Authentication on high critical infrastructures using interoperable federated identities

Armin Lunkeit, Jürgen Großmann

OpenLimit SignCubes AG
armin.lunkeit@openlimit.com

Fraunhofer Institute for Open Communication Systems FOKUS
juergen.grossmann@fokus.fraunhofer.de

Abstract: The technical guideline TR-03109 divides between the roles of the SMGW technician and the Gateway administrator whereas the Gateway administrator gains full access to the SMGW and the service technician has only very limited access rights. In many scenarios the service technician will also need full access to the Smart Meter Gateway which means that he must be able to change its role. Federated identities can help to create a solution that keeps the strict role enforcement between service technician and Gateway Administrator. This article presents an approach on the background of the current Smart Grid development and identity technology adopting approaches used for the German national ID card. A short discussion pertaining threats and risks completes the discussion.

1 Smart Grid Infrastructures – German approach

Based on the European Directive 2003/54/EG the EU member states are required to introduce intelligent measurement devices for electricity. The German government regulates this requirement in the law on energy industry (Energiewirtschaftsgesetz – EnWG), especially in §21c, §21d and §21e. The ministry of economics (BMWi) requested the Federal Agency for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik - BSI) to set up a technical guideline [3109-1] and Common Criteria protection profile [PP] addressing security and interoperability. The German smart grid approach requires a gateway component for data collection, consumption displaying and secure communication with meters, users and external entities. This component is called “Smart Meter Gateway (SMGW)”. The Smart Meter Gateway itself is not a measurement device; it is a data aggregation and communication unit that protects the privacy, integrity and authenticity of the consumer data during local storage and network communication. A hardware security module is built into the Smart Meter Gateway for protection of key material and cryptographic operations. Three logical and physical distinct networks are defined for the Smart Meter Gateway:

- The Wide Area Network (WAN)

- The Local Metrological Network (LMN)
- The Home Area Network (HAN)

The connection in the Local Metrological Network is required for communication with external meters. The Smart Meter Gateway itself is not a metering unit for electricity or gas; it serves a data collection unit that is responsible for the secure transfer of the collected consumption data to the energy supplier for billing reasons. The connection in the HAN network provides a report of the values measured by the meter responsible for his household and also provides a transparent proxy channel into the WAN. This proxy channel is required for proprietary communication of local power suppliers (e.g. solar panels) with external entities. At least the WAN connection provides communication services with external entities (e.g. the power supplier delivering energy to the household).

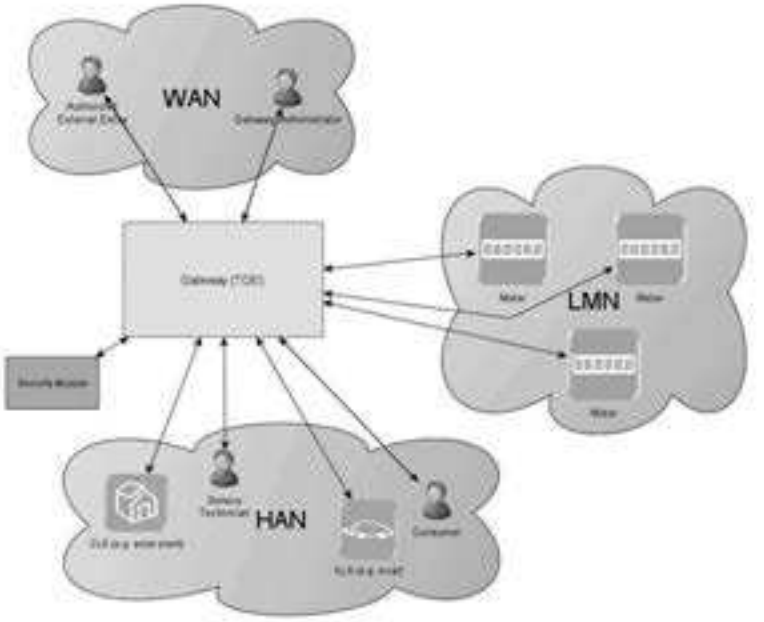

Figure 1 Smart Meter Gateway and it‘s environment [PP]

As shown in figure 1, one of the external entities in the WAN is the gateway administrator (GWA) who is a trustworthy external entity with the ability to control and configure the SMGW. The gateway administrator is a technical role and responsible for configuration of tariffing profiles, certificate management on the Smart Meter Gateway, firmware updates etc. and has also access to several log information. It is clearly stated that the gateway administrator does not have access to user any measured consumption data. Figure 1 does also show the Service Technician who has access to the Smart Meter Gateway from the Home Area Network and is able to access the system log information. The service technician has no possibility to initiate a firmware update or similar

operations. Vendors of Smart Meter Gateways must proof the fulfillment of the technical and security requirements defined in [PP] and [3109-1] of their product by Common Criteria and technical guideline certifications which also check the strict role separation.

