

## Inhalt

	Seite
Europäisches Vorwort .....	2
1 Anwendungsbereich.....	8
2 Normative Verweisungen .....	8
3 Begriffe .....	8
4 Abkürzungen und Akronyme.....	14
5 Kryptografische Anwendungen für die praktische Umsetzung von Systemen der Energietechnik .....	16
5.1 Kryptografie, kryptografische Schlüssel und Sicherheitsziele .....	16
5.2 Kryptografietypen .....	16
5.3 Verwendungsmöglichkeiten der Kryptografie .....	17
5.3.1 Ziele der Cybersicherheit .....	17
5.3.2 Vertraulichkeit .....	17
5.3.3 Datenintegrität.....	18
5.3.4 Authentifizierung .....	18
5.3.5 Unleugbarkeit.....	18
5.3.6 Vertrauen .....	18
6 Konzepte zum Schlüsselmanagement und Verfahren beim Betrieb von Systemen der Energietechnik.....	19
6.1 Sicherheitspolitik für das Schlüsselmanagementsystem .....	19
6.2 Entwurfsprinzipien des Schlüsselmanagements beim Betrieb von Systemen der Energietechnik.....	19
6.3 Verwendung von Transportschicht-Sicherheit (TLS).....	20
6.4 Gebrauch kryptografischer Schlüssel .....	20
6.5 Vertrauen durch eine Öffentliche-Schlüssel-Infrastruktur (PKI).....	20
6.5.1 Registrierungsstellen (RA) .....	20
6.5.2 Zertifizierungsstelle (CA).....	21
6.5.3 Zertifikate mit öffentlichem Schlüssel.....	21
6.5.4 Attribut-Zertifikate.....	21
6.5.5 Erweiterungen in Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten.....	22
6.6 Vertrauen durch selbstsignierte Nicht-PKI-Zertifikate .....	22
6.7 Autorisierungs- und Validierungslisten.....	23
6.7.1 Allgemeines.....	23
6.7.2 AVLS in unbeschränkten Umgebungen .....	23
6.7.3 AVLS in beschränkten Umgebungen .....	24
6.7.4 Verwendung selbstsignierter Zertifikate mit öffentlichem Schlüssel in AVLS .....	24
6.8 Vertrauen durch vorher vereinbarte Schlüssel.....	24
6.9 Sitzungsschlüssel.....	24
6.10 Protokolle, die beim Vertrauensaufbau verwendet werden .....	25

	Seite
6.10.1	Zertifizierungsanforderung ..... 25
6.10.2	Vertrauensanker-Verwaltungsprotokoll (TAMP)..... 25
6.10.3	Einfaches Zertifikatanmeldungsprotokoll (SCEP) ..... 25
6.10.4	Internet-Zertifikat-Verwaltungsprotokoll für X.509-Zertifikate in einer PKI ..... 25
6.10.5	Zertifikatmanagement über CMS (CMC)..... 26
6.10.6	Anmeldung über sicheren Transport (EST) ..... 26
6.10.7	Übersicht über die verschiedenen Protokolle..... 26
6.11	Gruppenschlüssel..... 26
6.11.1	Zweck von Gruppenschlüsseln ..... 26
6.11.2	Gruppendomäne der Interpretation (GDOI) ..... 27
6.12	Lebenszyklus des Schlüsselmanagements..... 32
6.12.1	Schlüsselmanagement im Lebenszyklus einer Einheit ..... 32
6.12.2	Lebenszyklus des kryptografischen Schlüssels ..... 33
6.13	Zertifikatmanagement-Vorgänge ..... 35
6.13.1	Zertifikatmanagement-Vorgang ..... 35
6.13.2	Initiale Zertifikaterzeugung ..... 35
6.13.3	Anmeldung einer Einheit ..... 35
6.13.4	Vorgang der Zertifikatsignierungsanforderung (CSR)..... 37
6.13.5	Zertifikatsperrlisten (CRLs)..... 38
6.13.6	Online-Zertifikat-Status-Protokoll (OCSP)..... 39
6.13.7	Serverbasiertes Zertifikatvalidierungs-Protokoll (SCVP) ..... 42
6.13.8	Kurzlebige Zertifikate..... 42
6.13.9	Zertifikaterneuerung ..... 43
6.14	Alternativer Vorgang für außerhalb der Einheit erzeugte asymmetrische Schlüssel ..... 44
6.15	Schlüsselverteilung symmetrischer Schlüssel mit unterschiedlichem Zeitrahmen ..... 45
7	Allgemeine Schlüsselmanagementanforderungen..... 45
7.1	Asymmetrische und symmetrische Schlüsselmanagementanforderungen ..... 45
7.2	Benötigte kryptografische Materialien ..... 45
7.3	Anforderungen an Zertifikate mit öffentlichem Schlüssel ..... 46
7.4	Schutz mit kryptografischem Schlüssel ..... 46
7.5	Verwendung bestehender Sicherheits-Schlüsselmanagement-Infrastruktur ..... 46
7.6	Verwendung von Objektbezeichnern ..... 46
8	Asymmetrisches Schlüsselmanagement..... 47
8.1	Zertifikaterzeugung und -installation ..... 47
8.1.1	Erzeugung und Installation privater und öffentlicher Schlüssel ..... 47
8.1.2	Erneuerung privater und öffentlicher Schlüssel ..... 47
8.1.3	Zufallszahlenerzeugung ..... 47
8.1.4	Zertifikatrichtlinie..... 47
8.1.5	Einheitenregistrierung zur Identitätseinrichtung ..... 47

