CONTENTS

[FOREWORD 3](#_Toc485991003)

[1 Scope 5](#_Toc485991004)

[2 Normative references 5](#_Toc485991005)

[3 Terms and definitions 6](#_Toc485991006)

[4 Security issues addressed by this specification 7](#_Toc485991007)

[4.1 Operational issues affecting choice of security options 7](#_Toc485991008)

[4.2 Security threats countered 7](#_Toc485991009)

[4.3 Attack methods countered 7](#_Toc485991010)

[5 Correlation of IEC 61850 parts and IEC 62351 parts 7](#_Toc485991011)

[5.1 IEC 61850-8-1 A-Profile for Client/Server communications 8](#_Toc485991012)

[5.1.1 Additional cipher suite support 8](#_Toc485991013)

[5.2 IEC 61850-8-2 A-Profile for Client/Server communications 8](#_Toc485991014)

[5.2.1 Additional cipher suite support 8](#_Toc485991015)

[5.3 Using OriginatorID for Client/Server Services 8](#_Toc485991016)

[6 Multicast Association Protocols 9](#_Toc485991017)

[6.1 Replay Protection 9](#_Toc485991018)

[6.1.1 GOOSE replay protection 9](#_Toc485991019)

[6.1.2 Sampled Value replay protection 13](#_Toc485991020)

[7 Security for SNTP 16](#_Toc485991021)

[8 Layer 2 security for profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sampled Value 16](#_Toc485991022)

[8.1 Overview of Ethertype (informative) 16](#_Toc485991023)

[8.2 Extended PDU 17](#_Toc485991024)

[8.2.1 General format of extended PDU 17](#_Toc485991025)

[8.2.2 Format of extension octets 17](#_Toc485991026)

[8.2.3 &mAC 19](#_Toc485991027)

[9 Substation configuration language extensions 20](#_Toc485991028)

[9.1 Originator ID 20](#_Toc485991029)

[9.2 Skew configuration 21](#_Toc485991030)

[9.3 SCL certificate extension 22](#_Toc485991031)

[9.3.1 &XferNumber 22](#_Toc485991032)

[9.3.2 &SerialNumber 22](#_Toc485991033)

[9.3.3 &Subject 22](#_Toc485991034)

[9.3.4 &IssuerName 22](#_Toc485991035)

[9.3.5 &CommonName 22](#_Toc485991036)

[9.4 Specification of AccessPoint security usage 23](#_Toc485991037)

[10 Conformance 23](#_Toc485991038)

[10.1 General conformance 23](#_Toc485991039)

[10.2 Conformance for implementations claiming IEC 61850 Client/Server 24](#_Toc485991040)

[10.3 Conformance for implementations claiming IEC 61850-8-2 Client/Server 24](#_Toc485991041)

[10.4 Conformance for implementations claiming GOOSE security 25](#_Toc485991042)

[10.5 Conformance for implementations claiming Layer 2 IEC 61850-8-1 MSV security 25](#_Toc485991043)

[10.6 Conformance for implementations claiming SNTP profile security 27](#_Toc485991044)

[**Bibliography** 28](#_Toc485991045)

[17](#_Toc485991046)

[Figure 2 – General format of extended PDU 17](#_Toc485991047)

[Figure 3 – SCL extensions for certificates 22](#_Toc485991048)

[Figure 4 – Extension to AccessPoint SCL definition 23](#_Toc485991049)

[Table 3 – Extract from IEC 61850-9-2 (informative) 13](#_Toc485991050)

[Table 2 – Allowed values for MAC signature value calculations 19](#_Toc485991051)

[Table 4 – Conformance table for IEC 61850 Security 24](#_Toc485991052)

[Table 5 – PICS for IEC 61850-8-1 Client/Server 24](#_Toc485991053)

[Table 6 – PICS for IEC 61850-8-2 Client/Server 24](#_Toc485991054)

[Table 7 – PICS for 61850-8-1 GOOSE security 25](#_Toc485991055)

[Table 7 – PICS for Layer 2 IEC 61850-8-1 GOOSE security 25](#_Toc485991056)

[Table 7 – PICS for Routable IEC 61850-8-1 GOOSE security 25](#_Toc485991057)

[Table 8 – PICS for Layer 2 IEC 61850-8-1 MSV security 26](#_Toc485991058)

[Table 7 – PICS for Layer 2 IEC 61850-8-1 GOOSE security 26](#_Toc485991059)

[Table 7 – PICS for Routable IEC 61850-8-1 GOOSE security 26](#_Toc485991060)

[Table 6 – PICS for SNTP profiles 27](#_Toc485991061)

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

* the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
* the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-6, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

|  |  |
| --- | --- |
| Enquiry draft | Report on voting |
| 57/805/DTS | 57/859/RVC |

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

This publication 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 publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

• transformed into an International standard,

• reconfirmed,

• withdrawn,

• replaced by a revised edition, or

• amended.

