# IEC 62351-6

Edition 1.0 2020-10

# INTERNATIONAL STANDARD

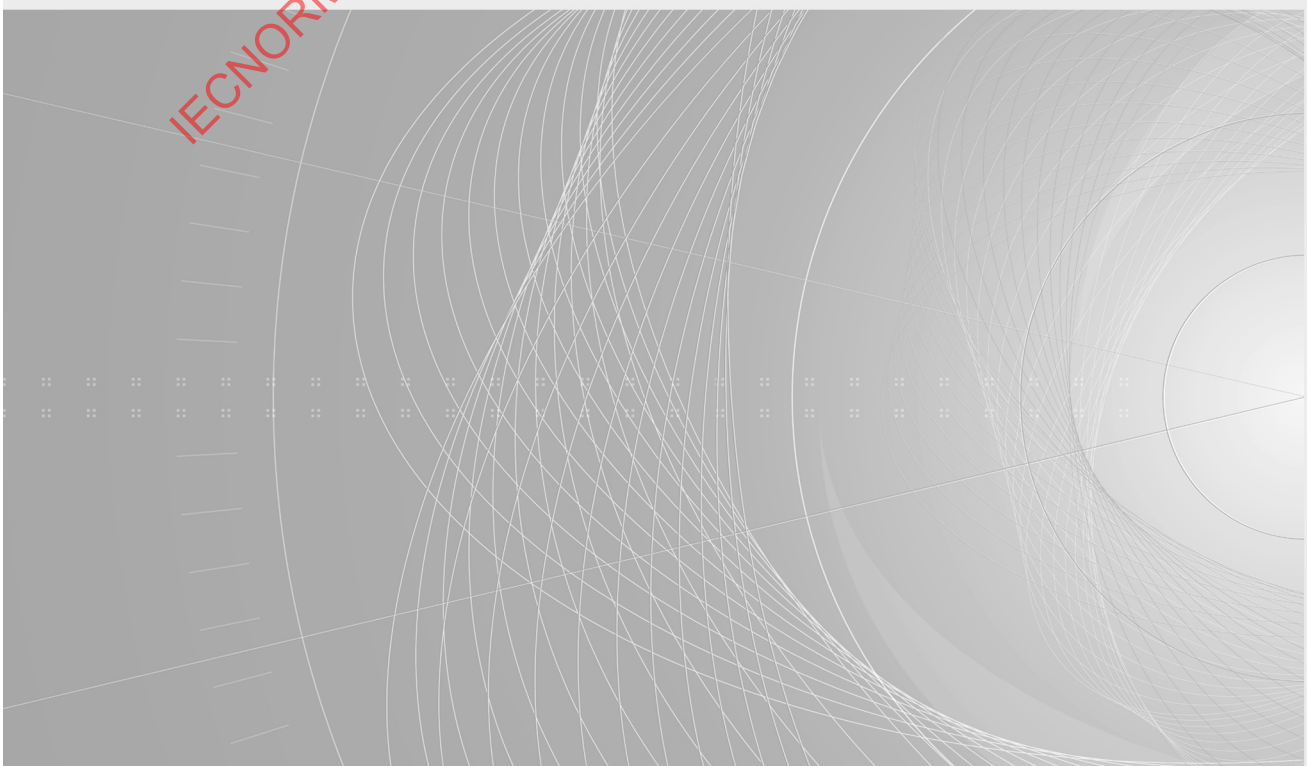
# NORME INTERNATIONALE

colour inside



## Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850

## Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850



IEC 62351-6:2020-10(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

# IEC 62351-6

Edition 1.0 2020-10

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside



## Power systems management and associated information exchange – Data and communication security – Part 6: Security for IEC 61850

## Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 6: Sécurité pour l'IEC 61850

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-9166-5

**Warning! Make sure that you obtained this publication from an authorized distributor.**
**Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATION SECURITY –

## Part 6: Security for IEC 61850

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.



International Standard IEC 62351-6 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this International Standard is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 57/2234/FDIS | 57/2258/RVD |

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

# POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATION SECURITY –

# Part 6: Security for IEC 61850

## 1 Scope and object

### 1.1 Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the IEC 61850 series. This document applies to at least those protocols listed in Table 1.

**Table 1 – Scope of application to standards**

| Number | Name |
|---|---|
| IEC 61850-8-1 | Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3 |
| IEC 61850-8-2 | Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP) |
| IEC 61850-9-2 | Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3 |
| IEC 61850-6 | Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in power utility automation systems related to IEDs |



The initial audience for this document is intended to be the members of the working groups developing or making use of the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this document is intended to be the developers of products that implement these protocols.

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

### 1.2 Namespace name and version

This new clause is mandatory for any IEC 61850 namespace (as defined by part 7-1 of IEC 61850 Edition 2).

The parameters which identify this new release of this namespace are:

- Namespace version: 2020
- Namespace revision: A
- Namespace name: “IEC 62351-6:2020A”
- Namespace release: 1

The table below provides an overview of all published versions of this namespace.

| Edition | Publication date | Webstore | Namespace |
|---|---|---|---|
| Edition 1.0 | 2020-? | IEC 62351-6:2020 | IEC 62351-6:2020 |

### 1.3 Code Component distribution

There is currently no code component scheduled for the code component downloading area.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-6, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-8-1, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-8-2, *Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)*

IEC 61850-9-2, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

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

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

IEC 62351-4:2020, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*

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

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*[1]

RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services*

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation Galois/Counter Mode (GCM and GMAC)*

## 3 Terms, definitions and abbreviated terms

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and IEC 61850-2 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

**3.1.1**
**electronic security perimeter**
logical border surrounding a network interconnecting critical cyber assets

**3.1.2**

**client**
functional unit that establishes an association and issues requests and receives services from a server.

**3.1.3**

**server**
functional unit that receives an association from a Client and provides services requested by the Client

### 3.2 Abbreviated terms

| | |
|---|---|
| ACSE | Association Control Service Element |
| APDU | Application Protocol Data Unit |
| ASDU | Application Service Data Unit |
| ASN.1 | Abstract Syntax Notation One |
| ESP | Electronic Security Perimeter |
| GDOI | Group Domain of Interpretation |
| GMAC | Galois Message Authentication Code |
| GOOSE | Generic Object Oriented Substation Event |
| GSE | Generic Substation Events |
| HMAC | Hashed Message Authentication Code |
| ICT | IED Configuration Tool |
| IED | Intelligent Electronic Device |
| KFA | Key Delivery Assurance |

[1] Restricted to SNTP profile only.

KDC Key Distribution Centre
MAC Message Authentication Code
SMV Sampled Measured Values
SCL Substation Configuration Language
SV Sampled Value

# 4 Security issues addressed by this document

## 4.1 Operational issues affecting choice of security options

For applications using Layer 2 IEC 61850-8-1 GOOSE and Layer 2 IEC 61850-9-2 Sampled Value and requiring 3 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that Layer 2 GOOSE and SV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this document does define a mechanism for allowing confidentiality for applications where the 3 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this document.

With the exception of confidentiality, this document sets forth a mechanism that allows co-existence of secure and non-secure PDUs.

## 4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this clause include:

- unauthorized modification (tampering) of information through message level authentication of the messages.

If encryption is employed, then the specific threats countered in this clause include:

- unauthorized access to information through message level authentication and encryption of the messages;
- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.
- information disclosure is countered.

## 4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specifications/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;
- tamper detection/message integrity: These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;
- replay: this threat will be countered through the use of specialized processing state machines specified within IEC 62351-4 and this document.

# 5 Correlation of IEC 61850 parts and IEC 62351 parts

## 5.1 General

There are four levels of interaction between the parts of the IEC 62351 series and parts of the IEC 61850 series. This part is concerned with the:

- Communication profile security regarding:
  - IEC 61850-8-1 Application Profile for Client/Server communications.
  - IEC 61850-8-2 Application Profile for Client/Server communications.
  - IEC 61850-8-1 Layer 2 T-Profile for GOOSE/GSE
  - IEC 61850-8-1 Layer 2 T-Profile for Multicast Sampled Values
  - IEC 61850-8-1 Layer 3 Routable GOOSE and Sampled Values
- Configuration extensions required for configuration of the Application and Transport communication profiles of concern. These extensions would impact IEC 61850-6.
- Object definitions, regarding security and identification, that are exposed at run-time as part of the IEC 61850-8-1 and IEC 61850-8-2 object mappings.
- The binding of Originator ID values to authenticated peers for Client/Server services.

The scope of this document provides security specifications for use within an Electronic Security Perimeter (ESP) and between ESPs.

## 5.2 IEC 61850-8-1 Profile for Client/Server communications

### 5.2.1 General

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall implement Clauses 5 and 6 of IEC 62351-4:2020.

IEC 61850-8-1 specifies the use of MMS within a substation. However, the scope of this specification provides security specifications for use within the substation and external to the substation (e.g. Control Centre to Substation).

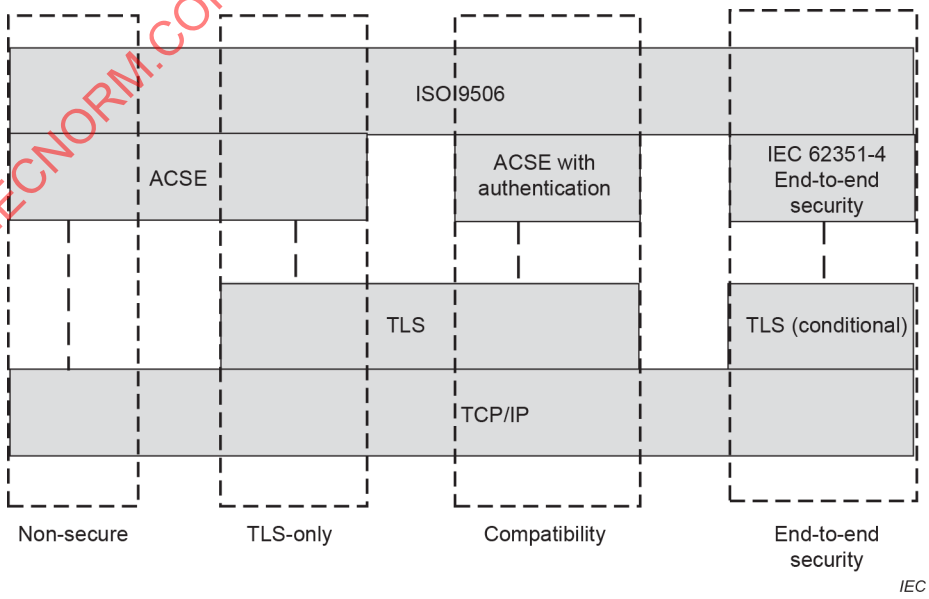



**Figure 1 – MMS Security Profiles**

Figure 1 shows the security profiles for IEC 61850 Client/Server associations based upon ISO/IEC 9506:

- Non-Secure: Implementations claiming conformance to this clause and Client/Server capability shall support the ability to be configured without securing connections per IEC 62351-4.
- TLS-Only: The use of TLS only is out-of-scope of this document. This profile may not provide the ability to provide user level Role Based Access Control (RBAC) for all use cases.
- Compatibility (per IEC 62351-4): Client implementations claiming conformance shall support the configuration and exchange of information utilizing ACSE Authentication per IEC 62351-4 and TLS. The use of TLS is mandatory.
- End-to-End: The support for this security profile is optional. However, in future editions of this standard, it is intended to make the support of this profile mandatory.

See Table 6 for a formal conformance statement.

#### 5.2.2 Control centre to substation

IEC 62351-4 shall be used without any other additions.

#### 5.2.3 Substation communications

The mandatory cipher suites are found in IEC 62351-4.

### 5.3 IEC 61850 security for profiles using VLAN IDs

For the IEC 61850 profiles specified that make use of VLAN IDs (e.g. IEC 61850-8-1 GOOSE, and IEC 61850-9-2) profile security shall be provided as specified in Clause 8.

### 5.4 IEC 61850-8-2 for Client/Server communications

IEC 61850 implementations claiming conformance to this document and declaring support for the IEC 61850-8-2 A-Profile for Client/Server communications shall implement the End-to-End security mechanism as specified by IEC 62351-4.

IEC 61850-8-2 does not support ACSE therefore, the IEC 62351-4 security mechanism of ACSE authentication (A-Profile) are not implemented or supported.

Additionally, IEC 61850-8-2 utilizes a T-Profile consisting of XMPP, which in turn controls TLS. Therefore, the TLS security mechanisms, and cipher suites, specified in IEC 62351-4 are out-of-scope for IEC 61850-8-2.

### 5.5 Using OriginatorID for Client/Server Services

There are several Common Data Classes (CDCs) defined in IEC 61850-7-3 and service tracking functions that explicitly define the ability to provide information about the originator of the control or service. The actual value representing the initiating entity in both IEC 61850-8-1 and IEC 61850-8-2 is originatorID and is a 64-octet octetstring.

The use of certificate-based authentication and security provides a mechanism for providing authoritative information regarding the originator. However, the size restriction of originatorID is not large enough to provide exposure of the Issuer and Serial Number. Therefore, implementations claiming conformance to this standard shall implement the optional DataAttribute certIssuer in the instance to the IEC 61850-7-3 CDCs of: CST, BTS, UTS, LTS, GTS, MTS, NTS, and STS.

The use of the value of the certIssuer Data Attribute follows:

- The value shall be a concatenation of the sequence of name values that may be present in the Issuer field. If there is more than one name in the sequence, the concatenation token shall be the "\" character, i.e. have a zero(0) length value if the client association is not authenticated.
- Have the value of the X.509 Issuer Name for a client association that is authenticated.
- If the concatenated value is greater than 255 characters, the value shall be truncated to 255 characters.
- If the client association was not authenticated through the use of certificates, the length of the certIssuer shall be zero(0) and therefore the value shall be NULL. All octets in the value shall be initialized to 0.

Implementations claiming conformance to this standard shall also utilize the originatorID Data Attribute as follows:

- If the certIssuer value is not NULL, the value of the X.509 certificate serial number shall be used for the value for clients associations that have been authenticated by use of a certificate. A certificate serial number is an encoded positive integer value. The encoded value shall be copied into the originatorID value, not including the tag or length.
- If the certIssuer value is NULL, the value of the originatorID may be "unknown" with "u" being the most significant octet of the value. Other values are a local issue.

# 6 Multicast Association Protocols

## 6.1 General

IEC 61850-8-1 and IEC 61850-9-2 specify two different application protocols that utilize the IEC 61850 Multicast Association model. These are GSE (e.g. GOOSE) and Multicast Sampled Values. These application protocols are mapped over two different T-Profile mappings.

The T-Profiles specified provide a Layer 2 and a Routable mapping of the application protocol. The combination of the A-Profiles and T-Profiles are commonly referred to as as Layer 2 or Routable (e.g. Layer 2 GOOSE or Routable GOOSE). This document specifies security behaviours that are common regardless of the T-Profile and specific security protocol extensions for the Layer 2 T-Profiles.

This clause specifies the expected behaviours for replay protection for both GOOSE and Multicast Sampled Values regardless of the T-Profile utilized.

## 6.2 Replay Protection

Replay protection can be implemented for GOOSE and Sampled Value A-Profiles with or without security extensions. The replay protection algorithms specified in the following clauses are for subscribers claiming conformance to this part and therefore replay protection is to be implemented regardless if the published GOOSE or Sampled Value APDU has security. The replay protection algorithm is implemented by the subscriber

### 6.2.1 GOOSE replay protection

#### 6.2.1.1 General

The normal GOOSE subscriber state machine in IEC 61850-8-1 does not detail how to transition out-of-order state numbers (stNum) or sequence numbers (sqNum) should be received.

