Gap Analysis for Information Security in Interoperable Solutions at a Systemic level: The KONFIDO Approach

J. Rasmussen, **P. Natsiavas***, K. Votis, K. Moschou, P. Campegiani, L. Coppolino, I. Cano, D. Marí, G. Faiella, O. Stan, O. Abdelrahman, M. Nalin, I. Baroni, M. Voss-Knude, V.A. Vella, E. Grivas, C. Mesaritakis, J. Dumortier, J. Petersen, D. Tzovaras, L. Romano, I. Komnios and V. Koutkias

* Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Greece

Presentation Structure

KONFIDO Overview

Aim: … to create a holistic paradigm for secure, cross-border exchange, storage and overall handling of healthcare data …

Core technologies:

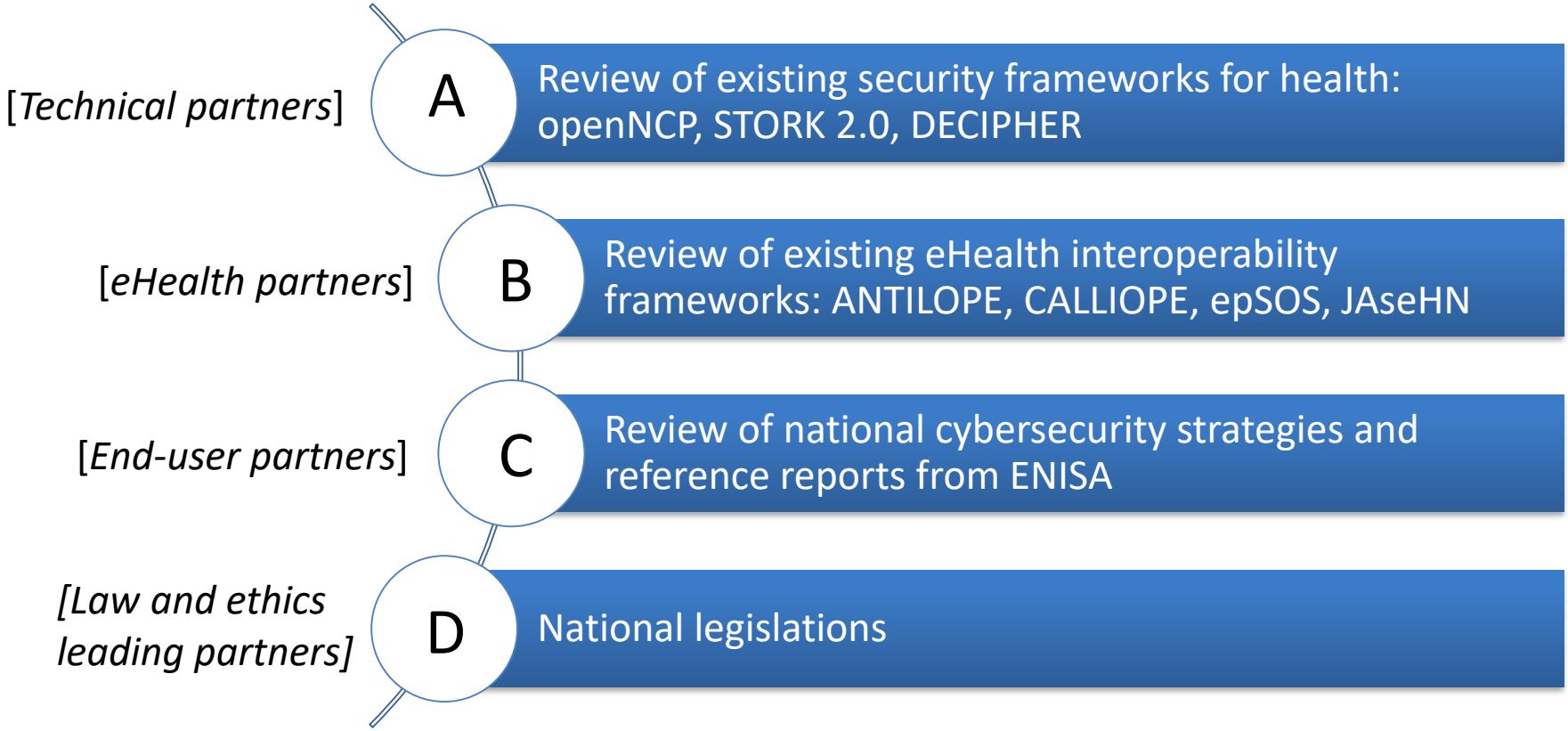
- Blockchain and advanced auditing mechanisms
- eID Support
- COTS CPU technology
- Homomorphic encryption
- Physical Unclonable Function (PUF) based security solutions relying on photonic technologies
- Security Information and Event Management (SIEM)

