

## DIN EN 62351-4



ICS 33.200; 35.030; 35.240.50

Einsprüche bis 2018-11-28

**Entwurf**

**Energiemanagementsysteme und zugehöriger Datenaustausch –  
IT-Sicherheit für Daten und Kommunikation –  
Teil 4: Profile einschließlich MMS  
(IEC 57/1860/CDV:2017);  
Deutsche und Englische Fassung prEN 62351-4:2017**

Power systems management and associated information exchange –  
Data and communications security –  
Part 4: Profiles including MMS  
(IEC 57/1860/CDV:2017);  
German and English version prEN 62351-4:2017

Gestion des systèmes de puissance et échanges d'informations associés –  
Sécurité des réseaux et des systèmes des communication –  
Partie 4: Profils comprenant MMS  
(IEC 57/1860/CDV:2017);  
Version allemande et anglaise prEN 62351-4:2017

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-09-28 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter [www.din.de/go/entwuerfe](http://www.din.de/go/entwuerfe) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [dke@vde.com](mailto:dke@vde.com) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/go/stellungnahmen-norm-entwuerfe](http://www.din.de/go/stellungnahmen-norm-entwuerfe) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 158 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

## Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN 62351-4:2017 „Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 4: Profile einschließlich MMS“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 57/1860/CDV:2017 „Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS“ unverändert in den Entwurf prEN 62351-4:2017 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzelektrotechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ([www.dke.de](http://www.dke.de)) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

# Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation – Teil 4: Profile einschließlich MMS

## Inhalt

|                                                                                            | Seite |
|--------------------------------------------------------------------------------------------|-------|
| ABSCHNITT 1 – ALLGEMEINES.....                                                             | 7     |
| 1 Anwendungsbereich und Zweck .....                                                        | 7     |
| 1.1 Anwendungsbereich.....                                                                 | 7     |
| 1.2 Zweck .....                                                                            | 7     |
| 2 Normative Verweisungen .....                                                             | 7     |
| 3 Begriffe und Abkürzungen.....                                                            | 9     |
| 3.1 Definierte Begriffe.....                                                               | 9     |
| 3.2 Zusätzliche Definitionen .....                                                         | 9     |
| 3.3 Definierte Abkürzungen.....                                                            | 11    |
| 3.4 Zusätzliche Abkürzungen.....                                                           | 11    |
| 4 In diesem Teil von IEC 62315 behandelte Sicherheitsfragen.....                           | 12    |
| 4.1 Sicherheit von Anwendungs- und Transportprofilen.....                                  | 12    |
| 4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird .....                               | 13    |
| 4.3 Angriffsverfahren, denen entgegengewirkt wird.....                                     | 14    |
| 4.4 Protokollierung .....                                                                  | 14    |
| 5 Bilaterale Vereinbarungen.....                                                           | 14    |
| ABSCHNITT 2 – T-PROFIL.....                                                                | 16    |
| 6 Sicherheit des T-Profiles .....                                                          | 16    |
| 6.1 Allgemeines.....                                                                       | 16    |
| 6.2 Verwendung der Transportschicht-Sicherheit (TLS).....                                  | 17    |
| 6.2.1 Deaktivierung der TLS .....                                                          | 17    |
| 6.2.2 Unterstützung von TLS-Chiffrensammlungen.....                                        | 17    |
| 6.2.3 Wiederaufnahme von TLS-Sitzungen.....                                                | 19    |
| 6.2.4 Einzelne Komponenten von Zertifikaten mit öffentlichem Schlüssel .....               | 19    |
| 6.2.5 Unterstützte Anzahl von Zertifizierungsstellen.....                                  | 19    |
| 6.2.6 TCP-Ports.....                                                                       | 19    |
| 6.2.7 Größe von Zertifikaten mit öffentlichem Schlüssel.....                               | 19    |
| 6.2.8 Bewertungsdauer für den Sperrstatus von Zertifikaten mit öffentlichem Schlüssel..... | 19    |
| 6.2.9 Validierung von Zertifikaten mit öffentlichem Schlüssel.....                         | 20    |
| 6.2.10 Umgang mit Sicherheitsereignissen .....                                             | 20    |
| ABSCHNITT 3 – ÜBERBLICK ÜBER ANWENDUNGSSICHERHEITSPROFILE .....                            | 20    |
| 7 Überblick über Anwendungssicherheitsprofile (informativ).....                            | 20    |
| 8 Verwendung von kryptografischen Algorithmen (informativ) .....                           | 21    |
| 8.1 Grundlegende kryptografische Definitionen.....                                         | 21    |

|                                                                                                  | Seite |
|--------------------------------------------------------------------------------------------------|-------|
| 8.2 Algorithmen mit öffentlichem Schlüssel.....                                                  | 21    |
| 8.3 Signaturalgorithmen .....                                                                    | 22    |
| 8.4 Symmetrische Verschlüsselungsalgorithmen, die nur zur Verschlüsselung verwendet werden ..... | 23    |
| 8.5 Algorithmen zur authentifizierten Verschlüsselung .....                                      | 23    |
| 8.6 Integritätsprüfwert-Algorithmen .....                                                        | 24    |
| 9 Objektbezeichnervergabe (normativ) .....                                                       | 24    |
| 10 Allgemeine Anforderungen an die oberen OSI-Schichten (normativ) .....                         | 25    |
| 10.1 Überblick.....                                                                              | 25    |
| 10.2 Allgemeines zu den Anforderungen an die oberen OSI-Schichten.....                           | 26    |
| 10.3 Anforderungen an das Sitzungsprotokoll .....                                                | 26    |
| 10.4 Anforderungen an das Darstellungsprotokoll .....                                            | 26    |
| 10.4.1 Kontextliste .....                                                                        | 26    |
| 10.4.2 Abstrakte Syntaxen .....                                                                  | 27    |
| 10.4.3 Darstellungs-Benutzerdaten.....                                                           | 27    |
| 10.4.4 ASN.1-Codierungsanforderungen .....                                                       | 28    |
| 10.5 Anforderungen an das Assoziationssteuerungsdienstelement(ACSE)-Protokoll.....               | 28    |
| 10.5.1 Protokollversion .....                                                                    | 28    |
| 10.5.2 Titel.....                                                                                | 28    |
| 10.5.3 Verwendung des ASN.1-Datentyps EXTERNAL .....                                             | 29    |
| ABSCHNITT 4 – MMS-A-SICHERHEITSPROFIL.....                                                       | 29    |
| 11 Spezifische OSI-Anforderungen an das A-Sicherheitsprofil (normativ) .....                     | 29    |
| 11.1 Einleitung.....                                                                             | 29    |
| 11.2 Anforderung an das Darstellungsprotokoll .....                                              | 29    |
| 11.3 ACSE-Anforderungen.....                                                                     | 30    |
| 11.3.1 Auswahl der Funktionseinheiten .....                                                      | 30    |
| 11.3.2 Anwendungskontext .....                                                                   | 30    |
| 11.3.3 Authentifizierungsmechanismus.....                                                        | 30    |
| 11.3.4 Authentifizierungswert .....                                                              | 30    |
| 12 MMS-Authentifizierungswert (normativ) .....                                                   | 31    |
| 12.1 MMS-Authentifizierungswert-Datentyp .....                                                   | 31    |
| 12.2 Behandlung der Assoziationsanforderung (AARQ-apdu) .....                                    | 32    |
| 12.2.1 Behandlung der AARQ-apdu durch den Client .....                                           | 32    |
| 12.2.2 Behandlung der AARQ-apdu durch den Server.....                                            | 32    |
| 12.3 Behandlung des Assoziationsergebnisses (AARE-apdu) .....                                    | 32    |
| 12.3.1 Behandlung der AARE-apdu durch den Server .....                                           | 32    |
| 12.3.2 Behandlung der AARE-apdu durch den Client.....                                            | 32    |
| ABSCHNITT 5 – ENDE-ZU-ENDE-ANWENDUNGSSICHERHEITSPROFIL.....                                      | 33    |
| 13 Überblick und allgemeine Prinzipien .....                                                     | 33    |

|                                                                                             | Seite |
|---------------------------------------------------------------------------------------------|-------|
| 13.1 Grundlegende Konzepte .....                                                            | 33    |
| 13.2 Zusammenhänge zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll..... | 34    |
| 13.3 Schnittstelle zwischen E2E-Sicherheit und geschütztem Anwendungsprotokoll.....         | 35    |
| 13.3.1 Allgemeines.....                                                                     | 35    |
| 13.3.2 ASN.1 als Schemadefinition.....                                                      | 35    |
| 13.3.3 XML-Schema Definition (XSD) .....                                                    | 35    |
| 14 Spezifische Anforderungen an eine OSI-Umgebung .....                                     | 36    |
| 14.1 Einleitung.....                                                                        | 36    |
| 14.2 Zusätzliche Anforderungen an die Darstellungsschicht.....                              | 36    |
| 14.3 Zusätzliche ACSE-Anforderungen .....                                                   | 37    |
| 14.4 Spezifische mit OSI zusammenhängende Protokollelemente .....                           | 37    |
| 14.4.1 OSI-Wrapping für den E2E-Sicherheits-Quittungsbetrieb .....                          | 37    |
| 14.4.2 OSI-Wrapping für die E2E-Sicherheits-Datenübertragung.....                           | 38    |
| 15 Assoziationsmanagement .....                                                             | 38    |
| 15.1 Allgemeines Konzept .....                                                              | 38    |
| 15.2 Allgemeine Syntax.....                                                                 | 38    |
| 15.3 Anforderung und Annahme des Quittungsbetriebs.....                                     | 39    |
| 15.3.1 Allgemeines.....                                                                     | 39    |
| 15.3.2 OSI-spezifische Überlegungen .....                                                   | 39    |
| 15.3.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen.....                                | 39    |
| 15.4 Zurückweisung der Assoziation durch das geschützte Anwendungsprotokoll .....           | 40    |
| 15.4.1 Allgemeines.....                                                                     | 40    |
| 15.4.2 OSI-spezifische Überlegungen .....                                                   | 40    |
| 15.4.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen.....                                | 40    |
| 15.5 Assoziationszurückweisung aufgrund von Sicherheitsproblemen .....                      | 40    |
| 15.5.1 Allgemeines.....                                                                     | 40    |
| 15.5.2 OSI-spezifische Überlegungen .....                                                   | 41    |
| 15.5.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen.....                                | 41    |
| 15.6 Sicherheitsabbruch der Datenübertragung .....                                          | 41    |
| 15.6.1 Allgemeine Syntax .....                                                              | 41    |
| 15.6.2 OSI-spezifische Überlegungen .....                                                   | 42    |
| 15.6.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen.....                                | 42    |
| 16 Datenübertragungsphase.....                                                              | 42    |
| 16.1 Normale Datenübertragung.....                                                          | 42    |
| 16.1.1 Allgemeine Syntax .....                                                              | 42    |
| 16.1.2 OSI-spezifische Überlegungen .....                                                   | 43    |
| 16.1.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen.....                                | 43    |
| 16.2 Abbruch durch geschütztes Anwendungsprotokoll .....                                    | 43    |

|                                                                                           | Seite |
|-------------------------------------------------------------------------------------------|-------|
| 16.2.1 Allgemeines .....                                                                  | 43    |
| 16.2.2 OSI-spezifische Überlegungen.....                                                  | 43    |
| 16.2.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen .....                             | 43    |
| 17 ClearToken-Datentypen .....                                                            | 43    |
| 17.1 Der Datentyp ClearToken1 .....                                                       | 43    |
| 17.1.1 Allgemeine Syntax.....                                                             | 43    |
| 17.1.2 Unterstützte Signaturalgorithmen.....                                              | 44    |
| 17.1.3 Diffie-Hellman-Menge.....                                                          | 45    |
| 17.1.4 Ableitung der gemeinsamen Schlüssel .....                                          | 45    |
| 17.1.5 Vertraulichkeitsparameter .....                                                    | 46    |
| 17.1.6 Zertifizierungspfad .....                                                          | 47    |
| 17.1.7 Unterstützte Integritätsalgorithmen .....                                          | 47    |
| 17.2 Der Datentyp ClearToken2.....                                                        | 47    |
| 17.3 Der Datentyp ClearToken3.....                                                        | 48    |
| 18 Festlegungen zur Authentifizierung und zur Integrität.....                             | 49    |
| 18.1 Der Datentyp Signature .....                                                         | 49    |
| 18.2 Der Datentyp authenticator .....                                                     | 49    |
| 19 Umgang mit E2E-Sicherheitsfehlern .....                                                | 49    |
| 19.1 Quittungsbetriebdiagnose .....                                                       | 49    |
| 19.2 Datenübertragungsdiagnose .....                                                      | 51    |
| 20 Verfahren für die Überprüfung der Assoziationsanforderung (normativ) .....             | 52    |
| 20.1 Überprüfung des Trägers der E2E-Sicherheit.....                                      | 52    |
| 20.1.1 Überprüfung des Trägers der E2E-Sicherheit in einer OSI-Umgebung.....              | 52    |
| 20.1.2 Überprüfung des Trägers der E2E-Sicherheit in einer Nicht-OSI-Umgebung .....       | 52    |
| 20.2 Überprüfung der Anforderung des E2E-Sicherheits-Quittungsbetriebs .....              | 53    |
| 20.2.1 Anforderung des E2E-Sicherheits-Quittungsbetriebs in einer OSI-Umgebung .....      | 53    |
| 20.2.2 Allgemeine Überprüfung der Anforderung des E2E-Sicherheits-Quittungsbetriebs ..... | 53    |
| 21 Verfahren für die Überprüfung des Assoziationsergebnisses (normativ).....              | 54    |
| 21.1 Überprüfung des Trägers der E2E-Sicherheit.....                                      | 54    |
| 21.1.1 Überprüfung des Trägers der E2E-Sicherheit in einer OSI-Umgebung.....              | 54    |
| 21.1.2 Überprüfung des Trägers der E2E-Sicherheit in einer Nicht-OSI-Umgebung .....       | 54    |
| 21.2 Spezifische Überprüfung des Ergebnisses des E2E-Sicherheits-Quittungsbetriebs .....  | 54    |
| 21.2.1 E2E-Sicherheits-Quittungsbetrieb in einer OSI-Umgebung .....                       | 54    |
| 22 Überprüfung der Sicherheitsparameter während der Datenübertragung.....                 | 55    |
| 22.1 Überprüfung in einer OSI-Umgebung.....                                               | 55    |
| 22.2 Überprüfung in einer Nicht-OSI-Umgebung .....                                        | 55    |
| 22.3 Allgemeine Überprüfungen.....                                                        | 55    |
| 22.3.1 Grundlegende Überprüfungen.....                                                    | 55    |

|                                                                                                             | Seite |
|-------------------------------------------------------------------------------------------------------------|-------|
| 22.3.2 Überprüfung des Authentifizierers .....                                                              | 55    |
| 22.3.3 Überprüfungen des Wertes von ClearToken2 .....                                                       | 55    |
| 23 Routing auf der Anwendungsschicht.....                                                                   | 56    |
| 23.1 Allgemeines zum Routing auf der Anwendungsschicht .....                                                | 56    |
| 23.2 Routing auf der Anwendungsschicht in einer OSI-Umgebung .....                                          | 56    |
| 23.3 Routing auf der Anwendungsschicht in einer Nicht-OSI-Umgebung .....                                    | 57    |
| 24 Konformität mit diesem Teil von IEC 62351.....                                                           | 57    |
| 24.1 Allgemeines.....                                                                                       | 57    |
| 24.2 Konformität mit dem T-Profil .....                                                                     | 57    |
| 24.3 Konformität mit dem A-Profil .....                                                                     | 58    |
| 24.4 Konformität der TASE.2-Sicherheit nach IEC 60870-6.....                                                | 58    |
| Anhang A (normativ) Formale ASN.1-Spezifikation für das A-Sicherheitsprofil.....                            | 59    |
| Anhang B (normativ) Formale ASN.1-Spezifikation für Ende-zu-Ende-Sicherheit .....                           | 60    |
| Anhang C (normativ) Formale XSD-Spezifikation für Ende-zu-Ende-Sicherheit .....                             | 66    |
| Anhang D (normativ) Spezifikation des Zertifikats mit öffentlichem Schlüssel der Endeinheit .....           | 72    |
| D.1 Anwendungsbereich des Anhangs.....                                                                      | 72    |
| D.2 Allgemeine Anforderung.....                                                                             | 72    |
| D.3 Spezifische Überlegungen zu OSI-Anwendungen.....                                                        | 72    |
| D.4 Grundlegende Anforderungen und Empfehlungen zur Struktur .....                                          | 72    |
| D.4.1 Komponente für die Version.....                                                                       | 72    |
| D.4.2 Komponente für die Seriennummer .....                                                                 | 72    |
| D.4.3 Komponente für den Signaturalgorithmus des Ausstellers .....                                          | 72    |
| D.4.4 Komponente für den Aussteller.....                                                                    | 73    |
| D.4.5 Komponente für die Gültigkeit.....                                                                    | 73    |
| D.4.6 Komponente für das betroffene Objekt .....                                                            | 73    |
| D.4.7 Komponente für die Informationen zum öffentlichen Schlüssel des betroffenen Objekts .....             | 73    |
| D.4.8 Komponenten für die eindeutige ID des Ausstellers und die eindeutige ID des betroffenen Objekts ..... | 74    |
| D.5 Erweiterungen .....                                                                                     | 74    |
| D.5.1 Erweiterung für den Schlüsselgebrauch .....                                                           | 74    |
| D.5.2 Erweiterung für einen alternativen Namen des betroffenen Objekts .....                                | 74    |
| D.5.3 Überprüfung der Sperre .....                                                                          | 74    |
| D.5.3.1 Erweiterung für CRL-Verteilungspunkte .....                                                         | 74    |
| D.5.3.2 Erweiterung für den Zugriff auf Informationen für zuständige Stellen .....                          | 75    |
| D.5.4 IEC-Erweiterung für Informationen zu Benutzerrollen .....                                             | 75    |
| Anhang E (normativ) Anforderungen an die unteren Schichten.....                                             | 76    |
| E.1 Anwendungsbereich des Anhangs.....                                                                      | 76    |
| E.2 Transportprotokollklasse 0 .....                                                                        | 76    |
| E.2.1 Vorgabe von zwingenden Längenbeschränkungen.....                                                      | 76    |

|                                                                                                  | Seite |
|--------------------------------------------------------------------------------------------------|-------|
| E.2.2 Antwort auf TPDUs ohne Unterstützung der Klasse 0 .....                                    | 76    |
| E.2.3 Transportselektoren.....                                                                   | 76    |
| E.3 IETF RFC 1006 .....                                                                          | 77    |
| E.3.1 Versionsnummer .....                                                                       | 77    |
| E.3.2 Länge.....                                                                                 | 77    |
| E.3.3 Keep-alive.....                                                                            | 77    |
| Anhang F (informativ) ASN.1-Definition von ACSE.....                                             | 78    |
| Literaturhinweise.....                                                                           | 82    |
| <b>Bilder</b>                                                                                    |       |
| Bild 1 – Anwendungs- und Transportprofile .....                                                  | 13    |
| Bild 2 – Nicht sicheres und sicheres TCP-T-Profil.....                                           | 16    |
| Bild 3 – Assoziationsaufbau.....                                                                 | 25    |
| Bild 4 – Zusammenhänge zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll ..... | 34    |
| Bild 5 – E2E-Sicherheit in einer TCP/IP-Umgebung .....                                           | 34    |
| Bild 6 – ASN.1-Schnittstelle zum geschützten Anwendungsprotokoll.....                            | 35    |
| Bild 7 – XSD-Schnittstelle zum geschützten Anwendungsprotokoll.....                              | 36    |
| <b>Tabellen</b>                                                                                  |       |
| Tabelle 1 – Kommentierte empfohlene Chiffrensammlungen aus IEC/TS 62351-4:2007 .....             | 18    |
| Tabelle 2 – Empfohlene Kombinationen von Chiffrensammlungen .....                                | 18    |
| Tabelle 3 – Maximale Größe der TP-Klasse 0 .....                                                 | 76    |

## ABSCHNITT 1 – ALLGEMEINES

### 1 Anwendungsbereich und Zweck

#### 1.1 Anwendungsbereich

Diese zweite Ausgabe dieses Teils von IEC 62351 erweitert den Anwendungsbereich der ersten Ausgabe in erheblichem Maße. Während die erste Ausgabe in erster Linie eine noch eingeschränkte Unterstützung der Authentifizierung während des Quittungsbetriebs (en: handshake) von Anwendungen auf Grundlage der Manufacturing Message Specification (MMS, Festlegung der Nachrichtenformate für Fertigungszwecke) beinhaltete, stellt diese zweite Ausgabe die Unterstützung einer erweiterten Integrität und Authentifizierung sowohl während der Phase des Quittungsbetriebs als auch während der Datenübertragungsphase bereit. Darüber hinaus ermöglicht sie die Verwaltung gemeinsam genutzter Schlüssel sowie die Verschlüsselung der Datenübertragung und stellt eine Ende-zu-Ende(E2E)-Sicherheit mit null oder mehr zwischengeschalteten Einheiten bereit. Während die erste Ausgabe nur Unterstützung von Systemen beinhaltete, die auf der MMS basieren, d. h. von Systemen, die Open Systems Interworking(OSI)-Protokolle nutzen, stellt diese zweite Ausgabe auch Unterstützung von Anwendungsprotokollen bereit, welche andere Protokollstapel, z. B. TCP/IP-Protokollstapel, verwenden. Diese Unterstützung wird so erweitert, dass Anwendungsprotokolle, die XML-Codierung verwenden, und andere Protokolle mit einem Quittungsbetrieb, welcher den Diffie-Hellman-Schlüsselaustausch unterstützen kann, geschützt werden. Diese erweiterte Sicherheit wird als E2E-Sicherheit bezeichnet.

