Role-based Access Control in the Digital Grid – A Review of Requirements and Discussion of Solution Approaches

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*—Critical infrastructures are increasingly under investigation regarding the reliable operation and resilience to ensure their provisioning of essential services to the citizens. One example for such critical infrastructures is the digital energy grid. It targets the control of increasingly fluctuating demand and generation of energy. Besides generation also the path to the final consumer has to be taken into account, resulting in the need for securing 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. The connection between both worlds is provided by sensors and actuators. In the past, this control communication network was mostly isolated from other communication networks, but today it is getting connected increasingly with external systems to support innovative cross-system services. This surge in connectivity also exposes the digital grid to cyber attacks. Therefore, access to resources like accumulated measurement information or control data needs to be protected to ensure a reliable operation. Legislation and operational best practice guideline activities have taken this into account and meanwhile 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. However, it has to be ensured that these technical means are not only provided technically, but are in fact applied correctly in operation. 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. Typical critical infrastructures in this context are the power grid, telecommunication, healthcare, transportation, water supply, just to state a few. Power system and communication networks even span across country borders, thereby are of multinational priority.

Digital grids, which are constantly a target of security investigations and enhancement as outlined in [1][2], are one example of CI. 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. Additionally, IT and OT environments have different characteristics in management and operation, which led to distinct domain specific security requirements in the past. This has to be taken into account when designing interconnected cyber-physical energy systems.

Cyber security measures typically are technical and organizational in nature. Operators of CI need to maintain their systems by complying with 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 between different vendor's products and solutions have been developed.

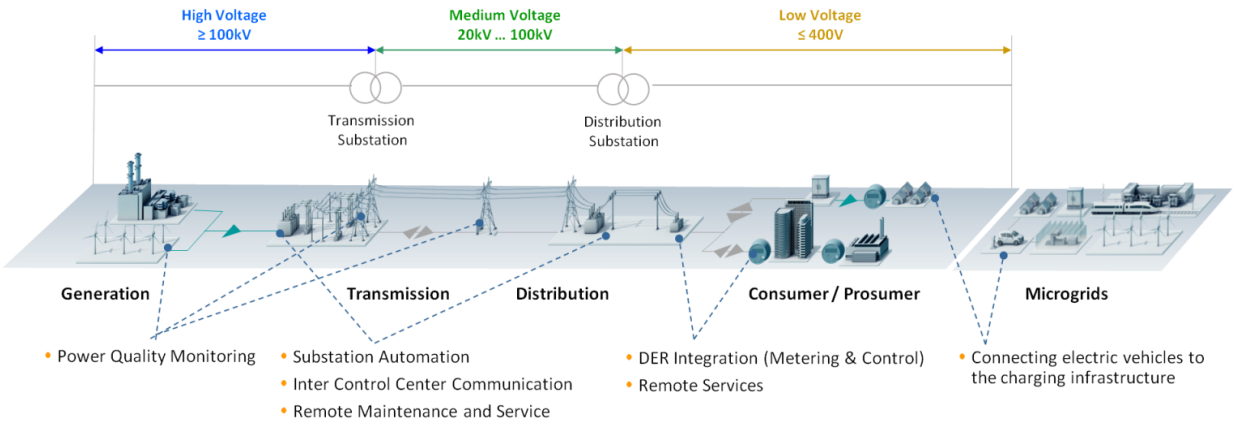

Figure 1. Overview Digital Energy Grid as Example for Critical Infrastructures

This contribution investigates into RBAC in general and specifically on the application in 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 describes a realization example for the proposed migration approach. Section VII investigates further identified challenges when integrating RBAC, while section VIII 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.

II. Examples of Domain-Specific Guidelines/Standards/Regulations

IT security in communication infrastructures is not a new topic. It has been addressed specifically in office IT environments for years. Although there are some commonalities through the convergence of networks of IT and OT, specifically regarding the utilized communication protocols and networks, there are some large differences in the management and operation of these infrastructures as seen in Figure 2 below.