Today's energy infrastructures use Command and Control Centers which allow the central administration of devices in the energy network. It is highly probable that these central communication nodes will also be responsible for the management of the Smart Meter Gateway in the household. They will act as smart grid management nodes and execute the gateway administrator role. We claim that the service technician will be required to perform operations (e.g. configuration, initiation of firmware updates) which are not foreseen for this technical role. Personal maintenance of a smart device in the household by a service technician is a cost issue. In case that a problem is encountered on a Smart Meter Gateway that needs to be solved by trained maintenance personal, this maintenance personal must possibly be able to gain full access to the Smart Meter Gateway similar to the gateway administrator. Therefore this article focuses on the administrative access to the Smart Meter Gateway. We discuss secure authentication of an administrator on the Command and Control Center and the enrollment of security policies in order to secure the access to the Smart Meter Gateway via potentially unsecure wide area networks.

2 Technical Background

2.1 Electronic Identities and Authentication

One approach for authentication with a secure token is the use of the electronic citizen card (nPA). This electronic citizen card comes with a rich set of innovative authentication functionality, e.g. PACE (Password Authenticated Connection Establishment) and EAC (Extended Access Control). These mechanisms have been widely discussed in publications ([BDFK11], [3110]).

The basic communication model of the German citizen card in order to access identity information stored on the card contains a trusted remote terminal, typically called eID-Server. The citizen card is served by a local eID-Client like the AusweisApp or the Open eCard-App. The communication between the eID-Client and the eID-Server is standardized in the technical guideline TR-03112-7. Upon this protocol stack several communication models are used, e.g. SOAP and SAML. The use of the German identity card in a federated identity environment allows its use in typical scenarios like Single Sign On (SSO). Research projects like SkIDentity are dedicated to definition of secure and trusted identity exchange in the cloud and utilize a rich set of different authentication technologies in one federated identity environment. Especially SkIDentity addresses the issue of using several identity tokens. The approach of using the electronic citizen card might face difficulties due to legal reasons but other technologies adopting the EAC-approach are available [OLSC].

2.2 Administrative Access to the SMGW

The mutual authentication between the gateway administrator and the smart meter gateway utilizes digital certificates. A signed UDP packet is sent to the smart meter gateway by the administrator and the new mutual authenticated TLS channel is established. The assignment of the administrator role on that new connection is mainly based on the digital certificate used by the smart grid management node during the TLS handshake phase. Once authenticated as gateway administrator, the Smart Meter Gateway allows the full administrative access, e.g. configuration of communication routes or key management of the built in HSM (hardware security module). The communication between the gateway administrator and the Smart Meter Gateway is secured by a mutual authenticated TLS channel using elliptic curve cipher suites. The smart meter gateway therefore owns a private key which is protected by the built in HSM, the root anchor of the Smart Meter Gateway PKI and the administrator's certificate are also configuration items of the gateway.

3 Electronic Identities in the Smart Grid Infrastructure

The technology of the German citizen card and its adoptions (e.g. the truedentity technology of OpenLimit) make use of secure communication protocols and provide a secure and reliable authentication. The authentication process delivers an attested digital identity. Based on that digital identity the enrolment of security policies is undertaken: Rights are granted and limitations are enforced. Using this approach the administrative access to smart grid devices even from untrusted networks is possible: The electronic identity contains security attributes that are verified and attested by an Identity provider and the smart grid management node can rely on this information. The communication between the service technician and the smart grid management node is protected by EAC and TLS.

