Security and Security Certificates for OpenADR systems

Content:

Background

In order to fulfill current security requirements and NIST Cyber Security guidelines, the OpenADR Alliance decided to implement server and client side digital certificates. This means that both the OpenADR Server (VTN) and the OpenADR Client (VEN) manufacturers need to purchase valid OpenADR-specific certificates to authenticate communication links. This provides a strong security mechanism for the transport layer. Common security mechanisms include RSA and ECC algorithms (details of these technologies are not relevant for this overview). RSA is commonly used but generally requires faster processors or longer calculation times to establish the connection. ECC is less common but has faster algorithms, hence it is better suited for embedded systems (less calculation time).

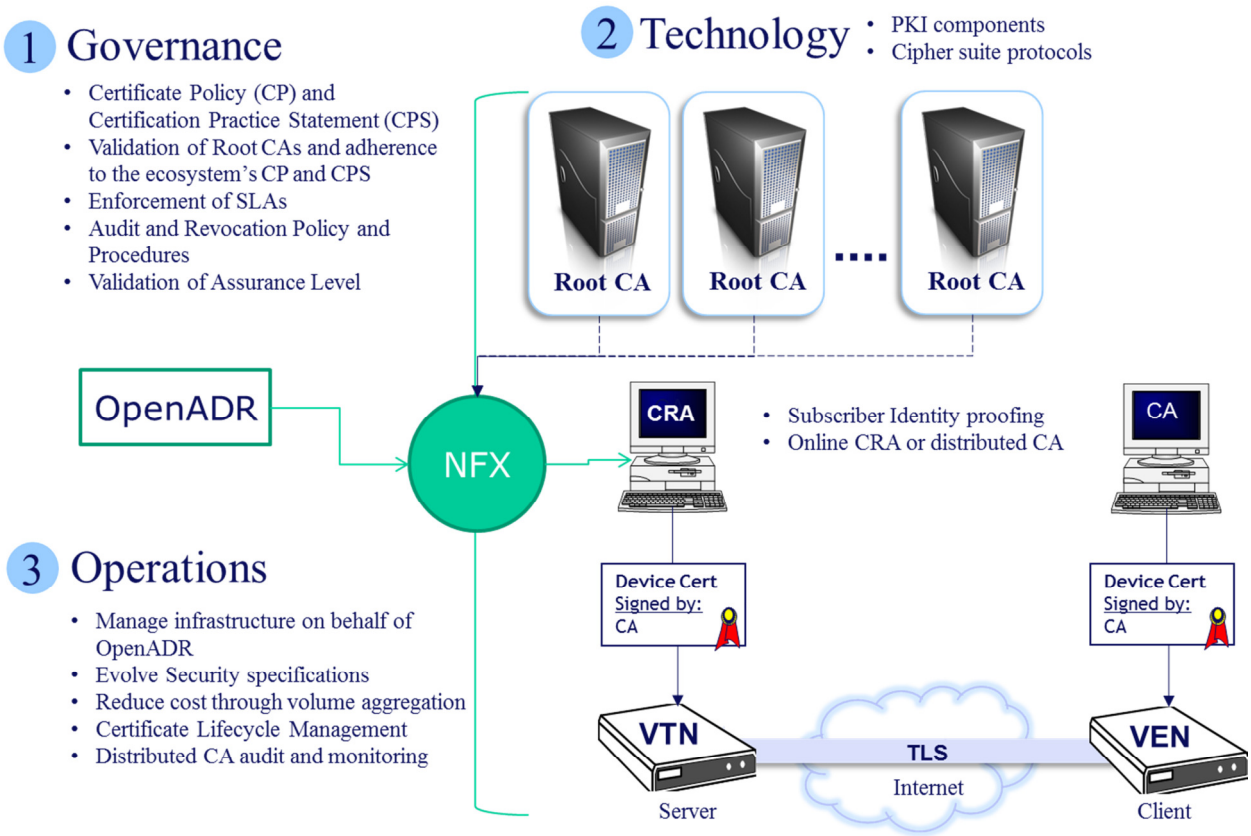
Another important requirement from the NIST recommendations is the certificate management. We have to have mechanisms in place that allow the control, authorization, issuance, and revocation of certificates in order to have a distinct 'paper' trail of the connection between manufacturer <–> client device <–> certificate.

