Purpose-bound Certificate Enrollment in Automation Environments

Rainer Falk and Steffen Fries
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {rainer.falk|steffen.fries}@siemens.com

***Abstract*—Information security is gaining increasing importance for networked control systems. Examples are industrial automation, process automation, and energy automation systems. Characteristic for all these systems is the data exchange between intelligent electronic devices – IEDs, which are used to monitor and control the operation. In energy automation these IEDs provide the data for a obtaining a system view of connected decentralized energy resources – DER. Based on the system view, a set of DER building a virtual power plant (VPP) can be managed reliably. The communication is realized through domain-specific protocols like IEC 61850 or IEC 60870-5. The communication is performed increasingly also over public networks. Therefore IT security is a necessary prerequisite to prevent intentional manipulations, thereby ensuring the reliable operation of the energy grid. Basis for protecting metering and control communication are cryptographic security credentials, which need to be managed not only during operation, but most importantly during installation (initial enrollment). This process needs to be as simple as possible to not increase the overall effort and to not introduce additional sources for failures. Hence, automatic credential management is needed to ensure an efficient management for a huge number of devices. This paper describes a new approach for the automatic initial security credential enrollment process during the installation phase of IEDs. The approach targets the binding of the installed IEDs to the operational environment and also to the intended utilization of the IED by embedding specific information into the enrollment communication, which is then reflected in the issued X.509 certificates.**

Keywords–security; device authentication; certificate enrollment; real-time; network access authentication; firewall; substation automation; smart grid; IEC 61850, IEC 60870-5, IEC 62351

I. INTRODUCTION

Decentralized energy generation, e.g., through renewable energy sources like solar cells or wind power, is becoming increasingly important to generate environmentally sustainable energy and thus to reduce greenhouse gases leading to global warming. Introducing decentralized energy generators into the current energy distribution network poses great challenges for energy automation as decentralized energy generation needs to be monitored and controlled to a similar level as centralized energy generation in power plants. This requires widely distributed communication networks. Distributed energy generators may also be aggregated on a higher level to form a so-called virtual power plant. Such a virtual power plant may be viewed from the outside in a similar way as a common power plant with respect to energy generation capacity. But due to its decentralized nature, the demands on communication necessary to control the virtual power plant are much more challenging. Moreover, these decentralized energy resources may also be used in an autonomous island mode, without any connection to a backend system.

Furthermore, the introduction of controllable loads on residential level requires enhancements to the energy automation communication infrastructure as used today. Clearly, secure communication between a control station and equipment of users (e.g., decentralized energy generators) as well as with decentralized field equipment must be addressed. Standard communication technologies as Ethernet and the Internet protocol IP are increasingly used in energy automation environments down to the field level [1] [2].

