Cyber Security for Europe

Research on Data Sharing in Open Banking & Medical Data Exchange

Personal Data Sharing - Emerging Technologies

Brussels, 7 October 2022

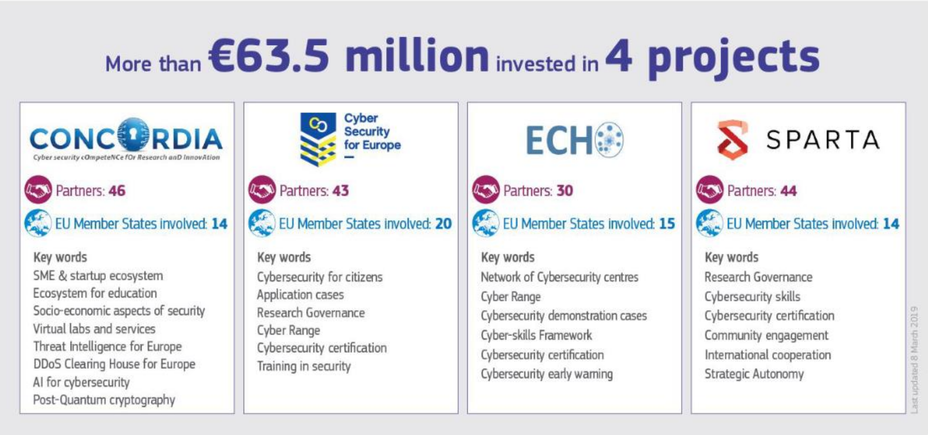
Stephan Krenn
AIT Austrian Institute of Technology

Joint work with David Goodman, Juan Carlos Perez Baun, …

CyberSec4Europe

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE



More than €63.5 million invested in 4 projects

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**

EU Member States involved: **14**

Key words

- SME & startup ecosystem
- Ecosystem for education
- Socio-economic aspects of security
- Virtual labs and services
- Threat Intelligence for Europe
- DDoS Clearing House for Europe
- AI for cybersecurity
- Post-Quantum cryptography

Cyber Security for Europe

Partners: **43**

EU Member States involved: **20**

Key words

- Cybersecurity for citizens
- Application cases
- Research Governance
- Cyber Range
- Cybersecurity certification
- Training in security

ECHO

Partners: **30**

EU Member States involved: **15**

Key words

- Network of Cybersecurity centres
- Cyber Range
- Cybersecurity demonstration cases
- Cyber-skills Framework
- Cybersecurity certification
- Cybersecurity early warning