	Digital Grid	Office IT
Protection target for security	Generation, transmission, distribution	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Can be critical	Delays accepted
Physical Security	Very much varying	High (for IT Service Centers)
Application of patches	Slow / restricted by regulation or certification	Regular / scheduled
Anti-virus	Hard to deploy, white listing	Common / widely used
Security testing / audit	Increasing	Scheduled and mandated

Figure 2: Comparison IT/OT management and operation

These differences in management and operation of the IT systems consequently lead to different security requirements as outlined in Figure 3.

	Digital Grid	Office IT
Security Awareness	Increasing	High
Security Standards	Under development, regulation	Existing
Confidentiality (Data)	Low – medium	High
Integrity (Data)	High	Medium
Availability / Reliability (System)	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	Medium to High	Medium

Figure 3: Comparison IT/OT high level security requirements

As outlined in [2] 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 4 below.

As visible 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 [3] or the Report of the Smart Grid Coordination Group addressing the European Mandate M/490 [4] and the report of the successor activity, the Smart Energy Grid Coordination Group (SEG-CG) [5], which explicitly recommend the support of RBAC in the context of system configuration, operation, and maintenance. In particular, the last referenced document from the SEG-CG explicitly addresses the authentication and authorization of users and processes in the context of substation automation.

Specifically for Germany and Austria, the BDEW White Paper [6] guideline has been published, addressing RBAC in the context of user management as applied to operations of energy and water utilities. This white paper was one main source for developing ISO 27019:2013 [7] as a domain-specific profile of the Information Security Management System defined in ISO 27002 [8]. 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 [9] 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 [10] 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 [11], 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.

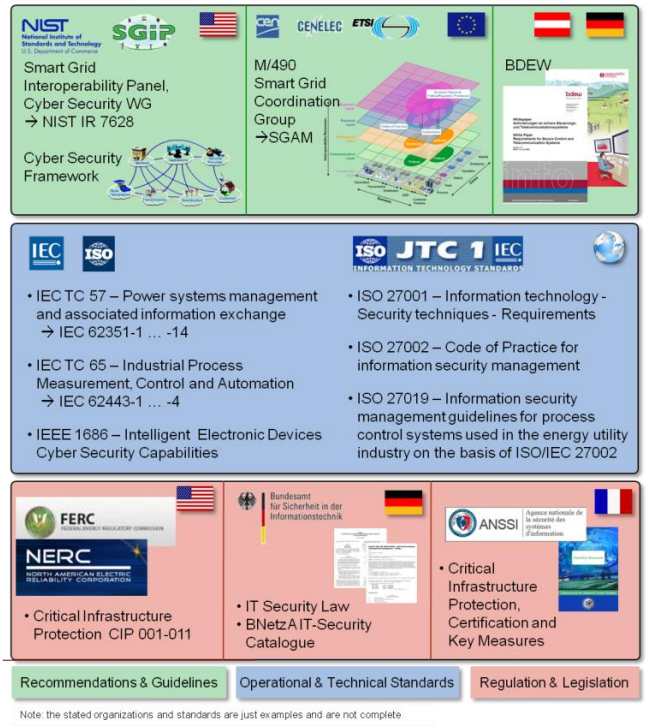

Figure 4. Examples for sources for security requirements for digital grid

From a regulatory perspective, examples are provided through the American NERC-CIP [12], the German IT-Security Act [13], and the IT security catalogue of the German network regulator group BNetzA, and the French ANSSI [14]. They all require security measures to support reliable grid operation, which are mapped in the first place to processes and organizational means, but finally, these need to be supported by appropriate technical means to operate the infrastructure appropriately. The following section elaborates technical means to address these requirements focusing on authentication and authorization to achieve access control.

III. Role Based Access Control – RBAC

This section provides an overview about the RBAC concept in general followed by an investigation into different technical approaches realizing this general concept in different ways.

