Security Test Cases

Contents

[Introduction 3](#_Toc492626504)

[Pre-conditions for the IOP 5](#_Toc492626505)

[IEC 62351-4 5](#_Toc492626506)

[Planning for Test Cases 6](#_Toc492626507)

[Planning for Test Cases 6](#_Toc492626508)

[Test Case Procedures 7](#_Toc492626509)

[Import of All Required CA Certificates (62351-4-1) 7](#_Toc492626510)

[Certificate Signing Request (62351-4-2) 7](#_Toc492626511)

[Support for Hierarchical Trust (62351-4-3) 7](#_Toc492626512)

[Import of Local Keys (62351-4-4) 8](#_Toc492626513)

[Import of Remote Certificates (62351-4-5) 8](#_Toc492626514)

[Import of Remote Certificates (62351-4-6) 8](#_Toc492626515)

[Application Authentication Only Testing (62351-4-7) 9](#_Toc492626516)

[Application Authentication and TLS Testing (62351-4-8) 9](#_Toc492626517)

[Ability to simultaneously support secure and non-secure associations (62351-4-9) 10](#_Toc492626518)

[Validation of behavior in the case of a certificate being revoked (62351-4-10) 10](#_Toc492626519)

[Connection behavior regarding non-configured certificate (62351-4-11) 11](#_Toc492626520)

[Removal of a Trusted CA Certificate (62351-4-12) 11](#_Toc492626521)

[OCSP revocation of a certificate (62351-4-13) 12](#_Toc492626522)

[OCSP validation of a certificate (62351-4-14) 12](#_Toc492626523)

[IEC 62351-6 12](#_Toc492626524)

[GOOSE replay protection 12](#_Toc492626525)

[Test Case Procedures 17](#_Toc492626526)

[GOOSE Replay (62351-6-1) 17](#_Toc492626527)

[Infrastructure Testing 18](#_Toc492626528)

[Firewall and ACL testing 18](#_Toc492626529)

[Syslog 18](#_Toc492626530)

[Test Case Procedures 19](#_Toc492626531)

[General Pre-conditions 19](#_Toc492626532)

[Normal Traffic Monitoring (Infrastruct-1, Syslog-1) 19](#_Toc492626533)

[Invalid Source IP Address (Infrastruct-2, Syslog-2) 19](#_Toc492626534)

[Invalid Source L2 GOOSE MAC Address (Infrastruct-3 , Syslog-3) 20](#_Toc492626535)

[Invalid Destination L2 GOOSE MAC Address (Infrastruct-4, Syslog-4) 20](#_Toc492626536)

[Invalid Source L2 GOOSE MAC Address (Infrastruct-5 , Syslog-5) 21](#_Toc492626537)

[Invalid Destination L2 GOOSE MAC Address (Infrastruct-6, Syslog-6) 21](#_Toc492626538)

[Detection of incorrect Port Number Access (Infrastruct-7, Syslog-7) 21](#_Toc492626539)

[Detection of incorrect Ethertype (Infrastruct-8, Syslog-8) 21](#_Toc492626540)

[DOS detection based upon no traffic (Infrastruct-9) 22](#_Toc492626541)

[Thoughts for Next IOP 23](#_Toc492626542)

[RBAC 23](#_Toc492626543)

[Encountered Standard Issues 24](#_Toc492626544)

[OCSP vs CRL use: 24](#_Toc492626545)

[Forms 25](#_Toc492626546)

[62351 Test Result Forms 25](#_Toc492626547)

[Infrastructure Forms 27](#_Toc492626548)

[PICS Form 27](#_Toc492626549)

[Test Result Form 29](#_Toc492626550)

# Introduction

In order to test IEC 61850-4 security, there are several types of certificates that need to be exchanged and used as the basis of the actual tests.

