Secured Substation Protection & Automation IED Firmware Management

ANCA CIORACA, MITAL KANABAR
GE Grid Solutions
Canada

SUMMARY

Substation Protection and Automation Intelligent Electronic Devices (IEDs) are essential components of the critical infrastructure in a typical power grid utility.
Digital interfaces to these IEDs are generally protected from the outside networks through firewalls and secure gateways, but such protection provides just one layer in a multi-layer defense in depth architecture, which is a must in the modern power grid.
There are other critical aspects to be addressed, such as ensuring that:
1. The IED may be upgraded only by authorized personnel and that it accepts only legitimate firmware at installation time and during software upgrades.
2. The IED is identified and authenticated in the environment where it is deployed, before it is allowed to join the network. The IED should be activated only if the authentication is successful.
3. The IED authenticates to other devices it communicates with for services, such as for procurement of keys, before exchanging any information.
The three aspects listed above are also critical from regulatory standards perspective, such as NERC CIP and IEC 62443. This paper describes solutions for these features, while using practical scenarios, where the steps are explained, starting with verifying the firmware legitimacy, authenticating the IED with the system it is deployed in and finally provisioning it.

KEYWORDS

IED = Intelligent Electronic Device
IEC = International Electrotechnical Commission
HMI = Human Machine Interface
IP = Internet Protocol
HSM = Hardware Security Module
RBAC = Role Based Access Control
M2M = Machine to Machine
CA = Certificate Authority
R-GOOSE = Routed Generic Object Oriented Substation Event
KDC = Key Distribution Center
GDOI = Group Domain Of Interpretation

anca.cioraca@ge.com

1 SECURING THE IED FIRMWARE

The IED firmware defines the behavior of the mission-critical power grid applications, so it is imperative that verification of firmware legitimacy is done at the time of installation or upgrades.
Securing the firmware implies one or both of the following operations performed on it:

a. Signing using a digital signature, which is attached to the firmware by the manufacturer and verified by the device itself, before the installation is permitted. A verified signature ensures the integrity and legitimacy of the firmware, the fact that it has not been intentionally modified or replaced while in transit, between the firmware provider and the customer site. It does not however protect the intellectual property contained in the firmware from prying eyes.
b. Encrypting the content using a digital encryption key. The content of the firmware is encrypted by the manufacturer and it must be decrypted at installation time, before the actual installation may begin. Encryption of the firmware protects the intellectual property contained in the firmware code.

1.1 A Cryptography Primer

1.1.1 Hashes

A hash is a small, but unique summary of a larger data.
An important requirement of hashes is collision resistance. This is what gives them uniqueness. Since hashes are unique, they are used to represent the integrity of the data and they are usually the base for digital signatures.

For creating a digital signature, a hash of the data is created, then signed with the private key of a public/private pair and the result is appended to the data. At destination, the signature is verified using the corresponding public key.

1.1.2 Public Key Cryptography

Public key cryptography uses pairs of keys: one public and a second one private.
The private key must be protected and should never leave the place where it was generated. Ideally it is kept in a specialized hardware, named Hardware Security Module (HSM).
The public key does not need to be protected from viewing. It needs however overwrite protection.
Public key cryptography is typically used for code signing.

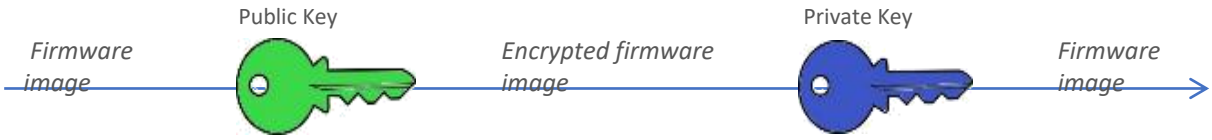
A hash of the firmware is created, then signed with the private key and the result is appended to the image. At destination, the signature is verified using the corresponding public key, already deployed on the device.

Figure 1: Signature – authentication of software/firmware

If encryption of the firmware is required, there are two choices.

Figure 2 presents the first choice, where asymmetric keys are used.
This method however is not very practical when encrypting big size data, such as firmware images tend to be, because the decryption time is quite long.
A second option uses symmetric keys, as shown in Figure 3.