Implementations claiming conformance to this standard shall implement the state machine shown in Figure 2. Additional security and replay checks may be implemented. For this clause, the Application is defined as the GOOSE Subscriber function and not the actual process that utilizes GOOSEData (per IEC 61850-7-2) in order to perform protection, etc.

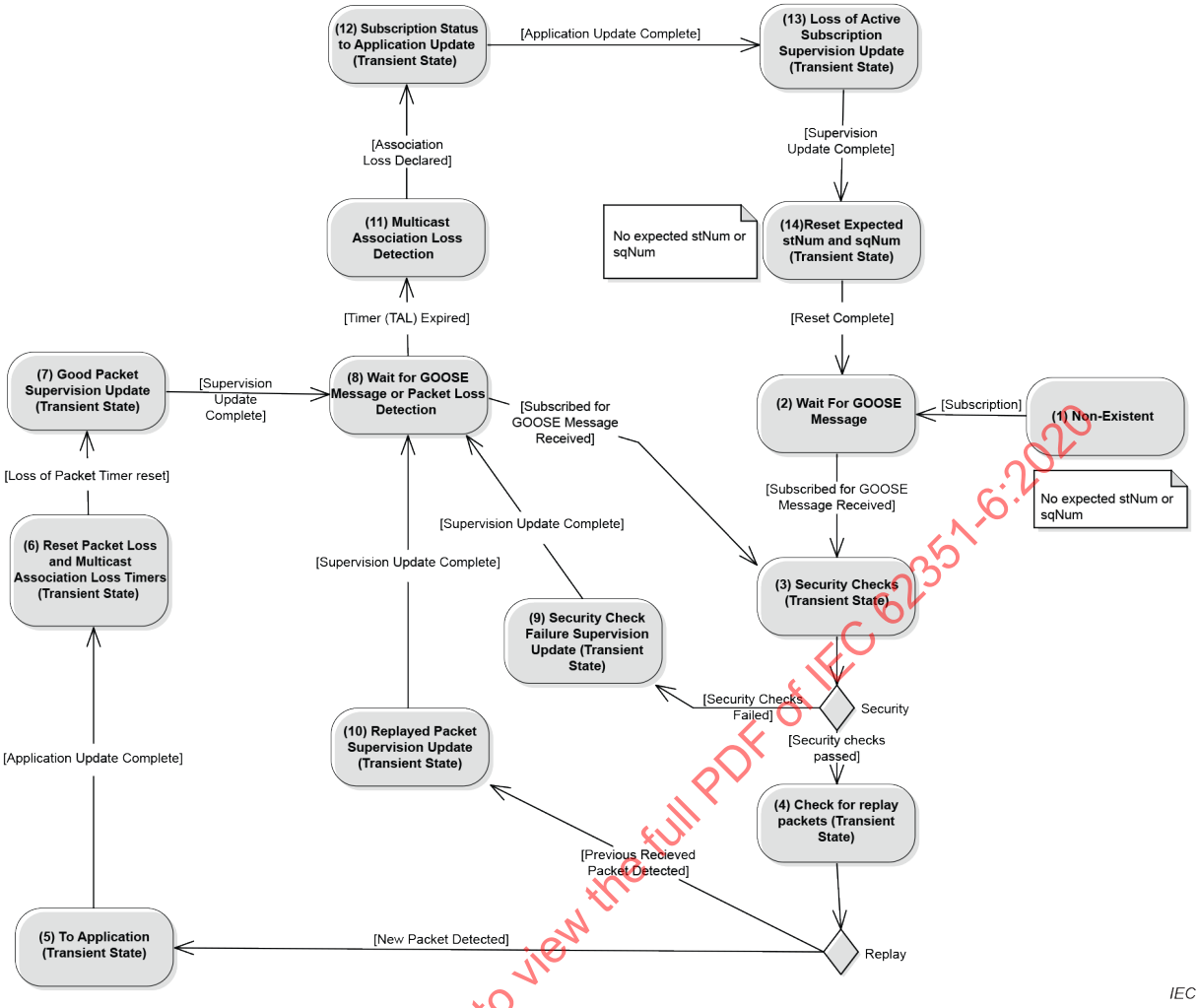



**Figure 2 – Replay Protection State Machine for GOOSE**

Figure 2 is relevant for GOOSE messages for which the subscriber has an active subscription shall be configured through the use of SCL and an ICT. Other configuration mechanisms are out-of-scope. Implementations claiming conformance to this clause shall maintain at least the following internal state machine variables: last received stNum (lastRcvStNum); last received sqNum (lastRcvSqNum); last received state change timestamp (lastRcvT); and an internal Time Allowed to Live (intTAL) value. The states and their transitions are defined as follows:

1) The Non-Existent state represents the state when there is no GOOSE subscription.
2) Upon activating the subscription (e.g. power-up or subscription configuration), the state machine will internally set the lastRcvStNum , lastRcvSqNum, lastRcvT, and intTAL to invalid since no GOOSE message has been received and the state machine transitions to the Wait for GOOSE Message state.

   Upon receiving the subscribed GOOSE message, the subscriber shall transition to the Security Checks state (State 3).
3) The processing in the Security Checks state is described in 6.2.1.2.

   If the Subscriber has never received a key from the KDC, it shall pass the security check for non-encrypted packets and perform a GROUP-PULL as defined by IEC 62351-9. Subscribers receiving an encrypted GOOSE messages, and not having the key for the ID conveyed in the GOOSE message shall transition to Security Check Failure and shall perform a GROUP-PULL as defined by IEC 62351-9.

   If the subscriber has been unable to receive keys prior to the expiration of the last key delivered, it shall report an alarm indicating that key delivery has failed and that expired keys are being assumed. It shall process packets whose keyID is the last key delivered.

Upon delivery of an unknown keyID, while using an expired key, the subscriber shall immediately perform a GROUP-PULL in order to synchronize keys.

If the security tests pass, the state machine shall transition to checking for replayed packets (State 4).

If the security checks fail, the state machine shall transition to the Security Check Failure Supervision Update state (State 9).

4) The Check for Replay state shall perform the procession in 6.2.1.3.

   If no replay is detected, a transition to the Application Update State (State 5) shall occur.

   If replay is detected, a transition to the Replayed Packet Supervision Update state (State 10) shall occur.

5) The “To Application” state shall decode the GOOSE packet. The decoded information shall be delivered to the Application if decoded stNum is not equal to lastRcvStNum. It is a local issue if a change of sqNum shall cause information to be delivered to the Application.

   The values of lastRcvStNum and lastRcvSqNum shall be updated to the values decoded from the GOOSE packet.

   The state shall transition to State 6.

6) The intTAL value shall be set to a value related to the decoded Time Allowed to Live (TAL) value. The Association Loss timeout shall also be reset to a locally determined value.

7) The supervision information shall be updated based upon the new packet information received. See 6.2.1.4 for processing requirements.

   Once the supervision information has been updated, a transition to State 8.

8) The value of intTAL shall be used to detect packet loss. The state shall start an expiration time based upon the current value of intTAL.

   If the value of intTAL is zero (e.g. expired), a transition to State 11 shall occur.

   If subscribed for GOOSE packet is received, the state shall transition to State 3.

9) The supervision information shall be updated based upon the security check failure information received. See 6.2.1.4 for processing requirements.

   Once the supervision information has been updated, a transition to State 8. No reset or setting of intTAL shall be performed.

10) The supervision information shall be updated based upon the replay detection information. See 6.2.1.4 for processing requirements.

    Once the supervision information has been updated, a transition to State 8. No reset or setting of intTAL shall be performed.

11) This state is used to determine when a subscription is no longer active. It differs from the packet loss detection in that it is a local issue.

    Once it is decided that the subscription is no longer active, the state transitions to State 12.

12) The application shall be updated such that it is aware that the subscription is no longer valid. The means through which this is performed is a local issue.

    After the application is updated, the state shall transition to State 13.

13) The supervision information shall be updated based upon the loss of an active subscription (e.g. LGOS.St shall change state). See 6.2.1.4 for processing requirements. Once the supervision information has been updated, a transition to State 14.

14) The values lastRcvStNum, and lastRcvSqNum shall be set to invalid and a transition to State 2 shall occur.

#### 6.2.1.2 Security Check Protection Requirements

This subclause specifies the processing required for checking GOOSE security parameters.

- The subscriber shall check if the AuthenticationValue (see 8.2.2.1) is expected as configured per IEC 61850-6 and the subscriber implements security.

  - If the AuthenticationValue is expected per configuration of the GSEControl.securityEnable and there is no AuthenticationValue provided, this shall result in a security check failure and no further security check processing will be required.
  - If there is no expected AuthenticationValue and a AuthenticationValue is provided, it shall be processed as if there were no AuthenticationValue and the value shall AuthenticationValue shall not be verified but shall not constitute a failure of the security checks.
  - If there is no expected AuthenticationValue and no AuthenticationValue is present this shall not constitute a security check failure.
  - If there is an AuthenticationValue and the subscriber does not support authentication this shall not constitute a security check failure.
- If encryption is being utilized, the packet shall be decrypted.

If none of the security checks fail, the state machine shall transition to the next state.

#### 6.2.1.3 Check for Replay State Processing Requirements

This clause specifies the processing required for checking for GOOSE packet replay.

- If the LPHD.Sim has transitioned to True, and the first simulated GOOSE has been processed, there shall be no replay detected. This indicates a transition from processing packets from a real publisher to process packets from a test set.
- If the LPHD.Sim has transitioned to False, and the first non-simulated GOOSE is being processed, there shall be no replay detected. This indicates a transition from processing simulated packets from a test set to processing packets from a real publisher.
- The subscriber shall check the timestamp (t) received in the GOOSE message versus lastRcvT. The processing is:
  - If the subscriber has an invalid value for lastRcvT, the subscriber shall update the value of lastRcvT to the value of “T received in the GOOSE message.
  - Otherwise, if the previous values of lastRcvT and lastRcvStNum were valid:
    i) If the lastRcvStNum value is less than the received stNum, the subscriber shall check that the value of “T received is no more than the local delivery deviation value older or newer than the subscriber’s local time. If the value of “T is outside of this range, this constitutes a failure and no further processing of the replay protection is needed as it has already failed.

       The use of delivery variance is a local issue.
- The subscriber shall check the stNum and sqNum received in the GOOSE message. The processing is:
  - If the subscriber has invalid states for lastRcvStNum and lastRcvSqNum the subscriber state machine shall set the values to:
    i) lastRcvStNum shall be set to the value of stNum received in the GOOSE packet.
    ii) lastRcvSqNum shall be set to the value of sqNum received in the GOOSE packet.

       No further replay checks are needed.
  - If there are valid values for lastRcvStNum and lastRcvSqNum, the subscriber shall:
    i) Determine if rollover of the sqNum was imminent. If the received stNum value is zero (0) then the values of lastRcvStNum and lastRcvSqNum shall be updated with the received stNum and sqNum values respectively.

       No further replay checks are needed.
    ii) If the received stNum is less than lastRcvStNum or sqNum is less than lastRcvSqNum this could be caused by one of two factors:

A packet replay or a multi-path delayed packet. In either case, the received GOOSE shall not be provided to the application and the state machine shall behave as if the packet was a replay. However, it will be a local issue if the Supervision state classifies this occurrence as a replay.

#### 6.2.1.4 Supervision Update State Processing Requirements

The Supervision Update State is a transient state and is used to represent the local updating of LGOS, local logs, standardized security logs, proprietary network management MIBs, and security event creation, as well as IEC 62351-7 standardized MIBs.

### 6.2.2 Sampled Value replay protection

#### 6.2.2.1 General

IEC 61850-9-2 does not detail how to transition out-of-order message delivery should be handled. In some cases, out-of-order delivery would not constitute replay and could just be based upon multi-path delivery delays. Unlike GOOSE, Sampled Values does not have a state number/sequence number construct available for use in replay protection. Therefore, implementations claiming conformance to this standard shall implement the following.

#### 6.2.2.2 Publisher

To prevent SV replay, the Security field of the SV protocol shall be present (see Table 2).

**Table 2 – Extract from IEC 61850-9-2 (Informative)**

| |
|---|
| ASN.1 Basic Encoding Rules (BER)<br>SavPdu::=<br>**SEQUENCE {** |
| noASDU [0] IMPLICIT INTEGER (1..65535), |
| security [1] ANY OPTIONAL, |
| asdu [2] IMPLICIT SEQUENCE OF ASDU<br>**}** |



Prevention of replay requires that publisher include the optional security field in the SavPdu and implements a form of integrity protection as specified for the different T-Profiles (e.g. Layer 2 or Routable).

The SavPdu Security field shall not be present if Sampled Value security is not being provided on a given message. If security is being utilized for the message, the field shall be present and its contents shall be:

```
IMPORT
security::=  [0] IMPLICIT SEQUENCE {
                    timestamp [0] IMPLICIT OCTETSTRING, --time of send
                    ...
                   }
```

**timestamp**

The timestamp attribute shall represent the approximate time at which the SV frame was formatted.

The octet format shall be per IEC 61850-8-1 for Timestamp.

The time accuracy of the value shall be at least 208 µsec.

#### 6.2.2.3 Subscriber

Based upon the SV security field being present, or using Routable SMV, the following state machine client rules shall apply:

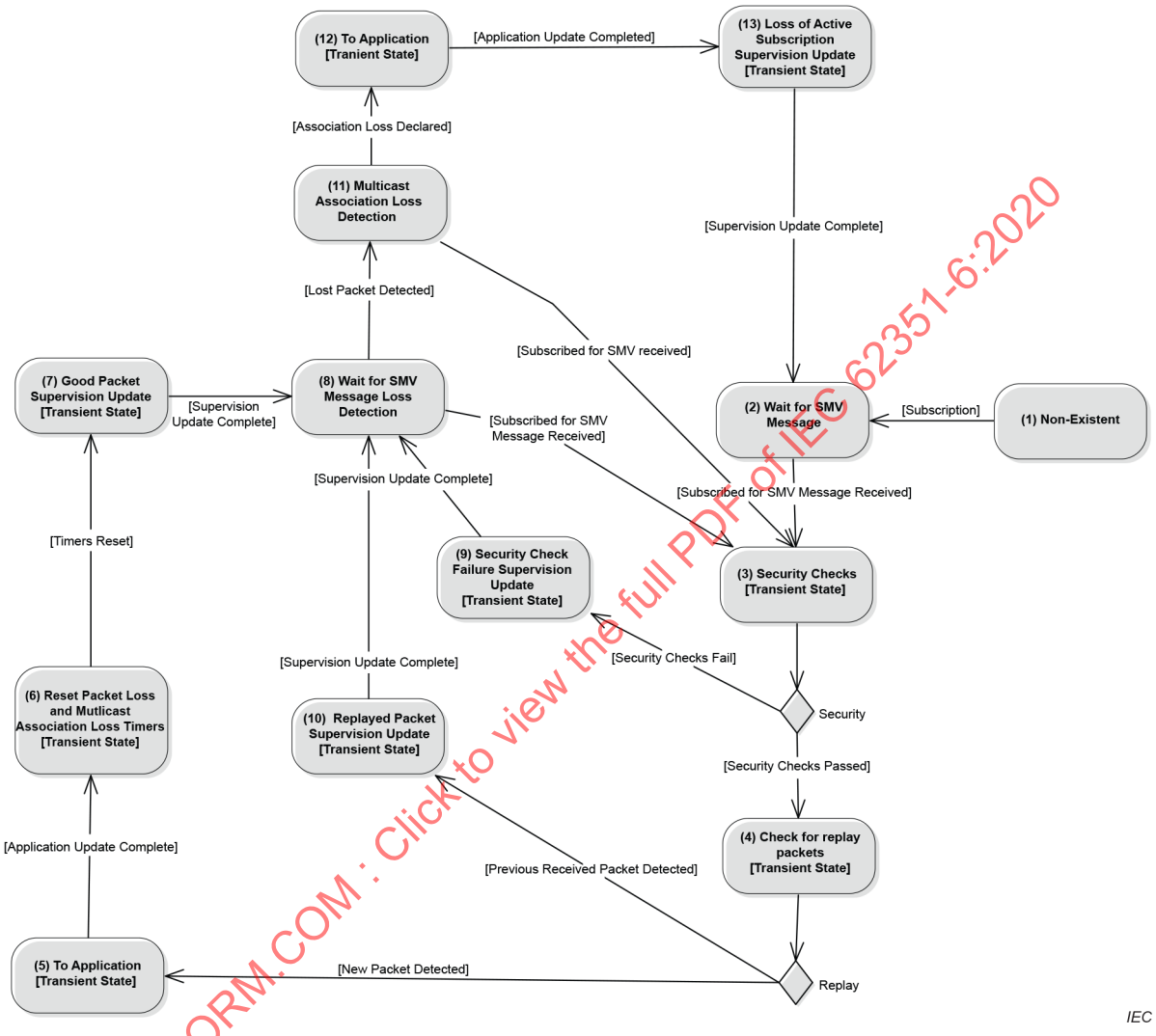



**Figure 3 – Replay Protection State Machine for SV**



Figure 3 is relevant for SV messages for which the subscriber has an active subscription which shall be configured through the use of SCL and an ICT. Other configuration mechanisms are out-of-scope. Implementations claiming conformance to this clause shall maintain at least the following internal state machine variables: last received security timestamp value (lastRcvT) and the time delay until the next packet is expected (expNxtPkt). The states and their transitions are defined as follows:

1) The Non-Existent state represents the state when there is no SV subscription.
2) Upon activating the subscription (e.g. power-up or subscription configuration), the state machine will internally set the lastRcvT and expNxtPk and the state machine transitions to the Wait for SV Message state.