	Seite	
8.1.6	Einheitenkonfiguration.....	48
8.1.7	Einheitenanmeldung .....	48
8.1.8	Aktualisierung der Vertrauensankerinformationen.....	50
8.2	Sperrung von Zertifikaten mit öffentlichem Schlüssel.....	51
8.3	Zertifikatgültigkeit .....	51
8.3.1	Gültigkeit von Zertifikaten.....	51
8.3.2	Zertifikatsperrung .....	51
8.3.3	Überprüfung des Zertifikatsperrstatus.....	51
8.3.4	Behandlung von Autorisierungs- und Validierungslisten (AVLs) .....	52
8.4	Zertifikatablauf und -erneuerung.....	57
8.5	Sichere Uhrzeitsynchronisation.....	57
9	Symmetrisches Schlüsselmanagement .....	58
9.1	Gruppenbasiertes Schlüsselmanagement (GDOI) .....	58
9.1.1	GDOI-Anforderungen .....	58
9.1.2	Internet-Schlüssel-Austausch Version 1 (IKEv1).....	58
9.1.3	Phase-1-IKEv1-Austausch im Hauptmodus Typ 2 .....	59
9.1.4	Phase 1/2 ISAKMP-Informationsaustausch Typ 5.....	63
9.1.5	Phase-2-GDOI-GROUPKEY-PULL-Austausch Typ 32 .....	64
9.1.6	GROUPKEY-PULL Gruppenschlüssel-Downloadaustausch.....	72
10	Verbindungen zu den Teilen von IEC 62351 und anderen IEC-Dokumenten .....	73
Anhang A (normativ) Erklärung zur Konformität der Protokollimplementierung (PICS).....		75
Anhang B (informativ) Zufallszahlenerzeugung (RNG).....		76
B.1	Typen der Zufallszahlenerzeugung.....	76
B.2	Deterministische Zufallsbiterzeuger .....	76
B.3	Nichtdeterministische Zufallsbiterzeuger .....	77
B.4	Entropiequellen .....	77
Anhang C (informativ) Flussdiagramme für Zertifikatanmeldung und -erneuerung.....		78
C.1	Zertifikatanmeldung.....	78
C.2	Zertifikaterneuerung .....	78
Anhang D (informativ) Beispiele für Zertifikatprofile.....		80
Literaturhinweise .....		84
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....		87
<b>Bilder</b>		
Bild 1 – Beziehung zwischen Zertifikaten mit öffentlichem Schlüssel und Attribut-Zertifikaten .....		22
Bild 2 – Verteilung des Gruppenschlüsselmanagements.....		27
Bild 3 – GDOI IKE Phase 1 – Authentifizierung und Sicherung des Kommunikationskanals.....		28
Bild 4 – GDOI Pull Phase 2 .....		29
Bild 5 – Auslösung der Schlüsselerneuerung durch die Einheiten .....		31