Es ist vorgesehen, dass dieser Teil von IEC 62351 als normativer Teil derjenigen Normen des IEC TC 57 angesehen wird, welche eine sichere Verwendung von Anwendungsprotokollen wie der MMS erfordern.

Es wird davon ausgegangen, dass es Implementierungen gibt, insbesondere Implementierungen des Inter-Control Centre Communications Protocol (ICCP), die von der ersten Ausgabe dieses Teils von IEC 52315 abhängen. Aus diesem Grund wurde die Spezifikation des A-Sicherheitsprofils aus der ersten Ausgabe in separaten Abschnitten ebenfalls aufgenommen. Implementierungen, die dieses A-Sicherheitsprofil unterstützen, arbeiten mit Implementierungen, die die erste Ausgabe dieses Teils von IEC 62351 unterstützen, zusammen.

Es werden spezielle Diagnoseinformationen für Ausnahmebedingungen für die E2E-Sicherheit bereitgestellt.

Dieser Teil von IEC 62351 bildet einen Satz verbindlicher und optionaler Sicherheitsspezifikationen, die für geschützte Anwendungsprotokolle zu implementieren sind.

#### 1.2 Zweck

Dieser Teil von IEC 62351 richtet sich zunächst an die Mitglieder der Arbeitsgruppen innerhalb des IEC TC 57, welche die Protokolle entwickeln oder nutzen. Damit die in diesem Teil von IEC 62351 beschriebenen Maßnahmen angewandt werden können, müssen sie in den Spezifikationen der Protokolle selbst anerkannt und referenziert werden.

Die anschließende Zielgruppe dieses Teils von IEC 62351 sind die Entwickler von Produkten, die diese Protokolle implementieren.

Teile dieses Teils von IEC 62351 können auch Managern und Führungskräften dabei helfen, Zweck und Anforderungen der Arbeit zu verstehen.

### 2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene

Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC/TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues.*

IEC/TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms.*

IE 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP.*

IEC 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control Role-based access control.*

IEC 62351-9:201x, *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management*

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

ISO 9506-1:2003, *Industrial automation systems — Manufacturing Message Specification – Part 1: Service definition.*

ISO 9506-2:2003, *Industrial automation systems — Manufacturing Message Specification – Part 2: Protocol specification.*

ISO/IEC 8073:1997 | Rec. ITU-T X.224 (1995), *Information technology – open systems interconnection – Protocol for providing the connection-mode transport service.*

ISO/IEC 8823-1:1994 | Rec. ITU-T X.226 (1994), *Information technology – open systems interconnection – connection-oriented presentation protocol: Protocol specification.*

Rec. ITU-T X.127 (1995), *Information technology – open systems interconnection – service definition for the association control service element.*

ANMERKUNG 1 Die entsprechende Internationale Norm ISO/IEC 8649:1996 wurde zurückgezogen.

Rec. ITU-T X.227 (1995), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification.*

ANMERKUNG 2 Die entsprechende Internationale Norm ISO/IEC 8650-1:1996 wurde zurückgezogen.

Rec. ITU-T X.227 (1995)/Amd.1 (1996), *Information technology – open systems interconnection – connection-oriented protocol for the association control service element: Protocol specification – Amendment 1: Incorporation of extensibility markers.*

ANMERKUNG 3 Die entsprechende Internationale Norm-Änderung ISO/IEC 8650-1:1996/Amd.1:1997 wurde zurückgezogen.

ISO/IEC 8824-1:2015 | Rec. ITU-T X.680 (2015), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

ISO/IEC 8825-1:2015 | Rec. ITU-T X.690 (2015), *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

ISO/IEC 8825-4:2015 | Rec. ITU-T X.693 (2015), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER).*

IETF RFC 1006:1987, *ISO Transport Service on top of the TCP, Version: 3.*

IETF RFC 3447:2003, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.*

IETF RFC 3526:2003, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.

IETF RFC 5114:2008, *Additional Diffie-Hellman Groups for Use with IETF Standards*.

IETF RFC 5246:2008, *The Transport Layer Security (TLS) Protocol, Version 1.2*.

### 3 Begriffe und Abkürzungen

#### 3.1 Definierte Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC/TS 62351-2.

#### 3.2 Zusätzliche Definitionen

##### 3.2.1

##### **abstrakte Syntax**

Festlegung von Anwendungsprotokoll-Dateneinheiten durch Anwendung von Notationsregeln, die von den zu ihrer Darstellung verwendeten Codierungsverfahren unabhängig sind

[QUELLE: ISO/IEC 7498-1:1994 | Rec. ITU-T X.200 (1994), 7.1.1.2]

##### 3.2.2

##### **Anwendungsinstanz**

Menge von Fähigkeiten verkörperndes aktives Element, das für Kommunikationssysteme geeignet ist und für die Anwendungsschicht definiert wird

##### 3.2.3

##### **Anwendungskontext**

Menge von Regeln, die von beiden ASO-Aufrufen gemeinsam benutzt werden, um eine Assoziation zu betreiben

[QUELLE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.4.5 (leicht modifiziert)]

##### 3.2.4

##### **Anwendungssicherheitsprofil**

diejenigen Aspekte eines Anwendungsprofils, die mit der Sicherheit zusammenhängen

##### 3.2.5

##### **Anwendungs-Dienstelement**

Satz von Anwendungsfunktionen, der die Fähigkeit bereitstellt für einen spezifischen Zweck die Zusammenarbeit von Anwendungsinstanz-Aufrufen zu ermöglichen

[QUELLE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.4.8]

##### 3.2.6

##### **Assoziation**

kooperierende Beziehung zwischen Anwendungsinstanz-Aufrufen, die die Informationskommunikation und die Koordination ihres gemeinsamen Betriebs für einen Zeitpunkt der Kommunikation ermöglicht. Diese Beziehung kann mittels der Übertragung von Anwendungsprotokoll-Steuerinformationen über einen zugrunde liegenden Dienst hergestellt werden.

[QUELLE: Rec. ITU-T X.217 (1995), 3.5.1 (leicht modifiziert)]

##### 3.2.7

##### **Assoziationssteuerungsdienstelement**

Anwendungs-Dienstelement, das die alleinigen Mittel für den Aufbau und die Beendigung von Anwendungsassoziationen in einer OSI-Umgebung bereitstellt

[QUELLE: ISO/IEC 9545:1994 | Rec. ITU-T X.207 (1993), 3.2.4 (leicht modifiziert)]

### 3.2.8

#### **bilaterale Vereinbarung**

Vereinbarung zwischen zwei Netzleitstellen, die die Datenelemente, auf die zugegriffen wird, und die Mittel für den Zugriff betrifft

[QUELLE: IEC 60870-6-503:2014, 3.3]

### 3.2.9

#### **bilaterale Tabelle**

rechentechnische Darstellung der bilateralen Vereinbarung. Die verwendete Darstellung ist lokal festzulegen.

[QUELLE: IEC 60870-6-503:2014, 3.4]

### 3.2.10

#### **Zertifizierungspfad**

geordnete Liste von einem oder mehreren Zertifikaten mit öffentlichem Schlüssel, beginnend mit einem vom Vertrauensanker signierten Zertifikat mit öffentlichem Schlüssel, und endend mit dem zu validierenden Zertifikat mit öffentlichem Schlüssel der Endeinheit. Alle zwischengeschalteten Zertifikate mit öffentlichem Schlüssel, falls vorhanden, sind CA-Zertifikate, in denen das betroffene Objekt des vorhergehenden Zertifikats mit öffentlichem Schlüssel der Aussteller des darauffolgenden Zertifikats mit öffentlichem Schlüssel ist.

[QUELLE: ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016), 3.5.21]

### 3.2.11

#### **Datenübertragungsphase**

Phase von der Fertigstellung des Aufbaus einer Assoziation bis zu der Initialisierung der Beendigung der Assoziation

Anmerkung 1 zum Begriff: In einigen Spezifikationen wird diese Phase als „Sitzung“ bezeichnet. Diese Bezeichnung wird hier vermieden, da sie sowohl in der OSI-Architektur als auch in der TLS verwendet wird.

### 3.2.12

#### **E2E-Sicherheit**

allgemeine Bezeichnung für die von dem A-Plus-Sicherheitsprofil und/oder dem AE-Plus-Sicherheitsprofil bereitgestellten Sicherheitseinrichtungen

### 3.2.13

#### **Ende-zu-Ende-Anwendungsprofil**

Anwendungsprofil, das Ende-zu-Ende-Sicherheit auf der Anwendungsschicht zwischen zwei Anwendungsinstanzen mit etwaigen zwischengeschalteten Anwendungsinstanzen zur Weitergabe festlegt

### 3.2.14

#### **Betrieb nach erster Ausgabe**

Szenario, in dem die Partner in einer Assoziation oder dem Aufbau einer Assoziation das A-Sicherheitsprofil verwenden, was den Betrieb mit einer der ersten Ausgabe dieses Teils von IEC 62351 entsprechenden Implementierung ermöglicht

### 3.2.15

#### **Schlüsselableitungsfunktion**

Funktion, die Oktett-Strings beliebiger Länge auf Oktett-Strings einer beliebigen, festgelegten Länge abbildet, sodass es rechentechnisch nicht möglich ist, Korrelationen zwischen Ein- und Ausgaben zu finden, und sodass es in dem Fall, dass ein Teil der Ausgabe, nicht aber die Eingabe gegeben ist, rechentechnisch nicht möglich ist, ein beliebiges anderes Bit der Ausgabe herzuleiten. Die genauen Anforderungen an die Sicherheit hängen von der Anwendung ab.

[QUELLE: ISO/IEC 18033-2:2007, 3.25]

### 3.2.16

#### **Füllwert**

einmalig verwendete Zahl

[QUELLE: ISO/IEC 9797-3:2012, 3.3]

### 3.2.17

#### **Präsentationsdatenwert**

in der abstrakten Syntax festgelegte Informationseinheit, die von dem zugrunde liegenden Dienst übertragen wird

[QUELLE: ISO/IEC 8822:1994 | Rec. ITU-T X.216 (1994), 3.4.6]

### 3.2.18

#### **geschütztes Anwendungsprotokoll**

Anwendungsprotokoll, das durch die E2E-Sicherheit geschützt wird

### 3.2.19

#### **Betrieb nach zweiter Ausgabe**

Szenario, in dem die Partner in einer Assoziation oder dem Aufbau einer Assoziation die E2E-Sicherheit nach diesem Teil von IEC 62351 verwenden

## 3.3 Definierte Abkürzungen

Für die Anwendung dieses Dokuments gelten die Abkürzungen nach IEC/TS 62351-2.

## 3.4 Zusätzliche Abkürzungen

|        |                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------|
| ACSE   | Assoziationssteuerungsdienstelement (en: association control service element)                               |
| APDU   | Anwendungsprotokoll-Dateneinheit (en: application protocol data unit)                                       |
| ASE    | Anwendungs-Dienstelement (en: application service element)                                                  |
| CBC    | Betrieb von Blockchiffren (en: Cipher Block Chaining)                                                       |
| DHE    | kurzlebiger Diffie-Hellman (en: Ephemeral Diffie-Hellman)                                                   |
| E2E    | Ende-zu-Ende (en: end-to-end)                                                                               |
| ECDHE  | kurzlebiger Elliptische-Kurven-Diffie-Hellman (en: Elliptic Curve Ephemeral Diffie-Hellman)                 |
| GCM    | Galois/Counter-Betriebsmodus (en: Galois/Counter Mode)                                                      |
| GMAC   | Galois-Nachrichtenauthentifizierungscode (en: Galois Message Authentication Code)                           |
| HMAC   | Schlüssel-Hash-Nachrichtenauthentifizierungscode (en: Keyed-hash Message Authentication Code)               |
| ICCP   | Protokoll für die Kommunikation zwischen Netzleitstellen (en: Inter-Control Centre Communications Protocol) |
| ICV    | Integritätsprüfwert (en: integrity check value)                                                             |
| MAC    | Nachrichtenauthentifizierungscode (en: message authentication code)                                         |
| OCSP   | Online-Zertifikat Status-Protokoll (en: Online Certificate Status Protocol)                                 |
| PDU    | Protokolldateneinheit (en: protocol data unit)                                                              |
| PDV    | Präsentationsdatenwert (en: presentation data value)                                                        |
| SDU    | Dienstdateneinheit (en: service data unit)                                                                  |
| SPDU   | Sitzungsprotokoll-Dateneinheit (en: session protocol data unit)                                             |
| TASE.2 | Fernwirk-Anwendungs-Dienstelement 2 (en: Telecontrol Application Service Element 2)                         |
| TPDU   | Transportprotokoll-Dateneinheit (en: transport protocol data unit)                                          |
| VPN    | virtuelles Privatnetz (en: virtual private network)                                                         |
| XER    | XML-Codierungsregeln (en: XML encoding rules)                                                               |
| XML    | erweiterbare Auszeichnungssprache (en: eXtensible markup language)                                          |
| XSD    | XML-Schema Definition (en: XML schema definition)                                                           |

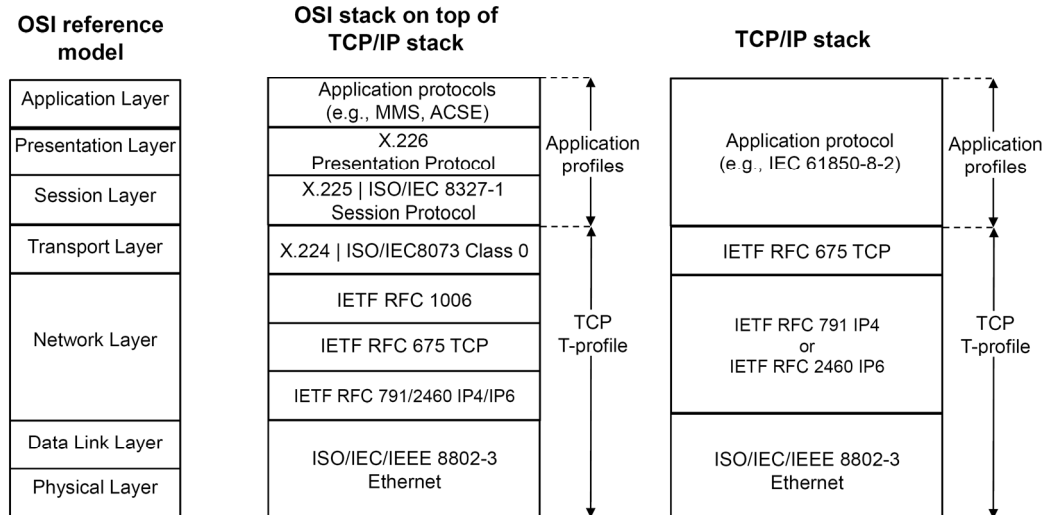
## **4 In diesem Teil von IEC 62315 behandelte Sicherheitsfragen**

### **4.1 Sicherheit von Anwendungs- und Transportprofilen**

Im Hinblick auf die Kommunikationssicherheit nach Festlegung in diesem Teil von IEC 62351 werden die folgenden Punkte behandelt:

- a) Transportprofile: Ein Transportprofil definiert die Protokolle und Anforderungen an die Schichten 1–4 des OSI-Referenzmodells.
- b) Anwendungsprofile: Ein Anwendungsprofil definiert den Satz von Protokollen und Anforderungen an die Schichten 5–7 des OSI-Referenzmodells.

Im Kontext von TC 57 werden zwei T-Profile und drei Anwendungssicherheitsprofile unterschieden. Diese Spezifikation legt die Sicherheitserweiterungen für alle beschriebenen Profile fest.



| Englisch                                   | Deutsch                                   |
|--------------------------------------------|-------------------------------------------|
| OSI reference model                        | OSI-Referenzmodell                        |
| Application Layer                          | Anwendungsschicht                         |
| Presentation Layer                         | Darstellungsschicht                       |
| Session Layer                              | Sitzungsschicht                           |
| Transport Layer                            | Transportschicht                          |
| Network Layer                              | Vermittlungsschicht                       |
| Data Link Layer                            | Sicherungsschicht                         |
| Physical Layer                             | Bitübertragungsschicht                    |
| OSI stack on top of TCP/IP stack           | OSI-Stapel auf dem TCP/IP-Stapel          |
| Application protocols (e.g., MMS, ACSE)    | Anwendungsprotokolle (z. B. MMS, ACSE)    |
| X.226                                      | X.226                                     |
| Presentation Protocol                      | Darstellungsprotokoll                     |
| X.225   ISO/IEC 8327-1                     | X.225   ISO/IEC 8327-1                    |
| Session Protocol                           | Sitzungsprotokoll                         |
| X.224   ISO/IEC8073 Class 0                | X.224   ISO/IEC 8073 Klasse 0             |
| IETF RFC 1006                              | IETF RFC 1006                             |
| IETF RFC 675 TCP                           | IETF RFC 675 TCP                          |
| IETF RFC 791/2460 IP4/IP6                  | IETF RFC 791/2460 IP4/IP6                 |
| ISO/IEC/IEEE 8802-3                        | ISO/IEC/IEEE 8802-3                       |
| Ethernet                                   | Ethernet                                  |
| Application profiles                       | Anwendungsprofile                         |
| TCP T-profile                              | TCP-T-Profil                              |
| TCP/IP stack                               | TCP/IP-Stapel                             |
| Application protocol (e.g., IEC 61850-8-2) | Anwendungsprotokoll (z. B. IEC 61850-8-2) |
| IETF RFC 675 TCP                           | IETF RFC 675 TCP                          |
| IETF RFC 791 IP4 or IETF RFC 2460 IP6      | IETF RFC 791 IP4 oder IETF RFC 2460 IP6   |
| ISO/IEC/IEEE 8802-3                        | ISO/IEC/IEEE 8802-3                       |

Bild 1 – Anwendungs- und Transportprofile

## 4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird

IEC TS 62351-1 enthält eine Diskussion der Sicherheitsbedrohungen und Angriffsverfahren.

