Distributed Intelligence for Cost-Effective and Reliable Distribution Network Operation

Deliverable (D) No: 11.3

Role-based access, anonymization, and security concepts for the comprehensive Smart Grid dashboard system

Author: OFFIS

Date: 03.02.2016

Version: 3.0

www.discern.eu

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 308913.

Title of the Deliverable	Role-based access, anonymization, and security concepts for the comprehensive Smart Grid dashboard system

WP number	WP title	WP leader
11	Methodologies for reusing and comparing information about Smart Grid projects	OFFIS
Task title	T11.3 Role-based access, anonymization, and security concepts for the comprehensive Smart Grid dashboard system	

Main Authors	Rafael Santodomingo/ OFFIS Maike Rosinger / OFFIS Mathias Uslar / OFFIS
Project partners involved	Raúl Bachiller / IBDR Lars Nordström/ KTH Carmen Calpe/ RWE Sarah Rigby/ SSEPD Miguel García Lobo / UFD Dag Wästlund / VRD

Type (Distribution level)
■ PU, Public
☐ PP, Restricted to other program participants (including the Commission Services)
☐ RE, Restricted to other a group specified by the consortium (including the Commission Services)
☐ CO, Confidential, only for members of the consortium (including the Commission Services)

Status
☐ In Process
☐ In Revision
■ Approved

Further information	www.discern.eu

Executive Summary

During the last decades large volumes of valuable data on electricity power systems (such as network models, ICT architectures, and technical solutions) have been generated by numerous European R&D Smart Grid projects. In addition to the increasing needs of data, the complexity of administration and managing of user rights is becoming more and more complex. It is one of the most important challenges in managing and sharing networks data.

With the upcoming paradigm change in daily business for traditional DSO and TSO operations; taking the smart grid viewpoint, complexity for the needed solutions is introduced by the new ICT applications – but also, ICT can provide meaningful tools to properly deal with the emerging complexity from a project management perspective.

In WP 11, DISCERN provides a meaningful web-based tool concept which shall be used alongside the defined and implemented tools during DISCERN in the very future. The schematic results from DISCERN set the basis for creating a web-based project management tool that aims at re-using Smart Grid data from both field trials and simulations by (European) Smart Grid projects, facilitating the re-use of existing SG solutions, comparing existing and future Smart Grid projects and, thus, enabling the integration of real world trials and simulations.

In this deliverable D11.3 “Role-based access, anonymization, and security concepts for the comprehensive Smart Grid dashboard system” concepts are presented for addressing issues directly with privacy and security of the data that will be stored in the comprehensive Smart Grid data repository. While D11.1 “Functional description of the comprehensive Smart Grid data repository” provides the functional viewpoint for the dashboard tool from a SGAM point-of-view, this deliverable focuses and the rights management from the user perspective, addressing the cross-cutting issue of information security as an important facet of the overall solution to be implemented. User access rights to process data as well as historical data is one of the most important ISMS topic to be addressed in modern IT operations. While other deliverables in DISCERN focused on the Operational Technologies (OT) part, the document specifically deals with the aspect of information technology (IT) security, and, thus, is limited to the scope of addressing the access to the data stored in the dashboard concept from WP 11. While DISCERN sets the basis for tools and methodologies, it also created the dashboard specification to settle a web-based tool as a portal solution to fully integrate Smart Grid sites and their stakeholders such as planning and operation experts, ICT& Standards specialists, and hardware/software simulation labs. This specification shall be further evaluated on and be implemented. This document provides an overview on how role-based access as a security access paradigm is applied in the very context of information security management systems (ISMS). We define the concept of Role-based Access Control in the context of the dashboard and provide an implementation and governance guideline in the very context of the dimensions working with data, function calls, roles for various users and technical process requirements for multi-user environments. The deliverable takes a generic approach to properly assess read, write and modify rights to the various actors from D11.1 and D11.2 and, thus, provides a governance blue-print when implementing the tool.