+ building upon existing solutions, e.g. OpenNCP/epSOS, eID/STORK2.0, DECIPHER, etc.

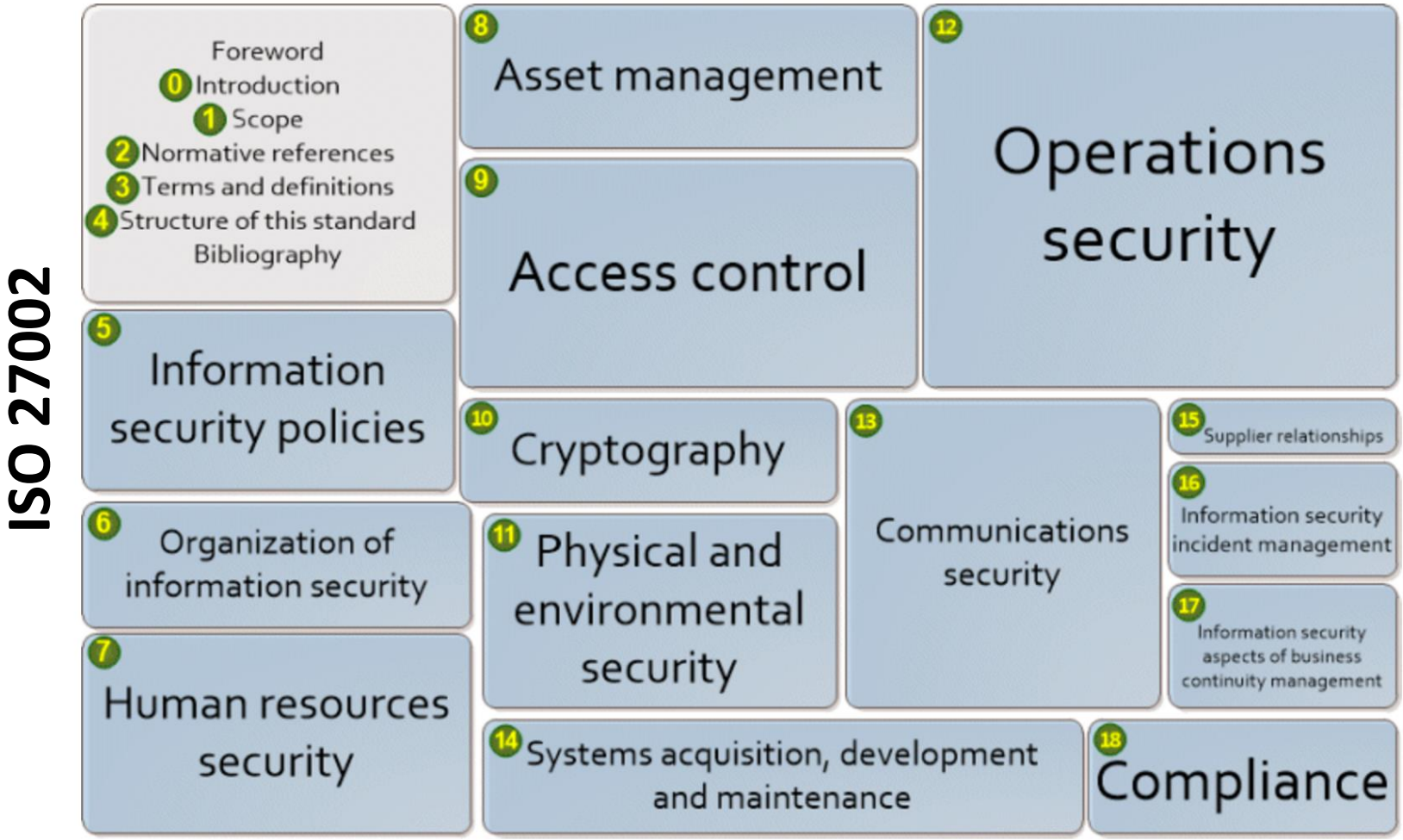
Gap Analysis Rationale

Systematic gap analysis for interoperable solutions at a systemic level with a focus on digital security of health related data

KONFIDO Gap Analysis Approach



Systematic Gap Analysis = Use of Standards



Gap Analysis: List of Used Standards

ISO	DOMAIN	TITLE	REFERENCE
ISO/IEC 27002	Information technology	Security techniques — Code of practice for information security management	https://www.iso.org/standard/54533.html
ISO/IEC 27010	Information technology - Security techniques	Information security management for inter-sector and inter-organizational communications	https://www.iso.org/standard/68427.html
ISO/IEC 27040	Information technology - Security techniques	Storage security	https://www.iso.org/standard/44404.html
IS0 27799	Health informatics	Information security management in health using ISO/IEC 27002	https://www.iso.org/standard/62777.html
ISO 22857	Health informatics	Guidelines on data protection to facilitate trans-border flows of personal health information	https://www.iso.org/standard/52955.html
ISO/IEC 25010	Systems and software engineering	Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models	https://www.iso.org/standard/35733.html

Gap Analysis: Template Structure

- Security policy
- Organizing 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
- Usability

Gap Analysis: Data Collection Method

- *Desk research*: Review of available material (reports/deliverables, publications, presentations, etc.) on the analysis subject
- *Expert opinion*: The information is from a source with concrete detailed expertise about the analysis subject (e.g. someone who was directly involved in the project, or who works in the respective organisation)
- *Interview*: The analysis subject was analysed through an interview with a person with particular knowledge on the analysis subject and security aspects

