Handling Role-based Access Control in the Digital Grid

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

Chaitanya Bisale
Energy Management
Siemens AG
Nuremberg, Germany
e-mail: {chaitanya.b}@siemens.com

***Abstract*—The operation of the digital energy grid, as one of the critical infrastructures, has to cope with the need to control of increasingly fluctuating demand and generation of energy, and also to ensure the reliable transmission and distribution of centrally and decentrally generated energy. Control is accomplished by utilizing a communication infrastructure in parallel to the actual power system infrastructure with connections to the physical world by sensors and actuators. In the past, this control communication network was mostly isolated from other communication networks, but is connected more and more with external systems to support innovative cross-system services. Increasingly, this open connectivity exposes the digital grid to cyber attacks. Therefore, access to resources like the communication connections or communicated data needs to be protected to ensure a reliable operation. Legislation and operational best practice guidelines have taken this into account and provide the necessary framework for defining specific communication security requirements. From the technical perspective, different security counter measures exist to cope with the given requirements, but it has to be ensured that these technical means are not only provided technically, but are in fact applied correctly in operation. Usability of security is essential to support the correct application of technical security measures. This paper reviews the requirements for role-based access control (RBAC), as well as currently targeted technical approaches to achieve RBAC in the digital grid. The goal is to provide more insight into the existing application of RBAC mechanisms and to identify gaps for future enhancements. Proposals to address the identified gaps are described, which are intended to be brought to the International Electrotechnical Commission (IEC) to enhance the security standard IEC 62351 for power system automation.**

Keywords–security; user and device authentication; role-based access control; substation automation; digital grid; cyber security; critical infrastructure; IEC 62351

I. INTRODUCTION

Critical Infrastructures (CI) are technical installations that are essential for the daily life of the society and the economy of a country, and also globally. Typical critical infrastructures in this context are the power grid, telecommunication, healthcare, transportation, water supply, just to state a few.

Digital Grids as one example of CI and especially their cyber security has gained more momentum over the last years. The increased threat level becomes visible, e.g., through reported attacks on critical infrastructure, but also through reactions in legislation, which explicitly require specific protection of critical infrastructures and reporting about serious attacks. There is a clear trend towards increased connectivity and tighter integration of systems from Information Technology (IT) in common enterprise environments with the Operation Technology (OT) part of the automation systems in the energy and industrial domains to provide enhanced services. This requires security measures to avoid negative effects of the formerly isolated OT. IT security in this context evolves to cyber security to underline the mutual relationship between the security and physical effects.

Cyber security measures typically comprise technical and organizational measures. Operators of CI need to maintain their systems by complying to an Information Security Management Framework while also coping with regulatory requirements. This requires technical support in the deployment environment. Such technical requirements relate to authentication and access control, or to secure and reliable communication for example. Within this paper, the focus is placed on access control, or more specifically on Role-based Access Control (RBAC).

RBAC is already a proven concept in IT systems. It is realized by many (operating) systems to control access to system resources. RBAC for the power automation environment is already considered in several requirements standards, guidelines, and also in regulatory requirements. Beside the requirements supporting this functionality, technical standards ensuring interoperability have been developed [5][8].

This paper targets the discussion of RBAC in general and focuses on the selected target scenario of the digital grid as depicted in Figure 1 below. Section II provides an overview of requirements from guidelines, standards, and regulations targeting access control specifically. Section III provides an overview of several state-of-the-art approaches for RBAC, while Section IV discusses the basic RBAC concept currently deployed in the digital grid. The identified shortcomings are addressed in Section V with first solution proposals that are intended to be brought to standardization. Section VI concludes the document.

Note that this paper addresses first ideas to tackle identified gaps in RBAC in the Digital Grid domain. Further investigation is necessary.