* Certificate Authority Certificate: “In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a **certificate authority** or **certification authority** (**CA**) is an entity that issues [digital certificates](https://en.wikipedia.org/wiki/Public_key_certificate). A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon [signatures](https://en.wikipedia.org/wiki/Digital_signature) or on assertions made about the private key that corresponds to the certified public key. A CA acts as a [trusted third party](https://en.wikipedia.org/wiki/Trusted_third_party)—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the [X.509](https://en.wikipedia.org/wiki/X.509) standard.” [From Wikipedia]
* TLS Certificates: These X.509 certificates are used to provide encrypted or protected transport layer messaging and are provided by a CA.
* Application Certificates: These X.509 certificates are used to provide authentication at the application layer. The next version of 62351-4 will also use this certificate to provide application level encryption and authentication, but this is out-of-scope of these tests.

“There are several commonly used filename extensions for X.509 certificates. Unfortunately, some of these extensions are also used for other data such as private keys.

* .pem – ([Privacy-enhanced Electronic Mail](https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail)) [Base64](https://en.wikipedia.org/wiki/Base64) encoded [DER](https://en.wikipedia.org/wiki/Distinguished_Encoding_Rules) certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
* .cer, .crt, .der – usually in binary [DER](https://en.wikipedia.org/wiki/Distinguished_Encoding_Rules) form, but Base64-encoded certificates are common too (see .pem above)
* .p7b, .p7c – [PKCS#7](https://en.wikipedia.org/wiki/PKCS7) SignedData structure without data, just certificate(s) or [CRL](https://en.wikipedia.org/wiki/Revocation_list)(s)
* .p12 – [PKCS#12](https://en.wikipedia.org/wiki/PKCS12), may contain certificate(s) (public) and [private keys](https://en.wikipedia.org/wiki/Private_key) (password protected)
* .pfx – PFX, predecessor of PKCS#12 (usually contains data in PKCS#12 format, e.g., with PFX files generated in [IIS](https://en.wikipedia.org/wiki/Internet_Information_Services))

[PKCS#7](https://en.wikipedia.org/wiki/PKCS7) is a standard for signing or encrypting (officially called "enveloping") data. Since the certificate is needed to verify signed data, it is possible to include them in the SignedData structure. A .P7C file is a degenerated SignedData structure, without any data to sign

[PKCS#12](https://en.wikipedia.org/wiki/PKCS12) evolved from the *personal information exchange* (PFX) standard and is used to exchange public and private objects in a single file.”. [From Wikipedia].

However, there are three types of objects that are exchanged:

1. Public CA root certificate (and any intermediate certificates – Note 1)
2. Public Server or Client “end entity” certificate issued (signed) by the CA root certificate (Note 1)
3. An out-of-band Private Key corresponding to the Client or Server certificate in 2. (Note 2)

All of these objects can be transported in one PKCS12 container (P12 file).

If private keys must be exchanged (Note 2), then only the PKCS12 format (P12 file) shall be used. This provides more protection for private keys, because the PKCS12 container (file) can be encrypted with a password. Although Private keys can also be transported in a PEM file, the PEM file format shall not be used because PEM does not support encryption of the contents and therefore increases the risk of loss or theft of the private key.

Notes:

1.      There may be one or more “Intermediate” certificates in the chain between the Client or Server “End entity” certificate and the Public CA root certificate. The server will also need these intermediate certificates.

2.      In a perfect world, with good security the private key is never exchanged. Instead the private key is generated on the device that needs a certificate, and the device supports “PKI enrolment”. In PKI enrolment, the device sends a certificate signing request (CSR) to a Certificate Authority for signing. The Certificate Authority authenticates the CSR, and signs the request. The result is a signed certificate that is sent back to the requesting device.

The signed certificate corresponds to the private key generated on the device.

However many devices today do not support PKI enrolment, or we may not have a tool that can act as a CA and sign CSRs.

Without PKI enrolment, we need to generate the device private key somewhere else, and exchange/transport the private key and associated certificate to the device. This process is associated with the significant risk of the private key being compromised (lost or stolen) in transit, even if the private key is transported in a PKCS12 file encrypted with a password.

 Exchanges between utilities (e.g. owners of the clients and servers) would be Public certificates (e.g. TLS, Application, and CA certificates). Exchanges from a CA to utilities would be of the Public CA Certificate and at a minimum the Private certificate and typically also a Public certificate.

