

Authenticate data users

Based on IEC 62559-2 edition 1
Generated from UML Use Case Repository with Modsarus® (EDF R&D Tool)

1. Description of the use case

1. Name of use case

Use case identification		
ID	Area(s)/Domain(s)/Zone(s)	Name of use case
	Access to data,Market for flexibilities,Operational planning and forecasting,Services related to end customers,Balance management	Authenticate data users

2. Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	2018-04-12	Kalle Kuk (Elering)		
2	2018-06-01	Kalle Kuk (Elering), Georg Rute (Elering)		
3	2018-06-28	Ricardo Jover (EDF), Eric Suignard (EDF)		
4	2018-07-02	Ricardo Jover (EDF), Eric Suignard (EDF)		
5	2018-08-10	Ricardo Jover (EDF), Eric Suignard (EDF)		
6	2018-08-19	Ricardo Jover (EDF), Eric Suignard (EDF)	"Delegated Authentication" changed into "Representation Rights"	
7	2018-08-02	Eric Suignard (EDF)		
8	2018-09-21	Eric Suignard (EDF), Ricardo Jover (EDF)	Remarks from Innogy, Elering (Automatic process for DEP, without Operator) and EirGrid.	
9	2018-10-04	Eric Suignard (EDF)	Version post WP5&9 physical meeting in Tallinn	
10	2018-10-17	Eric Suignard (EDF)	Version reviewed by WP5&9 partners	
11	2019-05-07	Eric Suignard (EDF)	WP6-7-8 demos alignment and miscellaneous changes	
12	2020-06-16	Eric Suignard (EDF)	innogy's and Elering's review	

3. Scope and objectives of use case

Scope and objectives of use case	
Scope	Access to private data and other information with restricted access through a Customer Portal and a Data Exchange Platform only to authorized users
Objective(s)	Support easy but secure access to data
Related business case(s)	

4. Narrative of Use Case

Narrative of use case

Short description

All data users need to be authenticated to a Customer Portal before having access to a Data Exchange Platform (DEP), for the exchange of individual metering data (private data) or any other information with restricted access.

Complete description

Summary of use case

- **Authentication process and representation rights delegation**

Description: Any person needing access to personal or commercial data needs to be authenticated to a Customer Portal for having access to the data via a DEP – either logging in through a Customer Portal or through third party application connected to a DEP.

This may involve:

- Consumer's/generator's access to own consumption/generation data;
- Access to a person's data by another person who has received representation rights from data owner.

After authenticating himself/herself, the data owner (e.g. electricity consumer is the owner of its consumption data) can give representation rights to any other person who can then act on behalf of the data owner.

Customer Portal operator checks the validity of the representation rights. If a representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.

After authenticating himself/herself, the person who has received the representation rights can see who is he/she representing and act on behalf of data owner.

- **Authenticate**

Description: Authentication means may include ID-card, mobile-ID or bank link. Information associated to authentication process may include name, surname and ID-code of individual customers; company name and registry code of corporate customers as well as name, surname and ID-code of their representatives.

- **Verify Logging Identification**

Description:

- **Verify Identity**

Description: Verifies the identity of authenticating parties.

- **Give access to data**

Description:

- **Access to Own Data**

Description:

- **Delegate Representation Rights**

Description: A data owner gives representation rights for data per consumption/generation point. He/she can also select types of data (e.g. historical consumption/generation data, sub-meter data, operational data) for which he/she gives representation rights. He/she selects the persons to whom he/she gives representation rights.

- **Register Representation Rights**

Description:

- **Verify Representation Rights**
Description: Customer Portal operator checks the validity of the representation rights.
- **Verify Representation Rights in a Foreign Country**
Description: If the representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.
- **Notify Representation Rights**
Description:
- **Authenticate**
Description:
- **Access to Delegated Data**
Description:

5. Key performance indicators (KPI)

6. Use case conditions

<i>Use case conditions</i>	
<i>Assumptions</i>	
1	eIDAS (electronic IDentification, Authentication and trust Services) regulation and its trust levels shall be applied
2	Private and/or commercially sensitive data needs to be exchanged
<i>Prerequisites</i>	
1	National or platform specific identification infrastructure – ID card, dedicated password, internet bank link, etc
2	Cross-border acknowledgment of different authentication schemes
3	GDPR (General Data Protection Regulation) shall be applied.