NOTE: OpenADR Certification should not be confused with an OpenADR Digital Certificate. OpenADR Certification means that VTNs and VENs have undergone OpenADR testing and conform to the current OpenADR interface specification. Part of this testing also checks whether the systems can handle the minimum security requirements. Passing testing plus additional paperwork enables the systems to claim to be OpenADR Certified. A list of certified devices can be found here - http://www.openadr.org/products. This certification does **not** mean that the manufacturers have valid

Digital Certificates built into their systems yet. Manufacturers achieving OpenADR Certification need to obtain the Digital Certificates via the OpenADR/NetworkFX portal. NetworkFX partners with Symantec a well-known digital certificate service provider to handle the issuance of OpenADR Digital Certificates. Manufacturers can then embed the digital certificates into their certified products at time of manufacture.

Setup for OpenADR

Generally it is possible for anybody to set up a Certificate Authority (CA). However, this is connected to very strict audit requirements, a need to high security servers, web portals etc. There is also a large liability inherent to these CAs. Utilities, Program Operators, and Server vendors could choose to set up their own CAs to generate server and client Security Certificates. In order to maintain a high level of transparency across all OpenADR implementations, we however strongly recommend using the OpenADR/NetworkFX portal for Digital Certificates. This will assure that the Certificates all have the same signature elements and can be traced effectively in case of any security breaches. The OpenADR setup is sketched in the following figure.



By using this setup, we can maintain maximum control over the certificates and the systems.

Test-, Evaluation-, and Production Certificates

Different types of certificates are available to manufacturers depending on their development stage.

1. Test Security Certificates – These certificates are not valid for real communication. However, they can be used or free for testing purposes. They are also used during certification testing
2. Evaluation Certificates – These certificates are valid for real implementations. However, they are only valid for a limited time (60-90 days). These certificates could be used for further interoperability testing with existing live systems.
3. Production Certificates – These certificates have a longer validity period (20 years) and should be used for real implementations

OpenADR Certificates can be obtained through the OpenADR/NetworkFX portal:

http://www.networkfx.net/testcerts/

Responsibilities

The OpenADR Alliance and NetworkFX are working on making OpenADR specific certificates available to members of the OpenADR Alliance that have certified products. DR Program Operators may choose who is responsible for obtaining the Digital Certificates. Generally manufacturers of VTNs and VENs are responsible to obtain and implement Security Certificates.

Certificate Requesting Accounts

The OpenADR web-based Certificate Request Account (CRA) has the capability to issue digital certificates in bulk with very low attendant cost to Manufacturers throughout the certificate management lifecycle. The following diagram presents a high level view of the OpenADR CRA:

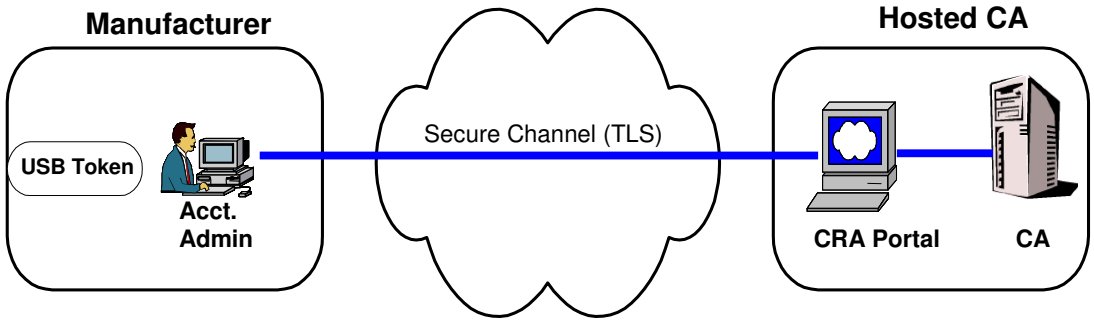


Figure 1: OpenADR CRA Architecture

In the OpenADR CRA architecture, the Manufacturer uses a standard web browser and hardware token (e.g., USB token for two factor authentication) to connect to the OpenADR CA's web interface. Via this interface, the Manufacturer may request VTN or VEN certificates and pick up batched signed certificates.

The CRA will not require any deployment at the Subscriber's site, other than the installation of the lightweight standalone client software needed to decrypt download file content. Therefore, immediate setup for a Manufacturer to request and receive device certificates is realized.

Figure 2 below illustrates the process for issuance of a CRA under the appropriate Root (RSA or ECC). The process consists of two sequences, Authorization and Issuance.