Für den Fall, dass die zu übertragenden Daten nicht verschlüsselt werden, umfasst dieser Teil von IEC 62351 die folgenden Bedrohungen, denen entgegengewirkt wird:

- unautorisierter Zugriff auf Informationen

Für den Fall, dass IEC 62351-3 angewendet wird, umfasst dieser Teil die folgenden Bedrohungen, denen entgegengewirkt wird:

- unautorisierter Zugriff auf Informationen mittels Authentifizierung auf Paketebene und Verschlüsselung der Nachrichten
- unautorisierte Veränderung (Manipulation) oder Diebstahl von Informationen mittels Authentifizierung auf Paketebene und Verschlüsselung der Nachrichten

#### 4.3 Angriffsverfahren, denen entgegengewirkt wird

Die folgenden Sicherheitsbedrohungen werden durch die Umsetzung der in diesem Dokument aufgeführten Spezifikation/Empfehlungen entschärft. Die Angriffsverfahren, denen mit IEC 62351-3 entgegengewirkt wird, sowie das zugehörige beschriebene T-Profil und die in diesem Teil von IEC 62351 festgelegten A-Sicherheitsprofile werden in der Liste nicht aufgeführt:

- Man-in-the-Middle: Dieser Bedrohung wird auf Transportebene (T-Profil) entgegengewirkt, und zwar mithilfe der Authentifizierungs- und Verschlüsselungsmechanismen, die von dem eingesetzten zugrunde liegenden Sicherheitsprotokoll bereitgestellt werden. Darüber hinaus werden auf der Anwendungsschicht Ende-zu-Ende-Authentifizierungs- und -Verschlüsselungsmechanismen definiert, um die Vertraulichkeit der Nachrichten auch dann sicherzustellen, wenn der Transport über zwischengeschaltete Einheiten erfolgt.
- Manipulationserkennung/Nachrichtenintegrität: Diesen Bedrohungen wird auf Transportebene (T-Profil) entgegengewirkt, und zwar mithilfe der Authentifizierungs- und Integritätsmechanismen, die von dem eingesetzten zugrunde liegenden Sicherheitsprotokoll bereitgestellt werden. Darüber hinaus werden auf der Anwendungsschicht Ende-zu-Ende-Authentifizierungs- und -Integritätsmechanismen definiert, um die Integrität der Nachrichten auch dann sicherzustellen, wenn der Transport über zwischengeschaltete Einheiten erfolgt.
- Wiedereinspielung: Dieser Bedrohung wird durch die Verwendung von spezialisierten Zustandsmaschinen für die Verarbeitung in Kombination mit der in diesem Teil von IEC 62351 festgelegten anfänglichen Authentifizierung und kryptografischen Bindung entgegengewirkt.

#### 4.4 Protokollierung

Es ist wichtig, dass sicherheitsrelevante Verletzungen in einem eigenen Protokoll aufgezeichnet werden, dessen Inhalt inhärent vor Manipulationen (z. B. der Veränderung oder dem Löschen von Informationen) geschützt ist. Implementierer sollten versuchen, genug Informationen aufzuzeichnen, um Sicherheitsaudits und Verfolgungen zu erleichtern. Wie diese Empfehlung tatsächlich umgesetzt wird, ist jeweils lokal festzulegen.

Die Überwachung und die für die Sicherheitsprotokollierung relevante Kommunikation und Definitionen werden in zwei einzelnen IEC 62351-Dokumenten behandelt: IEC 62351-7 behandelt die Überwachung im Zusammenhang mit der Netzwerkverwaltung und IEC 62351-14 wird die Sicherheitsprotokollierung behandeln.

### 5 Bilaterale Vereinbarungen

Dieser Abschnitt ist dann relevant und normativ, wenn dieser Teil von IEC 62351 gemeinsam mit dem Protokoll für die Kommunikation zwischen Netzleitstellen (ICCP), auch bekannt als Fernwirk-Anwendungs-Dienstelement 2 (TASE.2), nach Definition in IEC 60870-6-503:2014 0, IEC 60870-6-702:2014 0 und IEC 60870-6-802:2014 0 verwendet wird.

Bei der Implementierung der MMS für das ICCP müssen Mechanismen für die Konfiguration und Nutzung des Funktionsumfangs der sicheren Profile eingebaut werden. Im Allgemeinen muss Folgendes bereitgestellt werden:

- Ein Mechanismus für die Konfiguration der Informationen zu Zertifikaten mit öffentlichem Schlüssel und die Bindung dieser Informationen an die Zugriffsauthentifizierung (z. B. die bilateralen Tabellen)

- Ein Mechanismus für die Konfiguration des zulässigen eingehenden Transportprofils für den Zugriffskontrollmechanismus der Implementierung. Es werden die folgenden Auswahlmöglichkeiten vorgeschlagen:
  - DON'T\_CARE: würde anzeigen, dass der Aufbau einer MMS-Assoziation sowohl mit einem sicheren als auch mit einem nicht sicheren T-Profil zulässig wäre.
  - NON\_SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit dem nicht sicheren T-Profil zulässig wäre.
  - SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit dem sicheren T-Profil zulässig wäre.

Ein Mechanismus für die Konfiguration des zur Initialisierung einer MMS-Assoziation zu verwendenden Anwendungssicherheitsprofils. Es werden die folgenden Auswahlmöglichkeiten vorgeschlagen:

- NON\_SECURE: würde anzeigen, dass kein Anwendungssicherheitsprofil für die Zulassung des Aufbaus einer MMS-Assoziation verwendet werden darf.
  - SECURE: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit dem A-Sicherheitsprofil nach Definition in der ersten Ausgabe dieses Teils von IEC 62351 zulässig wäre.
  - END-TO-END SECURITY: würde anzeigen, dass der Aufbau einer MMS-Assoziation nur mit einem Ende-zu-Ende-Anwendungssicherheitsprofil zulässig wäre.
- Ein Mechanismus zur Übermittlung/Verifizierung der Assoziationsparameter. Diese Parameter sollten Adressinformationen, einen Hinweis auf das verwendete Profil (z. B. Ende-zu-Ende, sicher, nicht sicher) und die Parameter für die Authentifizierung im Quittungsbetrieb (en: handshake) beinhalten.

Diese Informationen müssen gemeinsam mit den erwarteten Assoziationswerten der konfigurierten MMS dazu verwendet werden zu ermitteln, ob eine MMS-Assoziation aufgebaut werden sollte. Welche Einheit über die tatsächliche Annahme entscheidet, ist jeweils lokal festzulegen.

Die folgende Tabelle enthält Empfehlungen potenzieller Kombinationen von Anwendungssicherheit und Transportsicherheit:

|                                   |              |                                                               |     |                                                                                                                             |     |     |          |     |     |
|-----------------------------------|--------------|---------------------------------------------------------------|-----|-----------------------------------------------------------------------------------------------------------------------------|-----|-----|----------|-----|-----|
| <b>Anwendungssicherheit (5–7)</b> | A            | A                                                             | A   | A+                                                                                                                          | A+  | A+  | AE+      | AE+ | AE+ |
| <b>Transportsicherheit (1–4)</b>  | Keine        | TLS                                                           | VPN | Keine                                                                                                                       | TLS | VPN | Keine    | TLS | VPN |
| <b>Anmerkung</b>                  | Nicht sicher | Zulässig, wenn T-/A-Profil an demselben Knoten beginnen/enden |     | Zulässig, wenn Ende-zu-Ende-Vertraulichkeit nicht erforderlich ist oder wenn T-/A-Profil an demselben Knoten beginnen/enden |     |     | Zulässig |     |     |

Es ist wünschenswert, dass, wenn eine einzelne MMS-Assoziation aufgrund von Änderungen an der Konfiguration neu gestartet werden muss, hierzu nicht auch andere MMS-Assoziationen neu gestartet werden müssen.

Die MMS-Implementierung sollte Ereignisse und Informationen im Zusammenhang mit Assoziationen, die aufgrund von Sicherheitsverletzungen zurückgewiesen wurden, protokollieren. In diesem Kontext erleichtert IEC 62351-7 die Überwachung solcher Ereignisse, während IEC 62351-14 die Protokollierung der Ereignisse festlegen wird.

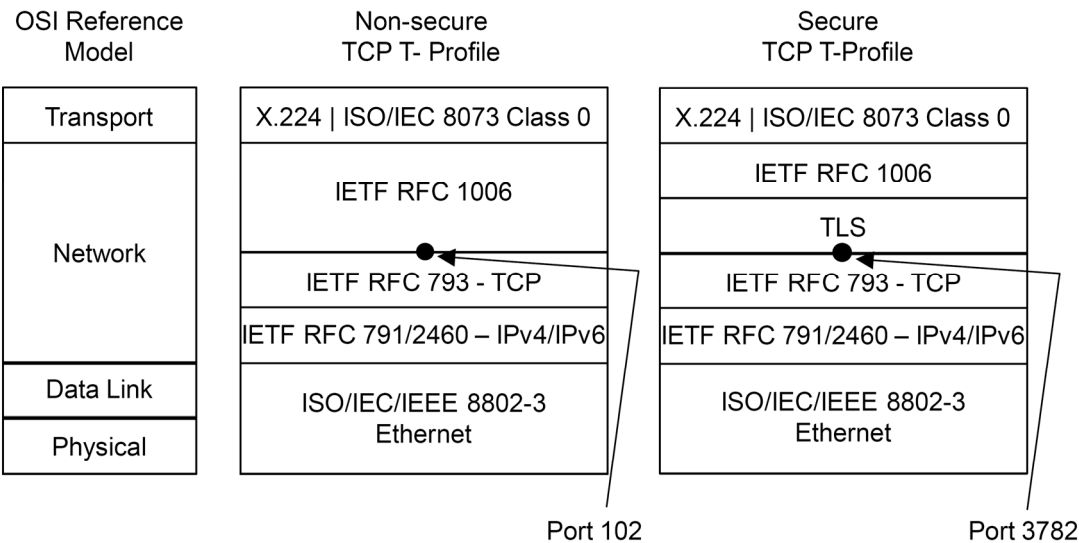
ABSCHNITT 2 – T-PROFIL

6 Sicherheit des T-Profiles

6.1 Allgemeines

Die Sicherheitsempfehlungen für das TCP-T-Profil sind nicht als Festlegung von Sicherheitsempfehlungen für TCP, IP oder Ethernet zu verstehen. Vielmehr legen die Spezifikationen in diesem Teil von IEC 62351 fest, wie die Transportschicht-Sicherheit (en: transport layer security; TLS) gemeinsam mit der TLS-Profilbildung in IEC 62351-3:2017 für die Sicherung von Datenverkehr nach IETF RFC 1006 zu verwenden ist.

Das Sicherheits-TCP-T-Profil nutzt die TLS (nach IETF RFC 5246), um vor dem Einsatz von IETF RFC 1006 für eine Verschlüsselung und Knotenauthentifizierung zu sorgen.



| Englisch                      | Deutsch                       |
|-------------------------------|-------------------------------|
| OSI Reference Model           | OSI-Referenzmodell            |
| Transport                     | Transport                     |
| Network                       | Vermittlung                   |
| Data Link                     | Sicherung                     |
| Physical                      | Bitübertragung                |
| Non-secure TCP T-Profile      | Nicht sicheres TCP-T-Profil   |
| X.224   ISO/IEC 8073 Class 0  | X.224   ISO/IEC 8073 Klasse 0 |
| IETF RFC 1006                 | IETF RFC 1006                 |
| IETF RFC 793 - TCP            | IETF RFC 793 – TCP            |
| IETF RFC 791/2460 - IPv4/IPv6 | IETF RFC 791/2460 – IPv4/IPv6 |
| ISO/IEC/IEEE 8802-3           | ISO/IEC/IEEE 8802-3           |
| Ethernet                      | Ethernet                      |
| Port 102                      | Port 102                      |
| Secure TCP T-Profile          | Sicheres TCP-T-Profil         |
| TLS                           | TLS                           |

Bild 2 – Nicht sicheres und sicheres TCP-T-Profil

Bild zeigt die beiden relevanten TCP-T-Profile. Das eine ist das standardmäßige, nicht sichere T-Profil nach RFC 1006. Das andere ist das sichere Profil aus IETF RFC 1006, das in diesem Teil von IEC 62351 festgelegt wird.

IETF RFC 1006 unterstützt nur die Verwendung der Transportklasse 0 aus ISO/IEC 8073 | Rec. ITU-T X.224.

## 6.2 Verwendung der Transportschicht-Sicherheit (TLS)

Die Transportschicht-Sicherheit ist nach den Festlegungen in IEC 62351-3:2017 zu verwenden. In IEC 62351-3:2017 wird die Festlegung ausgewählter Parameter gefordert. Dies erfolgt in den folgenden Unterabschnitten.

- a) Die zu unterstützenden verbindlichen TLS-Chiffrensammlungen
- b) Die empfohlene Festlegung hinsichtlich der Wiederaufnahme von Sitzungsparametern aus einer früheren Verbindung auf Grundlage der Sitzungslaufzeit
- c) Die empfohlene Festlegung hinsichtlich der Neuaushandlung von Sitzungsparametern auf Grundlage der Sitzungslaufzeit
- d) Die einzelnen Komponenten von Zertifikaten mit öffentlichem Schlüssel
- e) Die empfohlene Anzahl der zu unterstützenden CAs
- f) Der für die Unterscheidung zwischen sicherem (z. B. mit TLS) und nicht sicherem Datenverkehr zu verwendende TCP-Port
- g) Die maximale Größe des Zertifikats mit öffentlichem Schlüssel
- h) Die empfohlene Bewertungsdauer der Zertifikatsperrliste (en: certificate revocation list; CRL)
- i) Bei Verwendung von OCSP für die Überprüfung von Zertifikatsperrungen: der Umgang mit fehlgeschlagenen Zugriffen auf den OCSP-Antwortsender
- j) Der Umgang mit Aktionen zur Validierung von Zertifikaten mit öffentlichem Schlüssel
- k) Der Umgang mit Sicherheitsereignissen
- l) Die geforderte Konformität mit diesem Teil von IEC 62351

Die Konformitätserklärung wird in einem separaten Abschnitt am Ende dieses Dokuments bereitgestellt. Im folgenden Unterabschnitt werden die erforderlichen Werte und Einstellungen für diese Spezifikation definiert.

### 6.2.1 Deaktivierung der TLS

Die Implementierungen müssen eine Deaktivierung der TLS ermöglichen. Wenn die TLS deaktiviert ist, muss der TCP-Port 102 verwendet werden.

Die Deaktivierung der TLS darf entweder in Abhängigkeit von der zugrunde liegenden Sicherheit erfolgen, die über ein VPN bereitgestellt werden darf (womit in diesem Kontext ein Sicherheitsprotokoll unterhalb der TLS gemeint ist, IPsec oder ein anderes Protokoll), oder in Abhängigkeit von dem eingesetzten Anwendungssicherheitsprofil.

### 6.2.2 Unterstützung von TLS-Chiffrensammlungen

In den folgenden Unterabschnitten werden die zu unterstützenden TLS-Chiffrensammlungen definiert. Durch Spezifikationen, auf die verwiesen wird, kommen gegebenenfalls weitere verbindliche Chiffrensammlungen hinzu.

TLS priorisiert im TLS-Quittungsbetrieb die vorgeschlagenen Chiffrensammlungen in der Reihenfolge, in der sie auf der Liste der vorgeschlagenen Chiffrensammlungen in der *ClientHello*-Nachricht aufgeführt werden. Deshalb ist es erforderlich, dass die verbindlichen Chiffrensammlungen als Erste vorgeschlagen werden, gefolgt von den unterstützten optionalen Chiffrensammlungen.

#### 6.2.2.1 Verbindliche und empfohlene Chiffrensammlungen für die Unterstützung von 62351-4:2007

Alle Implementierungen, für die die Konformität mit der ersten Ausgabe dieses Teils von IEC 62351 erklärt wird, müssen mindestens TLS\_DH\_DSS\_WITH\_AES\_256\_SHA unterstützen.

Es wird empfohlen, die in Tabelle 1 (aus der ersten Ausgabe dieses Teils von IEC 62351) aufgeführten TLS-Chiffrensammlungen in Betracht zu ziehen. Angesichts von Weiterentwicklungen in der Kryptografie werden

einige Chiffrensammlungen nicht empfohlen. Diese werden in der Originaltabelle aus der ersten Ausgabe dieses Teils von IEC 62351 entsprechend gekennzeichnet.

**Tabelle 1 – Kommentierte empfohlene Chiffrensammlungen aus IEC/TS 62351-4:2007**

| Schlüsselaustausch |          | Verschlüsselung    | Hash | Quelle             | Unterstützung                         |
|--------------------|----------|--------------------|------|--------------------|---------------------------------------|
| Algorithmus        | Signatur |                    |      |                    |                                       |
| TLS_RSA_           |          | WITH_RC4_128_      | SHA  | RFC 2246 (TLS 1.0) | Abgelehnt (RC 4 als schwach erachtet) |
| TLS_RSA_           |          | WITH_3DES_ede_CBC_ | SHA  | RFC 2246 (TLS 1.0) | Optional                              |
| TLS_DH_            | DSS_     | WITH_3DES_ede_CBC_ | SHA  | RFC 2246 (TLS 1.0) | Optional                              |
| TLS_DH_            | RSA_     | WITH_3DES_ede_CBC_ | SHA  | RFC 2246 (TLS 1.0) | Optional                              |
| TLS_DHE_           | DSS_     | WITH_3DES_ede_CBC_ | SHA  | RFC 2246 (TLS 1.0) | Optional                              |
| TLS_DHE_           | RSA_     | WITH_3DES_ede_CBC_ | SHA  | RFC 2246 (TLS 1.0) | Optional                              |
| TLS_DH_            | DSS_     | WITH_AES_128_      | SHA  | RFC 4346 (TLS 1.1) | Optional                              |
| TLS_DH_            | DSS_     | WITH_AES_256_      | SHA  | RFC 4346 (TLS 1.1) | Verbindlich                           |
| TLS_DH_            |          | WITH_AES_128_      | SHA  | RFC 4346 (TLS 1.1) | Abgelehnt (anonym)                    |
| TLS_DH_            |          | WITH_AES_256_      | SHA  | RFC 4346 (TLS 1.1) | Abgelehnt (anonym)                    |

ANMERKUNG Der Aushandlungsmechanismus in der TLS wählt die letztendlich für eine bestimmte Verbindung verwendete Chiffrensammlung aus den konfigurierten zulässigen/vorhandenen Chiffrensammlungen aus.

#### 6.2.2.2 Verbindliche und empfohlene Chiffrensammlungen für diesen Teil von IEC 62315

Alle Implementierungen, für die die Konformität mit dieser Ausgabe dieses Teils von IEC 62341 erklärt wird, müssen mindestens TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA unterstützen. Dies ist auch die in IETF RFC 5246 definierte verbindliche zu unterstützende Chiffrensammlung.

