Horizon 2020
European Union funding
for Research & Innovation

Data security and privacy guidelines and feasible cyber security methods for data exchange platforms

D5.4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773505.

PROGRAMME	H2020 COMPETITIVE LOW CARBON ENERGY 2017-2-SMART-GRIDS
GRANT AGREEMENT NUMBER	773505
PROJECT ACRONYM	EU-SYSFLEX
DOCUMENT	**D5.4**
TYPE (DISTRIBUTION LEVEL)	☒ Public ☐ Confidential ☐ Restricted
DUE DELIVERY DATE	April 2021 (month 42)
DATE OF DELIVERY	31th of May, 2021
STATUS AND VERSION	FINAL V1
NUMBER OF PAGES	85
WORK PACKAGE / TASK RELATED	WP5 / T5.4
WORK PACKAGE / TASK RESPONSIBLE	Kalle Kukk / Priit Anton
AUTHOR (S)	Priit Anton (Guardtime), Liis Livin (Guardtime), Tuuli Lõhmus (Guardtime), Kristo Klesment (Guardtime), Kalle Kukk (Elering), Aivo Olev (Cybernetica), Philippe Szczech (AKKA), Simon Lilleeng (Enoco), Ulf Roar Aakenes (Enoco), Olav Rossøy (Enoco)

DOCUMENT HISTORY

VERS	ISSUE DATE	CONTENT AND CHANGES
V1	31/05/2021	Document submitted to EC

DOCUMENT APPROVERS

PARTNER	APPROVER
Elering	Kalle Kukk – Work Package Leader
EDF	Marie-Ann Evans – Technical Manager
EirGrid, EDF, SONI, VITO, E.ON, Elering, EDP NEW, EURACTIV, Zabala	EU-SysFlex Project Management Board
EIRGRID	John Lowry – Project Coordinator

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

AGR	Aggregator
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
ATDSR	'Affordable Tool' for smaller DSR units demonstrator
BL	Black Lantern
BUC	Business Use Case
CA	Certification Authority
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CG-SEG	Coordination Group on Smart Energy Grids
CIA	Confidentiality, Integrity, Availability
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Team
DEDE	Decentralised Energy Data Exchange adapter
DEP	Data Exchange Platform
DER	Distributed Energy Resources
DID	Decentralised Identifier
DMS	Distribution Management System
DoA	Description of Action
DoS	Denial of Service
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSO	Distribution System Operator
DSR	Demand Side Response
E/E/PE E/E/PES	Electrical/Electronic/Programmable Electronic Safety-related Systems
EC	European Commission
ECCo SP	ENTSO-E Communication & Connectivity Service Platform
ECI	European Critical Infrastructure
ECP	ECCo SP message delivery platform
EDX	ECCo SP's integration node, which enables the data exchange
EG	Expert Group
EIC	Energy Identification Code
eID	Electronic Identifier
eIDAS	European Regulation on electronic Identification, Authentication and trust Services

ENISA	European Union Agency for Cyber security
ENTSO-E	European Network of Transmission System Operators for Electricity
ePD	Directive on Privacy and Electronic Communications
ePR	ePrivacy Regulation
ESCO	Energy Service Company
ETSI	European Telecommunications Standards Institute
EU	European Union
EUC	Equipment Under Control
EX	Extender
FP	Flexibility Platform
FSP	Flexibility Service Provider
FTR	Forward-Looking Threat Research
GB	Green Button
GDPR	General Data Protection Regulation
GUI	Graphic User Interface
HMAC	Hash-based Message Authentication Code)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICCP	Institute for Certification of Computing Professionals
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IS	International Standard
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LS	Log Security
MMS	Manufacturing Message Specification
NCA	National Competent Authority
NERC	North American Electric Reliability Corporation
NIS	Directive on Security of Network and Information Systems
NIST	National Institute of Standards and Technology
NISTR	National Institute of Standards and Technology Report
NSM	Network and System Management
OBIS	Object Identification System
OES	Operator of Essential Service

OIS	Open Systems Interworking
OMS	Outage Management System
OPDM	ENTSO-E's Operational Planning Data Management
OSI	Open System Interconnection
PII	Personal Identifying Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMB	Project Management Board
RBAC	Role-Based Access Control
RES	Renewable Energy Sources
REST	Representational State Transfer
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SGIS	Smart Grid Information Security
SGTF	Smart Grid Task Force
SL	Security Level
SO	System Operator
SSO	Single Sign-On
SUC	System Use Case
TC	Technical Committee
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
UI	User Interface
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VPP	Virtual Power Plant
WP	Work Package
WG	Working group
XML	Extensible Markup Language

EXECUTIVE SUMMARY

The objective of this report is to provide data security and privacy guidelines and feasible cyber security methods for data exchange platforms. This report consolidates practical examples of EU-SysFlex data exchange demonstrators and explains how applicability of existing standards and commercial tools can provide security and privacy for energy grid deployments.

The report focuses primarily on **data exchange and related demonstrations** that are covered in **EU-SysFlex WP5 and in WP9**. EU-SysFlex **task 5.5 deliverable** "**Proposal for data exchange standards and protocols**" is recommended as introductory reading for the current document, it provides the background to relevant data exchange standards, legislation, organisations, and the demonstrations that were the basis of the current report. Moreover, the demonstrators rely on the EU-SysFlex task 5.2 **system use cases** which describe the privacy and security methods for energy data exchange. The knowledge of the use cases helps to understand the content provided in this report and thus **task 5.2 deliverable** "**Description of data exchange use cases based on IEC 62559 methodology**" is also primer for the current report.

The report on **"Data security and privacy guidelines and feasible cyber security methods for data exchange platforms"** helps to understand the legislative and regulatory background of GDPR and privacy in the case of cross-border data exchange platforms. This report supports the general objectives of EU-SysFlex that from the privacy perspective the aim is to solve the issue of addressing data owners' interest and the handling of personal identifiable information (PII). The managing of personal data is strongly connected to the potential risk of these data exposure to third parties. These threats and other cyber security vulnerabilities are covered from the legal and regulatory framework perspective. Moreover, the report addresses the applicability of cyber security techniques from a practical standpoint. Data exchange has increasing importance to provide next generation energy flexibility and demand response services. The secure and GDPR complaint mechanisms that support it are essential to future data exchange platforms.

The key findings of this report are as follows:

In the field of **privacy and GDPR** (Chapter 3)

1) The **current legislation and standards provide generally sufficient guidelines** how to ensure data protection through technology design, especially when updates to ePR and NIS, new Network Code on Cybersecurity, ISO/IEC 2700X:2021, etc. enter into force in the near future. However, there are areas where more work is needed. For example, when changing the smart meter operator (in case this is different from system operator) and transferring customer data and the consumption data from old to new one. Additionally, the complexity lies in investing sufficient resources into the privacy domain to enable privacy by design.
2) **The visibility and protection of private data** along with the links between systems providing customer data and PII is **limited**. There is a high risk that energy data managers, who are responsible for the protection of

data privacy are not able to apply sufficient security measures as they could be unaware of some links or processes which use private data without making the use clearly visible. This can lead to data leaks and increases cyberattacks against energy sector systems.

3) Personal data protection has to be considered at all the steps when building a data exchange platform (DEP). System operators and all the users of DEP must ensure that internal measures and processing consents are obtained and cyber security measures applied to avoid external threats.
4) GDPR articles 5-7 cover principles for processing personal data and required consent. While the regulation applies across European Union**, interpretations could differ for smart meter data collection and processing**. As one of the principles is data minimisation, frequent personal data collection including smart meter readings could need an explicit consent and a lawful reason.

In the **field of cyber security** (Chapter 4)

1) The current **legislation and regulatory framework** that provides guidelines for cyber security principles and standards covers the topic of this report well. The updates are underway for both legislation and regulatory frameworks (NIS1 and Network Code). The work on the cyber security aspects of energy platforms must continue to be prepared for future threats.
2) There is **lack of communication to exchange the data about cyber incidents both** in energy sector in general but also in the energy data exchange domain specifically. The experiences from different sector's technology providers and system operators need to be shared and used among the energy sector participants in order to learn from mistakes and achievements related to cyber incidents. While the new Network Code on Cybersecurity will address some of the issues, unfortunately the information sharing (e.g. on vulnerabilities, misconfigurations, 0-day exploits) between the adversaries is much more efficient.
3) The governance and control mechanisms need support from the participating organisations to make policy and business decisions and pave the way for different technological solutions and capabilities to have security by design as a main building block enabled from the beginning. Also, slow technology adaption by energy sector participants is a bottleneck in coping with cyber security challenges.

In the field of **cyber security of critical infrastructure** (Chapter 5)

1) It is **not possible to outsource the data platforms' critical infrastructure** from the organisation's jurisdiction area (to third parties outside physical country borders), unless there are direct steps made on national legislation level. Some data processed by critical infrastructure may be difficult to access by partners from other countries due to country level legislation which limits the setup for the energy data exchange platform.
2) It is recommended to have detailed risk assessment of the DPIA (Data Protection Impact Assessment) when outsourcing the critical infrastructure to third party provider. Regular reviews of risk assessment as well as clearly divided responsibilities are necessary to prevent data breaches.

In the **practical demonstrations of EU-SysFlex WP9** (Chapter 6)

1) Protecting personal data and managing governance of PII is supported by EU-SysFlex partners' technologies. These were successful in demonstrating cross-border security adapter deployment and use for data access, evidence creation and improved redundancy in systems.
2) The demonstrations did not prioritise the **resources for handling privacy and security by the data platform operators and service providers**. Setup shortcuts and simplifications of the data governance and management were made to execute demonstrations. EU-SysFlex WP9 partners concluded that in a production environment a more sophisticated approach for data governance is needed. This includes the handling of the accessibility of data, logging mechanisms, infrastructure for security and redundancy between all participants in data exchange scenarios.
3) The execution of the demonstrations proved that at least on proof-of-concept level **security adapters can be used cross-border** to **enable data exchange** for flexibility services. Elering's Estfeed platform was able to deliver this role of providing single access point for EU-SysFlex WP9 demonstration partners.

In the field of **tools and software solutions** (Chapter 7)

1) **Elering's Estfeed platform can be recommended as one possible solution** for building a **national data platform** and privacy respecting data exchange solutions for energy and smart meter data. The capabilities of Estfeed were well tested in WP9 and the future deployment of this solution is described in the system use cases that EU-SysFlex WP5 and WP9 focused on.
2) **Sharemind platform provided a good example** how results based on **private data can be shared between parties without the input data being exposed** to the third party service provider during the process. This proves that there are potential solutions that could be used by the system integrators and data platform providers to solve some of the privacy challenges in future energy data exchange platforms.
3) Based on the capabilities shown in demonstrations, **Black Lantern infrastructure application can be considered as an example** how critical **system logs could be protected** between different parties involved in energy data exchange. As a security solution that does not have access to shared data (using cryptography and anti-tamper hardware to achieve it) this infrastructure can be considered as a solution template in future system log security components and data exchange platforms.

1. INTRODUCTION

1.1 GOAL AND SCOPE

According to the EU-SysFlex Description of Action (DoA), the objectives of WP5 are to provide recommendations for data management in flexibility services when applied in a large scale (on an IT perspective) and to develop customer-centric data exchange model for flexible market design serving all stakeholders (TSOs, DSOs, suppliers, flexibility providers, ESCOs, etc.) and enable data exchange across the borders. The guidelines discussed in this deliverable are the result of the work conducted under the task 5.4, which aims to define data security and privacy guidelines and policies for the data exchange. Furthermore, many of these guidelines have been tested and demonstrated in the WP9.

The challenges related to data protection and potential cyber threats need to be considered when investigating the open and cross-border energy market. As the energy sector is adopting new technologies, digitalizing its systems and integrating more internet connected devices, the number of potential cyber vulnerabilities and data breeches are increasing dramatically. In 2019 the energy sector was identified as **the number one industry that was targeted by cyber-attacks** followed by logistics and automotive sectors, the software market etc.[1] according to the Hornet Security analysis.

This document explores existing privacy requirements (relevant to energy data exchange in EU) and gives an overview of the relevant legislation and cyber security standards, that provide the framework for the energy system security and data exchange and services management. In addition, this document discusses some existing and new security technologies, tools and methods that are relevant to secure energy data exchange. This document also provides an analysis of the practical implementation of these tools and presents an evaluation and suggestions on how to enhance the security and privacy for future energy systems.

In this report, the security and privacy concerns are explored in unison with the data exchange standards to clarify the aspects that need to be considered when building data centric energy services. Exchanged data falls into one of two categories: private or open. Open data covers freely available information and information that can be freely shared with all the data exchange partners and wider public. Private data is a broad category covering both personal data collected or processed and also commercially sensitive data (documents, scripts or datasets) meant for internal use by a company and for controlled sharing with other parties (e.g. energy consumption data). Personal data protection is discussed in detail in chapter 3. Not all private data has privacy concerns but can have great security value for providing the service, therefore must be protected. This is achieved by ensuring excellent cyber security which if further discussed in chapter 4.

The WP5 and WP9 of EU-SysFlex project investigate cross-border data exchange and the effects of the functioning flexibility market in cases where data sources are distributed across different countries. The aim of EU-SysFlex is to

[1] https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-energy-en.pdf

identify issues and solutions associated with integrating large-scale renewable energy sources (RES) into the grid and to create a plan to provide practical assistance to power system operators across Europe. This plan should involve data exchange requirements, including needs for further cyber security and privacy. Data exchange has increasing importance for liquid flexibility market involving a variety of services and products, with a plentiful number of flexibility providers and strong need for TSO-DSO coordination for acquiring the flexibility.

The term 'data (exchange) platform' captures in this deliverable the concepts of both 'data hub'[2] and 'data exchange platform' (DEP)[3] as defined in EU-SysFlex project, in most cases data hub acting also as DEP, unless specifically 'data hub' is considered.

1.2 STRUCTURE OF THE REPORT

This deliverable is structured as follows:

- Chapter 1 introduces the goals and scope of the document.
- Chapter 2 sets the perimeter for EU-SysFlex's cyber security policy and its relevance to the work conducted in task 5.4.
- Chapter 3 presents the privacy framework for energy data exchange and the management of data privacy under GDPR. In addition to covering the legislation side also the guidelines are provided, what needs to be focused on future flexibility energy market and interaction between different data exchange platforms (DEPs), keeping in mind the data owners' expectations and rights.
- Chapter 4 covers the general cyber security legislation landscape related to energy systems responsible for data exchange, summarizes the relevant existing standards and specifications and provides key points to be considered from the cyberthreats and risks perspective.
- Chapter 5 discusses the basic critical infrastructure cyber security aspects and how these should be applied in the energy data exchange scenarios.
- Chapter 6 provides practical examples from EU-SysFlex, focusing on energy data exchange demonstrations that were conducted under WP9, specific system use cases and the tools and techniques that were implemented.
- Chapter 7 provides a list of tools and software solutions useful for tackling the security and privacy challenges of the energy data exchange.
- Chapter 8 consolidates the outcomes and highlights of several H2020 energy security and flexibility services projects.

[2] Data Hub is an information system which main functionality is to store and make available measurements (e.g. meter data, operational data) and associated master data. Data Hubs are not necessarily centralized in a country or in a region.

[3] 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.

2. DEFINITION OF CYBER SECURITY POLICY

2.1 INTRODUCTION TO EU-SYSFLEX CYBER SECURITY POLICY

The cyber security policy of the project is based on two legal documents. Firstly, the **EU-SysFlex consortium agreement** with section 4.1 (General principles) about privacy and security, and secondly, the EU-SysFlex deliverable **M Requirement N3 (D12.3)** that is written and approved in WP12 Privacy and Cyber Security.

The goal of the aforementioned documents (EU-SysFlex confidential, not available for public) is to ensure a procedure for cyber security risk evaluation and mitigation actions, needed to manage the data handling and research results within the EU-SysFlex project. The cyber security risks within the EU-SysFlex project are central in the work packages that are responsible for demonstrations and simulations. In these parts of the project data is transported within the entities and between partners. Although the focus of this document is on the project demonstrations and the partners' work in WP4, WP6, WP7, WP8 and WP9, it relates to the protection of all research data within the EU-SysFlex project. Furthermore, as a standardised precautionary step, within the signed grant agreement all EU-SysFlex partners have verified that their company/institution will comply with vigilant data protection precautions. See **Chapter 4 Cyber security legislation and regulations** for details.

2.2 THE GOVERNANCE OF CYBER SECURITY POLICY IN EU-SYSFLEX

The governance of cyber security in the project has been the individual responsibility of each partner‘s company/institution. Each partner has had the responsibility to inform the WP leader and the EU-SysFlex PMB of any misconduct, data breach, intrusion incidents that have occurred. In such cases, appropriate actions would be put into motion in compliance with the regulations mentioned above.

2.3 CYBER SECURITY POLICY DETAILS AND RELEVANCE TO TASK 5.4

The work in WP5.4 has followed the approved measures by EU-SysFlex for handling processes, data and communication in secure way.

In 2016, the European Union formally adopted the "Directive on security of network and information systems" (NIS Directive) – the first piece of EU-wide legislation on cyber security [4]. The main objective of NIS Directive is to ensure that a common high-level security of network and information systems will be achieved across member states. Thus the Directive requires member states to take several significant measures in regard to cyber security. The NIS Directive was formally transposed into member states (and thus to EU-SysFlex partner countries) legislation in May 2018.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

The cyber security measures stated in the NIS Directive include the application of a set of binding network and information system security and incident reporting obligations to a wide range of critical infrastructure operators, termed ‘Operators of Essential Services’ (or OES), including **energy**, transport, health, drinking water supply and distribution and digital infrastructure. Evidently, also covering the domain to which some of the partners in the EU-SysFlex project belong.

3. DATA PROTECTION REGULATIONS AND JURISDICTIONS

3.1 INTRODUCTION TO DATA PROTECTION

Digital data-driven technologies have been at the centre of innovation for the last years and are continuing to enable growth for European economy. As people generate more and more data with each technological step, the focus of protection of fundamental rights must be at the heart of data collection and processing. To release Europe's potential for innovation, European Commission has been working on several initiatives in the past decade that foster development of data economy while preserving privacy, security, safety and ethical standards[5].

With General Data Protection Regulation (EU) 2016/679 (GDPR), the EU created a solid framework for digital trust that regulates personal data collection and processing. Other initiatives that have fostered the development of the data economy are the Regulation on the free flow of non-personal data (FFD), the Cyber security Act (CSA) and the Open Data Directive. Sector-specific legislation in energy sector also benefits from regulations on data access for smart metering information[6] and electricity network data[7].

Personal data collection and processing regulations are highly relevant for smart grid environment as smart grids provide near real-time information about energy consumption and generation. As the EU is continuing smart electricity meter rollout, the volume of personal data collected in energy sector will increase rapidly in the coming years. By 2019, approximately 37% of the electricity meters in the EU were smart meters[8].

ETSI defines Smart Grid as an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. [9]

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, if collected together, can lead to the identification of a particular person, also constitute personal data. Examples of personal data would be a name, a home address, and an ID card number.[10] Private data is any information that is intended to be secured from public view, regardless of inclusion of personal data.

Smart meter data is considered as personal data for several reasons. The reasons why smart meter data must be treated as personal data:

[5] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf
[6] Directive 2019/944
[7] Commission Regulation (EU) 2017/1485, Commission Regulation (EU) 2015/703
[8] https://www.euractiv.com/section/energy/news/smart-meter-woes-hold-back-digitalisation-of-eu-power-sector/
[9] https://www.etsi.org/technologies/smart-grids
[10] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

1. Data generated by smart meter (e.g., consumption data, load graphics, alerts) is associated with unique identifier, usually a smart meter identification number. For domestic use, this is directly linked with an individual responsible for the billing account and can therefore be identified among other energy consumers.
2. The information about consumer's energy consumption is used to make decisions that affect the individual. This would be to determine any charges but is not limited to billing purposes only.

In addition, as one of the aims of the smart meter rollout across the EU is to reduce the overall energy consumption, the information about the behaviour of the consumers is essential for energy suppliers and networks.[11]

Growing number of devices connected in smart grids present challenges to the protection of personal data and privacy. Smart grids facilitate collection of user data that can reveal personal information, such as habits, life-patterns, and hours spent at home[12].

Data protection is extremely important for energy DEP operators as they facilitate access to private data, and for different stakeholders like suppliers and flexibility providers as they require personal identifiable information (PII) for billing and service provision purposes. Some of this information must be kept for years, therefore ensuring all relevant consents and clear information for customers who has access to their data is extremely important for long-term data protection.

3.2 BACKGROUND ON RELEVANT REGULATIONS

General Data Protection Regulation (EU) 2016/679 (GDPR) was implemented on 25th of May 2018. General Data Protection Regulation is, as the name makes clear, a regulation. GDPR is explicitly relevant for personal data only (and no for other private data). Unlike an EU directive, it applies across all member states without the need for each country to transpose it into national law. Compliance with GDPR is required from any DEP operator and energy stakeholder in Europe but as there are further country specific regulations, those must be considered, which can complicate cross-border data exchange. Article 25 of the GDPR on data protection by design and by default requires that data controllers implement appropriate technical and organisational measures – both at the time when the means for processing is determined and at the time of the processing itself.

In addition to GDPR, there is a new upcoming privacy regulation called ePrivacy Regulation (ePR) that will be an upgrade of Directive on Privacy and Electronic communications (ePD). This directive is an older piece of legislation, enacted in 2002 and amended in 2009. It requires each EU country to pass their own national laws on data protection and privacy. It regulates several important issues, such as consent, confidentiality, spam, cookies, and treatment of traffic data. The intention of upgraded ePR is to complement the GDPR. When the regulation passes, several country-specific laws will be changed and a single data protection standard for electronic communication

[11] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf
[12] https://brusselsprivacyhub.eu/publications/ws08.html

will be created in the EU. The proposal was adopted by the European Commission in 2017 and the proposal for a regulation on a high level of privacy rules for all electronic communications includes:

- **stronger rules**: all people and businesses in the EU will have the same level of protection of their electronic communications. Businesses will also benefit from one single set of rules across the EU.
- **communications content** and metadata: privacy is guaranteed for communications content and metadata. Metadata – data that describes other data, such as author, date created and location – have a high privacy component and should be anonymised or deleted without explicit consent, unless the data is needed for billing.
- **more effective enforcement**: the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.[13]

3.2.1 GDPR RIGHTS AND SUPERVISION

Metering values are the personal data of customers. Suppliers, balance responsible parties and system operators have a natural right to access this data as part of their contractual or regulated responsibilities. Beyond that, customers should be in control of what entities have access to their metering values, and they should be able to grant third parties' access to the data if they opt to[14].

