schlüssel und Sicherheitsziele ... 13

5.2 Kryptografietypen ... 13

5.3 Verwendungsmöglichkeiten der Kryptografie ... 14

5.3.1 Ziele der Cybersicherheit ... 14

5.3.2 Vertraulichkeit ... 14

5.3.3 Datenintegrität ... 14

5.3.4 Authentifizierung ... 15

5.3.5 Unleugbarkeit ... 15

5.3.6 Bedarf nach Vertrauen zur Erreichung der Ziele ... 16

6 Konzepte zum Schlüsselmanagement und Verfahren beim Betrieb von Systemen der Energietechnik (informativ) ... 16

6.1 Sicherheitspolitik für das Schlüsselmanagementsystem ... 16

6.2 Entwurfsprinzipien des Schlüsselmanagements beim Betrieb von Systemen der Energietechnik ... 16

6.3 Gebrauch kryptografischer Schlüssel ... 17

6.4 Vertrauen bei der PKI-Kryptografie ... 17

6.4.1 Registrierungsstellen (RA) ... 17

6.4.2 Zertifizierungsstellen (CA) ... 17

6.4.3 Vertrauen durch X.509-Zertifikate ... 18

6.5 Vertrauen durch selbstsignierte Zertifikate ... 19

6.6 Zertifikat-White-Listing ... 19

6.7 Vertrauen durch vorher vereinbarte Schlüssel ... 20

6.8 Sitzungsschlüssel ... 20

6.9 Protokolle, die beim Vertrauensaufbau verwendet werden ... 20

6.9.1 Vertrauensanker-Verwaltungsprotokoll (TAMP) ... 20

6.9.2 Einfaches Zertifikatanmeldungsprotokoll (SCEP) ... 20

6.10 Gruppenschlüssel ... 21

6.10.1 Zweck von Gruppenschlüsseln ... 21

Seite

6.10.2 Gruppendomäne der Interpretation (GDOI) 21
6.10.3 IKEv2 22
6.10.4 GDOI symmetrische Schlüsselverteilung 22
6.10.5 GDOI-Schlüsselerneuerung (Pull-Verfahren) 22
6.10.6 GDOI-Schlüsselerneuerung (Push-Verfahren) 26
6.10.7 Alternativer GDOI-Schlüsselerneuerungsvorgang mit engerer Synchronisation der Schlüsselaktualisierung 26
6.11 Lebenszyklus des Schlüsselmanagements 27
6.11.1 Schlüsselmanagement im Lebenszyklus einer Einheit 27
6.11.2 Lebenszyklus des kryptografischen Schlüssels 28
6.12 Zertifikatmanagement-Vorgänge 30
6.12.1 Zertifikatmanagement-Vorgang 30
6.12.2 Initiale Zertifikaterzeugung 30
6.12.3 Anmeldung einer Einheit unter Verwendung von SCEP 30
6.12.4 Vorgang der Zertifikatsignierungsanforderung (CSR) 31
6.12.5 Zertifikatsperrlisten (CRLs) 32
6.12.6 Online-Zertifikat Status-Protokoll (OCSP) 33
6.12.7 Serverbasiertes Zertifikatvalidierungs-Protokoll (SCVP) 35
6.12.8 Kurzlebige Zertifikate 35
6.12.9 Zertifikaterneuerung 36
6.13 Alternativer Vorgang für außerhalb der Einheit erzeugte asymmetrische Schlüssel 36
6.14 Schlüsselverteilung symmetrischer Schlüssel mit unterschiedlichem Zeitrahmen 37
7 Allgemeine Schlüsselmanagementanforderungen (normativ) 37
7.1 Asymmetrische und symmetrische Schlüsselmanagementanforderungen 37
7.2 Benötigte kryptografische Materialien 38
7.3 Digitale Zertifikate 38
7.4 Schutz mit kryptografischem Schlüssel 38
7.5 Verwendung bestehender Sicherheits-Schlüsselmanagement-Infrastruktur 38
8 Asymmetrisches Schlüsselmanagement (normativ) 38
8.1 Zertifikaterzeugung und -installation 38
8.1.1 Erzeugung und Installation privater und öffentlicher Schlüssel 38
8.1.2 Einheitenregistrierung zur Identitätseinrichtung 39
8.1.3 Einheitenanmeldung bei der CA 39
8.1.4 Aktualisierungsmanagement für das CA-Wurzel-Zertifikat 40
8.2 Zertifikatgültigkeit 40
8.2.1 Gültigkeit von Zertifikaten 40
8.2.2 Zertifikatsperrung 40
8.2.3 Überprüfung des Zertifikatsperrstatus 40
8.3 Zertifikatablauf und -erneuerung 40