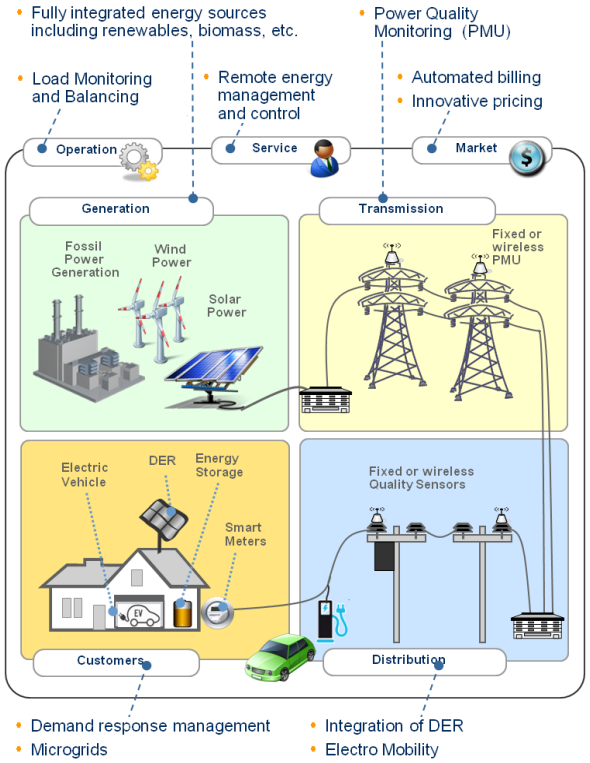

Figure 1. Typical Smart Grid Scenarios

 ISBN: 978-1-61208-349-0

Figure 1 depicts example Smart Grid scenarios showing the increased communication demand, e.g., through the integration of microgrids, controllable loads, and also electro mobility. IT security is a base requirement to be addressed in all the scenarios to ensure the reliable operation of the smart grid. One base for the secure interaction are typically security credentials in the form of X.509 digital certificates, corresponding private keys, and a related security policy. All need to be provisioned during device installation and maintained during operation. Especially the exchange of devices with spare parts should not lead to breaches in security, which could occur if the key material of the replaced devices is not handled appropriately. To ensure that this key material cannot be misused, e.g., in the context of an unintended service or in an unintended environment, the key material has to be bound to the respective device purpose. Existing options, e.g., using key usage extensions in X.509 certificates, may not always be sufficient, as they relate to the actual usage of the cryptographic key and not to the device application environment. The purpose-binding of a cryptographic key described in this paper therefore restricts the key acceptance depending on location information, and potential other parameters.

The remainder of this paper is structured as follows: Section II provides an overview of two example Smart Grid use cases. Section III depicts an overview of secure communication with respect to the use cases explained before. This section motivates the handling of security key material. Section IV introduces the Public Key Infrastructure as means for credential handling. Section VI introduces existing certificate enrollment methods, while Section VI describes an enhancement to have purpose bound certificates. Section VII concludes the paper and provides an outlook.

II. SMART GRID USE CASES

To motivate communication security, two example use cases are addressed in this paper, substation automation and DER incorporation in energy control networks. They are explained in the following two subsections.

A. Substation Automation

Automation networks are typically shared networks connected in a ring, star, or bus topology, or a mixture of these. Most often, the time-critical part is realized on a dedicated network segment, while the rest of the communication supporting the automation systems is performed on networks with lower performance requirements.

An example for energy automation is the communication within a substation. A substation typically transforms voltage levels, and includes power monitoring and protection functions. The example in Figure 2 shows a typical setup of a primary substation. The red rectangle shows the area, in which the IEDs communicate status information and provide this information into the substation automation zone and further up the hierarchy to the control center.

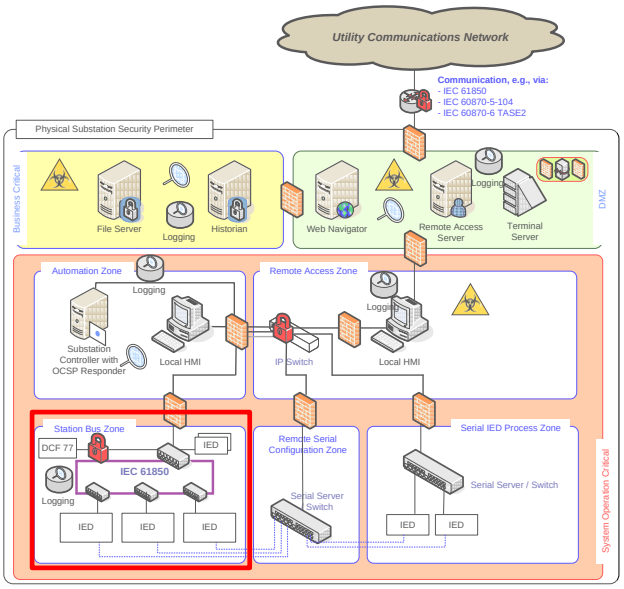

Figure 2. Substation – Functional Split into Zones

As depicted in Figure 2, the substation bus can be realized as ring, connecting the protection relays, acting in real-time. There is a connection to other zones within the substation, separated from the real-time part using Firewalls. Examples are the automation zone or the remote access zone. Another example is the zone storing the historian information also interacting with a backend SCADA system. The historian is a device for archiving measurements, events, and alarms of the substation. Figure 2 already shows security elements deployed within a substation, like Firewalls, virus checking tools, or access control means to components or data.