   Upon receiving the subscribed SV message, the subscriber shall transition to the Security Checks state (State 3).
3) The processing in the Security Checks state is described in Clause 6.2.2.3.1.

If the security tests pass, the state machine shall transition to checking for replayed packets (State 4).

If the security checks fail, the state machine shall transition to the Security Check Failure Supervision Update state (State 9).

4) The Check for Replay state shall perform the procession in Clause 6.2.2.3.2.

If no replay is detected, a transition to the Application Update State (State 5) shall occur.

If replay is detected, a transition to the Replayed Packet Supervision Update state (State 10) shall occur.

5) The “To Application” state shall decode the SV packet. The decoded information shall be delivered to the Application.

The state shall transition to State 6.

6) The expNxtPkt value shall be set the value according to the following calculation:

Dynamic calculation of expNxtPk is allowed for systems that do not configure based upon SCL. The dynamically calculated value of expNxtPk is the same calculation but based upon the values received in the actual SV APDU.

The value of expNxtPk is defined to be:

For smpMod = SmpPerSec:

expNxtPk = (noASDU/smpRate) * 2

For smpMod = SecPerSmp:

expNxtPk = smpRate * noASDU * 2

For smpMod=SmpPerPeriod:

expNxtPk = ((noASDU/smpRate)/(nominal frequency)) * 2

Expiration of the timer cause a transition to a state that may add an addition delay to the actual declaration that a multicast subscription loss.

The Association Loss timeout shall also be reset to a locally determined value.

7) The supervision information shall be updated based upon the new packet information received. See 6.2.1.4 for processing requirements.

Once the supervision information has been updated, a transition to State 8 shall occur.

8) If subscribed for SV packet is received, the state shall transition to State 3.

The local multicast association loss detection timer shall be started when the state is entered from a state other than state 8. If the timer expires, there shall be a transition to State 11.

9) The supervision information shall be updated based upon the security check failure information received. See Clause 6.2.2.3.3 for processing requirements.

Once the supervision information has been updated, a transition to State 8 shall occur.

10) The supervision information shall be updated based upon the replay detection information. See Clause 6.2.2.3.3 for processing requirements.

Once the supervision information has been updated, a transition to State 8 shall occur.

11) This state is used to determine when a subscription is no longer active. It differs from the packet loss detection in that it is a local issue. Upon detection of lost subscription, the state shall transition to State 12.

If a subscribed for SVmessage is received, the state shall transition to State 3.

12) The application shall be updated such that it is aware that the subscription is no longer valid. The means through which this is performed is a local issue.

After the application is updated, the state shall transition to State 13.

13) The supervision information shall be updated based upon the loss of an active subscription (e.g. LSVS.St shall change state). See Clause 6.2.2.3.3 for processing requirements.

#### 6.2.2.3.1 Security Check Protection Requirements

This subclause specifies the processing required for checking SV security parameters.

- The subscriber shall check if the AuthenticationValue (see 8.2.2.1) is expected per the configuration of the control block per IEC 61850-6:2018 and the subscriber implements security.
  - If the AuthenticationValue is expected per configuration of the SampledValueControl.securityEnable and there is no AuthenticationValue provided, this shall result in a security check failure and no further security check processing will be required.
  - If there is no expected AuthenticationValue and a AuthenticationValue is provided, it shall be processed as if there were no AuthenticationValue and the value shall AuthenticationValue shall not be verified but shall not constitute a failure of the security checks.
  - If there is no expected AuthenticationValue and no AuthenticationValue is present this shall not constitute a security check failure.
  - If there is an AuthenticationValue and the subscriber does not support authentication this shall not constitute a security check failure.
- If encryption is being utilized, the packet shall be decrypted.

If none of the security checks fail, the state machine shall transition to the next state.

#### 6.2.2.3.2 Check for Replay State Processing Requirements

This clause specifies the processing required for checking for SV packet replay.

- The subscriber shall check the security timestamp (t) received in the SV message versus lastRcvT. The processing is:
  - If the subscriber has an invalid value for lastRcvT, the subscriber shall update the value of lastRcvT to the value of the security timestamp received in the SV message.
  - If the subscriber has a previously received value, it shall check that the new received value is greater than the previous value.

The subscriber shall monitor the smpCnt as increasing in value.

#### 6.2.2.3.3 Supervision Update State Processing Requirements

The Supervision Update State is a transient state and is used to represent the local updating of LSVS, local logs, standardized security logs, proprietary network management MIBs, and security event creation, as well as IEC 62351-7 standardized MIBs.

## 7 Security for SNTP

IEC 61850-8-1 and IEC 61850-8-2 specify the use of SNTP for the purposes of time synchronization.

Implementations claiming conformance to this document shall implement the RFC 5905 profile for SNTP including mandatory use of the authentication algorithms.

# 8 Layer 2 security for profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sampled Value

## 8.1 Overview of Ethertype (informative)

This document extends the normal Layer 2 IEC 61850 GOOSE and Layer 2 IEC 61850-9-2 Sampled Measured Value PDUs. The normative definition of the Layer 2 IEC 61850 GOOSE and Sampled Measured Value is in Annex C of IEC 61850-8-1:2011.

## 8.2 Extended PDU

### 8.2.1 General format of extended PDU

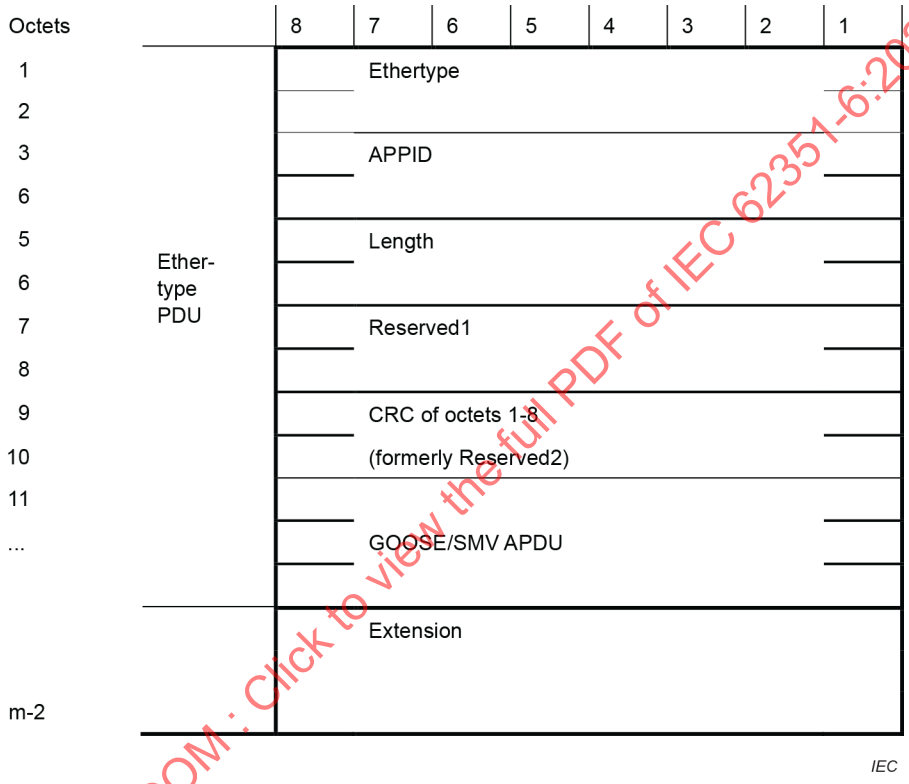



**Figure 4 – General format of extended PDU**



Figure 4 depicts the fact that the Reserved1 and Reserved2 fields are to be used for implementations claiming conformance to this specification in regard to GOOSE and SV security. This specification specifies that the:

– **Reserved1** field shall be used to include the number of octets conveyed by the extension octets. This value shall be contained in the first octet of the Reserved1 field. A value of zero(0) shall indicate that no extension octets are present. The structure of the Reserved 1 is defined in Figure 5.

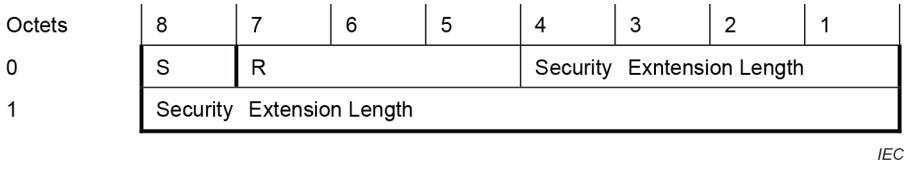



**Figure 5 – Definition of Reserved 1**

– **Reserved2** field shall contain a 16-bit CRC, as calculated per ISO/IEC 13239 (ISO HDLC). The CRC shall be calculated over Octets 1 to 8 of the VLAN information of the Extended PDU.

  The CRC shall be present if the Extension Length has a non-zero value.

### 8.2.2 Format of extension octets

#### 8.2.2.1 General

The format of the extension octet area shall be:

```
Extension::= {
        [0] IMPLICIT SEQUENCE {
                [1] IMPLICIT SEQUENCE Reserved OPTIONAL,
                [2] IMPLICIT OCTETSTRING Private OPTIONAL,
                [3] IMPLICIT OCTETSTRING Reserved OPTIONAL, --do not use
                [4] IMPLICIT AuthenticationValue OPTIONAL,
                [5] IMPLICIT OCTETSTRING mAC OPTIONAL,
                ...,
                }
        ...,
        }
```

Extension shall be encoded per ASN.1 Basic Encoding Rules.

The Reserved SEQUENCE is used to reserve future standardized extension per this specification. If no extension, besides Authentication and Encryption is defined in this specification, this SEQUENCE shall not be present.

Therefore, a SEQUENCE of NULL length shall be considered non-conformant to this specification.

The Private SEQUENCE is provided to allow vendors to convey Private information. The scope of the semantics and syntax of the contents of this SEQUENCE is out-of-scope of this specification and shall only be interoperable via prior agreement. This SEQUENCE shall only be present if there are actual contents being conveyed.

If there is the AuthenticationValue present, there shall be a mAC value.

#### 8.2.2.2 mAC

The calculated MAC value shall be used for the authentication/integrity of the octets that starts with the Ethertype Identifier for GOOSE or SV through the end of the GOOSE/SV APDU, security extensions excluding the tag, length and value of the mAC. The calculations shall not include the MAC production. The value of the parameter shall be calculated based upon the algorithm specified.

The value of the MAC shall be treated as ASN.1 OCTETString values.

The allowed MAC functions are: HMAC-SHA256, and AES-GMAC.

The mandatory MAC functions HMAC-SHA256 and AES-GMAC shall be supported.

The allowed MAC lengths can be found in Table 9 and Table 10, the calculated MAC value may be truncated, per RFC 2104.

Therefore, the MAC enumerated values, used in the Security Algorithm shall be as defined in RFC 8052.

The MAC-None option is provided for testing and shall not be used in operational systems. It indicates that no MAC value (e.g. MAC) is being calculated. Therefore, for MAC-None, the length octet of mAC contains a value of zero (0).

The output length shall be no less than eight (8) octets.

The periodicity between rekey is related to the strength of the MAC. In particular, the guidance for AES-GMAC needs to be evaluated. The relevant document is NIST Special Publication 800-38D (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf).

The action due to detection of an invalid MAC being received shall be documented as specified in Clause 10. It is recommended that the information not be processed and that some type of security related event be triggered. The event type is a local issue but could be per IEC 62351-7 and/or the incrementing of AuthFail attribute of a Generic Security Application GSAL Logical Node.

If encryption of the GOOSE or SV APDU is being utilized, the MAC shall be on the encrypted APDU.

The information covered by the MAC is shown as the calculated mAC domain in Figure 6.

The information in the Extension includes all of the Extension production except for the mAC. Figure 6 shows the coverage for implementations claiming conformance to IEC 62351-6 using AuthenticationValue and mAC only

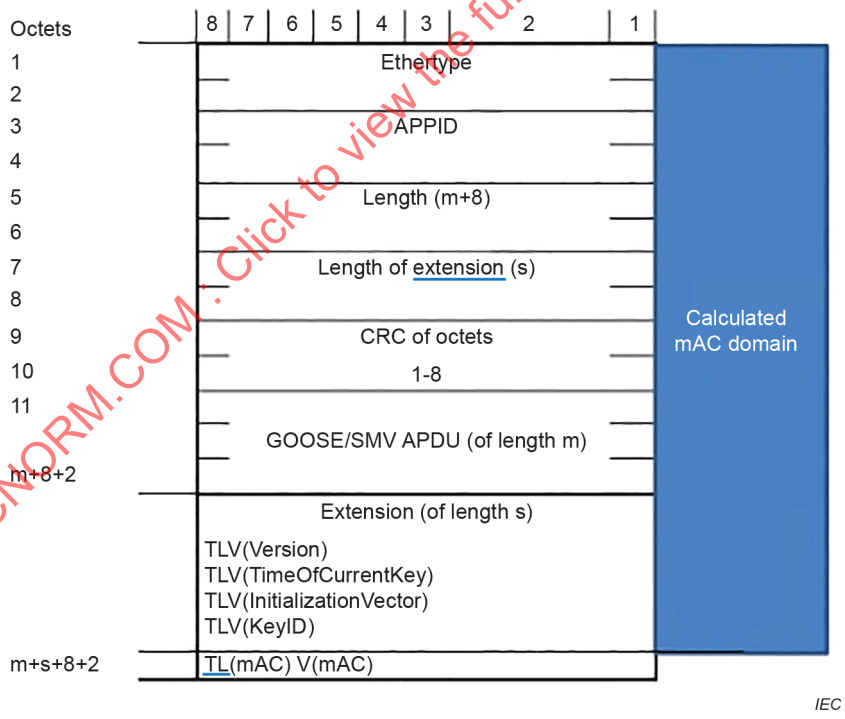



**Figure 6 – Calculated MAC Domain**

GOOSE APDU encryption is specified for R-GOOSE as it may travers public networks. Encryption of L2 GOOSE/SV packets is left out of scope. For R-GOOSE encryption AES-GCM shall be applied. AES-GCM realizes authenticated encryption. In addition, AES-GCM allows additional authenticated data as preceding information before the plaintext to be encrypted. This allows to perform the integrity protection and the encryption of the GOOSE APDU in a single run.