 ISBN: 978-1-61208-556-2

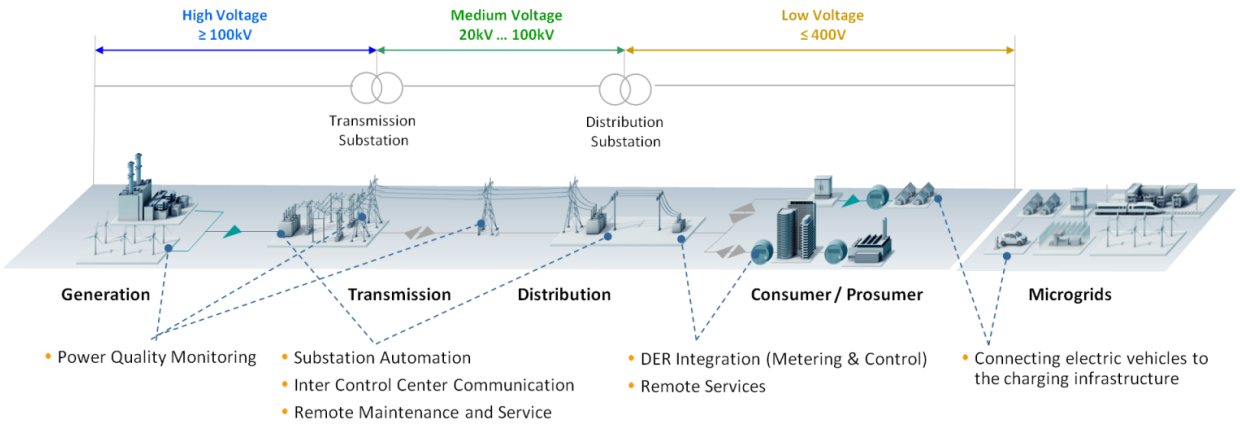

Figure 1. Overview Digital Energy Grid as Example for Critical Infrastructures

II. EXAMPLES OF DOMAIN-SPECIFIC GUIDELINES/STANDARDS/REGULATIONS

As outlined in [1] for secure communication, a variety of security requirements exist for digital grids. An overview of the most relevant standards, guidelines, and regulations is shown in Figure 2 below.

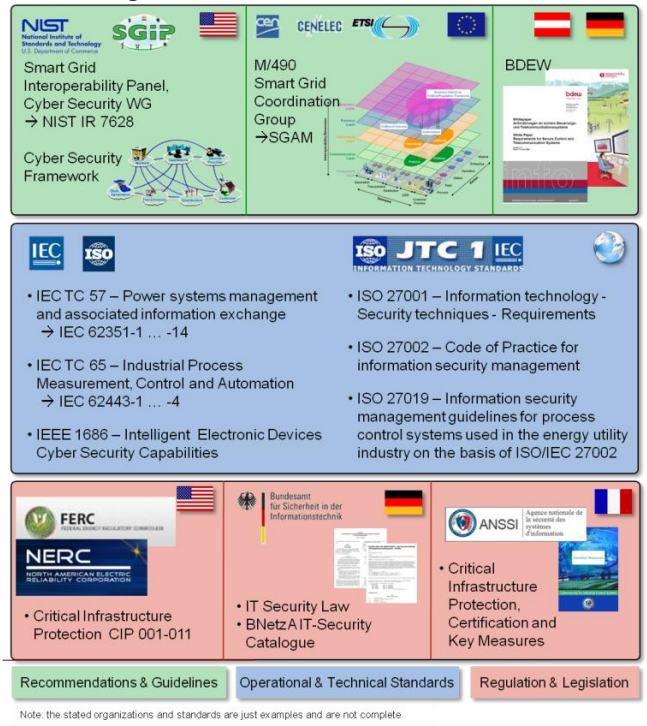

Figure 2. Examples for sources for security requirements for digital grid

Starting from the top in Figure 2, guidelines are available from the National Institute for Standards and Technology (NIST) of the U.S. through the "Guidelines for Smart Grid Cyber Security" in NIST IR 7628 [2] or the Report of the Smart Grid Coordination Group addressing the European Mandate M/490 [3], which explicitly recommend the support of RBAC in the context of system configuration, operation, and maintenance. Specifically for Germany and Austria, the BDEW White Paper [4] guideline has been published, addressing RBAC in the context of user management.

This white paper was one main source for developing ISO 27019:2013 [5] as a domain-specific profile of the Information Security Management System defined in ISO 27002 [6]. Both ISO documents address requirements for an operator regarding the handling of information security and require support for RBAC. Similar requirements can also be found in IEC 62443-2-1 for industrial environments. IEC 62443-3-3 [7] goes one step beyond by specifically defining, which foundational security requirements can be technically addressed with RBAC, without prescribing a specific technical solution. IEEE 1686 [8] is even more specific here, as it defines a minimum number of roles and also the associated rights. The last standard to be mentioned is IEC 62351-8 [9], providing specific technical means for binding RBAC information to entities in access tokens and to utilize them in communication. The latter can already be used to address some of the requirements stated before.

From a regulatory perspective, examples are provided through the American NERC-CIP [10], the German IT-Security Act [11], and the IT security catalogue of the German network regulator group BNetzA, and the French ANSSI [12]. They all require security measures to support reliable grid operations, which are mapped to processes and organizational means, but they also need the technical means to operate the infrastructure appropriately. The following section elaborates technical means to address these requirements.

III. STATE OF THE ART APPROACHES SUPPORTING RBAC

Security administration is simplified through the use of roles and constraints to organize subject access levels. RBAC in general can reduce costs within an organization, as it accepts that changes in roles and responsibilities of (especially) employees occur more frequently than the changes in the rights within roles. The basic idea of RBAC is to define roles according to responsibilities within the business organization. Permissions required to perform the duties of a role are assigned to the respective role. A subject, i.e., typically human user, is assigned roles according to his business responsibilities. This helps to achieve separation of

 ISBN: 978-1-61208-556-2

duty by ensuring that a user is assigned only the roles according to his responsibilities, and possesses only the permissions required to fulfill his duties. Restrictions can be placed to prevent a single subject from being assigned to roles having a conflict of interest. RBAC also includes the concept of temporary roles to realize dynamic separation of duty: Over time, a subject may act in different roles. At any point in time, the subject only possesses the permissions of the currently active role or roles.

The general concept of RBAC is shown in Figure 3, which is the enhanced approach explained in [9]. As shown, the role separates the subject from the permissions. The permissions define certain rights on objects, like read or write operations on specific objects (e.g., files). The role itself bundles a set of permissions, which can be assigned to users. This subject assignment enables separation of duty, which is necessary to also support auditing of actions. Additionally, constraints may further be used to either restrict roles or to enable special handling in situations like emergency cases. Examples of constraints required in digital grids specifically are:

- *Area of Responsibility or scope* allows restricting the effectiveness of an issued RBAC token, e.g., to an organizational unit or a geographical location or area.
- *Operational constraints* allow a local augmentation of the associated rights if the (hosting) object detects or is informed about specific circumstances. As an example, an Engineer may not be allowed to perform certain actions, e.g., on a protection relay, in an emergency case.

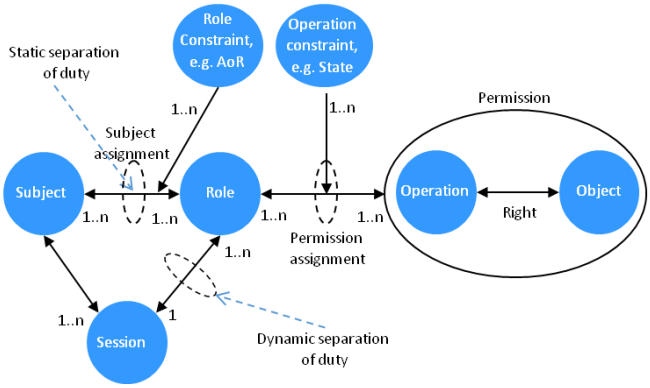

Figure 3. General concept for RBAC

The separation of the assignment of subjects-to-role and role-to-rights enables a flexible and centralized management of subject-to-role assignment that tends to be dynamic. At the same time, it can be combined with a well-defined role-to-permission-assignment that has more static character.

Figure 4 illustrates the concept of RBAC on a user base. In the upper part, the subject-role-right association is shown. Here "Tom" is assigned the role "Engineer". Acting in this role "Tom" is entitled to "view" and "control" objects. Objects may include status values or switching objects. It also shows the dynamic and static assignments between subjects, roles and rights. The example illustrates that granting the right "view" to "Mary" can be added by assigning the role "Engineer" to "Mary" without changing the associated rights on objects.

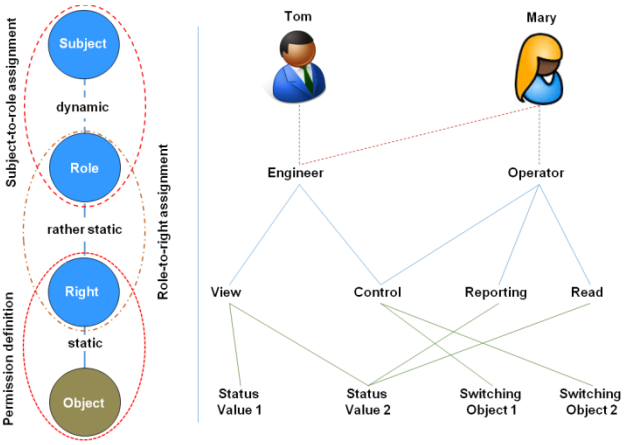

Figure 4. Basic RBAC concept applied in Digital Grids

To allow a subject to act in a distinct role, authentication is often a precondition, ensuring that the subject is who it claims to be and that it is entitled to act in this role. For this there already exist various solutions, often relying on a three-party-model, in which an identity and access server issues some form of security tokens or tickets to provide authorization information. Examples are Kerberos [13], the security assertion markup language (SAML) [14], OAuth 2.0 [15], and OpenID Connect [18]. Also domain specific approaches like X.509 certificate enhancements in IEC 62351-8 [9] for power automation have been standardized, which will be briefly introduced in the following. While they all rely on a security token mechanism, they differ, e.g., in the communication relations for the token exchange (protocols), the token format, the underlying cryptographic algorithms and the target application use cases.

A. *Kerberos*

Kerberos v5, specified in RFC 4120 [13], is a three-party system and protocol to be used for network authentication. In this system there exists a trusted third party, to which all participants authenticate as shown in Figure 5.

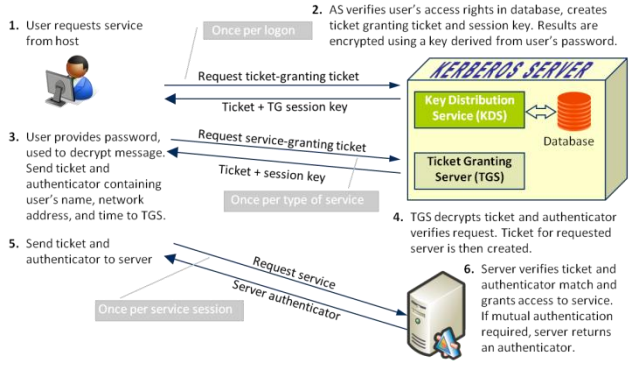

Figure 5. Kerberos authentication and authorization

This trusted third party grants tickets upon request to allow access to specific services or resources. Kerberos relies on symmetric cryptography for the authentication and also the ticket protection and binding and uses ASN.1 for the encoding. Kerberos is widely used and part of common operating system like Windows.

 ISBN: 978-1-61208-556-2

B. Security Assertion Markup Language (SAML)

SAML 2.0 was defined by OASIS in [14] and is an XML based protocol to exchange authentication and authorization information between a client, an identity provider (the SAML server) and the service provider. The SAML server uses so called SAML assertions to provide statements or claims about the client. Three types can be roughly distinguished: authentication, assertions, and authorization. Especially the latter allows realizing RBAC. SAML builds on assertions symmetric and asymmetric cryptography. Hence, SAML assertions are security tokens utilizing XML signatures and XML encryption to protect the contained information. For the authentication at the identity provider, SAML does not require a specific method and thus may be used with username/password combinations or X.509 certificate based authentication or others. SAML is often used in Single-Sign-On solutions and federation scenarios. It may be used also in open authorization (OAuth 2.0) for the token realization, as described in the following subsection.

C. Open Autorization (OAuth 2.0)

The OAuth 2.0 framework is specified in RFC 6749 [15] and defines an authorization method for accessing a resource. Since OAuth 2.0, this framework can be used with various applications and protocols, whereas the original OAuth was bound to the HTTP protocol. OAuth 2.0 also relies on tokens, which are requested by a user agent, issued by an authorization server and verified at the resource server. The tokens may be provided by reference or by value. OAuth 2.0 defines the handling of the security tokens (access token), as well as the format but allows for an own definition of the token content. Beside the pure request of access tokens, a client may request for a token for a specific scope. The supplied tokens are provided according to the bearer model or the proof-of-possession (PoP) or holder of key (HoK) model. Bearer token can be used to get access to an associated resource without demonstrating possession of a cryptographic key. In contrast, the PoP/HoK token model, requires the proof of possession of a corresponding cryptographic key in order to utilize the token, as defined in RFC 7800 [16]. Note that according to [17], plain OAuth 2.0 is intended for authorization. It may support authentication, e.g., in the combination with OpenID Connect (see next subsection). OAuth addresses typical Web-based access scenarios.

D. OpenID Connect

OpenID Connect is a security protocol to offload user authentication from a server hosting a resource to a trusted third party. It is defined by the OpenID Consortium. The core is specified in [18]. It utilizes the OAuth 2.0 protocol flows to obtain ID tokens, which are encoded as JSON web token (JWT, see also [19]). These ID tokens contain assertions about authenticated users from an authorization server. Optionally, access tokens as defined in OAuth 2.0 can be utilized to retrieve asserted user authorization information. OpenID Connect is used for web-based clients and also native clients in a variety of applications.

E. Digital Grid specific X.509 Certificate Enhancements

Another option to support RBAC has been taken in IEC 62351-8 [9] for power system automation. This standard relies on the authentication based on X.509 [20] certificates and corresponding private keys. In digital grids protocols like TLS are applied, which utilize X.509 key material.

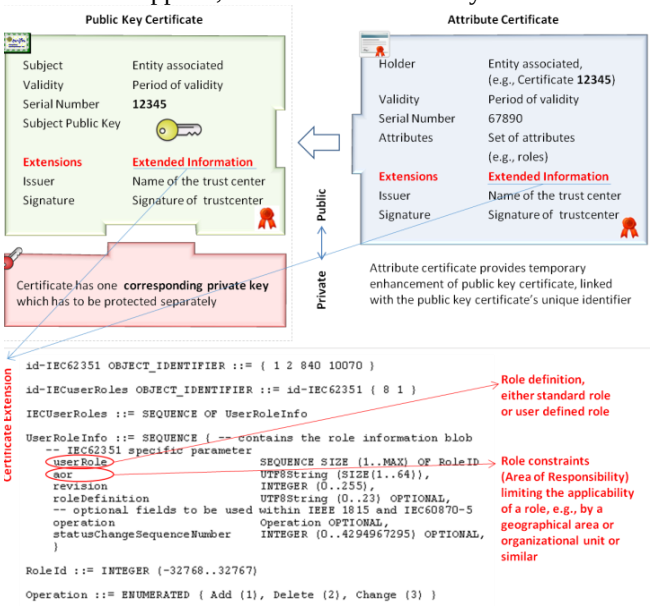

Figure 6. X.509 certificate enhancements (adopted from [9])