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

Table 1 Acronyms

ACS	Access data about communication protocols and standard data models
ATS	Access technical reports on Smart Grid cyber security
CIM	Common Information Model
CKP	Calculate Key Performance Indicators
D	Deliverable
DSO	Distribution System Operator
ETSI	European Telecommunications Standards Institute
GUI	Graphical User Interface
IEC	International Electrotechnical Commission
IOP Tool	Interoperability Tool
ISO	International Organization for Standardization
ISMS	Information Security Management Systems
ISS	Integrate Smart Grid simulations
IT	Information Technology
KPI	Key Performance Indicator
OT	Operational Technology
RBAC	Role-Based Access Control
RGD	Re-use Grid Data
RID	Re-use ICT data
RKP	Re-use Key Performance Indicators
RSG	Reference Smart Grid data
RTF	Re-use technical functions
SGAM	Smart Grid Architecture Model
SGCG	Smart Grid Coordination Group
WP	Work Package

1. Introduction

1.1. Scope of the document

The deliverable D11.3 is the written output of the task T11.3 “Functional description of the comprehensive Smart Grid dashboard system” within the DISCERN work package WP11 “Methodologies for reusing and comparing information about Smart Grid projects” and is based on the deliverable D11.1 “Functional description of the comprehensive Smart Grid data repository”.

In D11.1, the functional requirements and architecture underpinning the future development of a Smart Grid dashboard system were described. It aims at improving reusability of data as collected and produced by European R&D Smart Grid projects, facilitating comparison of Smart Grid projects, and facilitating integration of Smart Grid simulations. The relation to D11.2 consists of the need to ensure important and privacy related data is safe from users which have not the corresponding rights to access the data.

This deliverable presents concepts for addressing issues directly related to privacy and security of the data that shall be stored by humans or systems in the comprehensive Smart Grid data repository dashboard. The role-based access concept will determine the access rights to this data as well as functional and meta-data access rights. The defined anonymization concept will avoid sensible data being traced back to individual users (solving possible privacy issues). The security concept should, when implemented, protect the dashboard system against intrusion attacks (e.g. manipulation by humans or systems) by serving it as a decentralised system providing information only upon request. Unlike the other deliverables, this aspect of the future dashboard has a strong focus not on the technical or standards related-issues arising, but on the organisational, soft aspects of information security.

Furthermore, this deliverable could also be reused for another similar repository system, where the definition of similar roles and actors is required.

1.2. Structure of the document

The document comprises the following main sections:

Section 1 introduces the document.

Section 2 presents a list of general terms and definitions.

Section 3 presents the general approach of security in information management systems regarding ISO/IEC TR 27019 and the role-based access control concept from the IEC 62351-8 standard in a brief way in section 3.2.

Section 4 briefly describes an overview of the dashboard context and how it is related to this document. Furthermore, it presents the application of the security aspects for the Smart Grid dashboard from section 3.

Finally, section 5 concludes this report.

Annex A provides detailed information about the access rights summarised in section 4.3.

2. Terms and Definitions

The following terms and definitions are defined in the IEC 62351 standards series [IEC 62351-8] and help the reader to understand the role-based access concept in the relevant depth needed.

- **Access token**

  Evidence or testimonials concerning one's right to credit, confidence, or authority.

- **Identity provider**

  Creates, maintains and manages identity information; typically used in Single Sign-On (SSO) scenarios.

- **Object**

  As used in the standard [sic!, IEC 62351-8], an object can be any system resource subject to access control such as a file, printer, terminal, database record, etc.

- **Operation**

  An operation is an executable image of a program, which upon invocation executes some function/activity for the subject.

- **Right**

  A right defines an atomic set of accessing privileges assigned to a particular system object.

- **Role**

  A role is a job function within the context of an organization with some semantics associated regarding the authority and responsibility conferred on the user assigned to the role.

  A role subsumes a set of rights.

- **Session**

  A session is an encounter between a user and an application or with the computer in general. One user session is the time between starting the communication channel (either local or remote) and terminating (either by the user or the system).