3.2.1.1 CUSTOMERS' RIGHTS

TABLE 1 CUSTOMERS' RIGHTS ACCORDING TO GDPR (BASED ON EU-SYSFLEX D5.2)

RIGHTS	DESCRIPTIONS	SUCS
To be informed	The 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.	'Manage data logs'
To have data access	The right to secure direct access of one's own personal data and to any processing, storage or sharing details.	'Authenticate data users', 'Manage data logs', 'Transfer energy data'
To correct data	The right to rectify data if it is inaccurate or incomplete.	'Erase, restrict and rectify personal data'
To erase data	The right to request the deletion or removal of personal data where tin cases where there is no compelling reason for its continued processing.	'Erase, restrict and rectify personal data'
To restrict data processing	The right to withdraw consent or restrict the processing or sharing their data. Explicit and unambiguous informed consent must be obtained.	'Manage access permissions'

[13] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[14] https://eepublicdownloads.entsoe.eu/clean-documents/news/THEMA_Report_2017-03_web.pdf

To move data	The right to request and acquire a copy of the data in a portable format.	Transfer energy data
To object to data processing	The right to object to being subject to public authorities or companies processing their data without explicit consent.	'Manage access permissions'
To avoid automated decision-making	The right not to be a subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning a person or similarly affects said person.	'Manage data logs', 'Manage access permissions'

3.2.1.2 DATA PROTECTION OFFICER

According to the GDPR, the primary role of the data protection officer (DPO) is to ensure that their organisation processes the personal data of any individual in compliance with the data protection rules. The controller and the processor must ensure that the data protection officer is involved in all issues which relate to the protection of personal data. The data protection officer directly reports to the highest management level of the controller or the processor.

Tasks of the data protection officer depend on the organisation but, according to GDPR, "at minimum these are:

1. to inform and advise the controller or the processor;
2. to monitor compliance with the GDPR and any national data protection law applicable;
3. to provide advice as regards the data protection impact assessment;
4. to cooperate with the supervisory authority and act as the contact point for the supervisory authority on issues."

3.2.2 PERSONAL DATA IN SMART GRID

As discussed above, devices connected to the smart grid can collect a lot of data. Not all of this will be personal data, but here are several examples that are classified as personal data, and any collection or processing has to follow regulations for personal data.

Specifically, for the smart grid applications, some examples of personal data would be:

- consumer registration data (names, contact information and addresses);
- usage data as it provides insight into the daily life;
- amount of energy and power provided to grid as this gives information about energy resources;
- billing data and consumer's payment method.[15]

[15] https://ec.europa.eu/energy/sites/default/files/documents/dpia_for_publication_2018.pdf

3.2.3 CROSS-BORDER DATA EXCHANGE AND DATA PROCESSING

One of the main aims of GDPR is to provide legal framework which can *remove the obstacles to flows of personal data within the European Union*. The customer's data can move from one country to another, but the rights are unaffected, therefore it must still be possible to access data.

For beneficial use of smart meters, the importance of data processing is paramount. According to GDPR, any personal data processing laws apply for both automatic and manual processing. For processing to be lawful, personal data should be processed based on the consent of the data subject concerned or some other legitimate basis. There are several legitimate reasons for processing personal data, for example collecting remote readings for billing.

GDPR articles 5-7 cover principles for processing personal data and required consent. While the regulation applies across European Union, interpretations could differ for smart meter data collection and processing. As one of the principles is data minimisation, frequent personal data collection including smart meter readings could need an explicit consent and a lawful reason.

The Danish interpretation of article 6 of the GDPR states that the frequent data collection from heat meters can be done without customer consent if the energy supplier uses that data either in the interest of the public to save energy and minimise energy losses, or for improving the energy efficiency of its operations. So, although processing of personal data is allowed, it may only take place if providers of smart metering solutions also comply with the fundamental principles set out in article 5 on processing of personal data.[16] In the UK, the energy suppliers can obtain daily readings for customers' energy consumption data without the explicit consent which can be withdrawn.[17] These two country examples illustrate how the interpretation is done. Each EU country has some deviations that need to be considered when setting up energy data exchange solutions.

Personal data which have undergone pseudonymisation, but which could be attributed to a natural person using additional information, should be still considered as personal data. According to GDPR article 26, the principles of data protection do not apply to anonymous information.

When ePR passes, this covers the following relevant parts of processing:

- Providers of services must erase or anonymize data when it is no longer needed. Keeping the data is only allowed for billing purposes or if users have given their consent. Users must also be informed why data is being processed and for how long it is held.
- Location-related data collection is only allowed if the data is anonymized. Users must be informed, consent to the service, and be given an opportunity to opt out.[18]

[16] https://www.euroheat.org/wp-content/uploads/2018/01/2_GDPR_Steen-Schelle-Jensen-Digital-Heat.pdf
[17]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758281/Smart_Metering_Implementation_Programme_Review_of_the_Data_Access_and_Privacy_Framework.pdf
[18] https://www.osano.com/articles/eprivacy-guide

3.3 GENERAL DATA PROTECTION GUIDELINES

Data protection starts with building a system that is resilient and includes several security layers to avoid data breaches. Unfortunately, data leaks from energy sectors are far from uncommon. For example, ENTSO-E, organization that ensures coordination of European electricity markets had its network compromised in March 2020[19]. In December 2020, an electricity provider in the UK reported a data breach affecting all their 270 000 customers[20]. While more incidents are reported in North America, latest from March 2021 when Eversource, the largest energy supplier in New England, suffered a data breach after customers' personal information was exposed on an unsecured cloud server.

The responsibility for data protection in EU is placed on the data collector and processor by the GDPR but according to analysis of GDPR sanctions, processors are not always compliant themselves. For example, in 2020 a Spanish energy company Iberdrola Clientes was fined twice for GDPR non-compliance, total fines exceeded €100 000. In 2021 Electricity Authority of Cyprus was fined €40 000 for 'insufficient legal basis for data processing'. One of the largest fines so far in energy sector has been 3 million euros to Italian Eni Gas e Luce[21]. Those examples illustrate how internal procedures for data collection and processing must be properly in place and monitored to ensure the highest protection of personal data and compliance with GDPR. Failure in internal data management can be costly in both fines and reputation.

3.3.1 GUIDELINES TO DATA PROTECTION MANAGEMENT RELATED TO EU-SYSFLEX WP9 DEMONSTRATIONS

The simplest suggestion for successful data protection management could be to avoid any personal data in the system operation unless absolutely necessary. This kind of separation is more challenging than expected and resources required to execute the work are often underestimated.

During the set-up of EU-SysFlex data exchange related demonstrations, it appeared that the identification of personal data usage in the processes was not obvious in all cases. The task 5.2 "Identification, description and analysis of data exchange system use-cases (SUC)" defined the system use cases specifically for personal data mapping. As the result the SUCs could be divided between two groups: those handling explicitly the private data and those that delivered rather energy business processes like aggregation, system operation, flexibility management without primary focus on PII. However, it does not mean that the latter group involves not personal data – for example, flexibility bids and flexibility activations can in some cases be considered as private data. It was concluded that the privacy and data handling processes should be considered horizontally across all use cases and demonstrations, specifically focusing on personal data management in each SUC.

Based on the questionnaire conducted in EU-SysFlex task 5.1 (*Questionnaire for learning from different data exchange models*) with the data platform operators, there was a clear indication that the privacy and personal data

[19] https://www.cyberscoop.com/european-entso-breach-fingrid/
[20] https://www.bbc.com/news/technology-55350995
[21] https://www.enforcementtracker.com/

handling was invisible in general energy data exchange landscape[22]. Privacy and GDPR were in general highly prioritised, but the mechanisms of how to apply the differentiation of personal data and general system was unclear.

When going into more detail with the possible changes and guidelines then the first suggestion to data protection management is to invest resources to create a clear understanding which systems and business processes require personal data and which do not. This will allow them to make decisions in early stages, like on the system architecture level, and not later when it would be much more costly. Similarly to cyber security domain, any early mistake in data exchange can exponentially grow and create high risk for security breaches and cyber security incidents. Patching architecture flaws at later stages is not the optimal way to approach building the energy data exchange platform.

Secondly, the compliance with the 8 rights stated in the table 1 require additional system layers that deal with the privacy and data. This means that the governance and control of the customers' data as well as exchanging the information under each data operator and energy market stakeholder (market operator, system operator, flexibility service provider) supervision must be synchronised. In the EU-SysFlex WP9 demonstrations the challenge was solved without much contradiction as the Elering's Estfeed secure adapters were used as the access point to authorisation and governance. The lesson learned from executing the demonstrations was that each participant still had to apply their own system security and privacy solution. The interaction with different partners' security components was more time consuming and complex.

Thirdly, the EU-SysFlex demonstrations in the WP9 showed that the responsibility of personal data management must be defined in more detail. In case there are third party service providers (like cloud infrastructure provider, system security service etc.) that one or the other participant in data exchange demonstration is unaware of, the responsibilities and actions should be defined. This is important to avoid the "grey areas" where parties expect that the others will cover the system security.

3.3.2 GUIDELINES RELATED TO DESIGNING THE GDPR COMPLIANT SOLUTION

Handling of the PII data has an important role in complying with GDPR. The identification of persons, based on the data that is available is becoming easier just because the massive amounts of data and links between data are growing. The use of solutions and applications in everyday lives is the main driver behind this. In relation to EU-SysFlex project and initiative to foster cross-border data exchange and energy services that rely more on data, the ways to manage PII are critical. Based on the project partners' experience here are main aspects to be emphasized.

The distancing from any PII data usage as a protection layer

There are several options to reduce personal data processing and therefore simplify compliance. Any time when anonymisation can be used, it is beneficial to process anonymous data. Often in smart metering, anonymisation is

[22] https://eu-sysflex.com/wp-content/uploads/2021/03/EUSYSFLEX-5.1.3-Report-Data-Platforms-FINAL-1.pdf

not an option, therefore the data must be protected before processing. Deploying privacy-enhancing technologies can allow high measurement intervals for smart meters while protecting PII data. Some of the examples that could be used are[23]:

- encryption of meter data – different temporal resolutions could be encrypted with different keys to serve different purposes of varying accuracy requirements and distributed on a need-to-know basis.
- masking protocols that allow for secure aggregation of meter data to hide the meter data of individual households in the sum of a number of households.
- homomorphic encryption to aggregate the meter data of multiple households.
- mesh networks to aggregate encrypted meter data hierarchically.
- privacy-preserving linkable anonymous credential protocols.

GDPR compliance by design

Planning can ensure that data processing is compliant, and system is robust. Simplified steps to follow for any GDPR compliant design are following:

- data protection impact assessment completed as part of process analysis.
- data encryption/data anonymisation.
- role based access to data.
- logging of activities.
- procedures in place to.
- contingency plan[24].

European Commission’s Smart Grid Task Force has designed data protection impact assessment template, that can be helpful in designing GDPR compliant processes. The workflow can be seen in Figure 1.

[23] https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en
[24] https://www.euroheat.org/wp-content/uploads/2018/01/2_GDPR_Steen-Schelle-Jensen-Digital-Heat.pdf

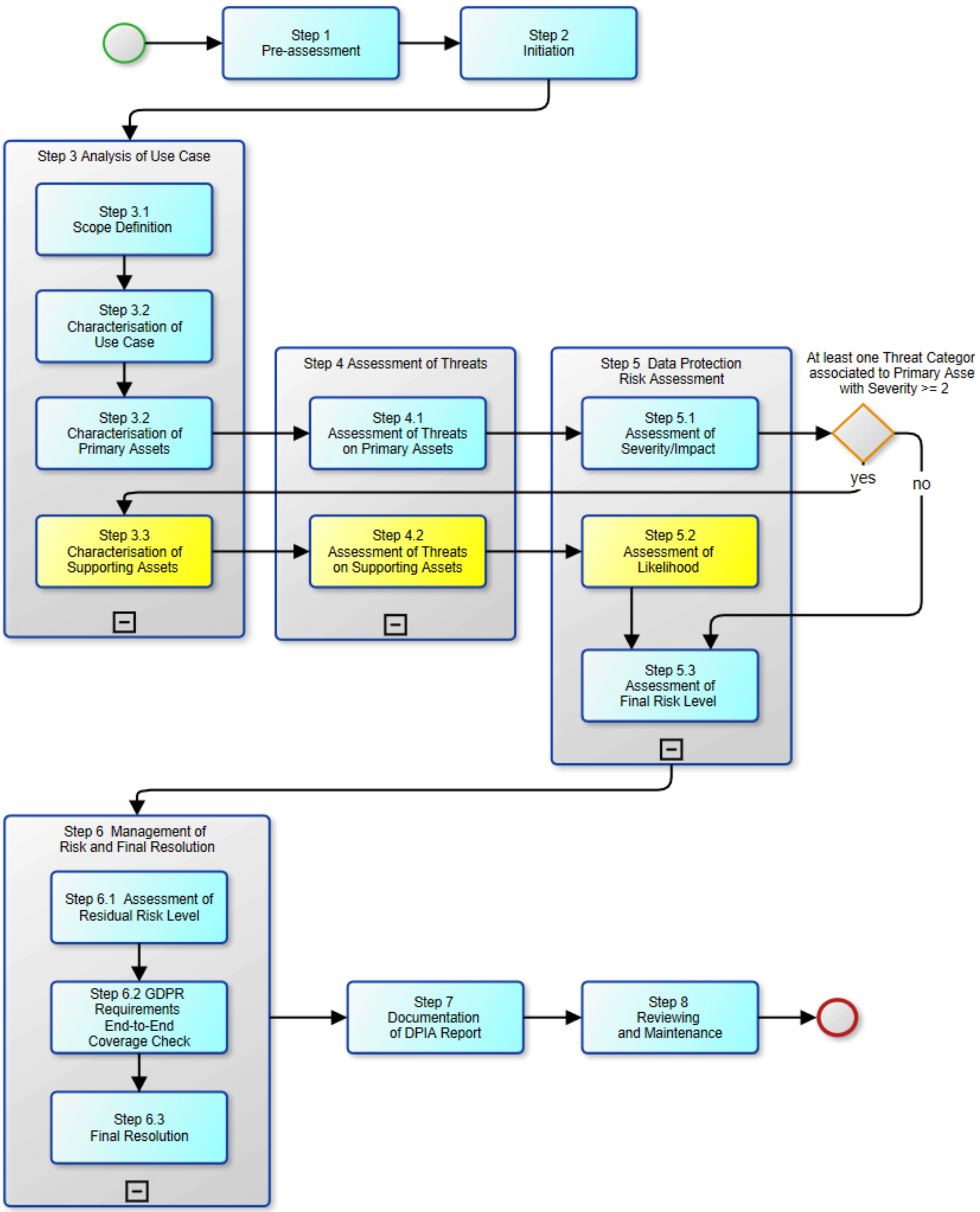


FIGURE 1 END-TO-END VIEW OF DATA PROTECTION IMPACT ASSESMENT WORKFLOW[25]

What can be quickly derived from the GDPR compliance workflow is the amount of work that is required to reach the step 7 documentation of DPIA report. When looking at the energy data exchange SUCs that WP9 is focusing on, then the complexity is growing because there is a need to consider multiple parties that interact with each other in cross-border data exchange. There are at least two major things that are achieved when system is aligned with DPIA workflow. Firstly, the in-depth analysis of the system for adding data protection assessment will also point out the areas where more efficient data management and reduction of business logic could be applied, and secondly,

[25] https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

improve the general security of the system by increasing the visibility for the operator as well as reduction of vulnerabilities (data leaks).

3.3.3 GREEN BUTTON INTIATIVE APPROACH

When looking at the practices that directly focus on complying with the personal data protection the Green button (GB) initiative stands out as a good example. GB is a bottom-up approach of putting the data owners' rights first when building the data centric services in the energy sector. From the perspective of 8 rights that GDPR gives (see table 1 in section 3.2.1.1) to customers, the Green button initiative delivers the functionality to end-users. The revocation of access rights is also supported by systems. Eventually there is much room left for the companies developing the data access services, so the GB is not a silver bullet solving the GDPR challenges and rather gives structure and coherent way of enabling easy data access keeping in mind the rights that data owners have.

"Green Button[26] is U.S. developed specification that helps utility companies provide consumption time-series data published by DSO (electricity, gas, water data etc.) to the customer directly from utility website (in CSV or XML format) or indirectly (via sharing data with third-party applications) in a secure manner to keep the anonymity of the person behind the data. A detailed description of the Green Button standard is available at the Green Button website, which also contains links to technical implementation (Green Button Data, 2020). At the moment, GB has been implemented in Ontario, Canada and 12 states within the United States, including California, New York, Arkansas, North Carolina, and others (Green Button Alliance, 2020).

GB falls under international standards (potentially complies with GDPR) and works at different scales (industrial and residential). Metered data is not currently transmitted or collected using the GB Energy Usage Information schema, although possible. The Green Button standard requires utilities to implement "The OAuth 2.0 Authorization Framework" (RFC 6749) standard's "Client Credential", "Authorization Code", and "Refresh Token" Grant flows, which generate OAuth 2.0 access tokens. The OAuth 2.0 access tokens are then required to access the utilities customer's data by the Third Party. Green Button does not participate in the wholesale market bidding and contract process. All GB transmissions require the data to be sent using SSL encryption via the HTTPS protocol and both the utility and Third Party are required to use SSL certificates issued by fully audited Certificate Authorities. Customers can request authorized access to their data by Third Parties be revoked. The NAESB REQ.21 ESPI standard defines the authorization process, which includes controlling what data can be provided to Third Parties by the utilities when implementing the standard. How a utility performs authentication, data access, authentication and authorization logging is beyond the scope of the standard (Green Button Developer, 2020)."[27]

[26] https://www.energy.gov/data/green-button
[27] https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf

3.3.4 KEY TAKEAWAYS FOR ENERGY DATA EXCHANGE IN PRIVACY AND GDPR DOMAIN

Overall, the EU wide regulations and directives are setting the rules for energy domain's data exchange in Europe. The new ePR will also strengthen the privacy of smart meter users when it passes and evens out some the differences between member states.

Three key aspects must be considered while designing and running any privacy-preserving energy data exchange. Firstly, the solution must be technically compliant with GDPR and respect all the rules of handling personal data. Secondly, the risk management forms an important part of running a data exchange platform and will have to be regularly reviewed and updated to include up-to-date information. Finally, the privacy-preserving solutions are linked to overall cyber security and to managing risk of data breaches. The cyber security risks are ever rising with increasing number of smart connected devices and digitalised networks. Digital resilience and security by design form the baseline for the compliance with the GDPR. The cyber security standards and guidelines are further discussed in the next chapter.

One more general lesson that was learned about applying privacy when executing the demonstrations was that each participant still had to apply their own system security and privacy solution. The interaction with different partners' security components was more time consuming and complex. This additional demand for resources and dedicated time must be included into planning phase when dealing with private data in demonstrations.

4. CYBER SECURITY LEGISLATION, GUIDELINES AND STANDARDS

4.1 INTRODUCTION

The core focus of the cyber security in EU-SysFlex is on bidirectional and multilateral information exchange related to national data hubs/platforms, data sources (smart meters, sub-meters, RES), and data users connected to these platforms. This includes the legislation that forms the foundation for systems operations and the practical demonstrations of WP9 covered in chapter 6 and 7.

A decade ago, discussions over security and privacy mainly focused on physical incidents in energy networks and cyber incidents in IT systems. Current trends of the European energy system are the increased cross-border market integrations and coordination needs for system operators, a rapid uptake of decentralised energy resources, and application of digitised solutions.[28] This requires an integrated view on physical and cyber security requirements.

The efforts by EU Commission and energy sector participants for enhancing security in energy resulted in several fundamental documents. The guidelines for cyber security in future energy networks will be defined by the Network Code on cyber security[29]. Based on the interim report published recently there is need:

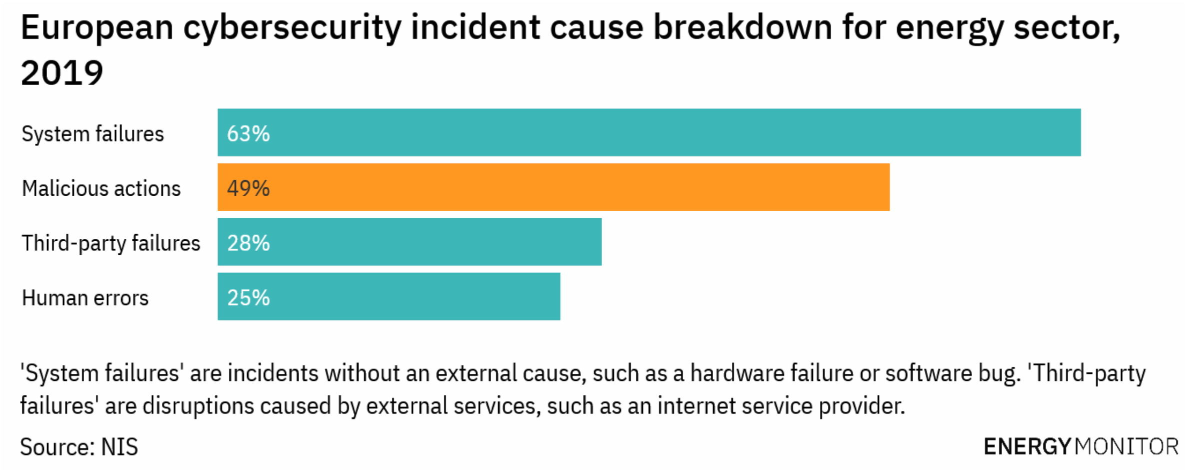
- to protect the energy system based on current and future threats and risks;
- to support the functioning of the European society and economy in crisis situation;
- to create trust and transparency for cyber security in the supply chain for components and vendors used in the energy sector;
- to harmonize maturity and resilience for cyber security across EU with defined minimum level while favouring higher maturity.

The importance of cyber security is rising in all IT domains and the energy sector is no exception. The driver for the energy sector to build cyber resilient systems and invest more resources is the raising risks from adversaries, the vulnerabilities in legacy systems and larger impact to economy and business in general, when there are failures to provide energy services. The data exchange between energy systems and related flexibility services that support the green deal initiative of EU will have heightened risk of cyber-attacks because of their importance for the business is growth in the energy sector. According to the Tripwire research study[30] there has been a constant rise of cyber security incidences in energy sector since 2016. Moreover, in the report “Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector 2018”[31] it has been highlighted that energy systems across the globe have experienced cyber-attacks. Examples of existing cases are the often-quoted attack on a Ukrainian DSO (2015), the self-inflicted incident in the Austrian TSO system due to a cross-border

[28] https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf
[29] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf
[30] https://www.tripwire.com/company/press-releases/2016/04/tripwire-study-energy-sector-sees-dramatic-rise-in-successful-cyber-attacks
[31] https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf

miscommunication (2013), and the malware targeting industrial control systems at Saudi Arabia energy infrastructure (2017). These cases illustrate how the described trends of increased cross-border operational coordination, real-time system impact and new communication layers added to legacy assets, increase the need for proper cyber security strategies implemented by energy organisations.

When looking at the overall energy sector system failures, malicious actions have been causing more energy sector breakdowns compared to human errors and third-party failures (see Figure 2).



'System failures' are incidents without an external cause, such as a hardware failure or software bug. 'Third-party failures' are disruptions caused by external services, such as an internet service provider.

Source: NIS

FIGURE 2 EUROPEAN CYBER SECURITY INCIDENTS IN ENERGY SECTOR 2019[32]

To tackle the cyber security challenges for energy data exchange and its supporting systems several security regulations and directives have been enforced. The following sections cover the relevant documents that should be considered when executing the system use cases that are defined in task 5.2. The framework presented here is furthermore applied in practice in EU-SysFlex WP9 demonstrations.

4.2 CYBER SECURITY LEGISLATION AND GUIDELINES IN EU

In this chapter the overview of the NIS directive, the selection of EU states guidelines and EU security union strategy is provided.

The Directive on Security of Network and Information Systems (known as "NIS Directive" [33]) was passed in 2016 to address some of the challenges highlighted in section 4.1. The NIS Directive is applicable since May 2018 and is implemented across the EU. The directive aims to oblige operators of essential services (OES) to apply appropriate security measures and to notify serious cyber incidents to the relevant national authority. The NIS Directive requires cyber security management and includes incident reporting obligations. Operators of essential services in the energy sector must notify incidents that have a significant impact on the continuity of their services. In case of incidents, OES must notify national single point of contact of the involved country.

[32] https://energymonitor.ai/technology/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector
[33] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Several countries, such as Germany, UK, Sweden, Denmark and Italy have published sector specific cyber security guidance to help energy sector companies focus their efforts. Others, such as Netherlands, Hungary, Spain, France and Finland, along with the NIS Cooperation Group and the European Union Agency for Cyber security have published general cyber security guidance and best practices. Many of the requirements brought by the NIS Directive have existed previously in national legislation in one form or another.[34]

In July 2020, the Commission adopted the EU Security Union Strategy, which acknowledged the increasing interconnection and interdependency between physical and digital infrastructures. It underlined the need for a more coherent and consistent approach between the ECI Directive[35] and the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the EU.

The aim is to increase the general security of the EU by improving cyber security and ensuring uninterrupted functioning of essential services. The improved cyber preparedness for organisations could reduce number of successful cyberattacks this preventing financial losses or need to lay off employees. The framework could also have wider impact on society by decreasing levels of cybercrime and terrorism.

Moreover, the increase in overall cyber security could prevent environmental damage in case of the attack on an essential service. This could affect energy and water supply and distribution sectors in particular. The NIS initiative could reduce the environmental impact by encouraging the use of efficient latest generation ICT infrastructures and services to replace less secure and inefficient legacy infrastructures. In addition, decreasing the number of costly cyber incidents in the EU, the resources could be directed into sustainable investments instead.

Furthermore, the suboptimal implementation or design of cyber security solutions in one member state could affect the level of cyber security in the other EU member states given the intense cross-border collaborations. The review of NIS directive has shown a wide divergence in its implementation by member states, including in relation to its scope and implementing the security and incident reporting obligations. Those obligations were therefore implemented in significantly different ways at national level.

Additional set of guidelines that help Member States to navigate on cyber security in the energy sector were provided by European Commission in April 2019[36]. There are three main pillars that these recommendations cover:

- real-time requirements of energy infrastructure components;
- cascading effects;
- legacy and state-of-the-art technology.

[34] https://www.twobirds.com/en/news/articles/2020/global/nis-directive-and-the-energy-sector-a-patchwork-of-national-implementations
[35] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/national-security/eci-directive
[36] https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

The update for NIS directive currently in progress will encourage more convergent approach and will strengthen the security and simplify cross-border collaborations. The draft for new legislation includes Article 22 which governs standardisations and guidelines:

1. To promote convergent implementation, the use of European or internationally accepted standards and specifications relevant to the security of network and information systems is encouraged without any discrimination or imposing of a particular type of technology.
2. ENISA will publish advice and guidelines based on existing standards.[37]

The article 22 and the actions that ENISA is taking towards upgrading energy sector security are important to follow, when building future energy data exchange solutions.

4.3 CYBER SECURITY STANDARDS

The current chapter complements the standards overview document (Proposal for data exchange standards and protocols) delivered in Task 5.5[38]. The standardisation landscape and legislative documents, covered in chapter 2 of D5.5 are the same for cyber security domain applied in energy data exchange and relevant systems. This chapter investigates specific standards that are important for ensuring cyber security when building energy data exchange solutions and executing the system use cases presented in Task 5.2.

While the cyber security standards' landscape for IT systems in general and also for the energy sector specifically is large research area, not all the relevant standards were covered in this report. The main criterion for the cyber security standards selection was the relevance towards data exchange as demonstrated in WP9. There were several important standards that were considered but not addressed in detail in this report, e.g.:

- NIST SP 800-53 rev. 5 Security and Privacy Controls for Federal Information Systems and Organizations
- ISO/IEC 29003 Information technology – Security techniques – Identity proofing
- ISO/IEC/IEE 42010:2011 Systems and software engineering — Architecture description
- ISO/IEC 27033-4:2014 Securing communications between networks using security gateways
- ISO 22301 - Business Continuity Management System

4.3.1 ISO/IEC 27002:2013 INFORMATION SECURITY MANAGEMENT FOR PROCESS CONTROL SYSTEMS SPECIFIC TO THE ENERGY UTILITY INDUSTRY

High-level description

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to:

[37] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN
[38] https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines.

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; compliance. At the end of 2021, a major update is expected in ISO/IEC 2700X:2021.

Location/area of application

ISO/IEC 27002:2013 and its predecessor (year 2005) is a cornerstone to any system that requires information security management and controlling the processes. Applicability of this standard is horizontal to energy utility systems as well as in energy data exchange related solutions.

Link to EU-SysFlex System Use Cases

ISO/IEC 27002:2013 is essential for the project as it satisfies (entirely or partially) the many SUCs from EU-SysFlex Task 5.2: 'Aggregate energy data', 'Anonymize energy data', 'Authenticate data users', 'Manage access permissions', 'Collect energy data', 'Transfer energy data', 'Manage Data logs', 'Manage sub-meter data', 'Calculate flexibility baseline', 'Exchange data between DER and SCADA', 'Manage flexibility activations', 'Manage flexibility bids', 'Predict flexibility availability'.

4.3.2 IEC 62351 POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE (DATA AND COMMUNICATIONS SECURITY)

High-level description

IEC 62351 is maintained in IEC TC57 WG15 and defines explicit security measures to protect data exchange in power systems. Besides the specification of security measures, parts of the standard also provide general guidelines for designing power systems with security in mind. The set of IEC 62351 parts covers different scenarios and applies directly to substation automation deploying IEC 61850 and IEC 60870-x protocols as well as in adjacent communication protocols supporting energy automation, like ICCP (TASE.2) used for inter-control centre communication. It also targets the integration of DER via classical protocols and already considers the application of web-based services for DER integration.

Main topics addressed in these scenarios comprise:

- mutual authentication for communicating entities in power systems using power system specific communication means;
- coordination Group on Smart Energy Grids (CG-SEG);
- cyber-security and Privacy;
- security covering complete CIA (integrity and confidentiality, integrity and availability) of data exchange between the communicating entities, realized as transport security or application layer security for serial and routed protocols;
- ensuring data availability by creating necessary data infrastructure – data exchange platforms connecting data hubs and other data sources;
- role-based Access Control;
- security monitoring and event logging;
- security architecture design recommendations.

Technical overview

A clear goal of IEC 62351 is the assurance of end-to-end security, which can be achieved on different OSI levels. The standard comprises multiple parts that are in different state of completion (see next subsection). While the focus was placed on the security of data in motion, the security for data at rest will be considered in newer parts as well.[39]

As the IEC 62351 covers the full spectrum of the communication security and logs that is a fundamental part of any energy grid system, the applicability can also be defined to any system that requires controlled communication between participants and monitoring the system. The document consists of 14 main parts that are presented in table 2.

TABLE 2 MAIN CHAPTERS OF IEC 62351

IEC 62351	Definition of Security Services for
1	Introduction and overview
2	Glossary of terms
3	Security for profiles including TCP/IP
4	Security for profiles including MMS
5	Security for IEC 60870-5 and Derivatives
6	Security for IEC 61850 profiles
7	Network and system management (NSM) data object models
8	Role-Based Access Control for Power systems management
9	Credential Management
10	Security Architecture Guidelines
11	Security for XML File
12	Resilience and Security Recommendations for Power Systems with DER
13	What Security Topics Should Be Covered in Standards and Specifications
14	Security Event Logging and Reporting

[39] https://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CGSEG_CSP_Report.pdf

The positioning and applicability of IEC 62351 standard can be shown if it is compared to other communication standards. The main communication standards that provide input to IEC 62351-5 are IEC 60870-5-104 & DNP3 and the IEC 60870-5-101 & serial DNP3. On the other side, IEC 62351 has direct connection to providing baseline and input to the IEC 62251-3 Profiles including TCP/IP. Other dependencies to the IEC 62351 that can be highlighted, are IEC 60870-6 TASE.2 (ICCP), IEC 61850-8.1 with MMS and IEC 61850-8.2 XML over XMPP. They provide input to Profiles including MMS and similar Payloads. There is also direct link between IEC 62351-11: Security for XML Files and the IEC 61970 & IEC 61958 CIM.

From technical perspective one of the most important part of the standard is part 4. “Profiles including MMS and derivatives”. This part of IEC 62351 specifies security requirements both at the transport and the application layer. First by primarily providing support at the application layer for authentication during handshake for Manufacturing Message Specification (MMS) it also provides support for extended integrity and authentication both for the handshake phase and for the data transfer phase. It provides energy systems for shared key management and data transfer encryption at the application layer and it provides security end-to-end (E2E) with zero or more intermediate entities. IEC 62351 part 4 provides the support for systems based on MMS, i.e. systems using an Open Systems Interworking (OIS) protocol stack together with support for application protocols using other protocol stacks e.g. and Internet protocol suit.[40]

Link to EU-SysFlex System Use Cases

The IEC 62351 satisfies (entirely or partially) the following SUCs from EU-SysFlex Task 5.2: ‘Aggregate energy data’, ‘Anonymize energy data’, ‘Authenticate data users’, ‘Manage access permissions’, ‘Collect energy data’, ‘Transfer energy data’, ‘Manage data logs’, ‘Manage sub-meter data’, “Verify and settle activated flexibilities”, ‘Calculate flexibility baseline’, ‘Exchange data between DER and SCADA’, ‘Manage flexibility activations’, ‘Manage flexibility bids’, ‘Predict flexibility availability’.

4.3.3 ISO/IEC 27019 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY CONTROLS FOR THE ENERGY UTILITY

High-level description

ISO/IEC 27019[41] covers a range of security techniques, including physical and digital security. The key areas for digital security are access control, operations’ security including logging, and communications security. The standard also covers security incident management and ensuring compliance.

Location/area of application

With the growing importance of Advanced Metering infrastructure (AMI), the application area of IEC 27019 is also raising. When countries are upgrading their national and regional smart meter infrastructure the use of the standard is done in parallel. Same dynamics applies when building new RES infrastructure is deployed.

[40] https://webstore.iec.ch/publication/30079

[41] https://webstore.iec.ch/preview/info_isoiec27019%7Bed1.0%7Den.pdf

Technical overview

The main area this standard focuses on central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices.

In relation to the EU-SysFlex data exchange and system use cases the three areas in relation to this standard need to be highlighted. Firstly, the supporting information systems used for the process control domain. This document includes descriptions of supplementary data visualization handling, how to execute controlling, monitoring, data archiving, historian logging, reporting both for the visibility and documentation and evidence purposes. Secondly, providing examples for the AMI components, including the smart meters and measurement devices. Thirdly, covering techniques of the software, firmware and applications installed on above-mentioned systems contributing to DMS (Distribution Management System) applications or OMS (Outage Management System).

In addition to these areas, the following technologies listed below that are more related to AMI deployment, are covered in the document. These areas are less related to data exchange and fall into the domain of physical and digital security of infrastructure and SCADA:

- Digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements.
- Communication technology used in the process control domain, covering the networks, telemetry, telecontrol applications and remote-control technology.
- Digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms.
- Energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations.
- Distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations.[42]

Link to EU-SysFlex System Use Cases

The ISO/EIC 27019 satisfies (entirely or partially) the following SUCs from EU-SysFlex Task 5.2: ‘Authenticate data users’, ‘Manage access permissions’, ‘Transfer energy data’, ‘Manage data logs’.

4.3.4 IEC 62443 INDUSTRIAL COMMUNICATION NETWORKS - IT SECURITY FOR NETWORKS AND SYSTEMS

High-level description

IEC 62443[43] is not a single specification but provides a relatively complete framework of specifications. The individual parts cover common definitions, and metrics, requirements on setup of a security organization (ISMS related), and processes, defining technical requirements on a secure system, and to secure system components. The document is grouped into four clusters covering:

[42] https://www.iso.org/standard/68091.html
[43] https://webstore.iec.ch/searchform&q=62443

- common definitions, and metrics;
- requirements on setup of a security organization (ISMS related), and solution supplier and service provider processes;
- technical requirements and methodology on a secure system at system-wide level;
- requirements to the secure development lifecycle of system components, and security requirements to such components at a technical level (broken down from the system-wide requirements).

In IEC 62443 (information technology) security requirements are presented through different automation domains, including energy automation, railway automation, building automation, process automation, and others (CEN-CENELEC-ETSI CG-SEG, 2016). The security life cycle, organisational security, and system/components security guidelines that the IE 62443 provides make it relevant to EU-SysFlex from the data exchange perspective.

Location/area of application

IEC 62433 application area covers the entire energy sector including how future energy flexibility market participants should set up organisational, system and component level security.

Technical overview

These are the technical requirements that IEC 62433 focuses on:

- Authentication control Account management, PKI, etc.
- Use control Authorization, session management, audits, etc.
- System integrity Communication, session & data integrity, malware protection, etc.
- Data confidentiality Data encryption and secure purging of old data
- Restricted data flow Network, applications and device partitions
- Timely response Monitoring, logging and timely response
- Resource availability Smart resource management, system backup, etc.
- Application requirements malware protection mechanisms, mobile code extra security
- Embedded requirements secure booting, malicious code protection, etc.
- Host device requirements secure booting, malicious code protection, etc.
- Network device requirements authentication, RBAC (role-based access control), secure booting, etc.

From the cyber security risk assessment view the IEC 62433 applies a principle of a complex automation system structured into zones that are connected by so called “conduits”. For each zone, the targeted security level (SL) is derived from a threat and risk analysis. The threat and risk analysis evaluates the exposure of a zone to attacks as well as the criticality of assets of a zone. IEC 62443 defines security levels and zones for the secure system design and the security requirements that must be met to reach a certain SL. From the structure, each security requirement consists of a baseline requirement and zero or more requirement enhancements to strengthen security and thus increase the SL (CEN-CENELEC-ETSI CG-SEG, 2016).

Link to EU-SysFlex System Use Cases

The IEC 62433 satisfies (entirely or partially) the following SUCs from EU-SysFlex Task 5.2: ‘Aggregate energy data’, ‘Anonymize energy data’, ‘Authenticate data users’, ‘Manage access permissions’, ‘Collect energy data’, ‘Transfer energy data’, “Manage data logs’, ‘Manage sub-meter data’, ‘Calculate flexibility baseline’, ‘Exchange data between DER and SCADA’, ‘Manage flexibility activations’, ‘Manage flexibility bids’, ‘Predict flexibility availability’.

4.3.5 IEC 61508 FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS

High-level description

IEC 61508 is an international standard published by the International Electrotechnical Commission consisting of methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems. It is titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). IEC 61508 is a basic functional safety standard applicable to all kinds of industry. It defines functional safety as: “part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.” The fundamental concept is that any safety-related system must work correctly or fail in a predictable (safe) way.

Location/area of application

While being widely adopted by the car and machinery industry there can be some uptake also in the energy production (power plants with critical processes and risk mitigation activities) as well as in metering points (validation and auditing).

Technical overview

The IEC 61508 consist of 7 parts: General requirements, Requirements for electrical/electronical/programmable electronic safety-related systems, Software requirements, Definitions and abbreviations, Examples, Guidelines and overview of techniques and measures.

Central to the standard are the concepts of probabilistic risk for each safety function. The risk is a function of frequency (or likelihood) of the hazardous event and the event consequence severity. The risk is reduced to a tolerable level by applying safety functions which may consist of E/E/PES, associated mechanical devices, or other technologies. Many requirements apply to all technologies but there is strong emphasis on programmable electronics especially in the software requirements related to this.

IEC 61508 has the following views on risks:

- Zero risk can never be reached, only probabilities can be reduced.
- Non-tolerable risks must be reduced.
- Optimal, cost effective safety is achieved when addressed in the entire safety lifecycle.

Specific techniques ensure that mistakes and errors are avoided across the entire life cycle of information systems. Errors introduced anywhere from the initial concept, risk analysis, specification, design, installation, maintenance and through to disposal could undermine even the most reliable protection. IEC 61508 specifies techniques that should be used for each phase of the life cycle.[44]

Link to EU-SysFlex System Use Cases

The IEC 61508 satisfies (partially) the following SUCs from Task 5.2: 'Manage access permissions', 'Collect energy data', 'Manage data logs', 'Manage sub-meter data'.

4.3.6 CEN/TR 17167 COMMUNITCATION SYSTEM FOR METERS

High-level description

The CEN/TR 17167[45] Communication system for meters is standard that covers wide range of security mechanisms, protocols to be used, specification for the Application Layer for meters, applying communication cycles, access control and overall structure of the Object Identification System (OBIS) and the mapping of all commonly used data items in metering equipment to their identification codes.

The standard consists of the following parts: Data Exchange, Wired Meter Bus Communication, Application protocols, Communication systems for meters and remote reading of meters (incl. Wireless meter readout), Wireless M-Bus relaying, Local Bus, Transport and security services, Examples and supplementary information[46].

Location/area of application

Application area needs some more interaction from the industry side to collect feedback how it can be used in larger scale. The expansion of smart meter infrastructure instances will contribute to wider use of the CEN/TR 17167.

Technical overview

The Data exchange portion of the standard covers M-Bus connections and the set-up of data flows, including the twisted pair M-Bus link layer, Baud rates, data writing permissions, output/input configuration and metadata collection (consumer information etc.). The core elements of this standard are M-Bus protocol layers. The upper M-Bus protocol layers can be used with various Physical Layers and with Data Link Layers and Network Layers, which support the transmission of variable length binary transparent messages. The Upper M-Bus protocol layers have been optimized for minimum battery consumption of meters especially in case of wireless communication. Moreover, the standard covers the optimisation of the resources on board the smart meter, managing the security threats and providing data flow, frequency according to business requirements. The applicability examples of this standard give a system developer an excellent basis how to implement this information to industry scale solutions.

[44] https://en.wikipedia.org/wiki/IEC_61508
[45] https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:61828,6275&cs=18819BFC6B1C078A25D18DB396F7B6A44
[46] https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:61822,6275&cs=11F1FF49B726A0CAD275A261977CC8533

Link to EU-SysFlex System Use Cases

The CEN/TR 17167 satisfies (entirely or partially) the following SUCs from Task 5.2: 'Authenticate data users', 'Manage access permissions', 'Manage data logs', 'Collect energy data', 'Transfer energy data', 'Manage sub-meter data'.

4.4 KEY TAKEAWAYS FROM CYBER SECURITY LEGAL AND STANDARDS' REQUIREMENTS

The underlying legislation that gives the fundamental guidelines for these recommendations are set by the European Union NIS Directive (Directive (EU) 2016/1148) and the GDPR Regulation (Regulation (EU) 2016/679).

Before EU-SysFlex project conducted its work in cyber security the basic principles that shape the focus in cyber security in energy data exchange domain can be highlighted from the Smart Grid Task Force Expert Group 2 report (2019)[47]:

1. "Protect the energy system based on current and future threats and risks.
2. Have effective plans in place to ensure that an energy crisis is managed, to limit the effect upon the European society and economy.
3. Create trust and transparency for cyber security in the supply chain for components and vendors used in the electricity subsector.
4. Harmonized maturity and resilience for cyber security across EU with defined minimum level while favouring higher maturity using a risk-based approach."

These four focus areas can be used as a guideline to address cyber security in organisations and cyber security challenges of European electricity energy system. From the data security perspective and enabling the energy data exchange between energy network participants the two areas to invest are protection against the cyberthreats and the creation of trust and visibility. More specifically, for EU-SysFlex project creating trust and having harmonised approach for cyber security is critical to enable the business between different platforms and in cross country energy market. The governance model between interacting energy systems and common way to detect, communicate and respond to threats are needed. The analysed existing standards (see chapter 4.3) cover minimum cyber security requirements for energy system and data exchange management, critical infrastructure implementation and operational part, and cyber threat. Nevertheless, the interaction between organisations and technical limitations hinder achieving the common goal of having higher cyber resilience and risk management capability.

The main obligations that are set for energy grid operators (from NIS directive) are:

- a specific Computer Security Incident Response Team (CSIRT) at Member State level should be established;
- the necessity to identify the operators of essential services (OES) including energy operators. Those energy operators identified as OES will have to implement appropriate security measures with principles that are general to all sectors;

[47] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

- the operators of essential services will have the obligation to notify incidents to their relevant National Competent Authority (NCA). SGTF EG2 is adding several recommendations that are helping to understand how to approach these obligations as well as focus on joint effort for new security measures.

The recommendations outlined in this report can be summarized in three main sections:

- Baseline Protection for Energy System Operators
    - Information Security Management System set-up (ISO/IEC 27001:2013) with consideration of ISO/IEC 27002:2013 and ISO/IEC 27019:2017.
    - Minimum security requirements protecting the EU Energy System (utilizing the EU Cyber security Act).
- Advanced Cyber security Implementation for Energy System Operators of Essential Services
    - Protection of current infrastructure.
    - Supply chain risk management process.
    - Protection against cross-border and cross organisational risks through proper analysis and risk treatment.
    - Active participation in an early warning system.
- Supportive Elements and Tools
    - Sector-specific guidance on crisis management for operators.
    - Sector-specific guidance on supply chain security for operators.
    - Energy cyber security maturity framework (a tool to assess maturity and to steer cyber security implementation).

European Commission and European associations of system operators (e.g. see announcement of ENTSO-E[48]) believe that next network code in the energy field should be for cyber security issues. This would rely on the work already conducted by SGTF EG2. Also there is already draft framework guidelines for network codes issued recently by ACER, that is under public consultation (next version targeted end of June 2021), and will be affecting the landscape of the security solutions in energy sector[49].

In conclusion, the multifaceted reasons for “grey areas” in security should be further investigated, especially in those cases where security solutions are purchased from third parties that cover only part of the energy supply chain. The weakest link of a security system are the user and level of cyber hygiene as the exploitability options for the adversaries are unlimited. It is critical to put more emphasis and effort into testing and training of personnel to be compliant with their task-related security requirements.

[48] https://www.entsoe.eu/news/2020/05/26/response-to-the-european-commission-s-public-consultation-to-establish-the-priority-list-of-network-codes/

[49] https://www.acer.europa.eu/Official_documents/Public_consultations/PC_2021_E_04/Draft%20Framework%20Guideline%20on%20sector-specific%20rules%20for%20cybersecurity%20aspects%20of%20cross-border%20electricity%20flows.pdf

5. INFRASTRUCTURE REQUIREMENTS FOR ENSURING CYBER SECURITY

5.1 INTRODUCTION

The proposal for Network Code on cyber security defines the objective to protect energy systems from current and future threats and risks as a priority. The role of the infrastructure setup cannot be underestimated to fulfil this task.

Energy sector participants function in a complex digital resilience and infrastructure setup reality. The legacy systems, possibly not even meant to have live access over internet are combined with supporting systems, in combination with IoT devices and large amount of connection points. This mix of different technology lays a heavy burden on how the infrastructure security is preserved, as the sensors may have limited cyber resilience capabilities. Eventually the failure on the infrastructure level from “add on” system can lead to security breach or in worse case failure to provide the energy services.

There are two main scenarios of data exchange platforms for TSOs/DSOs that are used for infrastructure. The first option is building and operating the infrastructure “in house” and the second option is using a third-party service to offer necessary setup for the data exchange.

Outsourcing (a part of) the data exchange solution means that responsibilities (security included) are shared between multiple parties. This can cause adversaries to exploit the situation where responsibility is not defined throughout the full value chain and attacking weakest links of the system become possible. The general practice in such scenarios is to apply the general service level agreement of the infrastructure provider (telecom operator, cloud infrastructure provider etc.). The problem lies in the fact that the data hub/platform operator is securing only a portion of the whole data flow. The full chain of custody from the metering points (smart meters generating the results) to low voltage grid data node, to central data hub/platform, the data fusion, including customer portal or Customer Response Management (CRM) input and eventually the delivery to service provider, making use of the data is not covered by this infrastructure provider. This leads to possible areas where data breach could happen without the clear indication who is responsible. To be more precise, a shared responsibility model that is improperly defined could lead to blurred lines between data infrastructure provider’s and other value chain parties’ security responsibilities resulting eventually in data breach. In every situation, the responsibility always stays with the Data Controller. The goal is to protect the data and prevent data breaches along the full cycle and be able to find responsible parties if incident happens.

There is always a trade-off of cost of security/privacy when deciding to allocate investments into system data breach prevention. Critical point to address, when dealing the data breaches is how to collect the evidence when different parties are responsible for the sections of the data exchange. These grey areas during data exchange prevent system operators to agree on the responsibility when getting the service from infrastructure provider.

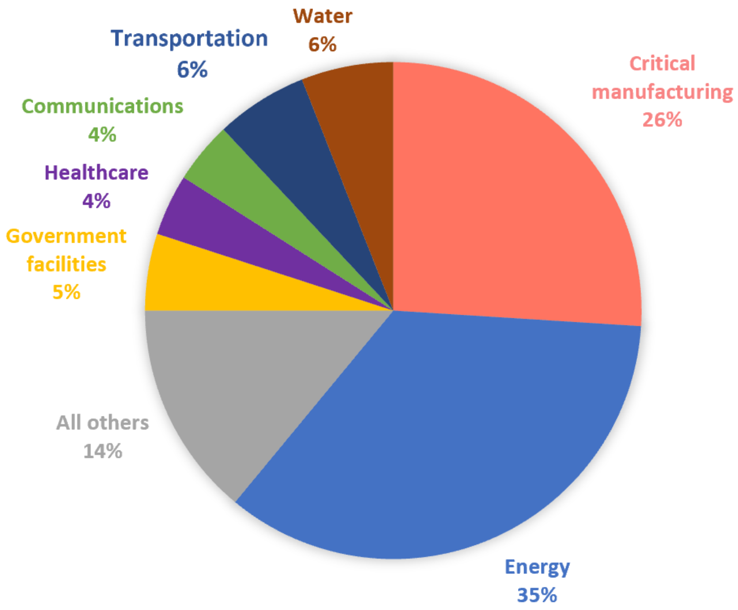


FIGURE 3 CRITICAL INFRASTRUCTURE CYBER INCIDENTS[50]

There is a tendency not to report publicly most cyber incidents in any sector, including energy sector. Nevertheless the seriousness of cyber threats for energy sector infrastructure can be presented, when comparing the number of the cyber incidents against energy critical infrastructure with other sectors like government, healthcare and manufacturing. The energy sector has become a prime target for cyber attacks in past years. This is presented in Figure 3 above. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports that from 2013 to 2015, out of 796 incidents there were 35% of attacks against the energy sector critical infrastructure.

There are dangers of improper management of cyber security for energy sector. This is cross-sector problem covering the energy, gas, water critical infrastructure horizontally[51]. In the case of exposed metering infrastructure, low voltage substation system or supervisory control and data acquisition (SCADA) systems, we can reliably say, based on past research Trend Micro has carried out, that such systems are indeed of interest to attackers — and have been for quite some time now. Based on the Trend Micro Forward Looking Threat Research (FTR) team report published in 2013, there is a real horizontal threat to the infrastructure. "Research that were carried out to explore exactly this. In the first research, we set up a global network of 12 high-interaction honeypots that mimicked water plants using a combination of real-world SCADA equipment and custom machines designed to look exactly like the network of real facilities we had examined in the past. In the experiment, every single system was attacked, with 15 percent of those attacks considered critical, i.e., would have caused catastrophic failure in the equivalent real-world environment. Not only are critical systems from the water, energy and similar industries exposed and vulnerable on the internet today — they are also an active target for attack."[52] This can be similarly transferred to the situation where low level (low voltage network, customer metering points) data sources, like smart meters can be attacked to affect the services on a much higher level. Eventually leading to failure to provide service on a much wider coverage.

[50] https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf
[51] https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf
[52] Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries

In addition to the general view of threats to energy sector, if we look at the more detailed level of the energy system architecture that is dedicated to data exchange, there are multiple areas that require various and adequate level of security. Even if the provider/consumer of the energy data is not directly connected to the critical infrastructure the use of certificates, encryption, monitoring tools and sophisticated access controls should be applied. This can be seen in the architecture example of data exchange between DSO, TSO, service provider, auditor and aggregator displayed in figure 4.

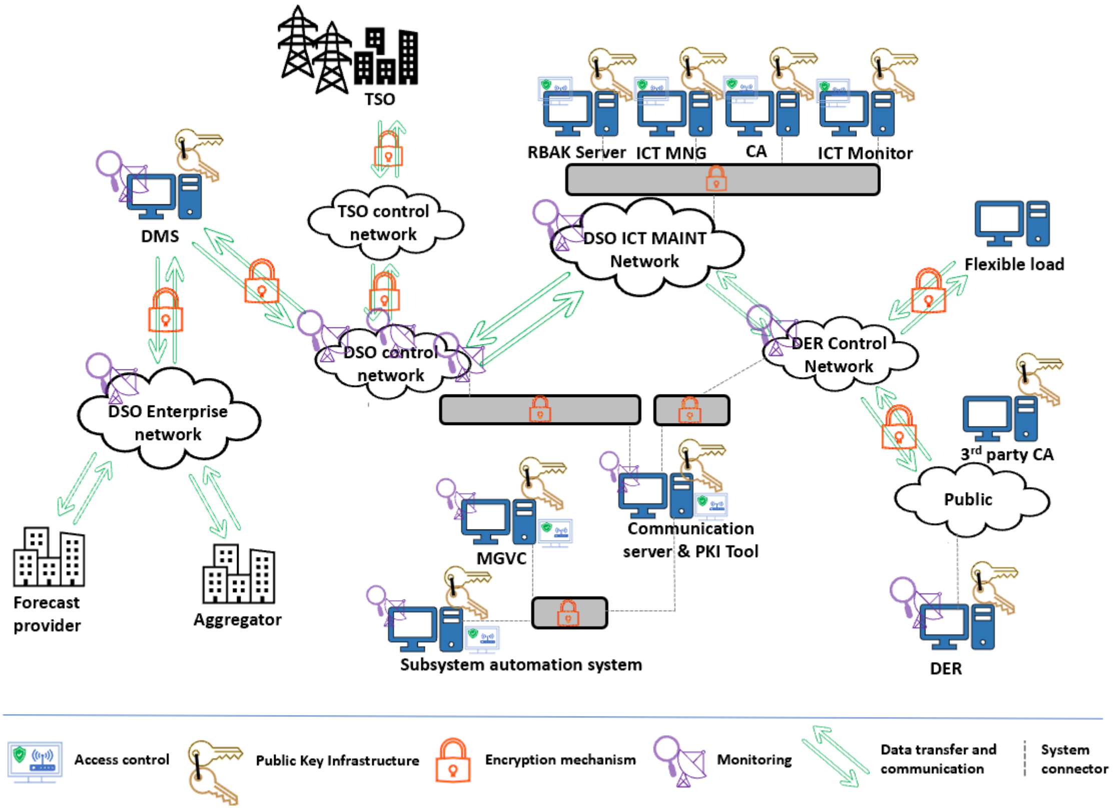


FIGURE 4 ARCHITECTURE EXAMPLE FROM CEN-CENELEC-ETSI CG-SEG - CYBER SECURITY AND PRIVACY REPORT[53]

An overview of secure architecture of a use case is presented in Figure 4 where, starting from the security requirements of the use case, the main solution standards have been integrated into the DER Control component architecture. As the main communication channels are protected by means of the authentication and encryption mechanisms recommended by IEC 62351 parts 3-4-5-6 (represented by a lock). A digital certificate-based system (Certification Authority – CA in the picture) is deployed in order to guarantee the authentication of the different parties exchanging information, as recommended by IEC 62351-9. To monitor and detect anomalies a structure for capturing and analysing monitoring objects and log information is developed where different monitoring agents are scattered over the ICT architecture. These agents may perform local analysis and create alarms and/or report values to server agents placed at the ICT maintenance centre where a global view of the ICT systems is supervised by operators and correlation functions are performed enabling the application of automatic recovery measures. In operational systems, there are limitations to what extent automatic recovery can be used and manual mechanisms are also in place.

[53] https://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CGSEG_CSP_Report.pdf

5.2 CRITICAL DATA INFRASTRUCTURE REQUIREMENTS

In electricity subsection of energy sector, infrastructures and facilities for generation and transmission of electricity in respect of supplying electricity are considered critical infrastructures according to Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[54]. ENISA conducted desktop research on international security standards, guidelines and good practices per sector and the security requirements for OES were mapped to international standards used by operators covering all business sectors under scope. The electricity sector standards and good practices are outlined in table 3 and further discussed below.

TABLE 3 INTERNATIONAL STANDARDS AND GOOD PRACTICES APPLICABLE ACROSS THE ELECTRICITY SUBSECTOR[55]

SUBSECTOR	STANDARDS	GOOD PRACTICES
Electricity	• NIST SP800-82 Guide to Industrial Control Systems (ICS) Security • ISO 27019 -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. • NERC CIP Series "Critical Infrastructure Protection Cyber Security": CIP–002 to CIP-011. • IEEE STANDARD 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security • IEC 61850 - Power Utility Automation	• Cyber security model electricity subsector cyber security capability maturity model (es-c2m2) - U.S. Department of Energy • NISTR 7628 - Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements • ENISA Appropriate security measures for Smart Grids - ENISA • Best practices for handling smart grid cyber security - California Energy Commission

One of the challenges many Security Directors and Managers have to deal with is a lack of understanding about what security risk is[56] but it is essential to assure: 1) the integrity of the Assets (systems providing services, data flow, infrastructure), 2) the reliable supply of energy (energy service downtime as a most critical metrics), 3) the health of the workers, 4) the health and security of the public and 5) sustainable and protected environment. This report focuses on the first component, the assets integrity, and how the supporting infrastructure should be operated. A crucial step in understanding the security risk is having the necessary information. The goal of the practises and standards, presented in Table 3 is to create a common understanding, how energy systems operate. This helps to share the experience (malfunctions, cyber incidents, data breaches) between energy sector participants and learn how to patch, build and design more cyber-resilient systems. From the critical architecture

[54] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
[55] https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/
[56] https://ec.europa.eu/home-affairs/sites/default/files/e-library/docs/pdf/2010_reference_security_management_plan_en.pdf#zoom=100

perspective this learning curve is extremely important because infrastructure set-up the decisions usually last 10-20 years.

5.3 KEY TAKEAWAYS FROM INFRASTRUCTURE REQUIREMENTS

There is a shift from air-gapped SCADA networks to the automated and remotely accessible solutions in energy sector. This is even more true in the case of deploying and operating data hubs and data exchange platforms that are serving as an easy, single access point for smart meter distributed infrastructure. There is gradually growing risk that when adding more data sources, and services that require access to data the security breach will happen. Compared to the air-gapped, single owner setup, it requires a different approach and sharing of responsibility.

It is not possible to outsource the critical infrastructure from the organisation jurisdiction area, unless there is specific country level legislation that allows it. This constrains the setup for the energy data exchange platforms.

It is recommended to have detailed risk assessment in the form of the DPIA when outsourcing the critical infrastructure relevant to data exchange to third party provider. The main goal is to protect the data from the beginning. In the situation where the security is breached, the reduction of “grey areas” between participants who share the infrastructure is extremely important.

Infrastructure management costs are not to be underestimated for security. Adding additional security layers in later stages can be high cost and low reward for system operator.

6. COLLECTION OF PRACTICAL GUIDELINES AND EXAMPLES BASED ON EU-SYSFLEX WP9 DEMOS

6.1 INTRODUCTION

This chapter draws together the guidelines and regulations presented in preceding chapters and practical examples from the EU-SysFlex project with the focus on the energy data exchange demonstrations conducted in WP9. Specific SUCs with corresponding techniques and available tools are also discussed. Finally, the key lessons learned from the practical demonstrations are highlighted.

The horizontal common view of the privacy and cyber security management is provided by using EU-SysFlex task 5.2 **system use cases** as a baseline. The reflections from some of these use cases and the tools owned by each WP9 partner are used to demonstrate secure energy data exchange. Not all the SUCs from the D5.2 are explicitly related to privacy and cyber security. Based on the use case analysis conducted in **D5.2** "**Description of data exchange use cases based on IEC 62559 methodology**"[57] there were 6 SUCs that were essential to security demonstration. These 6 baseline SUCs are:

- 'Anonymize energy data'.
- 'Authenticate data users'.
- 'Manage access permissions'.
- 'Erase, restrict and rectify personal data'.
- 'Manage data logs'.
- 'Manage sub-meter data'.

In addition to the link to D5.2 there are also findings from D5.5 that are related to privacy and cyber security standardisation. These statements are evaluated to some extent in the demonstrations with the goal to provide their relevance to the practical examples.

The 6 key findings in **data exchange standards and protocols (D5.5)**[58] that are reflected in this report are:

1) Regarding data user's authentication, the right to access own data as well as the ability to share information related to authentication and representation rights are addressed in some specifications but not explicitly in standards.
2) Regarding consent management some specification exist but no explicit standards for giving and sharing access permissions.
3) Regarding personal data management it is addressed in some specifications and standards but not explicitly about sharing erasure and rectification information.
4) Ability to share information related to data logs has very limited coverage in standards.
5) Additional CIM coverage for personal data portability, for access to own data, and for transfer of personal data to other parties is recommended, incl. cross-border.

[57] https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex-Task-5.2-D5.2-FINAL.pdf
[58] https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf

6) CIM coverage is recommended for sharing access permissions (consent management) between data owners, concerned DEPs, applications and data sources. The CIM profiling of 'Customer Consent' business object confirmed the need for CIM extensions.

The following sections of this chapter further discuss energy data exchange challenges with the focus on privacy and cyber security based on the seven WP9 demonstrations.

6.2 CYBER SECURITY DEMO – GUARDTIME

Introduction:

The general goal of the demonstration was to provide high security service from a third party (incl. for infrastructure) to encrypt, sign and store critical system logs of data exchange platforms. Additionally, it was also important to provide the capability of mitigating various attack vectors including MITM attacks, malware embeds or physical attacks.

The key differentiating features about this demonstration were related to data security and confidentiality. Features that were illustrated during the demonstration:

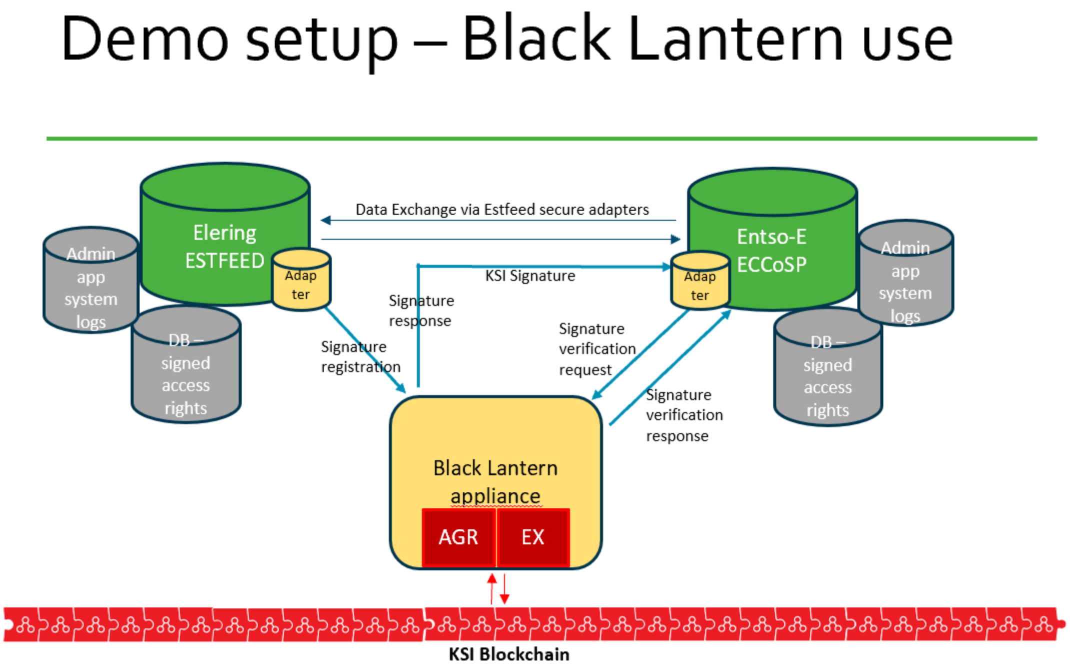
- the control for accessing logs was staying on customer side as a new security authority,
- the service provider (providing the log security and infrastructure) had no access to data received from the users that were involved in log management and sharing.

In the cyber security demonstration, the goal was to assure the security of the processes and the logs in the situation where there are multiple trusted parties involved among participants that exchange relevant energy data. During the demonstration, additional security layer was added to provide the system logs' alternative validation and verification functionality and use them as evidence where needed. The case of data exchange between ENTSO-E's and Elering's platforms was selected for the demonstration. Both, the ECCo SP test network and Estfeed platform were part of the demonstration.

The functionalities that were addressed in the demonstration included:

- Administration of application logs and log feed
- Logs' storage mechanism
- Third party infrastructure instance (Black Lantern (BL) protocol to send/receive logs)
- Adapter and session generation (BL and logs data source (Estfeed, ENTSO-E)
- Infrastructure and adapter configuration tool (including governance)
- Key management (Master admin key (Organisation) + Query mechanism)
- Visualisation tool and data feed
- Events sequence mechanism (presenting the log evidence)

The basic concept for this demonstration is presented in figure 5.



Demo setup – Black Lantern use

FIGURE 5 CYBER SECURITY DEMONSTRATION MAIN COMPONENTS AND SETUP

The components involved in the demonstration were:

- TSO system 1 (Estfeed) admin application
- TSO system 2 (ECCo SP) admin application
- System logs (using syslog)
- Adapters (Communication protocol, encryption, sign and verify process)
- Anti-tamper hardware Black Lantern instance (gateway, storage)
- KSI Blockchain access for eIDAS compliant signature service

Relationship to SUCs:

This solution is closely related to the 'Authenticate data users', 'Manage access permissions', 'Manage data logs'.

Demo description and security guidelines:

Two main building blocks used to run the demonstration were **the KSI Blockchain technology** stack and the **Black Lantern Anti tamper hardware**. In addition to the existing security features provided by the Estfeed secure adapter, the log security component and hardware were be used to offer integrity of security logs.

Two use cases were shown during the cyber security demo:

- Integrity of logs – During demonstration Black Lantern infrastructure was deployed and it provided access to the KSI blockchain service to enable KSI functionalities of providing the signatures to achieve log integrity. Besides the log integrity Black Lantern provided a secure gateway for KSI services and reduced the risk from potential attack vectors. From the end-user perspective, access to log security component via Black Lantern is invisible as it was operating in the background. Two system operators in data exchange demo could select

KSI Blockchain based log security in addition to RFC3161 time stamping service used in the Estfeed secure adapter.

- Log storage – In addition to providing KSI Blockchain access, Black Lantern was used as a secure log storage. The goal was to offer an alternative log protection solution for the data exchange in addition to the existing security module running in the Estfeed platform. From the end-user perspective, when Guardtime's security module was selected for securing the logs, it provided secure storage of the logs, verification of integrity of stored logs, and export of logs with proof of integrity.

The interaction between the Estfeed – ECCo SP data exchange demonstration and added elements from cyber security demonstration can be seen in figure 6.

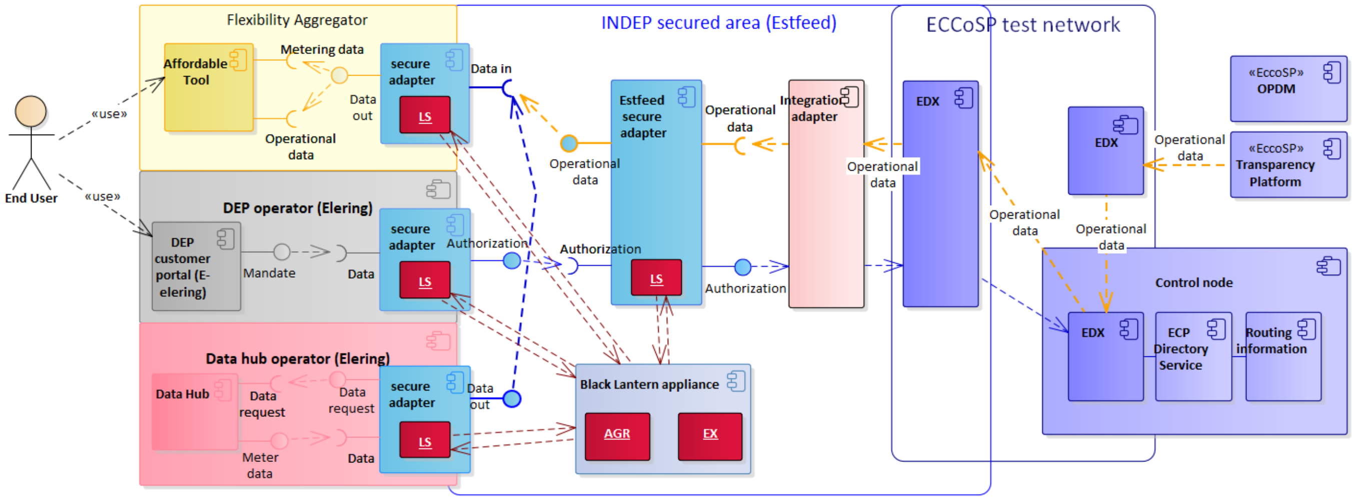


FIGURE 6 ELEMENTS OF CYBER SECURITY DEMONSTRATION[59]

Log Security components (LS) provided the access to additional features for the system operator. Black Lantern appliance provided the secure infrastructure and key functionality described in the two use cases above. The Aggregator (AGR) and Extender (EX) components were vital elements for enabling secure, massive scale integrity verification.

In the EU-SysFlex report D5.5 "Proposal for data exchange standards and protocols", it was highlighted that sharing information related to data logs has very limited coverage in standards. The aim for the cyber security demonstration was to focus specifically on this topic. The ability to enable multiple parties to share critical system information was demonstrated. This functionality could enable more resilient solutions for cross-border data exchange as the system logs could be shared in a secure manner.

[59] EU-SysFlex deliverable 9.3: Cross-border and cross-sectoral data exchange (not publicly available)

6.3 "AFFORDABLE TOOL FOR SMALLER DSR UNITS" DEMO – ENOCO

Introduction:

The aim of affordable tool for smaller DSR units (ATDSR) demonstration was to develop a **software application** facilitating the **availability and collection/aggregation** of distributed and small **flexibility sources** for ancillary services. An interface between this tool and Estfeed data exchange platform was developed to verify the usefulness of such a platform. The result of ATDSR was to bring smaller energy prosumers (customers of ATDSR) actively to the energy market through provision of flexibility services.

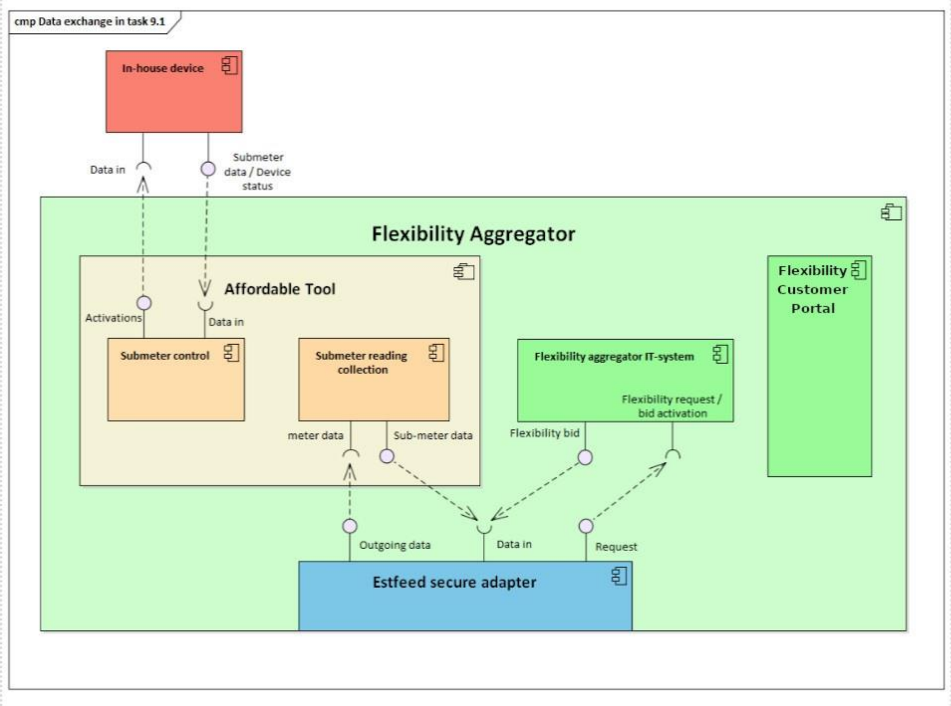


FIGURE 7 HIGH-LEVEL ARCHITECTURE OF AFFORDABLE TOOL FOR SMALLER DSR UNITS FOR PROVIDING FLEXIBILITY SERVICES DEMONSTRATION[60]

Component description of figure 7:

- Estfeed secure adapter: Enables international data exchange through secured channels.
- Sub-meter Control: Communicates with in-house devices, receives sub-meter data, device status and flexibility activations.
- Sub-meter reading collection: stores meter and sub-meter data, aggregates meter data and exposes interface for reading/sending sub-meter / meter data.
- Flexibility aggregator IT-system: Makes bids and receives activations.
- Flexibility customer portal: Gives the small consumers/participants in the aggregated flexibility a GUI to view and administrate their flexibility contribution.

[60] EU-SysFlex deliverable 9.1: Affordable Tool for Smaller DSR Units for providing flexibility services

Relationship to SUCs:

This solution is closely related to the ‘Authenticate data users’, ‘Manage access permissions’, ‘Manage data logs’, ‘Manage sub-meter data’.

Demo description and security guidelines:

Data management for flexibility services has been tested and demonstrated in WP9. The demonstrations focused on various aspects of data management, including cross-border communication between data exchange platforms and with different stakeholders to facilitate cross-border exchange of flexibility services.

The components of ATDSR were:

- TSO’s data hub and customer portals from data service provider side.
- Flexibility Platform used by aggregator (FSP).
- Affordable tool for flexibility offering.
- Estfeed secure adapters to enable international data exchange through secure channels.

ATDSR ensured the data exchange through the Estfeed secure adapter that had been developed using the documentation and guidelines provided by Elering. The adapter provided an interface to the Estfeed system. Each system communicating over Estfeed system was connected to its adapter that relays the Estfeed messages to other adapters using the Estfeed protocol secured with TLS.

The developed application functionalities included:

- providing connection to the Estfeed DEP via dedicated adapter.
- accessing services provided by the FP (Flexibility Platform) as an FSP (Flexibility Service Provider) via the DEP.
- providing services required by the FP to submit and activate bids.
- automatically reacting to activation orders submitted by/via the FP.

As mentioned before, the ATDSR is related to several SUCs and functionalities are fulfilled by the different components inside the application. Authentication of data users is verified and checked when the user logs into the application. Every user is stored in the database with their respective role. For demonstration purposes, the roles were not specified, and the application only consisted of one superuser with access to everything inside the application.

The application uses services provided by Estfeed and creates a secure connection via the Estfeed platform. This platform ensures that all communication goes through the Estfeed adapter. All communication over the Estfeed protocol is secured using TLS. One requirement for using this service was to log and store every transaction between the application and Estfeed. These logs were stored safely in the database and were useful for verifying and checking potential errors that might have occurred.

Since the ATDSR relies on measurement data from households, this had to be provided to the application. A small application was created to generate the data as personal data was not used because of GDPR restrictions and the lack of sending activation orders to real households. The application simulates a small number of households and generates a series of consumption-data that is presented in the ATDSR application. The household application creates raw measurement data, aggregates them into hourly, daily and yearly values and stores them in a database accessible within the ATDSR. This application is responsible for the data transfer from the households to the ATDSR. The application simulating the households stores all the measurements through the standard messaging protocol MQTT. MQTT uses a publish/subscribe architecture where the clients are authorized with a username and password to the MQTT-broker. Clients can post and subscribe on topics and whenever some data is received on the topic all the clients subscribing receive it. All measurements from a particular source are sent under its own topic to the broker and stored in InfluxDB by the broker. The ATDSR also receives these data, for example when showing the consumption data live-feed.

The different sub-meter devices have their own entries in the relation database with its own UUID. The application that generates the sub-meter data sends a payload containing the unique UUID, measurement-value and timestamp. The data are then stored in InfluxDB and can be retrieved using the relational database fetching the sub-meter UUID and asking InfluxDB for the measurement-values for the given UUID.

6.4 FLEXIBILITY PLATFORM DEMO – AKKA

Introduction:

The security mechanisms implemented in the Flexibility Platform (FP) are mainly the ones provided by the Estfeed data exchange platform and its related protocols.

Estfeed platform is based on X-ROAD, a system for enabling secure communication between organizations without the need to implement any security protocol on their organizational level, except the access control policy which remains under their responsibility. It is characterized by a decentralized architecture, making it resilient to security risks and weaknesses such as DoS (Denial of Service) or single point of failure.

The Flexibility Platform is interfaced with other systems to exchange data through a set of APIs using the X-ROAD functionalities where the X-ROAD Security adapters are considered as the entry points to the X-ROAD ecosystem.

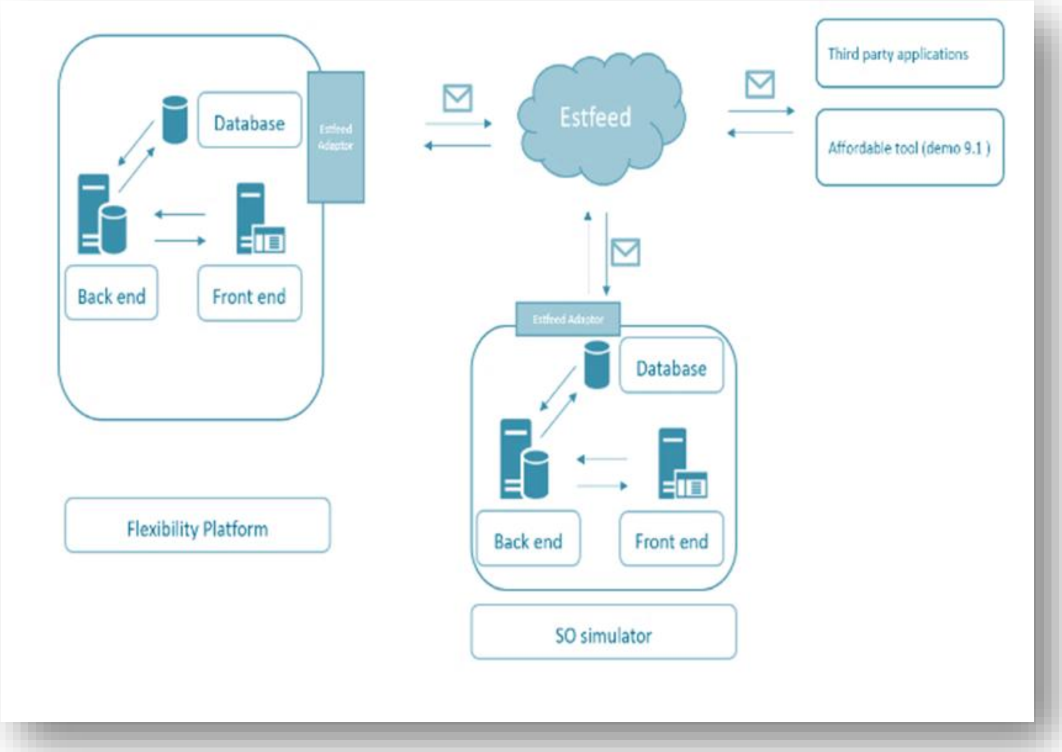


FIGURE 8 FLEXIBILITY PLATFORM - OVERALL ARCHITECTURE[61]

Relationship to SUCs:

This solution is closely related to the ‘Authenticate data users’, ‘Manage access permissions’, ‘Manage data logs’, ‘Manage sub-meter data’.

Demo description and security guidelines:

In terms of the security mechanisms used in the demo to secure the Flexibility Platform, the crucial elements to consider were concluded to be the following. Firstly, the Flexibility Platform was hosted in the internal network of AKKA, which means, AKKA’s security policy was applied to the FP like any asset in the internal network. It was secured with many endpoint security tools (anti-virus, firewalls and proxies) as well as traffic monitoring tools (Intrusion Detection systems, Anti DoS, etc.).

Secondly, on top of that, the data exchange between the Flexibility Platform and external systems was ensured with the security features provided by X-ROAD, which revolved around the following features:

- Encrypted communication: the communication between the FP and the other applications (such as SO simulator) is done via an encrypted way through the X-ROAD security adapters located in each of these systems and using the TLS protocol.

[61] EU-SysFlex deliverable 9.2: Application for TSO-DSO flexibility data exchange - Flexibility platform (not publicly available)

- Authentication with certification: the X-ROAD Security adapter authenticates Information Systems (Both service consumer and producer) using digital certificate, and all the parties involved in the data exchange sign their message before sending them.
- Logs: The X-ROAD Security adapter generates timestamped log files of the data exchange, serving as non-repudiation mechanism.

Finally, the authorizations to access the resources of the Flexibility Platform was managed by the FP itself and the authorizations to access to the APIs offered by the FP is managed by the Estfeed security component.

6.5 BIG DATA DEMO – AKKA

The big data demo used the same security mechanisms as the ones implemented in the FP demo, namely the usage of Estfeed platform and the security tools provided by the AKKA infrastructure (firewalls, proxies, Intrusion Detection systems, Anti DoS). Additionally, some components had been studied and proposed as part of the deliverable 5.3[62] to support these mechanisms and to guarantee privacy protection, access monitoring and the respect of the global security standards over the whole data lifecycle. The premise was that a basic big data solution is usually composed of big data components which lack strong integrated security functions. Therefore, it was important to add some components specifically dedicated to the security to a big data cluster.

In the D5.3 report, the following components were highlighted:

- Apache Ranger, an open-source centralized security framework for Hadoop and non-Hadoop technologies. Ranger provides functionalities to manage authorization, audit and administration of access control policies.
- Apache Knox provides authentication services for users who access the cluster from the external.
- ARX, open-source software for a data anonymization to protect sensitive personal data.

6.6 ECCO SP DEMO – CYBERNETICA

Introduction and demo description:

In “ENTSO-E” demonstration, data exchange between different market parties was tested. ENTSO-E has operational data available via their ECCo SP platform. This was integrated with an Estfeed secure adapter to enable data exchange with Elering data hub. Accordingly, it was possible to demonstrate how consumers can log on to e-Elering customer portal and retrieve operational data about their metering points in addition to consumption.

Third parties (e.g. an aggregator) could have access to both types of data through a single access point – either integrating their applications with Elering’s Estfeed platform or ENTSO-E’s ECCo SP platform. Third party could have access to data assuming the data is either public or it has received authorization from the consumer (in case of meter data) or from the network operator (in case of operational data).

[62] https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex_Task53_deliverable_v1_FINAL.pdf

Data is exchanged over secure channels in International Data Exchange Platform secured area. Secure adapters relay requests and data to either party over secured channels and according to given authorization or ownership.

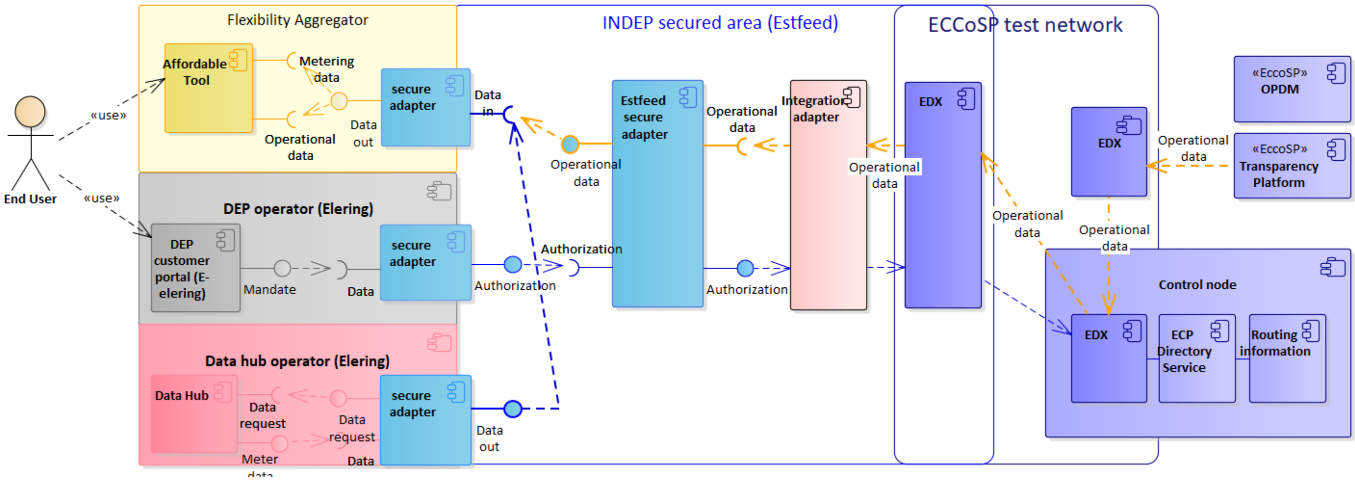


FIGURE 9 COMPONENTS INVOLVED IN DATA EXCHANGE BETWEEN ELERING AND ENTSO-E[63]

Component descriptions:

- **Estfeed secure adapter**: Enables international data exchange over secured channels and in accordance with authorizations from data owner.
- **Integration adapter**: Adapter, developed as part of demo, that enables translating Estfeed data exchange protocol to ECCo SP data exchange protocol.
- **EDX:** ECCo SP's integration node, which enables the data exchange.
- **Control node:** ECCo SP node, which controls the traffic within ECCo SP test network.
- **ECP Directory Service:** Service providing information on services available within ECCo SP network, and the address of relevant EDX node.
- **Routing information:** Database for services.
- **OPDM:** ENTSO-E's confidential data database for Operational Planning Data Management, which is only shared with partners based on permission.
- **Transparency Platform:** ECCo SP's platform for sharing operational data about electricity networks.

In the analysis, conducted in the EU-SysFlex WP5 tasks, the required architecture for integrating with ENTSO-E's DEP was identified. To provide the integration between different DEPs, an integration adapter needed to be developed to convert between Estfeed and ECCo SP message formats. Authorization in ECCo SP was given on TSO level, with ability to relay information further to different parties within this authorization. As such, Elering as TSO was sent authorization, while Flexibility Aggregator was able to consume provided operational data.

ECCo SP has two parts: ECP and EDX. ECP is a message delivery platform that allows message exchange between applications. In addition, it supports users receiving or sending messages directly through a user interface. ECP

[63] EU-SysFlex deliverable 9.3: Cross-border and cross-sectoral data exchange (not publicly available)

includes the concept of services but it is provided by a network's central Broker component, not by an ECP endpoint. The parties exchanging data are called ECP endpoints, like Estfeed's adapters. For applications an ECP endpoint is an API, for users it is a user interface. One ECP network consists of Endpoints, a Broker and a Directory. It is possible to have multiple such networks and in that case the Directories of each network are interconnected and allow the Endpoints from different networks to exchange information. Moreover, it is possible to add custom plugins which can modify how ECP informs applications about received messages and custom message handlers which can process messages before sent to the receiving ECP endpoint and the application. ECP supports three types of message exchange methods: webservices, AMQP send/receive messages and a file-based interface (only for those unable to use the two first methods).

Relationship to SUCs:

This solution is closely related to the 'Anonymize energy data', 'Authenticate data users', 'Manage access permissions', 'Manage data logs'.

Security aspects:

The data exchanged in this demonstration is private meter data. Data owner's consent to exchange data is being checked by the Estfeed Platform. It is important that the application the owner gave consent to and the application behind an ECP endpoint are the same. For this reason, the data should not be delivered to any other ECP endpoints as in Estfeed it is possible to give consent to only one application which the Estfeed – ECP integration is acting as.

The demonstration used personal data, meaning the data owner's consent was needed, and it had to be known beforehand which application would eventually receive and process the personal data. This means that the receiving ECP node and application were preconfigured and the process was not dynamic. The ECP integration to an Estfeed adapter was named and registered in the Estfeed Platform as an application with the same name that the consuming application behind the ECP endpoint. Changing the receiving application later would have required a reconfiguration of ECP, the integration, application name in the Estfeed platform and data owners would have needed to give new consents to the new application.

6.7 BASELINE APPLICATION AND FLEXIBILITY DEMO – CYBERNETICA

Introduction:

The goal of the demo was to demonstrate how privacy-preserving data exchange can protect personal data while allowing systems to calculate results from that data.

"Baseline Application" integration demonstration integrated data providers (in this specific case consumption data from data hub), business process owner (in this case Flexibility Platform operator made responsible to provide flexibility baseline) and users of the business process output (in this case system operators using baselines for financial settlement) via Estfeed and in a privacy-preserving way. All private meter data was encrypted at the data provider, then sent to the Flexibility Platform using a dedicated Estfeed service.

Estfeed assures that the data owner had given an explicit consent to Flexibility Platform to access their private data for baseline calculation purposes and/or to system operator as user of the baseline. Flexibility Platform might calculate the baseline itself or outsource the task to a third party. Since the data was encrypted, the Flexibility Platform or the third party had no direct access to it as data was be processed in three Sharemind MPC servers. In addition, the third party would not have had access to the baseline itself in this approach. Privacy is ensured by the Sharemind MPC technology if the parties hosting the MPC servers are independent and do not collude to break the privacy of individual consumers. No Sharemind MPC server can individually break the privacy.

Relationship to SUCs:

This solution is closely related to the ‘Authenticate data users’, ‘Manage access permissions’, ‘Manage data logs’, ‘Erase, restrict and rectify personal data’.

Demo description and security aspects:

The demonstration built upon the ENTSO-E and Elering data exchange demonstration, although the ECCo SP network part was not important for this demonstration but only the data retrieval from Estfeed. The main idea of the demonstration was to show how a system (Flexibility Platform in this case) could use private data to calculate something (a baseline for a consumer resource) without ever having access to the source data. This has important implications that in many cases if the source data is a means to some end (a calculation result) then the source data does not have to be made available which means more applications could take advantage of it and data owner’s privacy is better protected.

The demonstration implemented an architecture that was proposed in the results presented in the deliverable 5.3[64]. It was discussed how to connect Sharemind with its split architecture of three distinct servers each processing only a third of the total data to Estfeed which by design must know which application it provides the data and has no support for sharing different part of the data with different applications. The chosen scenario to demonstrate was baseline calculation which requires historical meter data (from a data hub) which is personal data. At the same time the Flexibility Platform does not need access to the actual meter data – it only requires the baseline result.

To connect Sharemind with Estfeed, an integration application was created which just forwarded requests and results. On the Estfeed side a special service was added with a feature to divide the requested data into 3 parts, encrypt all the parts with different private keys and then send the encrypted data to the three Sharemind MPC servers. The actual calculation of the baseline was also done on Sharemind. This setup allowed the integration application to only have access to encrypted data and the baseline calculation result and made sure that personal data was only processed on Sharemind and nowhere else. A user interface was also developed to imitate and actual Flexibility Platform. It would allow a user to create a request to calculate a baseline given two dates chosen by the user and visually display the baseline result on a graph.

[64] https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex_Task53_deliverable_v1_FINAL.pdf

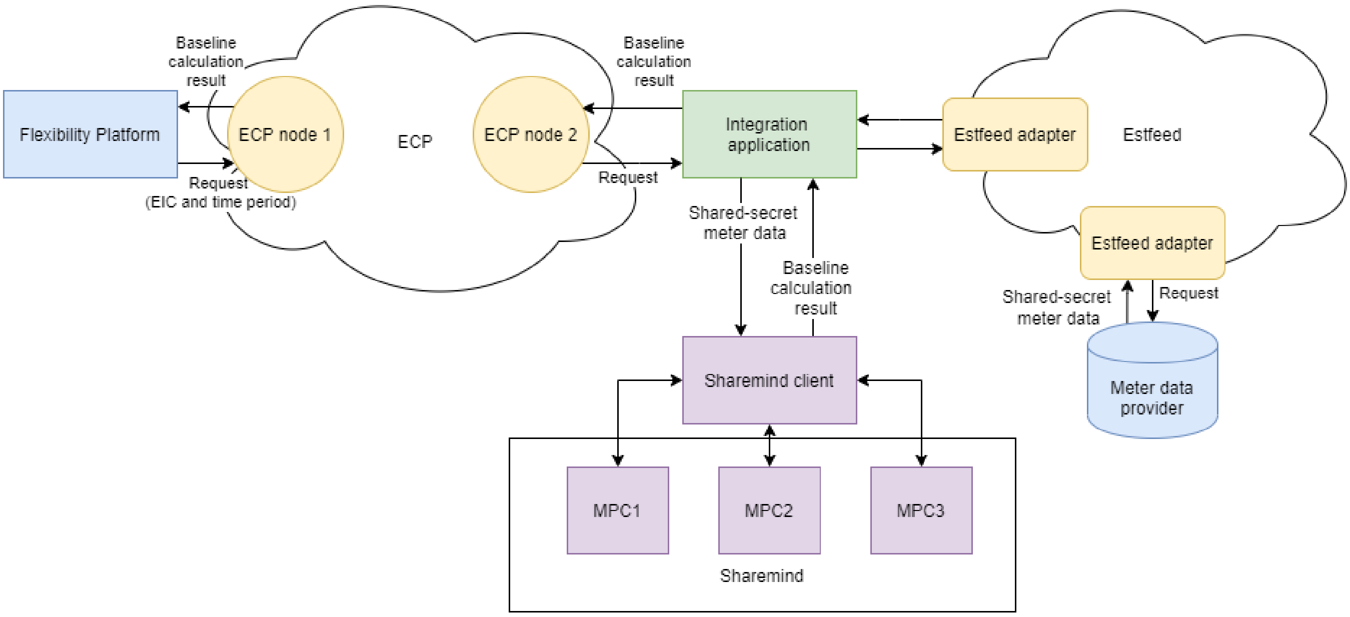


FIGURE 10 DATA EXCHANGE FLOW BETWEEN SHAREMIND, ESTFEED, FLEXIBILITY PLATFORM[65]

Estfeed was able to still validate that the Flexibility Platform had data owner's consent to perform the baseline calculation. A special Estfeed service was developed and the data owner was able to specifically provide their consent to the Flexibility Platform so that their data would only be used for just the intended purpose and nothing more.

The demonstration was able to preserve data owner's privacy while allowing the Flexibility Platform to receive a result calculated using that data. The demonstration proposed an architecture that could make every service of the Estfeed DEP preserve user privacy by first encrypting and obfuscating data and only using it in a secure environment for only the intended purposes. Using Estfeed enabled the demonstration to ensure that the owner of the data was aware that the data was used for just baseline calculation purposes but in a privacy-preserving way.

6.8 ESTFEED DEMO – ELERING

Introduction:

Estfeed platform is used horizontally in all the WP9 demonstrations. The role and functionality in each demo were different, but generally the core element of access, security and connections for the energy data exchange was delivered via Estfeed security adapters.

Elering's DEP Estfeed can interface with various data sources and these data could be used in the applications desired. In short, Estfeed:

- connects data sources, applications and market participants;
- provides secure access and management of consumption data and related rights;

[65] EU-SysFlex deliverable 9.3: Cross-border and cross-sectoral data exchange (not publicly available)

- provides access to the following data sources: – Electricity Data Hub, Gas Data Hub, Central Commercial Register, Electricity price (Nord Pool), weather forecast (Foreca);
- promotes applications that increase energy production, transport and consumption efficiency.[66]

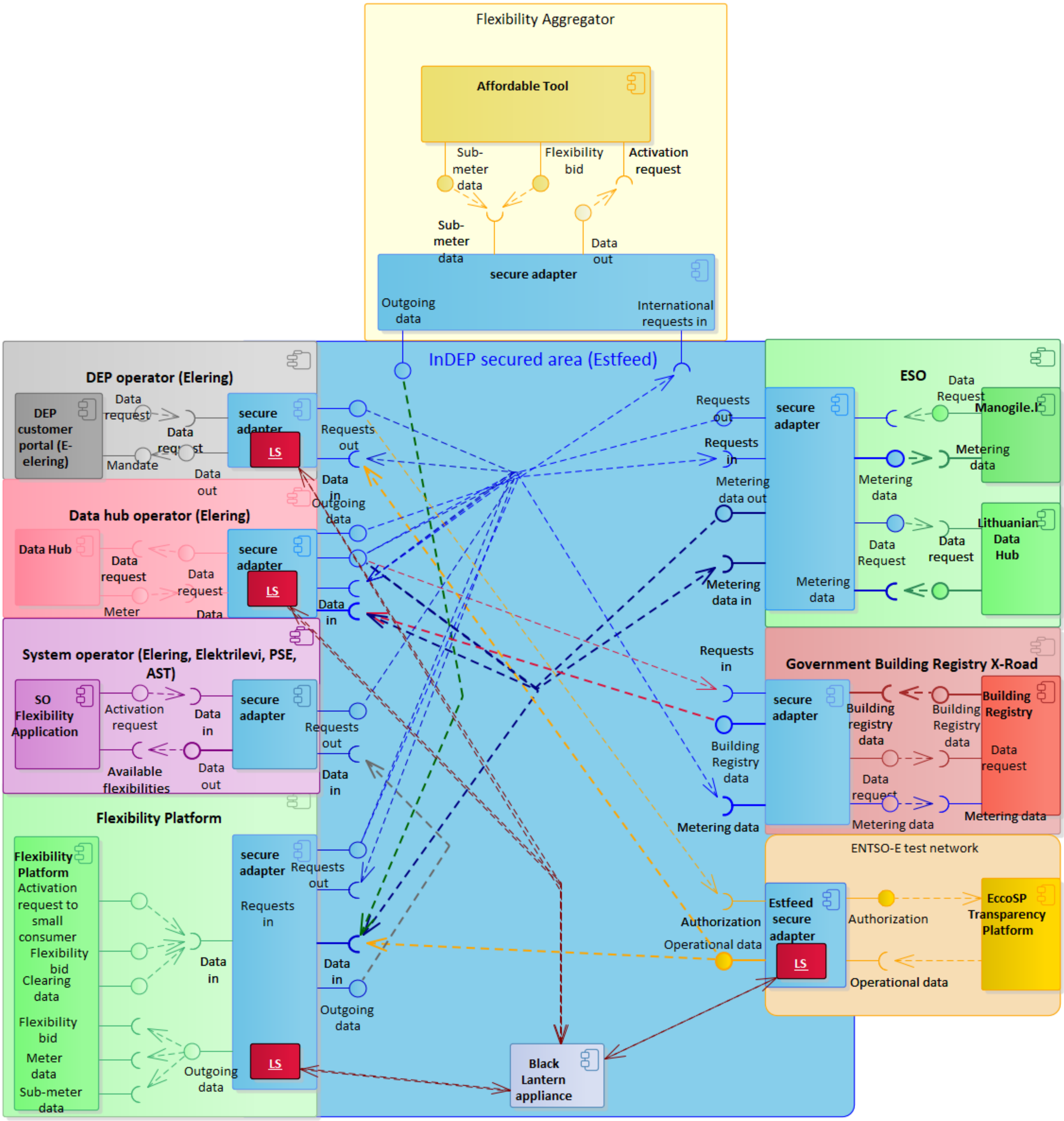


FIGURE 11 BASIC CONCEPT OF ESTFEED USED IN EU-SYSFLEX WP9 DEMOS[67]

[66] https://elering.ee/en/smart-grid-development

[67] EU-SysFlex deliverable 9.3: Cross-border and cross-sectoral data exchange (not publicly available)

The basic concept of the Estfeed can be seen in the figure 11. The central point of all EU-SysFlex WP9 demonstrations are the Estfeed secure adapters. These are providing the governance and control mechanisms for demonstrations and are a starting point for the data exchange, requests and authorisation. A dedicated Estfeed 'research' environment was used in all WP9 demonstrations. This unified approach simplified the execution of each demonstration and helped to execute relevant SUCs.

Besides the general approach of using Estfeed secure adapters as a connection point between different participants it is important to highlight which parties are enabled through Estfeed. Data exchange involves three parties (see figure 12):

- Application information system – consumer of data and services; communicates with the Estfeed system using Estfeed protocol.
- Source information system (data source) – provider of data and services; communicates with the Estfeed system using Estfeed protocol.
- Estfeed system – mediator of data and services between applications and data sources.

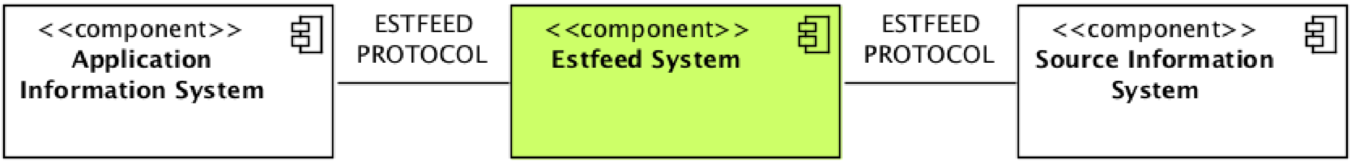


FIGURE 12 ESTFEED PROTOCOL[68]

Relationship to SUCs:

This solution is closely related to the 'Authenticate data users', 'Manage data logs', 'Manage access permissions', 'Manage sub-meter data', 'Erase, restrict and rectify personal data'.

Demo security aspects:

The main security aspects can be listed here:

- To ensure interoperability of flexibility services one needs to focus on data interoperability next to harmonising regulatory/business processes. Therefore, the system use-cases designed for "Flexibility Platform" address the issue of homogeneous and secure data management through the concept of Data Exchange Platform. Proper data management contributes to the participation of stakeholders across the geographical borders and of any asset.
- Residents of one country are able to access their meter data and share the data with other stakeholders using services (e.g. consent management) provided by DEP located in another country, it is possible to remove barriers from accessing meter data from different organizations in different countries. The biggest obstacles are different levels of authentication available in different countries; however, this is being solved within scope of eIDAS.

[68] https://elering.ee/sites/default/files/attachments/estfeed_protocol_1.13_Y-1029-1.pdf

- Data providers and data users connected to different DEPs (ECCo SP, Estfeed) can exchange data by ensuring interoperability of DEPs. This was demonstrated for private data sharing use case whereby one platform benefitted from consent services provided by another platform. The demonstration was able to add value to ECCo SP by using the consent checking capabilities of Estfeed which allowed it to validate that the application behind ECCo SP had data owner's consent to receive some private data.
- Using dedicated privacy-preserving technologies (Sharemind in this case) it is possible to preserve data owner's privacy while allowing a third-party application (Flexibility Platform in this case) to receive a calculated result based on such private data (calculation of Flexibility Service Provider's baseline in this case). Use of DEP (Estfeed) ensures that the data owner is aware that the data is used for just given (baseline calculation) purposes but in a privacy-preserving way.
- It is possible to integrate alternative signing mechanisms to the critical logs that provide the information about the data exchange and participants. The risk of losing critical data logs was reduced from the three aspects: a) signing with different technology; b) adding additional log storage; c) including anti-tamper infrastructure to an existing solution.

6.9 KEY TAKEAWAYS OF EU-SYSFLEX WP9 DEMOS TO PRIVACY AND CYBER SECURITY

Access to the data plays a key role in future energy sector business and has been clearly indicated as such by TSOs, DSOs, regulators, brokers and data owners. The current selection of demonstrations of this report focused predominantly on **data exchange** (incl. cross-border data exchange) **demonstrations** that were covered in **EU-SysFlex WP9**. Due to the nature of the WP9 demonstrations, most of them inherently related critically to a variety of privacy requirements and cyber security aspects, making this WP compared to others an excellent sample-study for this report. Consequently, the other demonstrations in the project (conducted under WP6, WP7, WP8) were not addressed in this report.

The following aspects of the WP9 demonstrations were analysed:

- The importance of governance mechanism – how the Estfeed plays the role in access control for cross-border data exchange.
- Relevance of each participant and their interaction with each other in situations of handling internal system security and logs monitoring.
- Shared responsibility between participants – must be done on the system by design level and supported by the business processes and SLA.
- Incident handling – this requires highly dependable logging solution and trust mechanisms for system logs. The distribution of logs in each separate system is unavoidable, so there have to be mechanisms to share critical system information in parallel to data exchange between different parties.

The takeaways from the demonstrations are:

- Protecting personal data and managing governance of PII can be accomplished using technologies of EU-SysFlex partners. The demonstrations were successful in cross-border security adapter deployment and use for data access, evidence creation and improved redundancy of systems.
- The demonstrations clearly indicated that **expected resources to handle privacy and security are underestimated**. In the demonstrations' setup shortcuts were needed, and data governance and management were simplified to execute demonstrations. In a production environment a more sophisticated approach how each participant, who is responsible for the data input, should handle the accessibility of data, logging mechanisms, infrastructure for security and redundancy.
- Elerings' Estfeed platform filled the role of single access point for EU-SysFlex WP9 demonstration partners. The execution of the demos proved that security adapters can be used cross-border to enable data exchange for flexibility services.
- As the result of the matchmaking between standards and data logs management in the WP9 demonstrations it was concluded that sharing information related to data logs has limited coverage in standards.

7. PRACTICAL SOLUTIONS AND TOOLS APPLICABLE TO EU-SYSFLEX DEMONSTRATIONS

7.1 INTRODUCTION

The execution of the EU-SysFlex WP9 demonstrations was enabled by using different existing solutions and tools that project participants owned. The tools that had most impact from the cyber security and privacy perspective to execute the WP9 demonstrations are highlighted in this chapter. This list of tools and software solutions could be useful for tackling the security and privacy challenges of the energy data exchange in the future. The list provided here is not complete and represents just a small group of solutions that were necessary for WP9.

7.2 GUARDTIME DEMONSTRATION TOOLS

7.2.1 BLACK LANTERN LOG SECURITY TOOL

Description:

Black Lantern Security Appliance[69] is an integrated hardware and software platform, which purpose is to mitigate both remote and physical attacks against one's infrastructure and applications. Black Lantern completely changes the protection paradigm by being able to identify, defeat, deter, and react against high level reverse engineering attempts or cyber-attacks against the appliance itself, its hosted applications, and network-based critical assets.

Relationship to EU-SysFlex data exchange SUCs:

This solution is closely related to the ’Manage data logs’ use case.

Functionality:

Black Lantern can be applied either as a security solution from Gateway for KSI blockchain or as a Highly Secure Compute Platform. For the purpose of EU-SysFlex WP9 security demo, it was used as gateway.

Black Lantern is a Hardened KSI® Gateway

Black Lantern Security Appliance comes with a built in KSI Gateway running in protected environment to ensure continued operations even when the infrastructure expands into areas where there may no longer be physical control over the hardware. Black Lantern guarantees the integrity of the system and proves it through the KSI instrumentation.

Black Lantern is a Highly Secure Compute Platform

The Black Lantern combines the usual capabilities of an Application Server with additional metro-class encryption, communication, and active defence measures. Black Lantern Products can defend themselves from Advanced Persistent Threats regardless of deployment location or physical access to ensure QoS and SLA for the applications it hosts.

[69] https://guardtime.com/hardware/blacklantern

Not only can Black Lantern protect itself against remote attacks, but it is also capable of defending itself from physical attacks – where an attacker has the device on a reverse engineering bench. Black Lanterns are designed to survive in the most harassing environments.

Resiliency

Black Lantern defends itself from denial-of-service attack by policing traffic at the data-link layer (OSI layer 2). The Black Lantern's layer 2 is content-aware – meaning it can identify specific traffic and de-prioritize everything else. This ensures that Black Lantern can recover its performance while it is the target of a denial-of-service attack.

It is also possible to throttle traffic from a single client node in the event that single device attempts to flood the Black Lantern with requests. Since this network stack is content-aware at the hardware level, it can rapidly identify and report any traffic that might indicate the presence of a rogue device in an infrastructure.

Production deployment accreditation offers flexibility for Guardtime solutions using Black Lantern blockchain appliances. The National Information Assurance Partnership (NIAP) evaluation of the Black Lantern ensures secure management, control and auditing layers while extending security to the application. NIST certified cryptography libraries ensure secure implementation.

The role that Black Lantern infrastructure played in EU-SysFlex cyber security demonstration was related to two key functionalities that are part of any systems that exchange information and interact with each other. Firstly, providing integrity of logs – Black lantern infrastructure provides access to the KSI blockchain service to enable KSI functionalities of providing the signatures to achieve log integrity. Besides the log integrity Black Lantern provides a secure gateway for KSI services and reduces the risk from potential attack vectors. In the 'Manage data logs' use case the actors (two system operators) can select besides RFC-3161 time stamping service also KSI Blockchain based log security that is applied through the Estfeed secure adapter. Secondly, providing secure log storage and redundancy. Black Lantern provides a secure log storage and an alternative log protection solution for data exchange in addition to the existing security module running in the Estfeed platform. The secure storage of the logs, verification of integrity of stored logs, and export of logs with proof of integrity is delivered to the actors participating in demonstration.

7.2.2 KSI BLOCKCHAIN

Description:

KSI® Blockchain timestamping unlocks the digital trust needed for ambitious digitization projects, such as going cloud-native, broadly adopting AI, or moving to automated machine-to-machine processes. It is meant to build future-proof and scalable solution for cyber security, data protection and long-term archiving. For the digital assets' integrity verification and visibility to business processes, KSI® Blockchain delivers a massively scalable production grade solution. Guardtime's KSI® Blockchain Timestamping Service is compliant with the eIDAS regulation and is included in the European Trusted List. KSI® is the first blockchain-based technology to receive an eIDAS accreditation and marks an important step in the evolution of digital trust technologies[70].

Relationship to EU-SysFlex data exchange SUCs:
This solution is closely related to the 'Authenticate data users', 'Manage data logs'.

Functionality:
KSI Blockchain functionality delivered in the context of the EU-SysFlex WP9 cyber security demonstration focused on showing the APIs for cryptographic proof of data integrity, data provenance of the system logs. It provided the demonstration with an "enterprise solution" which is a permissioned DLT platform, designed for use in operational contexts, that delivers key differentiating capabilities like:

- Tagging system for electronic data designed for ingestion of data at a very large scale. KSI Blockchain timestamping scales to millions of events per second to support the volumes needed for the most ambitious data-driven solutions in the public and private sectors.
- A signature response in seconds and independent verification by third parties. KSI Blockchain timestamps can be verified independently of Guardtime or any third-party service provider by a widely witnessed blockchain-based trust anchor.
- Long-term verification and no certificates management. KSI timestamps can be stored and verified indefinitely, without the need for complex crypto-lifecycle management. KSI Timestamps are immune to quantum computing attacks, which makes them ideal for long-term archiving and future-oriented projects.

KSI signatures are server based, meaning that signing data requires online access to the KSI service. The verification of the signatures can be done both offline and online. There are two options for access to KSI:

- KSI Gateway – it has two endpoints, one for aggregation/signing and one for signature extension. For try-out these are available at: http://tryout.guardtime.net:8080/gt-signingservice and http://tryout-extender.guardtime.net:8081/gt-extendingservice.

The KSI Gateway uses HMAC-based authentication built in the KSI protocol:

- In addition, the KSI publications file URL is needed for signature extension and verification with the KSI SDK. For KSI services provided by Guardtime this is available at https://verify.guardtime.com/ksipublications.bin. KSI SDK is available for Java, .NET and C. The description and documents on how to access are provided to the try-out user account.

7.2.3 ACCESS AND GOVERNANCE CONTROL ADAPTER

Description:
Guardtime's data exchange adapters offer to the DSO, TSO or other energy data platform provider the smart meter data access functionality as data gatekeeper service. It provides governance and control mechanism for energy

[70] https://guardtime.com/timestamping

metering data. When installed, adapters create the link between the user's energy database and the service provider, allowing the consumer to see their energy data, select service providers and grant/revoke access to data.

Relationship to EU-SysFlex data exchange SUCs:
This solution is closely related to the Authenticate data users and 'Manage access permissions'.

Functionality:
Access and governance control adapter that enables the data gatekeeper service for data hubs/platforms and connection between different participants relevant to energy data exchange. It provides governance and control mechanism four energy data. The adapters will be an effective bridge between service providers system and data exchange platform operators fulfilling part of the requirements that come from GDPR, Green energy deal and open data access regulations side. The adapters add value to the existing and running platforms, so DSO/TSO can make a shortcut into sharing data and skip the planning/development phase on their existing platform.

Technology used to provide data exchange adapters functionality:

- Guardtime's KSI Blockchain® API provides technology for massive scale integrity verification and immutable audit trail generation.
- Hyperledger Indy-based decentralised identifiers provide a mechanism to link the data owners and service providers together (automated matchmaking functionality) and create a novel trusted way to authorize the access of data between the parties.

The benefits of simplified using access and governance control adapters are:

- Reduction of integration costs for governance mechanism for data access and controlling the risks involved to data sharing.
- Traceability of products and ensuring the integrity of critical data without the need for centralized authority.
- Reducing the chances of fraud and data manipulation, cutting out corresponding mediation expenses and transaction costs.

7.3 ELERING DEMONTRATION TOOLS

Description:
The Elering's Data Exchange Platform is a digital environment for information exchange in the electricity market for the purpose of changing open suppliers, forwarding consumption meter data between market participants, maintaining the data, performing the obligations imposed on market participants by the law and ensuring the rights granted to them.

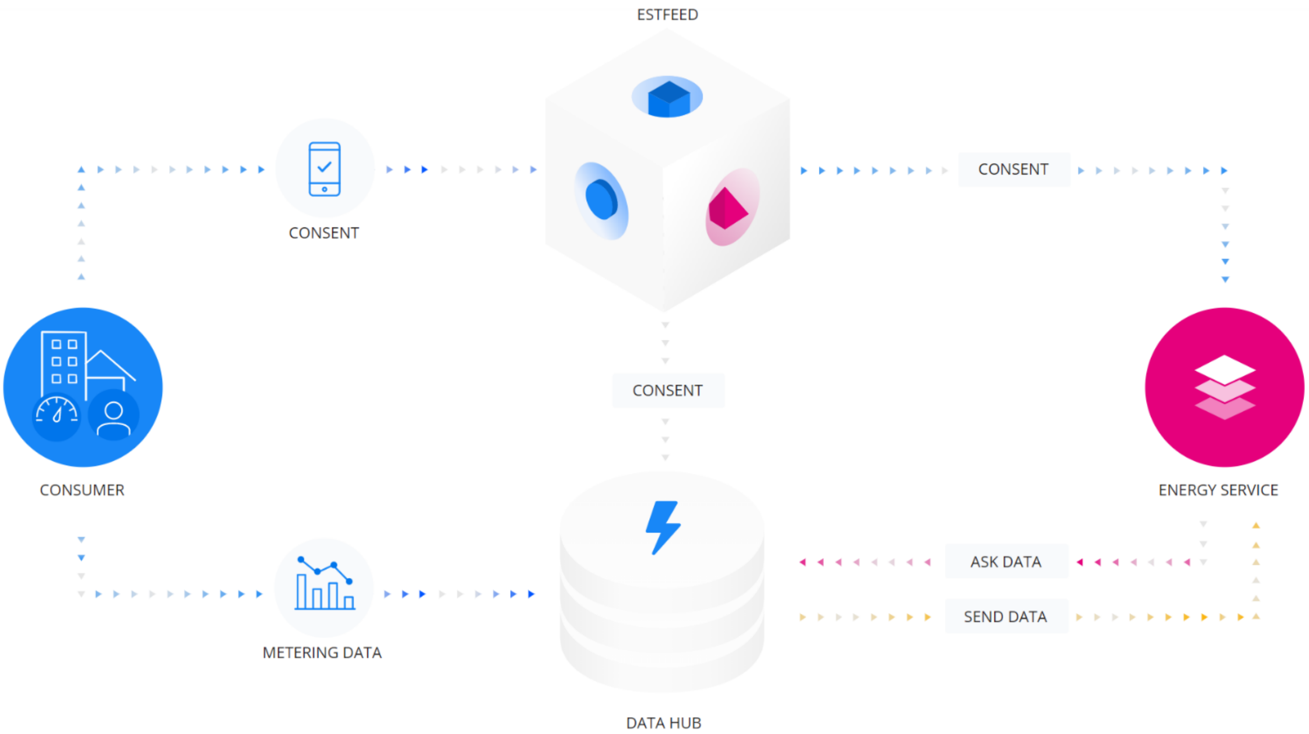


FIGURE 13 ESTONIAN DATA EXCHANGE PLATFORM MAIN CONCEPT[71]

The purpose of the Estonian Data Exchange Platform is to provide efficient information exchange in the open electricity market following the principle of equality. DEP, and Data Hub as part of the concept, provide equal access to consumption meter data to all authorized market participants and enables changing suppliers quickly as presented in figure 13.

Relationship to EU-SysFlex data exchange SUCs:
This solution is closely related to the 'Authenticate data users', 'Manage access permissions', 'Manage data logs', 'Collect energy data', 'Transfer energy data', 'Manage sub-meter data'.

Functionality:
"The Estonian Data Hub is developed by Elering who are also responsible for the subsequent maintenance of the whole system. Network operators are responsible for the volume and quality of the submitted data, the accuracy and hourly resolution of consumption meter data, and the validity of the submitted client data. Open suppliers are responsible for the validity of the information found in the submitted electricity sales agreements.

Elering's client portal (e-elering) gives the market participants access to their meter data and enables downloading the data. The client portal also provides the market participants an overview of all information concerning the participant found on the Data Hub: agreement deadlines, open suppliers, hourly meter data, the market participant's EIC code, and the EIC codes of the metering points linked to the market participant." [72]

[71] https://www.estfeed.eu/en/technology
[72] https://www.elering.ee/sites/default/files/attachments/DataHub_guide%20for%20using_102017_EN%20ED.pdf

All market participants can provide authorizations for accessing previous meter data via e-elering client portal; this is mainly to enable them to receive personalized offers from open suppliers. The market participant's data can be accessed by those who have a statutory right to access the data or who have been given authorization to access the data by the market participant themselves. In order to transmit personal data to open suppliers who the private consumer has not signed an agreement with or who have not received an authorization to access the data via the Data Hub, the person requesting said personal data must have the authorization of the private consumer. The authorization must conform to the requirements established in Section 12 of the Personal Data Protection Act.[73]

Data Hub acts as data source sharing data with authorized market participants' applications. "Application information system and data source information system exchange data with the Estfeed system over mutually authenticated TLS (HTTPS) connections. Certificates are exchanged between interconnected systems for mutual authentication (certificate pinning). In deployment cases, where the information system is deployed to the same host together with the Estfeed system endpoint (Estfeed adapter), regular HTTP can be used for data exchange. The standard HTTP method is HTTP POST in both directions, where both Estfeed adapter and the information system call an URL to push data. For an application, an optional pull method is also supported. In this case, the application will periodically poll the Estfeed adapter for incoming messages."[74]

The data exchange through Estfeed is enabled by the Estfeed protocol that has three layers that allows the involved parties to share information.
The relevant parties from Estfeed protocol perspective are:

- "Application information system (application IS) – consumer of data and services; communicates with the Estfeed system (application adapter) using Estfeed protocol.
- Data Source information system (data source IS) – provider of data and services; communicates with the Estfeed system (source adapter) using Estfeed protocol.
- Estfeed system – mediator of data and services between applications and data sources."[75]

The layers that are used inside Estfeed protocol are:

- Protocol between Information System and Estfeed (including push and pull methods)
- Publish Protocol
- Request-Response Protocol
- Error Handling

[73] https://www.estfeed.eu/en/home
[74] https://elering.ee/sites/default/files/attachments/estfeed_protocol_1.15_Y-1029-1.pdf
[75] https://member.e.elering.ee/api/support-materials/download/fce9d1bc-fc1b-465f-b8dd-6c2719a372dc/Estfeed%20Protocol-v28-20200505_095022.pdf

7.4 AKKA DEMONSTRATION TOOLS

Description:

The descriptions below provide an overview of the components which have been selected as security components in the big data reference architecture of task 5.3.[76] However, they have not been used in the WP9 demo because they were considered out of the scope of the demo implementation.

Apache Ranger is an open-source centralized security framework for Hadoop and non-Hadoop technologies. Ranger is based on **ABAC security (attribute-based-access-control)** providing functionalities to manage **authorization, audit** and **administration** of access control policies. While Ranger is more related to the authorization aspects, on the other hand **Apache Knox** streamlines security for services and users who access the cluster data and execute jobs.

Relationship to EU-SysFlex data exchange SUCs:

This solution is closely related to the 'Authenticate data users', 'Manage access permissions', 'Manage data logs', 'Collect energy data', 'Transfer energy data', 'Manage sub-meter data'.

Functionality:

Apache Ranger

The open-source big data technologies which can benefit from Ranger support are: HDFS, Hive, HBase, YARN, Kafka, Storm, Atlas, Solr, NiFi, Sqoop, Presto and Knox.

Ranger provides these features:

- **Authorization policy**: defining access to data and data stores based on user roles.
- **Group permission:** defining access to data and data stores based on user groups.
- **Auditing:** monitoring of all accesses and tracking them into audit logs.
- **Administration:** Ranger is strongly integrated with Apache Atlas. Atlas provides data governance capabilities and serves as a common metadata store that is designed to exchange metadata both within and outside of the Hadoop stack. Ranger provides a centralized user interface that can be used to define, administer and manage security policies consistently across all the components of the Hadoop stack. The Atlas-Ranger integration unites the data classification and metadata storing capabilities of Atlas with security enforcement in Ranger.

The latest version of Ranger provides also **time-aware access control** for those resource where authorizations don't depend only on user role but also on current time. The time-aware use cases addressed by Ranger are the management of the access control of:

[76] https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex_Task53_deliverable_v1_FINAL.pdf

- resources where the authorization is based on the time of access (e.g. revoke any access to the resources while the database is under maintenance, i.e. scheduled maintenance policy);
- resources globally distributed across data-centers (e.g. synchronize accesses based on time-zone location).

According to these two use cases and considering the EU-SysFlex context, Apache Ranger can address the requirements specified under the SUC 'Manage access permissions'. In particular, Ranger can be used to "give authorization by data owners (e.g. consumers) to other parties interested in using this data" accomplishing the objective of "facilitating exchange of personal and other sensitive data as well as associated energy services (incl. across country borders)".**Error! Bookmark not defined.**

Moreover, Ranger can be used for internal Big Data governance task to temporarily disable access permission between data components. For example, while the periodical nightly batch job is running, it can be necessary to avoid further data ingestion into HDFS by temporarily revoking the write permission to the Kafka-to-HDFS consumers. Finally, due to the auditing functionalities of Ranger it is possible to record all the accesses made from the data owners, accomplishing so the SUC 'Manage data logs' which scope states literally "making available security logs including data access logs and authorization logs" with the objective of "ensure personal data protection". "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)."**Error! Bookmark not defined.**

Apache Knox Gateway

While Ranger is more related to the authorization aspects, on the other hand **Apache Knox** streamlines security for services and users who access the cluster data and execute jobs. This process is also called **authentication** and, in the EU-SysFlex context, is expressed by the SUC 'Authenticate data users' which states "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".**Error! Bookmark not d efined.**

Apache Knox Gateway is an open-source security reverse proxy for interacting with Apache Hadoop ecosystem in a secure way providing authentication, service level authorization, and many other functionalities to manage any HTTP interaction addressed to the cluster.

The main advantage of Apache Knox is the ability to extend the reach of REST APIs to the internet while still securing the cluster and working with Kerberos (see the paragraph dedicated at the end for more details). Moreover, Apache Ranger can provide **SSO authentication** through Knox and this makes their integration one of the best choices for big data security.

One of the main motivations of the birth of Knox was the need of encapsulating and minimizing the burden of Kerberos on HTTP client side. The added value of Knox is high flexibility and extendibility in order to inject different types of policy.

The two main services of Knox are:

- **Proxying Services**
  - Protected access to platform resources.
  - Pluggable and composable provider chain: it is possible to mix and match which providers to use for authentication or for federating an authentication event.
- **Authentication Services**
  - KnoxSSO: a web UI to provide SSO capabilities to cluster, by enabling users to login once and gain access to cluster resources.
  - KnoxToken: a simple REST API for acquiring tokens that can be used to represent the same authentication event until it expires or is explicitly invalidated.

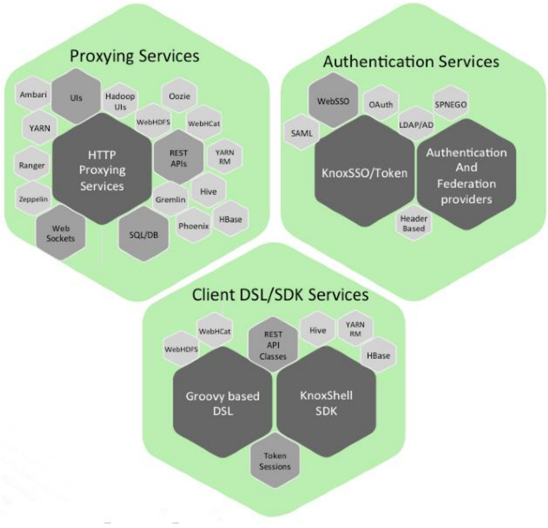


FIGURE 14 APACHE KNOX SERVICES[77]

The main benefits of Apache Knox are:

- **Proxying** to
  - abstract network details (e.g. hiding the IP addresses host names and ports used within the cluster);
  - avoid enabling SSL for all the backend service;
  - provide a single access point to centralize control and reduce administration overhead;
- **Kerberos encapsulation** to simplify the access to the Big Data platform (see Figure 15 below);
- **Extend API reach for the clients** in order to be able to consume resource from the Big Data platform;
- Knox Admin UI for
  - **Auditing;**

[77] https://knox.apache.org/

  - service-level authorization (mentioned just for sake of completeness, but in practice managed by Ranger integration);
- **Enterprise integration, e.g**.
  - LDAP/AD integration for directory services;
  - Authentication protocols (e.g. SAMLv2, OAuth, etc.);
  - **SSO integration.**

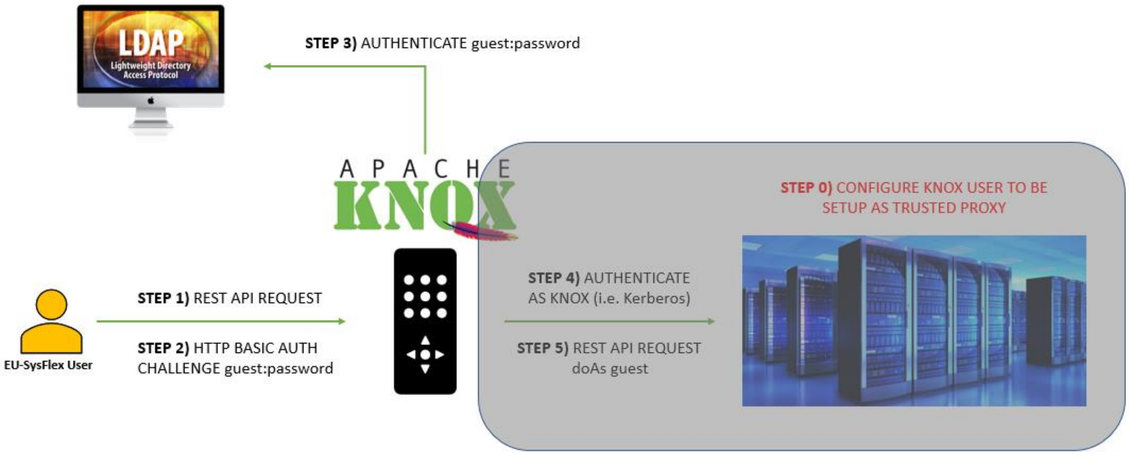

LDAP
Lightweight Directory Access Protocol
STEP 3) AUTHENTICATE guest:password
APACHE KNOX
STEP 0) CONFIGURE KNOX USER TO BE SETUP AS TRUSTED PROXY
STEP 1) REST API REQUEST
STEP 2) HTTP BASIC AUTH CHALLENGE guest:password
EU-SysFlex User
STEP 4) AUTHENTICATE AS KNOX (i.e. Kerberos)
STEP 5) REST API REQUEST doAs guest

FIGURE 15 APACHE KNOX – KERBEROS ENCAPSULATION[77]

According to Figure 155, Knox must be first configured in order to appear as a trusted proxy for the backend services. Indeed, Knox cannot impersonate by default a trusted user if not explicitly configured to do that, like any new entity added to a "kerberized" system (see step 4). At the same time, it also asserts the identity of the user that is authenticated at the front door (see step 1 & 2; in the step 3 an example of LDAP authentication). The grey box surrounding the Big Data framework highlight the Kerberos encapsulation, i.e. thanks to Knox the client can be unaware of Kerberos.

7.5 CYBERNETICA DEMONTRATION TOOLS

Data owners encrypt the full database on-site with the Sharemind importer and upload to the Sharemind Application Server. Data analysts build and run queries without accessing the data. Instead, Sharemind utilises secure computing technology to process data without removing the protection. All query results are also encrypted and only the user making the query can decrypt them.

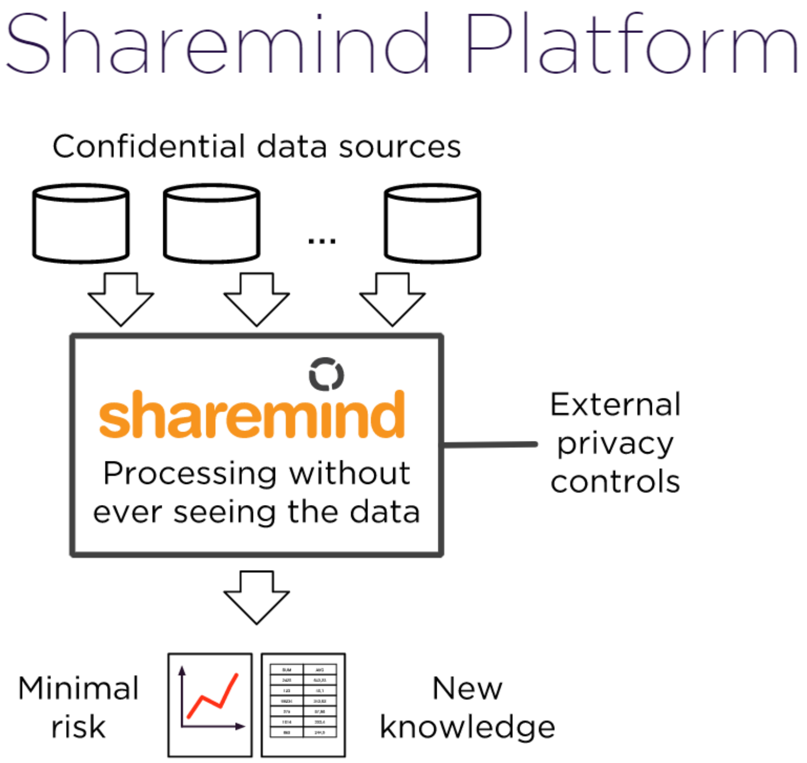

Sharemind Platform
Confidential data sources
...
sharemind
Processing without ever seeing the data
External privacy controls
Minimal risk
New knowledge

FIGURE 16 SHAREMIND PLATFORM [78]

Selected third parties control what can be computed and what results can be released. Sharemind advantages are:

- to enable starting new businesses or services based on data that could not be accessed before;
- to use more data in decision making, processes or research;
- to go so far beyond data protection requirements that they may not apply anymore;
- to use better privacy guarantees as market advantage;
- to use Sharemind developer tools to build privacy-preserving data mining solutions that integrate with workflow.[78]

According to a survey[79] conducted among the members of the Estonian IT industry consortium, nearly everybody would use the results for making decisions. However, the majority also requested that anonymisation techniques be put in place to prevent larger companies from abusing data from smaller ones. With these requirements, using Sharemind was an easy choice to make. Especially, as the IT companies were ready to host its servers.

7.6 KEY TAKEAWAYS FOR USE TOOLS AND SOFTWARE FOR PRIVACY AND SECURITY

To sum up, three takeaways from **tools and software solutions** section can be made:

- **Elering's Estfeed platform can be recommended as one of possible solutions** for building a **national data hub/platform** and privacy respecting data exchange solutions for energy and smart meter data. The

[78] https://sharemind.cyber.ee/secure-computing-platform/
[79] https://eprint.iacr.org/2011/662

capabilities of Estfeed were well tested in WP9 and the future deployment of this solution is described in the system use cases that EU-SysFlex WP5 and WP9 focused on.

- **Sharemind platform provided a good example** how results based on **private data can be shared between parties without the input data being exposed** to the third party service provider during the process. This proves that there are potential solutions that could be used by the system integrators and data platform providers to solve some of the privacy challenges in future energy data exchange platforms.
- Based on the capabilities shown in demonstrations, **Black Lantern infrastructure application can be considered as an example** how critical **system logs could be protected** between different parties involved in energy data exchange. As a security solution that does not have access to shared data (using cryptography and anti-tamper hardware to achieve it) this infrastructure can be considered as a solution template in future system log security components and data exchange platforms.

8. RELEVANT PROJECTS AND CYBER SECURITY INITIATIVES

8.1 INTRODUCTION

Besides the EU-SysFlex WP9 demonstration, it is also important to provide brief reference to other projects and initiatives that address the security and privacy element in energy data exchange. This will help to draw a parallel on how other projects are dealing with the privacy and cyber security issues and what are the connection points between the key results of those projects and findings in this report. The projects presented in this section were selected according to two main criteria. Firstly, the compilers of this document were familiar with these projects. And secondly, the goals of selected projects match with the aims of WP5.4.

8.2 BRIDGE INITATIVE IN DATA EXCHANGE CYBER SECURITY

BRIDGE is a European Commission's initiative which unites Horizon 2020 Smart Grid, Energy Storage, Islands, and Digitalisation projects to facilitate the collaboration among the projects[80]. Projects come together in several working groups and in more ad-hoc working streams to discuss and draw conclusions and recommendations in the areas of common interest for projects themselves and relevant for EC. This avoids duplicating the works and increases generalisation for recommendations. Working group on data management has produced several reports that discuss cyber security and data privacy.

A report on cyber security[81] gives general cyber security recommendations based on the survey conducted among collaborative projects:

- To consider complexity, cost and required effort when considering cyber security recommendations.
- To develop a certification framework with a focus on definition of minimal requirements for devices/products; development of tools, processes and guidelines for audit and tests; process and lifecycle management.
- To develop and demonstrate attack detection, situational awareness, incident management and resilience systems.
- To share threat intelligence information between relevant actors to help them preparing and reacting successfully.
- To promote best practices at every level of the concerned organisations.

The second report relevant to cyber security and privacy is from July 2018 where some of the barriers experienced by the collaborators are discussed and recommendations given[82]. The recommendations follow analysis of the main issues many energy projects are facing. Technological, legislative and ethical aspects of data collection, processing and general cyber security are covered by the report.

[80] https://www.h2020-bridge.eu/
[81] https://www.h2020-bridge.eu/wp-content/uploads/2020/01/D3.12.e_BRIDGE_Cybersecurity-report.pdf
[82] https://www.h2020-bridge.eu/wp-content/uploads/2018/06/BRIDGE-Data-Management-WG-Findings-and-Reco-July-2019.pdf

8.3 FLEX4GRID

The Flex4Grid[83] activity aimed at providing a system for new market players offering data analytics and aggregation services for Distribution System Operators (DSO) to forecast and influence the load on the grid avoiding blackouts caused by network overloads or lack of power supplies. Based on the anonymised and aggregated information supplied by Flex4Grid applications, the DSOs can plan and react on consumption and generation peaks by providing business incentives to prosumers in the value chain to balance the energy load. Flex4Grid also enables communication between prosumers' grid tie inverters to control the amount of power coming to the network to avoid network overload.

On the prosumers' side, Flex4Grid aimed at simplifying the integration of building management system and renewable energy sources such as solar panels, wind turbines and energy storages as well as a better energy management and optimisation according to real-time electricity costs and other incentives offered by the energy retailers.

Flex4Grid provides a holistic data management solution for smart grids that unifies the data exchange between DSOs and their customers by integrating different complementary components brought in by the partners. Together with a control interface to building management systems, home automation systems and smart appliances this has resulted in efficient network management of smart grids and allows the integration of prosumers in the distribution network. The Flex4Grid system was built from components with a high technology readiness level (TRL5-9) provided by the technical project partners to ensure a successful integration.

Flex4grid project applied various techniques to ensure privacy and cyber security for smart grid integration of prosumers, for example pseudonymisation, dynamic identities, aggregation, and access protocols. Flex4grid report "Final Security and Privacy Module"[84] tackles the security and privacy issues from two viewpoints. The first is organisational and related to procedures that enable security and privacy provisioning. The second is mechanisms and services and their implementation. At that point classical security services need to be provided, from authentication and confidentiality to access control. The report also includes details on implementation in the smart grid.

8.4 WISEGRID

WiseGRID[85] provides services for the actors of the distribution network in different scenarios to promote more sustainable energy grids, empowering the prosumers and enabling the establishment of a near real-time pan-European energy balancing market. The aim was to demonstrate an integrated Ecosystem that establishes an innovative approach for the management of the power grids.

[83] https://www.flex4grid.eu/
[84] https://www.flex4grid.eu/wp-content/uploads/646428-Flex4Grid_%E2%80%93_D2.3_Final_Security_and_Privacy_Module.pdf
[85] https://www.wisegrid.eu/

WiseGRID integrates and demonstrates innovative and advanced Demand-Response mechanisms that facilitate the active participation, protection and empowerment of the European consumers and prosumers in the energy grid and market, through flexible RES generation, self-consumption and storage, or through intermediaries such as aggregators and suppliers on behalf of the former. WiseGRID also addresses the smartening of the distribution grid, including both technologies and methods to gain advanced monitoring and awareness of variable generation and consumption loads, as well as the integration of VPPs (Virtual Power Plants) and microgrids as active balancing assets; the integration of renewable energy storage systems in the network, such as batteries or heat accumulator; and the integration of tools to plan the deployment of electric mobility services, as well as the management of loading and unloading of these vehicles, including the possible use of their batteries as storage systems or VPPs.

8.5 SOFIE

SOFIE H2020 project[86] enables creation of business platforms, based on existing IoT platforms and distributed ledgers, without needing to negotiate with any gatekeepers. The wide applicability of the approach was tested through four pilots: food supply chain, energy flexibility marketplace, context-aware mobile gaming, and energy data exchange. This section focuses on the *Decentralized Energy Data Exchange* (DEDE) pilot, describing the proof-of-concept that was developed within the pilot **for secure data exchange and agreements to data access rights between smart meter data and infrastructure owners and energy service providers (intermediaries, distributors, brokers).** A general overview of the pilot can be seen in Figure 17.

The DEDE pilot was led by Guardtime in a consortium of ten international partners from academia and industry. The pilot developed and used the capabilities of the SOFIE federated platform and Energy grid adapters to deliver the required functionality to stakeholders focusing on the deployment of the **DEDE adapters,** which are the main integration points for any third party using the solution. DEDE adapters are deployed in the Elering's Estfeed live environment and in the DSO (small group of regional smart meters) test site, in single smart meter units.

DEDE adapters provide robust and novel data governance and control that meets the requirements of GDPR and fulfils main data access security aspects (EU future network code on cyber security), enabling connected parties in the energy grid to: 1) grant access to different data access points; 2) use different data sources (national, regional data hubs, smart meter data); 3) monitor the process of who gives/receives data through their platform, and 4) provide immutable evidence and cryptographic proof of processes, transactions for auditing and security purposes.

[86] https://www.sofie-iot.eu

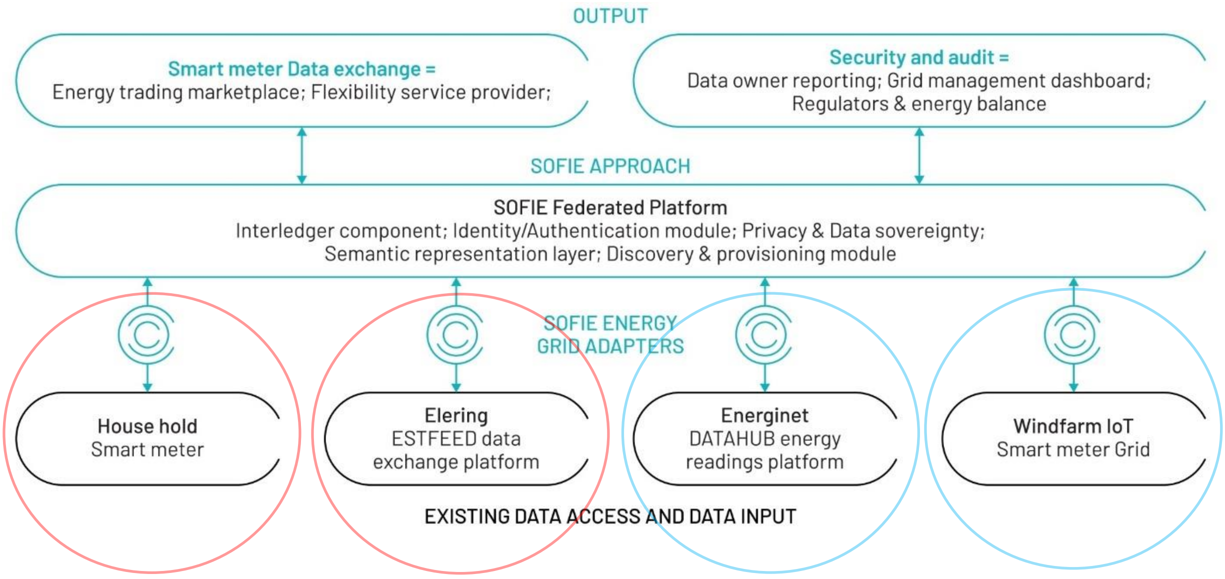

OUTPUT
Smart meter Data exchange =
Energy trading marketplace; Flexibility service provider;
Security and audit =
Data owner reporting; Grid management dashboard;
Regulators & energy balance
SOFIE APPROACH
SOFIE Federated Platform
Interledger component; Identity/Authentication module; Privacy & Data sovereignty;
Semantic representation layer; Discovery & provisioning module
SOFIE ENERGY GRID ADAPTERS
House hold
Smart meter
Elering
ESTFEED data exchange platform
Energinet
DATAHUB energy readings platform
Windfarm IoT
Smart meter Grid
EXISTING DATA ACCESS AND DATA INPUT

FIGURE 17 SOFIE PROJECT ENERGY DATA EXCHANGE DEMONSTRATION GENERAL OVERVIEW[86]

The DEDE adapters enable trust between parties who exchange energy meter readings. The adapters create a secure connection between all participants that are integrated to the network. This includes searching and interacting with interested parties, which is the first and fundamental step in data governance and control. Using the identifiers and credentials, a secure protocol is applied to grant and revoke the access to digital assets. In DEDE adapters deployment the latter is smart meter data (metering point ID, location, consumption/production measurements feed, time, date). Privacy by design allows creating connections without sharing private data between participants. The private data is held in each participant's wallet. Users can control the access through mobile app to enable onboarding the infrastructure they own and include local instances or data hub components they are part of. The underlying procedure of constant monitoring and event registering guarantees immutable evidence. All participants can trust these events and they are also verifiable by third parties for auditability and regulatory purposes.

DEDE adapters' platform incorporates specific measures to mitigate and prevent security and privacy risks during energy data exchange. Firstly, **only those transactions are supported that originate from authorised entities**. This means that electronic identities (eID) are a must and with the DEDE adapters' deployment the participant(s) receive an eID according to regulations and legislation. Decentralized identifiers (DID) are used to enable data owners' full control over their data giving them independence from third party identity providers. Secondly, **all transactions must be authentic and verifiable** which means that all participants use DIDs for authentication, having full control over their DIDs. Additionally, all interactions between the parties are signed by KSI Blockchain – the hash of the interaction payload will be time-stamped and later verified if required. Finally, DEDE adapters **do not store any metering data in the system,** hence eliminating the risk of data security breaches that might occur during data storage processes. The data is stored on the data owner's or on the data hub side, and for data exchange, a secure communication channel is created between the participants where only the allowed parties have access to the data.

DEDE pilot’s proof-of concept demonstrates that cross-border energy data exchange and that at the same time third party auditability and compliance to regulations is achievable.

From the SUCs perspective that are covered in EU-SysFlex WP5 and WP9 the contribution by SOFIE project results can be linked with the ‘Authenticate data users’, ’Manage access permissions’, ’Manage data logs’ use cases. The approach of providing a decentralised identifier when authenticating the users in case there is need to get data from different data hubs can be a powerful tool, to accomplish two things. Firstly, to have a freedom to choose any country specific central authority that handles the authorisation. As there are multiple participants that want to be part of the authorisation mechanism across countries, there has to be a political decision made, how to manage the governance of authorisation. Secondly, this approach to data logs as additional security measure can complement as a third party verification mechanism in case of dispute.

BIBLIOGRAPHY

ACER. *Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows report* Retrieved on May 12th 2021 from https://www.acer.europa.eu/Official_documents/Public_consultations/PC_2021_E_04/Draft%20Framework%20Guideline%20on%20sector-specific%20rules%20for%20cybersecurity%20aspects%20of%20cross-border%20electricity%20flows.pdf

Apache Knox. Retrieved on April 5, 2021 from https://knox.apache.org/

Article 29 Data Protection Working Party (2011*). Opinion 12/2011 on smart metering.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf

BBC News. Kleinman, Z. (17.12.2020). *People's Energy data breach affects all 270,000 customers* https://www.bbc.co.uk/news/technology-55350995

Bräutigam, T et al. (2020). *NIS Directive and the energy sector: a patchwork of national implementations* https://www.twobirds.com/en/news/articles/2020/global/nis-directive-and-the-energy-sector-a-patchwork-of-national-implementations

Bogdanov, D., Talviste, R., Willemson, J. (2011). *Deploying secure multi-party computation for financial data analysis.* Cryptology ePrint Archive: Report 2011/662 https://eprint.iacr.org/2011/662

BRIDGE Data Management WG (2019-1). *Cybersecurity and Resilience*. https://www.h2020-bridge.eu/wp-content/uploads/2020/01/D3.12.e_BRIDGE_Cybersecurity-report.pdf

BRIDGE Data Management WG (2019-2). *Main findings and recommendations*. https://www.h2020-bridge.eu/wp-content/uploads/2018/06/BRIDGE-Data-Management-WG-Findings-and-Reco-July-2019.pdf

CEN standard. CEN/TC 294 - *Communication systems for meters* (2018)

CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (2016). Cyber Security & Privacy. https://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CGSEG_CSP_Report.pdf

Cybernetica (2017). *Estfeed Protocol. Protocol Specification*. https://elering.ee/sites/default/files/attachments/estfeed_protocol_1.13_Y-1029-1.pdf

Cybernetica *Sharemind.* Retrieved on February 10, 2021 from https://sharemind.cyber.ee/secure-computing-platform/

Cyberscoop. Lyngaas, S. (09.03.2020) *European power grid organization says its IT network was hacked* https://www.cyberscoop.com/european-entso-breach-fingrid/

Directive 2008/114/EC. Council *Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN

Directive 2016/1148. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595849589059&uri=CELEX:32016L1148

Directive 2019/944. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0944&from=EN

ENISA (2018). *Mapping of OES Security Requirements to Specific Sectors* https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/

ENTSO-E (2020). *Response to the European Commission's public consultation to establish the priority list of Network Codes.* https://www.entsoe.eu/news/2020/05/26/response-to-the-european-commission-s-public-consultation-to-establish-the-priority-list-of-network-codes/

ENTSO-E report by Thema (2017). *Data exchange in electric power systems: European State of Play and Perspectives* https://eepublicdownloads.entsoe.eu/clean-documents/news/THEMA_Report_2017-03_web.pdf

EU-SysFlex: Kukk, K (2019). *European level legal requirements to energy data exchange*. https://eu-sysflex.com/wp-content/uploads/2019/10/EUSYSFLEX-5.1.5-Legal-requirements-to-data-exchange-2019.10-FINAL.pdf

EU-SysFlex: Siöstedt, S., Wang-Hansen, M. (2021). *Report Data Platforms.* https://eu-sysflex.com/wp-content/uploads/2021/03/EUSYSFLEX-5.1.3-Report-Data-Platforms-FINAL-1.pdf

EU-SysFlex deliverable 5.2: Suignard, E.; Jover, R.; Albers, W.; Budke, J.; Kukk, K. (2020*). Description of data exchange use cases based on IEC 62559 methodology*. https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex-Task-5.2-D5.2-FINAL.pdf

EU-SysFlex deliverable 5.3: Tkaczyk, A.; Sochynskyi, S., Kukk, K., Szczech, P.; Dam, F.; Benedetti, R.; Abdullayeva, G.; Kurylenko, O.; Gucwa, G.; Siöstedt, S.; Aakenes, U. R.; Good, N.; Curtis, M.; Wattam, S.; Brauns, K.; Kuhaupt, N.; Sahk, A.; Sokk, V.; Albers, W.; Budke, J.; Calpe, C.; Staudt, M.; Lehtmets, K. M. (2020). *New big data collection, storage, and processing requirements as identified from the EU-SysFlex use cases*. https://eu-sysflex.com/wp-content/uploads/2020/10/EU-SysFlex_Task53_deliverable_v1_FINAL.pdf

EU-SysFlex deliverable 5.5: Kukk, K., Winiarski, L., Requardt, B., Suignard, E., Effantin, C., Sochynskyi, S., Tkaczyk, A., Lambert, E., Anton, P., Rossøy, O., Good, N., Jover, R., Trees, K., Albers, W. (2021). *Proposal for data exchange standards and protocols*. https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf

EU-SysFlex deliverable 9.1: Lilleeng, S., Rossøy, O. (2021) D9.1 *Affordable Tool for Smaller DSR Units for providing flexibility services.* (Not publicly available.)

EU-SysFlex deliverable 9.2: Ranaivo-Rakotondravelona, M., Szczech, P., Yar, A.-G., Kochmanier, R., Lubczynski, W., Kukk, K. (2021) D9.2 background report *Application for TSO-DSO flexibility data exchange - Flexibility platform.* (Not publicly available.)

EU-SysFlex deliverable 9.3: Kukk, K., Trees, K., Kuhi, K., Olev, A., Szczech, P., Anton, P. (2021). D9.3 background report *Cross-border and cross-sectoral data exchange.* (Not publicly available.)

EU-SysFlex deliverable 12.3 (2019). M Requirement N3. (Not publicly available.)

European Commission (2020). *A European strategy for data* https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

European Commission website (March 2021). *Proposal for an ePrivacy Regulation*. Retrieved on April 13, 2021 from https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

European Commission website (April 2021). *Recommendation of 3.4.2019 on cybersecurity in the energy sector* https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

European Commission ENISA website (April 2021). *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection* https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/national-security/eci-directive

European Data Protection Supervisor (EDPS) (2019). *TechDispatch #2: Smart Meters in Smart Homes* https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en

Elering website on smart grid development. Retrieved on April 27th 2021 from https://elering.ee/en/smart-grid-development

Estfeed platform landing page (Elering, 2021) *Description of Estfeed platform* https://www.estfeed.eu/en/home

Estfeed platform technology (Elering, 2021) *Description of Estfeed platform and technical details.* https://www.estfeed.eu/en/technology

Estfeed platform guide (Elering, 2021*) Estonian data hub Guide for using and joining the Estonian Data Hub by Elering*https://www.elering.ee/sites/default/files/attachments/DataHub_guide%20for%20using_102017_EN%20ED.pdf

Estfeed protocol technical specification (2019). https://member.e.elering.ee/api/support-materials/download/fce9d1bc-fc1b-465f-b8dd-6c2719a372dc/Estfeed%20Protocol-v28-20200505_095022.pdf

ETSI Smart Grid definition and introduction. Retrieved on January 6th, 2021 from https://www.etsi.org/technologies/smart-grids

Ferris, N., and van Renssen, S. (2021) *Cybersecurity threats escalate in the energy sector.* Retrieved on April 27, 2021 from https://energymonitor.ai/technology/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector

Fischer, L., Uslar, M., Morrill, D., Döring, M., and Haesen, E. (2018). *Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector Final report* https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf

Flex4grid *Flex4grid project introduction*. Retrieved on February 22, 2021 from https://www.flex4grid.eu/

Flex4grid WP2. *Final Security and Privacy Module*. Retrieved on March 23, 2021 from https://www.flex4grid.eu/wp-content/uploads/646428-Flex4Grid_%E2%80%93_D2.3_Final_Security_and_Privacy_Module.pdf

GDPR Enforcement Tracker. Data retrieved on April 20, 2021 from https://www.enforcementtracker.com/

Green Button Developer. (2018). Information retrieved on April 17, 2021 from https://openei.org/wiki/Green_Button_Developer

Green Button Happenings (Blog). Information retrieved on April 17, 2021 from https://www.greenbuttonalliance.org/happenings

Guardtime website on *Black Lantern and Timestamping*. Information retrieved on February 11, 2021 from https://guardtime.com/hardware/blacklantern; https://guardtime.com/timestamping

Harnser Group for the European Commission (2010). *A Reference Security Management Plan for Energy Infrastructure* https://ec.europa.eu/home-affairs/sites/default/files/e-library/docs/pdf/2010_reference_security_management_plan_en.pdf#zoom=100

Hornetsecurity (2020). *Cybersecurity Special: Cyber Attack Target Number One.* https://www.hornetsecurity.com/data/downloads/reports/document-cybersecurity-special-energy-en.pdf

IEC standard: *EC 62351-4:2018 Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives*

IEC technical specification: *IEC TS 62443 Industrial communication networks*

ISO standard: *ISO/IEC 27019 Information technology— Security techniques — Information security controls for the energy utility industry*

ISO standard: *ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry*

Jasmontaite, Lina (2017). *Workshop: Data protection and the energy sector: smart grids.* https://brusselsprivacyhub.eu/publications/ws08.html

KSI Blockchain general overview. Data retrieved on April 19 from https://guardtime.com/timestamping

Osano Ramirez, N. (15.01.2021) *ePrivacy: The EU's other data protection rule* https://www.osano.com/articles/eprivacy-guide

Proposal Directive (2020). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

Regulation 2015/703*. Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R0703&from=EN

Regulation 2016/679. *Regulation (EU) 2016/679 of the European Parliament and of the Council* of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Regulation 2017/1485. Commission regulation (EU) 2017/1485 of 2 August 2017 *Establishing a guideline on electricity transmission system operation.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1485&from=EN

Schelle Jensen, S. (2018). *Presentation: Intervention on GDPR & experience from Denmark* https://www.euroheat.org/wp-content/uploads/2018/01/2_GDPR_Steen-Schelle-Jensen-Digital-Heat.pdf

Simon, F. (2019). *Smart meter woes hold back digitalisation of EU power sector* EURACTIV https://www.euractiv.com/section/energy/news/smart-meter-woes-hold-back-digitalisation-of-eu-power-sector/

Smart Grid Task Force 2012-14 Expert Group 2 (2018). *Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment: Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

Smart Grid Task Force Expert Group 2 (2017). *Interim Report: Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity.* https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf

Smart Grid Task Force Expert Group 2 (2019). *Final Report: Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management*. https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

SOFIE project *SOFIE H2020 project overview*. Retrieved on April 11, 2021 from https://www.sofie-iot.eu

Trend Micro. Hilt, S., Huq, N., Kropotov, V., McArdle, R., Pernet, C., and Reye, R. (2018) *White Paper: Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries* https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf

Tripwire press release (2016). *Tripwire Study: Energy Sector Sees Dramatic Rise in Successful Cyber Attacks*. https://www.tripwire.com/company/press-releases/2016/04/tripwire-study-energy-sector-sees-dramatic-rise-in-successful-cyber-attacks

UK Department for Business, Energy & Industrial Strategy (2018). *Smart Metering Implementation Programme: review of the Data Access and Privacy Framework*. https://www.gov.uk/government/publications/smart-metering-implementation-programme-review-of-the-data-access-and-privacy-framework

US Department of Energy Office of Electricity Delivery & Energy Reliability (2018). *Multiyear Plan for Energy Sector Cybersecurity* https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

Wisegrid. Retrieved on March 9, 2021 from https://www.wisegrid.eu/

COPYRIGHT

This document as well any changes in this document will be notified to PMB.

The EC / Innovation and Networks Executive Agency is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under EC-GA No 773505.