

DIN EN 50090-3-4

ICS 97.120

Einsprüche bis 2017-07-19

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

Home and Building Electronic Systems (HBES) –
Part 3-4: Specification of KNX S AL, Secure Service, Secure configuration and security
Resources;
German version FprEN 50090-3-4:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-05-19 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 bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle
kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter 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 127 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 50090-3-4:2017 „Elektrische Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-4: Informationssicherheit auf Anwendungsschicht, Dienste, Konfiguration und Ressourcen“ (Schluss-Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und der Französischen Fassung abgeglichen ist, ist die englische Originalfassung der FprEN 50090-3-4:2017 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Das europäische Dokument FprEN 50090-3-4:2017 „Home and Building Electronic Systems (HBES) – Part 3-4: Specification of KNX S AL, Secure Service, Secure configuration and security Resources“ wurde vom TC 205 „Home and Building Electronic Systems (HBES)“ des Europäischen Komitees für Elektrotechnische Normung (CENELEC) erarbeitet und von CENELEC den Nationalen Komitees zur Stellungnahme vorgelegt.

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 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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] sind 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.

**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: Specification of KNX S AL,
Secure Service, Secure configuration and
security Resources

Dieser Entwurf für eine Europäische Norm wird den CENELEC-Mitgliedern zur CENELEC-Umfrage vorgelegt.
CENELEC Termin: 2017-05-05

Er wurde von CLC/TC 205 erstellt.

Wenn aus diesem Entwurf eine Europäische Norm wird, sind die CENELEC-Mitglieder 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.

Dieser Entwurf für eine Europäische Norm wurde von CENELEC in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. 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.

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

Warnvermerk: Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäische Norm in Bezug genommen werden.



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.

Projekt: 58780

Ref. Nr. FprEN 50090-3-4:2017 D
AVA Documents
Document Sharing Hub

Inhalt

	Seite
Europäisches Vorwort.....	3
Einleitung	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe und Abkürzungen	5
3.1 Begriffe	5
3.2 Abkürzungen	7
4 Allgemeine Einführung (informativ)	7
4.1 Allgemeines	7
4.1.1 Allgemeiner Überblick über die ESHG-Sicherheit	7
4.1.2 Produkttypen	7
4.1.3 Sichere und unverschlüsselte Kommunikation in einer Anlage	8
4.1.4 Voraussetzungen	8
4.1.5 Produktschemabeispiele	8
4.1.6 Einschränkungen	10
4.2 Allgemeiner Überblick	11
4.2.1 Merkmale der ESHG-Datensicherheit	11
4.2.2 Anordnung der ESHG-Datensicherheit im ESHG-Stack	12
5 Spezifikation	13
5.1 Stack und Kommunikation	13
5.1.1 Sichere Application Layer	13
5.1.2 Application Layer	43
5.1.3 Anwendungsschnittstellenschicht	44
5.1.4 Vermittlungsschicht nach DIN EN 50090-4-2 – Handhabung der sicheren APCI „3F1h“	53
5.2 Ressourcendefinition oder verwendete Ressourcen	53
Anhang A (informativ) Verwendung des CCM-Modus	54
A.1 Ziel	54
A.2 Definitionen	54
A.3 CCM-Operation	54
Anhang B (informativ) Beispiele – Vollständige Codierung einer sicheren ESHG-APDU	58
B.1 Allgemeines	58
B.2 S-A_Data-PDU	58
B.3 S-A_Data-PDU	59
B.4 S-A_Sync.req	61
B.5 S-A_Sync.res	62
Literaturhinweise	64

Europäisches Vorwort

Das vorliegende Dokument (FprEN 50090-3-4:2017) wurde durch CLC/TC 205, „Home and Building Electronic Systems (HBES)“ (Elektrische Systemtechnik für Heim und Gebäude (ESHG)), erarbeitet.

Das vorliegende Dokument ist gegenwärtig zum Einstufigen Abnahmeverfahren (en: Unique Acceptance Procedure) eingereicht.

Die folgenden Zeitpunkte werden vorgeschlagen:

- | | | |
|---|-------|---|
| • spätestes Datum, zu dem die Existenz dieses Dokuments auf nationaler Ebene bekannt gegeben werden muss | (doa) | dor + 6 Monate |
| • spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss | (dop) | dor + 12 Monate |
| • spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen | (dow) | dor + 36 Monate
(bei der Abstimmung zu bestätigen oder abzuändern) |

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*;
- FprEN 50090-3-4, *Systemtechnik für Heim und Gebäude (ESHG) – Teil 3-4: Informationssicherheit auf Anwendungsschicht, Dienste, Konfiguration und Ressourcen*.

Einleitung

Das Europäische Komitee für elektrotechnische Normung (fr: Comité Européen de Normalisation Electrotechnique; CENELEC) weist darauf hin, dass die Übereinstimmung mit diesem Dokument die Verwendung eines Patents hinsichtlich (... betroffenes Thema ...) in (... Abschnitt ...) bedeuten kann.

CENELEC nimmt keine Stellung zur Rechtmäßigkeit, zur Gültigkeit und zum Anwendungsbereich dieses Patentrechts.

Der Halter dieses Patentrechts hat CENELEC zugesichert, dass er bereit ist, über kostenlose Lizenzen oder Lizenzen zu vernünftigen und nicht diskriminierenden Geschäftsbedingungen mit Antragstellern in der ganzen Welt zu verhandeln. In diesem Zusammenhang ist die Erklärung des Halters dieses Patentrechts bei CENELEC registriert. Informationen sind erhältlich bei:

... Name des Halters des Patentrechts ...

... Adresse ...

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.cenelec.eu/EN/IPR/Patents/IPRdeclaration.pdf>).

1 Anwendungsbereich

Diese Europäische Norm legt die Sicherheit für die ESHG-Kommunikation (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 DIN EN 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 ESHG-Datensicherheit sowie die zugehörigen Ressourcen (deren Format herstellerspezifisch sein darf) und Verfahren fest.

4.1.2 Produkttypen

Die ESHG-Datensicherheit ist so ausgelegt, dass sie auf allen vorhandenen ESHG-Kommunikationsmedien 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 verfügt möglicherweise über mehrere unterschiedliche Empfänger 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 nachstehend sind bidirektionale Geräte dargestellt.

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

¹⁾ Hauseigentümer, Gebäudeeigentümer, Gebäudenutzer usw.

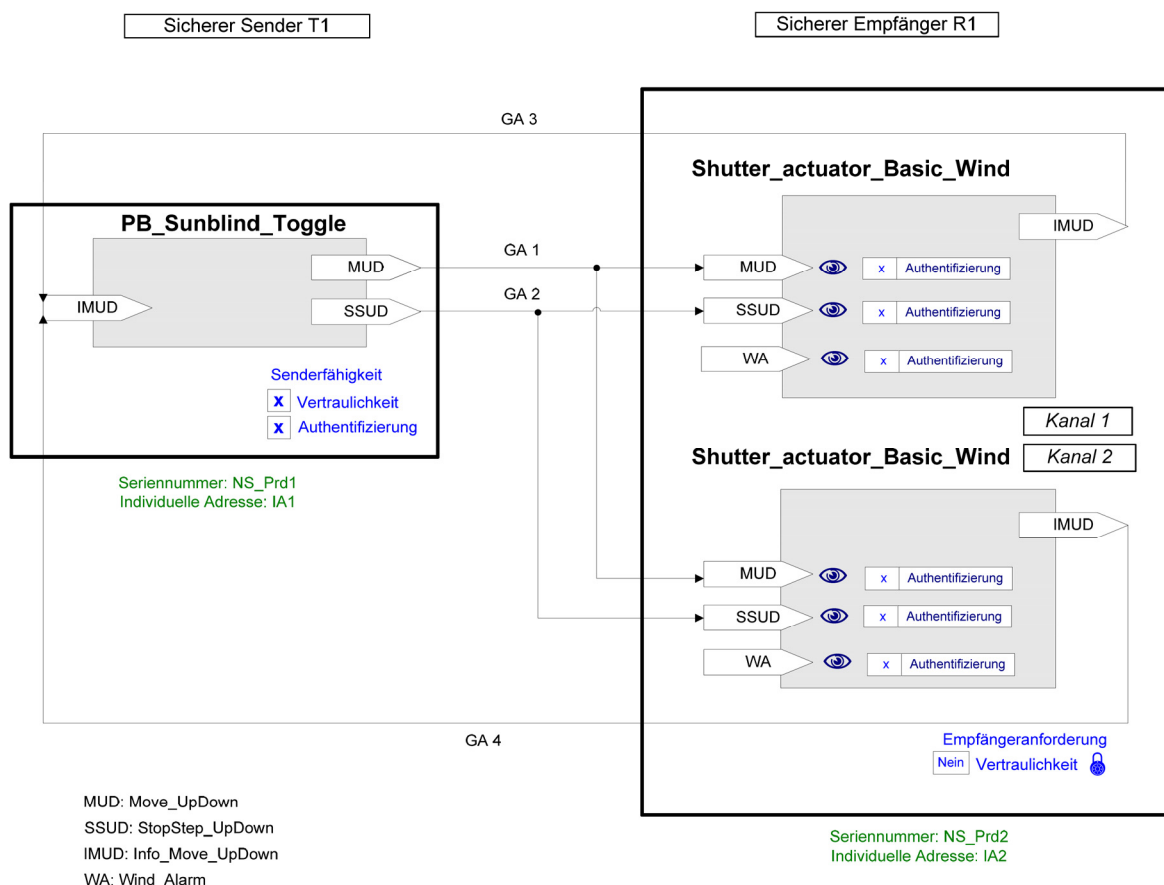


Bild 1 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der nur eine Authentifizierung erfordert

Die Verbindungen werden während der Konfiguration hergestellt. Die Sicherheitseinstellungen können standardmäßig im Produkt und in einer Offline-Produktbeschreibung definiert werden, oder sie dürfen 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 nachstehend sind bidirektionale Geräte dargestellt.