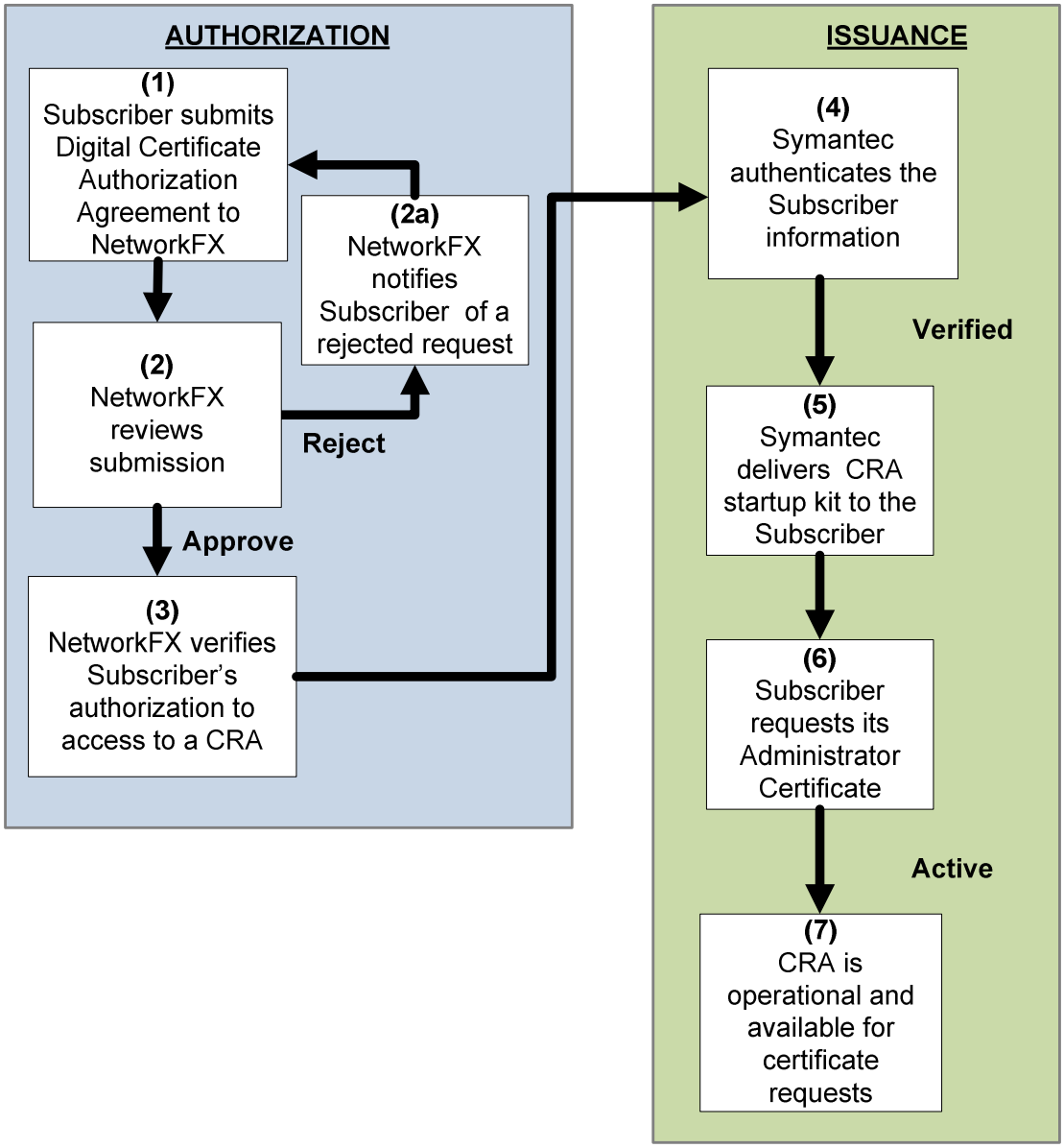


Figure 2: Manufacturer Authorization & Issuance Process

Authorization

Step 1	Manufacturers wishing to enroll in the Certificate Issuance service must execute an "Digital Certificate Authorization Agreement (DCAA)," including completion of the customer profile and naming document. Manufacturers must submit a signed DCAA to the Service Contact listed in Contact Information Section. The agreement can be sent via facsimile or email.

Step 2	NetworkFX will review the submission and either accept or reject it.

Step 2a	If the submission is rejected, NetworkFX will notify the Manufacturer and provide a reason for the rejection. The Manufacturer may resubmit the DCAA after the reason for rejection has been addressed.

Step 3	NetworkFX will verify with OpenADR Alliance that the Manufacturer is authorized to receive a CRA once NetworkFX has received an executed DCAA, a complete customer profile and naming document, and received payment for the first year's maintenance. NetworkFX notifies Symantec of vendors authorized to receive a CRA startup kit.

CRA Issuance

Step 4	Symantec will authenticate and verify the identity of the manufacturer as follows: First, Symantec will verify that the corporate and administrator contacts are, in fact, employees of the company; either by speaking with them or another verifier, i.e., receptionist. Delays may be caused if we are not able to reach the employee(s) or if a potential verifier will not, or cannot verify employment or if the manufacturer is located outside the US, there are sometimes delays with customs for the shipment of the CRA startup kit (mentioned below). Second, Symantec will look up the Dun and Bradstreet number to assure that the address and name of the company are the same as that under which they enrolled. (*A Dun and Bradstreet number is not required, but it can speed up the process). A delay may be caused if there are any discrepancies in the address information. In most instances, Verification and Authentication can be accomplished within 24-48 hours. However as stated above, some situations may occur that may cause delays.

Step 5	Symantec delivers the CRA startup kit (A blank hardware token (e.g., a USB token), software to use the token and instructions on how to request the Account Administrator certificate) to the Administrator(s) specified by the customer profile section of the DCAA.

Step 6	The manufacturer installs the token reader and drivers and is directed to an enrollment page that generates the private key and provisions the Account Administrator certificate onto the token. The Administrator Certificate will be used to authenticate the Administrator to the CA web interface and to upload certificate request files.

Step 7	The CRA system is now operational. The manufacturer's designated Administrator(s) may now request device certificate (see section 0).

Device Certificate requests via the CRA

Once the Manufacturer is enrolled for the CRA service, the Manufacturer's Administrator may request device certificates using the process described in this section.