B. DER Incorporation

Decentralized Energy Resources (DER) may be connected to the Smart Grid at two different connection points. Depending on the amount of energy provided, they may be connected to the low voltage network or to the medium voltage network (distribution network). The first one is rather typical for DER in residential areas, like a solar panel, while the connection to the medium voltage network is done for larger deployments like wind power farms or solar parks. Necessary for both is the connectivity to a communication infrastructure to allow a control center to act on provided information about current energy generation, but also to provide scheduling information to the DER, e.g., depending on the weather forecast, to better balance the feed in of energy into the electrical network. Communication with the DER may be done using different communication technologies, like Power Line Communication (PLC) or wireless communication via the UMTS network. For the distribution network operator (DNO), it is essential to know, which DERs are associated to his operational control. This can be supported by the used security credentials using additional information depending, e.g., on the geographic location of a DER or on the association with a dedicated DNO.

 ISBN: 978-1-61208-349-0

III. SECURE COMMUNICATION IN SMART GRID

IEC 61850 [3], [4] is a standard for communication in the domain of energy automation. It is envisaged to be the successor of the currently used standards IEC 60870-5-104 and DNP3 especially used in the North American region. IEC 61850 enables interoperability between devices used in energy automation. For example, two IEC 61850 enabled devices of different manufacturers can exchange a set of clearly defined data, and the devices can interpret and use these data to achieve the functionality required by the application due to a standardized data model. In particular, IEC 61850 enables continuous communication from a control station to decentralized energy generators or to IEDs (like protection relays) in a substation.

IT security is increasingly important in energy automation as on part of the Smart Grid. Here, the IEC 62351 framework [5] with currently 11 parts kicks in, defining security services for IEC 61850 based communication covering different deployment scenarios using serial communication, IP-based communication, and also Ethernet communication. The latter one is used locally within a substation to cope with the high real-time requirements. While it may be not always necessary to encrypt the communication to protect confidentiality, there is a high demand to protect the communication against manipulation and to allow for source authentication. IEC 62351 relies on existing security technologies as much as possible and profiles it for the application environment . One example is the application of Transport Layer Security (TLS, RFC 5246 [6]) to protect TCP-based communication. Here, IEC 62351 basically reduces the manifold options of TLS to ease interoperability. Another example is the adoption of Group Domain of Interpretation (GDOI, RFC 6407 [7]) as group-based key management to distribute key material for the protection of status information and event signaling between IEDs in a substation or across substations using Wide Area Networks (WANs).

A specific characteristic throughout IEC 62351 is the consequent application of X.509 certificates and corresponding private keys for mutual authentication on network layer and application layer. This requires an efficient handling of X.509 key material and the availability of this information right from the installation. There is a strong need to provide these credentials without increasing the installation effort. For instance, devices may generate their own key pair, but certification needs to bind this key pair to the operational. This is a challenge from the pure technical perspective as a high number of devices need to be equipped with the key material. But also from the network operator process point of view this is challenging, as the key material has a lifecycle and needs to be updated once in a while. These aspects will be addressed in the following sections.

IV. PUBLIC KEY INFRASTRUCTURE - PKI

A PKI typically contains a variety of services requiring interfaces in the devices utilizing the PKI and also an accompanying process. In general, a Public Key Infrastructure provides a secure, reliable, and scalable environment for the complete lifecycle of key material, i.e., generating, distributing and querying public keys for secrecy, correctness, and sender verification. Moreover, it binds the "owner" to the public key using a digital certificate and thus enables identification of users and components utilizing certificates. Furthermore, it maintains and distributes status information for the lifetime of that binding, i.e., from the generation till the revocation. The general functionality and formats are described in RFC 5280 [8].

The following list provides a short overview about the different components, which are depicted in Figure 3:

- **Registration authority (RA)** authenticates the user or IED or the data submitted by the user or IED, performs an authorization check and initiates the certificate generation at the CA. For machine-to machine communication the RA can be used to mediate between the device applying for a certificate and the CA.
- **Certification authority (CA)** is a trusted entity that certifies public-keys by issuing certificates.
- **Key/certificate archive** is a repository in which the CA stores certificates and/or generated key pairs.
- **Key generation** is a function of the PKI responsible for the generation of key material (public and private keys), which are certified through the CA
- **Public Directory** is a (usually publicly readable) database to which the CA stores all issued certificates
- **Revocation Lists** are also a publicly readable database to which the CA stores all revoked certificates

