

DIN EN 50090-3-4

ICS 97.120

**Elektrische Systemtechnik für Heim und Gebäude (ESHG) –
Teil 3-4: Informationssicherheit auf Anwendungsschicht, Dienste,
Konfiguration und Ressourcen;
Deutsche Fassung EN 50090-3-4:2017**

Home and Building Electronic Systems (HBES) –
Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security
Resources;
German version EN 50090-3-4:2017

Systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) –
Partie 3-4: Spécification des KNX S AL, Service sécurisé, configuration sécurisée et
Ressources en matière de sécurité;
Version allemande EN 50090-3-4:2017

Gesamtumfang 67 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-06-12 angenommene Europäische Norm als DIN-Norm ist 2018-04-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 50090-3-4:2017-06.

Für dieses Dokument ist das nationale Arbeitsgremium K 716 „Elektrische Systemtechnik für Heim und Gebäude (ESHG)“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (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.

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.

Elektrische Systemtechnik für Heim und Gebäude (ESHG) –
Teil 3-4: Informationssicherheit auf Anwendungsschicht, Dienste, Konfiguration
und Ressourcen

Home and Building Electronic Systems (HBES) –
Part 3-4: Secure Application Layer, Secure
Service, Secure configuration and security
Resources

Systèmes électroniques pour les foyers
domestiques et les bâtiments (HBES) –
Partie 3-4 : Spécification des KNX S AL, Service
sécurisé, configuration sécurisée et Ressources
en matière de sécurité

Diese Europäische Norm wurde von CENELEC am 2017-06-12 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 50090-3-4:2017 D

Inhalt

	Seite
Europäisches Vorwort.....	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe und Abkürzungen	6
3.1 Begriffe	6
3.2 Abkürzungen	8
4 Allgemeine Einführung (informativ)	8
4.1 Allgemeines	8
4.2 Allgemeiner Überblick.....	12
5 Spezifikation	14
5.1 Stack und Kommunikation.....	14
5.2 Ressourcendefinition oder verwendete Ressourcen.....	55
Anhang A (informativ) Verwendung des CCM-Modus.....	56
A.1 Ziel	56
A.2 Definitionen.....	56
A.3 CCM-Operation	56
Anhang B (informativ) Beispiele – Vollständige Codierung einer sicheren ESHG-APDU.....	61
B.1 Allgemeines	61
B.2 S-A_Data-PDU	61
B.3 S-A_Data-PDU	62
B.4 S-A_Sync.req	63
B.5 S-A_Sync.res.....	64
Literaturhinweise.....	65
 Bilder	
Bild 1 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der nur eine Authentifizierung erfordert.....	10
Bild 2 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der sowohl eine Authentifizierung als auch Vertraulichkeit erfordert	11
Bild 3 – Anordnung der ESHG-Datensicherheit im ESHG-Stack	13
Bild 4 – Anordnung der S-AL in der Application Layer	15
Bild 5 – Sichere APDU (Beispiel für TP1).....	16
Bild 6 – Format von B_0	17
Bild 7 – Format des Feldes „TPCI/APCI _{Sec} “ in B_0	17
Bild 8 – Format von Ctr _j	18
Bild 9 – Sichere Daten bei ausschließlicher Verwendung von Authentifizierung (Beispiel für TP1)	18
Bild 10 – Sichere Daten bei Verwendung von Authentifizierung und Vertraulichkeit.....	20

	Seite
Bild 11 – Format der verschlüsselten sicheren APDU (informativ)	22
Bild 12 – Sicherheitssteuerungsfeld	23
Bild 13 – Tool-Zugriff	23
Bild 14 – Format der Sequenznummer	25
Bild 15 – Format der S-A_Sync_Req-PDUs (Beispiel – Feld „SCF“ mit gesetztem Tool-Schlüssel und gesetzter SBC-Kennzeichnung).....	28
Bild 16 – Format der S-A_Sync_Res-PDU (Beispiel – Feld „SCF“ mit gesetztem Tool-Schlüssel und gesetzter SBC-Kennzeichnung).....	30
Bild 17 – Interaktivität der Application Layer für Dienste, die nicht fernbestätigt wurden	33
Bild 18 – Interaktivität der Application Layer für Dienste, die fernbestätigt wurden	34
Bild 19 – Handhabung der Dienstprimitiven „T_Data_Group.ind“ durch die S-AL (informativ).....	36
Bild 20 – Handhabung der Dienstprimitiven „T_Data_Group.req“ durch die S-AL (informativ)	37
Bild 21 – Handhabung der Dienstprimitiven „T_Data_Tag_Group.ind“ durch die S-AL (informativ)	38
Bild 22 – Handhabung der Dienstprimitiven „T_Data_Tag_Group.req“ durch die S-AL (informativ)	39
Bild 23 – Handhabung der Dienstprimitiven „T_Data_Individual.ind/.con“ und „T_Data_Connected.ind/.con“ durch die S-AL (informativ)	41
Bild 24 – Handhabung der Dienstprimitiven „T_Data_Individual.req“ und „T_Data_Connected.req“ durch die S-AL (informativ)	42
Bild 25 – Hohe Zahl an Verbindungen mit vielen unterschiedlichen Berechtigungen verursachen umfangreiche Definitionsdaten.....	47
Bild 26 – Durch die Einführung von Rollen wird die Anzahl der unterschiedlichen Berechtigungsdefinitionen für jeden Datenpunkt reduziert	48
Bild 27 – Beispiel für Rollen in der Tabelle mit Punkt-zu-Punkt-Schlüsseln	50
Bild A.1 – Blockdiagramm für AES-128 mit CBC-MAC	57
Bild A.2 – Blockdiagramm für AES-CTR-Modus	59
Tabellen	
Tabelle 1 – Sicherheitsmerkmale der ESHG-Schichten (informativ)	13
Tabelle 2 – Sicherheitsalgorithmusbezeichner.....	23
Tabelle 3 – System-Broadcast-Kennzeichnung	24
Tabelle 4 – Setzen der SBC-Kennzeichnung in der S-A_Data-PDU	24
Tabelle 5 – Sicherheits-Whitelist und Sicherheits-Blacklist für Dienste	52
Tabelle 6 – Sicherheits-Zwischenliste für Dienste	53
Tabelle 7 – Sicherheits-Zwischenliste für Datenpunkte	54
Tabelle 8 – Kommunikationsmodus für Broadcast-Kommunikationsmodus empfangene sichere Dienste	54

Europäisches Vorwort

Dieses Dokument (EN 50090-3-4:2017) wurde erarbeitet von CLC/TC/205 „Elektrische Systemtechnik für Heim und Gebäude (ESHG)“.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-06-12
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-06-12

EN 50090-3 besteht aus folgenden Teilen:

- EN 50090-3-1, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-1: Anwendungsaspekte – Einführung in die Anwendungsstruktur*
- EN 50090-3-2, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-2: Anwendungsaspekte – Anwendungsprozess ESHG Klasse 1*
- EN 50090-3-3, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-3: Anwendungsaspekte – ESHG-Interworking-Modell und übliche ESHG-Datenformate*
- EN 50090-3-4, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-4: Informationssicherheit auf Anwendungsschicht, Dienste, Konfiguration und Ressourcen*

Einleitung

KNX Association als Kooperationspartner von CENELEC bestätigt dies insoweit, als dass die Norm Patente und ähnliche Rechte enthält, wobei die Mitglieder der KNX Association bereit sind, mit Bewerbern weltweit zu gerechten, angemessenen und nicht benachteiligenden Bedingungen über deren Lizenzierung zu verhandeln.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können, ohne dass diese vorstehend identifiziert wurden. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte kenntlich zu machen.