IEC 62351-8 leverages the option to enhance the ASN.1 structure of X.509 certificates with a specific extension. This extension carries information about the roles and constraints and can be added to X.509 public key certificates or X.509 attribute certificates as shown in Figure 6. The flexibility of attribute certificates can be leveraged in use cases, in which the user to role association is rather dynamic. User-bound public key certificates typically have a longer validity, while attribute certificates may have a much shorter validity and are only valid in conjunction with the associated public key certificate. Via the corresponding private key it can be proven, that a user may act in a certain role. As this approach is defined as an extension, protocols utilizing X.509 key material can directly leverage the approach. Note that for the token issuer, i.e., a certification authority, enhancements are likely to be necessary to support the RBAC extension.

IV. RBAC SPECIFICS IN THE DIGITAL GRID

As shown in Figure 6, for power systems supporting IEC 62351-8, an extension for carrying role information in X.509 certificates has been standardized, which may belong to a user, a device, or an application. This approach can be directly applied in use cases, in which protocols utilizing X.509 key material like Transport Layer Security (TLS, RFC 5246) are used. Moreover, this approach also supports application layer authentication and authorization, which can be required, if the communication link spans multiple hops. In both cases, beside the certificate validation it also involves the verification of the relying party that the applicant entity is entitled to utilize the X.509 certificate by checking the

 ISBN: 978-1-61208-556-2

possession of a corresponding private key. This involves asymmetric cryptography for digital signature generation and verification. Compared to pure symmetric cryptography based approaches, this is costly. Hybrid methods addressing this establish a session, in which a X.509 certificate is involved in the negotiation of a symmetric session key, which is used in (different) security services to protect the session. The whole session is then executed in the context of a specific user, having an assigned role. As substation automation protocols like IEC 61850 utilize a session based approach for the transport or the application connection, this concept is immediately applicable. Note that for the generation of a digital signature, access to the private key is necessary. This private key needs to be protected accordingly, as it is necessary as proof, that the user is authorized to act in a certain role via the corresponding certificate. For devices or applications this protection may be achieved with secured memory or specific hardware modules that allow operation but not exporting of the private key. For a service technician, this protection will most likely be offered by a security token like a smart card or similar.

Current installations in digital grids often utilize a different concept by performing a local form of RBAC depending on the environment. Communication between entities in a control center for instance is performed based on either locally or centrally associated users to permission groups. This ensures that the local execution of commands can only be done if the appropriate permissions are granted, but does not necessarily provide a remote entity to verify who is going to perform a dedicated operation. This information may be necessary for audit purposes, and a complete audit trail would require having the complete chain from the remote point to the executing entity to comprehend the specific action. The approach described in IEC 62351-8 supports also a local audit trail through the capability to connect identity and access information in the access token. In substations, the local physical access may already be sufficient to get access to communicating entities.

While the approach utilizing X.509-based access tokens has its merits, it is not immediately applicable in all use cases. Also, one has to keep in mind that the infrastructure of the power grid has grown over many years and that the lifetime of installed devices is long, reaching 20-25 years. Two examples are used here to show potential shortcomings.

1. In substation automation, field devices often feature a local human-machine-interface (HMI) handled by a service technician. These field devices typically do not feature a local interface for a smart card, but only a small screen and a number keyboard pad allowing entering a personal identification number (PIN) or a passcode. Hence, RBAC information cannot be provided directly, but may be fetched by the field device..
2. As outlined in [21] web-based services based on XMPP are specified for the integration of decentralized energy resources (DER) into the digital energy grid. These services may leverage already existing technologies that support RBAC, such as OpenID Connect or OAuth 2.0 instead of building a parallel infrastructure for handling X.509 based RBAC.