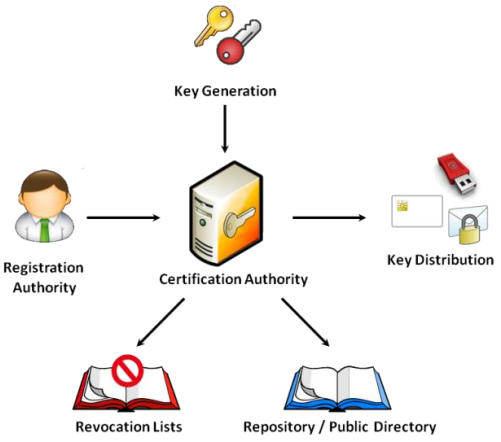

Figure 3. PKI Components

In the context of smart grid, a PKI may be operated by a utility company working as internal PKI, or it may be a public PKI, also depending on the target use case and the need for interoperation between different parties. Moreover, the functionality provided by the PKI needs to be streamlined to the target environment to avoid unnecessary effort. In any case, the devices utilizing key material issued by the CA need to provide the technical interfaces to accomplish this task. This is described in more detail in IEC 62351-9 targeting the key management explicitly.

 ISBN: 978-1-61208-349-0

Section VI describes an enhancement of the typical used PKI setup by introducing an intermediary, which provides all operational environment specific information. This avoids the pre-configuration of IEDs with this information.

V. EXISTING CERTIFICATE ENROLLMENT METHODS

This section describes common methods for certificate enrollment taking device capabilities into account. Capabilities in this context relate to local and remote key generation. Typically local generation of key material is desired to avoid the handling of private keys outside the devices. Note that depending on the key usage, there may be requirements to also have the private key available in a trust center to ensure that encrypted information can be accessed even the device hosting the private key was either damaged or has been compromised.

A. Manual Enrollment

Manual enrollment relates to the manual connection of a device to an engineering tool to provide the key material during a local configuration session, prior to the connection in the target network. This approach requires a significant initial configuration effort and is especially cumbersome in case of device replacements. It may be realized using an offline engineering network to bootstrap the security credentials for connected devices. Here, the devices or components do not possess a cryptographic credential up front, as the separate network is assumed to be physically secure. In the simplest form, it may be a direct connection of an engineering laptop to the component to be administered using purely local point-to-point communication.

B. Automated Enrollment

Automated enrollment refers to the initial configuration of devices including the key material. This is shown in Figure 4. Field devices are connected to the network and contact the PKI server to obtain certified key material.

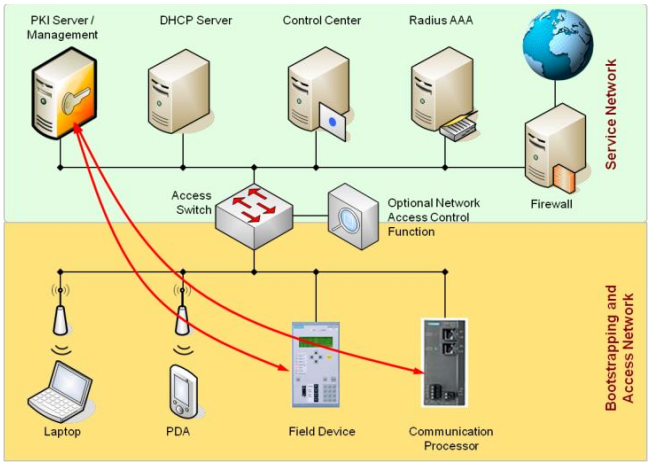

Figure 4: Automated distribution using management protocols

Here, the field devices generate their public/private key pairs locally and send a Certificate Signing Request (CSR) for the public key to the RA/CA (part of the PKI server). Part of the CSR may be a serial number of the device, against which the PKI server can check a configured list of devices allowed to be enrolled. This authorization may also be realized by other means like one-time passwords. According to RFC 2986 [9] the CSR is defined n ASN.1 as shown in Figure 5 below.

```
CertificationRequest ::= SEQUENCE {
   certificationRequestInfo
     CertificationRequestInfo,
   signatureAlgorithm AlgorithmIdentifier{{
     SignatureAlgorithms }},
   Signature BIT STRING
   }

CertificationRequestInfo:
   CertificationRequestInfo ::= SEQUENCE {
   version       INTEGER { v1(0) } (v1,...),
   subject       Name,
   subjectPKInfo SubjectPublicKeyInfo{{
    PKInfoAlgorithms }},
   Attributes [0] Attributes{{
    CRIAttributes }}
   }

SubjectPublicKeyInfo { ALGORITHM : IOSet}
    ::= SEQUENCE {
    Algorithm AlgorithmIdentifier {{IOSet}},
    subjectPublicKey BIT STRING
   }
```