CEN und CENELEC stellen online eine aktuelle Liste mit den für ihre Normen relevanten Patenten bereit. Anwender sind angehalten, diese Liste einzusehen, um aktuelle Informationen hinsichtlich Patenten zu erhalten (<ftp://ftp.cencenelec.eu/EN/IPR/Patents/IPRdeclaration.pdf>).

1 Anwendungsbereich

Diese Europäische Norm legt die Sicherheit offener Kommunikationssysteme der ESHG (Elektrische Systemtechnik für Heim und Gebäude) fest.

Sie basiert auf ISO/IEC 24767-2 „Sicherheit von Heim-Netzwerken – Teil 2: Interne Sicherheitsdienste: Sicheres Kommunikationsprotokoll für Middleware“.

Eine sichere ESHG-Lösung hat mehrere Vorteile.

- Sie bietet mehr Sicherheit für das drahtlose ESHG-RF-Kommunikationsmedium:
ESHG-RF-Funkrahmen mit unverschlüsselter Kommunikation können problemlos nachverfolgt werden (z. B. durch einen Sniffer).
- Sie ermöglicht sichere Anwendungen.
Eine sichere Kommunikation ist für Rollladen- und Türsteuerungen sowie für Einbruchschutzsysteme besonders wichtig, um Manipulationen zu vermeiden (Einbrecher ...).
Auch für Zähleranwendungen ist eine sichere Kommunikation besonders wichtig, um z. B. Stromverbrauchsdaten zu schützen.
In diesem Dokument werden keine Anwendungstypen definiert.

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).

EN 50090-1:2011, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 1: Aufbau der Norm*

EN 50090-3-2, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-2: Anwendungsaspekte – Anwendungsprozess ESHG Klasse 1*

EN 50090-4-1, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 4-1: Medienunabhängige Schicht – Anwendungsschicht für ESHG Klasse 1*

EN 50090-4-2, *Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 4-2: Medienunabhängige Schicht – Transportschicht, Vermittlungsschicht und allgemeine Teile der Sicherungsschicht für ESHG Klasse 1*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach 50090-1:2011 und die folgenden Begriffe.

3.1.1

Zugriffskontrolle

(en: Access Control)

Definition und Evaluierung, welcher Kommunikationspartner auf welche Daten zugreifen oder welche Dienste aufrufen darf, wobei alle Kommunikationspartner mit denselben Rechten für alle Daten und Dienste in Rollen zusammengefasst werden und für jede Rolle sowie für jeden Daten- oder Dienstbestandteil die entsprechenden Berechtigungen definiert werden

3.1.2

Sicherheits-Blacklist

(en: Security Black List)

Standardliste mit Diensten oder Datenpunkten die nur akzeptiert werden dürfen, wenn eine sichere, vertrauenswürdige ESHG-Kommunikation verwendet wird

3.1.3

Schlüsseltext

(en: cipher text)

Oberbegriff zur Bezeichnung von verschlüsselten Daten

Anmerkung 1 zum Begriff: Schlüsseltext ist das Gegenteil von Klartext.

3.1.4

Berechtigung

(en: permission)

Definition und Bedingungen (unverschlüsselt, Authentifizierung, Vertraulichkeit) der von einer Rolle akzeptierten Funktionen, wenn auf einen Datenpunkt in einem Gerät zugegriffen wird oder wenn Dienste von einem Kommunikationspartner akzeptiert werden

3.1.5

Klartext

(en: plain data)

Oberbegriff zur Bezeichnung von unverschlüsselten Daten, deren Inhalt vom Dienst und vom Benutzer abhängig ist und die keine Vertraulichkeit und Authentifizierung erfordern

Anmerkung 1 zum Begriff: Klartext ist das Gegenteil von Schlüsseltext.

3.1.6

sicherer Datenpunkt

(en: secure Data Point (secure DP))

Datenpunkt, der eine Authentifizierung und/oder Vertraulichkeit erfordert

3.1.7

Rolle

(en: role)

Kennzeichnung einer Gruppe aus Verbindungen zu einem Gerät (Multicast, Unicast und weitere), die über die gesamte Anwendungsschnittstellenschicht (en: Application Interface Layer (AIL)) hinweg über dieselben Berechtigungen verfügen

3.1.8

sichere Verbindung

(en: secure link)

Verbindung zu einem sicheren Datenpunkt

3.1.9

Ressourcen für sichere Verbindungen

(en: Security Link Resources)

Gesamtheit der folgenden Ressourcen:

- Tabelle mit Punkt-zu-Punkt-Schlüsseln;
- Tabelle mit Gruppenschlüsseln;
- Tabelle mit sicheren individuellen Adressen;
- Tool-Schlüssel

3.1.10

Sicherheitskennzeichen für Gruppenadressen

(en: Group Address Security Flags)

Kennzeichnung in einem Konfigurationstool, ob für eine Gruppenadresse keine sichere Kommunikation verwendet wird oder eine sichere Kommunikation mit Authentifizierung und/oder Vertraulichkeit

3.1.11

Sicherheits-Whitelist

(en: Security White List)

Standardliste mit Diensten oder Datenpunkten, die immer mit unverschlüsselter Kommunikation akzeptiert werden

3.2 Abkürzungen

CFB	Cipher Feedback
FDSK	werksseitiger Einrichtungsschlüssel (en: Factory Default Set up Key)
IV	Initialisierungsvektor (en: Initialization Vector)
MaC	Management-Client (en: Management Client)
MaS	Management-Server (en: Management Server)
MAC	Nachrichten-Authentifizierungscode (en: Message Authentication Code)
MiM	Man-in-the-Middle
P-AL	Unverschlüsselte Application Layer
SAI	Sicherheitsalgorithmusbezeichner (en: Security Algorithm Identifier (SAI))
S-AL	Sichere Application Layer (en: Secure Application Layer)
SCF	Sicherheitssteuerungsfeld (en: Security Control Field)
SeqNr	Sequenznummer (en: Sequence Number)
SFCC	gemeinsamer Sicherheitsfehlerzähler (en: Security Failure Common Counter)
SFL	Sicherheitsfehler in Verbindungen (en: Security Failures on Links)
SHD	sicherer Header (en: Secure Header)
SKI	Sicherheitschlüsselinformationen (en: Security Key Information)

4 Allgemeine Einführung (informativ)

4.1 Allgemeines

4.1.1 Allgemeiner Überblick über die ESHG-Sicherheit

Dieses Dokument legt die Datensicherheit offener Kommunikationssysteme der ESHG sowie die zugehörigen Ressourcen (deren Format herstellerepezifisch sein darf) und Verfahren fest.