The following figure shows the AES-GCM processing based on the packet shown in Figure 7.

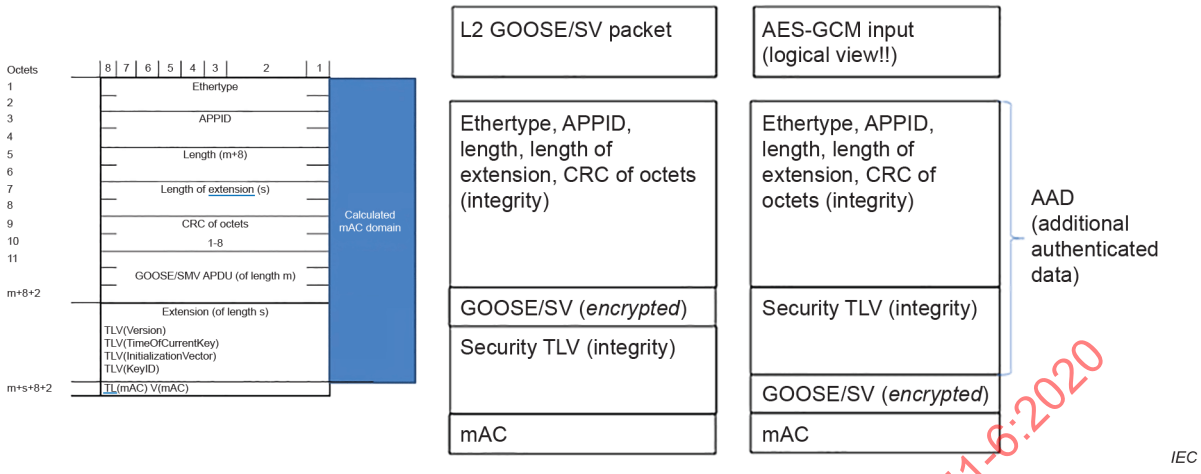



**Figure 7 – AES-GCM application on the example of a L2 GOOSE/SV packet.**

In Figure 7, the organization of the elements under the AES-GCM column represents a logical view only and does not represent the order in which these elements occur in the L2 GOOSE/SV packet.

Implementation note: Typical interfaces for AES-GCM functions offer the provisioning of data in chunks. This allows the data that is to be encrypted and integrity protected to be processed separately from the data that is only integrity protected. By leveraging this functionality, the overhead of restructuring the memory buffer holding the GOOSE/SV packet before invoking AES-GCM can be saved at the cost of separate function calls for integrity protection of {Ethertype, APPID, Length, Length of extension, CRC of octets}, encrypted GOOSE/SV APDU and the Extension.

### 8.2.2.3 AuthenticationValue

#### 8.2.2.3.1 General

```
AuthenticationValue ::= SEQUENCE {
  version [0] IMPLICIT INTEGER,
  timeOfCurrentKey [1] IMPLICIT INTEGER (0..4294967295),
  timrOfNextKey [2] IMPLICIT INTEGER,
  initializationVector [3] IMPLICIT OCTET STRING OPTIONAL,
  keyID [4] IMPLICIT INTEGER
  ...
  }
```



#### 8.2.2.3.2 Version

The Version component shall contain the extension protocol version number as specified by this document. The value shall be an unsigned integer value and shall be greater than zero(0).

The value assigned for the Version shall be: 1.

#### 8.2.2.3.3 TimeofCurrentKey

The TimeofCurrentKey component shall be an unsigned Integer value. The value of the attribute shall represent the SecondSinceEpoch. SecondSinceEpoch shall be the interval in seconds continuously counted from the epoch 1970-01-01 00:00:00 UTC.

The value is based upon information provided by the KDC as specified in IEC 62351-9.

NOTE SecondSinceEpoch corresponds with the Unix epoch.

Some operating systems have a 32-bits Signed value that represents SecondsSinceEpoch (e.g. Unix). For implementations in such operating systems, it shall be the implementation's responsibility to provide the appropriate time offsets to allow the full range of the Unsigned Integer value to be used.

In the case of an operating system with an internal 64 bits time representation, it should be shortened to unsigned 32 bits. The choice of representation of time as an unsigned 32 bit number makes the representation not affected by the Year 2038 problem.

#### 8.2.2.3.4 TimetoNextKey

The TimetoNextKey component shall be a signed integer value. The value of the attribute represents the number of seconds prior to a new key being used. A negative value is reserved to indicate that no new key has been scheduled to be placed into service. Any positive value shall be used to indicate the number of seconds prior to the new key being placed into service. A value of zero indicates that there is no expiration.

Prior to setting a positive value, the Group Manager (e.g. IED) shall determine the new key that will be applied. This will allow the subscribers to use the Group Key Management Protocol to obtain the new assigned key prior to expiration.

The positive number shall be the relative time until the new key is put into service. Therefore, the number is decremented until the new key is in actual use. When the new key is placed into use, the TimeofCurrentKey attribute value is updated.

The value is the value provided by the KDC as specified in IEC 62351-9.

#### 8.2.2.3.5 InitializationVector

The InitializationVector component is an optional field that shall be present if the MAC or encryption algorithm requires an initialization value. This value, if present, shall be changed on a per APDU basis and shall be used for both encryption and MAC generation. The initialization vector (InitializationVector) shall be 16 octets long, generated by a cryptographically secure pseudo random number generator being different for each AuthenticationValue. Best practices for cyber related initialization vector generation should be utilized.

#### 8.2.2.3.6 Key ID

The value of Key ID is a four (4) octet value that was assigned by the KDC as a reference to the key that is in use.

The Key ID selection shall be based upon the contents of the User Data:

- For User Data that contains payloads containing a single DataSet of information, the Key ID shall be the Key ID provided by the KDC for the particular DataSet.
- For MNGT payloads, the Key ID shall be the value assigned to the DataSet provided by the KDC.

### 8.2.2.4 Requirements on publishers

#### 8.2.2.4.1 General

Publishers claiming conformance to this part of the standard shall conform to GDOI key management as specified by IEC 62351-9 and RFC 8052.

#### 8.2.2.4.2 Requirements on subscribers

Upon layer 2 GOOSE or SV message, where security extensions are configured:

- the receiving client shall calculate the AuthenticationValue for the APDU as specified in 8.2;
- if the MAC verification succeeds, then the client should proceed with the processing of the APDU.

# 9 Substation configuration language extensions

## 9.1 Service capability

### 9.1.1 Access Point support security for GOOSE Publisher

The scl:tGSESettings has been extended with an attribute kdaParticipant. If true, the KDA is supported by the publisher access point as specified in IEC 62351-9.

The scl:tGSESettings has been extended with sublement scl:McSecurity containing two attributes signature and encryption.

The McSecurity element describes the supported security options available at each GOOSE control block.

If signature is true (default false), then the publisher supports the GOOSE security extensions as specified in 8.2.

If encryption is true (default false), then the publisher supports the GOOSE security extensions as well as the encryption of the GOOSE Pdu as specified in Clause 8.

When McSecurity is missing, the GOOSE Publisher does not support the security extensions specified in 8.2.

### 9.1.2 Access Point support security for SV Publisher

The scl:tSMVSettings has been extended with an attribute kdaParticipant. If true, the KDA is supported by the publisher access point as specified in IEC 62351-9.

The scl:tSMVSettings has been extended with sublement scl:McSecurity containing two attributes signature and encryption.

The McSecurity element describes the supported security options available at each SV control block.

If signature is true (default false), then the publisher supports the SV security extensions as specified in 8.2.

If encryption is true (default false), then the publisher supports the SV security extensions as well as the encryption of the SaVPdu as specified in 8.2.

When McSecurity is missing, the SV Publisher does not support the security extensions specified in 8.2.

### 9.1.3 Acces Point support security for GOOSE and SMV subscriber

The scl:tClientServices has been extended with subelement scl:McSecurity containing two attributes signature and encryption.

The McSecurity element describes the supported security feature at the multicast subscriber.

If signature is true (default false), then the subscriber supports the security extensions as specified in 8.2.

If encryption is true (default false), then the subscriber supports the security extensions as well as the encryption of the subscribed multicast Pdu as specified in 8.2.

When McSecurity is missing, the subscriber does not support the security extensions specified in 8.2.

#### 9.1.4 Server Access Point support security for TPAA

The Services element of SCL shall be extended to allow the implementations to provide information about their support for security.

The request for the extension has been captured in the https://iec61850.tissue-db.com/tissue/1674.

The XML element that shall be used for Server declarations, shall be:

```
xs:element name="Security" type="tSecurity" minOccurs="0" maxOccurs="1">

    <xs:complexType name="tSecurity">
        <xs:attribute name="ACSEAuthentication" type="xs:boolean" default="false"/>
        <xs:attribute name=E2ESecurity" type="xs:boolean" default="false"/>
    </xs:complexType>
```

If the Security element is not present, this shall indicate that Security is not supported.

#### 9.1.5 Client Access Point support security for TPAA

The ClientServices element of SCL shall be extended to allow the implementations to provide information about their support for security.

The request for the extension has been captured in the https://iec61850.tissue-db.com/tissue/1674.

The XML element that shall be used for Client declarations, shall be:

```
xs:element name="Security" type="tSecurity" minOccurs="0" maxOccurs="1">

    <xs:complexType name="tSecurity">
        <xs:attribute name="ACSEAuthentication" type="xs:boolean" default="false"/>
        <xs:attribute name=E2ESecurity" type="xs:boolean" default="false"/>
    </xs:complexType>
```

If the Security element is not present, this shall indicate that Security is not supported.

### 9.2 Publish with security enabled

#### 9.2.1 GOOSE

The attribute securityEnabled (default = ‘none’) of scl:tGSEControl activates the security extension of the GOOSE Pdu as specified by 8.2. If missing, the GOOSE Pdu is sent without security extension.

#### 9.2.2 SV

The attribute securityEnabled (default = ‘none’) of scl:tSampledValueControl activates the security extension of the SaVPdu as specified by 8.2. If missing, the SaVPdu is sent without security extension.

### 9.2.3 Key Policy and Management

The key information, and the algorithm selection for hash and encryption, shall be provided per the GDOI specification found in IEC 62351-9 and RFC 8052.

### 9.3 Use of Simulation

Simulated APDUs, as defined by the Simulation Bit=true, shall use the same cyber policies and information as the source packets from the non-test device.

Encryption, if performed, shall encrypt the GOOSE/SV APDU in its entirety.

## 10 Extension of LGOS and LSVS

The IEC 61850-7-4 specified LGOS LN class shall be extended as specified in Table 3 to indicate that a security violation has been detected for a configured subscription.

**Table 3 – Extension of the LGOS class**

| LGOS class extension for Security Violation status information | | | | |
|---|---|---|---|---|
| **Data object name** | **Common data class** | **T** | **Explanation** | **M-O-C nds/ds** |
| **Status information** | | | | |
| SecViol | SPS | T | A security violation has been detected for this supervised GOOSE subscription | M / F |

The IEC 61850-7-4 specified LSVS LN class shall be extended as specified in Table 4 to indicate that a security violation has been detected for a configured subscription.

**Table 4 – Extension of the LSVS class**

| LSVS class extension for Security Violation status information | | | | |
|---|---|---|---|---|
| **Data object name** | **Common data class** | **T** | **Explanation** | **M-O-C nds/ds** |
| **Status information** | | | | |
| SecViol | SPS | T | A security violation has been detected for this supervised SMV subscription | M / F |



## 11 Conformance

### 11.1 General conformance

Implementations claiming conformance to this specification shall provide an extended Protocol Implementation Conformance Statement (PICS) as set forth in the following clauses. For some profiles, additional Protocol Implementation eXtra InformaTion (PIXIT) information may need to be provided.

For the following clauses and tables, the following definitions apply:

– m: mandatory support – the item shall be implemented;
– c: conditional support – the item shall be implemented if the stated condition exists;
– o: optional support – the implementation may decide to implement the item;
– x: excluded – the implementation shall not implement this item;

– i: out-of-scope – the implementation of the item is not within the scope of this specification.

– AtLeastOne(x) – indicates that at least one of the declarations must be supported for the grouping of (x).

The information in Table 5 shall be provided for an implementation claiming support for this specification.

**Table 5 – Conformance table**

| | Profile Description | Client | | Server | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| G1 | Support for IEC 61850-8-1/ISO 9506 security Client/Server | o | AtLeastOne(1) | o | AtLeastOne(1) | |
| G2 | Support for IEC 61850-8-1 L2 GOOSE security | o | AtLeastOne(1) | o | AtLeastOne(1) | |
| G3 | Support for IEC 61850-9-2 L2 SMV security | o | AtLeastOne(1) | o | AtLeastOne(1) | |
| G4 | Support for IEC 61850-8-1 Routable GOOSE security | o | AtLeastOne(1) | o | AtLeastOne(1) | |
| G5 | Support for IEC 61850-9-2 Routable SMV security | o | AtLeastOne(1) | o | AtLeastOne(1) | |
| G6 | Supported for IEC 61850-8-2 | o | | o | | |
| G7 | Support for SNTP security | o | | o | | |
| | | | | | | |

## 11.2 Conformance for implementations claiming IEC 61850-8-1 ISO 9506 profile security

### 11.2.1 General

The information in Table 6 shall be provided for implementations claiming support of the security profile for ISO 9506 / IEC 61850 profile.

**Table 6 – PICS for IEC 61850-8-1 ISO 9506 profile**

| | Capability | Client | | Server | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| S1a | IEC 62351-4 ACSE Authentication | m | | o | | |
| S1b | IEC 62351-4 TLS Support with ACSE Authentication | m | | c1 | | |
| S1c | TLS authentication evaluation on application layer | o | | o | | |
| S1d | IEC 62351-4 Mandatory TLS Cipher Suites | m | | c2 | | |
| c1 – shall be 'm' if IEC 62351-4 TLS Support with ACSE Authentication support is declared.<br>c2 – shall be 'm' if IEC 62351-4 TLS Support for ACSE Authentication or TLS for Authentication is declared. | | | | | | |

E2E

| | | | | | | |
|---|---|---|---|---|---|---|
| S1e | IEC 62351-4 E2E Support | o | | o | | |
| S1f | IEC 62351-4 TLS Support with E2E | c1 | | c1 | | |
| S1g | IEC 62351-4 Mandatory TLS Cipher Suites | c1 | | c1 | | |
| c1 – shall be 'm' if E2E support is declared | | | | | | |

General

| | | | | | | |
|---|---|---|---|---|---|---|
| S1h | Non-Secure Support | m | | m | | |
| S1i | VPN Support | i | | i | | |
| S1j | Tracking Services Supported | m | | o | | |
| S1k | Control Services Supported | o | | c1 | | |
| c1 – shall be "m" if server declares support for control services. | | | | | | |

### 11.2.2 IEC 62351-4 TLS Conformity for ISO-9506 Client/Server Profile using ACSE Authentication

For implementations claiming conformance to IEC 61850-8-1 Client Server using IEC 62351-4 and ACSE Authentication shall implement the mandatory statements in IEC 62351-3:2014, Table 2 and the requirements in Table 7.

**Table 7 – PICS for TLS IEC 61850-8-1 Client/Server using ACSE Authentication**

| | | Client | | Server | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| TLS811 | TLS conformity – IEC 62351-4:2020, 6.3.4.2 | o | | o | | The specified cipher suites have security vulnerabilities |
| TLS812 | TLS conformity – IEC 62351-4:2020, 6.3.4.3 | m | | m | | |
| | | | | | | |

### 11.3 Conformance for implementations claiming VLAN profile security

The information in Table 8 to Table 12 shall be provided for implementations claiming support of the security profile for VLAN IEC 61850 profile.

**Table 8 – PICS for VLAN profiles**

| | Capability | Client | | Server | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| S2a | SCL extensions | m | | m | | |
| S2b | IEC 61850-8-1 L2 GOOSE security | C1 | | C1 | | |
| S2c | IEC 61850-8-1 Routable GOOSE security | C1 | | C1 | | |
| S2d | IEC 61850-9-2 L2 SMV security | C2 | | C2 | | |
| S2e | IEC 61850-9-2 Routable SMV security | C3 | | C3 | | |
| C1 – shall be “m” for implementations claiming GOOSE security conformance.<br>C2 – shall be “m” for implementation claiming Layer 2 SMV security conformance.<br>C3 – shall be “m” for implementation claiming Routable SMV security conformance. | | | | | | |

**Table 9 – IEC 61850-8-1 L2 GOOSE Security**

| | Capability | Subscriber | | Publisher | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| L2G1 | IEC 62351-9 GDOI Key Distribution | m | | m | | |
| | Hash Algorithms (RFC 8052) | | | | | |
| L2G2 | • None | m | | m | | |
| L2G3 | • HMAC-SHA256-128 | m | | m | | |
| L2G4 | • HMAC-SHA256 | m | | m | | |
| L2G5 | • AES-GMAC-128 | m | | m | | |
| L2G6 | • AES-GMAC-256 | m | | m | | |
| | Confidentiality Algorithms (RFC 8052) | o | | o | | |
| L2G7 | • None | m | | m | | |
| L2G8 | • AES-CBC-128 | o | | o | | |
| L2G9 | • AES-CBC-256 | o | | o | | |
| L2G10 | • AES-GCM-128 | o | | o | | |
| L2G11 | • AES-GCM-256 | o | | o | | |
| L2G12 | IEC 62351-6 Replay Protection (clause 6.2.1) | m | | m | | |

**Table 10 – IEC 61850-9-2 L2 SV Security**

| | Capability | Subscriber | | Publisher | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| L2S1 | IEC 62351-9 GDOI Key Distribution | m | | m | | |
| | Hash Algorithms (RFC 8052) | | | | | |
| L2S2 | • None | m | | m | | |
| L2S3 | • HMAC-SHA256-128 | m | | m | | |
| L2S4 | • HMAC-SHA256 | m | | m | | |
| L2S5 | • AES-GMAC-128 | m | | m | | |
| L2S6 | • AES-GMAC-256 | m | | m | | |
| | Confidentiality Algorithms (RFC 8052) | i | | i | | |
| L2S7 | • None | i | | i | | |
| L2S8 | • AES-CBC-128 | i | | i | | |
| L2S9 | • AES-CBC-256 | i | | i | | |
| L2S10 | • AES-GCM-128 | i | | i | | |
| L2S11 | • AES-GCM-256 | i | | i | | |
| L2S12 | 62351-6 Replay Protection (clause 6.2.2) | m | | m | | |

**Table 11 – IEC 61850-8-1 Routable GOOSE**

| | Capability | Subscriber | | Publisher | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| RG1 | IEC 62351-9 GDOI Key Distribution | m | | m | | |
| | Hash Algorithms (RFC 8052) | | | | | |
| RG2 | • None | m | | m | | |
| RG3 | • HMAC-SHA256-128 | m | | m | | |
| RG4 | • HMAC-SHA256 | m | | m | | |
| RG5 | • AES-GMAC-128 | m | | m,c1 | | |
| RG6 | • AES-GMAC-256 | m | | m,c2 | | |
| | Confidentiality Algorithms (RFC 8052) | | | | | |
| RG7 | • None | m | | m | | |
| RG8 | • AES-CBC-128 | m | | AtLeastOne(1) | | |
| RG9 | • AES-CBC-256 | m | | AtLeastOne(1) | | |
| RG10 | • AES-GCM-128 | m | | m | | |
| RG11 | • AES-GCM-256 | m | | m | | |
| RG12 | 62351-6 Replay Protection (clause 6.2.1) | m | | m | | |

c1 – shall be used as the HASH algorithm if AES-GCM-128 is used for the confidentiality algorithm.

c2 – shall be used as the HASH algorithm if AES-GCM-256 is used for the confidentiality algorithm.

**Table 12 – IEC 61850-9-2 Routable SMV**

| | Capability | Subscriber | | Publisher | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| RS1 | IEC 62351-9 GDOI Key Distribution | m | | m | | |
| | Hash Algorithms (RFC 8052) | | | | | |
| RS2 | • None | m | | m | | |
| RS3 | • HMAC-SHA256-128 | m | | m | | |
| RS4 | • HMAC-SHA256 | m | | m | | |
| RS5 | • AES-GMAC-128 | m | | m,c1 | | |
| RS6 | • AES-GMAC-256 | m | | m,c2 | | |
| | Confidentiality Algorithms (RFC 8052) | | | | | |
| RS7 | • None | m | | m | | |
| RS8 | • AES-CBC-128 | m | | o | | |
| RS9 | • AES-CBC-256 | m | | o | | |
| RS10 | • AES-GCM-128 | m | | m | | |
| RS11 | • AES-GCM-256 | m | | m | | |
| RS12 | 62351-6 Replay Protection (6.2.2) | m | | m | | |
| c1 – shall be used as the HASH algorithm if AES-GCM-128 is used for the confidentiality algorithm.<br>c2 – shall be used as the HASH algorithm if AES-GCM-256 is used for the confidentiality algorithm. | | | | | | |

## 11.4 Conformance for implementations claiming SNTP profile security

The information in Table 13 shall be provided for implementations claiming support of the security profile for SNTP IEC 61850 profile.

**Table 13 – PICS for SNTP profiles**

| | | Client | | Server | | Value/Comment |
|---|---|---|---|---|---|---|
| | | f/s | | f/s | | |
| S7 | RFC 5905 | m | | m | | |

# Bibliography

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

RFC 6234, *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 2437, *PKCS #1: RSA Cryptography Specifications Version 2.0*

RFC 3174, *Secure Hash Algorithm (SHA1)*

NIST FIPS-197, *Advanced Encryption Standard (AES)*

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

## Partie 6: Sécurité pour l'IEC 61850

## AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62351-6 a été établie par le comité d'études 57 de l'IEC: Gestion des systèmes de puissance et échanges d'informations associés.

La présente version bilingue (2020-12) correspond à la version anglaise monolingue publiée en 2020-10.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62351, publiées sous le titre général *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.**

# GESTION DES SYSTÈMES DE PUISSANCE ET ÉCHANGES D'INFORMATIONS ASSOCIÉS – SÉCURITÉ DES COMMUNICATIONS ET DES DONNÉES –

# Partie 6: Sécurité pour l'IEC 61850

## 1 Domaine d'application et objet

### 1.1 Domaine d'application

La présente partie de l'IEC 62351 spécifie les messages, procédures et algorithmes qui permettent de sécuriser le fonctionnement de tous les protocoles fondés sur ou dérivés de la série IEC 61850. Le présent document s'applique au minimum aux protocoles répertoriés dans le Tableau 1.

**Tableau 1 – Domaine d'application des normes**

| Numéro | Intitulé |
|---|---|
| IEC 61850-8-1 | Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 8-1: Mise en correspondance des services de communication spécifiques (SCSM) – Mises en correspondance pour MMS (ISO 9506-1 et ISO 9506-2) et pour l'ISO/IEC 8802-3 |
| IEC 61850-8-2 | Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 8-2: Mapping des services de communication spécifiques (SCSM) – Mapping avec le protocole XMPP (*Extensible Messaging Presence Protocol*) |
| IEC 61850-9-2 | Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 9-2: Mise en correspondance des services de communication spécifiques (SCSM) – Valeurs échantillonnées sur ISO/IEC 8802-3 |
| IEC 61850-6 | Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 6: Langage pour la description de configuration pour la communication dans les postes électriques, entre les dispositifs électroniques intelligents (IED) |



Les premiers utilisateurs auxquels s'adresse le présent document sont les membres des groupes de travail qui développent ou utilisent les protocoles répertoriés dans le Tableau 1. Pour que les mesures décrites dans la présente spécification soient mises en œuvre, elles doivent être acceptées et référencées dans les spécifications des protocoles elles-mêmes. Le présent document est rédigé afin de permettre ce traitement.

Les premiers utilisateurs auxquels s'adresse le présent document sont présumés être les concepteurs de produits qui mettent en œuvre ces protocoles.

Des parties du présent document peuvent aussi être utiles aux gestionnaires et aux dirigeants pour comprendre l'objectif d'une activité et les exigences correspondantes.

### 1.2 Nom et version de l'espace de noms

Le présent nouvel article est obligatoire pour tout espace de noms de l'IEC 61850 (comme cela est défini par la partie 7-1 de l'édition 2 de l'IEC 61850).

Les paramètres qui identifient la nouvelle version de ces espaces de noms sont:

- La version de l'espace de noms: 2020
- La révision de l'espace de noms: A
- Le nom de l'espace de noms: "IEC 62351-6:2020A"

- La libération de l'espace de noms: 1

Le tableau ci-dessous donne un aperçu de toutes les versions publiées de cet espace de noms.

| Édition | Date de publication | Boutique en ligne | Espace de noms |
|---|---|---|---|
| Édition 1.0 | 2020-? | IEC 62351-6:2020 | IEC 62351-6:2020 |

### 1.3 Répartition des éléments de code

Il n'y a actuellement aucun élément de code prévu pour la zone de téléchargement des éléments de code.

## 2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61850-6, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 6: Langage pour la description de configuration pour la communication dans les postes électriques, entre les dispositifs électroniques intelligents (IED)*

IEC 61850-7-3, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 7-3: Structure de communication de base – Classes de données communes*

IEC 61850-8-1, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 8-1: Mise en correspondance des services de communication spécifiques (SCSM) – Mises en correspondance pour MMS (ISO 9506-1 et ISO 9506-2) et pour l'ISO/IEC 8802-3*

IEC 61850-8-2, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 8-2: Mapping des services de communication spécifiques (SCSM) – Mapping avec le protocole XMPP (Extensible Messaging Presence Protocol)*

IEC 61850-9-2, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 9-2: Mise en correspondance des services de communication spécifiques (SCSM) – Valeurs échantillonnées sur ISO/IEC 8802-3*

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security- Introduction to security issues* (disponible en anglais seulement)

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms* (disponible en anglais seulement)

IEC 62351-4:2020, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 4: Profils comprenant le MMS et ses dérivés*

IEC 62351-9, *Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 9: Gestion de clé de cybersécurité des équipements de système de puissance*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures* (disponible en anglais seulement)

ISO/IEC 9594-8 | Rec. UIT-T X.509: *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – L'annuaire: Cadre général des certificats de clé publique et d'attribut*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*[1]

RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services*

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation Galois/Counter Mode (GCM and GMAC)*

## 3 Termes, définitions et abréviations

### 3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC TS 62351-2 et de l'IEC 61850-2 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

**3.1.1**
**périmètre de sécurité électronique**
frontière logique entourant un réseau qui relie des cyberactifs essentiels

**3.1.2**
**client**
unité fonctionnelle qui établi une association et qui émet des demandes à un serveur et reçoit des services de la part de ce serveur

**3.1.3**
**server**
unité fonctionnelle qui reçoit une association de la part d'un client et qui fournit les services demandés par ce client

### 3.2 Termes abrégés

| | |
|---|---|
| ACSE | Association Control Service Element (élément de service de contrôle d'association) |
| APDU | Application Protocol Data Unit (unité de données de protocole d'application) |
| ASDU | Application Service Data Unit (unité de données du service d'application) |
| ASN.1 | Abstract Syntax Notation One (notation de syntaxe abstraite numéro un) |
| ESP | Electronic Security Perimeter (périmètre de sécurité électronique) |
| GDOI | Group Domain of Interpretation (domaine d'interprétation de groupe) |

[1] Limité au profil SNTP uniquement.

GMAC Galois Message Authentication Code (code d'authentification du message de Galois)

GOOSE Generic Object Oriented Substation Event (événement de poste orienté objet générique)

GSE Generic Substation Events (événement de poste générique)

HMAC Hashed Message Authentication Code (code d'authentification de message haché)

ICT IED Configuration Tool (outil de configuration de l'IED)

IED Intelligent Electronic Device (dispositif électronique intelligent)

KDC Key Distribution Centre (centre de distribution de clé)

MAC Message Authentication Code (code d'authentification de message)

SMV Sampled Measured Values (valeurs mesurées échantillonnées)

SCL Substation Configuration Language (langage de configuration de sous-station)

SV Sampled Value (valeur échantillonnée)

# 4 Problèmes de sécurité couverts par le présent document

## 4.1 Problèmes fonctionnels qui affectent le choix des options de sécurité

Pour les applications qui utilisent GOOSE couche 2 de l'IEC 61850-8-1 et Sampled Value couche 2 de l'IEC 61850-9-2 et qui exigent des temps de réponse de 3 ms, des configurations multidiffusion et une faible surcharge des processeurs, le chiffrement n'est pas recommandé. À la place, un processus de sélection de voie de communication (par exemple, le fait que GOOSE et SV couche 2 soient supposés être restreints à un LAN de sous-station logique) doit être utilisé pour la confidentialité des échanges d'informations. Cependant, le présent document ne définit pas un mécanisme qui permette la confidentialité des applications non concernées par le critère de distribution de 3 ms.

NOTE Les caractéristiques de performances actuelles d'une mise en œuvre qui revendique la conformité à la présente spécification technique ne relèvent pas du domaine d'application du présent document.

À l'exception de la confidentialité, le présent document décrit un mécanisme qui permet la coexistence de PDU sécurisés et non sécurisés.

## 4.2 Menaces à la sécurité contrées

Voir l'IEC TS 62351-1 pour des informations sur les menaces à la sécurité et les méthodes d'attaque.

En l'absence de chiffrement, les menaces particulières traitées dans le présent article comprennent:

- la modification non autorisée (altération) des informations par l'authentification des niveaux des messages.

Si un chiffrement est utilisé, les menaces particulières traitées dans le présent article comprennent:

- l'accès non autorisé à des informations à travers l'authentification des niveaux des messages et le chiffrement des messages;
- la modification non autorisée (altération) des informations ou le vol des informations par l'authentification et le chiffrement des niveaux des messages.
- la divulgation des informations est contrée.

### 4.3 Méthodes d'attaque contrées

La mise en œuvre appropriée des spécifications/recommandations traitées dans le présent document a pour objet de contrer les méthodes d'attaque suivantes:

- attaque de l'homme du milieu: cette menace est contrée par l'utilisation d'un mécanisme de code d'authentification de message spécifié dans le présent document;
- détection de l'altération/intégrité du message: Ces menaces sont contrées par l'algorithme utilisé pour créer le mécanisme d'authentification comme cela est spécifié dans le présent document;
- rejeu: cette menace est contrée au moyen de l'utilisation de diagrammes d'états de traitement spécialisés et spécifiés dans l'IEC 62351-4 et dans le présent document.

## 5 Corrélation entre les parties de l'IEC 61850 et les parties de l'IEC 62351

### 5.1 Généralités

Il existe quatre niveaux d'interaction entre les parties de la série IEC 62351 et les parties de la série IEC 61850. La présente partie concerne:

- La sécurité du profil de communication selon:
  - Le profil d'application de l'IEC 61850-8-1 pour les communications client/serveur.
  - Le profil d'application de l'IEC 61850-8-2 pour les communications client/serveur.
  - Le profil T de la couche 2 de l'IEC 61850-8-1 pour GOOSE/GSE.
  - Le profil T de la couche 2 de l'IEC 61850-8-1 pour des valeurs échantillonnées multidiffusion.
  - GOOSE et valeurs échantillonnées acheminables de la couche 3 de l'IEC 61850-8-1.
- Les extensions de configuration exigées pour la configuration des profils de communication application et transport d'intérêt. Ces extensions touchent l'IEC 61850-6.
- Les définitions d'objets relatifs à la sécurité et à l'identification qui sont exposés pendant une durée d'exécution en tant que partie des mises en correspondance de l'objet de l'IEC 61850-8-1 et de l'IEC 61850-8-2.
- La liaison des valeurs Originator ID aux homologues authentifiés pour les services client/serveur.

Le domaine d'application du présent document apporte des spécifications de sécurité pour l'utilisation dans un périmètre de sécurité électronique (PSE) et entre plusieurs PSE.

### 5.2 Profil de l'IEC 61850-8-1 pour les communications client/serveur

#### 5.2.1 Généralités

Les mises en œuvre de l'IEC 61850 qui revendiquent la conformité à la présente spécification et qui déclarent la prise en charge du profil de l'IEC 61850-8-1 utilisant le TCP/IP et l'ISO 9506 (MMS) doivent mettre en œuvre les Articles 5 et 6 de l'IEC 62351-4:2018.

L'IEC 61850-8-1 spécifie l'utilisation MMS dans un poste. Toutefois, le domaine d'application de la présente spécification fournit des spécifications de sécurité à utiliser à l'intérieur et à l'extérieur du poste (par exemple, entre le centre de commande et le poste).

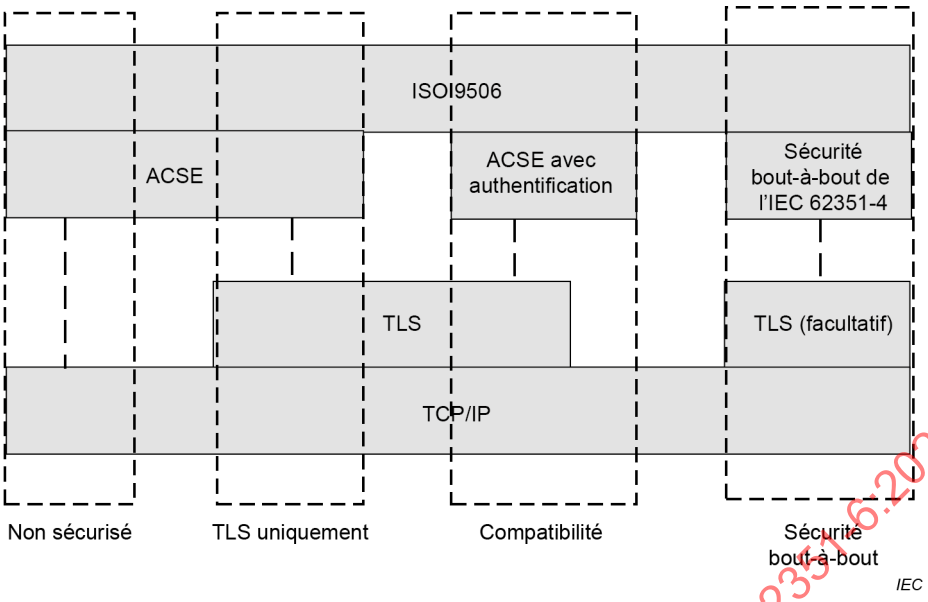



**Figure 1 – Profils de sécurité MMS**

La Figure 1 présente les profils de sécurité pour les associations client/serveur de l'IEC 61850 fondés sur l'ISO/IEC 9506:

- Non-secure: Les mises en œuvre qui revendiquent la conformité au présent article et à la capacité client/serveur doivent pouvoir être configurées sans sécuriser les connexions conformément à l'IEC 62351-4.
- TLS-only: L'utilisation de la TLS uniquement ne relève pas du domaine d'application du présent document. Ce profil ne permet pas de fournir un contrôle d'accès fondé sur le rôle (RBAC) au niveau de l'utilisateur.
- Compatibility (conformément à l'IEC 62351-4): Les mises en œuvre client qui revendiquent la conformité doivent prendre en charge la configuration et l'échange d'informations en utilisant l'authentification ACSE conformément à l'IEC 62351-4 et selon la TLS. L'utilisation d'un TLS est obligatoire.
- End-to-End: La prise en charge de ce profil de sécurité est facultative. Toutefois, dans les prochaines éditions de la présente norme, il est prévu de la rendre obligatoire.

Voir le Tableau 6 pour une déclaration formelle de conformité.

### 5.2.2 Du centre de commande au poste

L'IEC 62351-4 doit être utilisée sans autres ajouts.

### 5.2.3 Communications des postes

Les suites chiffrées obligatoires se trouvent dans l'IEC 62351-4.

## 5.3 Sécurité de l'IEC 61850 pour les profils qui utilisent des identifiants VLAN

Pour les profils IEC 61850 spécifiés qui utilisent des ID VLAN (par exemple, GOOSE de l'IEC 61850-8-1 et IEC 61850-9-2), la sécurité du profil doit être assurée comme cela est spécifié dans l'Article 8.

### 5.4 IEC 61850-8-2 pour les communications client/serveur

Les mises en œuvre de l'IEC 61850 qui revendiquent la conformité au présent document et qui déclarent la prise en charge du profil A de l'IEC 61850-8-2 pour les communications client/serveur doivent mettre en œuvre le mécanisme de sécurité entre extrémités, comme cela est spécifié par l'IEC 62351-4.

L'IEC 61850-8-2 ne prend pas en charge l'ACSE, par conséquent le mécanisme de sécurité de l'IEC TS 62351-4 de l'authentification de l'ASCE (profil A) n'est ni mis en œuvre ni pris en charge.

Par ailleurs, l'IEC 61850-8-2 utilise un profil T qui consiste en un XMPP qui à son tour commande la TLS. Ainsi, les mécanismes de sécurité de la TLS et les suites chiffrées spécifiés dans l'IEC 62351-4 ne relèvent pas du domaine d'application de l'IEC 61850-8-2.

### 5.5 Utilisation de OriginatorID pour les services client/serveur

Il existe plusieurs classes de données communes (CDC) définies dans l'IEC 61850-7-3 et des fonctions de suivi de service qui définissent explicitement la capacité à fournir des informations relatives à l'émetteur (originator) de la commande ou du service. La valeur réelle qui représente l'entité initiatrice dans l'IEC 61850-8-1 et dans l'IEC 61850-8-2 est originatorID, qui est une chaîne de 64 octets.

L'utilisation d'une sécurité et d'une authentification fondées sur des certificats fournit un mécanisme de fourniture d'informations fiables relatives à l'émetteur. Cependant, la restriction de taille de originatorID n'est pas assez importante pour fournir l'exposition de l'émetteur et du numéro de série. Par conséquent, les mises en œuvre qui revendiquent la conformité à la présente norme doivent mettre en œuvre l'attribut de données facultatif certIssuer dans l'instance des classes de données communes (CDC) de l'IEC 61850-7-3 de: CST, BTS, UTS, LTS, GTS, MTS, NTS, et STS.

L'utilisation de la valeur de l'attribut de données certIssuer suit:

- La valeur doit être une concaténation de la séquence des valeurs de nom qui peuvent être présentes dans le champ Issuer. S'il y a plus d'un nom dans la séquence, le jeton de concaténation doit être le caractère "\". À une longueur de zéro (0) si l'association de client n'est pas authentifiée.
- À la valeur du Issuer Name X.509 pour une association de client authentifiée.
- Si la valeur concaténée est supérieure à 255 caractères, elle doit être tronquée à 255 caractères.
- Si l'association de client n'a pas été authentifiée par des certificats, la longueur de certIssuer doit être zéro (0) et par conséquent la valeur doit être NULL. Tous les octets de la valeur doivent être initialisés à 0.

Les mises en œuvre qui revendiquent la conformité à la présente norme doivent également utiliser l'attribut de données originatorID comme suit:

- Si la valeur certIssuer n'est pas NULL, la valeur du numéro de série du certificat X.509 doit être utilisée pour la valeur des associations de clients qui ont été authentifiées par un certificat. Un numéro de série de certificat est une valeur entière positive encodée. La valeur encodée doit être copiée dans la valeur originatedID, n'incluant pas l'étiquette ou la longueur.
- Si la valeur de certIssuer est NULL, la valeur de originatorID peut être "unknown" avec "u" étant l'octet le plus significatif de la valeur. Les autres valeurs sont définies localement.

# 6 Protocoles d'association multidiffusion

## 6.1 Généralités

L'IEC 61850-8-1 et l'IEC 61850-9-2 spécifient deux protocoles d'application différents qui utilisent le modèle d'association multidiffusion de l'IEC 61850. Il s'agit de GSE (par exemple GOOSE) et de valeurs échantillonnées multidiffusion. Ces protocoles d'application sont mis en correspondance avec deux profils T différents.

Les profils T spécifiés fournissent une couche 2 et une mise en correspondance acheminable du protocole d'application. La combinaison des profils A et des profils T est communément appelée couche 2 ou acheminable (par exemple GOOSE couche 2 ou GOOSE acheminable). Le présent document spécifie les comportements de sécurité communs indépendamment du profil T et des extensions de protocole de sécurité spécifiques pour les profils T couche 2.

Le présent article spécifie les comportements attendus relatifs à la protection contre le rejeu pour GOOSE et valeurs échantillonnées multidiffusion indépendamment du profil T utilisé.

## 6.2 Protection contre le rejeu

La protection contre le rejeu peut être mise en œuvre pour les profils A GOOSE et Sampled Value avec ou sans extension de sécurité. Les algorithmes de protection contre le rejeu spécifiés dans les articles suivants concernent les abonnés qui revendiquent la conformité à la présente partie, et par conséquent la protection contre le rejeu doit être mise en œuvre sans tenir compte de la sécurité de l'APDU publiée de GOOSE ou Sampled Value. L'algorithme de protection contre le rejeu est mis en œuvre par l'abonné.

### 6.2.1 Protection contre le rejeu GOOSE

#### 6.2.1.1 Généralités

Le diagramme normal d'états d'abonné pour le service GOOSE de l'IEC 61850-8-1 ne détaille pas la façon dont il convient de recevoir les numéros d'état (stNum) ou les numéros de séquence (sqNum) hors d'usage.

Les mises en œuvre qui revendiquent la conformité à la présente norme doivent mettre en œuvre le diagramme d'états représenté à la Figure 2. Les vérifications de sécurité et de rejeu supplémentaires peuvent être mises en œuvre. Pour le présent article, l'application est définie comme la fonction de l'abonné GOOSE et non comme le processus réel qui utilise GOOSEData (conformément à l'IEC 61850-7-2) afin d'assurer la protection, etc.

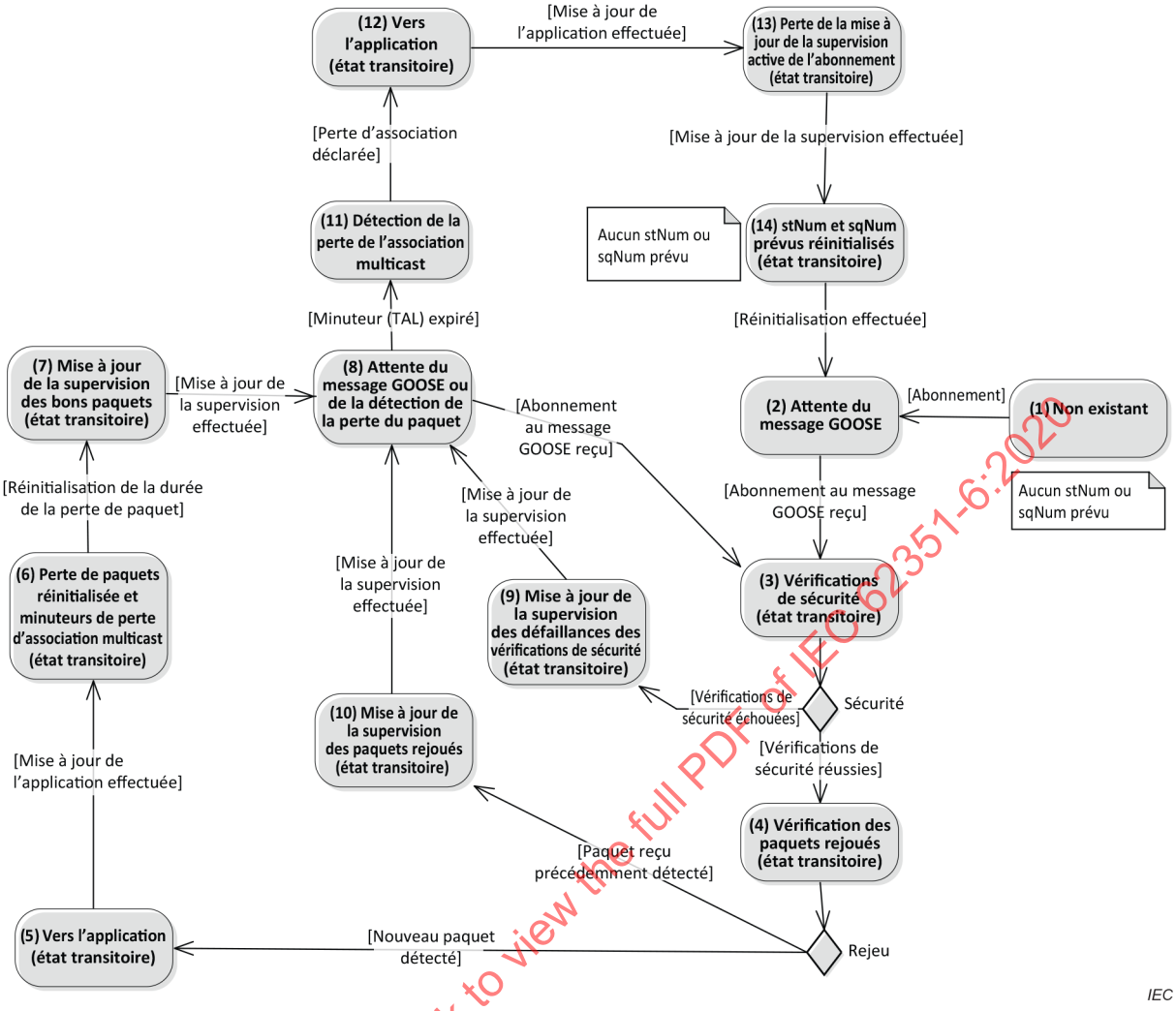



**Figure 2 – Diagramme d'états de protection contre le rejeu pour GOOSE**

La Figure 2 est pertinente pour les messages GOOSE pour lesquels l'abonné a un abonnement actif qui doit être configuré manuellement ou par un SCL et un ICT. Les autres mécanismes de configuration ne relèvent pas du domaine d'application. Les mises en œuvre qui revendiquent la conformité au présent article doivent maintenir au minimum les variables internes du diagramme d'états suivantes: dernier stNum reçu (lastRcvStNum); dernier sqNum reçu (lastRcvSqNum); dernier horodatage de changement d'état reçu (lastRcvT); et une valeur interne de durée de vie admise (intTAL). Les états et leurs transitions sont définis comme suit:

1) L'état Non existant représente l'état qui ne contient pas d'abonnement GOOSE.
2) À l'activation de l'abonnement (par exemple, lors du démarrage ou de la configuration de l'abonnement), le diagramme d'états règle en interne lastRcvStNum, lastRcvSqNum, lastRcvT et intTAL sur invalide puisqu'aucun message GOOSE n'a été reçu et que le diagramme d'états passe à l'état Attente du message GOOSE.