- **Subject**

  A user or an automated agent is a subject. A subject is a right holder. It shall have a name attribute whose value is mandatory. It is this name that shall be used to enrol a subject in a particular role.

- **User**

  A user is defined as a human being. A User can also be a subclass of the term actor used in DISCERN.

3. Security concepts for information systems in general

This section gives an overview of the security concepts for information security management systems in the energy utility industry in general, regarding the ISO/IEC TR 27019 and the role-based access control concept in particular, regarding the IEC 62351-8.

3.1. Information Security Management System ISO/IEC TR 27019

The international standard ISO/IEC TR 27019 “Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry” provides guidelines for Information Security Management Systems (ISMS) with the tailored scope for the energy utility industry. It extends existing principles to the domain (electric utilities) in scope.

One part of these standards is most important for the Smart Grid dashboard system. Its topic is about further supporting IT systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving and documentation purposes [ISO/IEC TR 27019].

It also includes a safety directive of protective measures for contractors (e.g. Partners of DSOs in R&D consortiums) that have to be fulfilled regarding process control systems and their data. These involve contractors, for example, who access data directly or indirectly (through remote-connection) to systems or networks, and also contractors, who store and use sensitive data in their own IT systems.

3.2. Role-based Access Control (IEC 62351-8)

Part eight of the IEC 62351 with the title “Role-based Access Control” describes the role based access concepts for power systems. The specification provides “[…] a distributed or service-oriented architecture where security is a distributed service and applications are consumers of distributed services” [IEC 62351-8].

3.2.1. Generic framework for access control

A generic framework for access control consists of a subject, an identity provider and an object. This framework is depicted in Figure 3-1.

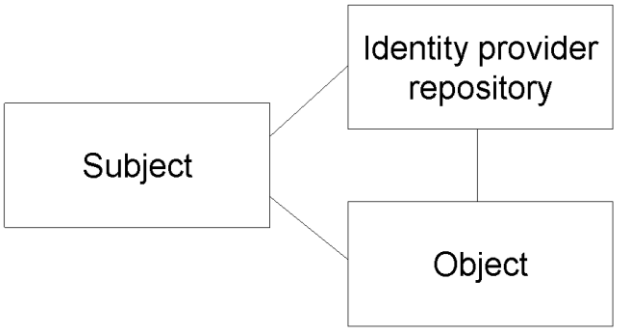

Figure 3-1: Generic framework for access control [IEC 62351-8]

In general, there are two ways (PULL and PUSH) how the subject can access the resources of the object through an access token, which is provided by the identity provider [IEC 62351-8].

- **PULL**

  The access token can be fetched by the object from the repository of the identity provider when the subject connects to the object.

- **PUSH**

  The subject can first fetch the access token from the repository of the identity provider prior to accessing the object.

3.2.2. RBAC Process model

The abstract concept of Role-Based Access Control (RBAC) tries to reduce the complexity and costs of security administration in large networks. The use of roles and constraints to organize subject access levels simplifying the security administration is in the core concept of RBAC.

The RBAC concept consists of the following components: subject, role, right for operations and objects, and session. The application in IEC 62351 is shown in Figure 3-2. It presents RBAC with static and dynamic separation of duty and the relationships between components. One subject is associated with many sessions and each subject is a mapping to possibly one or more roles.