Figure 2: Encryption – data scrambling so that it's not readable, unless decrypted

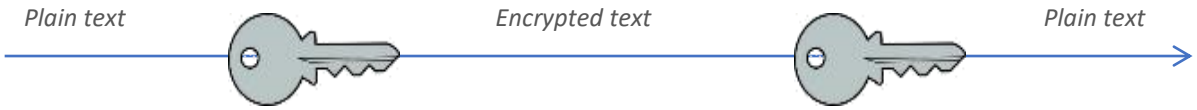


1.1.3 Symmetric Key Encryption

Symmetric key encryption is used for bulk data protection, when keeping the transmission and decryption time short is important.
Such is the case of encrypted firmware images, where fast decryption at installation time is important or the case of machine to machine (M2M) data communications, where the speed by which the data is parsed at destination is important.

Symmetric key encryption uses only one key for both encryption and decryption and the key must be well protected both by the encryptor and decryptor.
It is important that the distribution of the symmetric key is also well protected. Public key cryptography may be used for this purpose as well.

Figure 3: Encryption using symmetric keys



1.2 Firmware Code Signing Methodology

We recommend the use of public key cryptography for securing the firmware. As mentioned in the previous chapter, the firmware may be both signed and encrypted for secure transport between the manufacturer and the customer's site. A digital signature of the firmware is enough to provide the assurance of authenticity, which is the main concern for the customer. Additionally, if the firmware manufacturer is concerned with protecting its intellectual property, they may decide to also encrypt the firmware while in transit. Note that a firmware image is considered "in transit", after it leaves the secure environment of the manufacturer and up to the point when it is installed on a customer hosted IED.

This paper will only discuss the steps required for assurance of authenticity. Figure 4 details these steps.

But even before these steps may be performed, there are some preliminary operations by the IED manufacturer, which involve a decision for an adequate storage place for the key pairs to be used for signing and a decision on the certificate authority (CA) to be used for procurement of certificates to be associated with the keys.

It may be conceived that certain manufacturers may choose not to associate digital certificates to the keys used for signing the firmware and just internally manage the keys themselves. It is good practice however to use certificates, as they give assurance of legitimacy of the manufacturer and the validity of the keys. The certificate binds the keys to the specific manufacturer and associates a lifetime for the keys. The CA will watch the certificate for its lifetime and, if any suspicious activity is detected, it may revoke the certificate. Manufacturers and devices have the option of periodically questioning the CA as to the status of their certificates.

Regarding the storage of keys, ideally a Hardware Security Module (HSM) will be used for this purpose. This will guaranty the secure storage for the private key. The decision of using a local HSM, belonging to the device manufacturer, or one belonging to a public domain, such as Amazon, is an aspect to be considered. A local HSM, owned and operated by the IED manufacturer is suggested in order to minimize the chance of cryptographic material exposure.

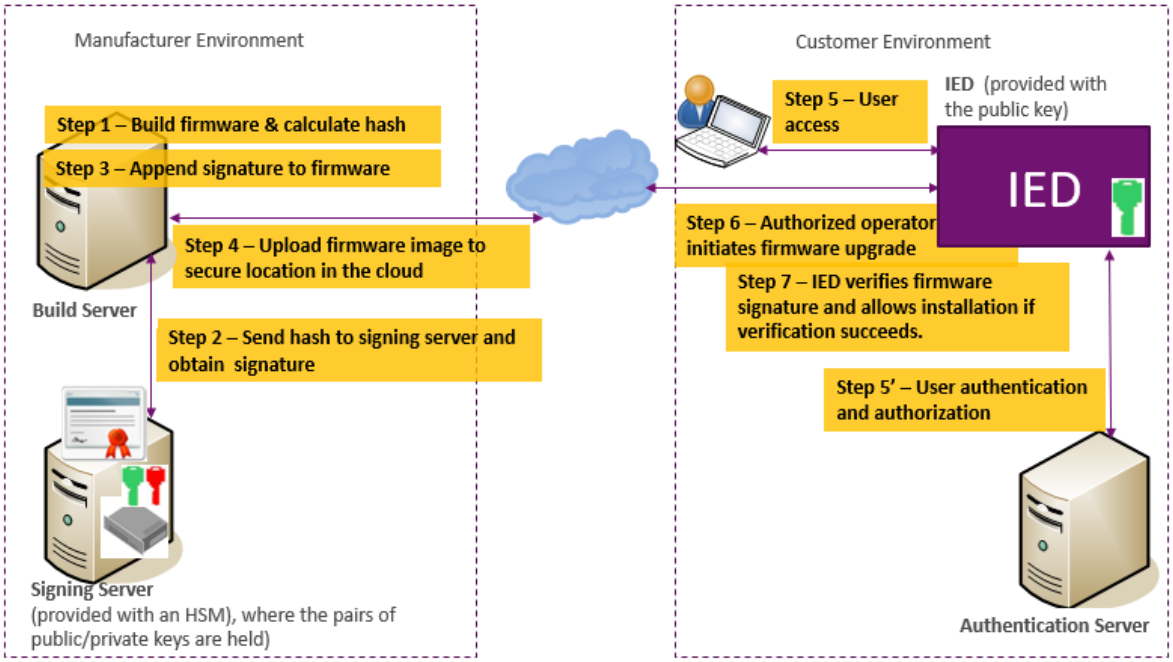
Once the storage is selected, the creation of a pair of public/private keys may be performed. We will call this pair: P/p. This may be done straight on the HSM. The HSM may connect with a CA and request a certificate to be associated with this key pair and with the IEDs that will use them. All IEDs from a specific product line will use the same certificate. The public key (P) will be downloaded on the IED as a one-time operation performed at the time when the IED is prepared for shipment. The private key (p) will be securely held in the HSM.