4.1.2 Produkttypen

Die Datensicherheit offener Kommunikationssysteme der ESHG ist so ausgelegt, dass sie auf allen vorhandenen Kommunikationsmedien offener Kommunikationssysteme der ESHG unterstützt wird (ESHG TP1, ESHG PL110, ESHG RF und ESHG IP).

Diese Dokumentversion stellt keine spezifischen Anforderungen an ESHG-Datenschnittstellen bereit.

ESHG-Koppler werden ebenfalls berücksichtigt. Das sichere ESHG-Rahmenformat (siehe Bild 5) ist so ausgelegt, dass es von vorhandenen und neueren ESHG-Kopplern verarbeitet werden kann.

BEISPIEL ESHG-TP1/RF-Koppler.

4.1.3 Sichere und unverschlüsselte Kommunikation in einer Anlage

Der Endbenutzer¹⁾ muss sich sicher sein können, dass keine unautorisierte Person seine Empfänger steuern kann (Rollläden, Türen ...).

Der Endbenutzer kann über mehrere unterschiedliche Empfänger verfügen und möchte nur für einige der Empfänger eine sichere Kommunikation implementieren.

BEISPIEL Der Endbenutzer benötigt eine sichere Kommunikation für die Rollläden im unteren Teil des Hauses, aber nicht für die Rollläden im oberen Teil des Hauses.

Für eine sichere Auslegung ist eine Erweiterung des ESHG-Stacks erforderlich. Es ist hilfreich auf Produkte zurückgreifen zu können,

- die sichere und unverschlüsselte Kommunikation verwenden,
- und auf andere Produkte, die nur sichere Kommunikation verwenden.

4.1.4 Voraussetzungen

Voraussetzung 1

Die sichere Kommunikation muss während der Laufzeit (typischerweise Multicast-Kommunikation) und während der Konfiguration (typischerweise Punkt-zu-Punkt-Kommunikation) unterstützt werden.

Voraussetzung 2

Die sichere Kommunikation wird vom Empfänger gefordert.

4.1.5 Produktschemabeispiele

4.1.5.1 Beispiel 1: Ein sicherer Sender ist mit einem Empfänger verbunden, der nur eine Authentifizierung erfordert

In Bild 1 unten sind bidirektionale Geräte dargestellt.

ANMERKUNG Bei einem unidirektionalen Gerät besteht keine Verbindung mit dem Datenpunkt „Info Status“ (IMUD).

¹⁾ Hauseigentümer, Gebäudeeigentümer, Gebäudenutzer usw.

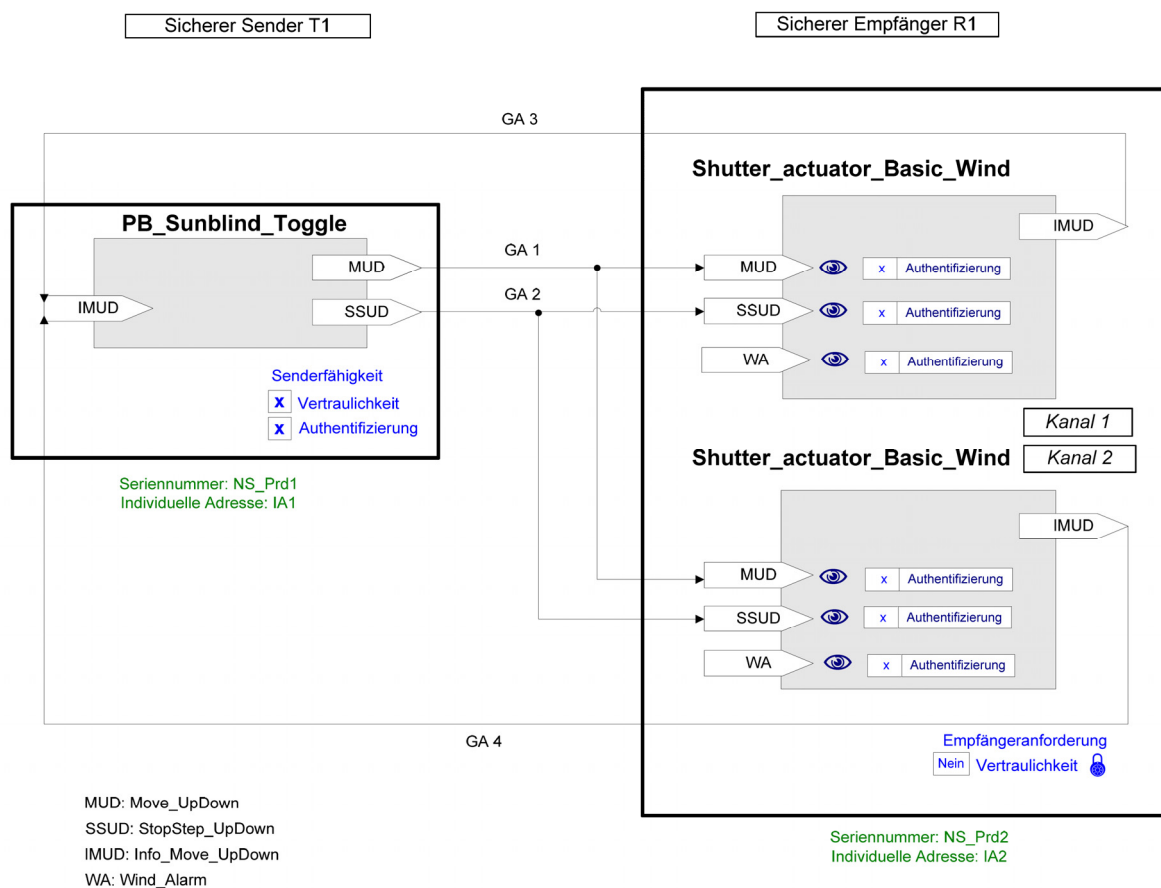


Bild 1 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der nur eine Authentifizierung erfordert

Die Verbindungen werden während der Konfiguration hergestellt. Die Sicherheitseinstellungen können standardmäßig im Produkt und in einer Offline-Produktbeschreibung definiert werden, oder sie können bei der Konfiguration festgelegt werden.