Es wird empfohlen, die in Tabelle 2 aufgeführten optionalen TLS-Chiffrensammlungen für die Verwendung in Betracht zu ziehen. Wie in Tabelle 2 vermerkt, stammen sie aus verschiedenen IETF-RFCs.

**Tabelle 2 – Empfohlene Kombinationen von Chiffrensammlungen**

| Schlüsselaustausch |          | Verschlüsselung   | Hash   | Quelle       | Unterstützung |
|--------------------|----------|-------------------|--------|--------------|---------------|
| Algorithmus        | Signatur |                   |        |              |               |
| TLS_RSA            |          | WITH_AES_128_CBC_ | SHA    | RFC 5246     | Verbindlich   |
| TLS_DH_            | RSA_     | WITH_AES_128_CBC_ | SHA256 | RFC 5246     | Optional      |
| TLS_DH_            | RSA_     | WITH_AES_128_GCM_ | SHA256 | RFC 5288 [4] | Optional      |
| TLS_DH_            | RSA_     | WITH_AES_256_GCM_ | SHA384 | RFC 5288 [4] | Optional      |
| TLS_ECDHE_         | RSA_     | WITH_AES_128_GCM_ | SHA256 | RFC 7525 [5] | Optional      |
| TLS_ECDHE_         | RSA_     | WITH_AES_256_GCM_ | SHA384 | RFC 7525 [5] | Optional      |
| TLS_ECDHE_         | ECDSA_   | WITH_AES_128_GCM_ | SHA256 | RFC 5289 [6] | Optional      |
| TLS_ECDHE_         | ECDSA_   | WITH_AES_256_GCM_ | SHA384 | RFC 5289 [6] | Optional      |

### 6.2.3 Wiederaufnahme von TLS-Sitzungen

Eine Implementierung, für die die Konformität mit dieser Spezifikation erklärt wird, muss eine mindestens alle zwei Stunden stattfindende Sitzungswiederaufnahme unterstützen.

ANMERKUNG Diese Anforderung gilt nicht für die Unterstützung der ersten Ausgabe dieses Teils von IEC 62351. Neuaushandlung von TLS-Sitzungen

Eine Implementierung, für die die Konformität mit dieser Spezifikation erklärt wird, muss eine Sitzungsneuaushandlung mit mindestens der halben CRL-Aktualisierungsperiode unterstützen (siehe 0).

### 6.2.4 Einzelne Komponenten von Zertifikaten mit öffentlichem Schlüssel

Von dieser Spezifikation werden keine einzelnen Komponenten von Zertifikaten mit öffentlichem Schlüssel gefordert.

ANMERKUNG Zur Unterstützung einer rollenbasierten Zugriffskontrolle mit Erweiterung für Zertifikate mit öffentlichem Schlüssel wird auf IEC 62351-8 verwiesen.

### 6.2.5 Unterstützte Anzahl von Zertifizierungsstellen

Implementierungen, die dieser Spezifikation entsprechen, müssen mindestens zwei verschiedene Zertifizierungsstellen unterstützen. Diese Anforderung entspricht dem in IEC 62351-9 beschriebenen Zertifikatmanagement, das von Anbietern und Betreibern verteilte Zertifikate mit öffentlichem Schlüssel beschreibt.

### 6.2.6 TCP-Ports

Für das nicht sichere T-Profil ist TCP-Port 102 nach Festlegung durch RFC 1006 zu verwenden.

Implementierungen, für die die Konformität mit dieser Spezifikation erklärt wird, müssen TCP-Port 3782 verwenden, um die Verwendung des sicheren TCP-T-Profils anzuzeigen.

### 6.2.7 Größe von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit diesem Teil von IEC 62351 erklärt wird, muss für Zertifikate mit öffentlichem Schlüssel mindestens eine Größe von 8 192 Oktetten unterstützen. Ob auch größere Zertifikate mit öffentlichem Schlüssel unterstützt werden, ist jeweils lokal festzulegen.

Eine Implementierung, die ein Zertifikat mit öffentlichem Schlüssel erhält, dessen Größe die von ihr unterstützte Größe überschreitet, muss die Verbindung beenden und ein Sicherheitsereignis melden („Warnung: Sitzung aufgrund nicht unterstützter Größe des Zertifikats mit öffentlichem Schlüssel beendet“).

### 6.2.8 Bewertungsdauer für den Sperrstatus von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit diesem Teil von IEC 62351 erklärt wird, muss eine mindestens alle 24 Stunden erfolgende CRL-Aktualisierung unterstützen. Die Standard-Bewertungsperiode für gesperrte Zertifikate mit öffentlichem Schlüssel beträgt 24 Stunden. Diese Bewertungsperiode muss konfigurierbar sein.

Eine Implementierung, welche OCSP für die Informationen aus der Überprüfung einer Sperre unterstützt, darf die OCSP-Antwort höchstens 24 Stunden im Cache speichern.

Wenn auf den CRL-Provider, den OCSP-Antwortsender oder eine lokal im Cache gespeicherte CRL oder OCSP-Antwort nicht zugegriffen werden kann, muss ein Sicherheitsereignis gemeldet werden („Warnung: Zertifikatssperrinformationen nicht verfügbar“). Nach IEC 62351-3:2017 darf die Tatsache, dass die Sperrinformationen nicht abgerufen werden können, nicht die Beendigung der Sitzung nach sich ziehen.

## 6.2.9 Validierung von Zertifikaten mit öffentlichem Schlüssel

Eine Implementierung, für die die Konformität mit dieser Spezifikation erklärt wird, muss den Aufbau oder die Neuaushandlung einer Verbindung abbrechen, wenn ein von dem Client oder dem Server verwendetes Zertifikat mit öffentlichem Schlüssel gesperrt oder abgelaufen ist.

Wenn aufgrund eines gesperrten oder abgelaufenen Zertifikats mit öffentlichem Schlüssel der Verbindungsaufbau verweigert oder eine Verbindung während der Sitzungsneuaushandlung abgebrochen wird, sollte ein Sicherheitsereignis gemeldet werden („Vorfall: gesperrtes Zertifikat“). Wenn das Zertifikat mit öffentlichem Schlüssel abgelaufen ist, muss ein Sicherheitsereignis gemeldet werden („Warnung: abgelaufenes Zertifikat mit öffentlichem Schlüssel“).

## 6.2.10 Umgang mit Sicherheitsereignissen

Informationen zu Sicherheitsereignissen und aus der Überwachung sollten der umgebenden Infrastruktur mittels Anwendung von IEC 62351-7:2017 und/oder IEC 62351-14 zugänglich gemacht werden. IEC 62351-7:2017 definiert den Umgang mit Informationen aus der Sicherheitsüberwachung, während IEC 62351-14 den Umgang mit Nachrichten mit Sicherheitswarnungen und Sicherheitsvorfällen festlegt.

# ABSCHNITT 3 – ÜBERBLICK ÜBER ANWENDUNGSSICHERHEITSPROFILE

## 7 Überblick über Anwendungssicherheitsprofile (informativ)

Während das T-Profil für Authentifizierung, Integrität und Vertraulichkeit auf der Transportschicht sorgt, bieten Anwendungssicherheitsprofile Sicherheit auf der Anwendungsschicht.

Diese zweite Ausgabe dieses Teils von IEC 62351 legt zwei Klassen von Anwendungssicherheitsprofilen fest:

- a) Ein Peer-to-Peer-Profil, das als A-Sicherheitsprofil bezeichnet wird und dem in der ersten Ausgabe dieses Teils von IEC 62351 festgelegten A-Profil entspricht. Es bietet nur MMS-basierten Anwendungsprotokollen Sicherheit und unterstützt deshalb nur einen OSI-Protokollstapel. Dieses Sicherheitsprofil wird hier aufgeführt, weil es von Communitys wie der ICCP-Community benutzt wird. Im Allgemeinen wird dringend empfohlen, auf sicherere Profile umzustellen. Dieses Profil bietet lediglich eine Peer-Authentifizierung auf der Anwendungsschicht während des Assoziationsaufbaus, für die Nachrichten im anschließenden Datenaustausch (Datenübertragungsphase) gibt es keine kryptografische Bindung. Es bietet keine Ende-zu-Ende-Authentifizierung und keine Integrität und Vertraulichkeit. Dieses Profil sollte nur gemeinsam mit dem sicheren T-Profil verwendet werden.

Die Spezifikation des A-Sicherheitsprofils ist in ABSCHNITT 4 enthalten.

- b) Ende-zu-Ende-Anwendungssicherheitsprofile, die Ende-zu-Ende-Sicherheit auf der Anwendungsschicht mit null oder mehr zwischengeschalteten Einheiten bieten, wohingegen das T-Profil nur auf den einzelnen Hops Sicherheit bietet.

Die Ende-zu-Ende-Anwendungssicherheitsprofile nach diesem Teil von IEC 62351 können sowohl in einer OSI-Umgebung (z. B. zur Unterstützung von IEC 61850-8-1) als auch in einer Nicht-OSI-Umgebung (z. B. zur Unterstützung von IEC 61850-8-2) eingesetzt werden.

Wenngleich die Sicherheitsinformationen von Ende zu Ende ausgetauscht werden, ist in gewisser Hinsicht eine zwischengeschaltete Einheit beteiligt, z. B., wenn das Routing nicht ausgeführt werden kann. Nähere Informationen können Abschnitt 0 entnommen werden.

Es werden zwei solche Ende-zu-Ende-Anwendungssicherheitsprofile festgelegt:

- 1) Das A-Plus-Sicherheitsprofil bietet Ende-zu-Ende-Authentifizierung und stellt die Nachrichtenintegrität während des Aufbaus einer Assoziation sowie für die anschließende, an die anfängliche Authentifizierung gebundene Datenübertragungsphase sicher.
- 2) Das AE-Plus-Sicherheitsprofil bietet den gleichen Schutz wie das A-Plus-Sicherheitsprofil. Darüber hinaus sorgt es für Vertraulichkeit (Verschlüsselung) während der Datenübertragungsphase.

E2E-Sicherheit wird hier als allgemeine Bezeichnung für die von dem A-Plus-Sicherheitsprofil und/oder dem AE-Plus-Sicherheitsprofil bereitgestellten Einrichtungen verwendet.

Die Spezifikation des E2E-Sicherheitsmechanismus befindet sich in ABSCHNITT 5.

## 8 Verwendung von kryptografischen Algorithmen (informativ)

Dieser Teil von IEC 62351 greift in starkem Maße auf kryptografische Algorithmen zurück, um die geforderte Sicherheit sicherzustellen.

ISO/IEC 9594-8:2017 | Rec. ITU-T X.509 (2016) definiert verschiedene ASN.1-Konstrukte für die formale Spezifikation kryptografischer Algorithmen. Diese werden zum einfacheren Nachschlagen unter 0 aufgeführt. In 0-0 werden die für diesen Teil von IEC 62351 relevanten kryptografischen Algorithmen aus verschiedenen Spezifikationen aufgeführt.

### 8.1 Grundlegende kryptografische Definitionen

```
ALGORITHM ::= CLASS {
    &Type          OPTIONAL,
    &id             OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
    [PARMS         &Type]
    IDENTIFIED BY  &id }
```

Die ASN.1-Informationsobjektklasse **ALGORITHM** wird für die formale Spezifikation von kryptografischen Algorithmen verwendet.

```
AlgorithmIdentifier{ALGORITHM:SupportedAlgorithms} ::= SEQUENCE {
    algorithm  ALGORITHM.&id({SupportedAlgorithms}),
    parameters ALGORITHM.&Type({SupportedAlgorithms}{@algorithm}) OPTIONAL,
    ... }
```

Der parametrisierte Datentyp **AlgorithmIdentifier** gibt die generelle Syntax für einen kryptografischen Algorithmus entsprechend der Definition über die ASN.1-Informationsobjektklasse **ALGORITHM** an.

Die kryptografischen Algorithmen werden beständig weiterentwickelt. Dieser Teil von IEC 62351 ist offen für neue und sicherere Algorithmen. Bei den folgenden Algorithmusspezifikationen handelt es sich um Spezifikationen, die als sicher für die Verwendung über eine längere Zeitspanne gelten (mit Ausnahme des Signaturalgorithmus **sha1WithRSAEncryptionAlgorithm**, der für den Betrieb nach erster Ausgabe mit aufgenommen wurde). Durch Spezifikationen, auf die verwiesen wird, und/oder durch Vereinbarungen der Implementierer kommen gegebenenfalls weitere in bestimmten Umgebungen zu verwendende kryptografische Algorithmen hinzu.

### 8.2 Algorithmen mit öffentlichem Schlüssel

An dieser Stelle werden zwei Algorithmen mit öffentlichem Schlüssel eingeführt:

```
rsaEncryptionAlgorithm ALGORITHM ::= {
    PARMS          NULL
    IDENTIFIED BY  rsaEncryption }

rsaEncryption          OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1) }
```

IETF RFC 4055 gibt die formale Spezifikation für die **rsaEncryptionAlgorithm**-Algorithmen mit öffentlichem Schlüssel an.

```
ecPublicKey ALGORITHM ::= {
    PARMS          OBJECT IDENTIFIER
    IDENTIFIED BY  id-ecPublicKey }
```

```
id-ecPublicKey      OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  ansi-x962(10045) keyType(2) 1 }      -- IETF RFC 5480
```

IETF RFC 5480 gibt die formale Spezifikation für den Algorithmus mit öffentlichem Schlüssel `ecPublicKey` an.

Der Algorithmus mit öffentlichem Schlüssel `ecPublicKey` erfordert eine Identifikation einer elliptischen Kurve als Parameter. Eine bestimmte elliptische Kurve wird durch einen Objektbezeichner (en: object identifier) identifiziert. Für diesen Teil von IEC 62351 sind die folgenden elliptischen Kurven relevant:

```
secp256r1           OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  ansi-x962(10045) curves(3) prime(1) 7 }

brainpoolP256r1     OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
  teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) 8 ellipticCurve(1)
  versionOne(1) 7 }
```

### 8.3 Signaturalgorithmen

Ein Signaturalgorithmus ist eine Kombination aus einem Hash-Algorithmus und einem Algorithmus mit öffentlichem Schlüssel, die bei der Erzeugung und Validierung digitaler Signaturen zum Einsatz kommt.

Die folgende Definition ist nur für das A-Sicherheitsprofil nach ABSCHNITT 4 relevant.

```
sha1WithRSAEncryptionAlgorithm ALGORITHM ::= {
  PARMS          NULL
  IDENTIFIED BY sha1WithRSAEncryption

sha1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) sha1WithRSAEncryption(5) }
```

IETF RFC 7427 0 gibt die formale Spezifikation für die `sha1WithRSAEncryptionAlgorithm`-Signaturalgorithmen an. Dieser Signaturalgorithmus bietet nur eine eingeschränkte Sicherheit.

Die folgenden Signaturalgorithmen sind für die Verwendung in der E2E-Sicherheit nach ABSCHNITT 5 relevant.

```
sha256WithRSAEncryptionAlgorithm ALGORITHM ::= {
  PARMS          NULL
  IDENTIFIED BY sha256WithRSAEncryption }

sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11) }
```

IETF RFC 7427 gibt die formale Spezifikation für die `sha256WithRSAEncryptionAlgorithm`-Signaturalgorithmen an.

```
ecdsa-with-SHA256-Algorithm ALGORITHM ::= {
  IDENTIFIED BY ecdsa-with-SHA256 }

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
```

IETF RFC 7427 gibt die formale Spezifikation für den Signaturalgorithmus `ecdsa-with-SHA256-Algorithm` an.

## 8.4 Symmetrische Verschlüsselungsalgorithmen, die nur zur Verschlüsselung verwendet werden

Wenn das AE-Plus-Sicherheitsprofil vorgeschlagen und angenommen wird, muss der Inhalt verschlüsselt werden. In diesem Unterabschnitt werden symmetrische Schlüsselalgorithmen aufgeführt, die auf dem AES-CBC basieren.

Die formalen Spezifikationen lauten wie folgt:

```

aes128-CBC ALGORITHM ::= {
  PARMS          AES-InitializationVector
  IDENTIFIED BY id-aes128-CBC }

aes256-CBC ALGORITHM ::= {
  PARMS          AES-InitializationVector
  IDENTIFIED BY id-aes256-CBC }

InitializationVector ::= OCTET STRING (SIZE (16))

aes OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) us(840)organization(1)
  gov(101) csor(3) nistAlgorithm(4) aes(1) }

id-aes128-CBC OBJECT IDENTIFIER ::= { aes 2 }

id-aes256-CBC OBJECT IDENTIFIER ::= { aes 42 }

```

IETF RFC 3602 0 enthält weitere Informationen zur Verwendung des AES-CBC.

Der Initialisierungsvektor (`InitializationVector`) muss 16 Oktette lang, zufällig (nicht vorhersagbar) und für jede verschlüsselte Nachricht anders sein. Dieser Initialisierungsvektor muss gemeinsam mit der verschlüsselten Nachricht übermittelt werden. Je nach gewähltem MAC-Algorithmus ist gegebenenfalls ein zusätzlicher IV für den MAC erforderlich.

Wenn das AE-Plus-Sicherheitsprofil vorgeschlagen und angenommen wird und der AES-CBC-Algorithmus und -Modus für die Verschlüsselung des Inhalts zu verwenden ist, muss zu diesem Zweck ein separater gemeinsam genutzter, symmetrischer Schlüssel generiert werden.

## 8.5 Algorithmen zur authentifizierten Verschlüsselung

Die AES-GCM-Technologie der authentifizierten Verschlüsselung dient der Verschlüsselung, Integrität und Authentifizierung oder aber der Integrität und Authentifizierung (in diesem letzten Fall wird von GMAC gesprochen).

Dieser Teil von IEC 62351 nutzt den AES-GCM nicht für die Verschlüsselung, sondern nur für Integrität und Authentifizierung. Wenn er als ICV, d. h. als GMAC, verwendet wird, darf er für das AE-Plus-Sicherheitsprofil mit AES-CBC-Verschlüsselung kombiniert werden.

```

aes128-GCM ALGORITHM ::= {
  PARMS          GCMParameters
  IDENTIFIED BY id-aes128-GCM }

aes256-GCM ALGORITHM ::= {
  PARMS          GCMParameters
  IDENTIFIED BY id-aes256-GCM }

```

Die zugehörigen Objektbezeichner werden wie folgt vergeben:

```

id-aes128-GCM OBJECT IDENTIFIER ::= { aes 6 }

id-aes256-GCM OBJECT IDENTIFIER ::= { aes 46 }

```

```
GCMParameters ::= SEQUENCE {  
    aes-nonce    OCTET STRING, -- recommended size is 12 octets  
    aes-ICVlen   AES-GCM-ICVlen DEFAULT 12 }
```

```
AES-GCM-ICVlen ::= INTEGER (12 | 13 | 14 | 15 | 16)
```

Der Datentyp `GCMParameters` umfasst die folgenden Komponenten:

- Die Komponente `aes-nonce` muss den AES-GCM-Initialisierungsvektor enthalten. IETF RFC 5084 (0) empfiehlt eine Länge von 12 Oktetten. Der Wert muss für jede Verwendung eines bestimmten Schlüssels anders sein, da die Sicherheit sonst gefährdet ist.
- Die Komponente `aes-ICVlen` muss die Länge des resultierenden ICV enthalten. IETF RFC 5084 empfiehlt eine Länge von 12 Oktetten.