A bilingual version of this publication may be issued at a later date.

# Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850. This specification 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 61850-9-2 | 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 electrical substations related to IEDs |

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

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

# 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 (all parts)~~ | *~~Communication networks and systems in substations~~* |
| IEC 61850-6:2017 | *Communication networks and systems* for power utility automation *– Part 6: Configuration description language for communication in electrical substations related to IEDs* |
| IEC 61850-7-3:2017 | *Communication networks and systems* for power utility automation *– Part 7-3: Basic Communication structure – Common Data Classes* |
| IEC 61850-8-1:2017 | *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 61850-9-1~~ | *~~Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link~~*  *Reason for removal: 61850 ED 2.1 has removed unicast SV.* |
| IEC 61850-9-2:2017 | *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* |
| ~~ISO 9506 (all parts)~~ | *~~Industrial automation systems – Manufacturing Message Specification~~*  *Reason for removal: Intend to remove all references to ISO 9506 and use references/nomenclature for 62351-4, IEC 61850-8-1, and IEC 61850-8-2.* |
| IEC 62351-4:2017 | *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS* |
| *IED 62351-9:2017* | *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management* |
| ~~ISO/IEC 8802-3~~ | *~~Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications~~*  *Reason for removal: Intend to remove all references to it and use references/nomenclature for 62351-4, IEC 61850-8-1, and IEC 61850-8-2* |
| ISO/IEC 13239 | *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures* |
| ~~IEEE Std. 802.1Q-2012~~ | *~~Virtual Bridged Local Area Networks~~*  *Reason for removal: Intend to remove all references to it and use references/nomenclature for 62351-4, IEC 61850-8-1, and IEC 61850-8-2. Wrong reference anyway* |
| RFC 5208 | X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| RFC 5905 | Network Time Protocol Version 4: Protocol and Algorithms Specification.  Restricted to SNTP profile only. |
| RFC 2313 | PKCS #1: RSA Encryption Version 1.5 |
| RFC 3447 | *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.* |
| RFC 6234 | *US Secure Hash Algorithms (SHA and HMAC-SHA)* |

# Terms and definitions

|  |  |
| --- | --- |
| SCL | Substation Configuration Language |
| ICT | IED Configuration Tool |
| IED | Intelligent Electronic Device |

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

# Security issues addressed by this specification

## 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 4 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 SMV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this specification does define a mechanism for allowing confidentiality for applications where the 4 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 specification.

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

## Security threats countered

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

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

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

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

1. unauthorized access to information through message level authentication and encryption of the messages;
2. unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

## Attack methods countered

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

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

# Correlation of IEC 61850 parts and IEC 62351 parts

There are four levels of interaction between IEC 62351 parts and parts of IEC 61850. In particular, this part is concerned with the:

* Communication profile security regarding:
  + IEC 61850-8-1 Application Profile(s) 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
* 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 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 specification provides security specifications for use for internal to an Electronic Security Perimeter (ESP) and between ESPs.

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

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 A-Profile for Client/Server communications shall implement the ACSE Authentication mechanism and TLS as specified by IEC 62351-4.

It is optional to support the end-to-end application security layer as specified by IEC 62351-4. The Edition 2 of this standard shall make the support for end-to-end application level security mandatory.

### Additional cipher suite support

The following cipher suite shall be supported in addition to those specified in IEC 62351-4.

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

NOTE: This additional cipher suite is suggested in order to allow less CPU utilization when the communication environment is within a substation.

## IEC 61850-8-2 A-Profile for Client/Server communications

IEC 61850 implementations claiming conformance to this specification 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 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 cypher suites, specified in IEC 62351-4 are out-of-scope for IEC 61850-8-2.

### Additional cipher suite support

The following cipher suite shall be supported in addition to those specified in IEC 62351-4.

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

NOTE: This additional cipher suite is suggested in order to allow less CPU utilization when the communication environment is within a substation.