4.1.5.2 Beispiel 2: Ein sicherer Sender ist mit einem Empfänger verbunden, der eine Authentifizierung und Vertraulichkeit erfordert

In Bild 2 unten sind bidirektionale Geräte dargestellt.

ANMERKUNG Bei unidirektionalen Geräten besteht keine Verbindung mit dem Datenpunkt „Info Status“ (IMUD).

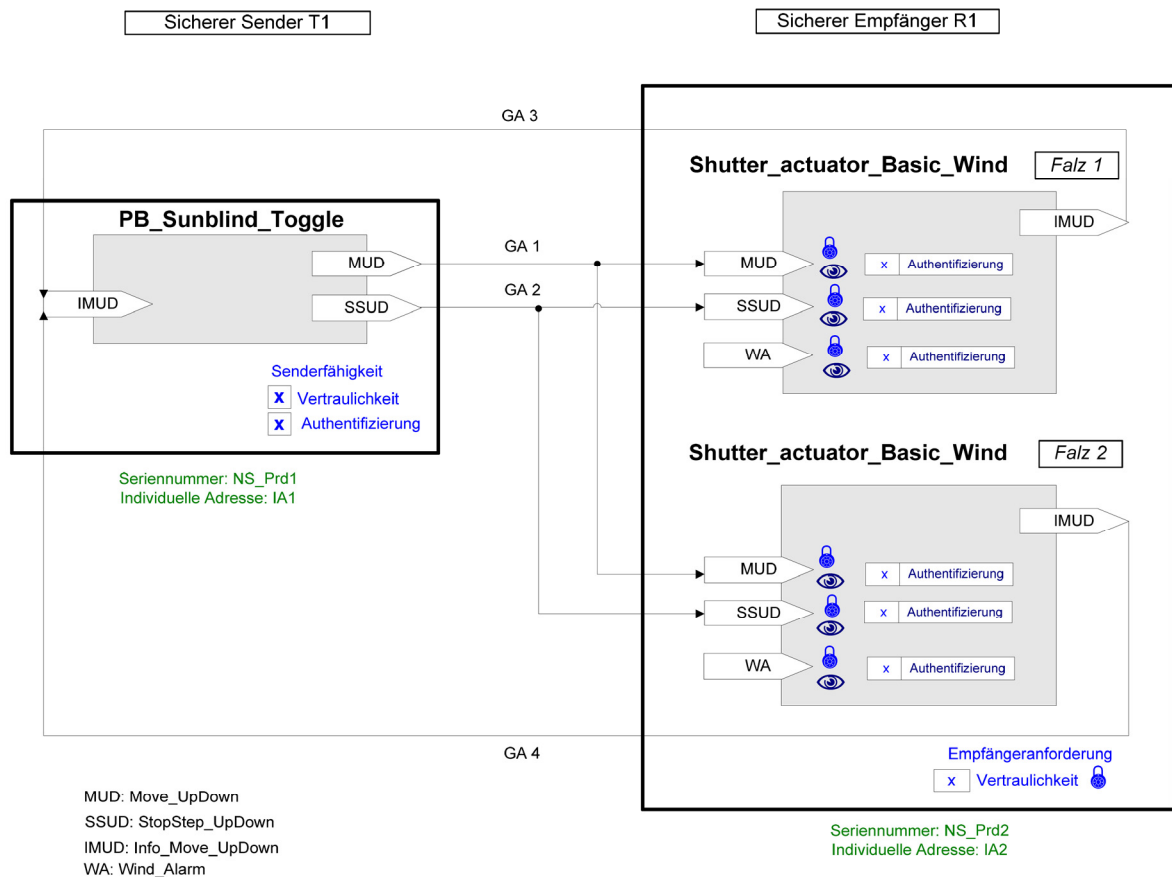


Bild 2 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der sowohl eine Authentifizierung als auch Vertraulichkeit erfordert

4.1.6 Einschränkungen

In diesem Dokument liegt der Schwerpunkt auf der ESHG-Sicherheit von Endgeräten während der Laufzeit und der Konfiguration (wobei die dafür erforderlichen Ressourcen herstellerspezifisch bleiben). Für die vollständige Unterstützung von ESHG-Sicherheit in ESHG-Systemen, ist Folgendes zusätzlich erforderlich, aber in dieser Dokumentversion noch nicht vollständig spezifiziert. Die unten aufgeführten Funktionen liegen außerhalb des Anwendungsbereichs dieser Normversion.

- Visualisierung und Schnittstellen:

Bei der Visualisierung muss das Visualisierungsgerät (z. B. Touchpanel) oder das Visualisierungstool die in dem ESHG-System verwendeten Sicherheitsschlüssel auf sichere Weise empfangen.

Zudem muss es sich bei der Schnittstelle (IP-Tunnelling, USB) um einen anerkannten Kommunikationspartner im System handeln oder sie muss mit dem Sequenznummer-Feld (en: Sequence Number Field (SeqNr)) der sicheren Geräte synchronisiert werden, mit denen sie kommuniziert (Senden und Empfangen).

- Medienkoppler zwischen einem sicheren ESHG-RF-Subnetzwerk und einem unverschlüsselten ESHG-Subnetzwerk

ANWENDUNGSFALL Ein vorhandenes ESHG-TP1-System wurde um ein ESHG-RF-Subnetzwerk erweitert. Da dieses naturgemäß offen ist, soll in dem ESHG-RF-Subnetzwerk eine sichere ESHG-Kommunikation implementiert werden. Dabei soll das vorhandene ESHG-TP1-System allerdings unverändert bleiben; das ESHG-TP1-System wird als sicher erachtet.

Dazu ist ein ESHG-TP1/RF-Medienkoppler erforderlich, der als „sicherer Proxy“ für die ESHG-TP1-Kommunikation in dem RF-Subnetzwerk dient und die ESHG-Datensicherheit handhabt, wenn sichere Telegramme von ESHG-RF nach ESHG-TP1 übergeben werden.

Dieser sichere ESHG-Proxy und der ESHG-TP1/RF-Medienkoppler (Sicherheitgateway) werden in dieser Normversion nicht modelliert.

