User Requirements Elicitation for Secure and Interoperable Health Data Exchange

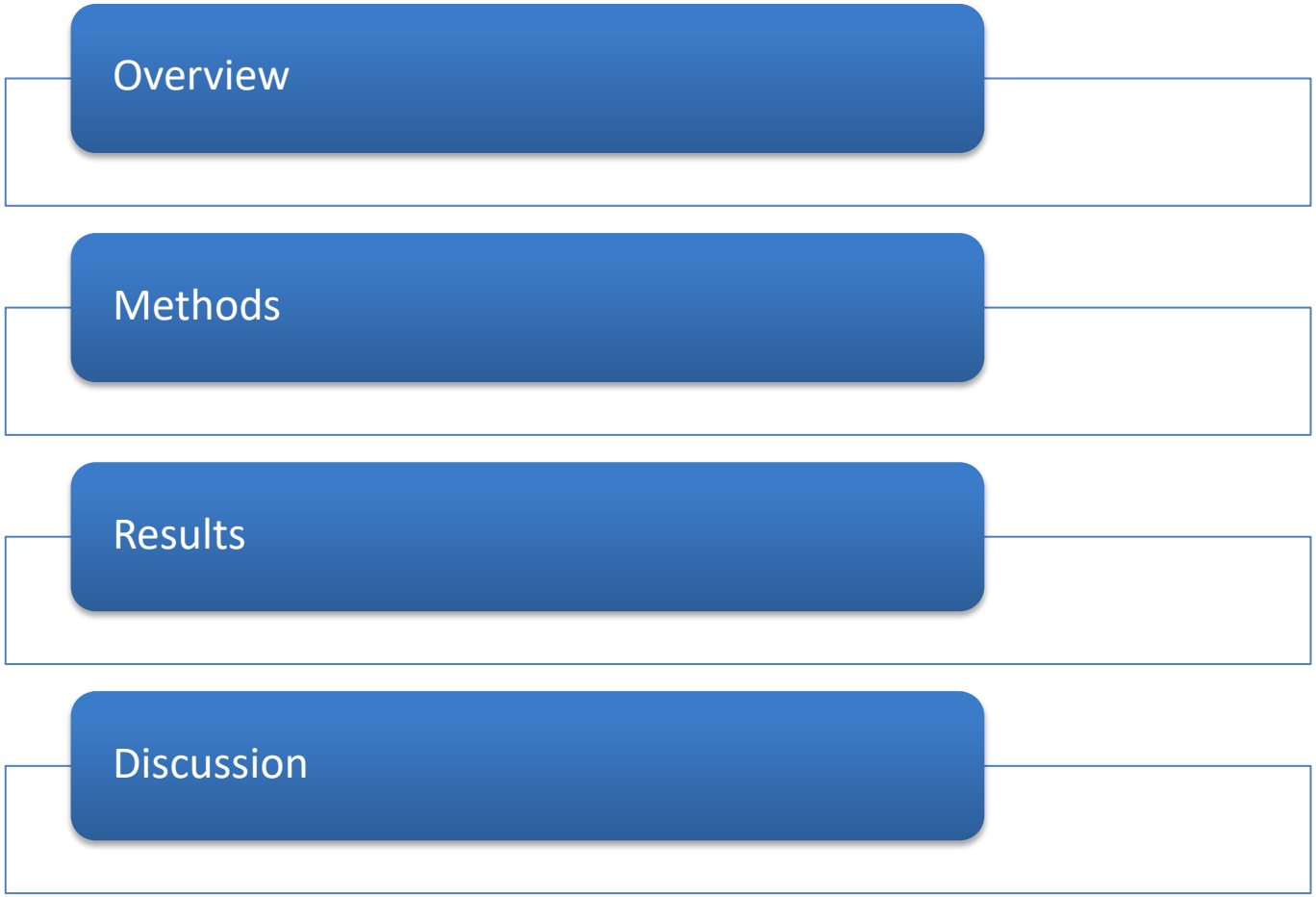
Pantelis Natsiavas[1], Christine Kakalou[1], Konstantinos Votis[2], Dimitrios Tzovaras[2], Nicos Maglaveras[3] and Vassilis Koutkias[1]