For the IOP, it will be assumed to validate certificate exchanges between utilities/endpoints and not CA to utility since some manipulation may be required for the CA to utility exchange and CAs should supply certificates in a format that the utility can utilized. The IOP will also assume that there will be multiple CAs being utilized by different endpoints.

# Pre-conditions for the IOP

Each participant will provide the following certificates for exchange to other endpoints:

* At least one CA Public certificate that does not expire during the IOP. The name of this certificate filenames shall be: <CA Name>\_Public.<extension>
* At least two Application Level certificates and two TLS certificates OR two combined certificates (e.g. used for both TLS and Application) that do not expire during the IOP. The reason for two is that one will be revoked as part of a test and there will need to be a replacement certificate provided. The certificate filenames will be named as follows:

<Company>\_<IEDNAME>\_<APP, TLS, COMBINED><\_Revoke >.extension

Where:

Company: Name of the end-user company
IEDName: IEC 61850 IED Name.
APP: Indicates application level certificate.
TLS: Indicates TLS level certificate
COMBINED: indicates that the certificate is to be used for both application and TLS levels.
\_Revoke: This is an indication if a CRL is being provided that includes this certificate
* A Certificate Revocation List (CRL) that contains the \_Revoke certificate.

# IEC 62351-4

The following table summarizes the test cases to be performed.

|  |  |
| --- | --- |
| Test Case | Description |
|  | Import of all required local CA Certificates |
|  | Certificate Signing Request – Maryam (Siemens) to develop test case and bring tooling for execution. – Deferred until next IOP. |
|  | CA hierarchical trust – will require certificates to be generated prior to the IOP |
|  | Import of all Private Keys and associated certificates (e.g. local endpoint) |
|  | Import of all remote CA Certificates |
|  | Import of a certificate that has been previously revoked |
|  | Connection establishment using Application authentication only |
|  | Connection establishment using Application and TLS authentication only |
|  | Connection establishment using non-secure connection in parallel to secure connection |
|  | Behavior after revocation list is applied |
|  | Use of a certificate/key that is signed by a CA (e.g. imported) that is not present in the cache. |
|  | Removal of Trusted CA certificate from local cache. |
|  | OSCP revocation of a certificate – Herb to research bringing an OCSP server and test cases. |
|  | OSCP validation of a certificate - Herb to research bringing an OCSP server and test cases. |
|  | ~~CRL revocation of a certificate that is in use.~~ It was moved into 62351-10 |

## Planning for Test Cases

### Planning for Test Cases

Many of these test cases require several different sets of certificates to be prepared and available from EACH participating entity. The purpose of this section is to allow participants to plan and generate the required certificates and CRLs in advance.

Each participant MUST bring the following:

* The CA certificate of the CA used to generate the certificates that are to be exchanged by the participant.
* One certificate that will not be on a revocation list (GOOD Certificate). If there are separate certificates required for TLS and ACSE, then two certificates shall be available.
* One certificate that will not be on a revocation list and will not be imported by the peer (NOT-IMPORTED-GOOD certificate). This certificate shall include a subject that is used in its other certificates.
* At least one certificate that is to be included on a CRL (PREVIOUSLY-REVOKED Certificate). It should be noted that the revocation test will result in these certificates no longer being able to be used between two peers.
* At least one certificate that is to be included on a CRL (TO-BE-REVOKED Certificate). It should be noted that the revocation test will result in these certificates no longer being able to be used between two peers.
* At least one certificate that is signed by the CA, but is not to be exchanged with the peers out-of-band (NON-EXCHANGED certificate).
* A CRL that contains the PREVIOUSLY-REVOKED Certificate. This CRL shall not contain the TO-BE-REVOKED certificate.
* A different CRL that includes the TO-BE-REVOKED certificate.

Additionally, the following need to be provided by somebody participating or witnessing the tests:

* A CA certificate that will be used to create a hierarchical chain of CAs and a Certificate that utilizes that chain.

## Test Case Procedures

### Import of All Required CA Certificates (62351-4-1)

Purpose: To prove that an implementation can import CA certificates from more than one CA.