Seite

9 Symmetrisches Schlüsselmanagement (normativ) ... 41
9.1 Gruppenbasiertes Schlüsselmanagement (GDOI) ... 41
9.1.1 GDOI-Anforderungen ... 41
9.1.2 GDOI-Nutzdatenerweiterungen ... 41
9.1.3 Nutzdatenidentifikation ... 44
9.1.4 Definitionen der gemeinsamen Nutzdatenantwortfelder ... 46
9.1.5 Richtlinienantwort ... 47
9.1.6 Schlüsseldownloadnutzdaten ... 48
9.1.7 Gemeinsame Schlüsselnutzdaten für den aktuellen und nächsten Schlüssel ... 48
9.1.8 Schlüsseldownloadtypen ... 50
10 Verbindungen zu den Teilen von IEC 62351 und anderen IEC-Dokumenten (informativ) ... 50
11 Verweisungen und Literaturverzeichnis ... 51
Anhang A Erklärung zur Konformität der Protokollimplementierung (PICS) ... 54
Anhang B Zufallszahlzahlenerzeugung (RNG) (informativ) ... 55
B.1 Typen der Zufallszahlenerzeugung ... 55
B.2 Deterministische Zufallsbiterzeuger ... 55
B.3 Nichtdeterministische Zufallsbiterzeuger ... 56
B.4 Entropiequellen ... 56
Anhang C Flussdiagramme für Zertifikatanmeldung und -erneuerung ... 57
C.1 Zertifikatanmeldung ... 57
C.2 Zertifikaterneuerung ... 57

Bilder

Bild 1 – Komponentenbeziehungen von X.509-Zertifikaten ... 19
Bild 2 – Verteilung des Gruppenschlüsselmanagements ... 21
Bild 3 – GDOI IKE Phase 1 – Authentifizierung und Sicherung des Kommunikationskanals ... 22
Bild 4 – GDOI-Pull – Authentifizierung und Sicherung des Kommunikationskanals ... 23
Bild 5 – Auslösung der Schlüsselerneuerung durch die Einheiten – Teil 1 ... 24
Bild 6 – Auslösung der Schlüsselerneuerung durch die Einheiten – Teil 2 ... 25
Bild 7 – Zustandsübergänge bei der Schlüsselverwendung nach IEC 61850-90-5 Ed.1 ... 26
Bild 8 – TimeOfCurrentKey und TimeToNextKey ... 27
Bild 9 – Schlüsselmanagement im Produktlebenszyklus ... 27
Bild 10 – Vereinfachter Lebenszyklus eines Zertifikats innerhalb einer Einheit ... 28
Bild 11 – Lebenszyklus des kryptografischen Schlüssels ... 29
Bild 12 – Beispiel für den SCEP-Einheiten-Anmeldevorgang ... 31
Bild 13 – CSR-Verarbeitung ... 32
Bild 14 – Zertifikatsperrliste ... 33
Bild 16 – Diagramm, das eine Kombination von CRL- und OCSP-Vorgängen verwendet ... 34
Bild 17 – Übersicht serverbasiertes Zertifikatvalidierungs-Protokoll mit Verwendung des OCSP-Backend ... 35

Seite

Bild 18 – Zertifikaterneuerung 36
Bild 19 – Zentrale Zertifikaterzeugung 37
Bild 20 – Standard-GDOI-Identifizierungsnutzdatum 42
Bild 21 – Allgemeines Format der GDOI-Nutzdatenerweiterung 43
Bild 22 – IP-Adresse 45
Bild 23 – Richtlinienantwortframe 47
Bild 24 – Definition der Schlüsseldownload-Antwortnutzdaten 49
Bild 25 – Die Beziehung von IEC 62351 Teil 9 zu anderen Teilen von IEC 62351 50

Tabellen

Tabelle 1 – RFC 6407 zugewiesene Hashbezeichner 42
Tabelle 2 – RFC 6407 zugewiesene Nutzdatenbezeichner 42
Tabelle 3 – Zugewiesene Nutzdatenbezeichner 44
Tabelle 4 – RFC 6407 Schlüsseldownload-Typbezeichner 48
Tabelle 5 – Schlüsseldownload-Typbezeichner 48