Security Test Cases

# 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 two types of certificates that are exchanged: Public and Private. 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.

# Test Cases

## 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. |
|  | 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 – Maryam and Bob |
|  | OSCP validation of a certificate - Maryam and Bob |
|  | CRL revocation of a certificate that is in use. |

## Firewall and ACL testing

Preconditions:

* Configuration of ACLs for Source and Destination IP addresses
* Configuration of ACLs for Source and Destimation L2 GOOSE address?

|  |  |
| --- | --- |
| 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 – Joel Greene |
|  | Invalid Ethernet Ethertype (e.g. non-GOOSE) |

## 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) |
|  |  |

Some others to think about:

GOOSE Replay

DOS detection through packet traffic MIB reading? Internal and External. Not looking at CIP compliance of switch.

## 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.

# Test Results Form