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 (but may also be an application or software process or an intelligent electronic device - IED), is assigned roles according to his business responsibilities. This helps to achieve separation of 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 5, which is the enhanced approach explained in [11]. 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, or a specific communication network area (subnet).
- *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. Note that these constraints are typically defined and handled in a device-centric manner and may not be included in the subject specific role assignment.

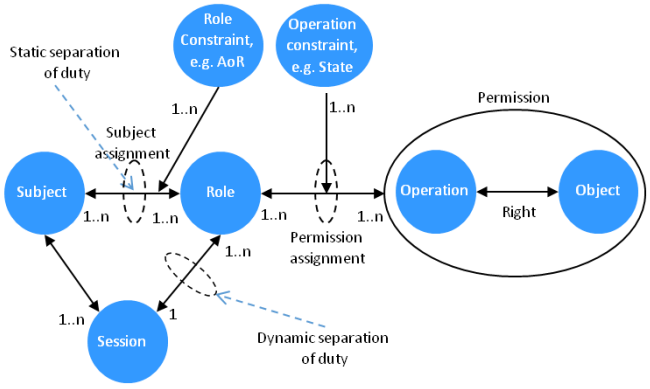

Figure 5. General concept for RBAC

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 6 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.

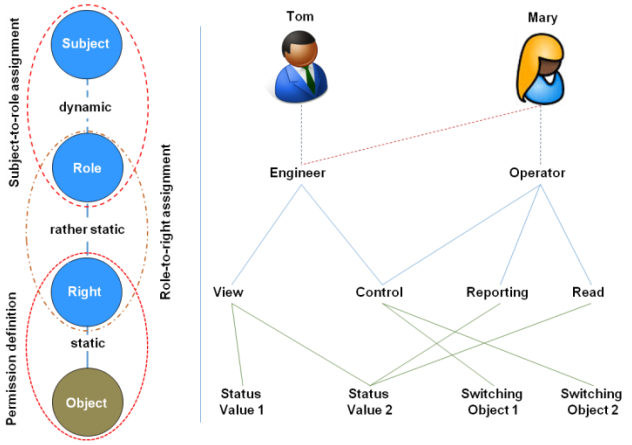

Figure 6. Basic RBAC concept applied in Digital Grids

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 [15], the security assertion markup language (SAML) [16], OAuth 2.0 [17], and OpenID Connect [20]. Also domain specific approaches like X.509 certificate enhancements in IEC 62351-8 [11] 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 [15], 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 7. Kerberos is widely used in different operating systems to allow access to network domain services or to realize single-sign-on.

As shown, the 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. The Key Distribution Server is responsible for the user authentication and the granting of service specific tickets. These tickets provide an authorization of the user to utilize the services. The tickets also allow for the distribution of a session key to the user and the service to secure the service access. This is enabled by another symmetric key, which is a long term key shared between the KDC and the service component. User authentication is also done using symmetric shared secrets, like a username and password. Besides this there also exist enhancements to allow for a certificate based user authentication.