- ESHG-Datensicherheit in einem Subnetzwerk außerhalb des Gebäudes und keine ESHG-Datensicherheit im Gebäude.
- Wenn einem Kommunikationspartner der Schlüssel zur Verifizierung eines sicheren Telegramms übermittelt wird, kann dieser Teilnehmer auch selbst sichere Telegramme senden. Die installierten Geräte würden auch reagieren, wenn der Teilnehmer eine individuelle Adresse verwenden würde, die in ihrer Tabelle mit Punkt-zu-Punkt-Schlüsseln oder in der Tabelle mit Gruppenschlüsseln hinterlegt ist.
- BEISPIEL 1 Der Zugang von Personen zu einem Gebäude wird per ESHG mit ESHG-Datensicherheit und Authentifizierung kontrolliert. Wenn der Gebäudemanager den Schlüssel an ein Visualisierungstool weiter gibt, kann das Tool das Zugriffskontrollsystem rechtmäßig als den tatsächlichen Absender der Telegramme verifizieren. Jedoch kann das Visualisierungstool mit dem erhaltenen Sicherheitsschlüssel wiederum selbst sichere Telegramme senden. Wenn das Visualisierungstool zudem die individuelle Adresse eines legitimen Geräts in dem Zugriffskontrollsystem verwenden und dessen Sequenznummer übernehmen würde, könnten die Empfänger nicht zwischen Telegrammen von den „regulären“ Absendern und Telegrammen vom Visualisierungstool unterscheiden.
- Mit der Einführung der ESHG-Datensicherheit wird es schwieriger festzustellen, ob die Ursache für einen Ausfall der Gruppenkommunikation in der Konfiguration der ESHG-Datensicherheit oder in anderen Aspekten der Gruppenkommunikation liegt. Derzeit wird eine erweiterte Diagnose von Gruppenobjekten erarbeitet.

BEISPIEL 2 Wenn ein sicherer Sender ein sicheres Telegramm an einen sicheren Empfänger sendet und der sichere Empfänger nicht reagiert, kann dies diverse Ursachen haben. Ohne Anwendung von Sicherheit können die folgenden Ursachen vorliegen:

- Die Gruppenadresse ist dem Empfänger nicht zugewiesen.
- Die Gruppenadresse ist nicht mit dem erwarteten Gruppenobjekt im Empfänger verknüpft.
- Die Kennzeichnungen für das Gruppenobjekt im Empfänger lassen das Schreiben des Gruppenobjektwertes nicht zu.
- Es liegen andere Ursachen im Empfänger vor, die eine Reaktion auf das Telegramm verhindern, z. B. gesperrter Zustand, eine Priorität usw.

Bei Verwendung von ESHG-Datensicherheit, können die folgenden Ursachen hinzukommen:

- Der Sender und der Empfänger verwenden unterschiedliche Schlüssel.
- Die individuelle Adresse des Senders ist nicht in der Tabelle mit Punkt-zu-Punkt-Schlüsseln oder in der Tabelle mit Gruppenschlüsseln des Empfängers hinterlegt.
- Es gibt Unregelmäßigkeiten mit der Sequenznummer des Senders.
- Der Sender verfügt nicht über die erforderlichen Berechtigungen (Rolle) zum Schreiben des Gruppenobjektwertes in den Empfänger.

4.2 Allgemeiner Überblick

4.2.1 Merkmale der ESHG-Datensicherheit

- Authentifizierung:

Anwendungsfall „Nur Authentifizierung“: Busmonitore und Visualisierungstools (z. B. Zähleranzeigen) müssen Datenverkehr analysieren können, ohne über einen Schlüssel zu verfügen (d. h., dass der Datenverkehr nicht authentifiziert werden kann). Die verringerte Sicherheit an diesen Punkten wird in einigen Fällen in gewisser Weise durch die erhöhte Sicherheit kompensiert, die durch das Fehlen des Schlüssels in manchen für Benutzer zugänglichen Geräten gegeben ist.

- Vertraulichkeit.
- Zugriffskontrolle durch Rollen und Berechtigungen.

4.2.2 Anordnung der ESHG-Datensicherheit im ESHG-Stack

Die ESHG-Datensicherheit wird wie in Bild 3 dargestellt von der sicheren Application Layer, der Application Layer und der Application Interface Layer (Anwendungsschnittstellschicht) verwaltet.

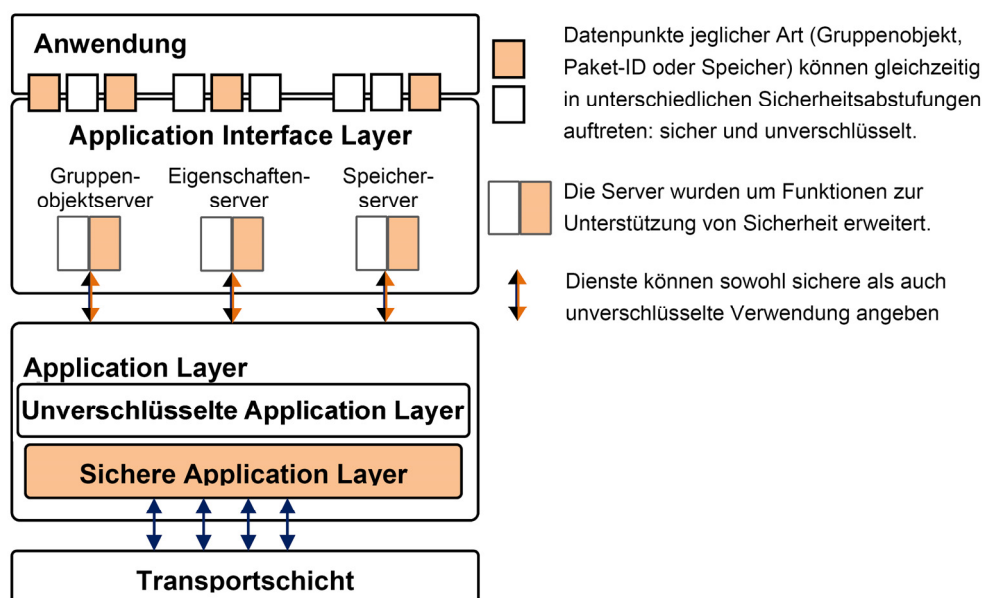


Bild 3 – Anordnung der ESHG-Datensicherheit im ESHG-Stack

Tabelle 1 bietet einen kurzen Überblick über die Handhabung der Sicherheit in diesen Schichten.