## 8.6 Integritätsprüfwert-Algorithmen

Integritätsprüfwert-Algorithmen legen fest, wie Informationen an Nachrichten anzuhängen sind, die eine Überprüfung der Integrität einer Nachricht sowie die Authentifizierung des Absenders (nicht aber die Unleugbarkeit) ermöglichen.

Nachfolgend werden Spezifikationen von ICV-Algorithmen aufgeführt, die von diesem Teil von IEC 62351 anerkannt werden.

Der HMAC mit SHA-256 wird wie folgt definiert:

```
hmacWithSHA256 ALGORITHM ::= {  
    PARMS          NULL  
    IDENTIFIED BY id-hmacWithSHA256 }
```

```
id-hmacWithSHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)  
    rsadsi(113549) digestAlgorithm(2) 9 }
```

Die formale Spezifikation kann dem Computer Security Object Register (CSOR) des NIST (0) entnommen werden.

Wie in 0 besprochen dürfen die AES-GCM-Algorithmen ohne Verschlüsselung auch als MAC-Algorithmen angesehen werden.

## 9 Objektbezeichnervergabe (normativ)

Die folgende Objektbezeichnerkante wird an diesen Teil von IEC 62351 vergeben:

```
secProfile OBJECT IDENTIFIER ::= { iso(1) standard(0) iec62351(62351) part4(4) }
```

Diese Kante wird in weitere Objektbezeichnerkanten für verschiedene Zwecke unterteilt.

Die folgende Kante wird an ASN.1-Module vergeben:

```
secModule OBJECT IDENTIFIER ::= { secProfile module(0) }
```

Die folgende Kante wird an abstrakte Syntaxen vergeben:

```
abstract-syntax OBJECT IDENTIFIER ::= { secProfile abstractSyntax(1) }
```

Die folgende Kante wird an Anwendungskontexte vergeben:

```
appl-context OBJECT IDENTIFIER ::= { secProfile appl-context(2) }
```

Die folgende Kante wird an Authentifizierungsmechanismen vergeben:

```
auth-mechanism OBJECT IDENTIFIER ::= { secProfile auth-mechanism(3) }
```

## 10 Allgemeine Anforderungen an die oberen OSI-Schichten (normativ)

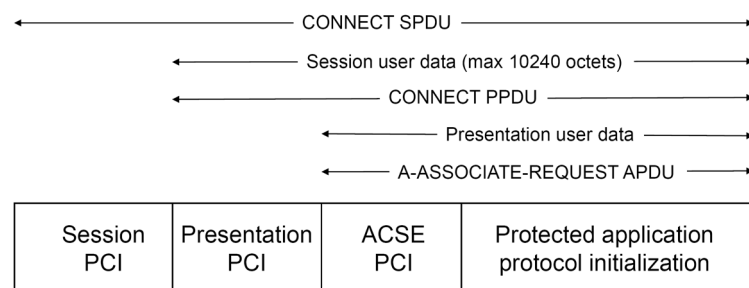
### 10.1 Überblick

Dieser Abschnitt ist nur für den Schutz von Anwendungsprotokollen relevant, die einen OSI-Protokollstapel verwenden. Für Anwendungsprotokolle, die einen TCP/IP-Stapel verwenden, ist er nicht relevant.

Die hier festgelegten Anforderungen an die oberen OSI-Schichten gelten für alle Anwendungssicherheitsprofile. Zusätzliche Anforderungen an die oberen OSI-Schichten für das A-Sicherheitsprofil sind in ABSCHNITT 4 und für Ende-zu-Ende-Sicherheitsanwendungsprofile in ABSCHNITT 5 festgelegt.

Vor dem Aufbau einer Assoziation zwischen zwei OSI-Anwendungsinstanzen muss eine zugrunde liegende Transportverbindung mit oder ohne TLS aufgebaut werden. Eine Transportverbindung unterstützt kein Multiplexen, d. h., dass über eine Transportverbindung nur eine Assoziation aufgebaut werden darf.

Der Aufbau der Sitzungsverbindung, der Darstellungsverbindung und der (Anwendungs-)Assoziation erfolgt in einem einzigen Austausch, siehe Bild. Dargestellt ist nur die Assoziationsanforderung, das Assoziationsergebnis hat jedoch die gleiche Struktur.



SPDU = session-protocol-data-unit  
PPDU = presentation-protocol-data-unit  
APDU = application-protocol-data-unit  
PCI = protocol-control-information

| Englisch                                      | Deutsch                                                                         |
|-----------------------------------------------|---------------------------------------------------------------------------------|
| CONNECT SPDU                                  | CONNECT-SPDU                                                                    |
| Session user data (max 10240 octets)          | Sitzungs-Benutzerdaten (max. 10 240 Oktette)                                    |
| CONNECT PPDU                                  | CONNECT-PPDU                                                                    |
| Presentation user data                        | Darstellungs-Benutzerdaten                                                      |
| A-ASSOCIATE-REQUEST APDU                      | A-ASSOCIATE-REQUEST-APDU                                                        |
| Session PCI                                   | Sitzungs-PCI                                                                    |
| Presentation PCI                              | Darstellungs-PCI                                                                |
| ACSE PCI                                      | ACSE-PCI                                                                        |
| Protected application protocol initialization | Initialisierung des geschützten Anwendungsprotokolls                            |
| SPDU = session-protocol-data-unit             | SPDU = Sitzungsprotokoll-Dateneinheit (en: session-protocol-data-unit)          |
| PPDU = presentation-protocol-data-unit        | PPDU = Darstellungsprotokoll-Dateneinheit (en: presentation-protocol-data-unit) |
| APDU = application-protocol-data-unit         | APDU = Anwendungsprotokoll-Dateneinheit (en: application-protocol-data-unit)    |
| PCI = protocol-control-information            | PCI = Protokollsteuerinformationen (en: protocol-control-information)           |

**Bild 3 – Assoziationsaufbau**

Die Anforderungen der Sitzungsschicht werden in den Protokollelementen (Protokollsteuerinformationen oder PCI) der Sitzungs-CONNECT-SPDU/-ACCEPT-SPDU ausgedrückt. Die Sitzungs-PCI müssen analysiert werden. Probleme in der CONNECT-SPDU führen zu einer REFUSE-SPDU, wohingegen Probleme in der ACCEPT-SPDU zu einer ABORT-SPDU führen. Details zur Fehlerbehandlung fallen nicht in den Anwendungsbereich dieses Teils von IEC 62351.

Die Anforderungen an die Darstellungsschicht werden in den PCI der Darstellungs-CP-PPDU (**CP-type**) ausgedrückt. Die Darstellungs-PCI müssen analysiert werden. Probleme in der CP-PPDU führen zu einer

CPR-PPDU (Connect Presentation Reject PPDU), wohingegen Probleme in der CPA-PPDU (Connect Presentation Accept PPDU) zu einer ARP-PPDU (Abnormal Release Provide Provider PPDU) führen. Details zur Fehlerbehandlung fallen nicht in den Anwendungsbereich dieses Teils von IEC 62351.

Die Sitzungs-Benutzerdaten, mit max. 10 240 Oktetten, müssen die CP-PPDU-/CPA-PPDU-PCI, die ACSE-PCI (einschließlich einer Instanz des Datentyps **E2E-SecAsso-OSI**) und jedwede von dem geschützten Anwendungsprotokoll (z. B. MMS) geforderten Initialisierungsdaten enthalten.

Der Versuch eines Assoziationsaufbaus zwischen zwei Einheiten wird von einer Einheit, dem Client (in Rec. ITU-T X.227 wird der Begriff „Requestor“ verwendet), initialisiert. Diese gibt eine **AARQ-apdu** aus. Die andere Einheit, der Server (in Rec. ITU-T X.227 wird der Begriff „Acceptor“ verwendet), antwortet mit einer **AARE-apdu**. Ergebnis ist entweder der Aufbau einer Assoziation oder das Fehlschlagen des Aufbaus.

## 10.2 Allgemeines zu den Anforderungen an die oberen OSI-Schichten

In der Manufacturing Message Specification (MMS) ist festgelegt, dass die Sitzungs-, Darstellungs- und ACSE-Protokolle nach ISO/ISP 14226-1 0 implementiert werden müssen. Diese ISP fordert die Übereinstimmung mit ISO/IEC ISP 11183-3. Rec. ITUT X.638 0 ist in technischer Hinsicht auf ISO/IEC ISP 11183-3 abgestimmt.

ANMERKUNG ISO/ISP 14226-1 wurde zurückgezogen.

## 10.3 Anforderungen an das Sitzungsprotokoll

Dieser Teil von IEC 62351 enthält die nachfolgend aufgeführten Anforderungen an das Sitzungsprotokoll. Diese Anforderungen werden in der Sitzungs-CONNECT-SPDU festgelegt:

- Die Protokolloption muss festlegen, dass erweiterte verkettete SPDUs nicht unterstützt werden.
- Die Versionsnummer muss auf 2 gesetzt werden.
- Ein oberer Grenzwert für die Größe der TSDU darf nicht eingestellt werden.
- In den Sitzungsanwenderanforderungen muss die Duplex-Funktionseinheit festgelegt werden. Andere Funktionseinheiten dürfen nicht ausgewählt werden (Kernel-Funktionseinheit wird standardmäßig ausgewählt).
- Datenüberlauf darf nicht verwendet werden.
- In der CONNECT-SPDU dürfen keine Benutzerdaten verwendet werden.
- In der CONNECT-SPDU müssen erweiterte Benutzerdaten verwendet werden.
- Benutzerdaten für die ABORT-SPDU, die länger als 9 Oktette sind, müssen unterstützt werden.

ANMERKUNG 1 In Rec. ITUT X.636 wird festgelegt, dass Benutzerdaten verbindlich sind, wohingegen in diesem Teil von IEC 62351 gefordert wird, dass anstelle von Benutzerdaten erweiterte Benutzerdaten verwendet werden.

ANMERKUNG 2 Da Version 2 des Sitzungsprotokolls verwendet wird, gilt für die Benutzerdaten der ACCEPT-SPDU und der ABORT-SPDU ein Höchstwert von 65 539 Oktetten (abzüglich einiger Oktette für Typ/Längen-Felder).

## 10.4 Anforderungen an das Darstellungsprotokoll

### 10.4.1 Kontextliste

Die Komponente **presentation-context-definition-list** der CP-PPDU (Connect Presentation PPDU) muss ein Element für jede definierte abstrakte Syntax enthalten, wofür der folgende Datentyp zu verwenden ist:

```
Context-list ::= SEQUENCE SIZE(2) OF SEQUENCE {  
    presentation-context-identifier Presentation-context-identifier,  
    abstract-syntax-name           Abstract-syntax-name,  
    transfer-syntax-name-list      SEQUENCE OF Transfer-syntax-name }
```

Dieser Datentyp verfügt über drei Komponenten für jedes Element der Sequenz:

- Einen **presentation-context-identifizier**, der vom Client ausgewählt wird. Dieser muss eine ungerade ganze Zahl sein, die für jedes Element der Sequenz verschieden ist.
- Einen **abstract-syntax-name**, der eine bestimmte abstrakte Syntax festlegen muss, die in die Kommunikation einzubinden ist. Der **Abstract-syntax-name** ist ein Objektbezeichner, der die bestimmte abstrakte Syntax bezeichnet.
- Eine **transfer-syntax-name-list**, die aus einem oder mehreren Elementen bestehen muss, von denen jedes den Objektbezeichner für ASN.1-Codierungsregeln festlegt. Dieser Teil von IEC 62351 verwendet die grundlegenden ASN.1-Codierungsregeln (en: basic encoding rules; BER) in einer OSI-Umgebung, die durch den folgenden Objektbezeichner bezeichnet werden:

```
{joint-iso-itu-t(2) asn1(1) basic-encoding(1)}
```

Ein Element vom Typ **Context-list** muss ein Element für die abstrakte Syntax **id-acseAS** enthalten (siehe 0).

#### 10.4.2 Abstrakte Syntaxen

Die abstrakte Syntax für ACSE nach Rec. ITU-T X.227 muss immer gemeinsam mit einem ausgewählten presentation-context-identifizier in der Kontextliste enthalten sein. Die Definition lautet wie folgt:

```
id-acseAS OBJECT IDENTIFIER ::=
    {joint-iso-itu-t(2) association-control(2) abstract-syntax(1) apdus(0) version(1)}
```

Je nach dem unterstützten Anwendungssicherheitsprofil muss eine zusätzliche abstrakte Syntax nach 0 oder 0 enthalten sein.

#### 10.4.3 Darstellungs-Benutzerdaten

ISO/IEC 8822 | Rec. ITU-T X.216 (0) definiert das Konzept des Präsentationsdatenwertes (PDV), der Daten mit einer bestimmten Syntax trägt. Die formale Spezifikation des Datentyps **user-data** lautet wie folgt:

```
User-data ::= CHOICE {
    simply-encoded-data    [APPLICATION 0]    IMPLICIT Simply-encoded-data,
    fully-encoded-data     [APPLICATION 1]    IMPLICIT Fully-encoded-data }
```

Für diesen Teil von IEC 62351 ist nur die Alternative **fully-encoded-data** relevant. Der Datentyp **Fully-encoded-data** ist wie folgt definiert:

```
Fully-encoded-data ::= SEQUENCE OF PDV-list
```

```
PDV-list ::= SEQUENCE {
    transfer-syntax-name      Transfer-syntax-name OPTIONAL,
    presentation-context-identifier Presentation-context-identifier,
    presentation-data-values  CHOICE {
        single-ASN1-type      [0] ABSTRACT-SYNTAX.&Type (CONSTRAINED BY {
            -- Type corresponding to presentation context identifier -- } ),
        octet-aligned          [1] IMPLICIT OCTET STRING,
        arbitrary              [2] IMPLICIT BIT STRING }
```

Für die Anwendung dieses Teils von IEC 62351 darf dies wie folgt vereinfacht werden:

```
User-data ::= SEQUENCE OF SEQUENCE {
    presentation-context-identifier Presentation-context-identifier,
    single-ASN1-type              [0] ABSTRACT-SYNTAX.&Type (CONSTRAINED BY {
        -- Type corresponding to presentation context identifier -- } ) }
```

Dabei ist **ABSTRACT-SYNTAX.&Type** eine Notation für einen beliebigen Datentyp.

#### 10.4.4 ASN.1-Codierungsanforderungen

ISO/ISP 14226-1 0 legt Folgendes fest:

Übereinstimmende Implementierungen müssen auch die folgenden Codierungsregeln unterstützen:

Für Bit-Zeichenketten (oder mittels Tagging von Bit-Zeichenketten abgeleitete Typen) in den MMS-PDUs, die kürzer als 256 Bit sind, sowie für Oktett-Zeichenketten (oder mittels Tagging von Oktett-Zeichenketten abgeleitete Typen) in den MMS-PDUs, die kürzer als 1 024 Oktette sind, dürfen keine zusammengesetzten Codierungen verwendet werden. Für derartige Zeichenketten darf nur primitive Codierung verwendet werden. Bei Eingang einer zusammengesetzten Bit- oder Oktett-Zeichenkette, die diese Vorgabe verletzt, darf die Empfängerimplementierung die zugehörige PDU zurückweisen oder ein P-U-Abort senden, sie darf aber kein P-P-Abort senden.

Es wird empfohlen, die oben genannten Anforderungen zu erfüllen, da Implementierungen, die diese Regeln befolgen, anderenfalls fehlschlagen können.

### 10.5 Anforderungen an das Assoziationssteuerungsdienstelement(ACSE)-Protokoll

Dieser Teil von IEC 62351 verwendet Funktionen aus Rec. ITU-T X.227 zum Assoziationssteuerungsdienstelement (ACSE).

#### 10.5.1 Protokollversion

Es ist nur Version 1 von ACSE relevant. Da diese Version die Standardversion ist, darf die Komponente `protocol-version` von `AARQapdu` und `AAREapdu` zwecks Reduzierung der Größe weggelassen werden.

#### 10.5.2 Titel

Für Titel muss die Form 2 (Objektbezeichnerform) verwendet werden. Die Verzeichnisnamen-Alternative (eindeutiger Name (en: distinguished name)) darf nicht verwendet werden, die Unterstützung dieser Alternative ist nicht erforderlich.

Die mit dem Titel zusammenhängenden Komponenten der `AARQ-apdu` müssen wie folgt codiert werden:

- a) Die Komponente `called-AP-title` muss vorhanden sein und einen Objektbezeichner enthalten, der die als Server fungierende Einheit eindeutig bezeichnet.
- b) Der `called-AE-qualifier` muss eine ganze Zahl enthalten, die den Server gemeinsam mit dem `called-AP-title` eindeutig identifiziert.

ANMERKUNG Die Abkürzung AE steht hier für „application entity“ (Anwendungsinstanz) und sollte nicht mit dem Begriff des AE-Plus-Sicherheitsprofils verwechselt werden.

- c) Die Komponenten `called-AP-invocation-identifizier` und `called-AE-invocation-identifizier` dürfen nicht vorhanden sein.
- d) Die Komponente `calling-AP-title` muss vorhanden sein und einen Objektbezeichner enthalten, der die als Client fungierende Einheit eindeutig bezeichnet.
- e) Der `calling-AE-qualifier` muss eine ganze Zahl enthalten, die den Client gemeinsam mit dem `calling-AP-title` eindeutig identifiziert.
- f) Die Komponenten `calling-AP-invocation-identifizier` und `calling-AE-invocation-identifizier` dürfen nicht vorhanden sein.

Die mit dem Titel zusammenhängenden Komponenten der `AARE-apdu` müssen wie folgt codiert werden:

- a) Wenn die Komponente `responding-AP-title` vorhanden ist, muss sie identisch mit dem Wert des `called-AP-title` der zugehörigen `AARQ-apdu` sein. Wenn diese Komponente nicht vorhanden ist, wird der Wert des `called-AP-title` der `AARQ-apdu` zugrunde gelegt.

- b) Der **responding-AE-qualifier** muss identisch mit dem Wert des **called-AE-qualifier** sein. Wenn diese Komponente nicht vorhanden ist, wird der Wert des **called-AE-qualifier** der **AARQ-apdu** zugrunde gelegt.
- c) Die Komponenten **responding-AP-invocation-identifizier** und **responding-AE-invocation-identifizier** dürfen nicht vorhanden sein.

Die oben genannten Anforderungen haben zur Folge, dass an die beteiligten Einheiten eindeutige Objektbezeichner vergeben werden müssen. Das Verfahren einer solchen Vergabe fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351.

### 10.5.3 Verwendung des ASN.1-Datentyps EXTERNAL

ACSE verwendet den Datentyp EXTERNAL sowohl in dem Datentyp **Authentication-value**, der für das A-Sicherheitsprofil verwendet wird, als auch in dem Datentyp **Association-information**.

Die Codierung des Datentyps EXTERNAL ist nach ISO/IEC 8825-1:2015 | Rec. ITU-T 690 (2015), 8.18.1, wie folgt festgelegt:

```
[UNIVERSAL 8] IMPLICIT SEQUENCE {
  direct-reference      OBJECT IDENTIFIER OPTIONAL,
  indirect-reference    INTEGER OPTIONAL,
  data-value-descriptor ObjectDescriptor OPTIONAL,
  encoding              CHOICE {
    single-ASN1-type    [0] ABSTRACT-SYNTAX.&Type,
    octet-aligned        [1] IMPLICIT OCTET STRING,
    arbitrary            [2] IMPLICIT BIT STRING } }
```

Für die Anwendung dieses Teils von IEC 62351 und in Übereinstimmung mit ISO/IEC 8824-1:2015 | Rec. ITU-T 680 (2015), 37.5, kann dies wie folgt reduziert werden:

```
[UNIVERSAL 8] IMPLICIT SEQUENCE {
  indirect-reference    INTEGER,
  single-ASN1-type     [0] ABSTRACT-SYNTAX.&Type } }
```

Dabei ist **ABSTRACT-SYNTAX.&Type** eine Notation für einen beliebigen Datentyp.