Gap Analysis: Summary of Outcomes for Technical Security Frameworks

Security Theme	STORK 2.0	DECIPHER	OpenNCP
Security Policy			
Organising Information Security			
Asset management			
Human Resources Security			
Physical and environmental security			
Communications and operations management			
Access Control			
Information systems acquisitions, developments and maintenance			
Information Security Incident Management			
Business Conformity Management			
Compliance			
Usability			

Gaps have been identified
No gap has been identified
Out of scope

Gap Analysis: Summary of Outcomes for eHealth Interoperability Frameworks

Security Theme	SemanticHealth Net	JAseHN	Antilope	epSOS
Security Policy				
Organising Information Security				
Asset management				
Human Resources Security				
Physical and environmental security				
Communications and operations management				
Access Control				
Information systems acquisitions, developments and maintenance				
Information Security Incident Management				
Business Conformity Management				
Compliance				
Usability				

Gaps have been identified

No gap has been identified

Out of scope

Gap Analysis: Recommendations

- *Strive for high adherence to standards across all domains and subjects as it ensures trust and is in line with the end-users' approach*
- *Take into account the users of a centralised technology and framework in terms of details of information security.*
- *Implement state-of-the-art security technologies and measures*
- *Ensure information security sustainability in technical solutions*
- *Explore further the implementation issues of the relevant security software frameworks*

Questions?

Have your say in the Ongoing KONFIDO Survey Targeting Citizens/Patients!

Please follow the link: https://goo.gl/7mX8eL

OR

Scan the QR code:

Thank you!

KONFIDO

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 727528.

Partners

EXUS (Coordinator), CERTH, CINI, CEA, TLX, EULAMB, TLB, EURECAT, MEDCOM, ICL, BIT4ID, PAUSIL, SUNDHED, AQUAS, IDIBAPS