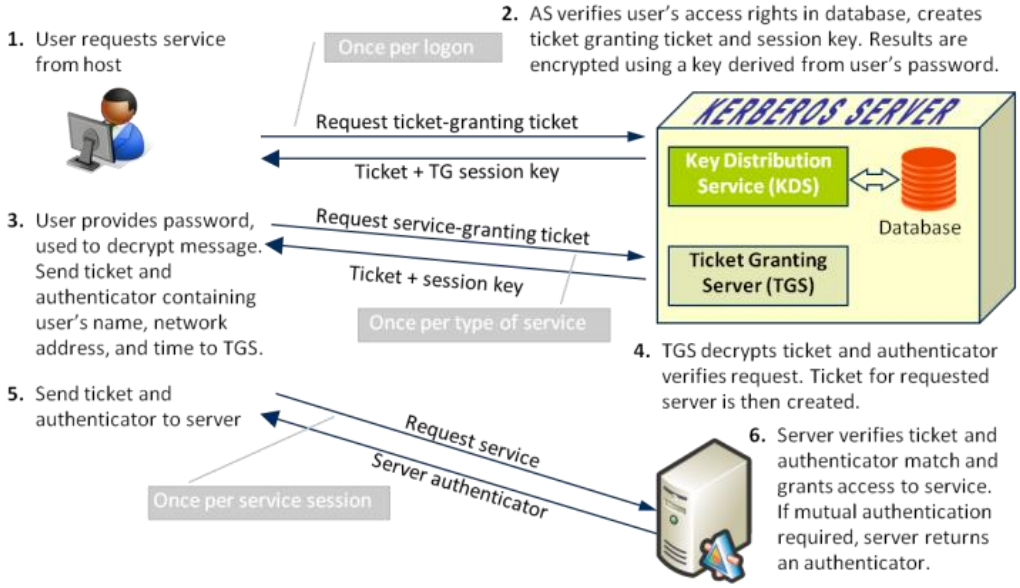

Figure 7. Kerberos authentication and authorization

B. Security Assertion Markup Language (SAML)

SAML 2.0 was defined by OASIS in [16] 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 [17] 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 [18]. Note that according to [19], plain OAuth 2.0 is intended for authorization. It may support authentication, e.g., in the combination with OpenID Connect (see the 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 [20]. It utilizes the OAuth 2.0 protocol flows to obtain ID tokens, which are encoded as JSON web token (JWT, see also [21]). 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. RADIUS

Remote Authentication Dial In User Service (RADIUS) [22] is a protocol used to realize access control of users and devices to networks. The protocol itself is typically applied for the communication between an authenticator and a repository performing the actual authentication.

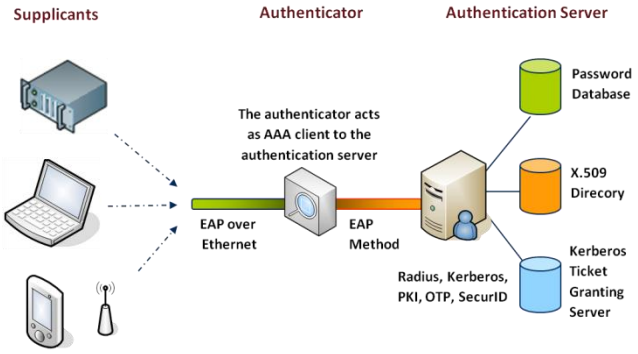

Figure 8. IEEE 802.1X Network Access Authentication

The RADIUS protocol may also be used in conjunction with the Extensible Authentication Protocol (EAP, IETF RFC 3748 [23]) to allow for direct entity authentication. EAP itself describes a container, which in turn allows for different authentication methods. Depending on the method chosen, is allows for authentication and also key establishment. This approach allows transmitting the authentication information from the accessing entity via the access node to the RADIUS server for verification. This approach is utilized for network access authentication in the context of IEEE 802.1X as shown in Figure 8.

F. Digital Grid specific X.509 Certificate Enhancements

Another option to support RBAC has been taken in IEC 62351-8 [11] for power system automation. This standard relies on the authentication based on X.509 [24] certificates and corresponding private keys. In digital grids protocols like TLS are applied, which utilize X.509 key material.

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 9.

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.