	Seite
Bild 6 – Schlüsselmanagement im Produktlebenszyklus .....	32
Bild 7 – Vereinfachter Lebenszyklus eines Zertifikats .....	33
Bild 8 – Lebenszyklus des kryptografischen Schlüssels .....	34
Bild 9 – Beispiel für den SCEP-Einheiten-Anmelde- und CSR-Vorgang .....	36
Bild 10 – Beispiel für den EST-Einheiten-Anmelde- und CSR-Vorgang .....	37
Bild 11 – CSR-Verarbeitung .....	38
Bild 12 – Zertifikatsperrliste .....	39
Bild 13 – Übersicht über das Online-Zertifikat-Status-Protokoll (OCSP).....	40
Bild 14 – Diagramm, das eine Kombination von CRL- und OCSP-Vorgängen verwendet .....	41
Bild 15 – Anrufabläufe für das Online-Zertifikat-Status-Protokoll (OCSP) .....	42
Bild 16 – Übersicht über ein serverbasiertes Zertifikatvalidierungs-Protokoll mit Verwendung des OCSP-Backend .....	42
Bild 17 – SCEP-Zertifikaterneuerung.....	43
Bild 18 – EST-Zertifikaterneuerung/Schlüsselerneuerung .....	44
Bild 19 – Zentrale Zertifikaterzeugung.....	45
Bild 20 – IKEv1 (RFC 2409)-Austausch im Hauptmodus mit digitalen RSA-Signaturen .....	59
Bild 21 – IKEv1-Austausch im Hauptmodus und Sicherheitsverbindungsdaten .....	60
Bild 22 – IKEv1-Austausch im Hauptmodus: Schlüsselaustauschnachrichten .....	61
Bild 23 – IKEv1-Austausch im Hauptmodus: ID-Authentifizierungsnachrichten .....	62
Bild 24 – IKEv1-HASH_I-Berechnung .....	62
Bild 25 – Phase-1-Informationsaustausch.....	63
Bild 26 – GD004FI GROUPKEY-PULL wie in RFC 6407 definiert.....	64
Bild 27 – GROUPKEY-PULL-Hash-Berechnungen.....	65
Bild 28 – GROUPKEY-PULL: ursprünglicher SA-Anforderungsaustausch.....	66
Bild 29 – Identifizierungsnutzdatum nach RFC 6407 .....	66
Bild 30 – ID_OID-Identifizierungsdaten .....	67
Bild 31 – 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF .....	68
Bild 32 – IPADDRESS ASN.1 BNF .....	69
Bild 33 – Beispiel für IecUdpAddrPayload ASN.1-Daten mit DER-Kodierung .....	69
Bild 34 – 61850_UDP_TUNNEL-Nutzdatum ASN.1 BNF .....	69
Bild 35 – 61850_ETHERNET_GOOSE/SV-Nutzdatum ASN.1 BNF.....	70
Bild 36 – RFC 6407 SA-TEK-Nutzdatum.....	70
Bild 37 – SA-TEK-Nutzdatum nach IEC 61850 .....	71
Bild 38 – GROUPKEY-PULL: Schlüssel-Downloadaustausch.....	72
Bild 39 – Die Beziehung von IEC 62351-9 zu anderen Teilen von IEC 62351 .....	73
Bild C.1 – Zertifikatanmeldung.....	78
Bild C.2 – Zustandsmaschine für die Zertifikaterneuerung.....	79

**Tabellen**

Tabelle 1 – Von der KDC unterstützte IKEv1-Anforderungen.....	58
Tabelle 2 – Objektbezeichner nach IEC 61850: verbindlich (m) oder optional (o).....	68
Tabelle D.1 – Beispiele für Betreiberzertifikate mit öffentlichem Schlüssel .....	81
Tabelle D.2 – Beispiele für OEM-Zertifikate .....	82
Tabelle D.3 – Beispiel für ein OCSP-Zertifikat .....	83