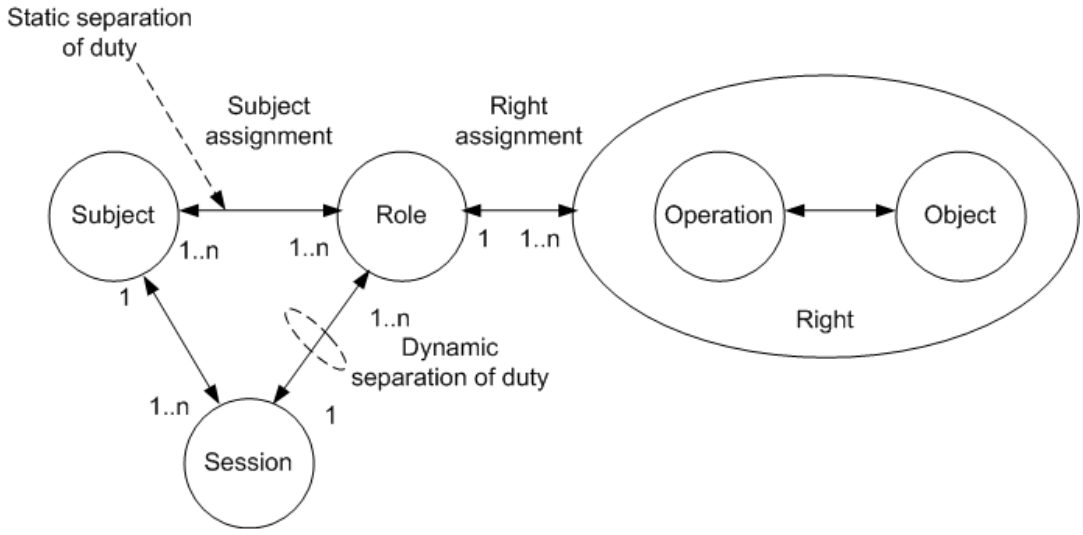

Figure 3-2: Diagram of RBAC with static and dynamic separation of duty [IEC 62351-8]

4. Security concept for the comprehensive Smart Grid dashboard system

Based on the security concept briefly described above, Figure 4-1 shows the context of this concept and the dashboard. The security part includes the standard ISMS ISO 27019 and the RBAC concept, which will be used for the future development of the dashboard. To realise these concepts, different roles with individually assigned access rights are identified based on the determined users (actors) and use cases from [D11.1]. Furthermore, the dashboard system shall be designed as a Web-based application, and consists of defined functionalities described in deliverable [D11.1]. This application shall provide a Graphical User Interface (GUI), where the interaction between the users and the dashboard system will occur.

Section 4.1 gives an overview of exchanged information and functions in the Smart Grid dashboard system. Section 0 then presents the roles of the dashboard system, which are derived from defined actors in [D11.1] and section 4.3 describes the access rights regarding the roles.