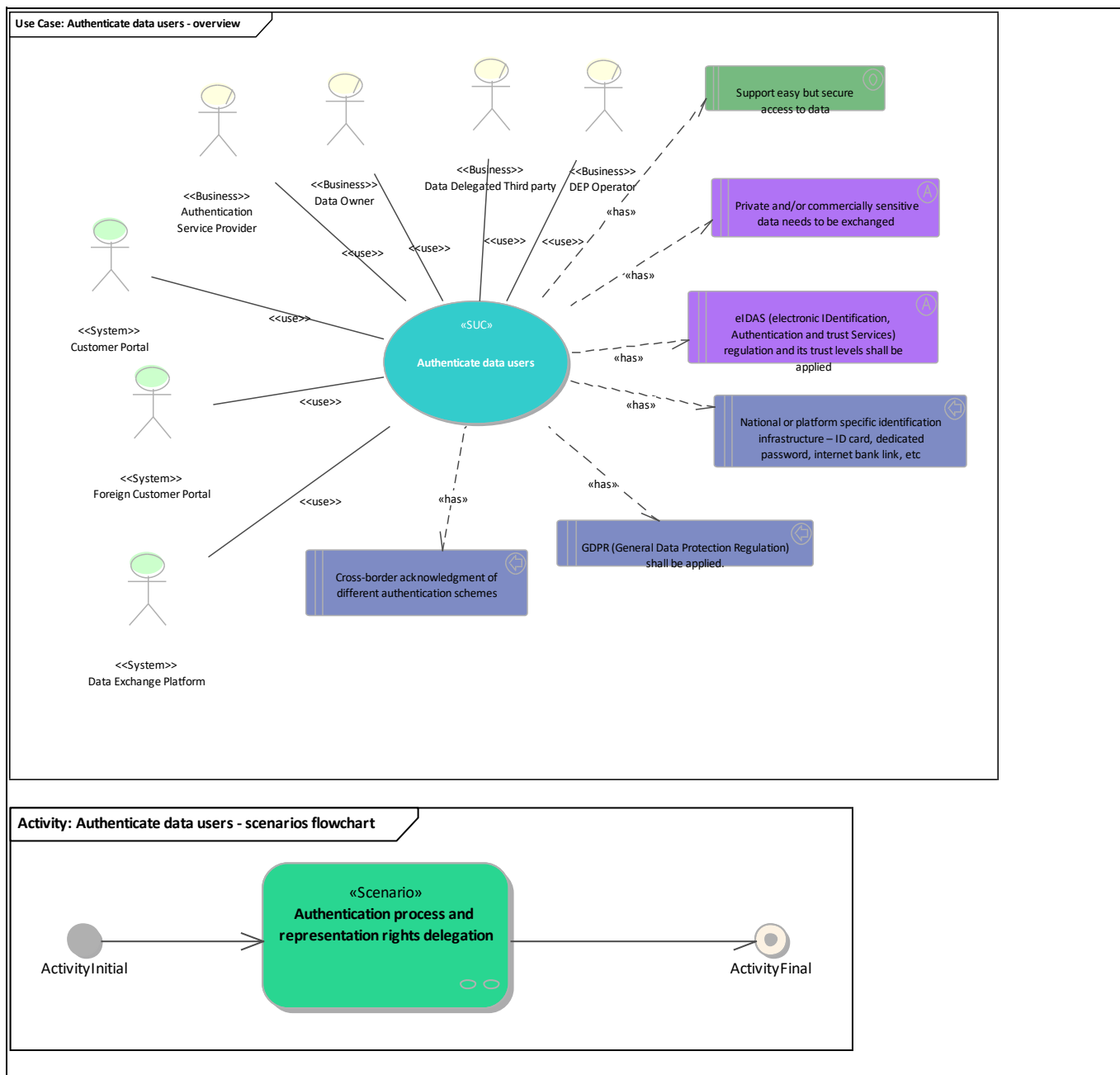
7. Further information to the use case for classification/mapping