Tabelle 1 – Sicherheitsmerkmale der ESHG-Schichten (informativ)

Merkmal	Schicht		
	S-AL	P-AL	AIL
Betriebsebene	Verbindungsebene		Dienstebene Datenpunktebene
Funktionen	- Verschlüsseln und Entschlüsseln von sicheren Telegrammen - Handhabung von Ausnahmen auf Verbindungsebene	- Weiterleiten des Dienstes der Application Layer mit den Sicherheitsmerkmalen zum Senden und Empfangen sowie Angabe der Art der Verbindung - Authentifizierung oder Vertraulichkeit - Verbindungsindex	- Zugriffskontrolle - Unterstützung von Rollen - Handhabung von Berechtigungen
Ressource	- Tabelle mit Punkt-zu-Punkt-Schlüsseln - Tabelle mit Gruppenschlüsseln - Tabelle mit sicheren individuellen Adressen - Sonstige	Keine	Tabelle mit Punkt-zu-Punkt-Schlüsseln

5 Spezifikation

5.1 Stack und Kommunikation

5.1.1 Sichere Application Layer

5.1.1.1 Allgemeine Anforderungen und Überblick

5.1.1.1.1 Einbettung der sicheren Application Layer in die Application Layer und grundlegende Funktionen

Die sichere Application Layer (en: Secure Application Layer (S-AL)) muss die ESHG-Datensicherheit auf Verbindungsebene verwalten.

Die S-AL muss ein Teil der Application Layer sein. Somit muss der Dienst „S-A_Data“ nah an den Diensten der Application Layer liegen können, und die Sicherheitsrichtlinien müssen möglichst an jeden Dienst der Application Layer angepasst werden können.

Die Verwendung der S-AL darf keinen Einfluss auf die Funktionalität der unverschlüsselten Application Layer (en: Plain Application Layer (P-AL)) haben.

- In Empfangsrichtung, nachdem der Dienst „S-A_Data“ akzeptiert wurde, muss die S-AL die Sicherheit in Abhängigkeit vom Kommunikationsmodus entweder basierend auf der Tabelle mit Punkt-zu-Punkt-Schlüsseln oder der Tabelle mit Gruppenschlüsseln prüfen, die unverschlüsselte Application-Layer-Protokolldateneinheit (APDU) wiederherstellen und bei erfolgreichem Abschluss die enthaltene unverschlüsselte AL-Dienstanforderung intern an die unverschlüsselte Application Layer weiterleiten.
- In Senderichtung muss die S-AL den unverschlüsselten AL-Dienst erneut in Abhängigkeit vom Kommunikationsmodus des für den Dienst „S-A_Data“ verwendeten Kommunikationsmodus entweder basierend auf der Tabelle mit Punkt-zu-Punkt-Schlüsseln oder der Tabelle mit Gruppenschlüsseln schützen und muss die sichere APDU per Dienst „S-A_Data“ übertragen.

Jedoch muss die unverschlüsselte Application Layer die Sicherheitsdienstparameter (par_auth, par_conf und link_index) transparent zwischen der S-AL und der AIL übergeben: siehe 5.1.2.

In Bild 4 ist die Anordnung der S-AL im ESHG-Kommunikationsstack dargestellt. Es zeigt die Handhabung von sicheren Telegrammen. Dies ist nur ein grundlegendes Schema. Es zeigt weder die Handhabung von unverschlüsselten Telegrammen noch mögliche Ausnahmen. Die Struktur und Prioritäten innerhalb der S-AL sind in diesem Bild nicht vollständig.

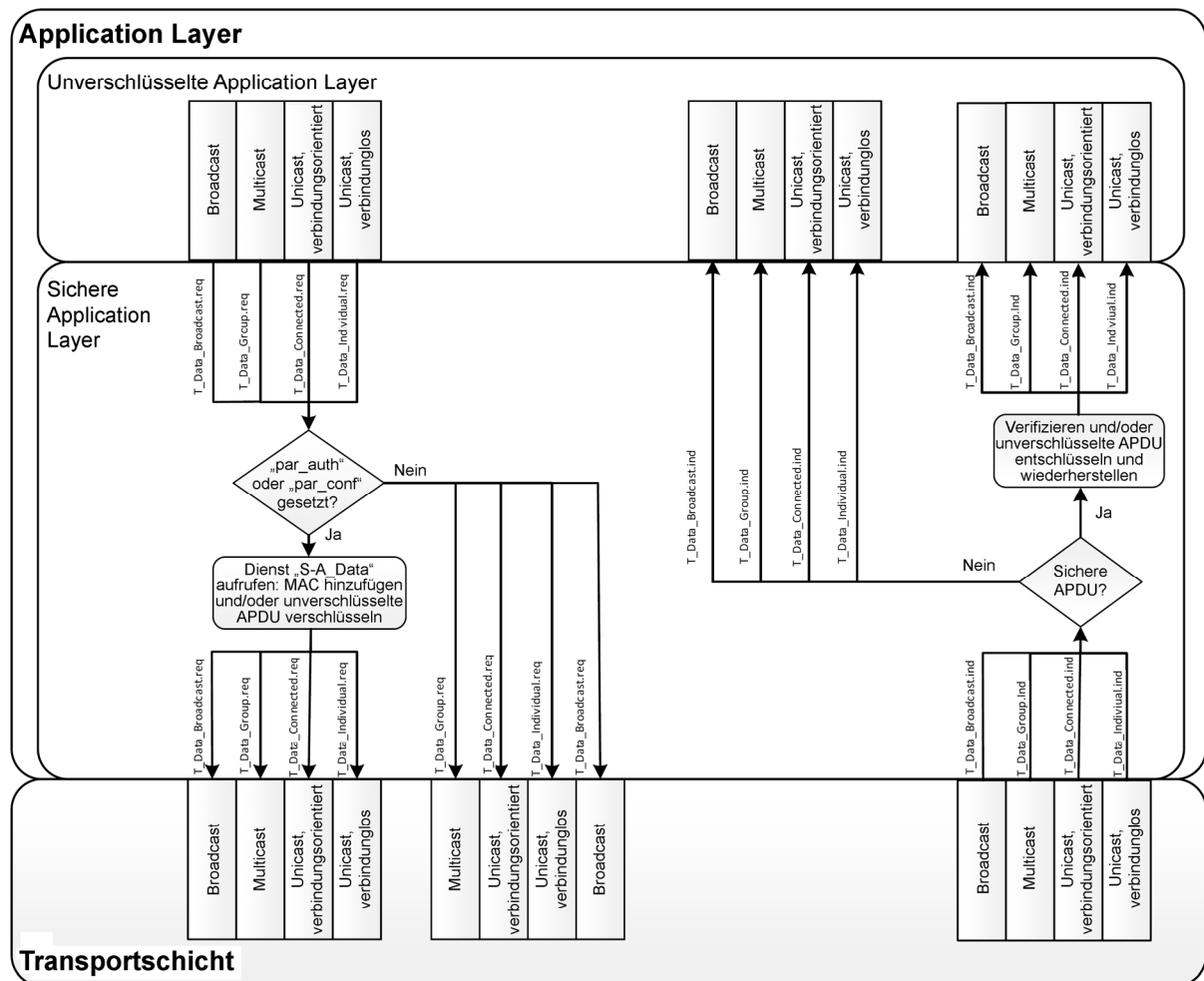


Bild 4 – Anordnung der S-AL in der Application Layer

5.1.1.1.2 S-AL – Überblick

Die S-AL muss die folgenden Funktionen aufweisen.