SPARTA

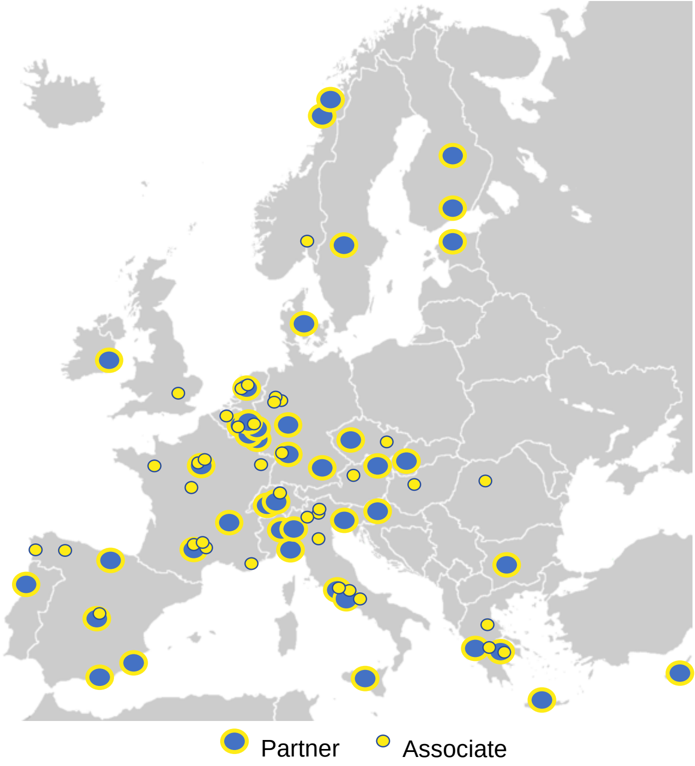
Partners: **44**

EU Member States involved: **14**

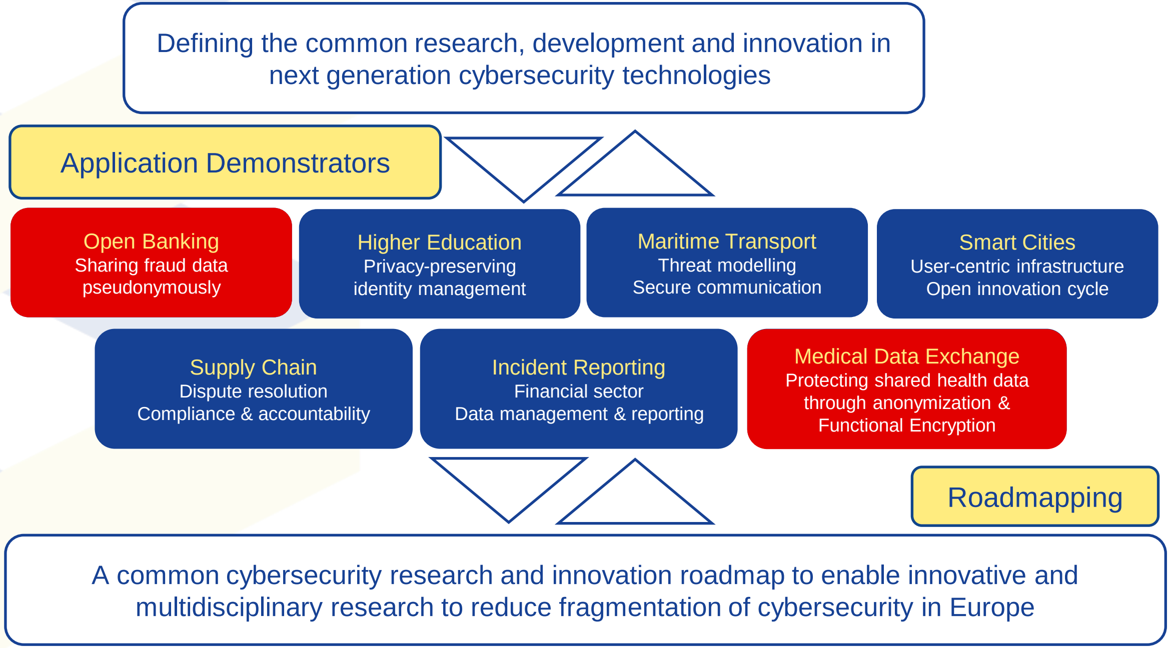
Key words

- Research Governance
- Cybersecurity skills
- Cybersecurity certification
- Community engagement
- International cooperation
- Strategic Autonomy

Last updated 8 March 2019



From Research to Innovation to Industry



Defining the common research, development and innovation in next generation cybersecurity technologies

Application Demonstrators

Open Banking
Sharing fraud data pseudonymously

Higher Education
Privacy-preserving identity management

Maritime Transport
Threat modelling
Secure communication

Smart Cities
User-centric infrastructure
Open innovation cycle

Supply Chain
Dispute resolution
Compliance & accountability

Incident Reporting
Financial sector
Data management & reporting

Medical Data Exchange
Protecting shared health data through anonymization & Functional Encryption

Roadmapping

A common cybersecurity research and innovation roadmap to enable innovative and multidisciplinary research to reduce fragmentation of cybersecurity in Europe

Cyber Security for Europe

Open Banking

OBSIDIAN

Open Banking Sensitive Data Sharing Network for Europe

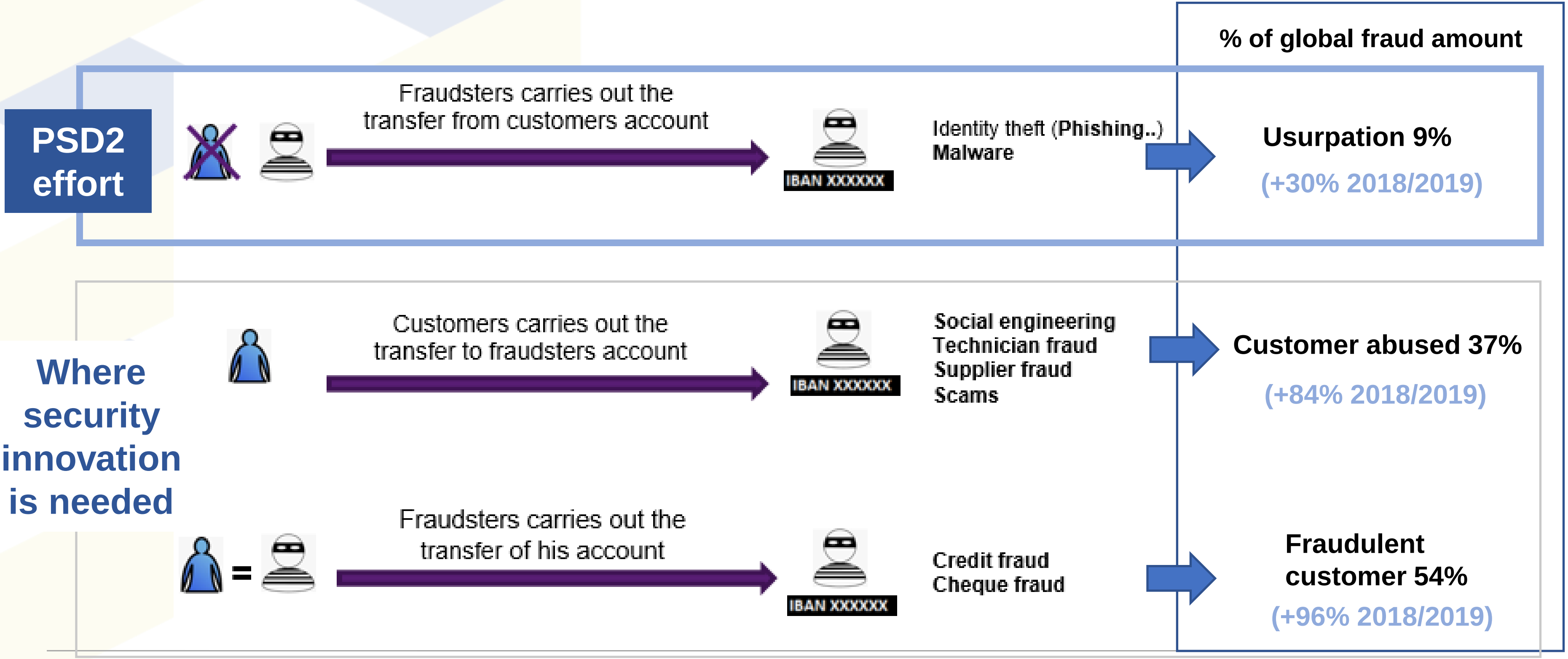
- High incidence of fraud regularly cost financial institutions – and their customers – very large sums of money.

- OBSIDIAN is a pilot **data sharing network** which supports the fight against fraud by **sharing false IBANs between banks** and is an effective approach to **detecting money laundering** or **terrorist financing**

- Participating banks experiencing potential fraud attempts will request confirmation of the right decision to take
  - The requests provide the core transaction data (IBAN et al) in a format which guarantees privacy and security network requirements.

Fraud Evolution

Why sharing fraud information is a good idea



% of global fraud amount

PSD2 effort

Fraudsters carries out the transfer from customers account

IBAN XXXXXX

Identity theft (Phishing..)
Malware

Usurpation 9%

(+30% 2018/2019)

Where security innovation is needed

Customers carries out the transfer to fraudsters account

IBAN XXXXXX

Social engineering
Technician fraud
Supplier fraud
Scams

Customer abused 37%

(+84% 2018/2019)

=

Fraudsters carries out the transfer of his account

IBAN XXXXXX

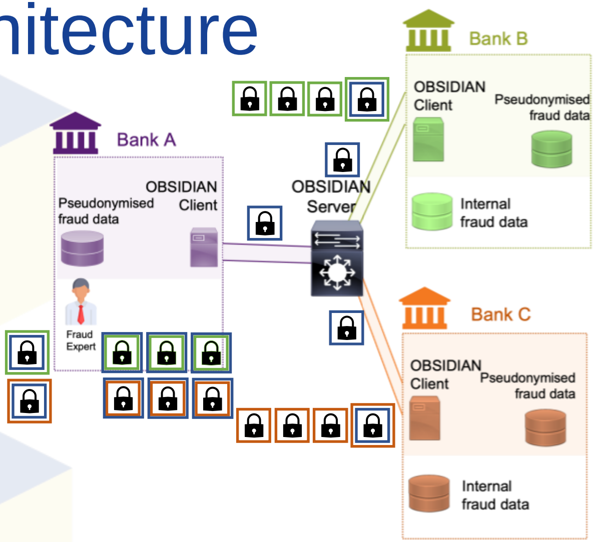
Credit fraud
Cheque fraud

Fraudulent customer 54%

(+96% 2018/2019)

OBSIDIAN – Architecture

- A fraud expert (or system) detects a suspicious transaction and uses the OBSIDIAN network to check the beneficiary's IBAN
- The OBSIDIAN client applies a pseudonymisation and sends the request to the server
- OBSIDIAN server broadcasts Bank A requests to the other network participants (Banks B and C)
- Each bank receiving the request re-randomizes the request



- Banks that received the request send back the re-randomized request and pseudonyms on fraudulent accounts
- The server relays the responses back to Bank A
- Bank A checks for matches

Reasons why banking secrecy is protected:

- ✓ Banks B and C don't know the request came from Bank A
- ✓ Bank A cannot identify the origin of the responses
- ✓ Banks B and C do not know the result of the request

In the exchange, no one knows who exchanged information with whom

OBSIDIAN – Innovation

Regulatory compliance

- ✓ GDPR Compliant
- ✓ Banking secrecy protected

International applicability

- ✓ Applicable to the countries with the most restrictive secrecy laws
- ✓ Can easily be expanded into a European network

Data never handed over

- ✓ The OBSIDIAN server **does not store fraud data**
- ✓ IBANs are always pseudonymised when exchanged
- ✓ Banks can take back their data whenever necessary (GDPR right to erasure)

Easy integration

- ✓ No complicated mathematics : technology easily understood by IT experts
- ✓ Simple integration : one client connected to one server only

OBSIDIAN – Collaborating Banks

- An OBSIDIAN network has been piloted with 8 major French banks under the umbrella of the French Banking Federation
- The crucial non-technical issues that OBSIDIAN addresses are:
  - GDPR compliance
  - Banking secrecy

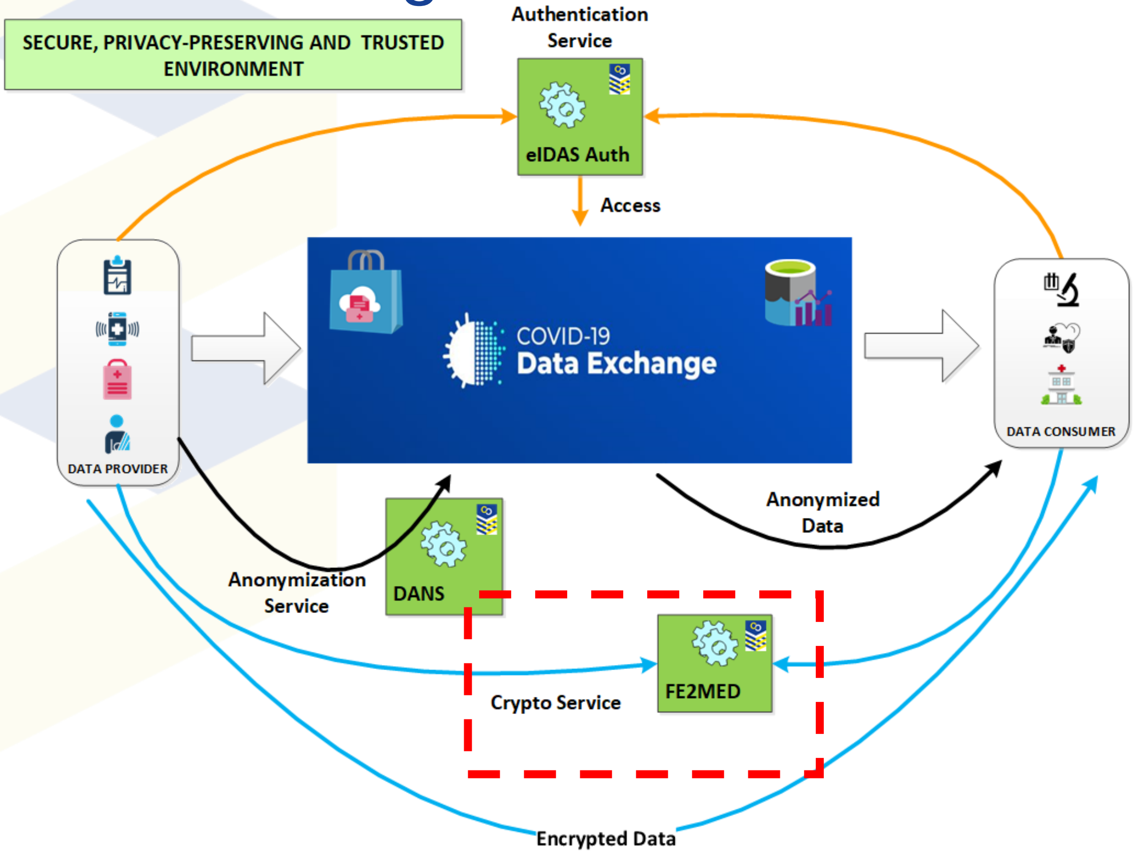
One of the issues is that most banks are not motivated to share their (data) assets and are innately conservative

However, the underlying premise – bank fraud – is getting worse, year-on-year and it is recognised that compliant data sharing is the way forward

Cyber
Security
for Europe

Medical Data Sharing

Medical Data Exchange

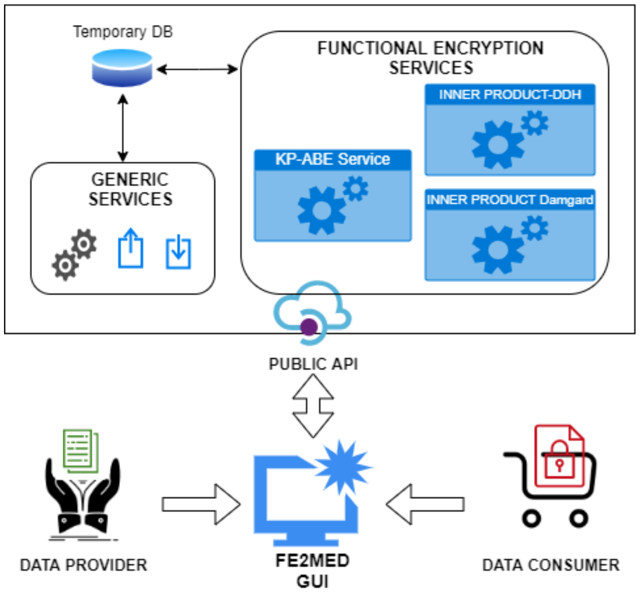


FE2MED (Functional Encryption To Medical Data)

- Secure personal and sensitive data
- Ensure confidentiality and data integrity
- The encrypted data are only accessible to certain allowed users

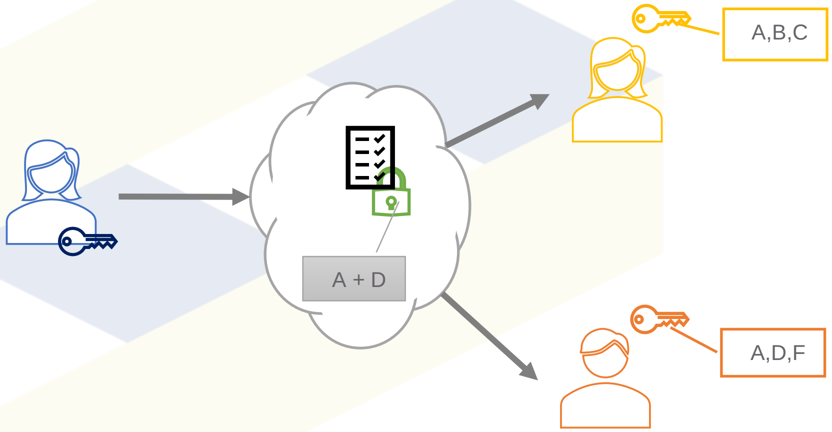
- Leverage two advanced primitives:
  - Attribute-based encryption
  - Functional encryption

FE2MED as a Service

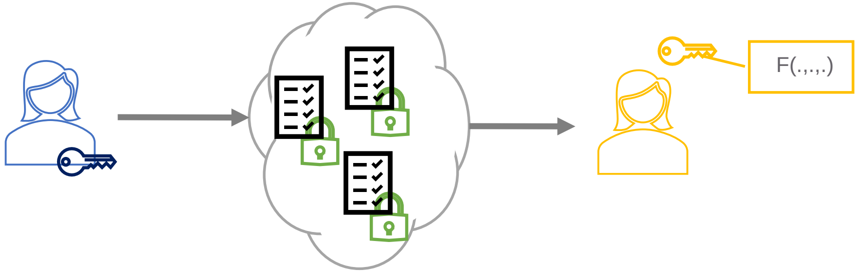


Advanced Encryption Schemes

Attribute-Based Encryption

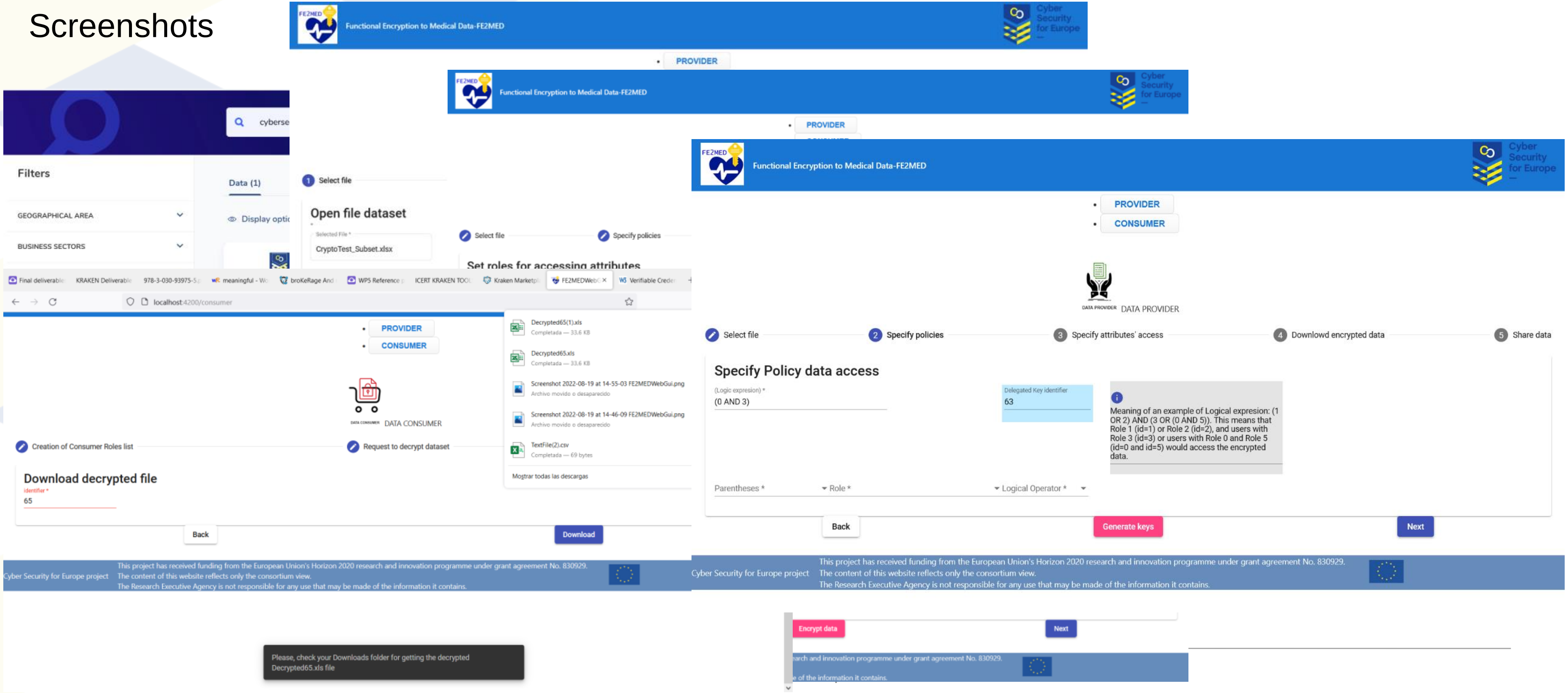


Functional Encryption



FE2MED GUI

Screenshots



Functional Encryption to Medical Data-FE2MED

- PROVIDER
- CONSUMER

Filters

GEOGRAPHICAL AREA

BUSINESS SECTORS

Data (1)

Display optic

1 Select file

Open file dataset

Selected File *
CryptoTest_Subset.xlsx

Select file — Specify policies

Set roles for accessing attributes

localhost:4200/consumer

DATA CONSUMER

Creation of Consumer Roles list — Request to decrypt dataset

Download decrypted file

identifier *
65

Back — Download

Decrypted65(1).xls
Completada — 33,6 KB

Decrypted65.xls
Completada — 33,6 KB

Screenshot 2022-08-19 at 14-55-03 FE2MEDWebGui.png
Archivo movido o desaparecido

Screenshot 2022-08-19 at 14-46-09 FE2MEDWebGui.png
Archivo movido o desaparecido

TextFile(2).csv
Completada — 69 bytes

Mostrar todas las descargas

Cyber Security for Europe project — This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830929.
The content of this website reflects only the consortium view.
The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Please, check your Downloads folder for getting the decrypted Decrypted65.xls file

DATA PROVIDER

Select file — 2 Specify policies — 3 Specify attributes' access — 4 Downlowd encrypted data — 5 Share data

Specify Policy data access

(Logic expresion) *
(0 AND 3)

Delegated Key identifier
63

Meaning of an example of Logical expresion: (1 OR 2) AND (3 OR (0 AND 5)). This means that Role 1 (id=1) or Role 2 (id=2), and users with Role 3 (id=3) or users with Role 0 and Role 5 (id=0 and id=5) would access the encrypted data.

Parentheses * — Role * — Logical Operator *

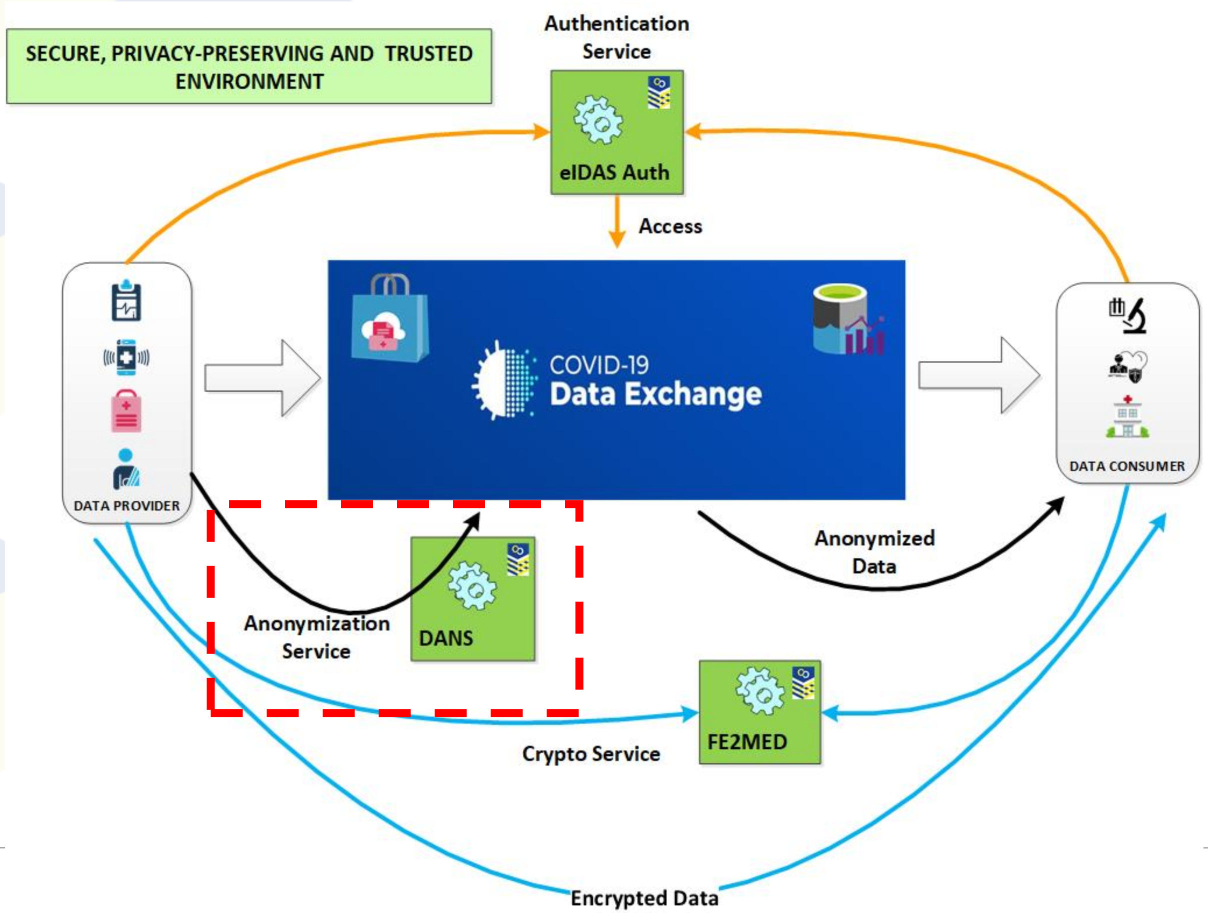
Back — Generate keys — Next

Cyber Security for Europe project — This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830929.
The content of this website reflects only the consortium view.
The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Encrypt data — Next

arch and innovation programme under grant agreement No. 830929.
e of the information it contains.

Data Anonymization



Data Anonymization

- ***k*-anonymity**
  - Each quasi-identifier tuple has at least *k* records in the anonymized dataset
  - Concepts: suppression, generalization