<i>Classification information</i>
<i>Relation to other use cases</i>
<i>Level of depth</i>
<i>Prioritisation</i>
<i>Generic, regional or national relation</i>
<i>Nature of the use case</i>
SUC
<i>Further keywords for classification</i>

8. General remarks

2. Diagrams of use case

<i>Diagram(s) of use case</i>



3. Technical details

1. Actors

Actors			
Grouping (e.g. domains, zones)		Group description	
Actor name	Actor type	Actor description	Further information specific to this use case
Customer Portal Operator	Business	Operates a Customer Portal.	

Authentication Service Provider	Business	Trust authority. Verifies the identity of authenticating parties. Some countries will have their own authentication service provider. For countries which will not, there may be a more global and to be defined one.	
Data Owner	Business	Any person who owns data and can give authorization to other parties to access them. Can be, inter alia: <ul style="list-style-type: none"> Flexibility Services Provider Market Operator Consumer Generator 	
Data Delegated Third party	Business	Any natural person who has received representation rights from a data owner.	
Foreign Customer Portal	System	Customer Portal for another country. Can also mean a separate portal in the same country.	
Customer Portal	System	Customer Portal manages data users' authentication, access permissions and data logs. Customer Portals store data related to its services (e.g. authentication information, representation rights, access permissions, data logs).	
Data Exchange Platform	System	Data exchange platform (DEP) is a communication platform the basic functionality of which is to secure data transfer (routing) from data providers (e.g. data hubs, flexibility service providers, TSOs, DSOs) to the data users (e.g. TSOs, DSOs, consumers, suppliers, energy service providers). DEP stores data related to its services (e.g. cryptographic hash of the data requested). The DEP does not store core energy data (e.g. meter data, grid data, market data) while these data can be stored by data hubs. Several DEPs may exist in different countries and inside one country.	
DEP Operator	Business	Data exchange platform operator owns and operates a communication system which basic functionality is data transfer.	

2. References

4. Step by step analysis of use case

1. Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition
1	Authentication process and representation rights delegation	<p>Any person needing access to personal or commercial data needs to be authenticated to a Customer Portal for having access to the data via a DEP – either logging in through a Customer Portal or through third party application connected to a DEP.</p> <p>This may involve:</p> <ul style="list-style-type: none"> Consumer's/generator's access to own consumption/generation data; 				

		<ul style="list-style-type: none"> Access to a person's data by another person who has received representation rights from data owner. <p>After authenticating himself/herself, the data owner (e.g. electricity consumer is the owner of its consumption data) can give representation rights to any other person who can then act on behalf of the data owner.</p> <p>Customer Portal operator checks the validity of the representation rights. If a representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.</p> <p>After authenticating himself/herself, the person who has received the representation rights can see who is he/she representing and act on behalf of data owner.</p>				
--	--	--	--	--	--	--

2. Steps - Scenarios

1. Authentication process and representation rights delegation

Any person needing access to personal or commercial data needs to be authenticated to a Customer Portal for having access to the data via a DEP – either logging in through a Customer Portal or through third party application connected to a DEP.

This may involve:

- Consumer's/generator's access to own consumption/generation data;
- Access to a person's data by another person who has received representation rights from data owner.