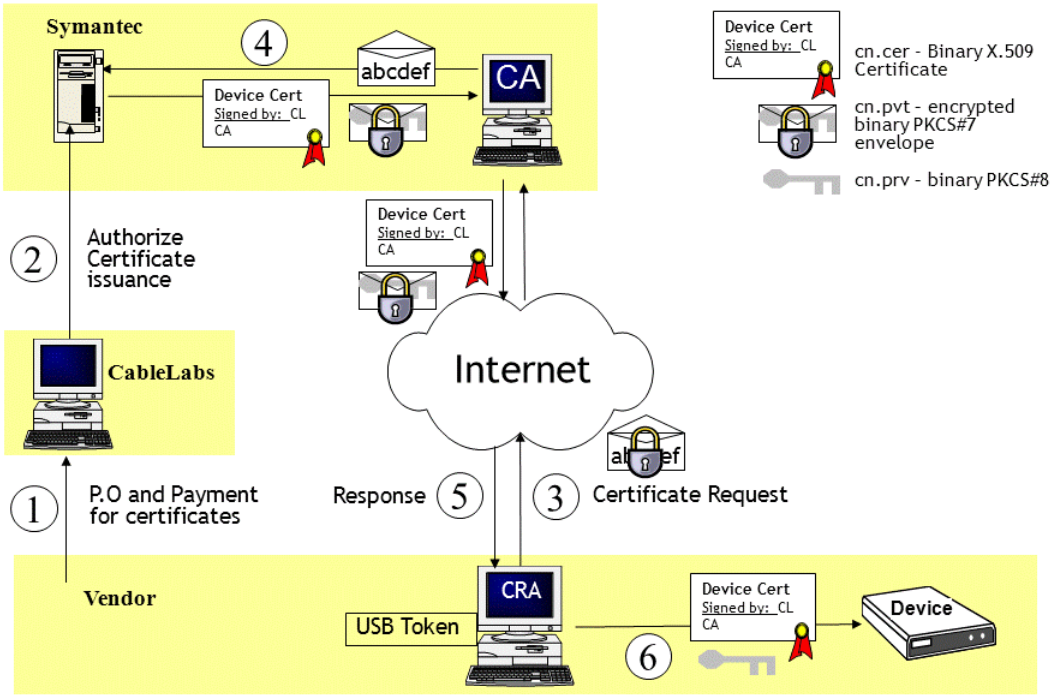


Figure 3 Device Certificate Request Process

Certificate Request Process (See Figure 3**):**

1. Manufacturer issues a Purchase Order (PO) for the number of certificates it wishes to purchase. NetworkFX sends invoice to manufacturer.
2. Once payment is received, NetworkFX authorizes Symantec to load the number of purchased certificates onto the account.
3. The Administrator authenticates to the CRA web page. The communication to this web page is encrypted and authenticated using the key and certificate on the Administrator's token. The Administrator may request the number of certificates up to but not exceeding the number of certificates the Manufacturer has purchased. The Administrator receives an acknowledgement of the request and is presented with a numbered receipt that identifies this particular request.

4. The CRA checks the request against the number of certificates authorized by NetworkFX for the Manufacturer . If the manufacturer has not exceeded its limit, the CA generates the certificates (and optionally the corresponding private keys) based on the information contained in the request. If fulfilling the entire request would exceed the Manufacturer's limit, then the CA will only generate certificates up to the Manufacturer's limit.
5. Once the request is complete, the CA informs the Administrator, via email, that their request has been completed. The Certificate response is placed on an access-controlled website. The Administrator via the CRA is sent the URL where this batch of certificates may be picked up. Access to this URL is protected via client and server authenticated TLS and requires the correct manufacturers' administrator certificate for access.
6. If the manufacturer has asked the CRA to generate the key pairs, the certificate request response is encrypted by the CRA into a binary PKCS#7 envelope. The response is decrypted using a lightweight client utility and the manufacturer's key on the token. Responses to certificate requests submitted as PKCS#10 certificate requests, will contain only certificates, thus will not be encrypted. Manufacturer can now embed the device certificates and corresponding private key into compliant OpenADR service devices.

Contact Information

To request OpenADR Alliance Digital Certificates please contact:

Digital Certificate Account Coordinator

NetworkFX, Inc.

858 Coal Creek Circle

Louisville, CO 80027-9750

Tel: (303) 661-3320

Fax: (303) 664-8131

Email: info@networkfx.net