[1]Institute of Applied Biosciences, Centre for Research & Technology Hellas

[2]Information Technologies Institute, Centre for Research & Technology Hellas

[3] Department of Electrical Engineering & Computer Science, McCormick School of Engineering & Applied Sciences, Northwestern University

Structure



User requirements elicitation rationale

Definition: User requirements elicitation is the process of exploiting **various information sources**, in order to "… *discover the current* ***product needs*** *and agree upon the vision and* ***goals*** *of the proposed project*"[1]

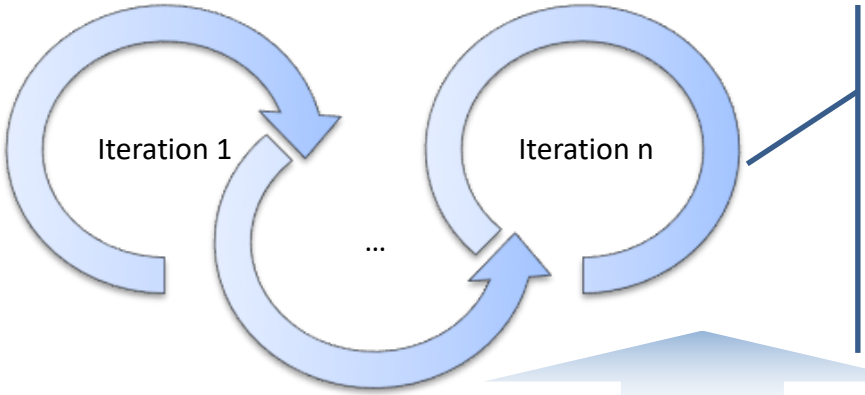
[1]Wong, L., et al.: A systematic literature review about software requirements elicitation. Journal of Engineering Science and Technology 12(2), 296–317 (2017).