## ABSCHNITT 4 – MMS-A-SICHERHEITSPROFIL

### 11 Spezifische OSI-Anforderungen an das A-Sicherheitsprofil (normativ)

#### 11.1 Einleitung

Dieser Abschnitt legt die spezifische ACSE-Anforderung an das A-Sicherheitsprofil für Systeme fest, die entsprechend dem Betrieb nach erster Ausgabe kommunizieren.

Das hier festgelegte Verfahren ist zu befolgen, wenn SECURE als die gegenseitige Vereinbarung zwischen zwei Systemen für den Anwendungsschichtbetrieb festgelegt wird.

#### 11.2 Anforderung an das Darstellungsprotokoll

In der **contextlist** muss eine spezielle abstrakte Syntax für die MMS mit einem zugehörigen **presentation-context-identifizier** enthalten sein (siehe 0).

Die abstrakte MMS-Syntax wird in ISO 9506-2, 24.11, wie folgt definiert:

```
id-mssAS OBJECT IDENTIFIER ::=
  { iso(1) standard(0) iso9506(9506) part(2) mms-abstract-syntax-version1(1) }
```

## 11.3 ACSE-Anforderungen

### 11.3.1 Auswahl der Funktionseinheiten

In dem A-Sicherheitsprofil wird gefordert, dass die **authentication**-Funktionseinheit mittels Setzen des **authentication**-Bits des Datentyps **ACSE-requirements** der **AARQ-apdu** und der **AARE-apdu** ausgewählt wird.

### 11.3.2 Anwendungskontext

Ein Anwendungskontext bildet eine Vereinbarung über alle für den Informationsaustausch relevanten Punkte. Dazu wird ein Satz von gemeinsam genutzten Regeln für die Kommunikation von Anwendungsinstanz-Aufrufen festgelegt.

Für das A-Sicherheitsprofil ist der folgende Anwendungskontext zu verwenden:

```
basic-AC OBJECT IDENTIFIER ::= { iso(1) standard(0) iso9506(9505) part(2) mms-application-  
context-version1(3) }
```

### 11.3.3 Authentifizierungsmechanismus

Die Komponente **mechanism-name** der **AARQ-apdu** oder **AARE-apdu** muss vorhanden sein und den folgenden Wert aufweisen:

```
version1-mechanism OBJECT IDENTIFIER ::= { auth-mechanism 1 }
```

Dadurch wird angezeigt, dass es sich bei dem Authentifizierungsmechanismus um den durch den Authentifizierungswert nach Abschnitt 0 definierten Mechanismus handelt.

ANMERKUNG Das Verfahren wird von dem Wert dieser Komponente nicht beeinträchtigt. Einige Implementierungen der ersten Ausgabe stellen möglicherweise nicht den richtigen Wert für diese Komponente bereit. Es wird empfohlen, die Implementierung so zu gestalten, dass sie gegenüber diesem Wert in einer empfangenen **AARQ-apdu** tolerant ist.

### 11.3.4 Authentifizierungswert

Rec. ITU-T X.227 definiert alternative Möglichkeiten zur Bereitstellung von Authentifizierungsinformationen, indem der folgende Datentyp in die Komponente **calling-authentication-value** der **AARQ-apdu** und die Komponente **responding-authentication-value** der **AARE-apdu** aufgenommen wird.

```
Authentication-value ::= CHOICE {  
  charstring [0] IMPLICIT GraphicString,  
  bitstring [1] IMPLICIT BIT STRING,  
  external [2] IMPLICIT EXTERNAL,  
  other [3] IMPLICIT SEQUENCE {  
    other-mechanism-name MECHANISM-NAME.&id({ObjectSet}),  
    other-mechanism-value MECHANISM-NAME.&Type({ObjectSet}  
      {@.other-mechanism-name}) } } }
```

Wenn das A-Sicherheitsprofil in der **AARQ-apdu** vorgeschlagen oder in der **AARE-apdu** ausgewählt wird, ist eine Instanz dieses Datentyps in die **AARQ-apdu** und die **AARE-apdu** aufzunehmen. Dann ist die Authentifizierung-Funktionseinheit auszuwählen.

Die Alternative **external** des Datentyps **Authentication-value** ist auszuwählen.

Der Datentyp **EXTERNAL** stellt eine Auswahl mehrerer Alternativen dar. Für die Anwendung dieses Teils von IEC 62351 darf der **Authentication-value** durch den folgenden vereinfachten Datentyp ersetzt werden:

```
Authentication-value ::= CHOICE {  
  external [2] IMPLICIT SEQUENCE {  
    identification CHOICE {
```

```

indirect-reference    INTEGER }, -- the presentation-context-identifier
                        -- for the mmsAuthenticationAS abstract
                        -- syntax
encoding              CHOICE {
    single-ASN1-type [0] MMS-Authentication-value } } }

```

ANMERKUNG In aktuellen Implementierungen ist die Komponente `identification` möglicherweise nicht enthalten. Die Implementierung sollte tolerant ausgelegt werden und davon ausgehen, dass die Implementierung des `STASE-MMS-Authentication-value-ASN.1`-Moduls aufgerufen werden muss und BER-codiert ist.

Eine Instanz des Datentyps `MMS-Authentication-value` muss die Authentifizierungsinformationen bereitstellen.

## 12 MMS-Authentifizierungswert (normativ)

Die Komponente `calling-authentication-value` der `AARQ-apdu` und die Komponente `responding-authentication-value` der `AARE-apdu` müssen die zur Authentifizierung erforderlichen Informationen enthalten.

Eine Instanz des in Rec. X.227 definierten ASN.1-Datentyps `Authentication-value` muss die erforderlichen Informationen enthalten. Die formale Spezifikation des Datentyps `Authentication-value` ist durch das `STASE-MMS-Authentication-value-ASN.1`-Modul in Anhang A gegeben.

ANMERKUNG – Da dieses Modul **IMPLICIT TAG** festlegt, wird implizites Tagging überall dort, wo es relevant ist, als gegeben angenommen. Es ist nicht erforderlich – aber durchaus zulässig – das lexikalische Element **IMPLICIT** zu verwenden.

### 12.1 MMS-Authentifizierungswert-Datentyp

Der Datentyp `MMS-Authentication-value` ist wie folgt definiert:

```

MMS_Authentication-value ::= CHOICE {
    certificate-based      [0] SEQUENCE {
        authentication-Certificate [0] SignatureCertificate,
        time                    [1] GeneralizedTime,
        signature             [2] SignedValue,
        ... }
    ... }

```

```

SignatureCertificate ::= OCTET STRING
-- (CONTAINING Certificate ENCODED BY der)

```

```

SignedValue ::= OCTET STRING

```

- Die Komponente `authentication-Certificate` muss ein **OCTET STRING** sein, der ein DER-kodiertes Zertifikat mit öffentlichem Schlüssel enthält, das an den Absender ausgestellt wird, um die in der Komponente `signature` bereitgestellte digitale Signatur zu bewerten. Anforderungen und Empfehlungen zur Codierung eines solchen Zertifikats mit öffentlichem Schlüssel sind in 0 enthalten. Die maximale Größe beträgt 8 192 Oktette.
- Die Komponente `time` muss die generalisierte GMT-(UTC-)Zeit enthalten, zu der der Authentifizierungswert erstellt wurde.
- Die Komponente `signature` muss eine Oktett-Zeichenkette enthalten, in die die Signatur eingekapselt ist. Die Signatur muss über die DER-codierte Instanz des Datentyps `GeneralizedTime` nach Festlegung durch die Komponente `time` erzeugt werden, darf jedoch weder das ASN1-Tag noch die ASN1-Länge enthalten.

Der Signaturalgorithmus muss `sha1WithRSAEncryptionAlgorithm` nach Definition in IETF RFC 3447 unter Verwendung des Signaturalgorithmus RSASSA-PKCS1-v1\_5 sein. Eine Angabe des verwendeten Signaturalgorithmus darf nicht enthalten sein. Es darf nur die Oktett-Zeichenkette enthalten sein, in der die digitale Signatur enthalten ist.

Der RSA-Schlüssel muss mindestens 2 048 Bit (256 Oktette) lang sein.

## 12.2 Behandlung der Assoziationsanforderung (AARQ-apdu)

### 12.2.1 Behandlung der AARQ-apdu durch den Client

Der Client muss eine Instanz des **MMS-Authentication-value** nach 0 generieren, die in die **AARQ-apdu** aufzunehmen ist.

### 12.2.2 Behandlung der AARQ-apdu durch den Server

Bei Erhalt einer **AARQ-apdu** muss der Server die empfangene **AARQ-apdu** analysieren, bevor er den Aufbau einer Assoziation akzeptiert.

- Wenn der Server einen Fehler erkennt, der nicht mit der Authentifizierung zusammenhängt, muss er in den Komponenten **result** und **result-source-diagnostic** der **AARE-apdu** entsprechend den Festlegungen in Rec. ITU-T X.227 Angaben zum Fehler zurückgeben. In diesem Fall dürfen die **responder-acse-requirements** nicht in der **AARE-apdu** enthalten sein.
- Wenn die Komponente **mechanism-name** der **AARQ-apdu** nicht vorhanden ist, ist eine **AARE-apdu** mit der auf **rejected-permanent** gesetzten Komponente **result** und der auf **authentication-mechanism-name-required** gesetzten **result-source-diagnostic** zurückzugeben.
- Wenn das in der Komponente **authentication-Certificate** des **MMS-Authentication-value** bereitgestellte Zertifikat mit öffentlichem Schlüssel nicht gültig ist (abgelaufen, gesperrt usw.), dann muss ein P-ABORT ausgegeben werden.
- Wenn der Wert in der Komponente **time** des **MMS-Authentication-value** um mehr als 10 min von der lokalen Zeit abweicht (bei Ausgleich der Zeitverschiebung), dann muss ein P-ABORT ausgegeben werden.
- Wenn innerhalb von 10 min zweimal der gleiche Wert für **time** eingeht, dann muss ein P-ABORT ausgegeben werden.
- Wenn die in der Komponente **signature** des **MMS-Authentication-value** bereitgestellte Signatur ungültig ist, dann muss ein P-ABORT ausgegeben werden.

## 12.3 Behandlung des Assoziationsergebnisses (AARE-apdu)

### 12.3.1 Behandlung der AARE-apdu durch den Server

Wenn der Server eine Assoziationsanforderung annimmt, muss er eine Instanz des **MMS-Authentication-value** nach 0 generieren, die in die **AARE-apdu** aufzunehmen ist.

### 12.3.2 Behandlung der AARE-apdu durch den Client

Wenn der Client eine **AARE-apdu** empfängt, deren Komponente **result** auf **accepted** gesetzt ist, muss er die empfangene **AARE-apdu** analysieren.

- Wenn der Client einen Fehler erkennt, der nicht mit der Authentifizierung zusammenhängt, muss er eine **ABRT-apdu** mit der entsprechenden Diagnose zurückgeben.
- Wenn die Komponente **mechanism-name** der **AARE-apdu** nicht vorhanden ist, ist eine **ABRT-apdu** mit der auf **acse-service-provider** gesetzten Komponente **abort-source** und der auf **authentication-mechanism-name-required** gesetzten Komponente **abort-diagnostic** zurückzugeben.
- Wenn das in der Komponente **authentication-Certificate** des **MMS-Authentication-value** bereitgestellte Zertifikat mit öffentlichem Schlüssel nicht gültig ist (abgelaufen, gesperrt usw.), dann muss ein P-ABORT ausgegeben werden.

- d) Wenn der Wert in der Komponente **time** des **MMS-Authentication-value** um mehr als 10 min von der lokalen Zeit abweicht (bei Ausgleich der Zeitverschiebung), dann muss ein P-ABORT ausgegeben werden.
- e) Wenn innerhalb von 10 min zweimal der gleiche Wert für **time** eingeht, dann muss ein P-ABORT ausgegeben werden.
- f) Wenn die in der Komponente **signature** des **MMS-Authentication-value** bereitgestellte Signatur ungültig ist, dann muss ein P-ABORT ausgegeben werden.

## ABSCHNITT 5 – ENDE-ZU-ENDE-ANWENDUNGSSICHERHEITSPROFIL

### 13 Überblick und allgemeine Prinzipien

#### 13.1 Grundlegende Konzepte

Die Spezifikation aus diesem Abschnitt kommt dann zum Tragen, wenn zwei miteinander kommunizierende Einheiten beide Ende-zu-Ende-Anwendungssicherheit, kurz E2E-Sicherheit, unterstützen.

E2E-Sicherheit wird für OSI-Umgebungen bereitgestellt, d. h. für Umgebungen, in denen das Anwendungsprotokoll einen OSI-Protokollstapel nutzt, und für Anwendungsprotokolle, die einen reinen TCP/IP-Stapel nutzen.

In einer OSI-Umgebung wird mittels ACSE ein anfängliches E2E-Sicherheits-Quittungsverfahren ausgeführt. Wie die Ausführung eines etwaigen E2E-Sicherheits-Quittungsverfahrens in einer reinen TCP/IP-Umgebung aussehen würde, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351.

Für die E2E-Sicherheit in OSI-Umgebungen gelten einige spezifische Anforderungen, die in Abschnitt 0 festgelegt sind.

Innerhalb einer OSI-Umgebung werden Assoziationen zwischen zwei Anwendungsinstanzen mithilfe des Assoziationssteuerungsdienstelements (ACSE) aufgebaut und – entweder in einem ordnungsgemäßen oder einem abweichenden Verfahren – wieder beendet. Zum einfacheren Nachschlagen wird die formale ASN.1-Definition des ACSE-Protokolls in 0 wiedergegeben.

Innerhalb der OSI-Umgebung wird die in ACSE eingebettete Authentifizierungs- und Initialisierungsfunktion mithilfe eines ASN.1-EXTERNAL-Konstrukts in die ACSE-Benutzerdaten implementiert.

## 13.2 Zusammenhänge zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll

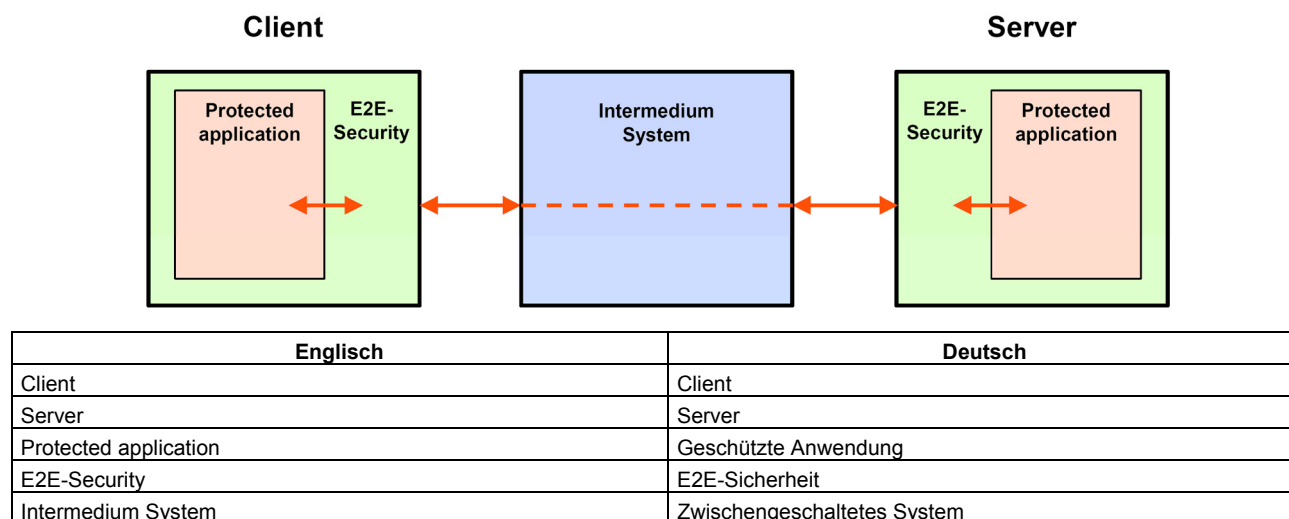


**Bild 4 – Zusammenhänge zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll**

In Bild sind die Zusammenhänge zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll dargestellt. Die geschützte Anwendung wird in gewisser Hinsicht als in die E2E-Sicherheit eingebettet angesehen, was bedeutet, dass die E2E-Sicherheit eine direkte Schnittstelle zur äußeren Umgebung hat und die geschützte Anwendung über die E2E-Sicherheit kommuniziert. Bei einer TCP/IP-Umgebung ergibt sich die Darstellung in Bild .

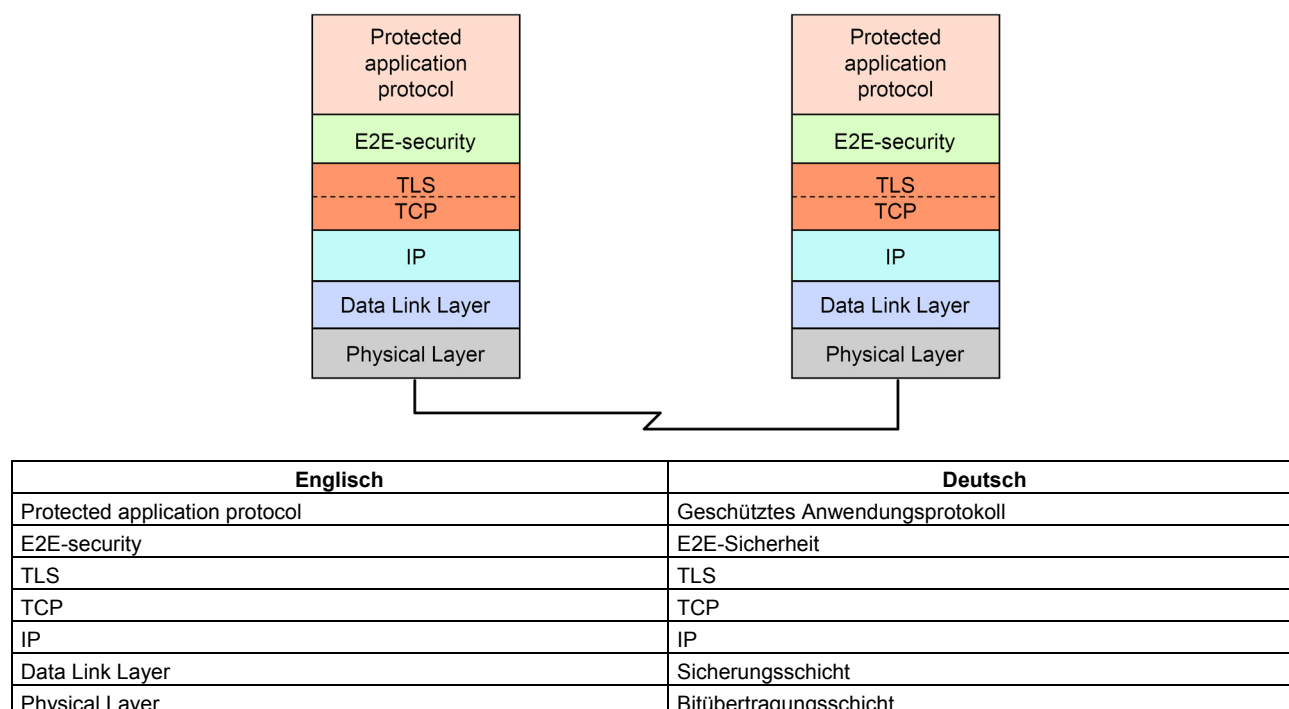


**Bild 5 – E2E-Sicherheit in einer TCP/IP-Umgebung**

Dieser Teil von IEC 62351 legt keine Dienstschnittstelle zwischen der E2E-Sicherheit und dem geschützten Anwendungsprotokoll fest, legt jedoch die Annahme zugrunde, dass eine Dienstdateneinheit (SDU) mit relevanten Informationen zwischen den Elementen ausgetauscht wird.