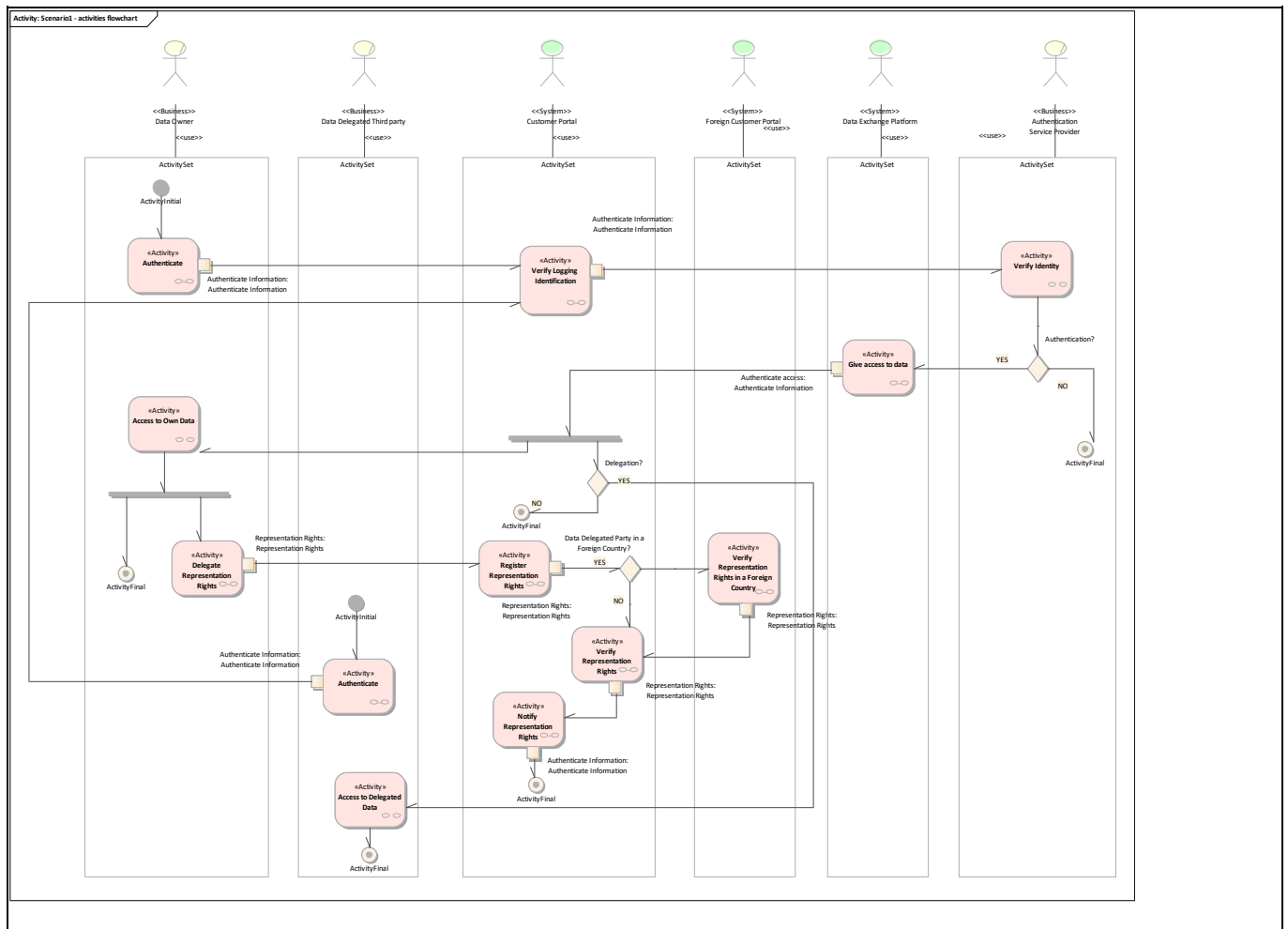
After authenticating himself/herself, the data owner (e.g. electricity consumer is the owner of its consumption data) can give representation rights to any other person who can then act on behalf of the data owner.