Requirements engineering process

Scenarios definition & analysis

Pan-European eHealth solutions acceptance and KONFIDO adaptation

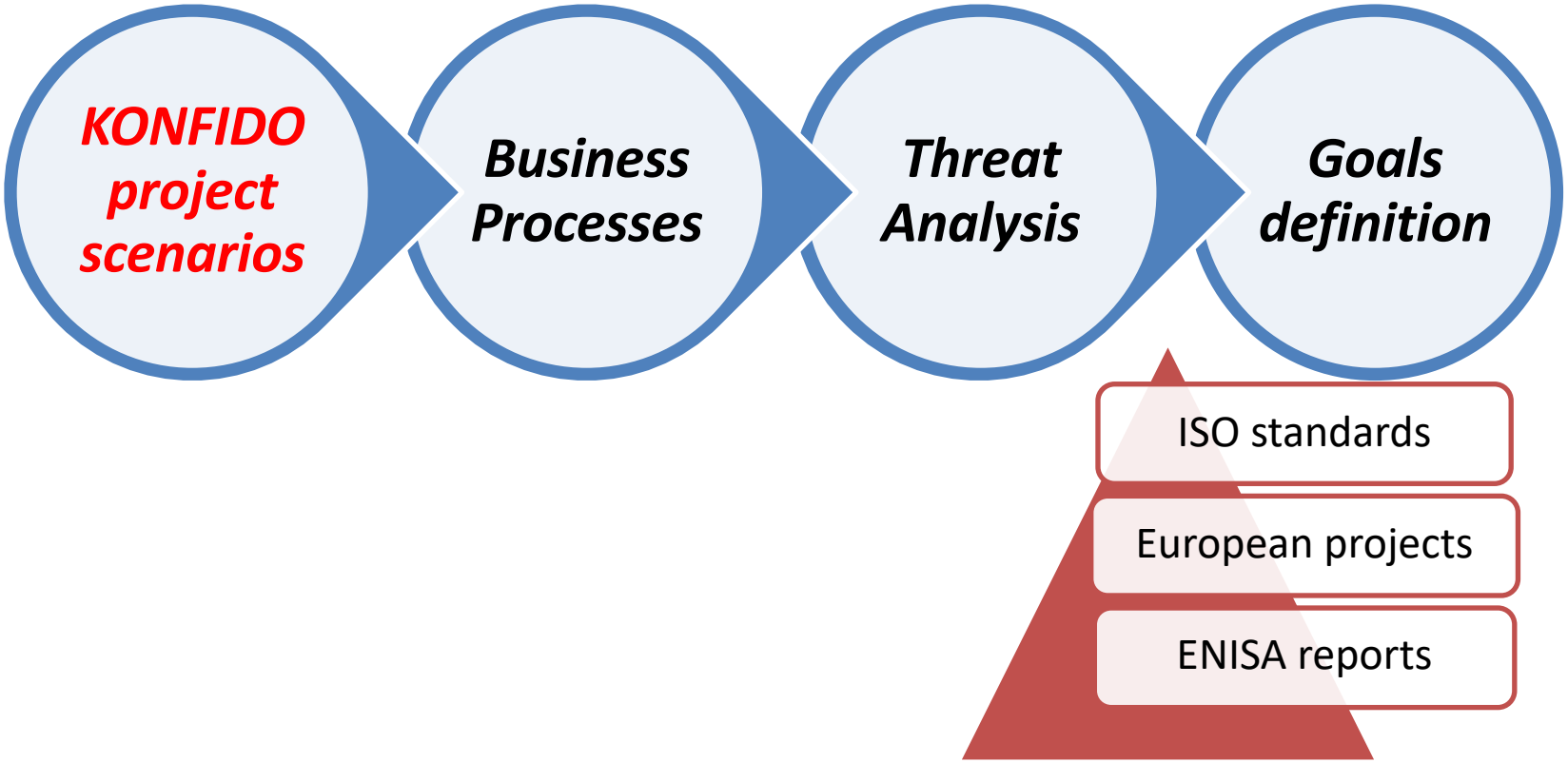
User requirements elicitation



Input from
- gap analysis
- Scenarios analysis
- Workshops
- surveys
- end-users
- etc.

System requirements and Specification

Methodology



Business processes definition

*Kenneth is a 65-year-old citizen ... planning to spend 10 days in Barcelona… His doctor informs him that thanks to the technology developed in KONFIDO which has been deployed nationally in both Denmark and Spain, he can **securely grant access** to healthcare professionals in Barcelona to **view** the necessary parts of his medical record ... Kenneth and the healthcare professionals in Barcelona can **authenticate** themselves with their national issued eID, … [data] will be **securely transmitted and registered** to his medical record in Denmark, while all the other parts of his record will **remain intact** (the novel auditing mechanism of KONFIDO **will keep track** of all transactions ensuring that medical data are protected against tampering, forging and deletion). This information will be also securely **shared** with the Danish specialist that is taking care of Kenneth, who can **follow-up** the incident and explain him what is the case.*