## 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 strong certificate based authentication and security provides a mechanism for providing authoritative information in regards to 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 will provide an additional Data Attribute to the IEC 61850-7-3 CDCs of: CST,BTS, UTS, LTS, GTS, MTS, NTS, and STS.

The Data Attribute shall be named certIssuer and will be of the Attribute Type Unicode255. The functional constraint shall be SR and the Data Attribute shall be added to the end of the current IEC 61850-7-3 tracking CDCs.

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. 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.

# Multicast Association Protocols

## 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 standard 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.

## 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.

### GOOSE replay protection

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

Implementations claiming conformance to this standard shall implement the state machine shown in Figure 1. Additional security and replay checks may be implemented.

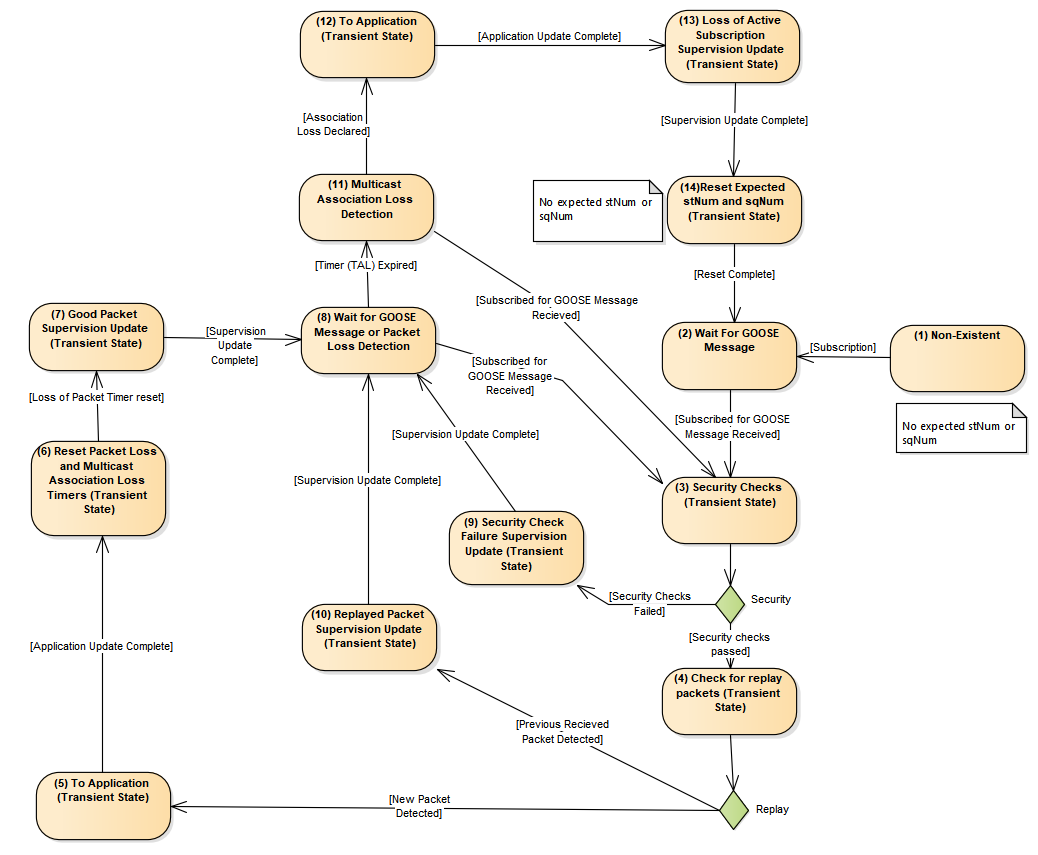


Figure 1: Replay Protection State Machine for GOOSE

Figure 1 is relevant for GOOSE messages for which the subscriber has an active subscription which may be manually configured or be configured through the use of SCL and an ICT. 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 (step 3).
3. The processing in the Security Checks state is described in clause 6.1.1.1.  
     
   If the security tests pass, the state machine shall transition to checking for replayed packets (Step 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 6.1.1.2.  
     
   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 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 update to the values decoded from the GOOSE packet.  
     
   The state shall transition to state 6.
6. The intTAL value shall be set 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 clause 6.1.1.3 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 clause 6.1.1.3 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 clause 6.1.1.3 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 and the expected stNum/sqNum shall be reset.  
      
    If a subscribed for GOOSE message 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. LGOS.St shall change state). See clause 6.1.1.3 for processing requirements.  
      