Every time a new firmware image or patch is built for the IED (Step 1), the firmware will be signed using the private key (p). A hash of the firmware will be calculated for this purpose on the build machine and securely sent to the HSM to be signed (Step 2). The HSM will provide the signature, which will be appended by the build machine to the firmware image (Step 3).
The signed firmware image will be uploaded to a secure location (Step 4).

At installation time the firmware upgrade is initiated by an authenticated and authorized person (Step 5). Ideally the user authentication is done using a central RADIUS or LDAP authentication server (Step 5’), where the database of valid users, their credentials and the associated roles is kept. The user to perform firmware upgrade must have a role that gives adequate authorization for this operation. The authorization model may follow the role based access control (RBAC) specified in IEC 62351-8 [1].

Once the user is authenticated and authorized, the firmware upgrade process may be initiated (Step 6). The firmware image is downloaded into an alternate memory location of the IED, so that the main image is not yet overwritten. The signature is extracted and verified against the public key P stored on the IED (Step 7). If the signature verification succeeds, the process of installing the new firmware is started. Otherwise the new firmware is not allowed on the IED and it is discarded.

Figure 4: Firmware signing and verification procedure



2 IED DEPLOYMENT AND PROVISIONING

The deployment and provisioning of the IED in a customer environment is an important aspect, which requires special attention not only functionality wise, but also from the cyber security perspective, as it may willingly or unwillingly offer chances for cyber events. Figure 5 details the process for deploying and provisioning an IED in a secure manner.

2.1 IED Provisioning

When new equipment, such as an IED, is procured, it may first go through a thorough verification in a customer's test lab and perhaps will receive a firmware upgrade, as described in the previous chapter.

After that, the IED is physically deployed in the field (Step 1), provisioned and then connected to the customer's operational network.

Device provisioning involves the creation and registration of certain entities that define the device, such as a unique identifier, a set of attributes and an identity certificate. Providing each IED with an identity certificate is a good security measure, as it gives assurance to the customer that only legitimate IEDs meant to operate in their environment will be authorized to join the network.

The identity certificate is different from the code signing certificate. The identity certificate is specific to each IED device deployed. As opposed to that, the code signing certificate is associated with a device type and it is the same for all the IEDs of that type.

A manufacturer may produce one code signing certificates for an entire product line and it may provide one default identity certificate with each IED it builds.

The identity certificate information needs to be loaded with the rest of the device information on the customer Device Provisioning Server responsible with authorizing and placing the IED into service (Step 2).

Once the identification data and the cryptographic information associated with the IED is loaded into the Provisioning Server, the IED may be powered up and a connection to the Device Provisioning Server established. The IED will authenticate itself with the