Threat analysis: STRIDE model

Spoofing: gaining access to a system via a false identity

Tampering: unauthorized modification of data

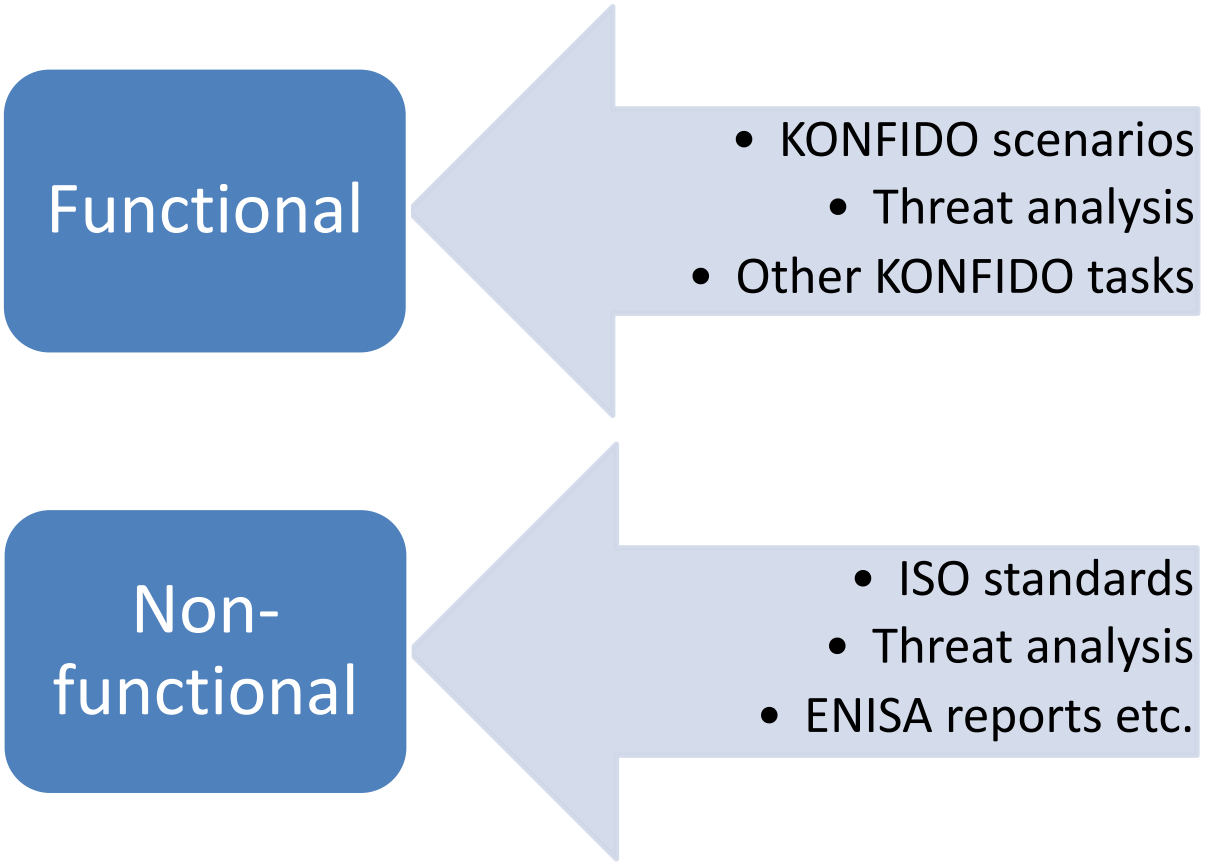
Repudiation: denial of actions (legitimate or not) users

Information disclosure: exposure of sensitive data

Denial of service: making a system unavailable

Elevation of privileges: self-assigning more privileges

Goal definition



Results – Business Processes

BP1: Grant access to own Medical Records
BP2: Access foreign patient's medical records
BP3: Authenticate using national eID infrastructure
BP4: Transmit data for tele-monitoring purposes
BP5: Access patient's medical record while transferred in ambulance
BP6: Exchange of triage information while patient transferred to the hospital via ambulance
BP7: Exchange of medical information between HCPs

Results – Assets for BP1

A1: Medical record information	The main asset to be protected.
A2: Patient credentials	For example, usernames, passwords etc.
A3: Patient authentication means	For example, eID card or computer.
A4: Intention of granting access to medical record	The intention of granting access to medical record is crucial. It could imply an attack attempt and the medical record owner should be notified, or it implies that the patient intends to have a medical transaction, and this is also an information to be protected.