Procedure:

1. The CA certificates used by the various participating vendors shall be provided to the participant.
2. The participant, being witnessed, will import the certificates and show that the certificates have been successfully imported. If successfully imported, this shall be a “pass”.

### Certificate Signing Request (62351-4-2)

### Support for Hierarchical Trust (62351-4-3)

Purpose: To prove that an implementation can hierarchical trust.

Precondition: A participating vendor will need to prepare a hierarchical trust chain for a CA and use this hierarchy for its exchanges.

Procedure:

1. The CA certificates used by the vendor shall be provided to the participant.
2. The participant, being witnessed, will import the certificates and show that the certificates have been successfully imported. If successfully imported, this shall be a “pass”.

### Import of Local Keys (62351-4-4)

Purpose: To prove that an implementation can import private keys and associated certificates.

Precondition: A participating vendor will need to have previously imported CA certificate used to sign the certificate.

Procedure:

1. Import the private key and the associated certificate.
2. The participant, being witnessed, will import the certificate and key and show that the certificate has been successfully imported. If successfully imported, this shall be a “pass”.

### Import of Remote Certificates (62351-4-5)

Purpose: To prove that an implementation can import other vendor’s public certificates.

Precondition: A participating vendor will need to have previously imported the vendor’s CA certificate used to sign the certificate being provided.

Procedure:

1. Import the public certificate.
2. The participant, being witnessed will show that the certificate has been successfully imported. If successfully imported, this shall be a “pass”.

### Import of Remote Certificates (62351-4-6)

Purpose: To prove that an implementation rejects an import of a previously revoked certificate.

Precondition: A participating vendor will need to have previously imported the CA certificate used to sign the certificate being provided.

Procedure:

1. Import or apply a CRL for containing the PREVIOUSLY-REVOKED certificate that is to be imported.
2. Attempt to import the PREVIOUSLY-REVOKED certificate.
3. The participant, being witnessed will show that the certificate has not been successfully imported and/or is marked as revoked and/or is shown to be on a local CRL list.

### Application Authentication Only Testing (62351-4-7)

Purpose: To prove that an implementation can perform strong authentication based upon the remote peer’s ACSE public certificate.

Precondition: A participating vendor will need to have previously imported the CA and public certificate used by the remote peer. Appropriate configuration to perform strong authentication by both peers will need to be performed.

Procedure:

1. Calling Node (Client) attempts to establish an association with the peer (Server).
2. Association between the peers should occur.
3. Demonstration of information flow between the client and the server shall be demonstrated.

### Application Authentication and TLS Testing (62351-4-8)

Purpose: To prove that an implementation can perform strong authentication based upon the remote peer’s ACSE public certificate and encrypts the connection.

Precondition: A participating vendor will need to have previously imported the CA and public certificate used by the remote peer. Appropriate configuration to perform strong authentication by both peers will need to be performed.

It is also recommended that a network analyzer be available so that the use of encryption can be verified.

Procedure:

1. Calling Node (Client) attempts to establish an association with the peer (Server).
2. Association between the peers should occur.
3. Demonstration of information flow between the client and the server shall be demonstrated.
4. Verification that encryption is occurring is required in order to pass.

### Ability to simultaneously support secure and non-secure associations (62351-4-9)

Purpose: To prove that an application can support secure and non-secure communications simultaneously.

Precondition: A participating vendor will need to have previously imported the CA and public certificate used by the remote peer. Appropriate configuration to perform strong authentication by both peers will need to be performed. 62351-8 should be performed previously so that a secure connection is present.

.

Procedure:

1. Calling Node (Client) attempts to establish an association with the peer (Server) using a non-authenticated and non-encrypted connection.
2. Association between the peers should occur.
3. Demonstration of information flow between the client and the server shall be demonstrated over the secure and non-secure connection is required.

### Validation of behavior in the case of a certificate being revoked (62351-4-10)

Purpose: To prove that an application will properly disconnect if a certificate that is in use is revoked.