Figure 5: Certification Request structure [9]

Several protocols are known for transmitting a CSR to a CA. Examples are:

- SCEP – Simple Certificate Enrollment Protocol [10]
- CMP – Certificate Management Protocol [11]
- CMC – Certificate Management over CMC [12]
- EST – Enrollment over Secure Transport [13]
- XML Key Management Specification [14]

These different protocols describe the communication of a CSR from a device to the CA, were the device ideally generates the key pair for itself. Additionally to identification information like the serial number, further information can be connected with the CSR, like a password (to be used to authorize a potential future revocation) or key usage restrictions. The CSR has to be protected to prevent illegitimate issuing of certificates. The CSR itself may be protected using the public key of the RA/CA as in case of SCEP. In case of CMP, the CSR is protected using an initial authentication key, and in EST, the CSR is transmitted over a secured communication link. Here TLS is applied, providing the opportunity to authenticate both peers during the connection establishment. Also, there may be an intermediate RA located between the device sending the CSR and the CA, which already performs the verification of the CSR to reduce the load on the CA.

When deployed in the operational environment, IEDs are typically not pre-configured. Hence, an intermediate component is used to enhance the CSR with additional information about the deployment environment before it is forwarded to the RA/CA. This information is not available at or provided by the sender of the CSR itself. The following

 ISBN: 978-1-61208-349-0

section describes such an enhancement of the CSR communication on the way from the devices to certification server. This enhancement is proposed to provide additional information about the environment in which the device is deployed. Such information can either be contained in the certificate to be issued or associated with the device certificate by other means, like a central configuration database. This approach helps identifying, e.g., a physical movement of components or devices to other locations. Hence, key material valid in one location may not be misused in a different location. Moreover, the approach also enhances the options for asset management, by providing fine-grained information already during the authentication processes, employing the enhanced certificate.

VI. ENHANCING CERTIFICATE ENROLLMENT WITH DEVICE PURPOSE BINDING

This section outlines the introduction of an additional network component to extend a CSR with additional information. Such additional information is encoded as additional attribute added to the original CSR as sent by the device. This attribute indicates the context or other deployment specific information, to be added to either the certificate or the configuration database.

This is achieved by adding a Certificate Attribute Intermediary (CAI) along the CSR communication path. The CAI adds at least one attribute to the original CSR (without otherwise manipulating the original CSR). The additional attribute acknowledges additional information about the operating environment. This additional information may be the membership of the CSR sender (device) to a dedicated zone or group or to a dedicated location either on a geographical base or on an organizational base. Moreover, the CAI may already check the CSR (like an RA) and signal this also in the attribute. The CAI may add information about intended usage restrictions of the certificate, depending on the device type and the security policy. This information can be part of the engineering information, which must then be available at the CAI. The CAI may also request that the certificate is issued using a dedicated signature algorithm.

The attribute and the CSR build the Extended Certificate Request (ECR). The ECR is protected by a cryptographic checksum, binding the attributes to the original CSR. Ideally, this is a digital signature of the CAI. This could be realized as PKCS#7 structure [15] or as XML structure, but may also be a symmetric checksum, involving a shared secret between the CAI and the CA. The ECR is then forwarded to the RA/CA, which verifies both the CSR and the additional attribute. If the RA and CA are separate entities, the CAI may be co-located with a local RA. After successful verification, the additional information from the attribute is included in the X.509 certificate within a certificate extension.

Depending on the applied enrollment protocol the ECR may be transmitted via a TLS protected communication path using, e.g., HTTP POST, HTTP GET or as REST or SOAP message).

Figure 6 depicts the on path enhancement of a CSR with attributes *aa1, …, aa3*. Also shown are potential functions to be performed by the CAI (e.g., CSR checking) and the enhanced functions on the RA/CA side.