    Once the supervision information has been updated, a transition to state 14. No reset or setting of intTAL shall be performed.
14. The values lastRcvStNum , lastRcvSqNum, and lastRcvT shall be set to invalid and a transition to state 2 shall occur.

#### Security Check Protection Requirements

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

* The subscriber shall check if the AuthenticationValue (see 7.2.2.3) is expected.
  + If the AuthenticationValue is expected 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.

#### Check for Replay State Processing Requirements

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

* 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.
  + If there is a valid value for lastRcvT and lastRcvStNum:
    - 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 configured skew 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 skew period shall be configurable and shall support a maximum-minimum of 10 seconds. The maximum value allowed to be configured shall be 30 seconds. This value shall be configurable through SCL as part of the GOOSE subscription mechanism (see clause 9.1).
* 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:
    - lastRcvStNum shall be set to the value of stNum received in the GOOSE packet.
    - 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:
    - 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.
    - If the received stNum is less than lastRcvStNum this 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.

#### 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.

### Sampled Value replay protection

IEC 61850-9-2 does not detail how to transition should 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.

#### Publisher

In order to prevent SMV replay, the Security field of the SMV protocol shall be present (see Table 2).

Table 2 – Extract from IEC 61850-9-2 (informative)

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

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 SMV frame was formatted.

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

The resolution of the value shall be at least 250 usec.

#### Subscriber

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

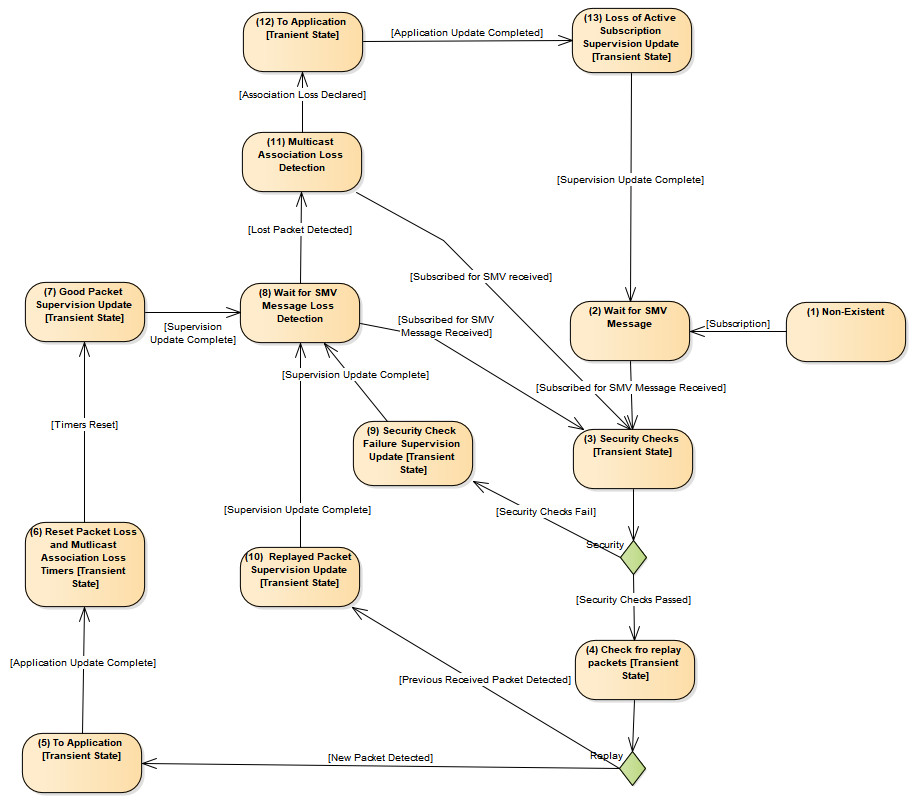


Figure 2: Replay Protection State Machine for SMV

Figure 2 is relevant for SMV messages for which the subscriber has an active subscription which may be manually configured or be configured through the use of SCL and an ICT. 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 SMV 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 SMV Message state.  
     
   Upon receiving the subscribed SMV message, the subscriber shall transition to the Security Checks state (step 3).
3. The processing in the Security Checks state is described in clause 6.2.2.2.1.  
     
   If the security tests pass, the state machine shall transition to checking for replayed packets (Step 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 6.2.2.2.2.  
     
   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 GOOSE packet. The decoded information shall be delivered to the Application.   
     
   The state shall transition to state 6.
6. The expNxtPkt value shall be set to the set 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 SMV APDU.  
     