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

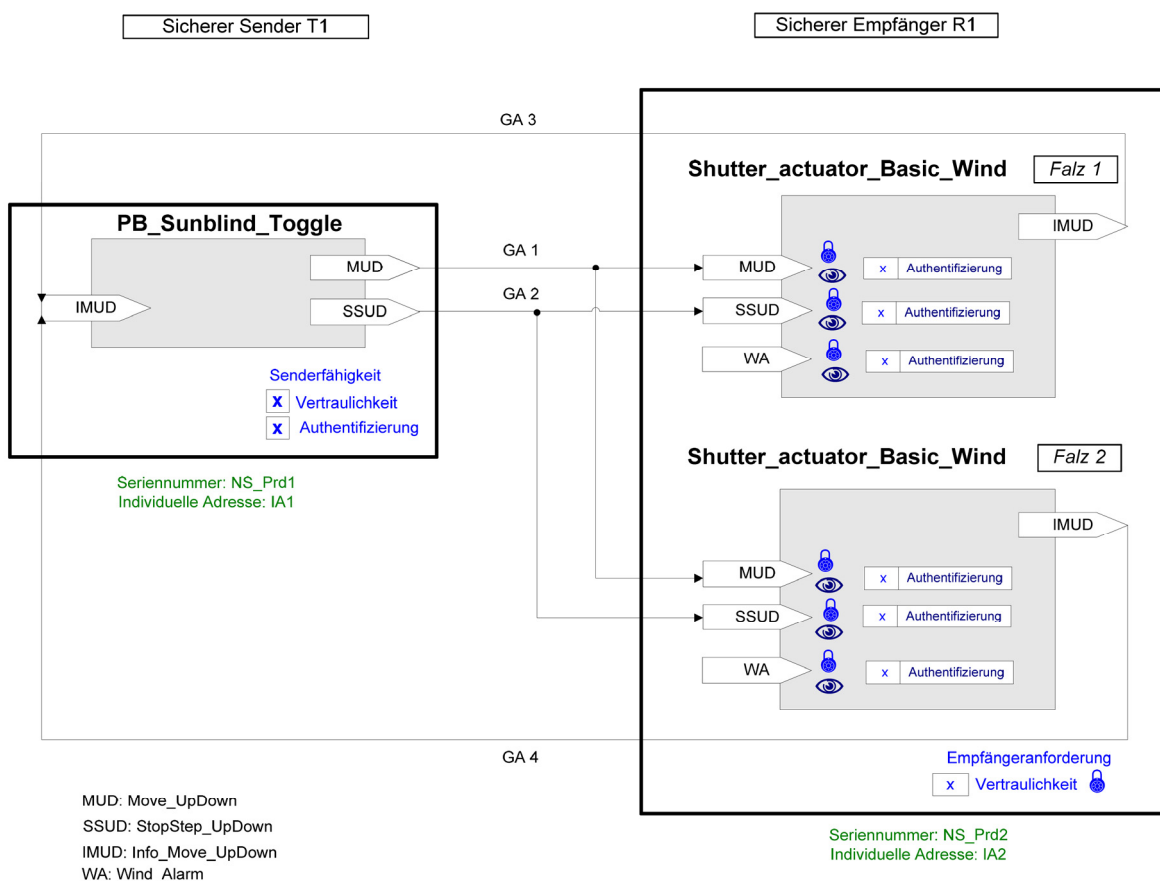


Bild 2 – Sichere Kommunikation zwischen einem sicheren bidirektionalen Sender und einem bidirektionalen Empfänger, der sowohl eine Authentifizierung als auch Vertraulichkeit erfordert

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 verwaltet.

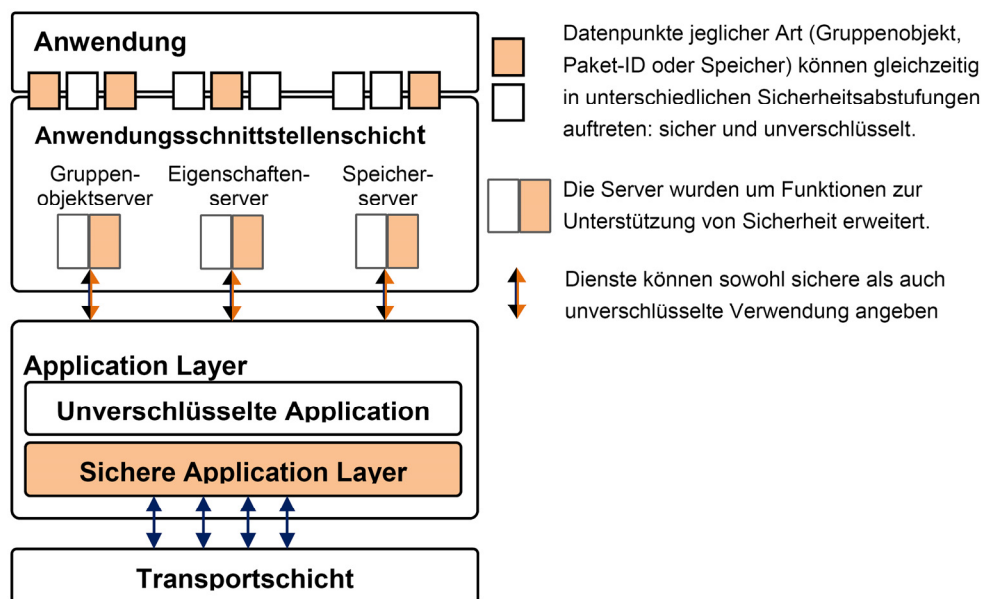


Bild 3 – Anordnung der ESHG-Datensicherheit im ESHG-Stack

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.



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.

5.1.1.1.3.1 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
- Telegrammauthentifizierungscode (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 Dienstes der unverschlüsselten Application Layer sein.

Format: Die Länge, die möglichen Unterfelder und deren Verschlüsselung müssen mit den Spezifikationen für den Dienst der unverschlüsselten Application Layer nach DIN 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.

- Telegrammauthentifizierungscode (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 Anforderungen unten 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.

Ctr_j

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

Byte 14 von Ctr_j muss „01h“ sein. Damit wird sichergestellt, dass B_0 und Ctr_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.

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

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							
								1	1	1	1	1	1	1	0	0	0	1												000000b																	

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“ wird das Feld „Vertraulichkeit“ gelöscht und das Feld „Authentifizierung“ wird gesetzt. Das Feld „SAI“ wird mit „00b“ ausgefüllt, 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“ enthalten sein.
 $A = SCF \mid 000000b \mid \text{Unverschlüsselte APDU (= unverschlüsselte APCI + Daten)}$
 $P = \{\text{leer}\}$
4. Die weitere Berechnung muss nach Anhang A erfolgen.
Der Block B_0 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.

Legende

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

 Schlüsseltext

Der Schlüsseltext der unverschlüsselten APDU und der MAC müssen wie folgt berechnet werden.

Telegrammerstellung

Der MAC muss mit dem CCM-Algorithmus berechnet werden und muss anschließend so für die CCM-Verschlüsselung verwendet werden, wie es in NIST SP 800-38A spezifiziert wird.

Sowohl für die Authentifizierung als auch für die Vertraulichkeit muss derselbe Schlüssel „k“ verwendet werden.

1. Im Feld „SCF“ wird das Feld „Vertraulichkeit“ und das Feld „Authentifizierung“ gesetzt; das Feld „SAI“ wird mit „00b“ ausgefüllt, 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.

Bei „Authentifizierung und Vertraulichkeit“

Bei „Authentifizierung und Vertraulichkeit“ muss „P⁽²⁾“ die unverschlüsselte APDU enthalten und A²⁾ darf die unverschlüsselte APDU nicht enthalten, da sie bereits in „P“ enthalten ist.

$$A = SCF$$

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

Die weitere Berechnung muss nach Anhang A.2 erfolgen.

Der Block B_0 muss nach der Spezifikation in 5.1.1.1.3.2 aufgebaut sein.

Die Blöcke Ctr_0 bis Ctr_n müssen nach der Spezifikation in 5.1.1.1.3.2 aufgebaut sein.

4. Nach Bild A.2 muss das Ergebnis C (Schlüsseltext) nach dem Feld „SeqNr“ auf ESHG übertragen werden.

Telegrammentschlüsselung und -verifizierung

Die Entschlüsselung und Verifizierung des Telegramms im Empfänger muss auf exakt dieselbe Weise gestartet werden wie im Sender und wie es in NIST SP 800-38A spezifiziert wird.

1. Das Feld „SeqNr“ verifizieren (siehe 5.1.1.3).
2. Das empfangene Telegramm mit dem Sicherheitsschlüssel entschlüsseln und die Nutzdaten rekonstruieren.

3. 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.)

5.1.1.1.4 Andere Sicherheitsalgorithmen

In Tabelle 2 sind die spezifizierten ESHG-Sicherheitsalgorithmen aufgeführt.

Werte für b7 und b6, die nicht definiert sind, sind reserviert. Diese Werte dürfen nicht verwendet werden.

Ein empfangenes sicheres Telegramm mit einem reservierten Wert für b_5b_4 muss ignoriert werden.

Anforderungen von möglichen zukünftigen Algorithmen

Der Algorithmus sollte nach der verfügbaren Hardwareleistung (Prozessorgeschwindigkeit, Arbeitsspeicher) ausgewählt werden. Dabei ist der Arbeitsspeicher das wichtigere Kriterium, da die Rechenzeit nur bei der erstmaligen Konfiguration des Geräts relevant ist.

5.1.1.2 Unterstützung des Dienstes „S-A_Data“

5.1.1.2.1 Dienst „S-A_Data“

5.1.1.2.1.1 Grundlegende Anforderungen

Die S-AL muss den Dienst „S-A_Data“ unterstützen. In Senderichtung muss dieser Dienst den Dienst der unverschlüsselten Application Layer schützen; in Empfangsrichtung muss der Dienst die Sicherheit einer empfangenen S-A_Data-PDU sicherstellen. Die S-AL muss das Sicherheitssteuerungsfeld innerhalb der sicheren Application Layer-Dienstdateneinheit (en: Application Layer Service Data Unit (ASDU)) handhaben.

ANMERKUNG In diesem Unterabschnitt wird nur der Dienst „S-A_Data“ spezifiziert. Es wird nicht spezifiziert, wann der Dienst anzuwenden ist. Dies ist abhängig vom Wert der Sicherheitsdienstparameter „par_auth“ und „par_conf“ und wird nachstehend in 5.1.1.5 „Sichere Handhabung der Dienste der Transportschicht“ näher erläutert.

Der Dienst „S-A_Data“ muss ein interner Dienst der Application Layer sein. Das Aufrufen des Dienstes darf nur in der S-AL unter Verwendung der Sicherheitsdienstparameter („par_auth“, „par_conf“ und „link_index“) der Dienste der unverschlüsselten Application Layer möglich sein; es darf nicht möglich sein, den Dienst explizit aufzurufen. Der Dienst „S-A_Data“ darf auf keiner externen Telegrammschnittstelle verfügbar sein.

Der Dienst „S-A_Data“ muss die unverschlüsselte AL-Dienst-PDU in Senderichtung durch die verschlüsselte sichere APDU und in Empfangsrichtung umgekehrt ersetzen.

Die lokale S-AL muss den Dienst „S-A_Data“ verwenden, um eine S-A_Data-PDU auf dem Bus zu übertragen. Die lokale S-AL muss die enthaltene unverschlüsselte AL-Dienst-PDU in Abhängigkeit von Folgendem schützen:

- Sicherheitsdienstparameter „par_auth“ und „par_conf“ des Dienstes der unverschlüsselten Application Layer;
- Sicherheitskonfigurationsinformationen in Abhängigkeit vom unverschlüsselten AL-Dienst (Schlüssel, TSAP-Typ);
- TSAP oder ASAP:
BEISPIEL Für eine andere Ziel-Gruppenadresse oder eine andere individuelle Zieladresse weicht der Schlüssel möglicherweise ab.
- Schichtparameter der S-AL.

Dies wird in den nachfolgenden Unterabschnitten näher spezifiziert.

Das Feld „SCF“ muss eine S-A_Data-PDU wie in Bild 12 dargestellt kennzeichnen.

Wenn die Remote-S-AL eine S-A_Data-PDU empfängt, muss diese die Sicherheit anhand der Sicherheitsressourcen prüfen und muss die S-A_Data-PDU je nach Ergebnis der Prüfung ablehnen oder intern an die Application Layer übertragen.

5.1.1.2.1.2 Sichere APDU

Die S-A_Data-PDU muss das in Bild 11 dargestellte Format aufweisen.

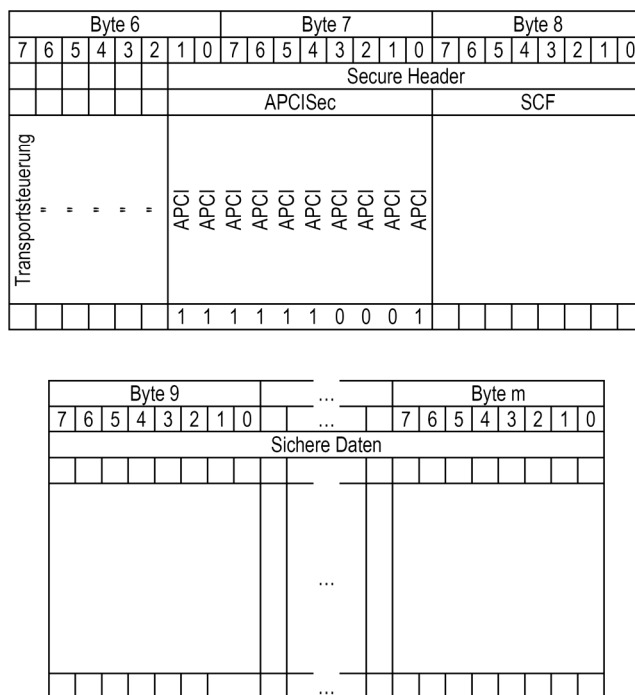


Bild 11 – Format der verschlüsselten sicheren APDU (informativ)

In den nachstehenden Abschnitten werden das Format und die Verwendung dieses Telegrammformats spezifiziert. Ein ausgearbeitetes Beispiel ist im Anhang B zu finden.

Die sichere APDU muss die folgenden Felder enthalten.

– Sicherer Header		
Definition:		Der sichere Header (en: Secure Header (SHD)) muss immer aus den Feldern „APCISec“ und „SCF“ bestehen.
	– APCISec	
	Definition:	Dies muss die dedizierte Protokollsteuerinformation der Application Layer sein, mit der die jeweilige APDU als sichere APDU gekennzeichnet werden muss.
	Wert:	APCISec = F31 _{APCI} = 3F1h = 1111110001b

– Sicherheitssteuerungsfeld																																																																					
Definition:	Das Sicherheitssteuerungsfeld (en: Security Control Field (SCF)) muss Angaben zur Vertraulichkeit, Authentifizierung, dem verwendeten Sicherheitsalgorithmus sowie zu möglichen Betriebsmodi enthalten.																																																																				
Codierung:	Das Feld „SCF“ muss 1 Byte groß sein und wie in Bild 12 dargestellt formatiert sein. <table><tr><td>b₇</td><td>b₆</td><td>b₅</td><td>b₄</td><td>b₃</td><td>b₂</td><td>b₁</td><td>b₀</td><td rowspan="2">Algorithmus</td><td rowspan="2">Dienst</td><td rowspan="2">Authentifizierung</td><td rowspan="2">Vertraulichkeit</td></tr><tr><td>T</td><td colspan="3">SAI</td><td>SBC</td><td colspan="3">S-AL-Dienst</td></tr><tr><td></td><td>0</td><td>0</td><td>0</td><td></td><td>0</td><td>0</td><td>0</td><td>CCM</td><td>S-A_Data-PDU</td><td>Ja</td><td>Nein</td></tr><tr><td></td><td>0</td><td>0</td><td>1</td><td></td><td>0</td><td>0</td><td>0</td><td>CCM</td><td>S-A_Data-PDU</td><td>Ja</td><td>Ja</td></tr><tr><td></td><td>0</td><td>0</td><td>1</td><td></td><td>0</td><td>1</td><td>0</td><td>CCM</td><td>S-A_Sync_Req-PDU</td><td>Ja</td><td>Ja</td></tr><tr><td></td><td>0</td><td>0</td><td>1</td><td></td><td>0</td><td>1</td><td>1</td><td>CCM</td><td>S-A_Sync_Res-PDU</td><td>Ja</td><td>Ja</td></tr></table> Bild 12 – Sicherheitssteuerungsfeld	b ₇	b ₆	b ₅	b ₄	b ₃	b ₂	b ₁	b ₀	Algorithmus	Dienst	Authentifizierung	Vertraulichkeit	T	SAI			SBC	S-AL-Dienst				0	0	0		0	0	0	CCM	S-A_Data-PDU	Ja	Nein		0	0	1		0	0	0	CCM	S-A_Data-PDU	Ja	Ja		0	0	1		0	1	0	CCM	S-A_Sync_Req-PDU	Ja	Ja		0	0	1		0	1	1	CCM	S-A_Sync_Res-PDU	Ja	Ja
b ₇	b ₆	b ₅	b ₄	b ₃	b ₂	b ₁	b ₀	Algorithmus	Dienst					Authentifizierung	Vertraulichkeit																																																						
T	SAI			SBC	S-AL-Dienst																																																																
	0	0	0		0	0	0	CCM	S-A_Data-PDU	Ja	Nein																																																										
	0	0	1		0	0	0	CCM	S-A_Data-PDU	Ja	Ja																																																										
	0	0	1		0	1	0	CCM	S-A_Sync_Req-PDU	Ja	Ja																																																										
	0	0	1		0	1	1	CCM	S-A_Sync_Res-PDU	Ja	Ja																																																										
– Tool-Zugriff (T)																																																																					
Definition:	Dieses Bit muss gesetzt sein, wenn die Sicherheit (Authentifizierung und/oder Vertraulichkeit) mit den Sicherheitsschlüsselinformationen eines Konfigurationstools implementiert wird. Es wird im Folgenden als „spezifischer Tool-Eintrag“ oder als „Tool-Schlüssel“ bezeichnet.																																																																				
Codierung:	<table><tr><td>b₅</td><td>Tool-Zugriff</td></tr><tr><td>0</td><td>Spezifischer Tool-Eintrag nicht belegt</td></tr><tr><td>1</td><td>Spezifischer Tool-Eintrag belegt</td></tr></table> Bild 13 – Tool-Zugriff	b ₅	Tool-Zugriff	0	Spezifischer Tool-Eintrag nicht belegt	1	Spezifischer Tool-Eintrag belegt																																																														
b ₅	Tool-Zugriff																																																																				
0	Spezifischer Tool-Eintrag nicht belegt																																																																				
1	Spezifischer Tool-Eintrag belegt																																																																				
– Sicherheitsalgorithmusbezeichner																																																																					
Definition:	Das Feld mit dem Sicherheitsalgorithmusbezeichner (en: Security Algorithm Identifier (SAI)) muss, sofern vorhanden, den verwendeten Sicherheitsalgorithmus und Betriebsmodus angeben und muss zusammen mit möglichen weiteren Sicherheitsalgorithmus-bezogenen Informationen verwendet werden.																																																																				
Codierung:	Tabelle 2 – Sicherheitsalgorithmusbezeichner <table><tr><td>b₆</td><td>b₅</td><td>b₄</td><td>Sicherheitsalgorithmus und Betriebsmodus</td></tr><tr><td>0</td><td>0</td><td>0</td><td>CCM (AES CTR für Vertraulichkeit und AES CBC für Authentifizierung) bei ausschließlicher Verwendung von Authentifizierung.</td></tr><tr><td>0</td><td>0</td><td>1</td><td>CCM mit Authentifizierung und Vertraulichkeit</td></tr></table> Andere Werte sind für zukünftige Normerweiterungen reserviert und dürfen nicht verwendet werden.	b ₆	b ₅	b ₄	Sicherheitsalgorithmus und Betriebsmodus	0	0	0	CCM (AES CTR für Vertraulichkeit und AES CBC für Authentifizierung) bei ausschließlicher Verwendung von Authentifizierung.	0	0	1	CCM mit Authentifizierung und Vertraulichkeit																																																								
b ₆	b ₅	b ₄	Sicherheitsalgorithmus und Betriebsmodus																																																																		
0	0	0	CCM (AES CTR für Vertraulichkeit und AES CBC für Authentifizierung) bei ausschließlicher Verwendung von Authentifizierung.																																																																		
0	0	1	CCM mit Authentifizierung und Vertraulichkeit																																																																		

		– System-Broadcast-Kennzeichnung (SBC)												
		Definition: Dieses Feld muss angeben, ob der resultierende Rahmen über einen Medienkoppler zu einem offenen Medium, das den System-Broadcast-Kommunikationsmodus unterstützt, per Broadcast bzw. per System-Broadcast-Kommunikationsmodus übergeben werden muss. Dieses Feld ist nur für den Sender relevant, um den Rahmen anhand des System-Broadcast-Kommunikationsmodus über einen Medienkoppler zu einem offenen Medium zu leiten, wenn der Rahmen in einem geschlossenen Medium im Broadcast-Kommunikationsmodus gesendet wurde, und für den Medienkoppler, damit dieser den Kommunikationsmodus bestimmen kann.												
		Codierung: <table><tr><th colspan="3">Tabelle 3 – System-Broadcast-Kennzeichnung</th></tr><tr><th>SBC</th><th>Name</th><th>Definition</th></tr><tr><td>0</td><td>Nach Dienst</td><td>Der Kommunikationsmodus wird vom verwendeten Dienst der Transportschicht definiert.</td></tr><tr><td>1</td><td>System-Broadcast</td><td>System-Broadcast muss als Kommunikationsmodus verwendet werden.</td></tr></table>	Tabelle 3 – System-Broadcast-Kennzeichnung			SBC	Name	Definition	0	Nach Dienst	Der Kommunikationsmodus wird vom verwendeten Dienst der Transportschicht definiert.	1	System-Broadcast	System-Broadcast muss als Kommunikationsmodus verwendet werden.
Tabelle 3 – System-Broadcast-Kennzeichnung														
SBC	Name	Definition												
0	Nach Dienst	Der Kommunikationsmodus wird vom verwendeten Dienst der Transportschicht definiert.												
1	System-Broadcast	System-Broadcast muss als Kommunikationsmodus verwendet werden.												

Die weiteren Felder in der sicheren APDU müssen von dem im Feld „Algorithmus“ angegebenen Sicherheitsalgorithmus sowie von der Verwendung der Authentifizierung und Vertraulichkeit abhängig sein. Dies wird in den nachfolgenden Unterabschnitten spezifiziert.

5.1.1.2.1.3 Kommunikationsmodus

In **Senderichtung** muss der Kommunikationsmodus gleich dem Kommunikationsmodus des anfordernden Dienstes der unverschlüsselten Application Layer sein, oder er muss dem im Dienstparameter „comm_mode“ angegebenen Kommunikationsmodus entsprechen. Die S-AL muss die SBC-Kennzeichnung nach Tabelle 4 setzen.

Tabelle 4 – Setzen der SBC-Kennzeichnung in der S-A_Data-PDU

Kommunikationsmodus des Dienstes der unverschlüsselten Application Layer	SBC-Kennzeichnung
Multicast	„Nach Dienst“
Broadcast	„Nach Dienst“
System-Broadcast	„System-Broadcast“
Punkt-zu-Punkt verbindungslos	„Nach Dienst“
Punkt-zu-Punkt verbindungsorientiert	„Nach Dienst“
ANMERKUNG Für die Definition der System-Broadcast-Kennzeichnung ist auf 5.1.1.2.1.2, Tabelle 3, Bezug zu nehmen.	

In **Empfangsrichtung** bestehen keine Anforderungen bezüglich der SBC-Kennzeichnung.

BEISPIEL Wenn eine T_Data_Group-PDU mit SBC-Kennzeichnung „System-Broadcast“ empfangen wird, wird dieses Telegramm akzeptiert.

5.1.1.2.1.4 Handhabung von Fehlern und Ausnahmen

Wenn in der Dienstprimitive „S-A_Data.req“ jegliche Fehler oder Ausnahmen auftreten, muss die S-AL dem Benutzer der unverschlüsselten Application Layer den Dienst der unverschlüsselten Application Layer negativ bestätigen („not_ok“).

Wenn z. B. die Implementierung von CCM nicht zusammen mit der Verwendung von „Nur Vertraulichkeit“ unterstützt wird, dies aber aufgrund der Kombination der Dienstparameter „par_auth“ und „par_conf“ (siehe 5.1.2.3) gefordert ist, muss der Dienst der unverschlüsselten Application Layer negativ bestätigt werden.

5.1.1.3 Handhabung der Sequenznummer

5.1.1.3.1 Handhabung der Laufzeit

Ziel

Die Sequenznummer muss die Datenaktualität sicherstellen und somit das System gegen Replay-Angriffe schützen.

Anforderungen an Sender und Empfänger

Der Sender muss den Wert der Sequenznummer für jede nachfolgende Übertragung an einem seiner sicheren Datenpunkte erhöhen. Es darf nur eine einzige Sequenznummer für jegliche sichere Kommunikation verwendet werden; es dürfen keine unterschiedlichen Sequenznummern pro sicherer Verbindung oder pro sicherem Datenpunkt verwendet werden.

Der Empfänger muss den Wert der Sequenznummer für jedes von der individuellen Adresse des Senders empfangene sichere Telegramm evaluieren. In offenen ESHG-Medien (ESHG RF, ESHG PL110) muss der Sender zusätzlich über die ESHG-Seriennummer und Domänenadresse identifiziert werden.

Format

Die Sequenznummer muss als unsigned 6 Byte (48 Bit) großer Zähler implementiert sein, wie in Bild 14 festgelegt.

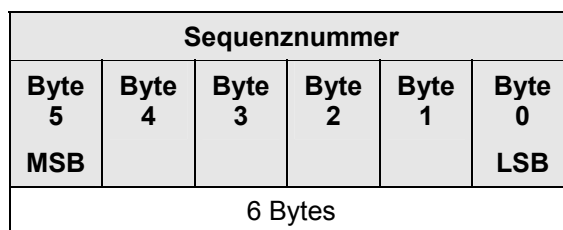


Bild 14 – Format der Sequenznummer

Grundlegendes Prinzip

Die Sequenznummer muss ein einfacher Zählerwert sein.

Dank des 6 Bytes umfassenden Formats dauert es über 100 000 Jahre bis das Ende des Zählers überschritten wird. Daher bestehen keine Anforderungen an die Handhabung von Zählerüberschreitungen bei Sequenznummern.

Für die spezifischen Anforderungen an die Handhabung der Sequenznummer für die einzelnen Kommunikationsmodi wird auf 5.1.1.5.3, 5.1.1.5.4, 5.1.1.5.5 und 5.1.1.5.6.2 Bezug genommen.

Übertragung

Der Sender muss für jegliche ausgehende Kommunikation eine einzige Sequenznummer beibehalten. Diese Sequenznummer muss in einer geeigneten Schnittstellenobjekteigenschaft gespeichert werden. Der Sender muss diesen Sequenznummernwert für die Übertragung über jede sichere Verbindung verwenden.

- Er muss diesen Wert in das Feld „SeqNr“ der sicheren APDU eintragen (siehe 5.1.1.1.3).
- Er muss den Wert der Sequenznummer bei der Berechnung des Initialisierungsvektors verwenden (siehe 5.1.1.1.3.4.2 und 5.1.1.1.3.5.2).

Nachdem die S-A_Data-PDU an die Transportschicht übergeben wurde, muss der Sender stets den Wert der Sende-Sequenznummer erhöhen.

Der Wert muss immer erhöht werden, unabhängig davon, wie das sichere Telegramm von den unteren Schichten weiter gehandhabt wird. Selbst wenn bei der Übertragung ein Fehler auftritt, z. B. aufgrund einer negativen Bestätigung der 2. Schicht, muss die Sequenznummer erhöht werden.

Empfang

Wenn ein Empfänger eine S-A_Data-PDU empfängt, muss dieser die darin enthaltene Sequenznummer mit der Sequenznummer vergleichen, die als „Letzte gültige SeqNr“ (en: Last Valid SeqNr) in der Tabelle mit sicheren individuellen Adressen für die individuelle Adresse des Senders der empfangenen S-A_Data-PDU gespeichert ist.

Wenn die individuelle Adresse des Senders nicht in der Tabelle mit sicheren individuellen Adressen gefunden wird oder der Konfigurationstool-Schlüssel nicht belegt ist, muss die S-A_Data-PDU ignoriert und der Rahmen verworfen werden; es darf kein Telegramm an die P-AL übergeben werden; abgesehen davon muss die Verarbeitung fortgesetzt werden.

ANMERKUNG 1 Bei S-A_Data-PDUs mit T=1 (Konfigurationstool-Schlüssel wird verwendet), ist die „Letzte gültige SeqNr“ für den Tool-Schlüssel-Zugriff außerhalb der *Tabelle mit sicheren individuellen Adressen* gespeichert.

- Wenn die empfangene Sequenznummer **größer** ist als die „Letzte gültige SeqNr“, muss die S-AL die S-A_Data-PDU akzeptieren.

Wenn die weiteren Sicherheitsprüfungen positiv verlaufen, muss der Empfänger den enthaltenen Wert für die Sequenznummer als die neue „Letzte gültige SeqNr“ des jeweiligen Senders in die Tabelle mit sicheren individuellen Adressen schreiben.

- Wenn die empfangene Sequenznummer **gleich** der „Letzten gültigen SeqNr“ ist, muss die S-AL die S-A_Data-PDU ignorieren. Sie darf nicht den gemeinsamen Sicherheitsfehlerzähler (en: Security Failure Common Counter (SFCC)) erhöhen.

ANMERKUNG 2 Somit wird es ermöglicht, dass eine zweite oder weitere Neuübertragung eines gültigen Rahmens durch die Sicherungsschicht des Senders, die sonst vom Empfänger nicht ordnungsgemäß als Neuübertragung erkannt werden würde, nicht fälschlicherweise als Wiedergabe eines aufgezeichneten Rahmens erkannt wird.

- Wenn die empfangene Sequenznummer **kleiner** ist als die „Letzte gültige SeqNr“, muss die S-AL wie folgt vorgehen.
 - Die S-AL muss die jeweilige S-A_Data-PDU ignorieren.
 - Die S-AL darf keine weiteren Telegramme von diesem Sender blockieren. Jegliche weiteren Telegramme von diesem Sender mit der richtigen Sequenznummer müssen wieder regulär verarbeitet werden.
 - Sie muss den gemeinsamen Sicherheitsfehlerzähler erhöhen. Bei den Sicherheitsfehlern in Verbindungen (en: Security Failures on Links) muss ein Eintrag mit der Verbindung, in der der Fehler aufgetreten ist, generiert oder aktualisiert werden, und es muss ein Fehler „E_SAIL“ gekennzeichnet werden.

Ressourcen

Sowohl der Sender als auch der Empfänger müssen für jeden Kommunikationspartner, mit dem eine sichere Verbindung besteht, die letzte gültige Sequenznummer in dem jeweiligen Eintrag der Tabelle mit sicheren individuellen Adressen speichern.

Anfangswert

Dabei muss es sich um folgenden Wert handeln:

- Wert im Auslieferungszustand und vor jeglicher sicheren Kommunikation über eine sichere Verbindung, oder
- Wert nach einem Master-Reset des Geräts.

Dieser Anfangswert darf nicht gleich Null sein, muss jedoch ein kleiner zufälliger Wert zwischen 1 und 255 sein.

5.1.1.3.2 Dienst „S-A_Sync“

Die hier beschriebene Vorgehensweise ist für den Fall bestimmt, dass ein Management-Client die aktuelle Sende-Sequenznummer eines Management-Servers und/oder den Wert der letzten gültigen Sequenznummer, die das Gerät für den Management-Client gespeichert hat, nicht kennt und diese Werte von dem Management-Server abrufen kann.

Der Benutzer der lokalen S-AL muss den Dienst „S-A_Sync“ verwenden, um die von der Remote-S-AL verwendete Sequenznummer sowie die Sequenznummer, die die Remote-S-AL von der lokalen S-AL erwartet, von der Remote-S-AL abzurufen.

- Der Benutzer der lokalen S-AL muss den Parameter **comm_mode** auf den Kommunikationsmodus setzen, der für die Übertragung der Anforderung verwendet werden muss.
 - Punkt-zu-Punkt (verbindungslos oder verbindungsorientiert, wenn eine Verbindung zur Transportschicht besteht)

Die Remote-S-AL muss mit einem lokalen ASAP adressiert werden, wobei es sich um den „IA_Index“ in der Tabelle mit sicheren individuellen Adressen handeln muss.

- Broadcast
- System-Broadcast
- Der Benutzer der lokalen S-AL muss den Parameter **key_select** auf den entsprechenden Schlüssel setzen, mit dem die Synchronisierung geschützt werden muss. Dies können Folgende sein:
 - der Tool-Schlüssel, oder

Der Tool-Schlüssel wird verwendet, wenn das Konfigurationstool ein sicheres Gerät verwalten möchte und die zu verwendende Sequenznummer sowie die vom Gerät verwendete Sequenznummer nicht kennt. In diesem Fall ist das Konfigurationstool der Benutzer der lokalen S-AL.

- der Schlüssel, der für den jeweiligen ASAP in der Tabelle mit sicheren individuellen Adressen gespeichert ist = IA_Index.

ANMERKUNG 1 Der Schlüssel, der für die Punkt-zu-Punkt-Kommunikation in der Tabelle mit Punkt-zu-Punkt-Schlüsseln gespeichert ist, wird in der Regel für die Synchronisierung verwendet, d. h., wenn ein sicheres Gerät die Sequenznummer von einem anderen sicheren Gerät abfragt.

ANMERKUNG 2 Auch für den (System-)Broadcast-Kommunikationsmodus wird der eindeutige Schlüssel für die Punkt-zu-Punkt-Kommunikation mit einem Management-Server verwendet, um das Telegramm zu schützen. Dabei kann nur ein einziges Gerät das Telegramm ordnungsgemäß verifizieren und darauf antworten, obwohl alle Geräte innerhalb der Domäne oder innerhalb der Anlage die Anforderung empfangen.

Der Benutzer der lokalen S-AL muss anhand des Parameters `serial_number` angeben, ob das Feld „KNX-Seriennummer“ (en: KNX Serial Number) in den S-A_Sync_Req-PDUs entweder:

- die KNX-Seriennummer des einzelnen Zielgeräts oder
- den Wert „0“ enthält.

Wenn der Dienst „S-A_Sync“ im System-Broadcast- oder Broadcast-Kommunikationsmodus verwendet wird, muss die KNX-Seriennummer enthalten sein, und der Wert darf nicht „0“ sein.

Wenn der Dienst „S-A_Sync“ im Kommunikationsmodus Punkt-zu-Punkt, verbindungslos/ verbindungsorientiert verwendet wird, darf das Feld „KNX-Seriennummer“ die erwartete KNX-Seriennummer des Kommunikationspartners oder den Wert „0“ enthalten.

Die lokale S-AL muss die Dienstanforderung akzeptieren und muss die S-A_Sync_Req-PDU generieren, wie in Bild 15 spezifiziert. Die lokale S-AL muss die SBC-Kennzeichnung entsprechend dem Parameter „`comm_mode`“ setzen.

Sichere APCI	SCF	SeqNr _{lokal}	KNX-Seriennummer	Aufforderung	MAC
10 Bits	1 Byte	6 Bytes	6 Bytes	6 Bytes	4 Bytes
3F1h	9Ah			N ₁	

Bild 15 – Format der S-A_Sync_Req-PDUs (Beispiel – Feld „SCF“ mit gesetztem Tool-Schlüssel und gesetzter SBC-Kennzeichnung)

Die lokale S-AL muss die Remote-S-AL mit einer Aufforderung N₁ auffordern und muss die Sequenznummer „SeqNr_{lokal}“ hinzufügen, die sie vermeintlich für die Kommunikation mit der Remote-S-AL verwenden wird (d. h. den aktuellen Wert der Sende-Sequenznummer).

Anders als bei „S-A_Data“ darf bei der Übertragung der S-A_Sync_Req-PDU der Wert der Sende-Sequenznummer nicht geändert werden.

Bei der Aufforderung muss es sich um einen unsignierten 6 Byte großen Ganzzahlwert handeln. Die lokale S-AL muss nach Möglichkeit nicht dieselbe Aufforderung mehrmals verwenden, indem sie den Wert nach jeder Verwendung erhöht oder einen ausreichend zufälligen Wert verwendet.

Die lokale S-AL muss die S-A_Sync_Req-PDU mit Authentifizierung und Vertraulichkeit schützen. In Abhängigkeit von dem Parameter „`key_select`“ muss die Schlüsselanforderung „`key_request`“ aus Folgendem bestehen:

- dem Tool-Schlüssel^{a)}, wobei das Kennzeichen „T“ im Feld „SCF“ gesetzt sein muss, oder
- den Schlüssel, der mit dem IA_Index der Remote-S-AL in der Tabelle mit Punkt-zu-Punkt-Schlüsseln verknüpft ist, wobei das Kennzeichen „T“ im Feld „SCF“ gelöscht sein muss.

Die lokale S-AL muss die S-A_Sync_Req-PDU mit Authentifizierung und Vertraulichkeit schützen, wie es in 5.1.1.1.3.5 für den Dienst S-A_Data spezifiziert ist.

A = SCF | ESHG-Seriennummer

P = Aufforderung

a) Wenn der Tool-Schlüssel noch nicht zugewiesen ist, verwendet der Management-Client den werksseitigen Einrichtungsschlüssel (en: Factory Default Set up Key (FDSK)).

Ctr₀ und B₀ müssen der Spezifikation in 5.1.1.1.3.2 entsprechen; die Sequenznummer muss die Sequenznummer des Senders sein, in diesem Fall „SeqNr_{lokal}“.

Die lokale S-AL muss die Anforderung in Abhängigkeit vom Parameter „comm_mode“ mit einer Primitive „T_Data_Individual.req“, „T_Data_Connected.req“, „T_Data_Broadcast.req“ oder „T_Data_SystemBroadcast.req“ an die lokale Transportschicht übergeben. Die Parameter „ASAP“ und „Priorität“ müssen den entsprechenden Parametern „TSAP“ und „Priorität“ der Dienstprimitive der Transportschicht zugeordnet werden; die Transportschicht-Dienstdateneinheit (en: Transport Layer Service Data Unit (TSDU)) muss dann eine S-A_Sync_Req-PDU sein.

S-A_Sync.req(ASAP, comm_mode, key_select)

- ASAP: Muss entweder den IA_Index der individuellen Adresse des Kommunikationspartners oder die Verwendung des Tool-Schlüssels angeben.
- comm_mode: Muss einer der Folgenden sein:
- Punkt-zu-Domäne, verbindungslos (Broadcast)
 - Punkt-zu-allen-Punkten, verbindungslos (System-Broadcast)
 - Punkt-zu-Punkt, verbindungslos
 - Punkt-zu-Punkt, verbindungsorientiert
- key_select: Muss angeben, ob die Kommunikation per Tool-Schlüssel oder mit dem Schlüssel, der für den ASAP (IA_Index des Kommunikationspartners) in der Tabelle mit Punkt-zu-Punkt-Schlüsseln gespeichert ist, geschützt werden muss.
- serial_number Die ESHG-Seriennummer des Kommunikationspartners oder der Wert „0“.

Die lokale S-AL muss einen Timeout-Timer von 6 s starten, wenn das Telegramm an die lokale Transportschicht übergeben wird.

Wenn die Remote-S-AL eine Primitive „T_Data_Individual.ind“, „T_Data_Connected.ind“, „T_Data_Broadcast.ind“ oder „T_Data_SystemBroadcast.ind“ mit TSDU = S-A_Sync_Req-PDU empfängt, muss sie zunächst das Feld „ESHG-Seriennummer“ verifizieren.

- Wenn die S-A_Sync_Req-PDU im System-Broadcast- oder Broadcast-Kommunikationsmodus empfangen wird, muss die S-AL verifizieren, dass der Wert im Feld „ESHG-Seriennummer“ nicht „0“ ist. Wenn dies nicht der Fall ist, muss die S-A_Sync_Req-PDU ignoriert werden. Dies darf nicht im Sicherheitsfehlerprotokoll (en: Security Failures Log) aufgezeichnet werden.
- Wenn die S-A_Sync_Req-PDU im Kommunikationsmodus Punkt-zu-Punkt, verbindungslos/verbindungsorientiert empfangen wird und die enthaltene ESHG-Seriennummer nicht „0“ und somit ungleich der eigenen KNX-Seriennummer ist, muss die S-A_Sync_Req-PDU ignoriert werden. Dies darf ebenfalls nicht im Sicherheitsfehlerprotokoll aufgezeichnet werden.
- Die S-A_Sync_Req-PDU muss weiterverarbeitet werden:
 - wenn das Feld „KNX-Seriennummer“ nicht „0“ und gleich der eigenen ESHG-Seriennummer ist, oder
 - wenn das Feld „ESHG-Seriennummer“ gleich „0“ ist.
- In allen anderen Fällen darf die S-A_Sync_Req-PDU nicht weiterverarbeitet werden.

Wenn die S-A_Sync_Req-PDU in der Remote-S-AL weiterverarbeitet wird, muss diese die Sicherheit verifizieren.

Wenn in der S-A_Sync_Req-PDU das Kennzeichen „T“ gesetzt ist, muss der Tool-Schlüssel verwendet werden; andernfalls muss der Schlüssel, der sich in der Tabelle mit Punkt-zu-Punkt-Schlüsseln befindet, mit dem „IA_Index“ verwendet werden, auf dessen Grundlage die Quelladresse des Telegramms in der *Tabelle mit sicheren individuellen Adressen* gefunden wird.

Wenn die Remote-S-AL einen Fehler aufweist, darf sie nicht auf die „S-A_Sync.req“ antworten.

- Wenn das Kennzeichen „T“ im Feld „SCF“ nicht gesetzt ist und die Remote-S-AL die Quelladresse des Telegramms „S-A_Sync.req“ nicht in der *Tabelle mit sicheren individuellen Adressen* findet, muss sie das Telegramm ignorieren.
- Wenn in der Remote-S-AL ein Fehler bei der Verifizierung der Sicherheit auftritt, muss sie das Telegramm ignorieren.

Wenn die Remote-S-AL die S-A_Sync_Req-PDU ordnungsgemäß entschlüsseln kann, muss sie mit einer S-A_Sync_Res-PDU antworten, wie in Bild 16 dargestellt.

Sichere APCI	SCF	Challenge XOR Random	SeqNr _{remote}	SeqNr _{lokal}	MAC
10 Bits	1 Byte	6 Bytes	6 Bytes	6 Bytes	4 Bytes
3F1h	9Bh				

Bild 16 – Format der S-A_Sync_Res-PDU (Beispiel – Feld „SCF“ mit gesetztem Tool-Schlüssel und gesetzter SBC-Kennzeichnung)

ANMERKUNG 3 Das Feld „ESHG-Seriennummer“ der S-A_Sync_Req-PDU wird in der S-A_Sync_Res-PDU durch das Feld „SeqNr_{lokal}“ ersetzt.

Die Remote-S-AL muss einen 6 Byte großen Zufallswert generieren und diesen per XOR-Verknüpfung mit der Aufforderung verknüpfen. Das Ergebnis muss der S-A_Sync_Res-PDU als Klartext im Feld „Challenge XOR Random“ (Aufforderung XOR Zufallszahl) hinzugefügt werden.

„SeqNr_{lokal}“ muss der Sequenznummer entsprechen, die die Remote-S-AL in der nachfolgenden Kommunikation von der lokalen S-AL erwartet, und „SeqNr_{remote}“ muss der Sequenznummer entsprechen, die die Remote-S-AL in der weiteren sicheren Kommunikation selbst verwenden wird.

„SeqNr_{lokal}“ in der Antwort entspricht der Sequenznummer, die die Remote-S-AL in der nachfolgenden Kommunikation von der lokalen S-AL erwartet; daher muss dies der Wert um „1“ erhöht sein, den die Remote-S-AL zuletzt von der lokalen S-AL empfangen hat. Dies ist die niedrigste Sequenznummer, die die Remote-S-AL von der lokalen S-AL akzeptiert. Dieser Wert unterscheidet sich in der Regel von dem Wert „SeqNr_{lokal}“ in der Anforderung.

- Der Benutzer der Remote-S-AL muss den Parameter „comm_mode“ der S-A_Sync_Res-PDU auf den gleichen Wert setzen, den der Parameter „comm_mode“ der Anforderung enthält, auf die geantwortet wird. Dies können folgende Werte sein:
 - Punkt-zu-Punkt (verbindungslos oder verbindungsorientiert, wenn eine Verbindung zur Transportschicht besteht)

Die lokale S-AL (Anfordernder) muss mit einem ASAP adressiert werden, wobei es sich um den „IA_Index“ der lokalen individuellen Adresse (Anfordernder) in der Tabelle mit sicheren individuellen Adressen der Remote-S-AL handelt. Dieser Index muss von der Remote-Transportschicht einer individuellen Adresse zugeordnet werden.

 - Broadcast oder
 - System-Broadcast
- Die Remote-S-AL muss die Antwort mit Authentifizierung und Vertraulichkeit schützen und dabei den in der Anforderung verwendeten Schlüsseltyp verwenden; daher muss es sich bei dem Parameter „key_response“ um einen der folgenden Schlüssel handeln:
 - den Tool-Schlüssel oder
 - den Schlüssel, der in der Tabelle mit Punkt-zu-Punkt-Schlüsseln für den „IA_Index“ der individuellen Adresse des Anfordernden konfiguriert ist.

Das Kennzeichen „T“ im Feld „SCF“ muss entsprechend gesetzt sein.

Die Remote-S-AL muss die S-A_Sync_Res-PDU mit Authentifizierung und Vertraulichkeit schützen, wie es in 5.1.1.1.3.5 für den Dienst S-A_Data spezifiziert ist.

$$A = SCF_i$$

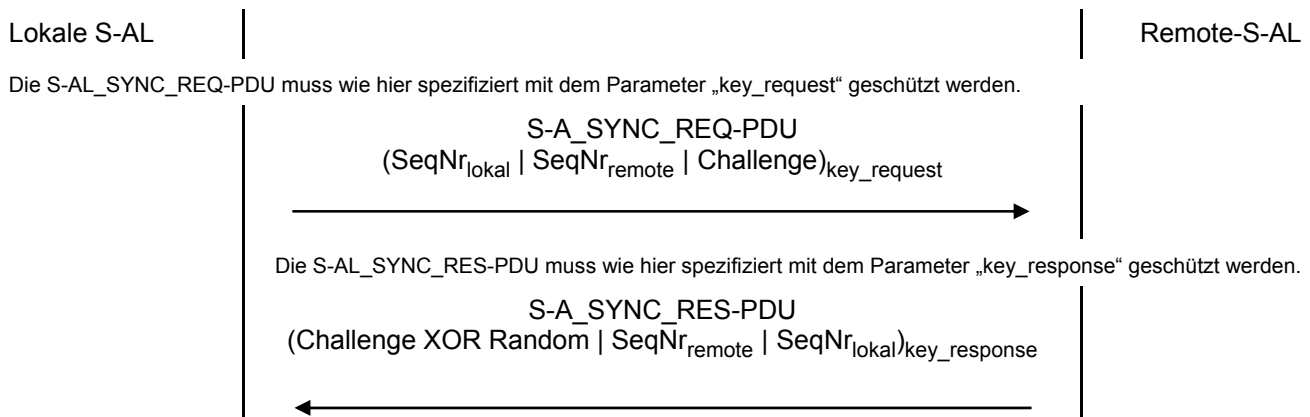
$$P = SeqNr_{remote} | SeqNr_{lokal}$$

Ctrl₀ und B₀ müssen nach der Spezifikation in 5.1.1.1.3.2 aufgebaut sein.

Die Remote-S-AL muss die Anforderung in Abhängigkeit vom Parameter „comm_mode“ mit einer Primitive „T_Data_Individual.req“, „T_Data_Connected.req“, „T_Data_Broadcast.req“ oder „T_Data_SystemBroadcast.req“ an die Remote-Transportschicht übergeben. Die Parameter „ASAP“ (IA_Index) und „Priorität“ müssen den entsprechenden Parametern „TSAP“ (individuelle Adresse) und „Priorität“ der Dienstprimitive der Transportschicht zugeordnet werden; die Transportschicht-Dienstdateneinheit (en: Transport Layer Service Data Unit (TSDU)) muss dann eine S-A_Sync_Res-PDU sein.

Entsprechend dem 2. Abschnitt nach Bild 15, darf bei der Übertragung einer S-A_Sync_Res-PDU die Sende-Sequenznummer der Remote-S-AL nicht geändert werden.

Die Telegrammsequenz muss wie folgt sein:



Wenn die lokale S-AL eine Primitive „T_Data_Individual.ind“, „T_Data_Connected.ind“, „T_Data_Broadcast.ind“ oder „T_Data_SystemBroadcast.ind“ mit TSDU = S-A_Sync_Res-PDU empfängt, muss sie wie folgt vorgehen:

- Sie muss den Wert des Parameters „Random“ berechnen, indem am Feld „Challenge XOR Random“ eine XOR-Operation mit der ursprünglichen Aufforderung durchgeführt wird, die die lokale S-AL beim Initiieren der S-A_Sync_Req-PDU selbst generiert hat.
- Dann muss sie die Sicherheit verifizieren.

Für die 6 Bytes von Ctrl_i muss sie den oben berechneten Zufallswert verwenden, siehe Bild 8.

Wenn in der S-A_Sync_Res-PDU das Kennzeichen „T“ gesetzt ist, muss der Tool-Schlüssel verwendet werden; andernfalls muss der Schlüssel verwendet werden, der durch die Tabelle mit sicheren individuellen Adressen und die Tabelle mit Punkt-zu-Punkt-Schlüsseln mit der Quelladresse des Telegramms verknüpft ist.

Wenn die lokale S-AL das Telegramm ordnungsgemäß entschlüsseln kann, muss sie dem Benutzer der lokalen S-AL den Dienst positiv bestätigen. Wenn jegliche Probleme wie ein Sicherheitsfehler oder eine Zeitüberschreitung auftreten, muss die lokale S-AL dem Benutzer der lokalen S-AL den Dienst negativ bestätigen.

S-A_Sync.res(ASAP, comm_mode, key_select, result)

- ASAP: Muss entweder den IA_Index der individuellen Adresse des Kommunikationspartners oder die Verwendung des Tool-Schlüssels angeben.
- comm_mode: Muss einer der Folgenden sein:
- Punkt-zu-Domäne, verbindungslos (Broadcast)
 - Punkt-zu-allen-Punkten, verbindungslos (System-Broadcast)
 - Punkt-zu-Punkt, verbindungslos
 - Punkt-zu-Punkt, verbindungsorientiert
- key_select: Muss angeben, ob die Kommunikation per Tool-Schlüssel oder mit dem Schlüssel, der für die individuelle Adresse gespeichert ist (per IA_Index des Kommunikationspartners in der Tabelle mit sicheren individuellen Adressen und der Tabelle mit Punkt-zu-Punkt-Schlüsseln), geschützt werden muss.
- result:
- ok: Die Sequenznummer der Remote-S-AL wurde ordnungsgemäß empfangen
 - not_ok: Bei der Anforderung der Sequenznummer der Remote-S-AL ist ein Fehler aufgetreten

Handhabung von Fehlern und Ausnahmen

- Die Fehlerhandhabung für Fehler bei der Entschlüsselung wird oben spezifiziert.
- Wenn die S-AL eine A_Secure-PDU mit SCF-Codierung für eine S-A_Sync_Req-PDU oder S-A_Sync_Res-PDU empfängt, die nicht im Kommunikationsmodus Punkt-zu-Punkt verbindungslos/verbindungsorientiert, Broadcast oder System-Broadcast übertragen wurde, muss sie das Telegramm ignorieren.

5.1.1.4 Registrierung von Sicherheitsfehlern

Die **Handhabung** von Sicherheitsfehlern ist vorgeschrieben und wird im Zusammenhang mit der Spezifikation der einzelnen Teile der S-AL beschrieben. In diesem Unterabschnitt wird nur die **Registrierung** von Sicherheitsfehlern spezifiziert.

Ein Sicherheitsfehler ist ausschließlich als Fehler spezifiziert, der bei der Sicherheitsprüfung im S-AL-Dienst auftritt. Jegliche andere Ausnahmen in der S-AL sind keine Sicherheitsfehler.

Ein Sicherheitsfehler bezieht sich daher lediglich auf den Vorgang „Sicherheit prüfen“ in den Beispiel-Flussdiagrammen in Bild 19, Bild 20, Bild 21, Bild 22, Bild 23 und Bild 24.

Die folgenden Ereignisse müssen als Sicherheitsfehler interpretiert werden.

Bei diesen Ereignissen muss der SFCC erhöht werden und der S-AL-Fehlerzähler in der Verbindung mit Sicherheitsfehler (en: Security Failure Link (SFL)) wird möglicherweise ebenfalls erhöht, sofern dieser implementiert ist.

- Entschlüsselungsfehler
- Abweichung zwischen dem berechneten MAC-Wert und dem empfangenen MAC-Wert.

Das folgende Ereignis kann als Sicherheitsfehler interpretiert werden.

Diese Ereignisse können zu einer Aktualisierung des Zählers für Sicherheitsfehler in Verbindungen führen.

- Empfang einer „SeqNr_{lokal}“ oder „SeqNr_{remote}“, die von der gespeicherten „SeqNr_{lokal}“ oder „SeqNr_{remote}“ abweicht, wenn die lokale S-AL annimmt, über den gültigen Wert für diese Sequenznummer zu verfügen.

BEISPIEL Wenn die lokale S-AL annimmt, dass sie über eine gültige „SeqNr_{lokal}“ verfügt, jedoch vom Kommunikationspartner eine höhere „SeqNr_{lokal}“ empfängt als erwartet, dann kann dies bedeuten, dass der Kommunikationspartner von einem anderen Client als dem Benutzer der S-AL mit einem ordnungsgemäß geschützten Tele-

5.1.1.5 Sichere Handhabung der Dienste der Transportschicht

5.1.1.5.1 Allgemeine Anforderungen

- In Empfangsrichtung, muss die S-AL für jeden Dienst der Transportschicht die folgenden Situationen handhaben, die vom Remote-Kommunikationspartner verursacht werden und bei denen es sich um Angriffe oder Versuche zur Umgehung der S-AL handeln kann.
 - Sie muss nach der unsicheren Verwendung von Verbindungen filtern, die in der Tabelle mit Punkt-zu-Punkt-Schlüsseln oder der Tabelle mit Gruppenschlüsseln enthalten sind.
 - Wenn das empfangene Telegramm geschützt ist, muss sie die Sicherheit verifizieren.
- In Senderichtung gibt es keine solchen Ausnahmen. Die Auswahl zwischen den Diensten der unverschlüsselten Application Layer und dem Dienst „S-A_Data“ muss anhand der Sicherheitsressourcen bestimmt werden.

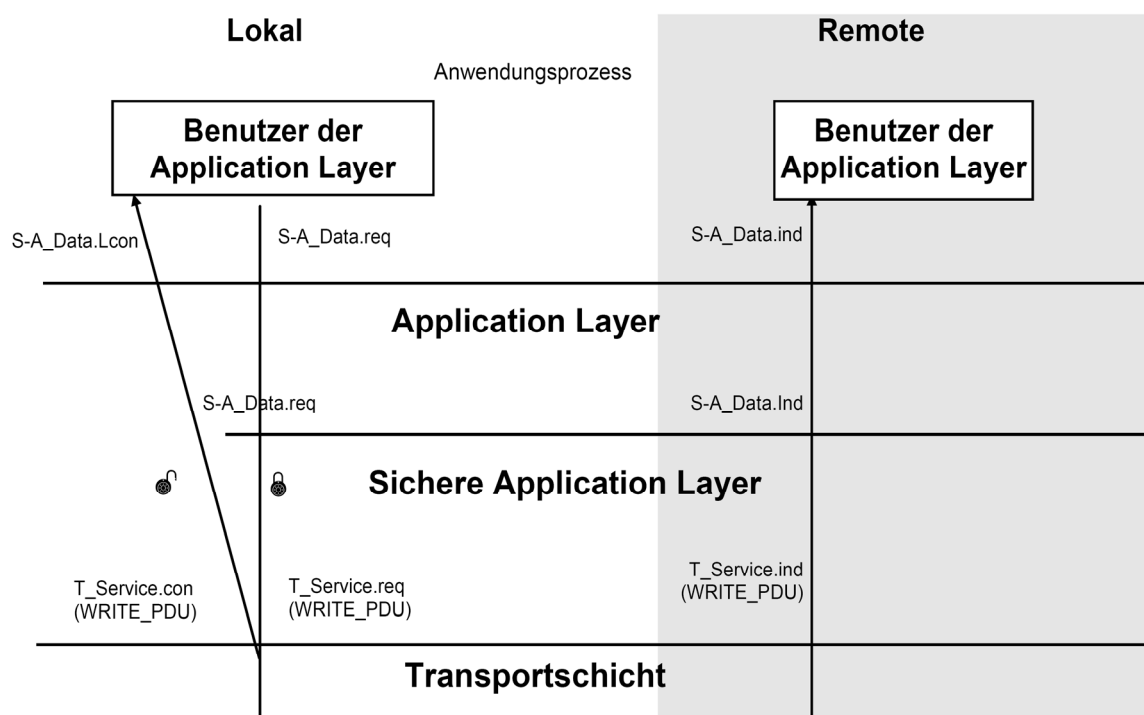


Bild 17 – Interaktivität der Application Layer für Dienste, die nicht fernbestätigt wurden

5.1.1.5.3 Sicherer Dienst der Application Layer im Multicast-Kommunikationsmodus – T_Data_Group

5.1.1.5.3.1 Verweisungen

Für die Spezifikation des Dienstes „T_Data_Group“ und die Handhabung von TSAPs und ASAPs in der Gruppenobjekt-Zuordnungstabelle wird auf DIN EN 50090-4-1, 3.1.1 „Beziehung zwischen TSAPs und ASAPs“, Bezug genommen.

5.1.1.5.3.2 Empfang – T_Data_Group.ind und T_Data_Group.con

In der Sequenz unten wird ein Entscheidungsbaum spezifiziert, der zu einer einzigen Schlussfolgerung für die Handhabung der Dienstprimitive „T_Data_Group.ind“ führt.

1. Wenn die Dienstprimitive „T_Data_Group.ind“ eine S-A_Data-PDU enthält, muss die S-AL den „GA_Index“ in der Tabelle mit Gruppenschlüsseln suchen.
 - 1.1 Wenn der „GA_Index“ in der *Tabelle mit Gruppenschlüsseln* gefunden wurde, muss die S-AL die enthaltene S-A_Data-SDU mit den im Feld „SCF“ angegebenen Sicherheitsmerkmalen entschlüsseln und die Sicherheit des Telegramms prüfen.
 - 1.1.1 Wenn die Sicherheitsprüfung ein positives Ergebnis liefert, muss die S-AL die P-AL entsprechend den enthaltenen Primitiven „A_GroupValue_Read.ind(/.Acon)“ oder „A_GroupValue_Write.ind(/.Acon)“ informieren, die aus dem Dienst „S-A_Data“ decodiert wurden. Die Sicherheitsdienstparameter „par_auth“ und „par_conf“ müssen entsprechend der Verwendung in der S-A_Data-PDU gesetzt werden, und der Index der sicheren Verbindung (link_index) muss ebenfalls übergeben werden.
 - 1.1.2 Wenn die Sicherheitsprüfung ein negatives Ergebnis liefert, muss die S-AL dies als Angriff interpretieren und entsprechend handhaben. (Siehe auch Ausnahme 1 unten). Das Telegramm darf nicht an die P-AL übergeben werden.
 - 1.2 Wenn der „GA_Index“ nicht in der Tabelle mit Gruppenschlüsseln gefunden wurde, muss die S-A_Data-PDU ignoriert werden. (Siehe auch Ausnahme 2). Das Telegramm darf nicht an die P-AL übergeben werden.
2. Wenn die Dienstprimitive „T_Data_Group.ind“ keine S-A_Data-PDU enthält, muss die S-AL das Telegramm unverändert an die P-AL übergeben. Die Sicherheitsdienstparameter *par_auth* und *par_conf* müssen beide gelöscht werden; der „link_index“ der Parameter muss auf „none“ gesetzt sein. Die Dienstprimitive „T_Data_Group.ind“ kann derzeit nur die Anzeigen „APCI_GroupValue_Write“, „APCI_GroupValue_Read“ oder „APCI_GroupValue_Response“ enthalten.

Handhabung von Fehlern und Ausnahmen

Es gilt die allgemeine Fehlerhandhabung nach der Spezifikation in 5.1.1.5.2. Es gibt keine spezifische Handhabung von Fehlern und Ausnahmen für die Dienstprimitiven „T_Data_Group.ind“ oder „T_Data_Group.con“.

Beispiel-Flussdiagramm

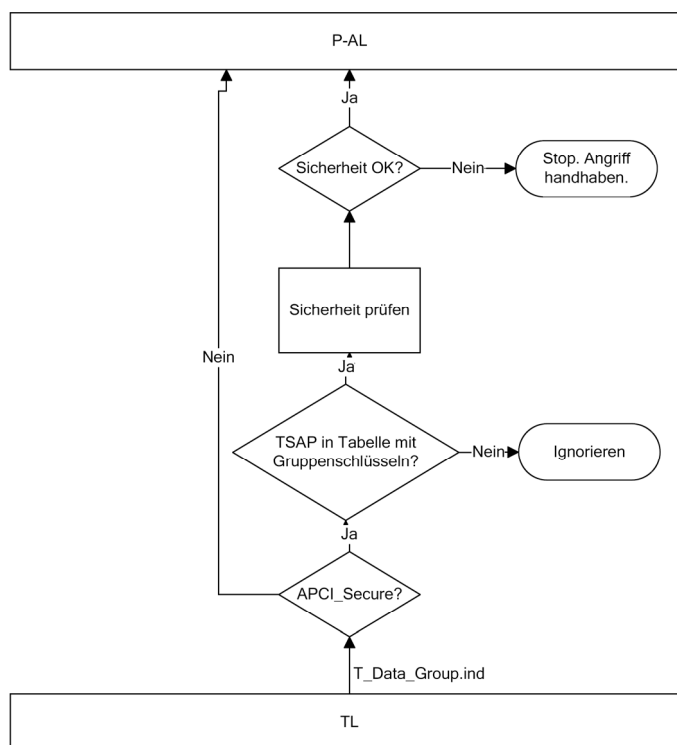


Bild 19 – Handhabung der Dienstprimitiven „T_Data_Group.ind“ durch die S-AL (informativ)

5.1.1.5.3.3 Senden – T_Data_Group.req

Wenn die S-AL eine APDU (APCI + Daten) handhabt, die anhand einer Dienstprimitive „T_Data_Group.req“ gesendet werden soll, muss die S-AL nach dem folgenden Entscheidungsbaum Schlussfolgerungen zur Handhabung basierend auf den Sicherheitsdienstparametern *par_auth* und *par_conf* des Dienstes der Application Layer ziehen.

1. Die S-AL muss die Sicherheitsdienstparameter *par_auth* und *par_conf* des Dienstes der Application Layer prüfen.
 - 1.1 Wenn einer dieser Parameter gesetzt ist, muss die S-AL prüfen, ob der für die Dienstprimitive „T_Data_Group.req“ verwendete TSAP (= GA_Index) in der *Tabelle mit Gruppenschlüsseln* enthalten ist.
 - 1.1.1 Wenn der TSAP in der *Tabelle mit Gruppenschlüsseln* gefunden wurde, muss die S-AL die im Dienst angeforderten Sicherheitsmerkmale anwenden (Authentifizierung und/oder Vertraulichkeit) und die sichere APDU generieren (siehe 5.1.1.1.3.1), die mit einer Dienstprimitive „T_Data_Group.req“ an die Transportschicht übergeben werden muss. (Siehe allgemeiner Fehler 3).
 - 1.1.2 Wenn der TSAP nicht in der *Tabelle mit Gruppenschlüsseln* gefunden wurde, muss die S-AL der AIL den Dienst der Application Layer negativ bestätigen.
 - 1.2 Wenn kein Sicherheitsdienstparameter gesetzt ist, muss die S-AL die APDU unverändert mit einer Dienstprimitive „T_Data_Group.req“ an die Transportschicht übergeben.

Handhabung von Fehlern und Ausnahmen

Es gilt die allgemeine Fehlerhandhabung nach der Spezifikation in 5.1.1.5.2. Es gibt keine spezifische Handhabung von Fehlern und Ausnahmen für die Dienstprimitive „T_Data_Group.req“.

Beispiel-Flussdiagramm

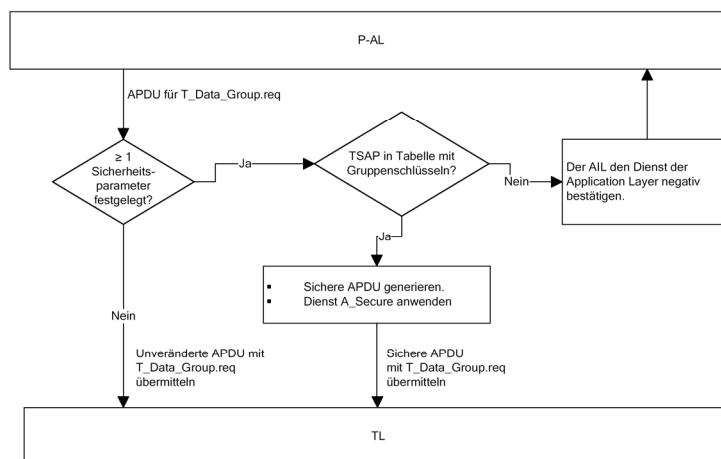


Bild 20 – Handhabung der Dienstprimitive „T_Data_Group.req“ durch die S-AL (informativ)

5.1.1.5.4 Sicherer Dienst der Application Layer im Multicast-Kommunikationsmodus – T_Data_Tag_Group

5.1.1.5.4.1 Verweisungen

Für die Spezifikation des Dienstes „T_Data_Tag_Group“ wird auf DIN EN 50090-4-2 Bezug genommen.

Im Folgenden wird eine Tabelle mit Zonenschlüsseln verwendet. Es dürfen nur die Einträge verwendet werden, in denen das Feld „Extended Frame Format“ gleich dem EFF-Typ der Dienstprimitive der Transportschicht oder der Application Layer ist, die gehandhabt wird.

5.1.1.5.4.2 Empfang – T_Data_Tag_Group.ind und T_Data_Tag_Group.con

In der Sequenz unten wird ein Entscheidungsbaum spezifiziert, der zu einer einzigen Schlussfolgerung für die Handhabung der Dienstprimitive „T_Data_Tag_Group.ind“ führt.

1. Wenn die Dienstprimitive „T_Data_Tag_Group.ind“ eine S-A_Data-PDU enthält, muss die S-AL die Zonenadresse (TSAP) in der *Tabelle mit Zonenschlüsseln* suchen. Der TSAP-Typ muss „empfangende LTE-Gruppenadresse“ sein.
 - 1.1 Wenn die Zonenadresse in der *Tabelle mit sicheren Verbindungen* gefunden wurde (möglicherweise durch die Evaluierung von Platzhaltern), muss die S-AL die enthaltene S-A_Data-SDU entschlüsseln und die Sicherheit des Telegramms prüfen.
 - 1.1.1 Wenn die Sicherheitsprüfung ein positives Ergebnis liefert, muss die S-AL die P-AL entsprechend den enthaltenen Primitiven „A_GroupPropValue_Read.ind“, „A_GroupPropValue_Response.ind“, „A_GroupPropValue_Write.ind“ oder „A_InfoReport.ind“ informieren, die aus dem Dienst „S-A_Data“ decodiert wurden.
Die Sicherheitsdienstparameter *par_auth* und *par_conf* müssen entsprechend der Verwendung in der S-A_Data-PDU gesetzt werden, und der Index der sicheren Verbindung (*link_index*) muss ebenfalls übergeben werden.
 - 1.1.2 Wenn die Sicherheitsprüfung ein negatives Ergebnis liefert, muss die SAL dies als Angriff interpretieren und entsprechend handhaben. Das Telegramm darf nicht an die P-AL übergeben werden.

- 1.2 Wenn die Zonenadresse nicht in der Tabelle mit Zonenschlüsseln gefunden wurde, muss die S-A_Data-PDU ignoriert werden. (Siehe auch 2). Das Telegramm darf nicht an die P-AL übergeben werden.
2. Wenn die Dienstprimitive „T_Data_Tag_Group.ind“ keine S-A_Data-PDU enthält, muss die S-AL die Dienstprimitive „T_Data_Tag_Group.ind“ unverändert an die P-AL übergeben. Die Sicherheitsdienstparameter *par_auth* und *par_conf* müssen beide gelöscht werden; der „link_index“ der Parameter muss auf „none“ gesetzt sein.

Handhabung von Fehlern und Ausnahmen

Es gilt die allgemeine Fehlerhandhabung nach der Spezifikation in 5.1.1.5.2. Es gibt keine spezifische Handhabung von Fehlern und Ausnahmen für die Dienstprimitiven „T_Data_Tag_Group.ind“ und „T_Data_Tag_Group.con“.

Beispiel-Flussdiagramm

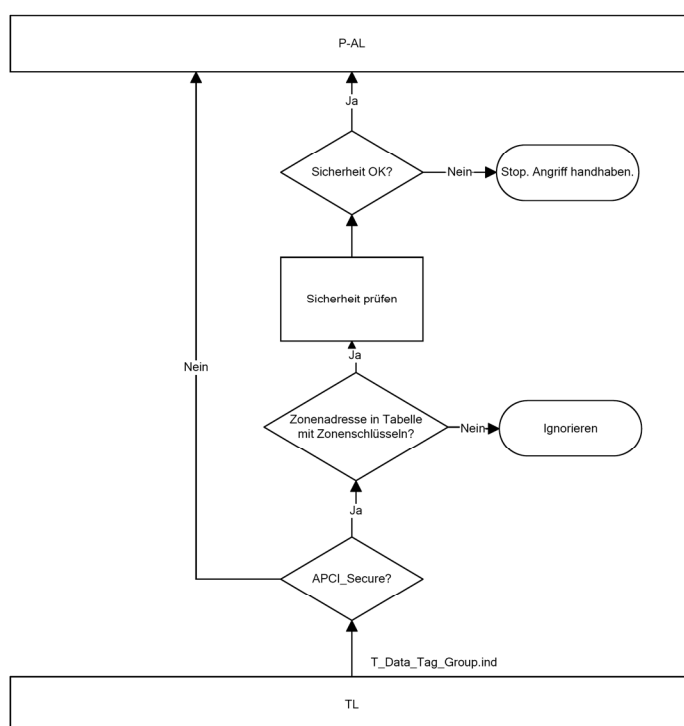


Bild 21 – Handhabung der Dienstprimitiven „T_Data_Tag_Group.ind“ durch die S-AL (informativ)

5.1.1.5.4.3 Senden – T_Data_Tag_Group.req

Wenn die S-AL eine APDU (APCI + Daten) handhabt, die anhand einer Dienstprimitive „T_Data_Tag_Group.req“ gesendet werden muss, muss die S-AL nach dem folgenden Entscheidungsbaum Schlussfolgerungen zur Handhabung basierend auf den Sicherheitsdienstparametern *par_auth* und *par_conf* des Dienstes der Application Layer ziehen.

1. Die S-AL muss die Sicherheitsdienstparameter *par_auth* und *par_conf* des Dienstes der Application Layer prüfen.
 - 1.1 Wenn einer dieser Parameter gesetzt ist, muss die S-AL die Zonenadresse und das für den Dienst der Application Layer verwendete Rahmenformat in der *Tabelle mit Zonenschlüsseln* suchen.
 - 1.1.1 Wenn die Kombination aus TSAP und Rahmenformat in der Tabelle mit Zonenschlüsseln gefunden wurde, muss die S-AL die im Dienstparameter der Application Layer angeforderten Sicherheitsmerkmale anwenden (Authentifizierung und/oder Vertraulichkeit) und