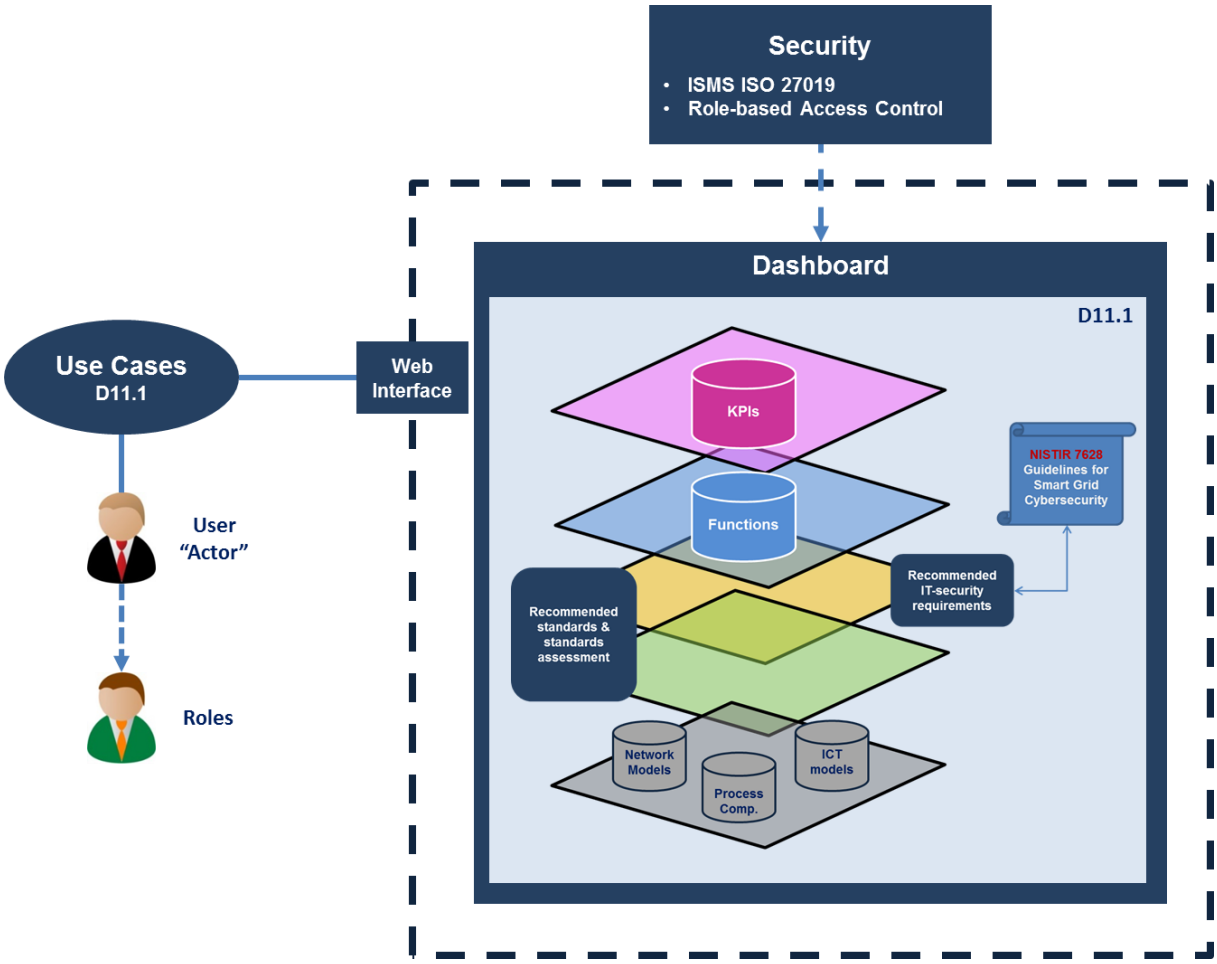

Figure 4-1: Context of the security concepts from IEC 62351-8 and the dashboard

4.1. Data and Functions in context of the dashboard

4.1.1. Data and Classification of Data

Table 2 shows an overview of all exchanged information of the dashboard system grouped by the identified use cases from [D11.1]. The data is classified in two groups: application data and system data. The application data is created and produced by the users of the system. The system data is data which is produced by the system (mostly meta-data and administrative data).

Table 2: Data stored in the Smart Grid dashboard system

Information exchanged per use case from D11.1	**Data Type Classification**
UC: RGD_1 - Reuse network models	
Network model	Application data
Anonymised model	Application data
Network model upload error	System data
Network model download error	System data
Results	Application data
UC: RGD_2 - Reuse process component models	
Process component model	Application data
Anonymised model	Application data
Process component model upload error	System data
Process component model download error	System data
Results	Application data
UC: RID_1 - Reuse ICT architectures	
ICT architecture model	Application data
Anonymised model	Application data
ICT architecture model upload error	System data
ICT architecture model download error	System data
Results	Application data
UC: ACS_1 - Find recommended Smart Grid standards for communication	
Smart Grid architecture models	Application data
IEC Recommended standards list	Application data
SGCG Recommended standards list	Application data
Recommended standards list	Application data
Complete Smart Grid architecture models	Application data
UC: ACS_2 - Carry out standards assessment	
Smart Grid architecture models	Application data
IEC Recommended standards list	Application data
SGCG Recommended standards list	Application data
Standard assessment list	Application data
Recommended Smart Grid architecture models	Application data