   The value of expNxtPk is defined to be:  
     
    For smpMod = SmpPerSec:  
     
    expNxtPk = (nofASDU/smpRate) \* 2  
     
   For smpMod = SecPerSmp:  
     
    expNxtPk = smpRate \* nofASDU \* 2  
     
   For smpMod=SmpPerPeriod:  
     
    expNxtPk = ((nofASDU/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 clause 6.2.1.3 for processing requirements.  
     
   Once the supervision information has been updated, a transition to state 8.
8. If subscribed for SMV packet is received, the state shall transition to state 3.  
     
   The local multicast association loss detection timer shall be started. 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 6.2.2.2.3 for processing requirements.  
     
   Once the supervision information has been updated, a transition to state 8.
10. The supervision information shall be updated based upon the replay detection information. See clause 6.2.2.2.3 for processing requirements.  
      
    Once the supervision information has been updated, a transition to state 8.
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.  
      
    If a subscribed for SMV message 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 6.2.2.2.3 for processing requirements.

##### Security Check Protection Requirements

This clause specifies the processing required for checking SMV security parameters.

* The subscriber shall check if the AuthenticationValue (see 7.2.2.3) is expected.
  + If the AuthenticationValue is expected 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.

##### Check for Replay State Processing Requirements

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

* The subscriber shall check the security 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 the security timestamp received in the SMV message.

##### 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.

# 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 standard whall implement the RFC 5905 profile for SNTP including mandatory use of the authentication algorithms.

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

## Overview of Ethertype (informative)

This specification extends the normal Layer IEC 61850 GOOSE and Layer 2 IEC 61850-9-2 Sampled Measured Value PDUs. ~~The outline of a PDU for GSE Management and GOOSE is given in Annex C of IEC 61850-8-1~~.

## Extended PDU

### General format of extended PDU

| Octets | | | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | | Ether-type  PDU |  | Ethertype | | | | | |  |
| 2 |  |  |  | | | | | |  |
| 3 |  | APPID | | | | | |  |
| 6 |  |  | | | | | |  |
| 5 |  | Length | | | | | |  |
| 6 |  |  | | | | | |  |
| 7 |  | Length of extension | | | | | |  |
| 8 |  | (formerly Reserved1) | | | | | |  |
| 9 |  | CRC of octets 1-8 | | | | | |  |
| 10 |  | (formerly Reserved2) | | | | | |  |
| 11 |  |  | | | | | |  |
| ... |  | GOOSE/SMV APDU | | | | | |  |
|  | |  |  |  | | | | | |  |
|  | |  |  | Extension | | | | | |  |
|  | |  |  |  | | | | | |  |
| m-2 | |  |  |  | | | | | |  |

*IEC 1053/07*

Figure 3 – General format of extended PDU

Figure 3 depicts the fact that the Layer 2 IEC 61850 GOOSE and MSV fields of Reserved1 and Reserved2 fields were reserved for the purposes of security. This part specifies that the fields shall be utilized as follows:

* **Reserved1 field** shall be used to specify the number of octets conveyed by the extension octets. This value shall be contained in the first octet of the Reserved1 field. The valid range of values is zero (0) through 255. A value of zero (0) shall indicate that no extension octets are present.

The second octet of the Reserved1 field shall be reserved for future use;

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

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

### Format of extension octets

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 SEQUENCE AuthenticationValue 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.

#### &AuthenticationValue Algorithm

AuthenticationValue ::= {  
 [0] IMPLICIT INTEGER Version,  
 [1] IMPLICIT INTEGER TimeofCurrentKey,  
 [2] IMPLICIT INTEGER TimeofNextKey,  
 [3] IMPLICIT OCTETSTRING InitializationVector OPTIONAL,  
 [4] IMPLICIT INTEGER KeyID,  
 [5] IMPLICIT OCTETSTRING mAC,  
 …,  
 }

##### &Version

The Version attribute shall contain the extension protocol version number as specified by this document. The attribute value shall be an Unsigned Integer Value.

The value assigned for the Version shall be: 1.

##### &TimeofCurrentKey

The TimeofCurrentKey attribute 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 shall not be adjusted for leap seconds.

NOTE SecondSinceEpoch corresponds with the Unix epoch.

Some operating systems have a 32-bit Unsigned 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.

##### &TimetoNextKey

The TimetoNextKey attribute shall be an Signed Integer value. The value of the attribute represents the number of seconds prior to a new key being used. If the Most Significant Bit is a value of one (1), representing a negative value, shall be used 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 minutes prior to the new key being placed into service.