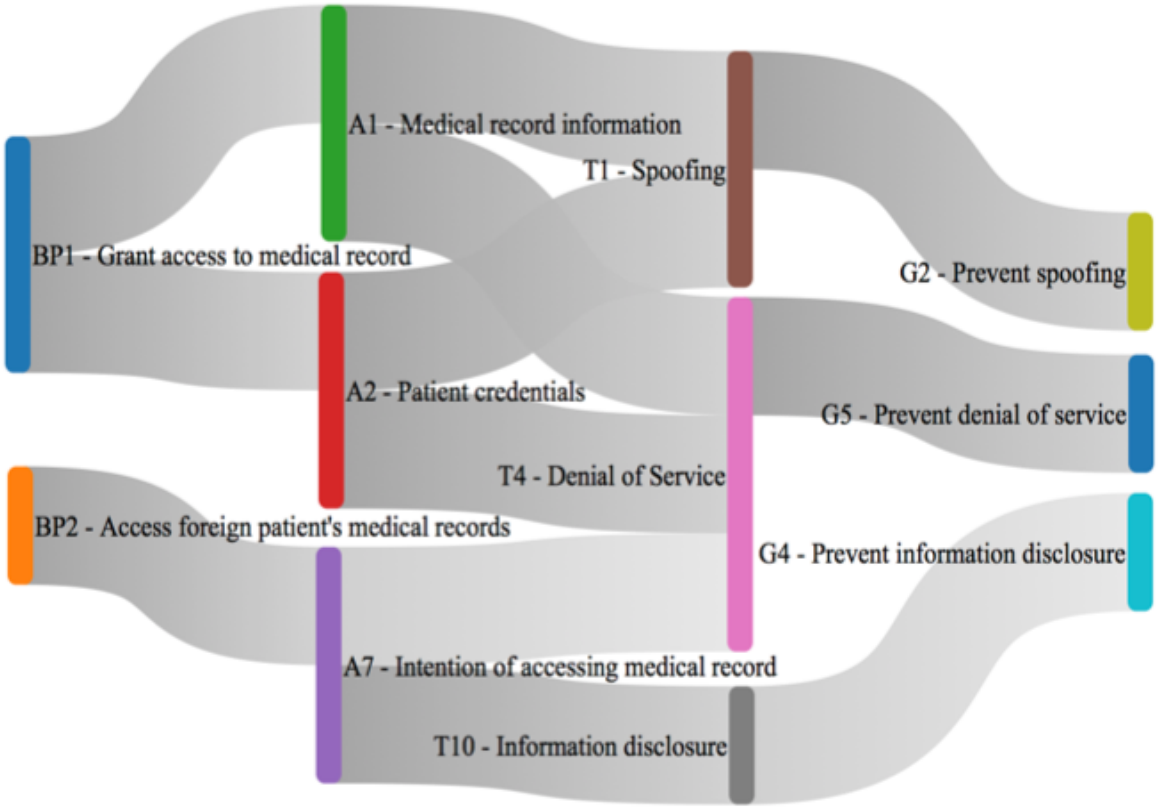
Results – Threats for BP1

Threat	Malicious actor(s)
T1: Spoofing	HCPs, other actors without a clear role in the BP
T2: Repudiation	Patients
T3: Information disclosure	HCPs, other actors without a clear role in the BP
T4: Denial of Service (DoS)	Other actors without a clear role in the BP
T5: Privilege Elevation	Other actors without a clear role in the BP
T6: Physical stealing	HCPs, other actors without a clear role in the BP

Results – Goals for BP1

G1: Grant access to Medical Records	BP (Functional)
G2: Prevent spoofing	STRIDE
G3: Prevent repudiation	
G4: Prevent information disclosure	
G5: Prevent DoS	
G6: Prevent privilege elevation	
G7: Prevent physical stealing attacks	
G8: Focus on usability	Other sources
G9: Allow another person to grant access to Medical Records	

Meta analysis – partial view



Conclusion

- Meta-analysis
  - Complex interdependencies
  - High value of standards as a guide
  - The number of interdependencies could be used to guide end-user goal prioritization

Thank you!

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