3.1 Adoption to Smart Grids

[PP] and [3109-1] define the roles of the gateway administrator and the service technician with different rights. The gateway administrator is a trustworthy entity that has full access to the Smart Meter Gateway. This includes the following:

- Configuration for measurement data, their processing and submission of electronic measurement data to external market entities
- Installation of firmware updates
- Configuration of access rights for external market entities within in the Smart Meter Gateway
- Configuration of the integrated security module
- Configuration of certificates in the Smart Meter Gateway

For privacy reasons the gateway administrator is not allowed to view current measurement data[1]. The service technician is only allowed to access system log information and diagnosis information. This enforces a strict separation between both roles. Beneath this role separation it must be taken into account that the service technician in person will need to change its role in order to act as a gateway administrator. This is required in order to install new communication profiles or firmware updates in case that the Smart Meter Gateway has encountered a problem is no longer working properly. In this case the service technician needs the possibility to access the smart grid management node in order to perform service operations that are only foreseen to be performed by the gateway administrator. Therefore an authentication method on the smart grid management node is required which enforces a reliable identification of the service technician in order to change his role. This role of the *natural person* is changed from service technician to gateway administrator.

3.2 Solution Concept

The previous chapter with a roughly description of the authentication framework we explained the technical interface for accessing electronic identity information. The service technician needs to authenticate itself with a secure token on the smart grid management node. Based on the authentication data this central system will gain access rights to the service technician so the service technician will change its role and now act as gateway administrator.

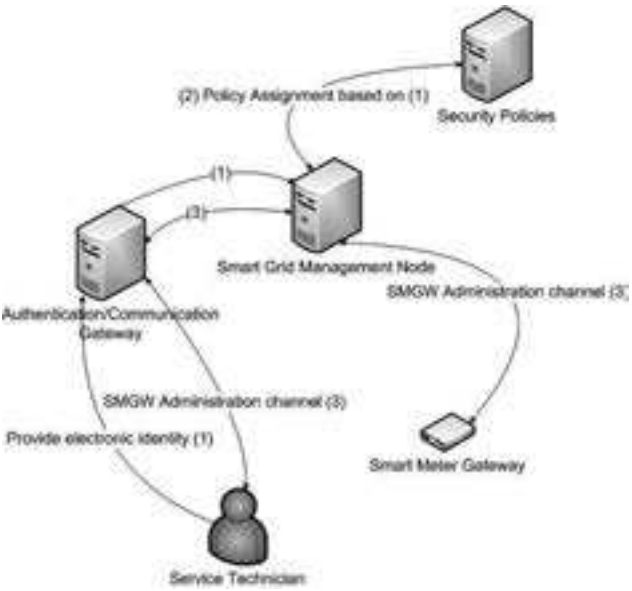

Figure 2 Solution concept

[1] Due to [PP] and [3109-1] this is only allowed for the service provides for billing reasons.

We introduce an authentication and communication gateway with the responsibility to authenticate the external entity and is moreover responsible to provide a secure remote communication channel that offers an appropriate level of security. Therefore an extension of the communication model described in the technical guideline TR-03112-7 is foreseen. The current standard describes the establishment of a TLS secured channel from the remote terminal to the client application and provides additional protection for the communication between the remote terminal and the chip with Secure Messaging keys agreed by using the elliptic curve version of Diffie-Hellman (ECDH). In our approach the secured channel (TLS and Secure Messaging Chanel) end in the client application. The client application makes use of this channel for transmission of commands and data from the external entity (service technician) to the authentication and communication gateway. Therefore an alternative token than the nPA is required, e.g. a chip card providing authentication keys for mutual TLS authentication.

This approach addresses one of the main issues of authentication: Even if the authentication is secure, the security of the consecutive communication depends on the provided security of the application utilizing the authentication service. Threat scenarios like session hijacking etc. are still relevant for web applications if authentication and communication security are not linked together. The presented approach combines authentication and offers reuse of the established secure communication channel so the channel is bound to the authentication based on the electronic identity.

This solution does not involve new exploitable interfaces and communication channels. The smart grid management node relies on the authenticity of the electronic identity and applies security policy for transmission of administrative commands initiated from a potentially untrusted network to the Smart Meter Gateway. The use of the EAC-secured channel between the service technician and the authentication and communication gateway in combination with the TLS provides a comprehensible security level.

3.3 Threats and Risks

Threat modeling analyzes the security of a system (hardware, software, networks) by utilization of assets, objectives, threats, attackers, vulnerabilities and countermeasures. This methodology is used by different IT-security frameworks, e.g. Common Criteria or the CORAS approach. The description of the threat model for the smart meter gateway is part of the protection profile [PP]. One important asset in [PP] is the privacy of the user's data. Neither the gateway administrator nor the service technician have permission to access any data that is specific for the customer. This includes consumption data as well as any other personal data. From the perspective of the smart meter gateway, our approach does not introduce any new threats to the smart meter gateway. The communication model of the smart meter gateway remains the same as required in the protection profile [PP] and the technical guideline [3109-1]. One of the essential threats to smart grid infrastructures is the model of central administration: We claim that the attacker in the network is more interested in manipulation of a smart grid management node than in attacking a single smart meter gateway. In our approach the authentication and communication gateway will be the object of interest for an attacker because it

offers the functionality of acting as a gateway administrator. This is attack scenario remains relevant even for the approach presented in [3109-1] with the difference that the smart grid management node would directly be offended. The presented approach does therefore not introduce a new threat to the smart grid on this level.