Precondition: A participating vendor will need to have previously imported the CA and public TO-BE-REVOKED certificate used by the remote peer. Appropriate configuration to perform strong authentication by both peers will need to be performed. 62351-8 should be performed previously so that a secure connection is present. The connection shall use the TO-BE-REVOKED certificates.

Procedure:

1. A CRL containing the Client’s TO-BE-REVOKED certificate should be applied to the Server.
2. The expected behavior is that the server should abort the connection.
3. Client should establish another secure connection to the server using a non-revoked certificate but the TO-BE-REVOKED certificate of the server.
4. A CRL should be applied to the Client indicating that the TO-BE-REVOKED certificate being used by the server has been revoked.
5. The expected behavior is that the Client should abort the connection.

### Connection behavior regarding non-configured certificate (62351-4-11)

Purpose: To prove that an application will behave properly if a certificate signed by an imported CA is utilized in an exchange but has not been previously imported.

Precondition: A participating vendor will need to have previously imported the CA.
.

Procedure:

1. The Client shall attempt to establish a connection to the server using the NOT-IMPORTED-GOOD certificate.
2. The expected behavior is that the server should declare the expected behavior. The expected behavior is that the connection should occur.

### Removal of a Trusted CA Certificate (62351-4-12)

Purpose: To prove that an application will behave properly if a certificate signed by an imported CA is utilized in an exchange where the CA certificate has been removed/revoked.

Precondition: A participating vendor will need to have previously imported the CA and GOOD certificates.

Procedure:

1. Establish a connection between the client and server. The connection should be established.
2. Disconnect between the client and server.
3. Remove the Client’s CA in the Server cache. A reboot should not be required.
4. Attempt to re-establish the connection. The connection should be refused.
5. Add the Client’s CA back into the server.
6. Establish a connection between the client and server. The connection should be established.
7. Disconnect between the client and server.
8. Remove the server’s CA in the client.
9. Attempt to re-establish the connection. The connection should be refused by the client.
10. Add the Client’s CA back into the server.
11. Establish a connection between the client and server. The connection should be established.

### OCSP revocation of a certificate (62351-4-13)

### OCSP validation of a certificate (62351-4-14)

# IEC 62351-6

The following table summarizes the test cases to be performed.

|  |  |
| --- | --- |
| Test Case | Description |
|  | Reaction to GOOSE Replay |

The next edition of IEC 62351-6 is specifying a state machine to minimize the issue of replay with L2 GOOSE. The current state is shown on page 12.

## 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 0.

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 0.

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 0 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 0 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 0 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 0 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 **Error! Reference source not found.**).
* 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.

## Test Case Procedures

### GOOSE Replay (62351-6-1)

Purpose: To observe the behavior of implementations based upon GOOSE replay. This is a network disruptive test and therefore, more than just security participants may be impacted.

Precondition: A PCAP of the GOOSE network traffic from 5 minutes previous. A switch port will also need to be configured to take untagged traffic and promote it to the appropriate integrated application VLAN ID.

Procedure:

1. Make sure that the integrated application is executing properly.
2. Play the PCAP and observe the behavior of the application.

Properly protected devices should continue to operate on the non-playback data.

# Infrastructure Testing

## Firewall and ACL testing

|  |  |
| --- | --- |
| Test Case | Description |
|  | Normal traffic generating no ACL alerts |
|  | Invalid Client Source IP address from Control Center to Substations |
|  | Invalid L2 GOOSE source address from Substation to Substation |
|  | Invalid L2 GOOSE destination address from Substation to Substation |
|  | Invalid L2 GOOSE source address from Substation to Control Center |
|  | Invalid L2 GOOSE destination address from Substation to Control Center |
|  | Incorrect Port Number access  |
|  | Invalid Ethernet Ethertype (e.g. non-GOOSE) |
|  | No Traffic on port (DOS test) |