- Unterstützung des Dienstes „S-A_Data“ siehe 5.1.1.2;
- Handhabung der Sequenznummer siehe 5.1.1.3;
- Handhabung von Sicherheitsfehlern siehe 5.1.1.4;
- Sichere Handhabung der Dienste der Transportschicht siehe 5.1.1.5.

In den folgenden Unterabschnitten werden diese und weitere Funktionen spezifiziert.

5.1.1.1.3 AES-128 mit CTR-Betriebsmodus (en: Counter Mode) und AES-CCM-Signatur (en: Counter with CBC-MAC)

5.1.1.1.3.1 Sichere Daten

Das allgemeine Format für sichere Daten mit diesem Algorithmus muss wie in Bild 5 dargestellt aufgebaut sein. Die sicheren Daten müssen die folgenden Felder enthalten. (Diese werden unten im Detail spezifiziert.)

- Sequenznummer (SeqNr) und
- unverschlüsselte APDU (000000b + APCI + ASDU = Daten) und

- Telegrammauthifizierungscode (en: Message Authentication Code (MAC)).

Die sichere Protokollsteuerinformation der Application Layer (en: Application Layer Protocol Control Information (APCI)) und das Sicherheitssteuerungsfeld (en: Security Control Field (SCF)) sind unabhängig vom Sicherheitsalgorithmus und werden in 5.1.1.2.1 spezifiziert.

Byte 6						Byte 7						Byte 8						Byte 9						...		Byte m																	
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	...		7	6	5	4	3	2	1	0		
								Sichere APDU																																			
TPCI						Sichere APCI						Sichere ASDU																															
												SCF						Sichere Daten																									
						10 Bits						8 Bits						n Bytes																									
						1	1	1	1	1	1	0	0	0	1																												

Legende

Spezieller Klartext für den ESHG-Dienst „S-A_Data“.

Bild 5 – Sichere APDU (Beispiel für TP1)

- Sequenznummer (SeqNr),
Siehe 5.1.1.3.
- 000000b

Dieser Konstantwert muss zur Anordnung der APCI auf denselben Bitpositionen verwendet werden wie in den Medien auf Feldebene. Dabei erfolgt die Anordnung auf den zwei höchstwertigsten Bits (en: Most Significant Bit (MSB)) in einem Byte und den zwei (APCI aus 4 Bits) oder sechs geringstwertigsten Bits (en: Least Significant Bit (LSB)) im nächsten Byte.
- Unverschlüsselte APDU (APCI + Daten):

Definition: Dies muss die APDU des unverschlüsselten Application-Layer-Dienstes sein.

Format: Die Länge, die möglichen Unterfelder und deren Verschlüsselung müssen mit den Spezifikationen für den Dienst der unverschlüsselten Application Layer nach EN 50090-4-1 übereinstimmen.

D. h., dass auch das optimierte Format verwendet wird. Dabei müssen Daten mit 6 Bits und weniger auf demselben LSB und im selben Byte angeordnet werden wie das LSB der APCI, und es müssen nach Möglichkeit Nullen vorangestellt sein. Bei Daten mit mehr als 6 Bits folgt nach der APCI ebenfalls „000000b“ und die Daten beginnen im nächsten Byte.
- Telegrammauthifizierungscode (en: Message Authentication Code (MAC)).
Siehe die folgenden Unterabschnitte.

5.1.1.1.3.2 Allgemeine Anforderungen

In diesem Unterabschnitt wird nur die ESHG-spezifische Verwendung der CCM-Parameter spezifiziert. Die Definition des CCM-Modus liegt außerhalb des Anwendungsbereichs dieses Dokuments. In Anhang A ist ein informativer Überblick über die resultierende Verwendung des CCM-Modus für ESHG zu finden.

Die nachfolgenden Anforderungen gelten sowohl für die Verwendung ausschließlich mit der Authentifizierung als auch für die Verwendung mit Authentifizierung und Vertraulichkeit.

Da in B_0 und Ctr_j Parameter und Zustände der Netz-Zugangsschicht und Transportschicht vorhanden sind, ist zwischen den Schichten der ESHG-Stack-Implementierung ein gewisses Maß an Kooperation erforderlich.

In Aufwärtsrichtung könnte dies durch eine Übergabe der erforderlichen Informationen in den „ind“-Telegrammen implementiert werden.

In Abwärtsrichtung müssen in den unteren Schichten Hilfsverfahren implementiert werden, sodass die S-AL z. B. einen Application Layer-Dienstzugangspunkt (en: Application layer Service Access Point (ASAP)) in eine Zieladresse auflösen kann. Die größte Herausforderung in einem verbindungsorientierten Fall stellt die Sequenznummer der Transportschicht dar (Teil des TPCI-Feldes). Das Füllen dieses Feldes kann sich bei einer Geräteimplementierung als schwierig erweisen.

B₀

Der Aufbau des ersten Blocks B₀ im CCM-Algorithmus muss ESHG-spezifisch sein. Dies wird in Bild 6 spezifiziert. Diese Felder aus dem ESHG-Rahmen werden an dieser Stelle angeordnet, damit sie im Kommunikationspfad zwischen Sender und Empfänger nicht unbemerkt verändert werden können.

Die Quelladresse, Zieladresse und Sequenznummer der Transportschicht sind nicht verfügbar, wenn über eine lokale Transportschichtverbindung auf den Management-Server zugegriffen wird. In diesem Fall müssen diese Felder in den Blöcken B₀ und Ctr_j auf „0“ gesetzt werden.

Byte-Nr.												
0 MSB	...	5	6	7	8	9	10	11	12	13	14	15 LSB
SeqNr für S-A_Daten und S-A_Sync_Req-PDU Random für S-A_Sync_Res-PDU			SA		DA		00h	AT	TPCI / APCISec		00h	q

Bild 6 – Format von B₀

Das Feld „AT“ muss den 8-Bit-Wert „A000EEEEb“ aufweisen, wobei „A“ gleich dem Adresstyp des ESHG-Rahmens sein muss. „EEEEb“ muss gleich dem erweiterten Rahmenformat (en: Extended Frame Format (EFF)) sein, wenn die Rahmen „L_Data_Extended“ verwendet werden. Andernfalls muss „EEEEb“ gleich „0000b“ sein.