We claim that the most relevant threat that must be taken into account is a malicious service technician. The protection profile does explicitly assume a person in role service technician as a potential attacker so our solution must also deal with that assumption. This threat might not be mitigated by a single measure, several measures must be combined:

- The smart meter gateway must offer self protection of its IT-components (e.g. check of firmware integrity and authenticity).
- The security policies applied to the service technician with remote administrative access to the smart meter gateway must ensure that no malicious operations can be performed and access rights are limited
- The ID management system must offer the possibility of identity revocation in case that a particular service technician has been identified as attacker

Our ongoing research will be focused on the analysis of the remaining risks resulting from that approach using CORAS ([BBD+06]), which provides a model based method for risk assessment. CORAS includes a methodology, a formal language and tool support for the analysis and assessment of risks and consists of eight steps for the risk assessment process. We have planned to consider current research activities, e.g. the DIAMONDS [ITEA2] project with the goal not only to identify risks but also to provide model of how vulnerability will influence the security of the whole system.

4 Conclusion

We discussed a possible use case for federated identities on the example of accessing a smart grid administration node through an untrusted network in order to gain administrative rights to a person in role service technician. Our approach does not utilize privilege escalation to the role of the service technician; it offers an approach how a natural person can change its role from service technician to gateway administrator. The benefit of that solution is the binding of an electronic identity to a secure communication channel. An authenticated communication channel is established and the authentication protocol is based on the protocol used for the German citizen card. Therefore a new component – the authentication and communication gateway – is introduced which is responsible for provision of the authenticated, secure communication channel. This article discussed the approach on the example of the smart grid environment but it can easily be adopted to other scenarios with the same challenges. We identified that no new threats are introduced pertaining the smart meter gateway and its environment but we identified that the assumption of the malicious service technician must be taken into account. Measures will be required that mitigate this scenario. Currently we are working on the analysis of this scenario in order to provide a full risk assessment of this scenario.

References

[3109-1] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI-TR-03109-1, Version 1.0, Bonn 18.03.2013, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html (Stand: 18.03.2013)

[3110] Bundesamt für Sicherheit in der Informationstechnik (Ed.): BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v2.1_P1pdf.pdf, 2012

[3112-7] Bundesamt für Sicherheit in der Informationstechnik (Ed.): Technical Guideline TR-03112-7 eCard-API-Framework – Protocols Version 1.1.2 28. February 2012,https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/API/api1_teil7_pdf.pdf?__blob=publicationFile, 2012

[BBD+06] Folker den Braber, Gyrd Brændeland, Heidi E. I. Dahl, Iselin Engan, Ida Hogganvik, Mass S. Lund, Bjørnar Solhaug, Ketil Stølen, Fredrik Vraalsen (Ed.): The CORAS Model-based Method for Security Risk Analysis, SINTEF, Oslo 2006, http://www.uio.no/studier/emner/matnat/ifi/INF5150/h06/undervisningsmateriale/060930.CORAS-handbook-v1.0.pdf, 2006

[BDFK11] Jens Bender,Ozgur Dagdelen, Marc Fischlin, Dennis Kügler (Ed.): The PACE-AA Protocol for Machine Readable Travel Documents, and its Security, http://fc12.ifca.ai/pre-proceedings/paper_49.pdf, 2011

[HHR+11] Detlef Hühnlein, Gerrit Hornung, Heiko Roßnagel, Johannes Schmölz, Tobias Wich, Jan Zibuschka: SkIDentity – Vertrauenswürdige Identitäten für die Cloud, http://www.ecsec.de/pub/2011_DACH_SkIDentity.pdf, 2011

[ITEA2] ITEA2 – DIAMONDS: http://www.itea2-diamonds.org/index.html, 2013

[OLSC] OpenLimit SignCubes AG: https://www.openlimit.com/de/produkte/truedentity.html, 2013

[PP] Bundesamt für Sicherheit in der Informationstechnik: Protection Profile for the Gateway of a Smart Metering System, Version 1.2, 18. March 2013 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile, 2013