Proposals are discussed in the next section for both examples.

V. PROPOSALS FOR RBAC ENHANCEMENTS

In the following, solutions are proposed for handling RBAC in legacy devices and in upcoming web-based applications building on consistent RBAC information. The real-world applicability of these proposals has to be evaluated.

A. Enabling RBAC on local HMI of legacy devices

As noted, a variety of devices may not feature an appropriate interface to interact with a X.509 credential of a service technician. Despite the missing local interface, these devices may be enabled to work with the X.509 credentials. One approach to be used here is the fetching of the X.509 credential from a trusted third party utilizing the local login and password of the service technician. Once the service technician provides his login credentials, the field device may query a central repository for the corresponding X.509 certificate also providing the login credentials for verification. This X.509 certificate needs to be enhanced with the RBAC extension defined in IEC 62351-8 and can then be verified by the field device. The verification of the corresponding private key is neglected here, as the X.509 certificate is rather used as an assertion by the third party. By already relying on X.509 certificates with RBAC extensions, this approach may be used as a migration path without involving device local asymmetric cryptographic operations.

The central repository may generate the credentials on demand or they may be provisioned with the X.509 certificates. In either case, the certificates may have a rather short lifetime, which simplifies the revocation handling on the field device. This approach has been considered in IEC 62351-8 with the focus on Lightweight Directory Access Protocol (LDAP) [22]. While LDAP support is typically available in control centers, it is not too widespread in substations. Protocols like the Remote Authentication Dial In User Service (RADIUS) [23] are rather used.

If one would want to use RADIUS out-of-the-box, access information can be provided as RADIUS allows extensions using vendor specific attributes. The drawback is the limitation of this field to effectively 250 bytes. As X.509 certificates are typically larger (even if used with shorter ECDSA key instead of the larger RSA key), this field can only be used to transmit a subset of the RBAC information. A necessary subset is proposed as:

```
BEGIN-VENDOR IEC
  ATTRIBUTE RoleID          1  integer
  ATTRIBUTE roleDefinition  2  string
  ATTRIBUTE AoR             3  string
  ATTRIBUTE revision        4  integer
  ATTRIBUTE ValidFrom       5  string
  ATTRIBUTE ValidTo         6  string
END-VENDOR IEC
```

The semantic of the parameter would be the same as in IEC 62351-8 and would support also a later processing of other token formats containing the same information. As RADIUS has some shortcomings, like missing message integrity or confidentiality or the application of the weak

MD5 hash algorithm, it is recommended to use TLS according to [24] to protect the message exchange between field devices and the RADIUS server. As stated above, this approach is intended to support migration in restricted use cases without changes or enhancements to RADIUS itself.

B. Supporting RBAC in web service scenarios

Integration of DER into the digital grid will be supported with IEC 61850-8-2 [25]. Here XMPP is used to enable the connection of field devices (DER controller) to the control site using a publish-subscribe infrastructure. While in [25] the application of session-based end-to-end RBAC in conjunction with X.509 credentials is enabled, further services offered by the publish-subscribe infrastructure may utilize a message-based approach and may require an end-to-middle RBAC approach. Applications could be presence monitoring, notification, or discovery of resources, which may be utilized by a virtual power plant operator. Here the application of OpenID Connect is envisioned, which would need to map the existing access token information to the access token format in the OpenID Connect context.

VI. Conclusions and Outlook

This paper described the general concept of role-based access control and its usage within the digital energy grid. Ongoing standardization work for using RBAC for energy control networks has been described. This paper discussed role-based access control in the digital grid, starting from an analysis of requirements in regulation and standardization. It provided an overview about existing technical approaches from other domains and discusses the specifics of the digital grid, the target domain. Two exemplary gaps have been identified for the incorporation of legacy devices and for future DER devices for which first solution sketches have been provided. The feasibility of these proposals is to be investigated from a security assessment point of view, as well as from an implementation point of view. Hence, at the time of writing, a proof-of-concept implementation was not yet available, but is envisioned as the next consequent step.