## Syslog

|  |  |
| --- | --- |
| Test Case | Description |
|  | Firewall and ACL normal traffic generating no ACL alerts (execute as part of Infrastructure-1) |
|  | Firewall and ACL invalid Source address from Control Center to Substations (execute as part of Infrastructure-2) |
|  | Firewall and ACL invalid L2 GOOSE source address from Substation to Substation (execute as part of Infrastructure-3) |
|  | Firewall and ACL invalid L2 GOOSE destination address from Substation to Substation (execute as part of Infrastructure-4) |
|  | Firewall and ACL invalid L2 GOOSE source address from Substation to Control Center (execute as part of Infrastructure-5) |
|  | Firewall and ACL invalid L2 GOOSE destination address from Substation to Control Center (execute as part of Infrastructure-6) |
|  | Firewall and ACL detection of invalid port number. |
|  | Firewall and ACL detection of invalid Ethertype |

## Test Case Procedures

### General Pre-conditions

Infrastructure components that are to be tested need to be configured with the following set of information. The configuration is constrained to what the component can actually be configured to support. Therefore, not the entire following configuration is required to participate in the testing.

* Configuration of ACLs for Source and Destination IP addresses is configured
* Configuration of ACLs for Source and Destination L2 GOOSE address is configured.
* Ethertype for L2 GOOSE is configured.

### Normal Traffic Monitoring (Infrastruct-1, Syslog-1)

Purpose: To prove that there are no false triggers based upon normal traffic and application patterns.

Procedure:

1. The infrastructure component will be monitored via Syslog or other means to make sure that no traffic has been disrupted/dropped due to ACL or filtering rule configuration. Monitoring shall be for 20-minutes.

If the infrastructure component supports Syslog, Syslog-1 may be passed if the Unit Under Test can be proved to send information to Syslog even if it contains false triggers.

### Invalid Source IP Address (Infrastruct-2, Syslog-2)

Purpose: To prove that the Unit Under Test can detect and enunciate a filter/ACL violation based upon a non-configured source IP-Address.

Precondition: A 61850 Client will be configured with an un-assigned IP address.

Procedure:

1. Client will attempt to establish a non-secure MMS connection through the Unit Under Test.

Based upon the UUT PICs, the connection will fail (e.g. PICS indicates dropped packets).

If the infrastructure component supports Syslog, Syslog-2 may be passed if the Unit Under Test can be proved to send information to Syslog indicating the violation.

### Invalid Source L2 GOOSE MAC Address (Infrastruct-3 , Syslog-3)

Purpose: To prove that the Unit Under Test can detect and enunciate a filter/ACL violation based upon a non-configured source MAC Address.

Precondition: A GOOSE Publisher, whose configuration information has NOT been configured in the UUT. The GOOSE publisher will be configured to publish to a destination address that the UUT has been configured to allow.

Procedure:

1. Publisher will begin publishing.

Based upon the UUT PICs, the packets must not traverse the UUT.

If the infrastructure component supports Syslog, Syslog-3 may be passed if the Unit Under Test can be proved to send information to Syslog indicating the violation .

### Invalid Destination L2 GOOSE MAC Address (Infrastruct-4, Syslog-4)

Purpose: To prove that the Unit Under Test can detect and enunciate a filter/ACL violation based upon a non-configured destination MAC Address.

Precondition: A GOOSE Publisher, will be configured to send a GOOSE to an unexpected destination which has NOT been configured in the UUT. The GOOSE publisher will be configured to publish from a source address that the UUT has been configured to allow.

Procedure:

1. Publisher will begin publishing.

Based upon the UUT PICs, the packets must not traverse the UUT.

If the infrastructure component supports Syslog, Syslog-3 may be passed if the Unit Under Test can be proved to send information to Syslog indicating the violation.

### Invalid Source L2 GOOSE MAC Address (Infrastruct-5 , Syslog-5)

This is the same test procedure as Infrastruct-3, but for infrastructure components in a different Integrated Application location.

### Invalid Destination L2 GOOSE MAC Address (Infrastruct-6, Syslog-6)

This is the same test procedure as Infrastruct-4 , but for infrastructure components in a different Integrated Application location.

### Detection of incorrect Port Number Access (Infrastruct-7, Syslog-7)

Purpose: To prove that the Unit Under Test can detect and enunciate an attempt of a IEC 61850 Client connection to the incorrect port (e.g. not 102 or 3782).