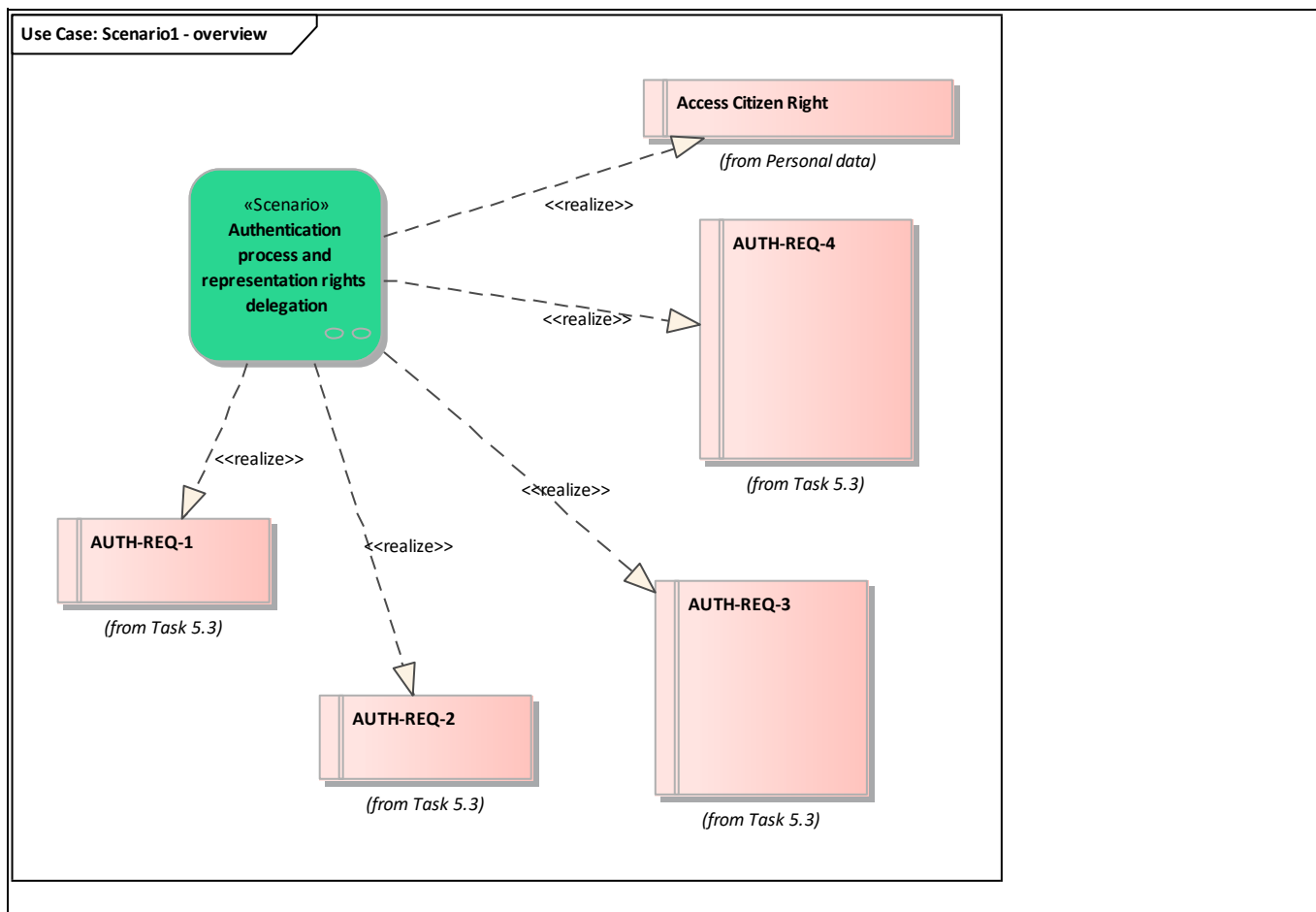
Customer Portal operator checks the validity of the representation rights. If a representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.