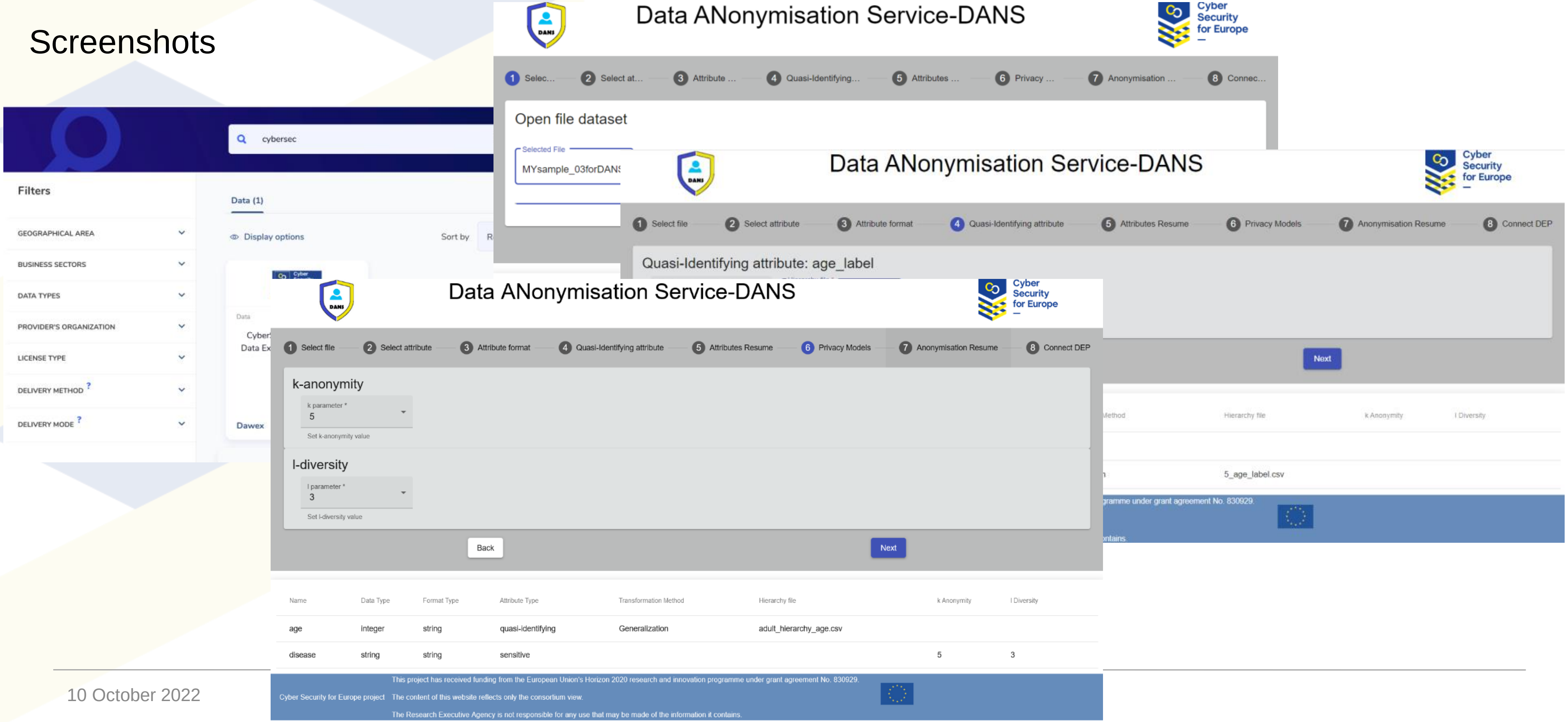
Name	Age	Gender	Disease
Alice	31	F	Cancer
Bob	28	M	No illness
Charlie	34	M	Heart-related
Dan	38	M	Cancer

Name	Age	Gender	Disease
*	31-40	F	Cancer
*	21-30	M	No illness
*	31-40	M	Heart-related
*	31-40	M	Cancer

- **l-diversity**
  - For each set of rows with identical quasi-identifiers, there are at least l distinct values for each sensitive attributes

DANS GUI

Screenshots


cybersec
Filters
GEOGRAPHICAL AREA
BUSINESS SECTORS
DATA TYPES
PROVIDER'S ORGANIZATION
LICENSE TYPE
DELIVERY METHOD ?
DELIVERY MODE ?
Data (1)
Display options
Sort by
Dawex
Data ANonymisation Service-DANS
1 Selec… 2 Select at… 3 Attribute … 4 Quasi-Identifying… 5 Attributes … 6 Privacy … 7 Anonymisation … 8 Connec…
1 Select file 2 Select attribute 3 Attribute format 4 Quasi-Identifying attribute 5 Attributes Resume 6 Privacy Models 7 Anonymisation Resume 8 Connect DEP
Back
Next

Open file dataset

Selected File: MYsample_03forDANS

Quasi-Identifying attribute: age_label

k-anonymity

k parameter *: 5

Set k-anonymity value

l-diversity

l parameter *: 3

Set l-diversity value

Name	Data Type	Format Type	Attribute Type	Transformation Method	Hierarchy file	k Anonymity	l Diversity
age	integer	string	quasi-identifying	Generalization	adult_hierarchy_age.csv		
disease	string	string	sensitive			5	3

Hierarchy file: 5_age_label.csv

Cyber Security for Europe project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830929.

The content of this website reflects only the consortium view.

The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Cyber
Security
for Europe

Thank you!

Stephan Krenn
Senior Scientist
AIT Austrian Institute of Technology
stephan.krenn@ait.ac.at

Further contacts: David Goodman <david@trustindigitallife.eu>
Juan Carlos Perez Baun <juan.perezb@atos.net>
CyberSec4Europe <info@cybersec4europe.eu>

Save the date:
MOMENTUM!
1 – 2 December, 2022
Brussels
https://cybersec4europe.eu/