Standardisation gaps list	Application data
UC: ATS_1 - Find recommended IT-security requirements	
Smart Grid architecture models	Application data
IT-security requirements list	Application data
Smart Grid architectures upload error	System data
UC: RTF_1 - Update functional categories	
Functional category	Application data
Rejection	System data
UC: RTF_2 - Reuse algorithms or automation logics	
Algorithms or Automation Logic	Application data
Algorithms or Automation Logic upload error	System data
Algorithms or Automation Logic download error	System data
Results	Application data
UC: RKP_1 - Update KPI categories	
KPI category	Application data
Rejection	System data
UC: RKP_2 - Reuse performance KPIs	
KPI	Application data
UC: ISS_1 - Create reference simulation scenarios	
Network model	Application data
Process component model	Application data
ICT architecture model	Application data
Algorithm	Application data
Automation logic	Application data
Co-simulation scenario	Application data
Co-simulation scenario error	System data
UC: RSG_1 - Get reference network model from DSO Observatory	
List of Reference network models	Application data
Reference network model	Application data
UC: CKP_1 - Calculate performance KPI	
Co-simulation scenario	Application data
Models	Application data
KPI models	Application data
Region	Application data
Regulation	Application data
Simulation values	Application data
Co-simulation results	Application data
KPI report	Application data
Co-simulation scenario error	System data

4.1.2. Functions defined for the Scope of RBAC

The Smart Grid dashboard system provides different functions which are applied to data objects (e.g., upload, store, get data, …). These are summarised and described in Table 3. The naming of the function resembles the verbs and nouns from IEC 61968 which was also used in the project DISCERN for message routing based on Common Information Model (CIM). The verbs and nouns provide signal information about the aspect of how a message is treated or shall be treated from the IT point of view – as those are also common to the OT in the utility, we opted to take the same approach for experts to recognize how their data is treated using their familiar (message) key words.

Table 3: Functions of the Smart Grid dashboard system

Function	**Description**
UPLOAD	A user uploads a data object in the Smart Grid dashboard system.
STORE	A data object is stored in the smart gird dashboard system.
GET	A user wants to download or order a data object. The Smart Grid dashboard orders a data object.
DOWNLOAD	A data object is sent/downloaded to a user or downloaded (from the web) into the Smart Grid repository. Tracking of who downloaded which data when.
REPORT	A data object is reported to a user.
GENERATE	A message detailing the errors during the import or download of a data object is created.
PROCESS	A data object is processed by either the Smart Grid repository or a user (tool) processes a data object.
CREATE	A user proposes to create a new data object (category).
SHOW	The data object is sent to a user, is shown in a tool, or is presented in the Smart Grid repository.
SELECT	A user selects a data object in the Smart Grid dashboard system.
SET UP	A user sets up a data object.
START	A user starts a data object.
CALCULATE	A user (tool) reports data objects.
LOG IN / OUT	Start or end the dashboard user activity
BLOCK /SUSPEND	To block temporally some data or operation
NOTIFY	A notification to tell to the party who has uploaded the data that someone is interested in viewing.

4.2. Roles Identified

In Table 4, different roles based on the determined actors from [D11.1] are identified and detailed.

Table 4: Roles of the Smart Grid dashboard system

Actor Grouping	Actor Name	Role Name	Description
Business Actor	Administrator	System Administrator	Person or organisation responsible for administrating the Smart Grid dashboard system.
Business Actor	Project	Internal Project User	Any member of a European (which have been identified originally as scope and prime stakeholders for WP11) R&D Smart Grid project interacting with the Smart Grid dashboard system with the aim of storing data or performing analyses & simulations. Project might refer to a: TSO, DSO, Research Institute, University, Consultant, or Technology Provider.
Business Actor	External Project	External Project User	Any member of a European R&D Smart Grid project interacting with the Smart Grid dashboard system with the aim of downloading/reusing data previously uploaded by Project, including performing their own analyses & simulations. Technically, also non European projects could participate, but typically opt to go for the US Smart Grid Clearinghouse which has a much more narrow scope compared to DISCERN. External Project might refer to a: TSO, DSO, Research Institute, University, Consultant, or Technology Provider.
Business Actor	Standardisation Bodies	External Project Standards	Groups responsible for developing and maintaining standards in the context of the Smart Grids and associated software tools and reports, such as: • **IEC –** International Electrotechnical Commission (IEC). In particular, the Technical Committee (TC) 57 deals with standards concerning power systems management and associated. ○ **IEC Smart Grid Standards Map –** Web platform developed by the International Electrotechnical Commission (IEC) that provides a map of Smart Grid standards to allow identification of the standards that are needed for any part of a Smart Grid (http://smartgridstandardsmap.com/). • **SGCG –** Smart Grid Coordination Group (SGCG) of European standardisation bodies (CEN-CENELEC-ETSI).