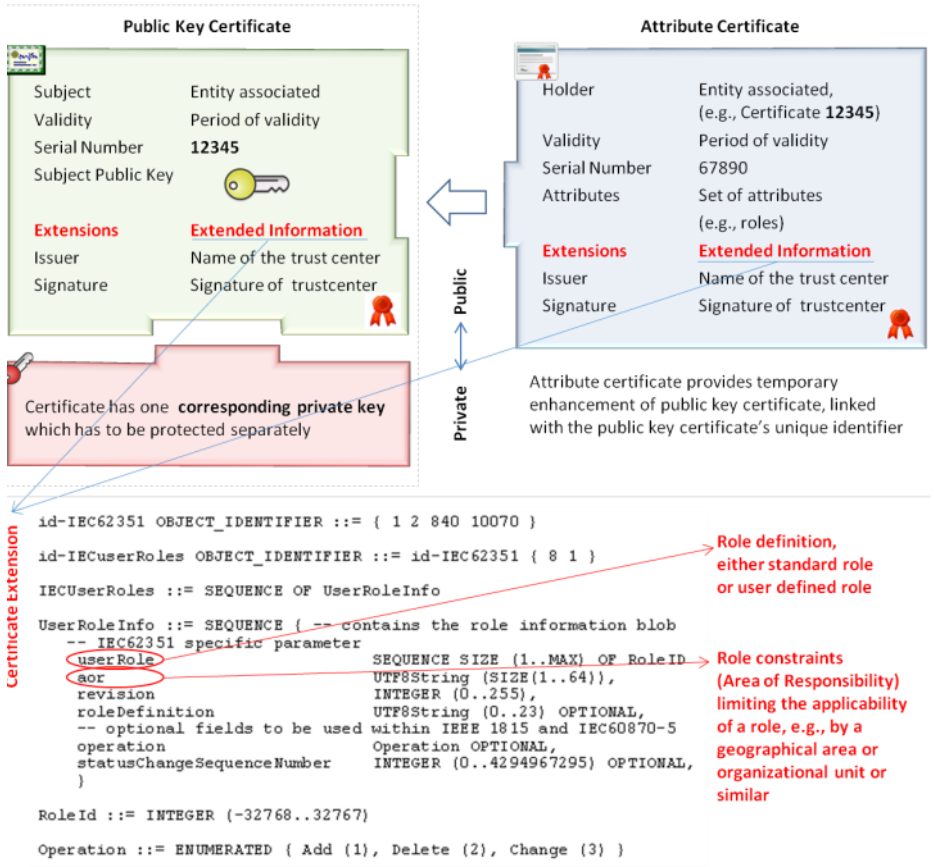

Figure 9. X.509 certificate enhancements (adopted from [11])

Besides the definition of the access token format as extension to X.509 certificates, the standard IEC 62351-8 already defines a set of mandatory roles and associated rights as shown in Figure 10.

Value	Role \ Right	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7...32767>	Reserved	For future use of IEC defined roles.										
<-32768...-1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

Figure 10. IEC 62351-8 defined roles and associated rights [11]

The definition of these roles ensures a minimum level of interoperability for different vendors' products.

IV. RBAC SPECIFICS IN THE DIGITAL GRID

As shown in Figure 9, 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 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 [25] 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 to handle 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. The goal for the proposals is the enabling of a smooth migration for the enabling of RBAC from existing environments not supporting certificate-based RBAC to a public key certificate or attribute certificate-based RBAC environment. The approach taken relies on a minor reduced data structure, as defined for certificate-based RBAC and transported in a different way for the migration case. This reliance enables to establishment of processes and interfaces, which serve for both, legacy and new equipment.

A. Enabling RBAC on local HMI of legacy devices

As noted, a variety of field 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) [26]. While LDAP support is typically available in control centers, it is not too widespread in substations. Mechanisms like the Remote Authentication Dial In User Service (RADIUS) [22] 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 material instead of the larger RSA key material), 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 kept the same as in IEC 62351-8 and therefore also supports 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 [27] 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 [28]. Here XMPP is used to enable the connection of field devices (DER controller) to the control site using a publish-subscribe infrastructure. While in [28] 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. REALIZATION EXAMPLE

In order to support power system operators in taking their first step towards centrally managed RBAC in substations that applies not just to the station level (as is typically the case today) but also to the field level, technology vendors providing field equipment, such as RTUs and protection relays, should consider offering RADIUS-based centralized user management and RBAC as currently proposed for standardization in IEC 62351-8. This has the clear advantage that operators can leverage their existing RADIUS infrastructure (or install afresh with reasonable effort) in their substations and can utilize the standardized vendor-specific attribute schema to centrally assign roles and other constraints for each of the users.