After authenticating himself/herself, the person who has received the representation rights can see who is he/she representing and act on behalf of data owner.

Requirement list (refer to "Requirement" section for more information)

Requirement R-ID	Requirement name
Cat1.Reg1	Access Citizen Right
Cat2.Reg2	AUTH-REQ-3
Cat2.Reg3	AUTH-REQ-4
Cat2.Reg4	AUTH-REQ-2
Cat2.Reg5	AUTH-REQ-1





Scenario step by step analysis

Scenario								
Scenario name		Authentication process and representation rights delegation						
Step No	Event	Name of process/activity	Description of process/activity	Service	Information producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1.1		Authenticate	Authentication means may include ID-card, mobile-ID or bank link. Information associated to authentication process may include name, surname and ID-code of individual customers; company name and registry code of corporate customers as well as name, surname and ID-code of their representatives.		Data Owner	Customer Portal	Logging Identification Data- Authenticate Information	Cat3 Req6
1.2		Verify Logging Identification			Customer Portal	Authentication Service Provider	Logging Identification Data-	

							Authenticate Information	
1.3		Verify Identity	Verifies the identity of authenticating parties.		<u>Authentication Service Provider</u>			
1.4		Give access to data			<u>Data Exchange Platform</u>	<u>Data Owner, Customer Portal, Data Delegated Third party</u>	Logging Identification Data-Authenticate Information	
1.5		Access to Own Data			<u>Data Owner</u>			
1.6		Delegate Representation Rights	A data owner gives representation rights for data per consumption/generation point. He/she can also select types of data (e.g. historical consumption/generation data, sub-meter data, operational data) for which he/she gives representation rights. He/she selects the persons to whom he/she gives representation rights.		<u>Data Owner</u>	<u>Customer Portal</u>	Representation Rights-Representation Rights	
1.7		Register Representation Rights			<u>Customer Portal</u>	<u>Customer Portal, Foreign Customer Portal</u>	Representation Rights-Representation Rights	
1.8		Verify Representation Rights	Customer Portal operator checks the validity of the representation rights.		<u>Customer Portal</u>	<u>Customer Portal</u>	Representation Rights-Representation Rights	
1.9		Verify Representation Rights in a Foreign Country	If the representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.		<u>Foreign Customer Portal</u>	<u>Customer Portal</u>	Representation Rights-Representation Rights	
1.10		Notify Representation Rights			<u>Customer Portal</u>	<u>Customer Portal</u>	Logging Identification Data-Authenticate Information	
1.11		Authenticate			<u>Data Delegated Third party</u>	<u>Customer Portal</u>	Logging Identification Data-	<u>Cat3.Reg6</u>

							Authenticate Information	
1.12		Access to Delegated Data			Data Delegated Third party			

- 1.1. Authenticate

Business section: Authentication process and representation rights delegation/Authenticate

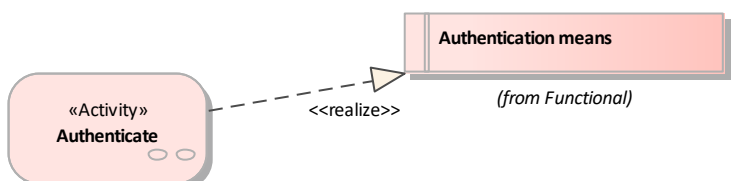
Authentication means may include ID-card, mobile-ID or bank link.

Information associated to authentication process may include name, surname and ID-code of individual customers; company name and registry code of corporate customers as well as name, surname and ID-code of their representatives.

Requirement list (refer to "Requirement" section for more information)

Requirement R-ID	Requirement name
Cat3.Reg6	Authentication means

Information sent:

Business object	Instance name	Instance description
Authenticate Information	Authenticate Information	
<div> <div>Use Case: Activity1 - overview</div>  </div>		

- 1.2. Verify Logging Identification

Business section: Authentication process and representation rights delegation/Verify Logging Identification

Information sent:

Business object	Instance name	Instance description
Authenticate Information	Authenticate Information	

- 1.4. Give access to data

Business section: Authentication process and representation rights delegation/Give access to data

Information sent:

Business object	Instance name	Instance description
Authenticate Information	Authenticate access	

- 1.6. Delegate Representation Rights

Business section: Authentication process and representation rights delegation/Delegate Representation Rights

A data owner gives representation rights for data per consumption/generation point.
 He/she can also select types of data (e.g. historical consumption/generation data, sub-meter data, operational data) for which he/she gives representation rights.
 He/she selects the persons to whom he/she gives representation rights.
Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Representation Rights	Representation Rights	

- 1.7. Register Representation Rights

Business section: Authentication process and representation rights delegation/Register Representation Rights

Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Representation Rights	Representation Rights	

- 1.8. Verify Representation Rights

Business section: Authentication process and representation rights delegation/Verify Representation Rights

Customer Portal operator checks the validity of the representation rights.
Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Representation Rights	Representation Rights	

- 1.9. Verify Representation Rights in a Foreign Country

Business section: Authentication process and representation rights delegation/Verify Representation Rights in a Foreign Country

If the representation right is given to a person in another country, then the Customer Portal operators of the involved countries share the information about representation rights between themselves.
Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Representation Rights	Representation Rights	

- 1.10. Notify Representation Rights

Business section: Authentication process and representation rights delegation/Notify Representation Rights

Information sent:

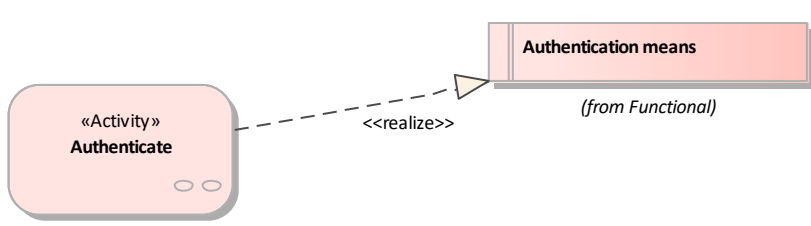
<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Authenticate Information	Authenticate Information	

- 1.11. Authenticate

Business section: Authentication process and representation rights delegation/Authenticate

Requirement list (refer to "Requirement" section for more information)	
Requirement R-ID	Requirement name
Cat3.Req6	Authentication means

Information sent:

Business object	Instance name	Instance description
Authenticate Information	Authenticate Information	
<div> <div>Use Case: Activity1 - overview</div>  </div>		

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
Logging Identification Data	Authenticate Information		
Representation Rights	Representation Rights		

6. Requirements (optional)

Requirements (optional)		
Categories ID	Category name for requirements	Category description
Cat1	Personal data	
Requirement R-ID	Requirement name	Requirement description
Req1	Access Citizen Right	Right to secure direct access of own personal data and to any processing, storage or sharing details
Requirements (optional)		
Categories ID	Category name for requirements	Category description
Cat2	Task 5.3	Requirements integrated from Task 5.3.
Requirement R-ID	Requirement name	Requirement description
Req2	AUTH-REQ-3	Ability to share information related to representation rights between data users and concerned Customer Portals

Req3	AUTH-REQ-4	Ability to share authentication information between data users, Customer Portal and Authentication Service Provider
Req4	AUTH-REQ-2	Authentication tools
Req5	AUTH-REQ-1	Right to access own data
Requirements (optional)		
Categories ID	Category name for requirements	Category description
Cat3	Functional	Functional requirements
Requirement R-ID	Requirement name	Requirement description
Req6	Authentication means	Authentication means may include ID-card, mobile-ID or bank link. Information associated to authentication process may include name, surname and ID-code of individual customers; company name and registry code of corporate customers as well as name, surname and ID-code of their representatives.

7. Common terms and definitions

8. Custom information (optional)