   Au moment de la réception du message GOOSE souscrit, l'abonné doit passer à l'état Vérifications de sécurité (étape 3).
3) Le traitement à l'état Vérifications de sécurité est décrit en 6.2.1.2.

   Si l'abonné n'a jamais reçu de clé du KDC, il doit satisfaire au contrôle de sécurité pour les paquets non chiffrés. Si l'abonné reçoit une clé du KDC mais qu'il ne possède pas la clé spécifiée par le keyID dans le message GOOSE, l'abonné passe en défaillance des vérifications de sécurité et doit effectuer un GROUP-PULL comme cela est défini par l'IEC 62351-9.

Si l'abonné n'a pas pu recevoir les clés avant l'expiration de la dernière clé livrée, il doit signaler une alarme qui indique que la distribution des clés a échoué et que les clés expirées sont définies par hypothèse. Il doit traiter les paquets dont le keyID est la dernière clé livrée. Lors de la distribution d'un keyID inconnu, alors qu'il utilise une clé expirée, l'abonné doit immédiatement effectuer un GROUP-PULL afin de synchroniser les clés.

Si les essais de sécurité sont concluants, le diagramme d'états doit passer à la vérification des paquets rejoués (étape 4).

Si l'essai de sécurité échoue, le diagramme d'états doit passer à l'état de mise à jour de la supervision des défaillances des vérifications de sécurité (état 9).

4) L'état de vérification de rejeu doit effectuer le traitement de 6.2.1.3.

   Si aucun rejeu n'est détecté, une transition vers l'état de mise à jour de l'application (état 5) doit se produire.

   Si un rejeu est détecté, une transition vers l'état de mise à jour de la supervision des paquets rejoués (état 10) doit se produire.

5) L'état "Vers l'application" doit décoder le paquet GOOSE. Les informations décodées doivent être livrées à l'application si le stNum décodé n'est pas égal à lastRcvStNum. Une modification de sqNum qui doit provoquer la livraison des informations à l'application est définie localement.

   Les valeurs de lastRcvStNum et de lastRcvSqNum doivent être mises à jour au niveau des valeurs décodées du paquet GOOSE.

   L'état doit passer à l'état 6.

6) La valeur intTAL doit être réglée sur une valeur liée à la valeur TAL décodée. La temporisation de la perte d'association doit également être réinitialisée à une valeur déterminée localement.

7) Les informations de supervision doivent être mises à jour en fonction des nouvelles informations de paquet reçues. Voir 6.2.1.4 pour des exigences relatives au traitement.

   Dès la mise à jour des informations de supervision, passer à l'état 8.

8) La valeur de intTAL doit être utilisée afin de détecter la perte de paquet. L'état doit entamer une durée d'expiration fondée sur la valeur actuelle de intTAL.

   Si la valeur de intTAL est de zéro (par exemple, expirée), un passage à l'état 11 doit se produire.

   Si l'abonnement au paquet GOOSE est reçu, l'état doit passer à l'état 3.

9) Les informations de supervision doivent être mises à jour en fonction des informations de défaillance des vérifications de sécurité reçues. Voir 6.2.1.4 pour des exigences relatives au traitement.

   Dès la mise à jour des informations de supervision, passer à l'état 8. Aucune réinitialisation ou aucun réglage de intTAL ne doit être effectué.

10) Les informations de supervision doivent être mises à jour en fonction des informations de détection de rejeu. Voir 6.2.1.4 pour des exigences relatives au traitement.

    Dès la mise à jour des informations de supervision, passer à l'état 8. Aucune réinitialisation ou aucun réglage de intTAL ne doit être effectué.

11) Cet état est utilisé pour déterminer si un abonnement n'est plus actif. Il diffère de la détection de la perte de paquet puisqu'il est défini localement.

    Dès lors qu'il a été décidé que l'abonnement n'est plus actif, l'état passe à l'état 12.

12) L'application doit être mise à jour de façon à être informée de la validité de l'abonnement. Les moyens d'effectuer la mise à jour sont définis localement.

    Après la mise à jour de l'application, l'état doit passer à l'état 13.

13) Les informations de supervision doivent être mises à jour sur la base d'une perte d'un abonnement actif (par exemple LGOS.St doit changer d'état). Voir 6.2.1.4 pour des exigences relatives au traitement.
    Dès la mise à jour des informations de supervision, passer à l'état 14.

14) Les valeurs lastRcvStNum et lastRcvSqNum doivent être réglées sur invalide et un passage à l'état 2 doit se produire.

#### 6.2.1.2 Exigences de protection de vérification de sécurité

Le présent paragraphe spécifie le traitement exigé pour la vérification des paramètres de sécurité GOOSE.

- L'abonné doit vérifier si AuthenticationValue (voir 8.2.2.1) est conforme à la configuration prévue conformément à l'IEC 61850-6 et s'il met en œuvre la sécurité.
  - Si AuthenticationValue est prévue par configuration de GSEControl.securityEnable et qu'aucune AuthenticationValue n'est fournie, cela doit résulter en une défaillance de la vérification de sécurité et aucun traitement de vérification de sécurité ultérieur n'est exigé.
  - S'il n'y a pas d'AuthenticationValue prévue et qu'une AuthenticationValue est fournie, elle doit être traitée comme s'il n'y avait pas d'AuthenticationValue. La valeur AuthenticationValue ne doit pas être vérifiée, mais elle ne doit pas constituer une défaillance des vérifications de sécurité.
  - S'il n'y a pas d'AuthenticationValue prévue et qu'aucune AuthenticationValue n'est présente, cela ne doit pas constituer une défaillance de la vérification de sécurité.
  - S'il y a une AuthenticationValue et que l'abonné ne prend pas en charge l'authentification, cela ne doit pas constituer une défaillance de la vérification de sécurité.
- Si le chiffrement est utilisé, le paquet doit être déchiffré.

Si aucune des vérifications de sécurité n'échoue, le diagramme d'états doit passer à l'état suivant.

#### 6.2.1.3 Exigences de traitement de l'état de vérification de rejeu

Le présent article spécifie le traitement exigé pour la vérification de rejeu de paquet GOOSE.

- Si LPHD.Sim est passé à TRUE, et que le premier GOOSE simulé a été traité, aucune relecture ne doit être détectée. Cela indique une transition entre le traitement des paquets d'un véritable éditeur et le traitement des paquets d'un ensemble d'essais.
- Si LPHD.Sim est passé à FALSE, et que le premier GOOSE non simulé est en cours de traitement, aucune relecture ne doit être détectée. Cela indique une transition entre le traitement de paquets simulés d'un ensemble d'essais et le traitement de paquets qui proviennent d'un véritable éditeur.
- L'abonné doit vérifier l'horodatage (t) reçu dans le message GOOSE par rapport à lastRcvT. Le traitement est:
  - Si l'abonné a un lastRcvT invalide, il doit mettre à jour la valeur de lastRcvT sur celle de "T" reçue dans le message GOOSE.
  - Si lastRcvT et lastRcvStNum sont valides:
    i) Si lastRcvStNum est inférieur au stNum reçu, l'abonné doit vérifier que la valeur de "T" reçue n'est pas supérieure à la valeur de l'écart de distribution locale plus ancienne ou plus récente que son heure locale. Si la valeur de "T" est hors de cette plage, cela constitue une défaillance. Aucun traitement ultérieur de la protection contre le rejeu n'est nécessaire puisqu'il a déjà échoué.

       L'utilisation de la variance de distribution est définie localement.
- L'abonné doit vérifier stNum et sqNum reçus dans le message GOOSE. Le traitement est:
  - Si l'abonné a des états invalides pour lastRcvStNum et lastRcvSqNum, le diagramme d'états d'abonné doit régler les valeurs sur:
    i) lastRcvStNum doit être réglé sur la valeur de stNum reçue dans le paquet GOOSE.
    ii) lastRcvSqNum doit être réglé sur la valeur de sqNum reçue dans le paquet GOOSE.

Aucune vérification de rejeu ultérieure n'est nécessaire.

– S'il existe des valeurs valides de lastRcvStNum et lastRcvSqNum, l'abonné doit:

i) Déterminer si le renversement de sqNum était imminent. Si la valeur de stNum reçue est zéro (0), alors les valeurs de lastRcvStNum et lastRcvSqNum doivent être mises à jour aux valeurs de stNum et sqNum respectivement.

Aucune vérification de rejeu ultérieure n'est nécessaire.

ii) Un stNum reçu inférieur à lastRcvStNum ou un sqNum inférieur à lastRcvSqNum peut être causé par un ou deux facteurs:

Un rejeu de paquet ou un paquet à cheminement multiple retardé. Dans les deux cas, le GOOSE reçu ne doit pas être fourni à l'application et le diagramme d'états doit se comporter comme si le paquet était un rejeu. Toutefois, si l'état de supervision classifie cette occurrence en rejeu, il est défini localement.

#### 6.2.1.4 Exigences de traitement de l'état de mise à jour de supervision

L'état de mise à jour de supervision est un état transitoire utilisé pour représenter la mise à jour locale de LGOS, des logs locaux, des logs de sécurité normalisés, des MIB à gestion de réseau propriétaire et de la création d'événements de sécurité, ainsi que les MIB normalisés de l'IEC 62351-7.

### 6.2.2 Protection contre le rejeu de Sampled Value

#### 6.2.2.1 Généralités

L'IEC 61850-9-2 ne détaille pas la façon dont il convient de traiter la livraison des messages hors service. Dans certains cas, la livraison hors service ne constitue pas un rejeu et peut simplement se fonder sur des délais de livraison à cheminement multiple. Contrairement à GOOSE, les valeurs échantillonnées n'ont pas de construction de nombre/nombre de séquences d'états pour la protection contre le rejeu. Par conséquent, les mises en œuvre qui revendiquent la conformité au présent document doivent mettre en œuvre ce qui suit.

#### 6.2.2.2 Éditeur

Afin d'empêcher le rejeu de SV, le champ de sécurité du protocole SV doit être présent (voir le Tableau 2).

**Tableau 2 – Extrait de l'IEC 61850-9-2 (Informatif)**

| |
|---|
| ASN.1 Basic Encoding Rules (BER)<br>SavPdu::=<br>**SEQUENCE {** |
| noASDU [0] IMPLICIT INTEGER (1..65535), |
| security [1] ANY OPTIONAL, |
| asdu [2] IMPLICIT SEQUENCE OF ASDU<br>**}** |

La prévention du rejeu exige que l'éditeur inclue le champ de sécurité facultatif dans SavPdu et qu'il mette en œuvre une forme de protection de l'intégrité comme cela est spécifié pour les différents profils T (par exemple couche 2 ou acheminable).

Le champ de sécurité SavPdu ne doit pas être présent si la sécurité de Sampled Value n'est pas fournie dans un message donné. Si la sécurité est utilisée pour le message, le champ doit être présent et son contenu doit être:

```
IMPORT
security::=  [0] IMPLICIT SEQUENCE {
                    timestamp [0] IMPLICIT OCTETSTRING, --durée d'envoi
                    …
                   }
```

**timestamp**

L'attribut horodatage doit représenter la durée approximative durant laquelle la trame SV a été formatée.

Le format d'octet doit être celui de l'horodatage de l'IEC 61850-8-1.

L'exactitude de la durée de la valeur doit être d'au moins 208 µsec.

### 6.2.2.3 Abonné

Sur la base du champ SV security présent, ou en utilisant un SMV acheminable, les règles de diagramme d'états de client suivantes doivent s'appliquer:

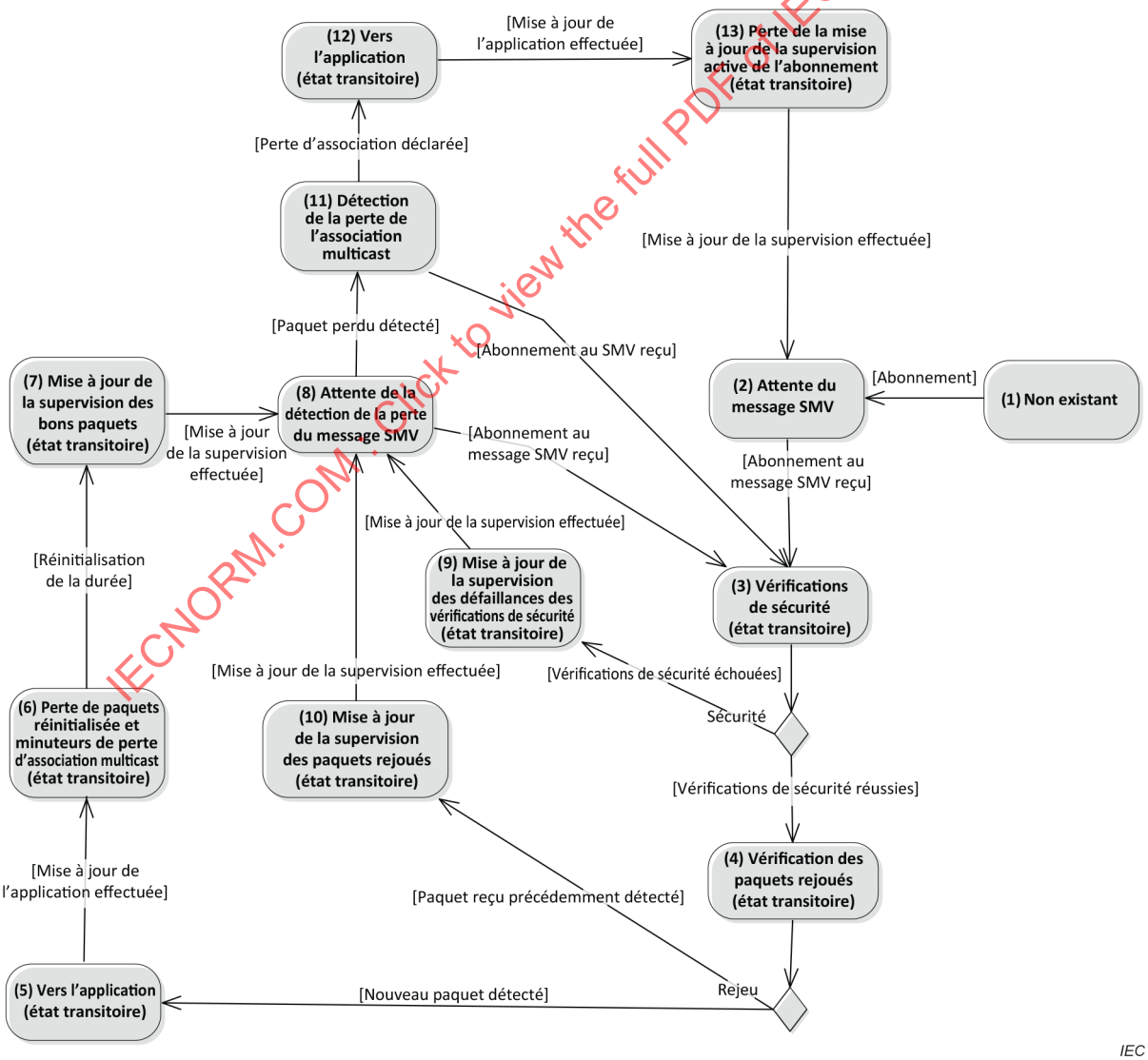



**Figure 3 – Diagramme d'états de protection contre le rejeu pour SV**

La Figure 3 est pertinente pour les messages SV pour lesquels l'abonné a un abonnement actif qui doit être configuré manuellement ou par un SCL et un ICT. Les autres mécanismes de configuration ne relèvent pas du domaine d'application. Les mises en œuvre qui revendiquent la conformité au présent article doivent maintenir au minimum les variables internes des diagrammes d'états suivantes: dernière valeur d'horodatage reçue (lastRcvT) et durée jusqu'au prochain paquet prévu (expNxtPkt). Les états et leurs transitions sont définis comme suit:

1) L'état Non existant représente l'état qui ne contient pas d'abonnement SV.
2) À l'activation de l'abonnement (par exemple, lors du démarrage ou de la configuration de l'abonnement), le diagramme d'états règle en interne lastRcvT et expNxtPk, et passe à l'état Attente du message SV.