In a substation automation environment, the CAI can be part the substation controller or the remote access server as the central ingress and egress point of the substation. This is depicted in Figure 7. The different steps describe the single steps for the ECR processing. Note that the prerequisite is the availability of the central RA/CA root certificate in the IED.

The following steps are performed for the initial enrollment of an energy automation device IED:

1. Generation of key material (public/private key), generation of the CSR within the IED
2. Send local generated CSR to Remote Access Server
3. Verification of CSR through Remote Access Server. Remote Access Server acts as CAI. Generation of attributes and ECR. Send ECR to central RA/CA server of the distribution network operator.
4. Verification of ECR signature through central RA/CA, verification of attributes (installation information, etc.); optional verification of original CSR
5. In case of successful verification device specific certificate will be generated and send to the remote access server of the substation.
6. Forwarding of certificate to IED
7. Local automated installation of certificate upon receiving and successful signature verification against local RA/CA root certificate.

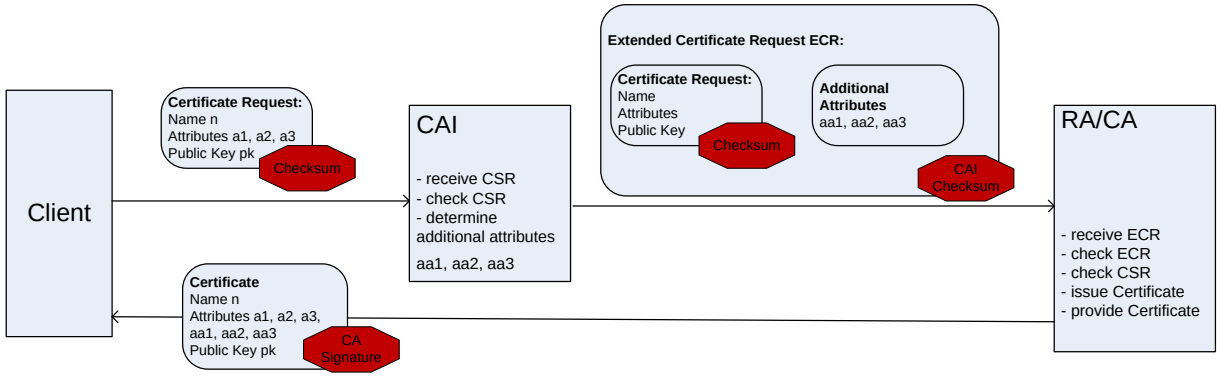

Figure 6: Realization option for on path CSR enhancement with attributes characterizing the deployment environment

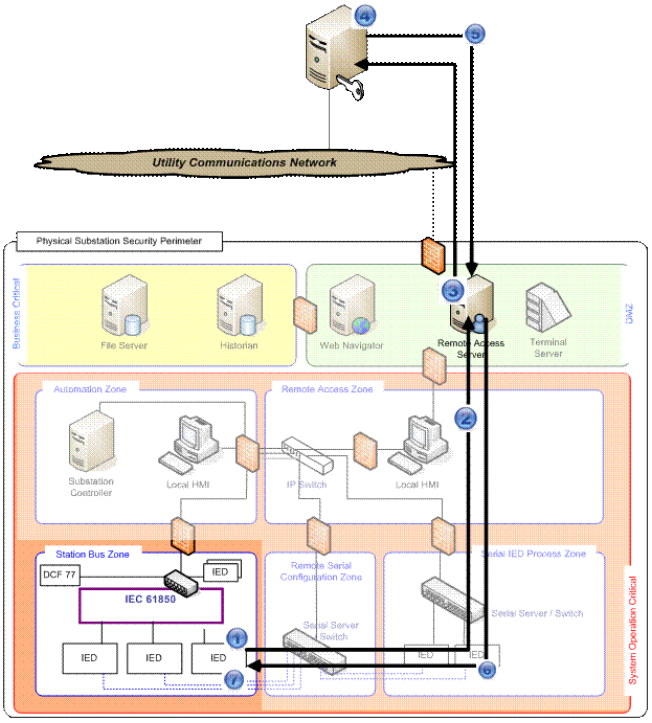

Figure 7: Enhancement of the CSR path in a substation

Note that this paper describes the concept of the enhancement. Implementations are not finished yet.