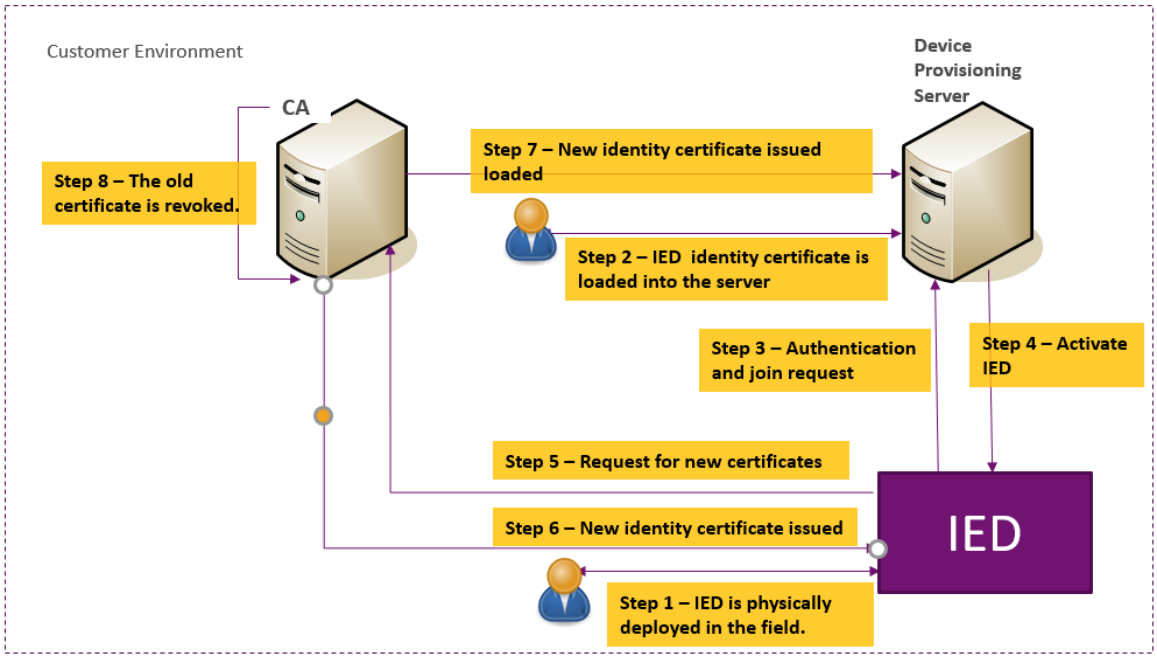
Provisioning Server, using its default identity certificate and it will ask for permission to join the network (Step 3). If the authentication is successful, the Device Provisioning Server will activate the device and put it into service (Step 4).

2.2 IED Re-Provisioning

Certain customers may not be satisfied with the level of security the default IED identity certificates provide and may wish to replace these certificates with ones issued by a Certificate Authority (CA) of their choice, whether a public one or a private one, hosted on their premises. Privately owned CAs may work better in isolated environments such as we see in the energy sector, also allowing for more control on the life cycle of certificates. The enhanced security is not the only reason a company may decide to replace default certificates. There are many types of devices from many vendors in a specific customer environment, including various servers, such as authentication and key distribution servers. All these devices need to be provided with identity certificates in order to interact securely with each other. Using one single CA for provisioning all these devices makes it much easier to manage and provides consistency.

For re-provisioning, the IED connects to the CA (either directly or through a registration authority RA) and requests a new certificate (Step 5). The CA provides the certificate (Step 6) to the IED and the device provisioning server (Step 7). As a last step, CA revokes the default certificate and it updates the Certificate Revocation List (CRL).

Figure 5: Device Provisioning



3 IED MACHINE TO MACHINE SECURE COMMUNICATIONS

The identification certificate initially provided with the IED or the one the IED owner replaced it with may be used for authenticating the IED for all communications in interactions with various servers that provide security services necessary during the lifetime of the IED, such as key provisioning for machine to machine communication or centralized user authentication. These services are usually not available within the electronic security

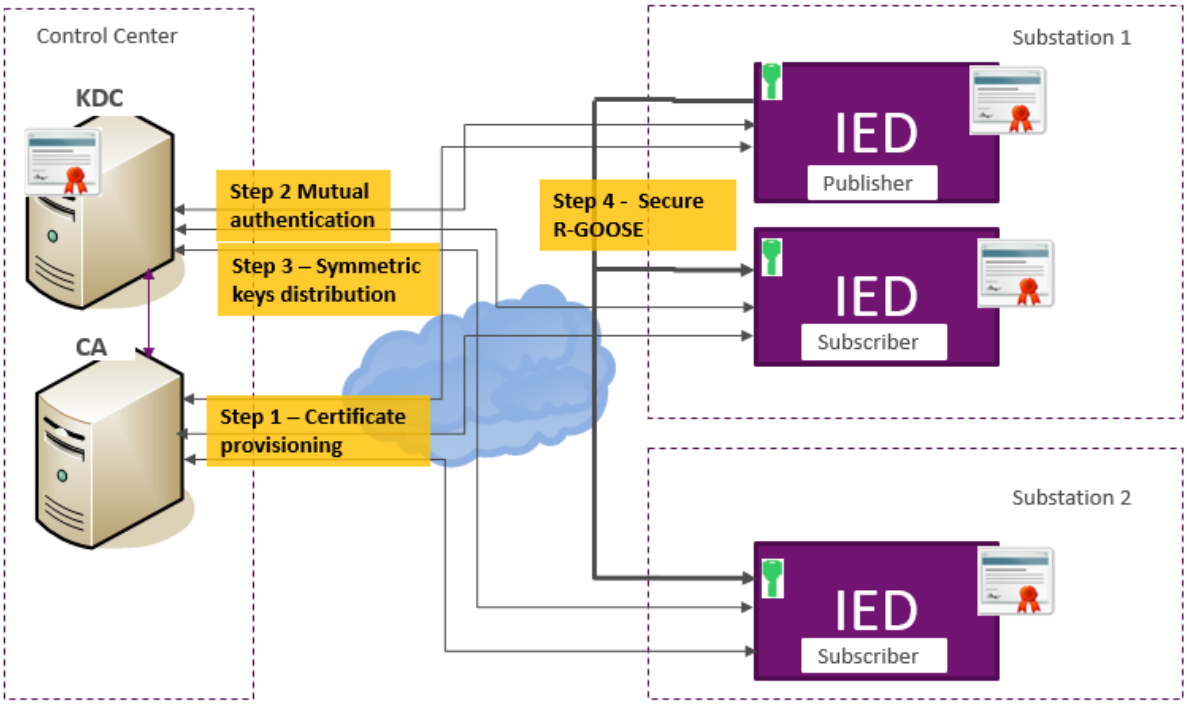
perimeter of the substation where the IED resides, so the communication between the IEDs and these services must be very well secured.

Figure 6 presents the use case of a machine to machine (M2M) communication scenario, where one IED (publisher) uses R-GOOSE (Routed GOOSE) multicast protocol to transmit commands to a multitude of IEDs (subscribers) dispersed in several substations. Since the communication channels between the publisher and subscribers must be secured, a symmetric key is used to sign and optionally encrypt the data between the IEDs involved in the R-GOOSE communications.

All IEDs belonging to this multicast group must obtain the key from a Key Distribution Center (KDC).
The IEDs, as well as the KDC, must be initially provisioned with a digital identification certificate (Step 1).
Once they all have valid certificates, the IEDs can start the conversation with the KDC, by first authenticating themselves (Step 2), using the identification certificates from step 1. The KDC will also provide its own certificate. Only after each side is satisfied with the authenticity and validity of the certificate, the negotiation for the symmetric keys may start and the KDC will provide the requested keys (Step 3).

A modified GDOI protocol, as described in IEC 62351-9 [2] may be used for the interaction with the KDC server. Whether this or a different protocol is employed, the requirement of mutual authentication between the KDC and each of the IEDs must be first satisfied. Only after the authentication succeeds, the KDC server will provide the required keys and R-GOOSE communication may run securely (Step 4).

Figure 6: Key Distribution for Secure M2M Communications



4 CONCLUSIONS

This paper aimed to identify and address some important aspects of cyber security, as applicable to the critical infrastructure protection of the electric grid.
The paper described solutions for secure firmware upgrade of IEDs, secure deployment and provisioning of IEDs and secure key distribution for machine to machine communication. It presented some practical scenarios, the case of a new device deployed in a substation and the case of secure procurement of keys for the authentication and encryption of M2M communications.
The proposed solutions are aligned with regulatory requirements for cyber security in critical infrastructure, such as described in NERC CIP [3] and IEC 62443-4 [4], and they make use of methods and mechanisms described in technical security standards for the power grid, specifically IEC 62351.

BIBLIOGRAPHY

[1] IEC 62351-8 - Power Systems Management and Associated Information Exchange – Data and Communication Security – Role Based Access Control
[2] IEC 62351-9 Power Systems Management and Associated Information Exchange - Data and Communication Security – Key Management
[3] NERC CIP https://www.nerc.com/pa/Stand/pages/cipstandards.aspx
[4] IEC 62443-4 Security for industrial automation and control systems,
Part 4-1: Secure product development lifecycle requirements
Part 4-2: Technical security requirements for IACS components
[5] Using High-Speed and Secured Routable GOOSE Mechanism
http://www.pacw.org/en/issue/june_2016_issue/secured_routable_goose_mechanism/using_highspeed_and_secured_routable_goose_mechanism.html