References

[1] S. Fries and R. Falk, "Ensuring Secure Communication in Critical Infrastructures," Proceedings IARIA Energy 2016, June 2016, ISBN: 978-1-61208-484-8, page 15-20, https://thinkmind.org/download.php?articleid=energy_2016_1_30_30060, [retrieved: March. 2017].

[2] NIST IR 7628, "Guidelines for Smart Grid Cyber Security," Sep. 2014, http://dx.doi.org/10.6028/NIST.IR.7628r1, [retrieved: March. 2017].

[3] SGIS "Smart Grid Information Security," Dec. 2014, ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf, [retrieved: March. 2017].

[4] BDEW White paper "Requirements for Secure Control and Telecommunication Systems," BDEW, Feb. 2015

[5] ISO TR 27019: Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002, March 2013

[6] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, June 2005.

[7] IEC62443-3-3:2013, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels," Edition 1.0, August 2013.

[8] IEEE 1686, "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities," Dec. 2013.

[9] ISO/IEC 62351-8, "Role-based access control for power system management," June 2011.

[10] NERC, North American Reliability Corporation, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, [retrieved: March. 2017].

[11] German IT Security Law, July 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf, (German), [retrieved: March. 2017].

[12] ANSSI Technical Note, Recommandations de sécurité concernant l'analyse des flux HTTPS, October 2015, http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_TLS_NoteTech.pdf (French) [retrieved: March. 2017].

[13] C. Neuman, T. Yu, S. Hartman, and K. Raeborn, "The Kerberos Network Authentication Service (V5)," RFC 4120, July 2005, https://tools.ietf.org/html/rfc4120, [retrieved: March. 2017].

[14] S. Cantor, J. Kemp, R. Philpott, and E. Maier, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, [retrieved: March. 2017].

[15] D. Hardt, "The OAuth 2.0 Authorization Framework," RFC 6749, October 2012, https://tools.ietf.org/html/rfc6749, [retrieved: March. 2017].

[16] M. Jones, J. Bradley, H.Tschofenig., "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)," RFC 7800, April 2016, https://tools.ietf.org/html/rfc7800, [retrieved: March. 2017].

[17] J. Richter, "User Authentication with OAuth 2.0," https://oauth.net/articles/authentication/, [retrieved: March. 2017].

[18] J. Bradley et al., "OpenID Connect Core 1.0 incorporating errata set 1," November 2014, http://openid.net/specs/openid-connect-core-1_0.html, [retrieved: March. 2017].

[19] M. Jones et al., "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants," May 2015, https://tools.ietf.org/html/rfc7523, [retrieved: March. 2017].

[20] D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, May 2008, https://tools.ietf.org/html/rfc5280, [retrieved: March. 2017].

[21] S. Fries, R. Falk, H. Dawidczak, and T. Dufaure, "Decentralized Energy in the Smart Energy Grid and Smart Market – How to master reliable and secure control," International Journal on Advances in Intelligent Systems, vol 9 no 1& 2, ISSN: 1942-2679, pg. 65-75, Sep. 2016.

[22] J. Sermersheim, "Lightweight Directory Access Protocol (LDAP): The Protocol," RFC 4511, June 2006, https://tools.ietf.org/html/rfc4511, [retrieved: March. 2017].

[23] C. Rigney et. al., "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000, https://tools.ietf.org/html/rfc2865, [retrieved: March. 2017].

[24] S. Winter et al, "Transport Layer Security (TLS) Encryption for RADIUS," RFC 6614, May 2012, https://tools.ietf.org/html/rfc6614, [retrieved: March. 2017].

[25] ISO 61850-8-2: Communication networks and systems for power utility automation, Part 8-2: Specific Communication Service Mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP), Work in Progress

 ISBN: 978-1-61208-556-2