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.

##### &InitializationVector

The InitializationVector field 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 PDU basis and shall be used for both encryption and MAC generation.

##### &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 User Data that contains payloads containing multiple DataSets, the Key ID shall be one of the Key IDs of the DataSets contained. Once the DataSet selection is made locally, the selected DataSet shall not be changed.
* For MNGT payloads, the Key ID shall be the value assigned to the DataSet provided by the KDC.

### &mAC

The calculated HMAC value shall be used for the authentication/integrity of the octets that starts with the Ethertype Identifier for GOOSE or SMV through the end of the GOOSE/SMV APDU. The HMAC calculations shall not include the hMAC production. The value of the parameter shall be calculated based upon the HMAC algorithm in RFC 2104.

The value of the HMAC and Signature production shall be treated as ASN.1 OCTETString values.

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

Additionally, the calculated MAC value may be truncated, per RFC 2104. The allowed truncations are 80, 128, and 256 bits.

Therefore, the HMAC enumerated values, used in the Security Algorithm field (see **Error! Reference source not found.**) shall be as defined in Table 3.

Table 3 – Allowed values for MAC signature value calculations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Enumerate Value | HMAC Algorithm | Number of bits | Designation | Mandatory (m), Optional (o) |
| 0 | None | None | MAC-None | c1 |
| 1 | SHA-256 | 80 | HMAC-SHA256-80 | m |
| 2 | SHA-256 | 128 | HMAC-SHA256-128 | m |
| 3 | SHA-256 | 256 | HMAC-SHA256-256 | m |
| 4 | AES-GMAC | 64 | AES-GMAC-64 | m |
| 5 | AES-GMAC | 128 | AES-GMAC-128 | m |
| c1 – Shall only be used when encryption is also in use. | | | | |

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

When a truncated value is used, the leftmost bytes of the computed value shall be used as the value known as a Message Authentication Code (MAC). 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 (<http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>).

The action due to detection of a invalid signature being received is a local issue. 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.

#### Requirements on publishers

Servers shall perform the algorithm as previously specified. If the publisher is not providing the AuthenticationValue, the AuthenticationValue shall not be present in the Extension octets.

Additionally, implementations that use the AuthenticationValue shall provide a public X,509 certificate for installation on the receiving clients.

#### Requirements on subscribers

The subscriber must have a local means of referencing the Source MAC Address to the AES 128 bit public Key provided by the server.

NOTE  It is recommended that the actual certificate be stored for this purpose, although it is not a requirement.

If there is no reference, then security extensions/processing should not occur.

Upon layer 2 GOOSE or SMV message, where security extension are configured:

* the receiving client shall calculate the AuthenticationValue for the APDU as specified in clause 8.2.2.1;
* the Reserved octets shall be decrypted by using the appropriate key and algorithm (reverse of clause 8.2.2.1);
* if the the signature verification succeeds, then the client should proceed with the processing of the APDU.

# Substation configuration language extensions

## Skew configuration

In many situations, the time skew for replay detection is dependent upon the characteristics of the transmission path latencies. As such the actual configuration of this information is a System Configuration Tool and communication configuration issue.

Implementations claiming conformance to this standard shall be able to have the skew configured on a per subscription basis for either GOOSE or SMV.

Both the GOOSE and SMV control blocks utilize the tControlWithIEDName production to indicate which IEDs (e.g. subscribers) should subscribe for the particular GOOSE or SMV. Communication paths from the publisher to subscribers may vary. Therefore skew values shall be specified on an individual IED subscription basis.



The attribute “skew” shall be added to the tControlWithIEDName production as optional. It shall contain the number of seconds to allow for skew detection for replay protection. The maximum value allowed to be configured is 30 seconds.

## SCL certificate extension

SCL shall be extended to include the following to allow definition of certificates that are to be used.