### 13.3 Schnittstelle zwischen E2E-Sicherheit und geschütztem Anwendungsprotokoll

#### 13.3.1 Allgemeines

Die abstrakte Syntax für das Protokoll zur Unterstützung der E2E-Sicherheit wird in Abstract Syntax Notation ONE (ASN.1) nach ISO/IEC 8824-1:2015 | Rec. ITU-T X.680 (2015) ausgedrückt. Die Verwendung von ASN.1 wird in 0 ausführlicher diskutiert.

Die abstrakte Syntax für das Protokoll wird auch in XML-Schema Definition (XSD) nach W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures 0 und nach W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes 0 ausgedrückt. Die Verwendung von XSD wird in 0 ausführlicher diskutiert.

#### 13.3.2 ASN.1 als Schemadefinition

Die formale ASN.1-Spezifikation für die E2E-Sicherheit befindet sich in 0.

```
End-to-End-Security {iso(1) standard(0) iec62351(62351)
part4(4) modules(0) version1(1)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

    <Entry PDU of protected application protocol>
    FROM <protected application protocol>;

ApplData ::= <Entry PDU of protected application protocol>
----
----
END
```

**Bild 6 – ASN.1-Schnittstelle zum geschützten Anwendungsprotokoll**

In Bild 6 ist dargestellt, wie das geschützte Anwendungsprotokoll in die abstrakte ASN.1-Syntax der E2E-Sicherheit eingebettet wird.

Die Eingangs-PDU eines geschützten Anwendungsprotokolls ist typischerweise eine Auswahl mehrerer PDU-Typen für verschiedene Zwecke.

ANMERKUNG – Beispielsweise ist die Eingangs-PDU für die MMS *mms pdu*, eine Auswahl von 14 verschiedenen PDU-Typen für verschiedene Zwecke.

Es gibt verschiedene Codierungsregeln für eine abstrakte ASN.1-Syntax. Dieser Teil von IEC 62351 fordert die Unterstützung der Basic Encoding Rules (BER) nach ISO/IEC 8825-1:2015 | Rec. ITU-T X.690 (2015). Wenn XML-Codierung erforderlich ist, dürfen darüber hinaus die XML-Codierungsregeln (XER) bzw. genauer die EXTENDED-XER nach ISO/IEC 8825-4:2015 | Rec. ITU-T X.693 (2015) unterstützt werden.

#### 13.3.3 XML-Schema Definition (XSD)

XSD ist eine alternative abstrakte Syntax, die für die XML-Codierung von PDUs verwendet werden darf. Wenn XML-Codierung erforderlich ist, muss entweder XSD oder ASN.1 EXTENDED-XER unterstützt werden.

Die XSD für die E2E-Sicherheit ist in 0 angegeben.

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oid:1.0.62351.4.0.3.1" xmlns:oss="http://www.oss.com/XSD"
xmlns:ns1="<name space>" targetNamespace="urn:oid:1.0.62351.4.0.3.1">
  <xsd:import namespace="<name space>" schemaLocation="mms.xsd"/>
  <xsd:complexType name="ApplData">
    <xsd:complexContent>
      <xsd:extension base="ns1:<Entry PDU>" />
    </xsd:complexContent>
  </xsd:complexType>
  ---
  ---
</xsd:schema>
```

Bild 7 – XSD-Schnittstelle zum geschützten Anwendungsprotokoll

In Bild 7 ist dargestellt, wie das geschützte Anwendungsprotokoll in die XSD der E2E-Sicherheit eingebettet wird.

Der `<name space>` ist der Namensraum für die XSD für das geschützte Anwendungsprotokoll und `<Entry PDU>` ist die Eingangs-PDU für das geschützte Anwendungsprotokoll.

## 14 Spezifische Anforderungen an eine OSI-Umgebung

### 14.1 Einleitung

Bei einer OSI-Umgebung gilt es einige Besonderheiten zu berücksichtigen, die nachfolgend zusammengefasst sind.

- Auf der Darstellungsschicht gelten einige besondere Anforderungen an den Darstellungskontext, die in 0 festgelegt sind.
- Die Quittungsbetriebsinformationen müssen in den ACSE-Benutzerdaten bereitgestellt werden:

Die ACSE-Benutzerdaten werden über den folgenden Datentyp definiert:

Association-information ::= SEQUENCE SIZE (1..MAX) OF EXTERNAL

Es ist nur eine einzige Instanz des Datentyps **EXTERNAL** erforderlich. Die Details zur Codierung des Datentyps **EXTERNAL** werden in 0 aufgeführt.

In einer OSI-Umgebung müssen die spezifischen Quittungsbetriebsinformationen in der Komponente **user-information** der **AARQ-apdu** und der **AARE-apdu** bereitgestellt werden. Wenn in einer **AARE-apdu** oder während der Datenübertragungsphase Fehler erkannt werden, dürfen Diagnoseinformationen in einer **ABRT-apdu** bereitgestellt werden. Dies wird unten näher betrachtet.

- Die Datenübertragungsinformationen müssen wie folgt bereitgestellt werden:

Fully-encoded-data ::= SEQUENCE OF PDV-list

Es ist nur eine einzige Instanz des Datentyps **PDV-list** erforderlich. Die Details zur Codierung des Datentyps **PDV-list** werden in 0 aufgeführt.

### 14.2 Zusätzliche Anforderungen an die Darstellungsschicht

Bei Verwendung des A-Plus-Sicherheitsprofils oder des AE-Plus-Sicherheitsprofils muss die folgende Spezifikation einer abstrakten Syntax gemeinsam mit einem zugehörigen **presentation-context-identifizier** aufgenommen werden (siehe 0):

e2eSecurityAS OBJECT IDENTIFIER ::=

```
{iso(1) standard(0) iec62351(62351) part4(4) abstract-syntax(1) e2eSecurity (2)
version1(1)}
```

### 14.3 Zusätzliche ACSE-Anforderungen

Die Komponenten `calling-authentication-value` und `mechanism-name` dürfen nicht in der `AARQ-apdu` enthalten sein. Die Komponenten `called-authentication-value` und `mechanism-name` dürfen nicht in der `AARE-apdu` enthalten sein.

Die E2E-Sicherheitsprofile erfordern nur den ACSE-Kernel.

Die Authentifizierungs- und Initialisierungsinformationen müssen in der Komponente `user-information` der `AARQ-apdu`, der `AARE-apdu` und der `ABRT-apdu` bereitgestellt werden, und nicht – wie bei der Unterstützung nach der ersten Ausgabe – in der Komponente `calling-authentication-value/responding-authentication-value`.

Die Informationen in dieser Komponente `user-information` bestehen aus drei Teilen:

- Initialisierungs- und Authentifizierungsinformationen, die in einem `ClearToken1` genannten Token bereitgestellt werden
- Initialisierungsinformationen, die von dem geschützten Anwendungsprotokoll (z. B. MMS) bereitgestellt werden. Wenn das geschützte Anwendungsprotokoll keine Initialisierungsinformationen liefert, liegen diese Informationen möglicherweise nicht vor.
- Eine digitale Signatur

Wenn das geschützte Anwendungsprotokoll MMS ist, ist der folgende Anwendungskontext zu verwenden:

```
e2eMmsAC OBJECT IDENTIFIER ::= { appl-context e2eMMS(1) }
```

Wenn für ein anderes OSI-basiertes geschütztes Anwendungsprotokoll E2E-Sicherheit benötigt wird, sollte dieses seinen Anwendungskontext selbst definieren.

### 14.4 Spezifische mit OSI zusammenhängende Protokollelemente

#### 14.4.1 OSI-Wrapping für den E2E-Sicherheits-Quittungsbetrieb

Zusätzlich zu dem allgemeinen E2E-Sicherheits-Quittungsbetrieb nach Abschnitt 0 muss eine Instanz des folgenden Wrapping-Datentyps enthalten sein:

```
E2E-SecAsso-OSI ::= [UNIVERSAL 8] SEQUENCE {
    indirect-reference          INTEGER,
    single-ASN1-type [0] EXPLICIT E2E-SecAsso }
```

Dieser Datentyp spiegelt die Codierung des Datentyps `EXTERNAL` entsprechend der Beschreibung in 0 wider.

ANMERKUNG 1 Als ASN.1 ist dies eigentlich ungültig, da das Tag `[UNIVERSAL 8]` in der abstrakten Notation nicht zulässig ist, es spiegelt jedoch die tatsächliche Codierung wider. Einige ASN.1-Tools haben diese strenge ASN.1-Beschränkung aufgehoben und akzeptieren die oben stehende Notation.

ANMERKUNG 2 Da die Spezifikation in 10.4.3 `EXPLICIT`-Codierung zugrunde legt, wird für die single-ASN-type-Komponenten hier `EXPLICIT`-Codierung festgelegt, wohingegen der Datentyp `E2E-SecAsso-OSI` in einem ASN.1-Modul enthalten ist, das `IMPLICIT`-Codierung als Standard festlegt.

Die Komponente `indirect-reference` legt den `Presentation-context-identifizier` nach Definition in 0 fest.

Der Datentyp `E2E-SecAsso` ist eine Spezifikation des allgemeinen Quittungsbetriebs nach 0.

#### 14.4.2 OSI-Wrapping für die E2E-Sicherheits-Datenübertragung

Bei der Datenübertragung in der OSI-Umgebung wird eine MMS-PDU gemeinsam mit ICV-Informationen in einer TD-PPDU übertragen, wie in ISO/IEC 8823-1 | Rec. ITU-T X.226 definiert. Sie wird als Instanz des Datentyps `user-data` in einer TD-PPDU übertragen.

Zusätzlich zu der Spezifikation der allgemeinen E2E-Sicherheits-Datenübertragung muss eine Instanz des folgenden Wrapping-Datentyps enthalten sein:

```
SecTransfer-OSI ::= SEQUENCE {  
    presentation-context-identifier INTEGER,  
    single-ASN1-type [0] EXPLICIT SecTransfer }
```

Der `presentation-context-identifier` ist der oben in 0 erwähnte.

Der Datentyp `secTransfer` ist eine Spezifikation der allgemeinen Datenübertragung nach Definition in 0.

### 15 Assoziationsmanagement

#### 15.1 Allgemeines Konzept

Das Quittungsverfahren wird für den Aufbau einer Assoziation (Verbindung) zwischen zwei Anwendungsinstanzen verwendet, wobei möglicherweise weitere Anwendungsinstanzen zwischengeschaltet sind.

ANMERKUNG 1 Der Begriff „Assoziation“ (en: association) entstammt der OSI-Umgebung. Hier wird er jedoch auch auf Nicht-OSI-Umgebungen bezogen.

ANMERKUNG 2 Der Begriff „Anwendungsinstanz“ (en: application entity) entstammt OSI-Umgebung. Hier wird er jedoch auch auf Nicht-OSI-Umgebungen bezogen.

#### 15.2 Allgemeine Syntax

Eine Instanz des Datentyps `E2E-security-handshake` liefert den Eingangspunkt zu den verschiedenen Datentypen des Assoziationsmanagements.

```
E2E-secAsso ::= CHOICE {  
    handshake [0] Handshake,  
    applReject [1] ApplicationReject,  
    secReject [2] HandshakeSecReject,  
    dtAbort [3] DtSecAbort,  
    ... }
```

Der Datentyp `E2E-secAsso` umfasst die folgenden Alternativen:

- Eine Instanz des Datentyps `Handshake` wird von dem Client oder Server bei der Beteiligung an einem Assoziationsmanagementaustausch verwendet. Dies wird in 0 ausführlicher diskutiert.
- Eine Instanz des Datentyps `HandshakeApplReject` wird von dem geschützten Anwendungsprotokoll verwendet, um die vom Client vorgeschlagenen Initialisierungsparameter zurückzuweisen. Dies wird in 0 ausführlicher diskutiert.
- Eine Instanz des Datentyps `HandshakeSecReject` muss vom Server in ein negatives Assoziationsergebnis aufgenommen werden, das auf Probleme bei mit der Sicherheit zusammenhängenden Informationen zurückzuführen ist. Dies wird in 0 ausführlicher diskutiert.
- Eine Instanz des Datentyps `DtSecAbort` muss von einem Kommunikationspartner aufgenommen werden, wenn während der Datenübertragungsphase ein Sicherheitsproblem auftritt. Dies wird in 0 ausführlicher diskutiert.

## 15.3 Anforderung und Annahme des Quittungsbetriebs

### 15.3.1 Allgemeines

Der Client darf eine neue Assoziation initialisieren, indem er eine Instanz des Datentyps **HandshakeRequest** in eine Assoziationsanforderung aufnimmt. Ein Server darf eine neue Assoziation annehmen, indem er eine Instanz des Datentyps **HandshakeRequest** in ein Assoziationsergebnis aufnimmt.

```
Handshake ::= SEQUENCE {  
    token1      [0] ClearToken1,  
    applInit    [1] ApplData OPTIONAL,  
    sign        [2] Signature,  
    ... }
```

Die PDU **HandshakePDU** deckt alle Fälle ab, in denen das geschützte Anwendungsprotokoll potenziell am Aufbau der Assoziation beteiligt ist. Weiterhin deckt sie die Zurückweisung des Assoziationsaufbaus durch das geschützte Anwendungsprotokoll ab.

Der Datentyp **HandshakePDU** umfasst die folgenden drei Komponenten:

- a) Die Komponente **token1** muss eine Instanz des Datentyps **ClearToken1** nach 0 enthalten.
- b) Wenn die Komponente **applInit** vorhanden ist, muss sie eine Instanz des zutreffenden Datentyps aus dem geschützten Anwendungsprotokoll enthalten.
- c) Die Komponente **sign** muss die Signatur nach 0 enthalten. Die Signatur muss über den Inhalt der Komponenten **token1** und **applInit** generiert werden.

Ein Client muss den Datentyp **Handshake** verwenden, um den Aufbau einer Assoziation anzufordern.

Wenn das unterstützte geschützte Anwendungsprotokoll MMS ist, muss eine Instanz des Datentyps **Initiate-RequestPDU** für den Datentyp **ApplData** aufgenommen werden.

Ein Server muss den Datentyp **Handshake** verwenden, um den Aufbau einer Assoziation anzunehmen.

Wenn das unterstützte geschützte Anwendungsprotokoll MMS ist, muss eine Instanz des Datentyps **Initiate-ResponsePDU** aufgenommen werden.

### 15.3.2 OSI-spezifische Überlegungen

In einer OSI-Umgebung muss der Client einen **Handshake**-Datenwert in die Komponente **user-information** der **AARQ-apdu** einfügen.

Der Server muss innerhalb der **AARE-apdu** Folgendes einfügen:

- a) einen **Handshake**-Datenwert in die Komponente **user-information**;
- b) eine Komponente **result** mit dem Wert **accepted**;
- c) eine Komponente **result-source-diagnostic** mit dem Wert **null**;

### 15.3.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Wie ein Datenwert des Quittungsbetriebs (Handshake) in einer Nicht-OSI-Umgebung behandelt wird, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Die jeweilige Spezifikation muss von dem geschützten Anwendungsprotokoll bereitgestellt werden.

## 15.4 Zurückweisung der Assoziation durch das geschützte Anwendungsprotokoll

### 15.4.1 Allgemeines

Der Datentyp `ApplicationReject` hat die folgende Syntax:

```
ApplicationReject ::= SEQUENCE {  
    token3      [0] ClearToken3,  
    applData    [1] ApplData OPTIONAL,  
    sign        [2] Signature,  
    ... }
```

Ein Server darf einen `ApplicationReject`-Datenwert verwenden, um den Aufbau einer Assoziation wegen von dem geschützten Anwendungsprotokoll festgestellter Probleme zurückzuweisen. Er darf auch dann verwendet werden, wenn ein Client oder ein Server während der Datenübertragungsphase auf einen Fehler im geschützten Anwendungsprotokoll stößt. Er umfasst die folgenden Komponenten:

- a) Die Komponente `token3` muss einen `ClearToken3`-Datenwert nach 0 enthalten.
- b) Wenn die Komponente `applData` vorhanden ist, muss sie einen `ApplData`-Datenwert mit Informationen zum Grund für die Zurückweisung enthalten.
- c) Die Komponente `sign` muss einen `Signature`-Datenwert nach 0 enthalten. Die Signatur muss über den Inhalt der Komponenten `token3` und `applData` generiert werden.

### 15.4.2 OSI-spezifische Überlegungen

Wenn das geschützte Anwendungsprotokoll im Falle einer Assoziationszurückweisung eine Dienstdateneinheit (SDU) zurückgibt, deren Inhalt einer `AARE-pdu` mit auf `rejected-permanent` oder `rejected-transient` gesetzter Komponente `result` entspricht, oder wenn es im Falle eines Fehlschlagens der geschützten Anwendung während der Datenübertragungsphase eine SDU zurückgibt, deren Inhalt einer `ABRT-apdu` entspricht, dann gilt:

- a) Wenn die Komponente `user-information` in der SDU vorhanden ist, muss die Information in der Komponente `user-information` den Wert des Datentyps `AppDate` annehmen; anschließend ist die Komponente `token3` als Präfix voranzustellen und die Komponente `sign` hinten anzuhängen.
- b) Wenn die Komponente `user-information` in der SDU nicht vorhanden ist, muss eine `E2E-SecAsso-OSI`-Instanz mit der Alternative `applReject` der `E2E-secAsso`-Instanz in die Komponente `information` ohne die Komponente `applInit` eingefügt werden.

### 15.4.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Wie eine Assoziation durch ein geschütztes Anwendungsprotokoll zurückgewiesen oder abgebrochen wird, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Die entsprechenden Spezifikationen müssen von dem geschützten Anwendungsprotokoll bereitgestellt werden.

## 15.5 Assoziationszurückweisung aufgrund von Sicherheitsproblemen

### 15.5.1 Allgemeines

Der Datentyp `HandshakeSecReject` darf in den beiden folgenden Fällen verwendet werden:

- a) Der Server muss eine neue Assoziationsanforderung zurückweisen, wenn er Probleme in einem der Elemente des E2E-Sicherheitsprotokolls feststellt.
- b) Der Client muss eine Assoziation abbrechen, wenn er eine Assoziationsannahme mit ungültigen E2E-Sicherheitsprotokollelementen empfängt.

Der Datentyp `HandshakeSecReject` hat die folgende Syntax:

```
HandshakeSecReject ::= SEQUENCE {
    token3      ClearToken3,
    diag        HandshakeDiagnostics,
    sign        Signature,
    ... }
```

Der Datentyp `HandshakeSecReject` umfasst die folgenden Komponenten:

- Die Komponente `token3` muss eine Instanz des Datentyps `ClearToken3` nach 0 enthalten.
- Die Komponente `diag` muss eine Instanz des Datentyps `HandshakeDiagnostics` nach 0 mit dem zutreffenden Diagnosecode enthalten.
- Die Komponente `sign` muss die Signatur nach 0 enthalten. Die Signatur muss über den Inhalt der Komponenten `token3` und `diag` generiert werden.

### 15.5.2 OSI-spezifische Überlegungen

Die Abbildung auf das ACSE-Protokoll hängt davon ab, ob die Assoziation vom Server zurückgewiesen oder vom Client abgebrochen wird.

- Wenn der Server eine Assoziationsanforderung zurückweist – außer bei einem Protokollfehler –, muss eine **AARE-apdu** zurückgegeben werden, für die Folgendes gilt:
  - Es muss eine **E2E-SecAsso-OSI**-Instanz mit der Alternative `secReject` der **E2E-secAsso**-Instanz in die Komponente `user-information` der **AARE-apdu** eingefügt werden. Die Komponente `diag` der **HandshakeSecReject**-Instanz muss den zutreffenden Wert annehmen.
  - Die Komponente `result` muss den Wert `rejected-permanent` annehmen.
  - Die Komponente `result-associated-diagnostic` muss den Wert `null` annehmen.
- Wenn der Client eine Assoziationsannahme zurückweist oder der Server eine Assoziationsanforderung aufgrund eines Protokollfehlers zurückweist, muss eine **ABRT-apdu** zurückgegeben werden, für die Folgendes gilt:
  - Es muss eine **E2E-SecAsso-OSI**-Instanz mit der Alternative `secReject` der **E2E-secAsso**-Instanz in die Komponente `user-information` der **ABRT-apdu** eingefügt werden. Die Komponente `diag` der **HandshakeSecReject**-Instanz muss den zutreffenden Wert annehmen.
  - Die Komponente `abort-source` nimmt den Wert `acse-service-user` an.
  - Die Komponente `abort-diagnostic` ist nicht vorhanden.

### 15.5.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Die Festlegung von Details hinsichtlich der Frage, wie ein geschütztes Anwendungsprotokoll Zurückweisungsinformationen nach 0 überträgt, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Diesbezügliche Festlegungen müssen im Rahmen der Spezifikation des geschützten Anwendungsprotokolls bereitgestellt werden.

## 15.6 Sicherheitsabbruch der Datenübertragung

### 15.6.1 Allgemeine Syntax

Wenn während der Datenübertragungsphase innerhalb der E2E-Sicherheitsunterstützung ein Sicherheitsproblem festgestellt wird, wird ein `DtSecAbort`-Datenwert ausgegeben. Die Integrität und Authentifizierung wird nicht durch einen ICV, sondern durch eine digitale Signatur bereitgestellt.

Der Datentyp `DtSecAbort` hat die folgende Syntax:

```
DtSecAbort ::= SEQUENCE {
    token3      ClearToken3,
    diag        DtDiagnostics,
```

```
sign      Signature,  
... }
```

Der Datentyp **DtSecAbort** umfasst die folgenden Komponenten:

- a) Die Komponente **token3** muss eine Instanz des Datentyps **ClearToken3** nach 0 enthalten.
- b) Die Komponente **diag** muss eine Instanz des Datentyps **DtDiagnostics** nach 0 mit dem zutreffenden ausgewählten Diagnosecode enthalten.
- c) Die Komponente **sign** muss die Signatur nach 0 enthalten. Die Signatur muss über die Werte der Komponenten **token3** und **diag** generiert werden.

### 15.6.2 OSI-spezifische Überlegungen

Es muss eine **ABRT-apdu** zurückgegeben werden, für die Folgendes gilt:

- a) Es muss eine **E2E-SecAsso-OSI**-Instanz mit der Alternative **dtAbort** der **E2E-secAsso**-Instanz in die Komponente **user-information** der **ABRT-apdu** eingefügt werden. Die Komponente **diag** der **DtSecAbort**-Instanz muss den zutreffenden Wert annehmen.
- b) Die Komponente **abort-source** muss den Wert **acse-service-user** annehmen.
- c) Die Komponente **abort-diagnostic** darf nicht vorhanden sein.

### 15.6.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Die Festlegung von Details hinsichtlich der Frage, wie ein geschütztes Anwendungsprotokoll Abbruchinformationen nach 0 überträgt, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Diesbezügliche Festlegungen müssen im Rahmen der Spezifikation des geschützten Anwendungsprotokolls bereitgestellt werden.

## 16 Datenübertragungsphase

### 16.1 Normale Datenübertragung

#### 16.1.1 Allgemeine Syntax

Der erfolgreiche Aufbau einer Assoziation markiert den Eintritt in die Datenübertragungsphase. Diese endet, wenn die Assoziation beendet wird.

Der Datentyp **secTransfer** hat die folgende Syntax:

```
SecTransfer ::= SEQUENCE {  
    token2      ClearToken2,  
    applData    CHOICE {  
        clear      ApplData,  
        encr       Encrypted-ApplData,  
        ... },  
    ...,  
    ...,  
    auth        Authenticator }
```

**Encrypted-ApplData** ::= OCTET STRING

Der Datentyp **secTransfer** umfasst die folgenden Komponenten:

- a) Die Komponente **token2** muss einen **ClearToken2**-Datenwert nach 0 enthalten.
- b) Die Komponente **applData** hat zwei Alternativen:
  - 1) Die Alternative **clear** muss den vom geschützten Anwendungsprotokoll festgelegten Datenwert enthalten.

- 2) Die Alternative **encr** muss einen verschlüsselten, vom geschützten Anwendungsprotokoll festgelegten Datenwert enthalten.
- c) Die Komponente **auth** muss den Integritätsprüfwert (ICV) nach Definition in 0 enthalten. Der ICV muss über den Wert der Komponenten **token2** und **appData** generiert werden.

### 16.1.2 OSI-spezifische Überlegungen

In einer OSI-Umgebung muss ein **secTransfer-OSI**-Datenwert in die Komponente **single-ASN1-type** des **user-data**-Datenwertes nach 0 eingefügt werden.

### 16.1.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Die Festlegung von Details zu dem **secTransfer**-Datenwert für eine Nicht-OSI-Umgebung fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Diesbezügliche Festlegungen müssen im Rahmen der Spezifikation des geschützten Anwendungsprotokolls bereitgestellt werden.

## 16.2 Abbruch durch geschütztes Anwendungsprotokoll

### 16.2.1 Allgemeines

Wenn die geschützte Anwendung einen Abbruch der Assoziation für nötig hält, wird eine Instanz des Datentyps **ApplicationReject** nach 0 verwendet. Diese sollte Informationen zu dem Grund für den Abbruch zurückgeben. Diese Informationen sind dann in der Komponente **appData** des **ApplicationReject**-Datenwertes bereitzustellen; anschließend ist die Komponente **token3** als Präfix voranzustellen und die Komponente **sign** hinten anzuhängen, sodass ein **HandshakeAppReject**-Datenwert entsteht.

### 16.2.2 OSI-spezifische Überlegungen

Wenn das geschützte Anwendungsprotokoll eine Dienstdateneinheit zurückgibt, deren Inhalt einer **ABRT-pdu** entspricht, dann muss die Information in der Komponente **user-information** den **ApplicationReject**-Datenwert annehmen.

### 16.2.3 Spezifische Überlegungen zu Nicht-OSI-Umgebungen

Die Festlegung von Details hinsichtlich der Frage, wie der **ApplicationReject**-Datenwert in einer Nicht-OSI-Umgebung zurückgegeben wird, fällt nicht in den Anwendungsbereich dieses Teils von IEC 62351. Diesbezügliche Festlegungen müssen im Rahmen der Spezifikation des geschützten Anwendungsprotokolls bereitgestellt werden.

## 17 ClearToken-Datentypen

### 17.1 Der Datentyp ClearToken1

#### 17.1.1 Allgemeine Syntax

Ein **clearToken1**-Wert liefert Informationen über den für die sichere Kommunikation zwischen zwei Kommunikationspartnern benötigten Sicherheitskontext. Er ist in Assoziationsanforderungen und -annahmen enthalten.

Der Datentyp **clearToken1** hat die folgende Syntax:

```
ClearToken1 ::= SEQUENCE {
    sigAlg      AlgorithmIdentifier {{SupportedSignatureAlgorithms}},
    dhKey       DiffieHellmanSet,
    time        TimeStamp,
```

```
icvAlgID      SET SIZE (1..MAX) OF
oid           ALGORITHM.&id ({Supported-ICV-Algorithms}),
confParams    ConfidentialityParms,
pkCert        PKCert,
certPath      CertPath OPTIONAL,
attCert       ACert OPTIONAL,
... }
```

TimeStamp ::= GeneralizedTime

PKCert ::= OCTET STRING  
-- (CONTAINING Certificate ENCODED BY der)

ACert ::= OCTET STRING  
-- (CONTAINING AttributeCertificate ENCODED BY der)

In der folgenden Objektmenge werden die von diesem Teil von IEC 62351 anerkannten ICV-Algorithmen aufgelistet.

Supported-ICV-Algorithms ALGORITHM ::= { hmacWithSHA256 | eas256-GCM, ... }

Der Datentyp `clearToken1` umfasst die folgenden Komponenten:

- Die Komponente `sigAlg` muss den Signaturalgorithmus nach 0 enthalten, der für die digitale Signatur zu verwenden ist.
- Die Komponente `dhKey` muss die Verwendung des Diffie-Hellman-Algorithmus nach 0 festlegen.
- Die Komponente `time` ist die generalisierte GMT-(UTC)-Zeit, zu der der `Handshake`-Datenwert erstellt wurde.
- Die K

omponente `icvAlgID` in der Assoziationsanforderung muss eine Liste der ICV-Algorithmus-Objektbezeichner enthalten, die vom Client angenommen werden. Der Server muss einen dieser Algorithmen auswählen und diesen Algorithmus im Assoziationsergebnis kenntlich machen.

- Die Komponente `confParams` muss einen `ConfidentialityParms`-Datenwert nach 0 enthalten.
- Die Komponente `pkCert` muss das Zertifikat mit öffentlichem Schlüssel der Endeinheit des Absenders enthalten.
- Wenn die Komponente `certPath` vorhanden ist, muss sie einen `CertPath`-Datenwert nach 0 enthalten. Sie darf fehlen, wenn die Sequenz der CA-Zertifikate anderweitig bereitgestellt wird oder wenn das Zertifikat mit öffentlichem Schlüssel der Endeinheit direkt von einem vom Empfänger anerkannten Vertrauensanker ausgestellt wird.
- Wenn die Komponente `attCer` vorhanden ist, muss sie ein Attributzertifikat enthalten, das Zugangssteuerungsinformationen bereitstellt.

### 17.1.2 Unterstützte Signaturalgorithmen

Der folgende Signaturalgorithmus muss unterstützt werden

```
SupportedSignatureAlgorithms ALGORITHM ::= {
  sha256WithRSAEncryptionAlgorithm |
  ecdsa-with-SHA256-Algorithm,
  ... }
```

`SupportedSignatureAlgorithms` ist eine Objektmenge, welche die unterstützten Signaturalgorithmen festlegt. Aufgrund der Erweiterungspunkte ( ... ) wird ein ASN.1-Tool einen beliebigen kryptografischen Algorithmus akzeptieren, unabhängig davon, ob er einen Signaturalgorithmus kennzeichnet oder nicht. Die Erweiterungspunkte dürfen im Rahmen einer Spezifikation, auf die verwiesen wird, oder im Rahmen einer Vereinbarung der Implementierer entfernt oder durch Kennungen zusätzlicher Signaturalgorithmen ersetzt werden.

ANMERKUNG 1 Die aufgeführten Signaturalgorithmen dürfen auch ersetzt werden, wenn die aufgeführten Algorithmen zu einem späteren Zeitpunkt nicht mehr als hinreichend sicher angesehen werden.

Die folgenden Kurven müssen für den **ecdsa-with-SHA256-Algorithm** unterstützt werden:

**SupportedCurves** OBJECT IDENTIFIER ::= { **secp256r1** | **brainpoolP256r1**, ... }

**SupportedCurves** ist eine Wertemenge, welche die unterstützten Kurven festlegt. Aufgrund der Erweiterungspunkte ( ... ) wird ein ASN.1-Tool einen beliebigen Objektbezeichner akzeptieren, unabhängig davon, ob er eine elliptische Kurve kennzeichnet oder nicht. Die Erweiterungspunkte dürfen im Rahmen einer Spezifikation, auf die verwiesen wird, oder im Rahmen einer Vereinbarung der Implementierer entfernt oder durch Kennungen zusätzlicher elliptischer Kurven ersetzt werden.

ANMERKUNG 2 Die aufgeführten Kurvenbezeichner dürfen auch ersetzt werden, wenn die aufgeführten Kurven zu einem späteren Zeitpunkt nicht mehr als hinreichend sicher angesehen werden.

### 17.1.3 Diffie-Hellman-Menge

Der Datentyp **DiffieHellmanSet** hat die folgende Syntax:

```
DiffieHellmanSet ::= SEQUENCE {
    groupId      INTEGER,      -- Group identifier
    dhPublicKey  OCTET STRING (SIZE(1..256)),
    nonce        OCTET STRING,
    ... }
```

Der Datentyp **DiffieHellmanSet** umfasst die folgenden Komponenten:

- a) Die Komponente **groupId** wird für den Diffie-Hellman-Schlüsselaustausch verwendet.
  - 3) Wenn kryptografische RSA-Algorithmen verwendet werden, muss diese Komponente die Gruppennummer für ein Paar aus Primzahl (p) und Generator (g) festlegen, entsprechend der Definition in IETF RFC 3526. Die 2 048-Bit-MODP-Gruppe mit der Gruppen-ID 14 muss unterstützt werden.
  - 4) Wenn kryptografische ECDH-Algorithmen verwendet werden, muss diese Komponente die Gruppen-ID 23 (die Kurve **secp256r1**) festlegen, entsprechend der Definition in IETF RFC 5114. Optional darf die Gruppen-ID 28 (die Kurve **BrainpoolP256r1**) verwendet werden (siehe 0 für die Definition dieser beiden Kurven).

Die Komponente **groupId** muss im Ergebnis den gleichen Wert aufweisen wie in der Anforderung. Bei einem abweichenden Wert muss ein Sicherheitsereignis gemeldet werden („Warnung: falsche DG-Gruppe ausgewählt“).

- b) Die Komponente **dhPublicKey** muss den öffentlichen Diffie-Hellman-Schlüssel des Absenders festlegen. Für jeden neuen Assoziationsaufbau muss ein neues, anderes Paar aus privatem und öffentlichem Diffie-Hellman-Schlüssel generiert werden. Für die Dauer der Assoziation muss der öffentliche Diffie-Hellman-Schlüssel des Servers von beiden Parteien bereitgehalten werden und der Server muss seinen privaten Diffie-Hellman-Schlüssel für eine spätere Erneuerung symmetrischer Schlüssel bereithalten (siehe 0).
- c) Die Komponente **nonce** muss für jedes Vorkommen eine neue Zufallswertinstanz beinhalten. Der Wert in der Assoziationsanforderung (oder PDU in der Datenübertragungsphase – siehe 0). IETF RFC 2631 legt einen Wert von 512 Bit (64 Oktette) fest.

Das Ergebnis eines Diffie-Hellman-Austauschs ist ein gemeinsames Geheimnis Z, das die Eingabe für die Schlüsselableitung zur Erzeugung symmetrischer Schlüssel für die Verschlüsselung und die Nachrichtenintegrität liefert.

### 17.1.4 Ableitung der gemeinsamen Schlüssel

Für das A-Plus-Sicherheitsprofil muss zwecks Erzeugung eines Integritätsprüfwertes für jede Richtung ein gemeinsamer symmetrischer Schlüssel erzeugt werden. Für das AE-Plus-Sicherheitsprofil ist für die Ver-

schlüsselung des Inhalts ein zusätzlicher gemeinsamer symmetrischer Schlüssel für jede Richtung erforderlich.

Als Schlüsselableitungsfunktion legt dieser Teil von IEC 62351 die Verwendung einer pseudozufälligen Funktion (en: pseudorandom function; PRF) fest, wobei diese Funktion in Form der Hash-Funktion HMAC-SHA-256 bereitgestellt wird.

Ein generierter Schlüssel ist der HMAC-SHA-256 der Verkettung der folgenden Komponenten unter Verwendung des Geheimnisses *Z* aus dem Diffie-Hellman-Verfahren als Schlüssel für die HMAC-SHA-256-Operation:

- eine als hexadezimale Zeichenkette geschriebene Konstante;
- der Wert der Komponente *nonce* des Wertes des Datentyps *DiffieHellmanSet* ohne Tag und Längfelder.

Bei gemeinsamen Schlüsseln für die Überprüfung der Integrität und der Authentifizierung muss die Konstante 0x2AD01C64 sein (basierend auf den Dezimalziffern von  $e = 2,718281828$ ).

Bei Schlüsseln für die Verschlüsselung des Inhalts muss die Konstante 0x54655307 sein (basierend auf den Dezimalziffern von  $\pi = 3,1415926535$ ).

Dies führt zu den folgenden Operationen:

- Integrity key  $IK_{Initiator} := PRF(DH_{Secret}, Constant_{Integrity} || nonce_{Requestor})$
- Integrity key  $IK_{Responder} := PRF(DH_{Secret}, Constant_{Integrity} || nonce_{Acceptor})$
- Encryption key  $IK_{Initiator} := PRF(DH_{Secret}, Constant_{Encryption} || nonce_{Requestor})$
- Encryption key  $IK_{Responder} := PRF(DH_{Secret}, Constant_{Encryption} || nonce_{Acceptor})$

Bei Schlüsseln, die in der Richtung vom Client zum Server verwendet werden, muss die Komponente *nonce* derjenigen aus der Assoziationsanforderung entsprechen und bei Schlüsseln, die in der Richtung vom Server zum Client verwendet werden, muss die Komponente *nonce* derjenigen aus dem Assoziationsergebnis entsprechen.

### 17.1.5 Vertraulichkeitsparameter

Der Datentyp *ConfidentialityParms* hat die folgende Syntax:

```
ConfidentialityParms ::= SEQUENCE {  
    conf          BIT STRING {  
        tlsProtected      (0), -- specifies IEC 62351-3  
        applProtected     (1), -- end-to-end application level enc  
        vpnOrIPsec        (2) }, -- out-of-current scope  
    encryption    SET SIZE (1..MAX) OF  
        oid          ALGORITHM.&id,  
    ... }  
Supported-encrypt-algorithms ALGORITHM ::= { aes256-CBC | aes256-GCM, ... }
```

In der Informationsobjektmenge *Supported-encrypt-algorithms ALGORITHM* wird nur ein einziger für diesen Teil von IEC 62351 zu verwendender symmetrischer Verschlüsselungsalgorithmus benannt.

**ANMERKUNG** Aufgrund der Erweiterungspunkte ( ... ) wird ein ASN.1-Tool einen beliebigen kryptografischen Algorithmus akzeptieren, unabhängig davon, ob es sich um einen symmetrischen kryptografischen Algorithmus handelt oder nicht. Die Erweiterungspunkte dürfen im Rahmen einer Spezifikation, auf die verwiesen wird, oder im Rahmen einer Vereinbarung der Implementierer entfernt oder je nach Anforderungen der jeweiligen Umgebung durch zusätzliche symmetrische Verschlüsselungsalgorithmen ersetzt werden.

Ein Wert des Datentyps *confidentialityParms* umfasst die folgenden Komponenten: