SLOVENSKI STANDARD
SIST EN 50090-3-4:2017

01-november-2017

Stanovanjski in stavbni elektronski sistemi (HBES) - 3-4. del: Specifikacija KNX S AL, varna storitev, varna konfiguracija in viri za varovanje

Home and Building Electronic Systems (HBES) - Part 3-4: Specification of KNX S AL, Secure Service, Secure configuration and security Resources

Ta slovenski standard je istoveten z: EN 50090-3-4:2017

ICS:

35.240.67	Uporabniške rešitve IT v gradbeništvu	IT applications in building and construction industry
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

SIST EN 50090-3-4:2017 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50090-3-4

August 2017

ICS 97.120

English Version

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

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

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

This European Standard was approved by CENELEC on 2017-06-12. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

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

Ref. No. EN 50090-3-4:2017 E

Contents

Page

European foreword

This document (EN 50090-3-4:2017) has been prepared by CLC/TC 205 "Home and Building Electronic Systems (HBES)".

The following dates are fixed:

- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2018-06-12
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2020-06-12

EN 50090-3 is composed with the following parts:

— EN 50090-3-1, *Home and Building Electronic Systems (HBES) — Part 3-1: Aspects of application —- Introduction to the application structure*;

— EN 50090-3-2, *Home and Building Electronic Systems (HBES) — Part 3-2: Aspects of application — User process for HBES Class 1*;

— EN 50090-3-3, *Home and Building Electronic Systems (HBES) — Part 3-3: Aspects of application — HBES Interworking model and common HBES data types*;

— EN 50090-3-4, *Home and Building Electronic Systems (HBES) — Part 3-4: Secure Application Layer, Secure Service, Secure configuration and security Resources*.

Introduction

KNX Association as Cooperating Partner to CENELEC confirms that to the extent that the standard contains patents and like rights, the KNX Association's members are willing to negotiate licenses thereof with applicants throughout the world on fair, reasonable and non-discriminatory terms and conditions.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. CENELEC shall not be held responsible for identifying any or all such patent rights.

CEN and CENELEC maintain online lists of patents relevant to their standards. Users are encouraged to consult the lists for the most up to date information concerning patents (ftp://ftp.cencenelec.eu/EN/IPR/Patents/IPRdeclaration.pdf).

1 Scope

This European Standard defines security for Home and Building HBES Open Communication System.

It is based on ISO/IEC 24767-2, Home network security / Secure Communication Protocol Middleware (SCPM).

Having a secure HBES solution has several advantages.

— It makes the HBES RF Communication Medium more secure:

  HBES RF Radio Frames in plain communication can easily be traced (by sniffer for example).

— It allows for secure applications.

  Secure communication is interesting in shutter – and door control and anti-intrusion security, in order to prevent intrusive commands (burglars…).

  It is also interesting in metering to protect for example electrical consumption data.

  This document does not define any type of application.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50090-1:2011, *Home and Building Electronic Systems (HBES) - Part 1: Standardization structure*

EN 50090-3-2, *Home and Building Electronic Systems (HBES) - Part 3-2: Aspects of application - User process for HBES Class 1*

EN 50090-4-1, *Home and Building Electronic Systems (HBES) - Part 4-1: Media independent layers - Application layer for HBES Class 1*

EN 50090-4-2, *Home and Building Electronic Systems (HBES) - Part 4-2: Media independent layers - Transport layer, network layer and general parts of data link layer for HBES Class 1*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50090-1:2011 and the following apply.

3.1.1
Access Control
definition and evaluation of which communication partner has the right to access which data or call which services, which is solved by collecting communication partners with the same rights for all data and services in Roles and defining for each Role and for each piece of data or service the Permissions that this Role has

3.1.2
Security Black List
standard list of services or DPs that shall exclusively be accepted using HBES Secure communication using confidentiality

3.1.3
cipher text
generic term that denotes the encrypted data

Note 1 to entry: Cipher text is opposed to *plain data*.

3.1.4
permission
definition and conditions (plain, authentication, confidentiality) of the functionality that will be accepted from a Role, in accessing a DP in a device or in accepting services from a communication partner

3.1.5
plain data
generic term that denotes unencrypted data, the content of which depends on the service and the user and not of confidentiality and authentication

Note 1 to entry: Plain data is opposed to *cipher text*.

3.1.6
secure DP
datapoint that requires either authentication and/or confidentiality

3.1.7
role
identification of a group of links to a device (multicast, unicast and other) that have the same Permissions throughout the AIL

3.1.8
secure link
link to a secure DP

3.1.9
Security Link Resources
whole collection of the following Resources:

— the Point-to-point Keys Table;

— the Group Keys Table;

— the Security Individual Address Table;

— the Tool Key

3.1.10
Group Address Security Flags
indication in a configuration tool whether for a Group Address, no secure communication will be used, or secure communication with authentication and/or confidentiality

3.1.11
Security White List
standard list of services or DPs that are always accepted using plain communication

3.2 Abbreviations

CFB	Cipher feedback
FDSK	Factory Default Setup Key
IV	Initialization Vector
MaC	Management Client
MaS	Management Server
MAC	Message Authentication Code
MiM	Man-in-the-Middle
P-AL	Plain Application Layer
SAI	Security Algorithm Identifier
S-AL	Secure Application Layer
SCF	Security Control Field
SeqNr	Sequence Number
SFCC	Security Failure Common Counter
SFL	Security Failure Links
SHD	Secure Header
SKI	Security Key Info

4 General Introduction (informative)

4.1 General

4.1.1 Common overview of HBES Security

This document specifies HBES Open Communication System Data Security, its Resources (of which the format may be manufacturer specific) and Procedures.

4.1.2 Product types

HBES Open Communication System Data Security is designed to be supported on all existing HBES Open Communication System Communication Media (HBES TP1, HBES PL110, HBES RF and HBES IP).

This document version does not introduce specific requirements on HBES data interfaces.

HBES Couplers are considered as well. The HBES Secure Frame format (see Figure 5) is designed so that it can be handled by existing HBES Couplers and newer.

EXAMPLE HBES TP1/RF Couplers.

4.1.3 Secure and plain communication in an installation

The end user [1)] wants to be sure that no unauthorized person will be able to control his receivers (shutters, doors….).

The end user can have many receivers of a unique kind and he would like to have secure communication only with some of them.

---

1) Home owner, building owner, building user, etc.

EXAMPLE He may require security for shutters in the lower part of the house, but not request security for shutters in the upper part of the house.

As secure design requires an extension of the HBES stack, it will be useful to have products:

— that use secure communication and plain communication, and

— other products that use only secure communication.

4.1.4 Prerequisites

Prerequisite 1

Secure communication shall be supported during runtime (typically multicast communication) and during Configuration (typically point-to-point communication).

Prerequisite 2

The need of a secure communication is a requirement from the receiver.

4.1.5 Product scheme examples

4.1.5.1 Example 1: A secure transmitter linked to a receiver that only requires Authentication

Figure 1 below deals with bidirectional devices.

NOTE For a unidirectional device, there is no link with the Datapoint "Info Status" (IMUD).

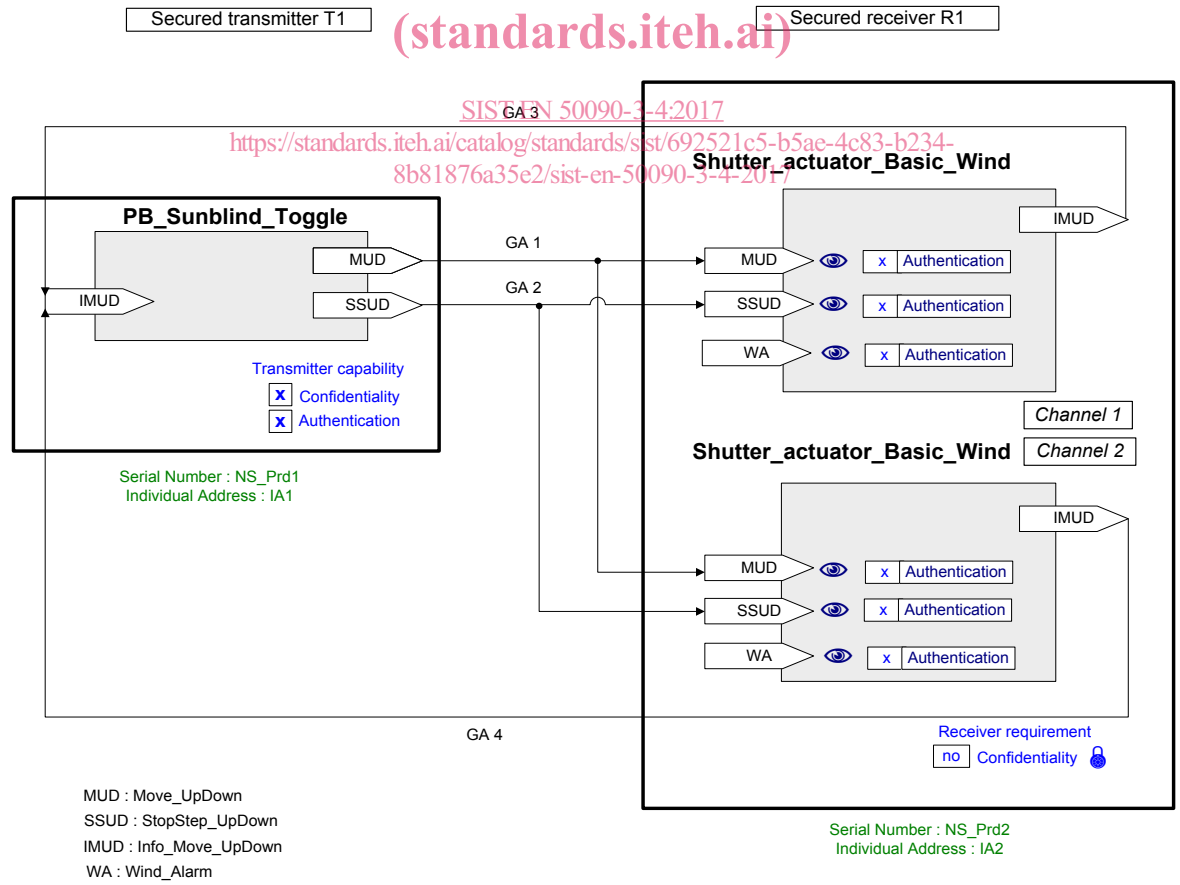

Figure 1 — Secure communication between a secure bidirectional transmitter and a bidirectional receiver that only requires authentication

The links are created during configuration. The security aspect can be defined by default in the product and in an offline product description or may be set by the configuration.

4.1.5.2 Example 2: A secure transmitter linked to a receiver that requires Authentication and Confidentiality

Figure 2 below deals with bidirectional devices.

NOTE For a unidirectional device, there is no link with the Datapoint “Info Status” (IMUD).

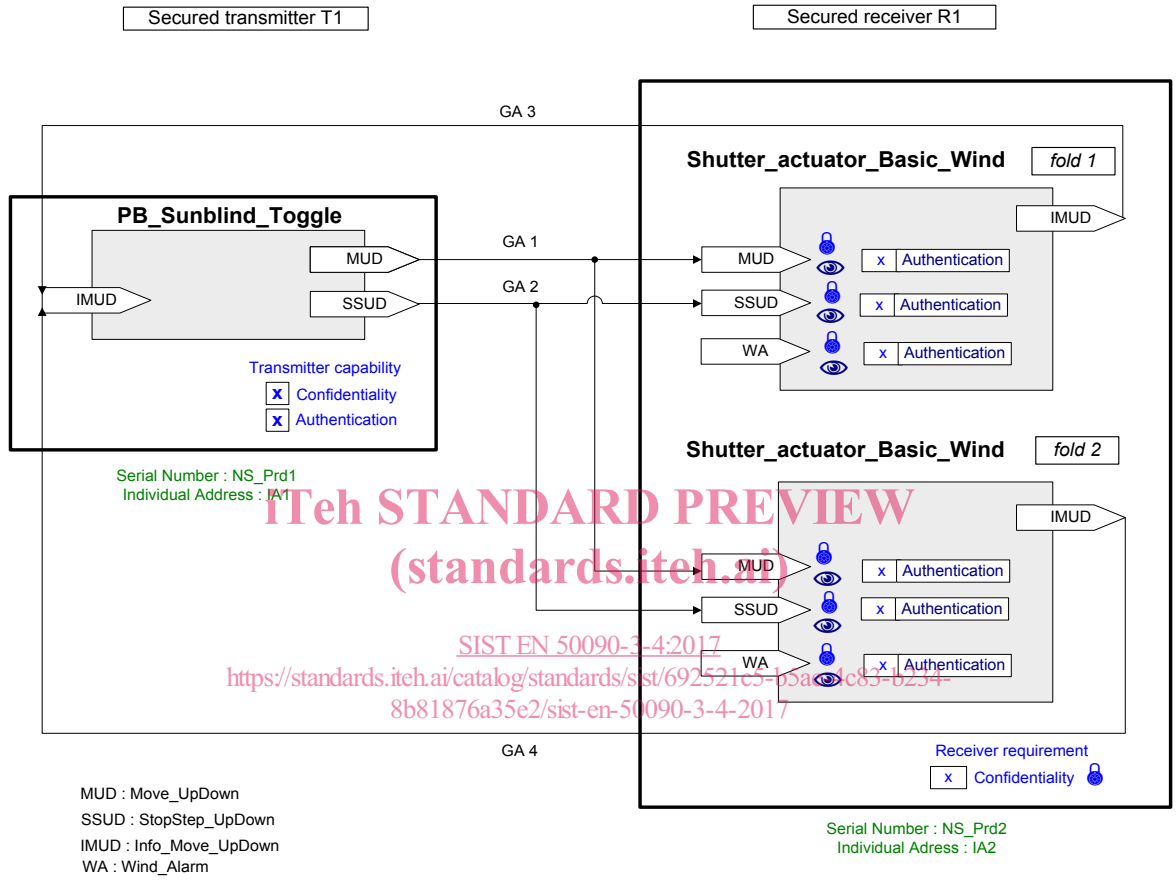

Figure 2 — Secure communication between a secure bidirectional transmitter and a bidirectional receiver that requires both authentication and confidentiality

4.1.6 Constraints

This document focusses on the HBES Security of end devices, for runtime and for configuration (although the resources needed for that are kept manufacturer specific). For the full-fledged support of HBES Security in HBES installations, the following is additionally considered necessary, but not yet in full specified in this document version. The functionality listed below is outside the scope of this standard version.

— Visualization and interfaces:

  Visualization requires that the visualization device (e.g. touch panel) or tool obtains in a secure way the security keys used in the HBES installation.

  Additionally, the interface (IP Tunnelling, USB) needs either to be a commissioned communication partner in the installation, or needs to be synchronized with the Sequence Number (SeqNr) field of the secure devices to which it communicates (sending and receiving).

— Media Coupler between a Secure HBES RF Subnetwork and a Plain HBES Subnetwork

USE CASE An existing HBES TP1 installation is extended with a HBES RF Subnetwork. Because of the open nature, it is chosen to have HBES Security communication on the HBES RF Subnetwork. Yet, it is not wanted that the existing HBES TP1 installation needs to be modified; the HBES TP1 installation is considered secure.

This requires that the HBES TP1/RF Media Coupler acts as a “Secure Proxy” for the HBES TP1 communication on the RF Subnetwork and handles the HBES Data Security when transferring secure messages from HBES RF to HBES TP1.

This HBES Secure Proxy and this HBES TP1/RF Media Coupler (“Security Gateway”) are not modelled in this standard version.

— HBES Data Security in a Subnetwork outside the building and no HBES Data Security inside the building.

— If a communication partner is given the key for the verification of a secure message, then this participant is also capable of sending secure messages itself. The installed devices would also react if it uses an IA that is present in their Point-to-point Keys Table or Group Keys Table.

EXAMPLE 1 Suppose that the access of people to a building is controlled using HBES with HBES Data Security, using authentication. If the building manager gives the used security key to a visualization tool, then this tool can rightfully verify the access control system as the proper sender of the messages. However, by having this security key, this visualization tool can itself in turn also send secure messages with this key. If the visualization tool would moreover use the IA of a legitimate device in the access control installation (and inherit its Sequence Number), then the receivers would also not be able to differentiate between messages from the “normal” senders and messages from this visualization tool.

— The introduction of HBES Data Security makes that in case of a failure of group communication it is more difficult to diagnose the cause to be either due to the configuration of the HBES Data Security or to other group communication aspects. Extended Group Object Diagnostics are currently being worked out.

EXAMPLE 2 If a secure sender sends a secure message to a secure receiver, and the secure receiver does not react, this can have many causes. Without security, there can be the following causes:

- The GA is not assigned to the receiver.
- The GA is not linked to the expected GO in the receiver.
- The flags for the GO in the receiver do not allow writing the GO-value.
- There are other causes in the receiver that make it not react to the message, like a locked state, a priority, etc.

Adding HBES Data Security, the following causes may be added:

- The sender and the receiver use different keys.
- The sender’s IA is not in the Point-to-point Keys Table or the Group Keys Table of the receiver.
- There is something wrong with the Sequence Number of the sender.

— The sender does not have the permission (Role) to write the GO-value in the receiver.

4.2 General Overview

4.2.1 Features of HBES Data Security

- Authentication:

  Use case for “Authentication only”: Bus-Monitors and Visualization Tools (e.g. counter displays) shall be able to analyse some traffic data without having the key (meaning the traffic cannot be authenticated). The reduced security of these points is somewhat compensated by the increased security of not having the key in some user accessible devices in some cases.

- Confidentiality.

- Access Control through Roles and Permissions.

4.2.2 Location of HBES Data Security in the HBES stack

HBES Data Security is handled by the Secure Application Layer (S-AL), the Application Layer and the Application Interface Layer, as indicated in Figure 3.

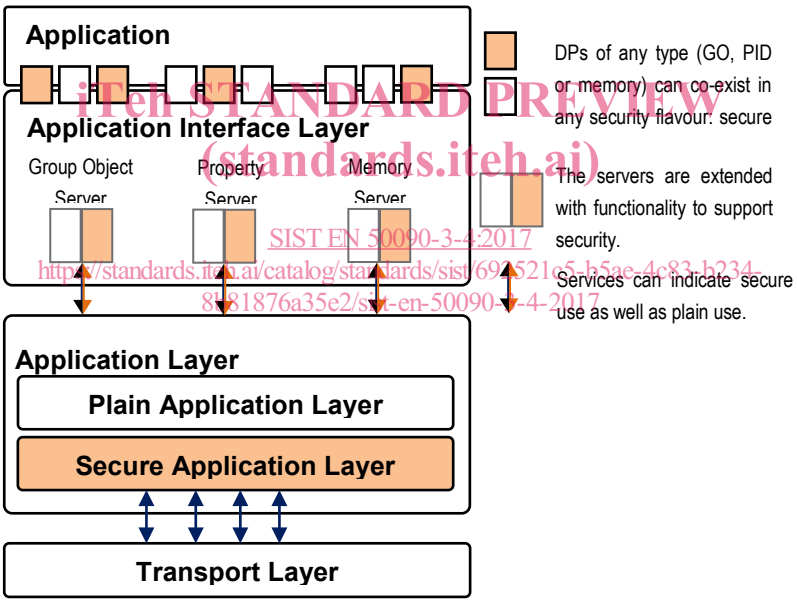

Figure 3 — Location of HBES Data Security in the HBES stack

Table 1 gives a brief overview of how security is handled at these layers.

Table 1 — Security features of the HBES layers (informative)

Feature	Layer		
	S-AL	P-AL	AIL
Operation Level	Link Level		Service Level Datapoint Level
Functionality	• Encrypt and decrypt secure messages • Handle exceptions at link level.	• Forward the AL-service with the security features for sending and receiving and the indication of the link. - Authentication or Confidentiality - Link Index	• Access Control - Support Roles - Handle Permissions
Resource	• Point-to-point Keys Table • Group Keys Table • Security Individual Address Table • and other	None.	• Point-to-point Keys Table

5 Specification

5.1 Stack and communication

5.1.1 Secure Application Layer

5.1.1.1 General requirements and overview

5.1.1.1.1 Embedding of the S-AL within the Application Layer and basic functionality

The Secure Application Layer (S-AL) shall take care of the HBES Data Security at the level of the links.

The S-AL shall be part of the Application Layer (AL). This shall allow that the S-A_Data- service be close to the Application Layer services and shall allow security policies to be possibly adapted to each Application Layer service.

The use of the S-AL shall not influence the functionality of Plain Application Layer.

- In reception direction, after accepting the S-A_Data-service, the S-AL shall check the security in function of the communication mode either according the Point-to-point Keys Table or according the Group Keys Table, restore the Plain APDU and if successful forward the contained plain AL-service request internally to the Plain Application Layer.

- In transmission direction, again in function of the communication mode that will be used either according the Point-to-point Keys Table or according the Group Keys Table for the S-A_Data-service, the S-AL shall secure the plain AL-service and shall transmit the secure APDU through the S-A_Data-service.

However, the Plain Application Layer shall transparently forward the security service parameters (par_auth, par_conf and link_index) between the S-AL and the AIL: see 5.1.2.

Figure 4 shows the location of the S-AL within the HBES communication stack. It shows the handling of secure messages. This is only a basic scheme. It does not show the handling of plain messages and the possible exceptions. The structure and priorities of the S-AL inside are not complete in this figure.

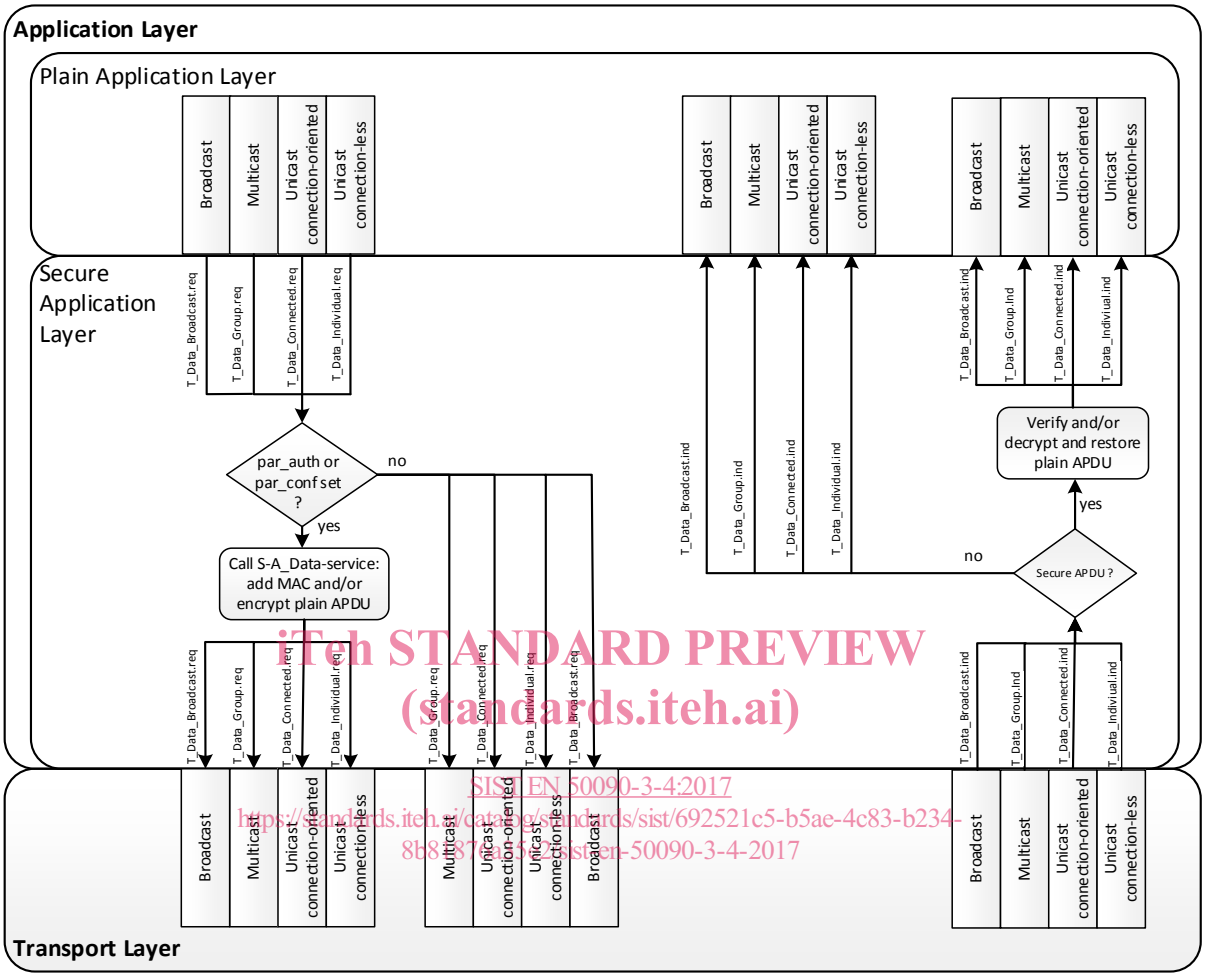

Figure 4 — Location of the S-AL within the Application Layer

5.1.1.1.2 S-AL – overview

The S-AL shall have the following functionality.

- Support the S-A_Data-service see 5.1.1.2;
- Handling of the Sequence Number: see 5.1.1.3;
- Handling of security failures see 5.1.1.4;
- Secure handling of the Transport Layer services see 5.1.1.5.

The following subclauses specify these and other functions.

5.1.1.1.3 AES-128 with CTR operation mode and AES-CBC-MAC signature (CCM)

5.1.1.1.3.1 Secure Data

The common format for the Secure Data with this algorithm shall be as specified in Figure 5. The Secure Data shall contain the following fields. (These are specified in detail below.)

— Sequence Number (SeqNr), and