<xs:complexType name="tCertificate">  
 <xs:complexContent>  
 <xs:extension base="tNaming">  
 <xs:sequence>  
 <xs:element name="XferNumber" type="xs:unsignedInt" minOccurs="0" maxOccurs="1" />   
 <xs:element name="SerialNumber" type="xs:normalizedString" minOccurs="1" maxOccurs="1" />  
 <xs:element name="Subject" type="tcert" minOccurs="1" maxOccurs="1"/>  
 <xs:element name="IssuerName" type="tcert" minOccurs="1" maxOccurs="1"/>  
 </xs:sequence>  
 </xs:complexContent>  
</xs:complexType>  
  
<xs:complexType name="tcert">  
 <xs:complexContent>  
 <xs:extension base="tNaming">  
 <xs:sequence>  
 <xs:element name="CommonName" type="xs:normalizedString" minOccurs="1" maxOccurs="1" >   
 <xs:element name="IDHierarchy" type="xs:normalizedString" minOccurs="1" />  
 </xs:sequence>  
 </xs:complexContent>  
</xs:complexType>

*IEC 1054/07*

Figure 4 – SCL extensions for certificates

### &XferNumber

This attribute shall be used to convey the number through which the sending IED shall refer to the certificate. The attribute value shall be present if the certificate is to be used for GOOSE or SMV. The valid range of values is 0 through 7.

### &SerialNumber

This attribute shall contain the serial number value of the certificate.

### &Subject

This complex type shall contain the identifying hierarchy of the certificate as present within the certificate for the Subject in the certificate.

### &IssuerName

This complex type shall contain the identifying hierarchy of the certificate as present within the certificate for the IssuerName in the certificate.

### &CommonName

This attribute shall contain the value of the CommonName as found within the certificate.

## Specification of AccessPoint security usage

<xs:complexType name="tAccessPoint">  
 <xs:complexContent>  
 <xs:extension base="tNaming">  
 <xs:choice minOccurs="0">  
 <xs:element name="Server" type="tServer">  
 <xs:unique name="uniqueAssociationInServer">  
 <xs:selector xpath="./scl:Association"/>  
 <xs:field xpath="@associationID"/>  
 </xs:unique>  
 </xs:element>  
 <xs:element ref="LN" maxOccurs="unbounded"/>  
 </xs:choice>  
 <xs:attribute name="router" type="xs:boolean" use="optional" default="false">  
 </xs:attribute>  
 <xs:attribute name="clock" type="xs:boolean" use="optional" default="false">  
 </xs:attribute>  
 <xs:element name="GOOSESecurity" type="tCertificate" use="optional" maxOccurs="7" >  
 <xs:element name="SMVSecurity" type="tCertificate" use="optional" maxOccurs="7" >  
 </xs:extension>  
 </xs:complexContent>  
</xs:complexType>

*IEC 1055/07*

Figure 5 – Extension to AccessPoint SCL definition

The AccessPoint SCL definition shall be extended to include GOOSESecurity and SMVSecurity for implementations claiming conformance to this specification a support for the appropriate security (e.g. GOOSE or SMV).

Implementations claiming to support Secure GOOSE shall have a minimum of one GOOSESecurity element present.

Implementations claiming to support Secure SMV shall have a minimum of one SMVSecurity element present.

Implementations claiming to support encryption, shall include the GOOSEEncryptioninUse or SMVEncryptioninUse attribute whose value(s) shall be the same as the XferNumber for the certificate intended to be used for both authentication and encryption.

# Conformance

## 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.

The information in Table 4 shall be provided for an implementation claiming support for this specification.

Editor’s Note: The PICS are not complete since rework of 62351-4 is required in order to complete.

Table 4 – Conformance table for IEC 61850 Security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Client** | | **Server** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| G1 | Support for IEC 61850-8-1 Client/Server security | o | AtLeastOne | o | AtLeastOne |  |
| G2 | Support for Layer 2 IEC 61850-8-1 Client/Server security | o | AtLeastOne | o | AtLeastOne |  |
| G3 | Support for SNTP Security | o |  | o |  |  |
|  |  | **Subscriber** | | **Publisher** | |  |
| G4 | Support for GOOSE security | o | AtLeastOne | o | AtLeastOne |  |
| G5 | Support for MSV security | o | AtLeastOne | o | AtLeastOne |  |
| AtLeastOne – At least one must be declared in order to claim conformance to this standard | | | | | | |

## Conformance for implementations claiming IEC 61850 Client/Server

The information in Table 5 shall be provided for implementations claiming support of the security profile for IEC 61850-8-1 Client/Server profile.

