

Manage data logs

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

1.1. 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	Manage data logs

1.2. Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	2018-06-01	Kalle Kuk (Elering)		
2	2018-07-10	Mandimby Ranaivo R. (AKKA)		
3	2018-08-02	Eric Suignard (EDF)		
4	2018-09-21	Eric Suignard (EDF)		
5	2018-10-04	Eric Suignard (EDF)	Version post WP5&9 physical meeting in Tallinn	
6	2018-10-17	Eric Suignard (EDF)	Version reviewed by WP5&9 partners	
7	2019-05-07	Eric Suignard (EDF)	WP6-7-8 demos alignment and miscellaneous changes	
8	2020-06-16	Eric Suignard (EDF)	innogy's and Elering's review	

1.3. Scope and objectives of use case

Scope and objectives of use case	
Scope	Making available security logs including data access logs and authorization logs.
Objective(s)	Ensure personal data protection.
Related business case(s)	

1.4. Narrative of Use Case

Narrative of use case	
Short description	
Data Owner's access to data logs contributes to personal data protection. The data logs include information about data access (e.g. who has accessed consumption data and when), authorizations (e.g. who has issued a new authorization and when) and authentication (e.g. who has identified himself/herself in Customer Portal and when).	
Complete description	
Via a Customer Portal, a Data Owner (e.g. electricity consumer is the owner of its consumption data) has access to data logs. They include two types of logs:	
<ul style="list-style-type: none"> Data access logs: e.g. who has accessed data and when Authorization logs: e.g. who has requested/received authorization to access data and when 	

- Authentication logs: e.g. who has identified himself/herself in Customer Portal and when

The Customer Portal operator makes the data logs available in the Customer Portal. In addition, in case of cross border data exchange, the Customer Portal operators of the involved countries share information about data logs between them.

Summary of use case

- Data Owner accesses data logs

Description: The Data Owner requests access to its data logs from the Customer Portal. In case of cross border data exchange, the later retrieves the data logs from the corresponding foreign Customer Portal. Finally, the Data Owner consults the requested data logs.

- Request data logs

Description: The Data Owner requests data logs to the Customer Portal. The request contains the desired log type:

- Data access (e.g. who has accessed data and when)
- Authorization (e.g. who has requested/received authorization to access data and when)
- Authentication logs (e.g. who has identified himself/herself in Customer Portal and when)

It also contains selection criteria like dates, log level etc.

- Retrieve data access logs

Description: The Customer Portal retrieves data access logs corresponding to the received selection criteria.

- Retrieve authorization logs

Description: The Customer Portal retrieves authorization logs corresponding to the received selection criteria.

- Retrieve data access logs

Description: The foreign Customer Portal retrieves data access logs corresponding to the received selection criteria and hands them over to the original Customer Portal.

- Retrieve authorization logs

Description: The foreign Customer Portal retrieves authorization request logs corresponding to the received selection criteria and hands them over to the original Customer Portal.

- Consult data logs

Description: The Data Owner receives the data log records he requested.

1.5. Key performance indicators (KPI)

1.6. Use case conditions

<i>Use case conditions</i>	
<i>Assumptions</i>	
1	Private and/or commercially sensitive data needs to be exchanged.
<i>Prerequisites</i>	
1	The data owner has successfully logged in the Customer Portal.
2	Cross-border access to data logs.: Data logs can be exchanged between Customer Portals from different countries.

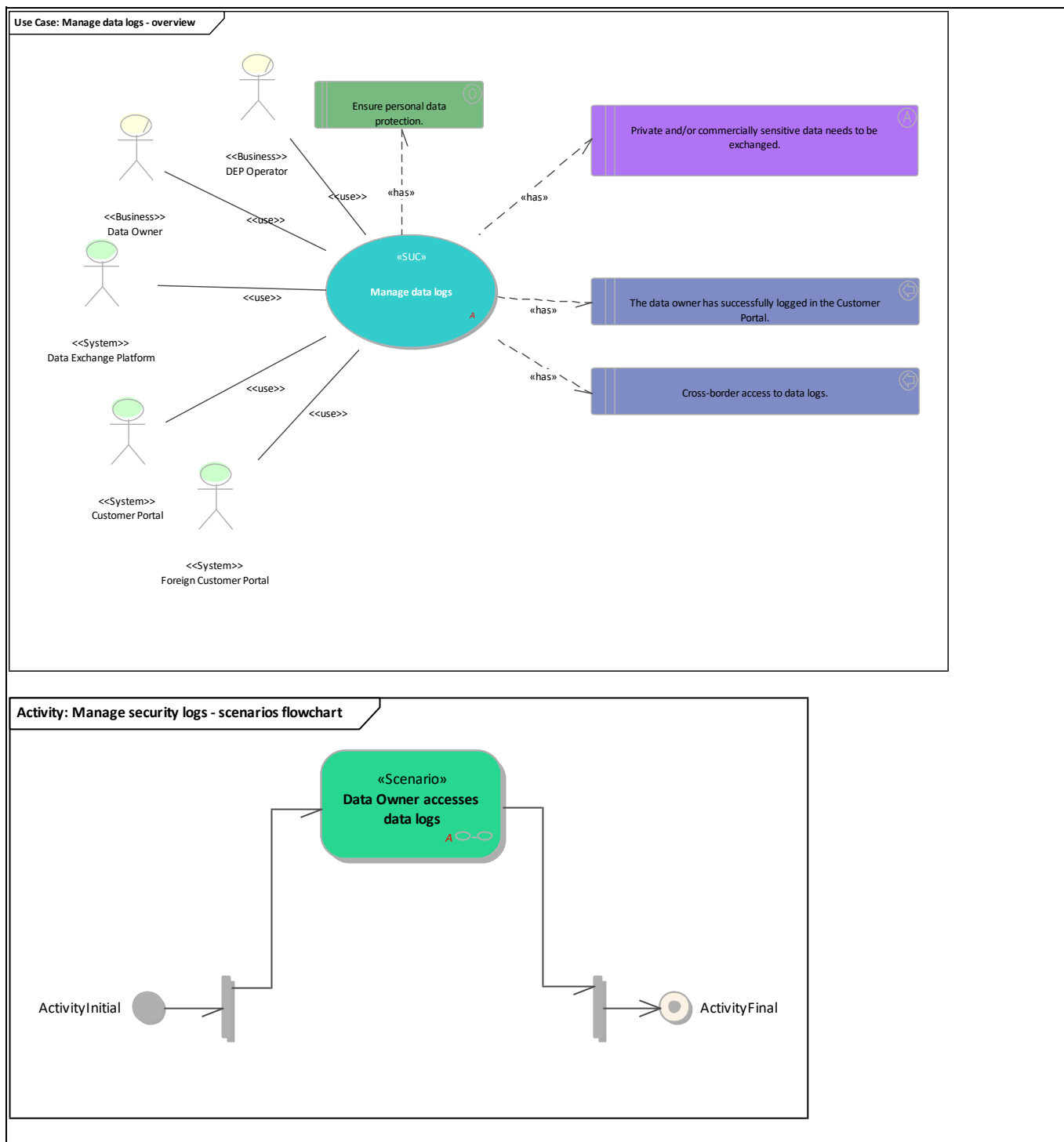
1.7. Further information to the use case for classification/mapping

<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>

1.8. General remarks

2. Diagrams of use case

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



3. Technical details

3.1. Actors

Actors	
Grouping (e.g. domains, zones)	Group description

Actor name	Actor type	Actor description	Further information specific to this use case
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.	The data exchange platform stores the security logs and makes them available upon request.
Foreign Customer Portal	System	Customer Portal for another country. Can also mean a separate portal in the same country.	
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 	
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).	
DEP Operator	Business	Data exchange platform operator owns and operates a communication system which basic functionality is data transfer.	

3.2. References

4. Step by step analysis of use case

4.1. Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario description	Primary actor	Triggering event	Pre-condition	Post-condition
1	Data Owner accesses data logs	The Data Owner requests access to its data logs from the Customer Portal. In case of cross border data exchange, the later retrieves the data logs from the corresponding foreign Customer Portal. Finally, the Data Owner consults the requested data logs.				

4.2. Steps - Scenarios

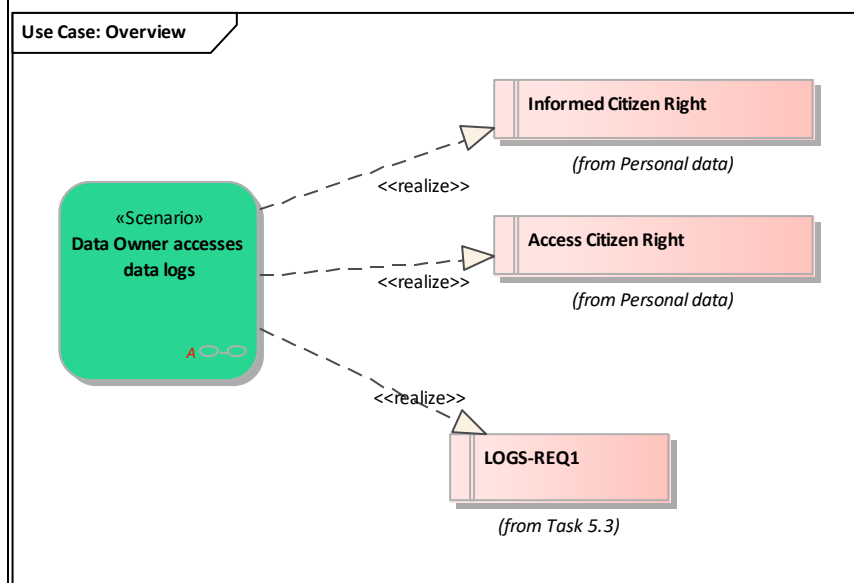
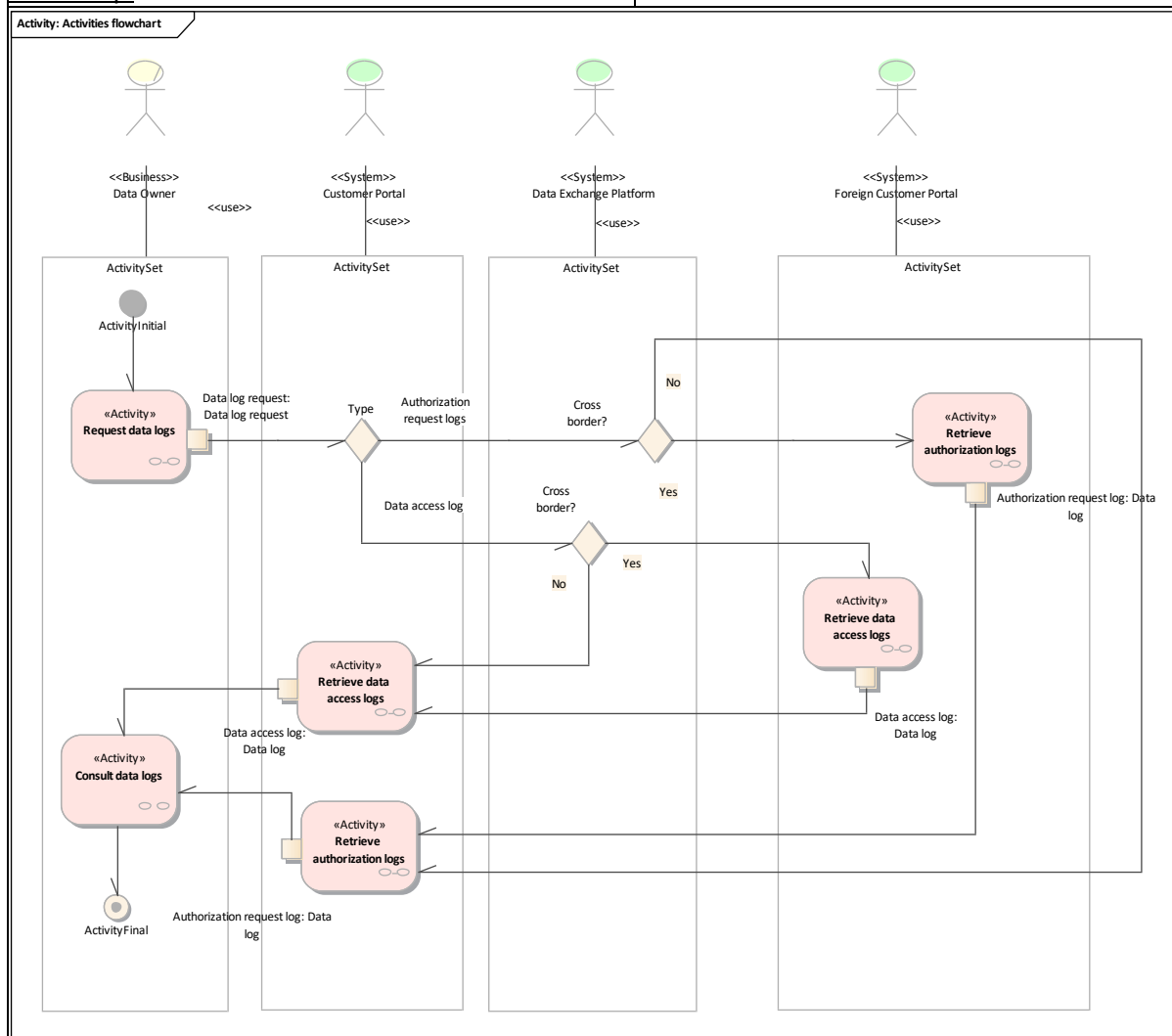
4.2.1. Data Owner accesses data logs

The Data Owner requests access to its data logs from the Customer Portal. In case of cross border data exchange, the later retrieves the data logs from the corresponding foreign Customer Portal. Finally, the Data Owner consults the requested data logs.

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

Requirement R-ID	Requirement name
Cat1.Reg1	Access Citizen Right

Cat1.Reg2	Informed Citizen Right
Cat2.Reg3	LOGS-REQ1



Scenario step by step analysis

Scenario								
Scenario name		Data Owner accesses data logs						
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		Request data logs	<p>The Data Owner requests data logs to the Customer Portal. The request contains the desired log type:</p> <ul style="list-style-type: none"> Data access (e.g. who has accessed data and when) Authorization (e.g. who has requested/received authorization to access data and when) Authentication logs (e.g. who has identified himself/herself in Customer Portal and when) <p>It also contains selection criteria like dates, log level etc.</p>		Data Owner	Foreign Customer Portal, Customer Portal, Foreign Customer Portal, Customer Portal	Info1-Data log request	
1.2		Retrieve data access logs	The Customer Portal retrieves data access logs corresponding to the received selection criteria.		Customer Portal	Data Owner	Info2-Data log	
1.3		Retrieve authorization logs	The Customer Portal retrieves authorization logs corresponding to the received selection criteria.		Customer Portal	Data Owner	Info2-Data log	
1.4		Retrieve data access logs	The foreign Customer Portal retrieves data access logs corresponding to the received selection criteria and hands them over to the original Customer Portal.		Foreign Customer Portal	Customer Portal	Info2-Data log	
1.5		Retrieve authorization logs	The foreign Customer Portal retrieves authorization request logs corresponding to the received selection criteria		Foreign Customer Portal	Customer Portal	Info2-Data log	

			and hands them over to the original Customer Portal.					
1.6		Consult data logs	The Data Owner receives the data log records he requested.		Data Owner			

- 1.1. Request data logs

Business section: Data Owner accesses data logs/Request data logs

The Data Owner requests data logs to the Customer Portal. The request contains the desired log type:

- Data access (e.g. who has accessed data and when)
- Authorization (e.g. who has requested/received authorization to access data and when)
- Authentication logs (e.g. who has identified himself/herself in Customer Portal and when)

It also contains selection criteria like dates, log level etc.

Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Data log request	Data log request	

- 1.2. Retrieve data access logs

Business section: Data Owner accesses data logs/Retrieve data access logs

The Customer Portal retrieves data access logs corresponding to the received selection criteria.

Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Data log	Data access log	

- 1.3. Retrieve authorization logs

Business section: Data Owner accesses data logs/Retrieve authorization logs

The Customer Portal retrieves authorization logs corresponding to the received selection criteria.

Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Data log	Authorization request log	

- 1.4. Retrieve data access logs

Business section: Data Owner accesses data logs/Retrieve data access logs

The foreign Customer Portal retrieves data access logs corresponding to the received selection criteria and hands them over to the original Customer Portal.

Information sent:

<i>Business object</i>	<i>Instance name</i>	<i>Instance description</i>
Data log	Data access log	

- 1.5. Retrieve authorization logs

Business section: Data Owner accesses data logs/Retrieve authorization logs

The foreign Customer Portal retrieves authorization request logs corresponding to the received selection criteria and hands them over to the original Customer Portal.

Information sent:

Business object	Instance name	Instance description
Data log	Authorization request log	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
Info1	Data log request	Contains the type of the requested logs (data access logs or authorization request logs) and other criteria like dates, log level etc.	
Info2	Data log	Contains the selected log records.	

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
Req2	Informed Citizen Right	Right to be informed of any personal data held, of how it is used or processed, of any breach, and of any disclosure/usage to third parties
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
Req3	LOGS-REQ1	Ability to share information related to data logs between data owners, concerned DEPs, applications and data sources

7. Common terms and definitions

8. Custom information (optional)