VII. CONCLUSIONS AND OUTLOOK

This paper described security enhancements for energy automation systems involved in substation communication and smart grid. The cryptographic protection of control communication requires that cryptographic keys and certificates are provisioned on energy automation devices. Manual configuration would not scale to the huge number of devices, and be prone to configuration errors. Therefore, automatic configuration of automation devices is required not only during the operation, but especially for the initial device enrollment. To ensure the correct configuration of cryptographic device credentials, information is required at which location a specific device has been installed. An additional network element has been described that trustfully enhances a certificate signing request issued by an automation device with information on the network segment in which the device has been installed. This allows the CA to issue a device certificate that is bound to the operational zone of the device ("location"). Moreover, additional information for the CSR processing can also be provided. A relying device towards which the considered device authenticates using this zone-bound certificate, can verify whether the device belongs to the own zone. This ensures that an automatically provisioned device is operable using the established configuration only within the corresponding zone. When the device is relocated or put out of service, its device certificate cannot be misused, e.g., in other zones.

Standardization is currently ongoing in the context of ISO/IEC62351-9, which defines interoperable means for automatic device credential management for energy automation equipment. The new approach described in this paper enhances the current credential management approach and will be proposed for to be considered in future energy automation security standards.

REFERENCES

[1] S. Fries and R. Falk, "Efficient Multicast Authentication in Energy Environments", Proc. IARIA Energy 2013, March 2013, ISBN 978-1-61208-259-2, pp. 65-71, http://www.thinkmind.org/download.php?articleid=energy_2013_3_30_40056 [retrieved Dec. 2013]

[2] M. Felser, "Real-time Ethernet – industry prospective," Proc. IEEE, vol. 93, no.6, June 2005, pp. 1118-1128, http://www.felser.ch/download/FE-TR-0507.pdf [retrieved: Dec. 2013]

[3] IEC 61850-5 – "Communication requirements for functions and device models", July 2003, http://www.iec.ch/smartgrid/standards/.

[4] "Efficient Energy Automation with the IEC 61850 Standard Application Examples", Siemens AG, December 2010, http://www.energy.siemens.com/mx/pool/hq/energy-topics/standards/iec-61850/Application_examples_en.pdf [retrieved: Dec. 2013].

[5] IEC 62351-x Power systems management and associated information exchange – Data and communication security, http://www.iec.ch/smartgrid/standards/.

[6] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, Aug. 2008, http://tools.ietf.org/html/rfc5246 [retrieved: Jan. 2014].

[7] B. Weiss, S. Rowles, and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, Oct. 2011, http://tools.ietf.org/html/rfc6407 [retrieved: Jan. 2014].

[8] D. Cooper et al, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008, http://tools.ietf.org/html/rfc5280 [retrieved: Jan. 2014].

[9] M. Nystrom and B. Kaliski, "PKCS #10: Certification Request Syntax Specification", RFC 2986, Nov. 2000, http://tools.ietf.org/html/rfc2986 [retrieved: Jan. 2014].

[10] M. Pritikin, A. Nourse, and J. Vilhuber, "Simple Certificate Enrolment Protocol", Internet Draft, Sep. 2011, http://tools.ietf.org/html/draft-nourse-scep-23 [retrieved: Jan. 2014].

[11] J.Schaad and M.Myers, "Certificate Management over CMS", RFC 5272, June 2008, http://tools.ietf.org/search/rfc5272 [retrieved: Jan. 2014].

[12] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), RFC 4210, Sep. 2005, http://tools.ietf.org/html/rfc4210 [retrieved: Jan. 2014].

[13] M. Pritikin, P. Yee, and D. Harkins, "Enrollment over Secure Transport", RFC 7030, Oct. 2013, http://tools.ietf.org/html/rfc7030 [retrieved: Jan. 2014].

[14] XML Key Management Specification http://www.w3.org/TR/xkms2/

[15] B. Kaliski, "PKCS#7 Cryptographic Message Syntax Version 1.5, RFC2315, March 1998, http://tools.ietf.org/html/rfc2315 [retrieved: Dec. 2013].

 ISBN: 978-1-61208-349-0