As a second migration step towards centralized user management, operators may couple the RADIUS user management with substation-spanning LDAP infrastructure, which is typically realized using Windows Active Directory services. This approach enables operators to choose between a bottom-up centralization of user management and RBAC, starting first with the critical substations and then moving a level higher to incorporate multiple substations with the LDAP-RADIUS coexistence. Alternatively, a top-down approach could also be realized, with a centralized LDAP-based user management that is made available to field devices in substations over RADIUS. Both approaches do not require supporting LDAP directly on the field device but only the capability to handle the RBAC information received via RADIUS. This is seen as advantage specifically for devices with limited resources or for field devices which are in the field for a long time already. A consequent subsequent step over time would be to employ a purely LDAP-based RBAC infrastructure from the substation-spanning level down to the field device level in order to benefit from a more secure and manageable operation as described in the previous section.

Figure 11 and the following description depict a realization example for a migration path. Integrating into this centralized user management infrastructure, field device vendors can support RBAC for user interactions in substations as illustrated in figure 6 with a user-IED interaction, using the pull-model described in IEC 62351-8. When a user initiates an interactive session with the IED, his username and password are collected and sent to the IED (1).

The IED, capable of centralized user management authenticates the user with the central user management system, which may be a RADIUS or LDAP server (2). Depending on whether the user-provided credentials could be successfully verified, the central user management system responds with an authentication success or failure message to the IED (3). Also in this step, if authentication is successful, the server either additionally sends the role / authorization information in its response to the IED (as with RADIUS) or the IED retrieves this information itself from the server (as with LDAP.) The IED accordingly informs the user of the authentication status (4) and creates a new session for the user with the required authorization level and permits the user to interact with it (5). From this point on, the central user management server is no longer involved in the logged-in user's interactions with the IED.

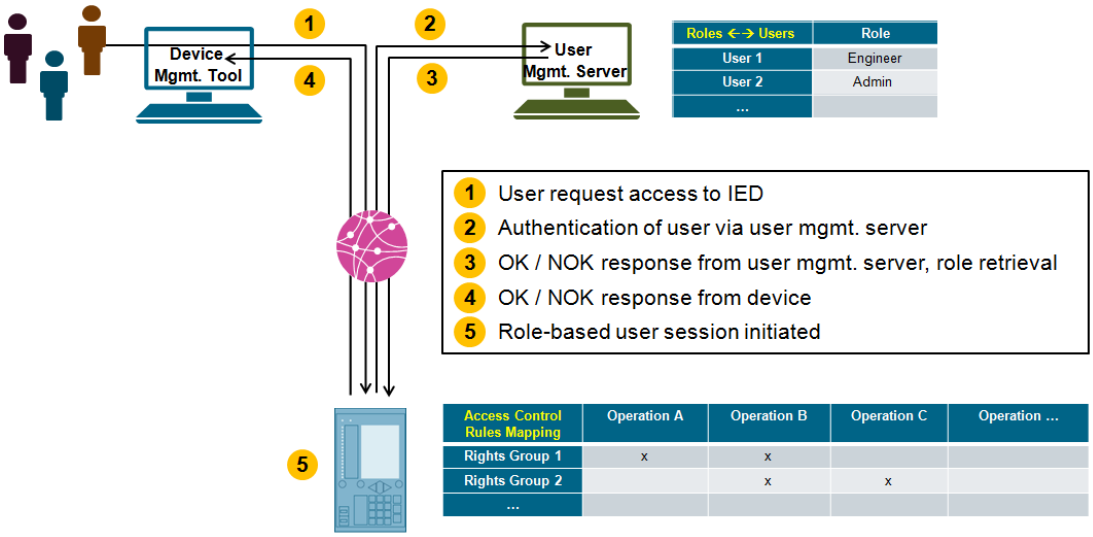

Figure 11. Central user management and RBAC as per IEC 62351-8

VII. Further identified RBAC challenges

Beside the stated solution approaches for binding RBAC information bound to a communication session and supporting migration from existing environments towards certificate supported RBAC, there are further challenges for the integration of a system spanning and vendor independent RBAC solution. These challenges relate to:

1. User- to-role assignment
   Currently, there is a heterogeneous landscape of options available to assign roles to users, which strongly depends on the target environment and on the operator assigning the roles. As in the case of information RBAC information transmission, it is expected to provide migration options between the different approaches. This is directly related with the next challenge.
2. Role-to-right assignment
   As shown in Figure 9 before, IEC 62351-8 already defines a set of mandatory roles. While these roles are intended to ensure a minimum level of interoperability, they are likely to be not flexible enough for all deployments, as an operator may have an own definition of roles and associated rights to be used. To enable a system-wide application of operator defined roles, an exchange format is necessary to describe the role to right association. This issue has also been recognized in standardization, which currently discusses the application of the eXtensible Access Control Markup Language (XACML, [29]) file format and syntax to address this.
3. Right-to-data object assignment
   The last challenge identified relates to the right to data object assignment. This is necessary to have the same interpretation and granularity of actions performed by a role on a component.

VIII. Conclusions and Outlook

This paper discusses role-based access control in the digital grid, starting from an analysis of requirements in regulation, standardization, and guideline activities. It provided an overview about existing technical approaches from other domains and discusses the specifics of the digital grid, the target domain. Feasibility of the migration of existing deployments using legacy devices to a standardized RBAC approach over multiple evolutionary steps has been shown. From an implementation and market adoption point of view, an interoperable vendor-neutral operation for central user management and RBAC according to IEC 62351-8 is yet to be seen, given the extremely hybrid and generation-spanning installed base of power system automation technologies in use today. The proposals made in this paper are intended to address these challenges in an incremental manner, leveraging existing infrastructure and paving the way for a sustainable, secure and manageable infrastructure of the years to come. The outlined proposal has been adopted by IEC for a revision of the currently revised standard IEC 62351-8 to better cope with the migration of existing installations to a future certificate supporting RBAC infrastructure. For this proposal a realization example has been discussed outlining a possible migration from RBAC in an existing environment utilizing the RADIUS protocol to a (user) certificate supported RBAC. Besides the discussion of solutions for identified integration problems also further challenges have been identified. This shows that further investigation and technical development is necessary to cope with all facets of a system spanning RBAC.

References

[1] S. Fries, R. Falk, and C. Bisale, “Handling Role-based Access Control in the Digital Grid,” Proccedings IARIA Energy 2017, ISBN: 978-1-61208-556-2, pp. 27-32, https://thinkmind.org/download.php?articleid=energy_2017_2_20_30024, [retrieved July 2017].

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

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

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

[5] SEG-CG “Cyber Security and Provacy,” Feb. 2017, ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CyberSecurity-Privacy-Report.pdf, [retrieved: July 2017].

[6] BDEW White paper “Requirements for Secure Control and Telecommunication Systems,” BDEW, February 2015.

[7] 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.

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

[9] 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.

[10] IEEE 1686, “IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities,” December 2013.

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

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

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

[14] 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].

[15] 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].

[16] 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].

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

[18] 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].

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

[20] 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].

[21] 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].

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

[23] B. Aboba et. al., "Extensible Authentication Protocol (EAP)", RFC 3748, https://tools.ietf.org/html/rfc3748, [retrieved: March 2017].

[24] 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].

[25] 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, pp. 65-75, September 2016.

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

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

[28] 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.

[29] eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard, January 2013, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html, [retrieved: July. 2017].