ANMERKUNG 1 Im Steuerfeld (CTRL), im erweiterten Steuerfeld (CTRLE) (TP1 und PL110) oder im ESHG-Steuerfeld (ESHG RF) sind die Wiederholungskennzeichen, die Priorität, der Hop Count und „ffff“ daher nicht geschützt. (Der Hop-Count-Wert ändert sich, wenn der Rahmen durch einen Koppler geleitet wird.)

Das Feld „TPCI / APCISec“ muss wie in Bild 7 dargestellt aufgebaut sein: die ersten 6 Bits müssen die Protokollsteuerinformation der Transportschicht (en: Transport Layer Protocol Control Information (TPCI)) des ESHG-Rahmens enthalten und die letzten 10 Bits müssen die sichere APCI (3F1h) enthalten.

Bitnummer	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Feldname	TPCI						Sichere APCI									
Wert							1	1	1	1	1	1	0	0	0	1

Bild 7 – Format des Feldes „TPCI/APCI_{Sec}“ in B₀

„q“ muss die Länge der Nutzdaten „P“ angeben: siehe A.3.

ANMERKUNG 2 Der Aufbau von „P“ ist abhängig vom S-AL-Dienst („S-A_Data“ ausschließlich mit Authentifizierung oder mit Authentifizierung und Vertraulichkeit sowie „S-A_Sync“). Dennoch wird „q“ immer als die Länge von „P“ spezifiziert.

$Ctrl_j$

Auch das Format des Blockzählers „ $Ctrl_j$ “ (siehe NIST/SP 800-38A) ist ESHG-spezifisch. $Ctrl_j$ muss wie in Bild 8 aufgebaut sein. Der Zähler $[j]$ für $Ctrl_0$ muss „00h“ sein.

Byte-Nr.												
0 MSB	...	5	6	7	8	9	10	11	12	13	14	15 LSB
SeqNr für S-A_Daten und S-A_Sync_Req-PDU Random für S-A_Sync_Res-PDU			SA		DA		00h	00h	00h	00h	01h	[j]

Bild 8 – Format von $Ctrl_j$

Byte 14 von $Ctrl_j$ muss „01h“ sein. Damit wird sichergestellt, dass B_0 und $Ctrl_j$ unabhängig von den Werten der Felder „AT“ und „TPCI“ in B_0 immer unterschiedliche Werte aufweisen.

Jeder Zählerwert muss durch Erhöhen des vorhergehenden Zählerwertes um „1“ berechnet werden.

$$Ctrl_j = Ctrl_{j-1} + 1 \quad // \text{ Bei } j = 1 \text{ bis } n; n \leq 255$$

5.1.1.1.3.3 Nur Vertraulichkeit

Dieser Anwendungsfall ist bei „AES-128 mit CTR-Betriebsmodus und AES-CCM-Signatur“ nicht möglich, da das Feld „MAC“ immer vorhanden sein muss.

5.1.1.1.3.4 Nur Authentifizierung

5.1.1.1.3.4.1 Format der sicheren Daten

Die Felder „SCF“, „SeqNr“ und „unverschlüsselte APDU“ dürfen nicht verschlüsselt werden. Auf diese Felder muss das Feld „MAC“ folgen.

Byte 6								Byte 7								Byte 8								Bytes 9 bis 14				...				...															
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0					...				...															
																Sichere APDU																															
TPCI								Sichere APCI								Sichere ASDU																															
																SCF								Sichere Daten																							
																								SeqNr								Unverschlüsselte APDU (APCI + Daten)								MAC							
								10 Bits								8 Bits								6 Bytes								n Bytes								4 Bytes							
								1111110001																				00000 0b																			

Legende

- Spezieller Klartext für den ESHG-Dienst „S-A_Data“.
- Klartext aus dem ursprünglichen Dienst der Application Layer.
- Schlüsseltext

Bild 9 – Sichere Daten bei ausschließlicher Verwendung von Authentifizierung (Beispiel für TP1)

ANMERKUNG Die Sequenznummer (SeqNr) wird unverschlüsselt übertragen und ermöglicht es dem Empfänger, die Aktualität schnell zu prüfen.

5.1.1.1.3.4.2 Telegrammverarbeitung (nur Authentifizierung)

Telegrammerstellung

Das Feld „MAC“ muss mit dem CCM-Algorithmus berechnet werden.

1. Im Feld „SCF“ muss das Feld „Vertraulichkeit“ gelöscht und das Feld „Authentifizierung“ gesetzt werden. Das Feld „SAI“ muss mit „00b“ ausgefüllt werden, um die Verwendung von „AES-128 mit CTR-Betriebsmodus und AES-CCM-Signatur“ zu kennzeichnen.
2. Das Feld „SeqNr“ muss den aktuellen Wert der Sende-Sequenznummer enthalten. Der Wert der Sende-Sequenznummer wird dann erhöht, nachdem das Telegramm an die lokale Transportschicht übergeben wurde, siehe 5.1.1.3.
3. Bei „Nur Authentifizierung“

Bei „Nur Authentifizierung“ muss „P“²⁾ leer sein, und die unverschlüsselte APDU muss folglich in „A“²⁾ enthalten sein.

A = SCF | 000000b | Unverschlüsselte APDU (=unverschlüsselte APCI + Daten)

P = {leer}

4. Die weitere Berechnung muss nach Anhang A erfolgen.
Der Block B0 muss nach der Spezifikation in 5.1.1.1.3.2 aufgebaut sein.
5. Bei ESHG müssen die 32 höchstwertigsten Bits von Y_n ($MSB_{32}(Y_n)$) als MAC verwendet werden.

Telegrammverifizierung

Der Empfänger muss das Telegramm auf exakt dieselbe Weise verifizieren wie der Sender und wie es in NIST/SP 800-38A spezifiziert wird.

1. Das Feld „SeqNr“ verifizieren (siehe 5.1.1.3).
2. MAC basierend auf den empfangenen Feldern berechnen, und sicherstellen, dass er mit dem empfangenen MAC-Wert übereinstimmt.

Wenn bei einem der beiden Verifizierungsschritte ein Fehler auftritt, muss das empfangene sichere Telegramm ignoriert und der Sicherheitsfehler gehandhabt werden. (Siehe 5.1.1.4.)

5.1.1.1.3.5 Authentifizierung und Vertraulichkeit

5.1.1.1.3.5.1 Format der sicheren Daten

Die sicheren Daten müssen die Sequenznummer, die verschlüsselte APDU und den MAC enthalten. Die verschlüsselte APDU muss auf der unverschlüsselten APDU basieren und mit dem AES-128-Algorithmus mit CTR-Betriebsmodus verschlüsselt werden.

²⁾ Für die Definition von „A“ und „P“ ist auf die CCM-Spezifikation in ISO/IEC 24767-2 Bezug zu nehmen. Bei „A“ handelt es sich um die zugehörigen Daten und bei „P“ um die Nutzdaten.