Table 5 – PICS for IEC 61850-8-1 Client/Server

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Client** | | **Server** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| CS811 | IEC 62351-4 ACSE Authentication | m |  | m |  |  |
| CS812 | TLS conformity - IEC 62351-4 section 2 | m |  | m |  |  |
| CS813 | AE+ conformity – 62351-4 section 5 | o |  | o |  | Is intended to be mandatory in Edition 2 of this standard. |
| CS814 | 62351-4 Mandatory Cipher Suite | m |  | m |  |  |
| CS815 | TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | m |  | m |  |  |
| CS816 | TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA256 | m |  | m |  |  |
|  | Tracking Services Supported | o |  | o |  |  |
|  | Control Services Supported | o |  | o |  |  |
|  | OriginatorID Supported | o | c1 |  | c2 |  |
|  | SCL Extension for OriginatorID | o | c1 | i | i |  |
| c1 –shall be ‘m’ if declaration for Client Tracking Services or Control Services is declared c2 – the support if declaration for Server Tracking Services or Control Services is declared | | | | | | |

Note: May need tables regarding mandatory cipher suites.

## Conformance for implementations claiming IEC 61850-8-2 Client/Server

The information in Table 6 shall be provided for implementations claiming support of the security profile for IEC 61850-8-2 Client/Server profile. IEC 61850-8-2 is inherently inter-ESP therefore there is only one PICS table provided.

Table 6 – PICS for IEC 61850-8-2 Client/Server

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Client** | | **Server** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| CS821 | AE+ conformity – 62351-4 section 5 | m |  | m |  | Is intended to be mandatory in Edition 2 of this standard. |
| CS822 | Mandatory Cipher Suite | m |  | m |  |  |
|  | Control Services Supported | o |  | o |  |  |
|  | OriginatorID Supported | o | c1 |  | c2 |  |
|  | SCL Extension for OriginatorID | o | c1 | i | i |  |
| c1 –shall be ‘m’ if declaration for Client Tracking Services or Control Services is declared c2 – the support if declaration for Server Tracking Services or Control Services is declared | | | | | | |

Once 62351-4 Conformance PICs for E2E security is fixed, place here.

## Conformance for implementations claiming GOOSE security

The information in Table 8 shall be provided for implementations claiming support of the security profile for the IEC 61850-8-1 GOOSE.

Table 7 – PICS for 61850-8-1 GOOSE security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| GSE1 | IEC 61850-8-1 Layer 2 GOOSE | o | AtLeastOne | o | AtLeastOne |  |
| GSE2 | IEC 61850-8-1 Routable GOOSE | o | AtLeastOne | o | AtLeastOne |  |
|  | SCL Skew Configuration (clause 9,2) | m |  | m |  |  |
|  | SCL Certificate Extension | m |  | m |  |  |

Table 8 – PICS for Layer 2 IEC 61850-8-1 GOOSE security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| SGO1 | IEC 61850-8-1 Layer 2 Security (clause 8.2) | m |  | m |  |  |
| SG02 | 62351-6 Replay Protection (clause 6.1.1) | m |  | m |  |  |

Table 9 – PICS for Routable IEC 61850-8-1 GOOSE security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| SGR1 | 62351-6 Replay Protection (clause 6.1.1) | m |  | m |  |  |

## Conformance for implementations claiming IEC 61850-8-1 MSV security

The information in Table 10 shall be provided for implementations claiming support of the security profile for the Layer 2 IEC 61850-8-1 MSV T-Profile.

Table 10 – PICS for Layer 2 IEC 61850MSV security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| GSV1 | IEC 61850-9-2 Layer 2 SV | o | AtLeastOne | o | AtLeastOne |  |
| GSV2 | IEC 61850-9-2 Routable SV | o | AtLeastOne | o | AtLeastOne |  |
|  | SCL Skew Configuration (clause 9,2) | m |  | m |  |  |
|  | SCL Certificate Extension | m |  | m |  |  |

Table 11 – PICS for Layer 2 IEC 61850-8-1 MSV security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| SV21 | IEC 61850-8-1 Layer 2 Security Extensions (clause 8.2) | m |  | m |  |  |
| SV22 | 62351-6 Replay Protection (clause 6.1.1) | m |  | m |  |  |

Table 12 – PICS for Routable IEC 61850-8-1 MSV security

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Subscriber** | | **Publisher** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| SVR1 | 62351-4 Replay Protection (clause 6.1.1) | m |  | m |  |  |

## Conformance for implementations claiming SNTP profile security

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

Table 6 – PICS for SNTP profiles

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Client** | | **Server** | | **Value/Comment** |
|  |  | f/s |  | f/s |  |  |
| SNTP1 | 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 2104,~~ *~~HMAC: Keyed-Hashing for Message Authentication~~*

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

~~RFC 3174,~~ *~~Secure Hash Algorithm (SHA1)~~*

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

\_\_\_\_\_\_\_\_\_\_\_