Precondition: Telnet client will be used on a node whose IP address has been configured to be allowed to pass through the UUT. A node on the other side of the UUT must have a “TCP-Listen” posted for the port that is to be used by the Telnet client.

Procedure:

1. Telnet client is used to establish a connection using non-configured port to a destination IP address that is on a white list in the UUT and that has the TCP-Listen posted.

The UUT is expected to block and enunciate the connection attempt. If the Telnet client succeeds in connecting, this represents a failure.

### Detection of incorrect Ethertype (Infrastruct-8, Syslog-8)

Purpose: To prove that the Unit Under Test can detect and enunciate a filter/ACL violation based upon a non-configured Ethertype.

Precondition: A GOOSE Publisher, will be configured to send a GOOSE to an allowed destination which. The GOOSE publisher will be configured to publish from to a non-configured Ethertype.

Procedure:

1. Publisher will begin publishing.

Based upon the UUT PICs, the packets must not traverse the UUT.

### DOS detection based upon no traffic (Infrastruct-9)

Purpose: To determine if the UUT can assist in preventing DOS attacks.

Precondition: Telnet client will be used on a node whose IP address has been configured to be allowed to pass through the UUT. The node on which the Telnet client is executed MUST not have the TCP KEEPALIVE set to less than 5 minutes.

Procedure:

1. Telnet client is used to establish a connection using port 102 to a destination IP address that is on a white list in the UUT and that has the TCP-Listen posted.

The UUT would be expected to allow the connection to occur.
2. Wait 5 minute (remember the TCP-KEEPALIVE is supposed to be set to 1 Minute) and determine if the Telnet connection has been terminated.

It would be expected if the UUT terminated the connection and enunciate the reason. The observer should record the time required for the UUT to terminate the connection.

## Thoughts for Next IOP

### RBAC

Verify IEC62351 Pull model

a.      Profile A



        Configure devices with LDAP server address and including public server certificate

        Add user in LDAP server, assign role to user, set initial password

        Configure password complexity in LDAP server

        User try to log in to a device --> User authenticate against LDAP (TLS)

        Pull user token from user certificate attribute

        Change password

        Add, Change, remove roles on that user

        Remove user in LDAP

        Verify the user has no access anymore

If ABB can’t supply LDAP server, will write up the test case, but won’t be able to execute. To positioned in the Control Center. Allow Roles to access one substation not the other (another use case).

# Encountered Standard Issues

## OCSP vs CRL use:

62351-3 clause 5.6.4.4 states the following:

“The management of the Certificate Revocation List (CRL) is a local implementation issue. Discussion of the management issues regarding CRLs can be found in IEC/TS 62351-1. Alternatively to local CRLs, OCSP may be used to check the revocation state of applied certificates. The application of OCSP is outlined in IEC/TS 62351-9.”

The end result is that it is unclear which the mandatory revocation mechanism and which is the optional mechanism. One of the mechanisms needs to be mandatory otherwise interoperability/deployment issues will occur in the field.

A majority of the security IOP group had thought that CRL was the mandatory mechanism.

# Forms

## 62351 Test Result Forms

|  |
| --- |
| Individual Company Tests |
| Company: |  |
| Product: |  |
| Witness: |  |
| Product Category | IED: | Firewall: | Other: |
| Test Case | Not Attempted | Pass | Fail | ProblemEncountered | Problem Number |
| 62351-4-1 |  |  |  |  |  |
| 62351-4-2 |  |  |  |  |  |
| 62351-4-3 |  |  |  |  |  |
| 62351-4-4 |  |  |  |  |  |
| 62351-4-5 |  |  |  |  |  |
| 62351-4-6 |  |  |  |  |  |
| 62351-4-11 |  |  |  |  |  |
| 62351-4-12 |  |  |  |  |  |
| 62351-4-13 |  |  |  |  |  |
| 62351-4-15 |  |  |  |  |  |
| 62351-4-16 |  |  |  |  |  |
| 62351-6-1 |  |  |  |  |  |
| Problems Encountered |
|  |  |
|  |  |

|  |
| --- |
| Paired Company Tests |
| Company 1: |  |
| Company 1 Product: |  |
| Company 2: |  |
| Company 2 Product: |  |
| Witness: |  |
| Product Category | IED: | Firewall: | Other: |
| Test Case | Not Attempted | Pass | Fail | ProblemEncountered | Problem Number |
| 62351-4-7 |  |  |  |  |  |
| 62351-4-8 |  |  |  |  |  |
| 62351-4-9 |  |  |  |  |  |
| 62351-4-10 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Problems Encountered |
|  |  |
|  |  |