			○ **SGCG IOP Tool –** Microsoft Excel tool/ repository developed by the Smart Grid Coordination Group (SGCG) of European standardisation bodies that includes recommended standards for Smart Grid solutions (http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx) • **NISTIR 7628 –** Technical report providing guidelines on Smart Grid Cyber Security. This was developed by international experts in Smart Grid Cyber Security and led by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce (http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf).
Business Actor	DSO Observatory	External Co-Project	Repository of reference network models for European distribution networks. This is maintained by the Joint Research Centre (JRC).
Business Actor	Smart grid Co-simulation Framework, Simulator	External Platform	• External platform that integrates Smart Grid simulators to perform complex co-simulation scenarios. • External simulator that imports models stored in the Smart Grid repository to perform analysis. It might refer to a Network Model simulator, Process Component simulator, ICT Architecture simulator, Power System Application simulator, or Intelligent Electronic Device simulator.
Internal Component	Repository, Co-simulation editor, KPI calculator	Internal Actor	• An internal component of the Smart Grid dashboard system containing models. It might refer to the Network Model repository, Process Component repository, ICT Architecture repository, Algorithm repository, Automation Logic repository, KPI repository, Regulation repository, or Co-simulation repository. • **Component layer repository** ○ **Network Model repository** – Repository within the Smart Grid dashboard system containing network models. It refers also to the interface between the Smart Grid dashboard system and external reference network models as stored in the DSO

			Observatory[1]. ▪ **Process Component repository** – Repository within the Smart Grid dashboard system containing process component models, e.g. generating units and loads. ▪ **ICT Architecture repository** – Repository within the Smart Grid dashboard system containing ICT architectures. • **Function layer repository** ○ **Algorithm & Automation Logic repository** – Repository within the Smart Grid dashboard system containing algorithms for performing technical functions as well as automation logics for intelligent electronic devices. • **Business layer repository** ○ **KPI repository –** Repository within the Smart Grid dashboard system containing formulas for calculation of Key Performance Indicators (KPIs). • **Co-simulation repository –** Repository within the Smart Grid dashboard system containing co-simulation scenarios that combine several models. • Editor within the Smart Grid dashboard system enabling users to create and edit co-simulation scenarios that use models stored in the repository. • Internal component within the Smart Grid dashboard system that calculates KPIs.

4.3. Access rights

We identified core access rights which are individually assigned to the corresponding roles.

[1] DSO Observatory: http://ses.jrc.ec.europa.eu/distribution-system-operators-observatory

Three rights are considered:

- **Read (r)**: This right enables users to view, access and execute the data objects.
- **Write (w)**: This right enables users to create new data, edit and delete existing data objects.
- **Manage (m)**: This right in addition to the *write* services enables users to give user rights for submitted data objects.

Table 5 gives an briefly overview of the assigned access rights to roles. The annex A provides detailed information about the access rights for individual roles, actors matching data items in an Excel spreadsheet.