   Au moment de la réception du message SV souscrit, l'abonné doit passer à l'état Vérifications de sécurité (étape 3).
3) Le traitement à l'état Vérifications de sécurité est décrit à l'Article 6.2.2.3.1.

   Si les essais de sécurité sont concluants, le diagramme d'états doit passer à la vérification des paquets rejoués (étape 4).

   Si l'essai de sécurité échoue, le diagramme d'états doit passer à l'état de mise à jour de la supervision des défaillances des vérifications de sécurité (état 9).
4) L'état de vérification de rejeu doit effectuer le traitement de l'Article 6.2.2.3.2.

   Si aucun rejeu n'est détecté, une transition vers l'état de mise à jour de l'application (état 5) doit se produire.

   Si un rejeu est détecté, une transition vers l'état de mise à jour de la supervision des paquets rejoués (état 10) doit se produire.
5) L'état "Vers l'application" doit décoder le paquet SV. Les informations décodées doivent être livrées à l'application.

   L'état doit passer à l'état 6.
6) La valeur expNxtPkt doit être réglée à la valeur déterminée par les calculs suivants:

   Le calcul dynamique de expNxtPkt est admis pour les systèmes dont la configuration ne se fonde pas sur SCL. La valeur de expNxtPkt est calculée dynamiquement selon le même calcul, ce dernier se fonde cependant sur les valeurs reçues dans le SV APDU réel.

   La valeur de expNxtPk est définie comme:

   Pour smpMod = SmpPerSec:

   expNxtPk = (noASDU/smpRate) * 2

   Pour smpMod = SecPerSmp:

   expNxtPk = smpRate * noASDU * 2

   Pour smpMod=SmpPerPeriod:

   expNxtPk = ((noASDU/smpRate)/(fréquence nominale)) * 2

   L'expiration du minuteur provoque le passage à un état qui peut ajouter un délai supplémentaire à la déclaration réelle d'une perte d'abonnement multidiffusion.

   La temporisation de la perte d'association doit également être réinitialisée à une valeur déterminée localement.
7) Les informations de supervision doivent être mises à jour en fonction des nouvelles informations de paquet reçues. Voir 6.2.1.4 pour des exigences relatives au traitement.

   Dès la mise à jour des informations de supervision, passer à l'état 8.
8) Si l'abonnement au paquet SV est reçu, l'état doit passer à l'état 3.

   Le minuteur de détection de perte d'association multidiffusion local doit être déclenché. Si le minuteur s'arrête, un passage à l'état 11 doit être effectué.

9) Les informations de supervision doivent être mises à jour en fonction des informations de défaillance des vérifications de sécurité reçues. Voir l'Article 6.2.2.3.3 pour des exigences relatives au traitement.

   Dès la mise à jour des informations de supervision, passer à l'état 8.

10) Les informations de supervision doivent être mises à jour en fonction des informations de détection de rejeu. Voir l'Article 6.2.2.3.3 pour des exigences relatives au traitement.

    Dès la mise à jour des informations de supervision, passer à l'état 8.

11) Cet état est utilisé pour déterminer si un abonnement n'est plus actif. Il diffère de la détection de la perte de paquet puisqu'il est défini localement.

    Si l'abonnement au message SV est reçu, l'état doit passer à l'état 3.

12) L'application doit être mise à jour de façon à être informée de la validité de l'abonnement. Les moyens d'effectuer la mise à jour sont définis localement.

    Après la mise à jour de l'application, l'état doit passer à l'état 13.

13) Les informations de supervision doivent être mises à jour sur la base d'une perte d'un abonnement actif (par exemple LSVS.St doit changer d'état). Voir l'Article 6.2.2.3.3 pour des exigences relatives au traitement.

#### 6.2.2.3.1 Exigences de protection de vérification de sécurité

Le présent paragraphe spécifie le traitement exigé pour la vérification des paramètres de sécurité SV.

- L'abonné doit vérifier si AuthenticationValue (voir 8.2.2.1) est conforme à la configuration prévue par le bloc de contrôle de l'IEC 61850-6:2018 et s'il met en œuvre la sécurité.
  - Si AuthenticationValue est prévue par configuration de GSEControl.securityEnable et qu'aucune AuthenticationValue n'est fournie, cela doit résulter en une défaillance de la vérification de sécurité et aucun traitement de vérification de sécurité ultérieur n'est exigé.
  - S'il n'y a pas d'AuthenticationValue prévue et qu'une AuthenticationValue est fournie, elle doit être traitée comme s'il n'y avait pas d'AuthenticationValue. La valeur AuthenticationValue ne doit pas être vérifiée, mais elle ne doit pas constituer une défaillance des vérifications de sécurité.
  - S'il n'y a pas d'AuthenticationValue prévue et qu'aucune AuthenticationValue n'est présente, cela ne doit pas constituer une défaillance de la vérification de sécurité.
  - S'il y a une AuthenticationValue et que l'abonné ne prend pas en charge l'authentification, cela ne doit pas constituer une défaillance de la vérification de sécurité.
- Si le chiffrement est utilisé, le paquet doit être déchiffré.

Si aucune des vérifications de sécurité n'échoue, le diagramme d'états doit passer à l'état suivant.

#### 6.2.2.3.2 Exigences de traitement de l'état de vérification de rejeu

Le présent article spécifie le traitement exigé pour la vérification de rejeu de paquet SV.

- L'abonné doit vérifier l'horodatage de sécurité (t) reçu dans le message SV par rapport à lastRcvT. Le traitement est:
  - Si l'abonné a un lastRcvT invalide, il doit mettre à jour la valeur de lastRcvT sur celle de l'horodatage de sécurité reçue dans le message SV.
  - Si l'abonné a une valeur précédemment reçue, il doit vérifier que la nouvelle valeur reçue est supérieure à la valeur précédente.

L'abonné doit surveiller le smpCnt en tant que valeur croissante.

#### 6.2.2.3.3 Exigences de traitement de l'état de mise à jour de supervision

L'état de mise à jour de supervision est un état transitoire utilisé pour représenter la mise à jour locale de LSVS, des logs locaux, des logs de sécurité normalisés, des MIB à gestion de réseau propriétaire et de la création d'événements de sécurité, ainsi que les MIB normalisés de l'IEC 62351-7.

## 7 Sécurité pour SNTP

L'IEC 61850-8-1 et l'IEC 61850-8-2 spécifient l'utilisation de SNTP pour la synchronisation temporelle.

Les mises en œuvre qui revendiquent la conformité au présent document doivent mettre en œuvre le profil RFC 5905 pour SNTP qui comprend l'utilisation obligatoire des algorithmes d'authentification.

## 8 Sécurité de couche 2 pour les profils pour GOOSE de l'IEC 61850-8-1 et Sampled Value de l'IEC 61850-9-2

### 8.1 Présentation de l'Ethertype (informative)

Le présent document étend les PDU des couches 2 de GOOSE de l'IEC 61850 et de Sampled Measured Value de l'IEC 61850-9-2. La définition normative de la couche 2 de GOOSE et de Sampled Measured Value de GOOSE de l'IEC 61850 se trouve dans l'Annexe C de l'IEC 61850-8-1:2011.

### 8.2 PDU étendu

#### 8.2.1 Format général d'un PDU étendu

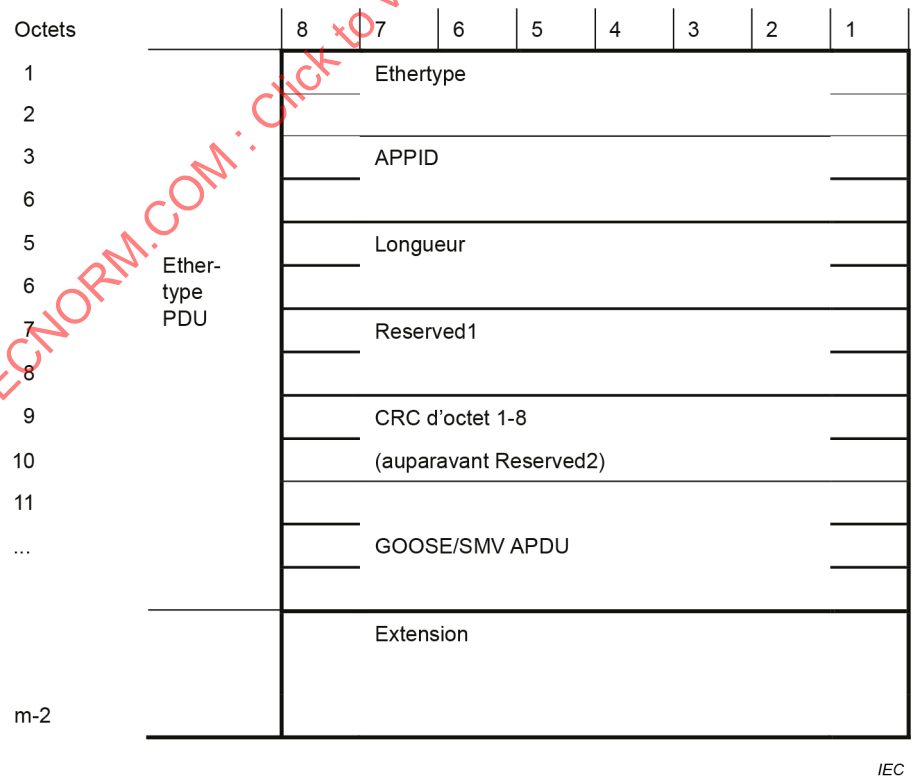



**Figure 4 – Format général d'un PDU étendu**

La Figure 4 décrit la façon dont les champs Reserved1 et Reserved2 doivent être utilisés pour les mises en œuvre qui revendiquent la conformité à la présente spécification en ce qui concerne GOOSE et la sécurité SV. Cette spécification précise que:

– Le champ **Reserved1** doit être utilisé pour inclure le nombre d'octets transmis par les octets d'extension. Cette valeur doit être comprise dans le premier octet du champ Reserved1. Une valeur de zéro (0) doit indiquer qu'aucun octet d'extension n'est présent. La structure de Reserved1 est définie à la Figure 5.

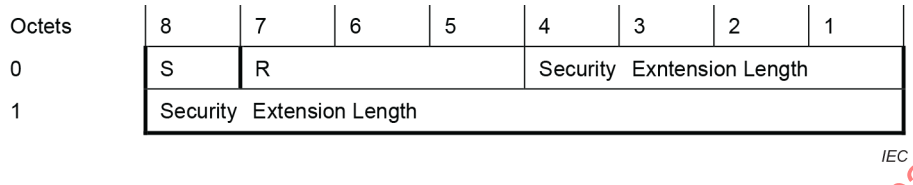



**Figure 5 – Définition de Reserved1**

– Le champ **Reserved2** doit contenir un CRC 16 bit, comme cela est calculé par l'ISO/IEC 13239 (ISO HDLC). Le CRC doit être calculé sur les octets 1 à 8 des informations VLAN du PDU étendu.

  Le CRC doit être présent si Extension Length possède une valeur non nulle.

### 8.2.2 Format des octets d'extension

#### 8.2.2.1 Généralités

Le format de l'octet d'extension doit être:

```
Extension::= {
        [0] IMPLICIT SEQUENCE {
                [1] IMPLICIT SEQUENCE Reserved OPTIONAL,
                [2] IMPLICIT OCTETSTRING Private OPTIONAL,
                [3] IMPLICIT OCTETSTRING Reserved OPTIONAL, --ne pas utiliser
                [4] IMPLICIT SEQUENCE AuthenticationValue OPTIONAL,
                [5] IMPLICIT OCTETSTRING mAC OPTIONAL,
                …,
                }
        …,
        }
```

L'extension doit être encodée par les règles de codage de base ASN.1.

La SEQUENCE Reserved est réservée à la future extension normalisée pour la présente spécification. S'il n'existe pas d'extension, à part l'authentification et le chiffrement définis dans la présente spécification, cette SEQUENCE ne doit pas être présente.

Par conséquent, une SEQUENCE de longueur NULL doit être considérée comme non conforme à la présente spécification.

La SEQUENCE Private est fournie afin de permettre aux fournisseurs de transmettre des informations privées. Le domaine d'application de la sémantique et de la syntaxe du contenu de cette SEQUENCE ne relève pas du domaine d'application de la présente spécification et ne doit être interopérable que par accord préalable. Cette SEQUENCE ne doit être présente que si un contenu réel est transmis.

Si AuthenticationValue est présente, il doit y avoir une valeur mAC.

#### 8.2.2.2 mAC

La valeur MAC calculée doit être utilisée pour l'authentification/l'intégrité des octets qui commencent avec l'identifiant Ethertype pour GOOSE ou SV jusqu'à la fin de l'APDU GOOSE/SV, les extensions de sécurité excluant la TLV MAC. Les calculs ne doivent pas inclure la production MAC. La valeur des paramètres doit être calculée en se fondant sur l'algorithme spécifié.

La valeur de MAC doit être traitée comme des valeurs ASN.1 OCTETString.

Les fonctions MAC admises sont: HMAC-SHA256 et AES-GMAC.

Les fonctions MAC obligatoires HMAC-SHA256 et AES-GMAC doivent être prises en charge.

Les longueurs MAC admises peuvent être trouvées dans le Tableau 9 et le Tableau 10. La valeur MAC calculée peut être tronquée conformément à la RFC 2104.

Par conséquent, les valeurs énumérées de MAC utilisées dans l'algorithme de sécurité doivent être celles définies dans la RFC 8052.

L'option MAC-None est fournie pour la soumission à l'essai et ne doit pas être utilisée dans les systèmes de production. Elle indique qu'aucune valeur MAC (par exemple, MAC) n'est calculée. Par conséquent, pour MAC-None, l'octet de longueur de mAC contient une valeur de zéro (0).

La longueur de sortie ne doit pas être inférieure à huit (8) octets.

La périodicité entre les nouvelles clés est liée à la force de MAC. Il est nécessaire, notamment, d'évaluer les recommandations pour AES-GMAC. Le document correspondant est le NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf).

L'action qui résulte de la détection d'une MAC invalide reçue doit être documentée comme cela est spécifié à l'Article 10. Il est recommandé que les informations ne soient pas traitées et que certains événements relatifs à la sécurité soient déclenchés. Le type d'événement est défini localement, mais peut relever de l'IEC 62351-7 et/ou de l'augmentation de l'attribut AuthFail d'un nœud logique d'application de sécurité générique GSAL.

Si le chiffrement de GOOSE ou SV APDU est utilisé, MAC doit se trouver sur l'APDU chiffré.

Les informations couvertes par MAC sont présentées comme le domaine mAC calculé à la Figure 6.

Les informations de l'Extension incluent toute la production de l'Extension à l'exception du mAC. La Figure 6 présente la couverture des implémentations qui revendiquent la conformité à l'IEC 62351-6 utilisant uniquement AuthenticationValue et mAC.