## Infrastructure Forms

### PICS Form

| Infrastructure Equipment PICS |
| --- |
| Company: |  |
| Product: |  |
| Product Category | Firewall: | Switch: | Other: |
| IEC 61850 Client/Server Related Capabilities  |
|  |  |  |  |  |  |
| Source IP Address  | Black List: |  | White List: |  | Range Based: |  |
| Destination IP Address | Black List: |  | White List: |  | Range Based: |  |
| Port 102 Allowance |  |  | White List: |  | Available Rule: |  |
| Port 3782 Allowance |  |  | White List: |  | Available Rule: |  |
| Invalid Port Detection | Black List: |  | White List: |  | Inverse White List |  |
| Deep Packet Inspection Support for MMS |  |  |  |  |  |
| Syslog Support for Violations |  |  |  |  |  |
| Packets Dropped for Violations |  |  |  |  |  |
|  |  |  |  |  |  |
| IEC 61850 L2 GOOSE Related Capabilities |
| L2 Source Address | Black List: |  | White List: |  | GMRP: |  | Other: |  |
| L2 Dest Address | Black List: |  | White List: |  |  |  | Other: |  |
| EtherType 0x88B8 | Black List: |  | White List: |  | AvailableRule: |  |  |  |
| Incorrect EtherType | Black List: |  | White List: |  | Inverse White List: |  |  |  |
| Deep Packet Inspection for GOOSE |  |  |  |  |  |  |  |
| Syslog Support for Violations |  |  |  |  |  |  |  |
| Packets Dropped for Violations |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| IEC 61850 L2 SMV Related Capabilities |
|  |  |  |  |  |  |  |  |  |
| L2 Source Address | Black List: |  | White List: |  | GMRP: |  | Other: |  |
| L2 Dest Address | Black List: |  | White List: |  |  |  | Other: |  |
| EtherType 0x88BA | Black List: |  | White List: |  | AvailableRule: |  |  |  |
| Incorrect EtherType | Black List: |  | White List: |  | Inverse White List: |  |  |  |
| Deep Packet Inspection for SMV |  |  |  |  |  |  |  |
| Rated Packets/Second | 96,000 |  |  |  |  |  |  |
| Syslog Support for Violations |  |  |  |  |  |  |  |
| Packets Dropped for Violations |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Routable GOOSE and SMV |
| Source IP Address  | Black List: |  | White List: |  | Range Based: |  |  |  |
| Destination IP Address | Black List: |  | White List: |  | Range Based: |  |  |  |
| Port 102 Allowance |  |  | White List: |  | Available Rule: |  |  |  |
| Invalid Port Detection | Black List: |  | White List: |  | Inverse White List |  |  |  |
| IGMPv2 Supported |  |  |  |  |  |  |  |
| IGMPv3 Supported |  |  |  |  |  |  |  |
| Deep Packet Inspection for R-GOOSE |  |  |  |  |  |  |  |
| Deep Packet Inspection for R-SMV |  |  |  |  |  |  |  |
| Syslog Support for Violations |  |  |  |  |  |  |  |
| Packets Dropped for Violations |  |  |  |  |  |  |  |

### Test Result Form

|  |
| --- |
| Individual Company Tests |
| Company: |  |
| Product: |  |
| Witness: |  |
| Product Category | Firewall: | Switch: | Other: |
| Test Case | Not Attempted | Pass | Fail | ProblemEncountered | Problem Number |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Problems Encountered |
|  |  |
|  |  |