Table 5: Access rights assigned to roles (access rights coded as: r = read, w = write and m = manage)

Role	**Rights**
System Administrator	r, w, m
Internal Project User	r, w, m
External Project User	r
External Project Standards	r, w
External Co-Project	r, w, m
External Platform	r, w, m
Internal Actor	r, w

4.3.1. Release / Get write access for third-party users

In the case of uploading models (e.g., network model and process component models), the users shall be able to decide who can access the model. It shall be possible to assign different level of access to different users. For instance, decide who can access the model as is, or who can access an anonymised version of data in order to avoid the project data being traced back to its origin.

4.3.2. Multi-editing in the system

To avoid collisions in the Smart Grid dashboard system when more than one user with *write* or *manage* rights want to edit the same data object at the same time, the Smart Grid dashboard system should be able to manage multi-editing of the data objects. The procedure to avoid multi-editing collisions is the following:

- If the data object is not being edited and the user has *write* or *manage* rights over that object, then the user can edit the object.
- If another user with *write* or *manage* rights wants to edit the same object the Smart Grid dashboard system generates a warning stating that the object is being edited by another user.
- If the first user selects “Release write access”, the second user is again able to edit the selected data object.

5. Conclusions

This document represents the deliverable D11.3 and is the output of Task 11.3 “Role-based access, anonymization, and security concept for the comprehensive Smart Grid data repository” in WP 11 in FP 7 DISCERN. Within the scope of the DISCERN WP 11 smart Grid dashboard, this deliverable focuses on the access right granted to several users of the systems on both the functions defined in D11.1 as well as the data defined in D11.2. The scope of D11.3 is to define a theoretical framework for the access rights to the users based on the proven concept of role-based access control RBAC.

Motivating the technology/ methodology from the point of view of ISMS, we use the IEC TC 57 WG 15 standards series 62351 focusing on Power systems management and associated information exchange - Data and communications security. Within the Part 8 of this series, the concept of role-based access control is set into context with power system data and the corresponding roles. Both ISMS and IEC 62351-8 are briefly described with their needed concepts for this report. Based on previous WP 11 work, the identified functions as well as the actors are put in context with the RBAC concept, granting preliminary access right to individual functions and data classes for roles to be implemented in latter stages of developing/ instantiating a dashboard. In addition, the scope is extended to deal with multi-users access to the data and functions and provides first ideas how to deal with a simple and elegant way to solve most issues arising at user level.

6. References internal and external to the project

6.1. Project documents

[D11.1] – DISCERN Deliverable 11.1: “Functional description of the comprehensive Smart Grid data repository”

[D11.2] – DISCERN Deliverable 11.2: ”Data management concept for the comprehensive Smart Grid data repository”

6.2. External documents

[IEC 62351-8] – “Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control”, 2011

[ISO/IEC TR 27019] – “Information technology -- Security techniques -- Information security management (ISMS) guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, 2013”

[IEC 62351 series] Power systems management and associated information exchange - Data and communications security, current base version, 2015

7. Revisions

7.1. Track changes

Name	Date (dd.mm.jjjj)	Version	Changes	
			Subject of change	page
Maike Rosinger / OFFIS Mathias Uslar / OFFIS Rafael Santodomingo/OFFIS	16.10.2015	0.1	Table of contents	
Maike Rosinger / OFFIS Mathias Uslar / OFFIS Rafael Santodomingo / OFFIS	26.11.2015	0.2	First draft version	
Maike Rosinger / OFFIS Mathias Uslar / OFFIS Rafael Santodomingo / OFFIS	03.12.2015	0.3	Consolidation	
Maike Rosinger / OFFIS Mathias Uslar / OFFIS Rafael Santodomingo / OFFIS	04.12.2015	1	Complete first version	
Maike Rosinger / OFFIS Mathias Uslar / OFFIS Rafael Santodomingo / OFFIS	21.01.2016	2.0	Internal review process: Comments and proposed amendments added from RWE, IBDR, and VRD all incorporated	
Carmen Calpe/ RWE	03.02.2016	3.0	Approval document	

Annex A. Access rights in detail

This annex provides detailed information about the access rights summarised in section 4.3.

Attached as a separate Excel spreadsheet file.