Empowering privacy and security in non-trusted environments

Objectives

WITDOM aims at producing a framework for end-to-end protection of data in untrusted and fast-evolving ICT-based environments.
WITDOM puts particular focus in scenarios requiring data outsourcing, where new threats, vulnerabilities and risks require end-to-end security solutions that can foster progress for the lifetime of applications they support.
The WITDOM framework uses security-and-privacy-by-design methodologies, and advance the state of the art in effective protection of personal and sensitive data in the following areas:

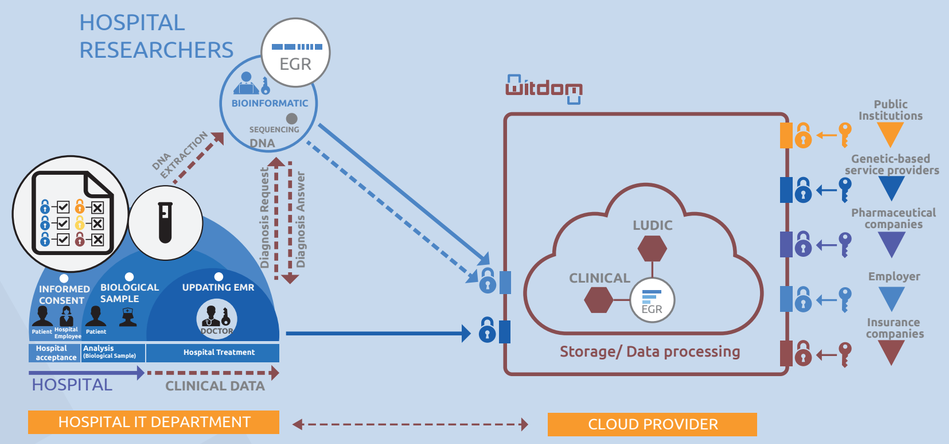
- Privacy enhancing techniques, perturbation mechanisms and privacy metrics
- Privacy-preserving cryptographic techniques supporting encrypted processing
- Cryptographic techniques for integrity and verifiability of outsourced processes
- European legal landscape.

Scenarios

The WITDOM framework is instantiated and validated in two privacy-sensitive application scenarios:

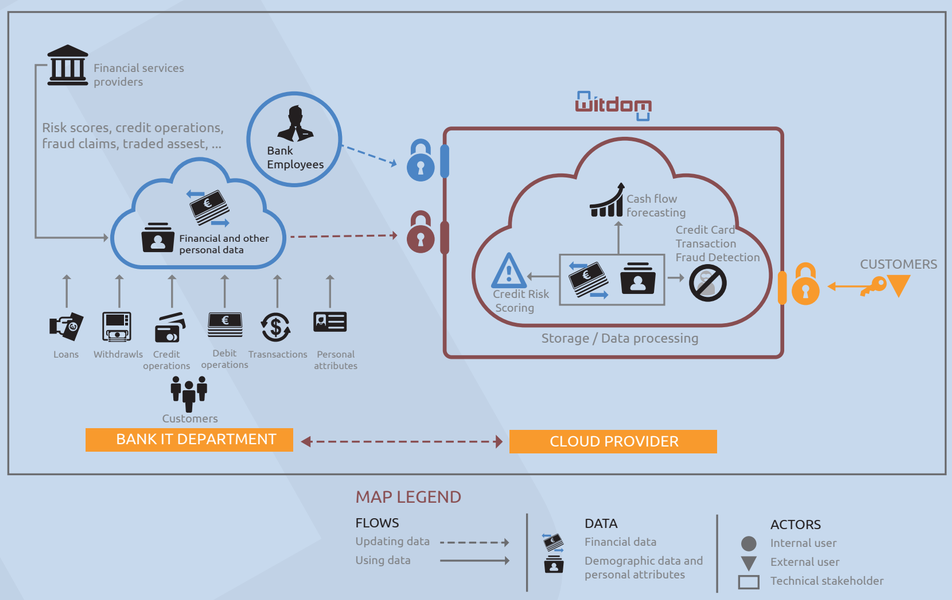
e-Health

Genetic/proteomic data protection, shared for large-scale research analyses and outsourced clinical analysis.



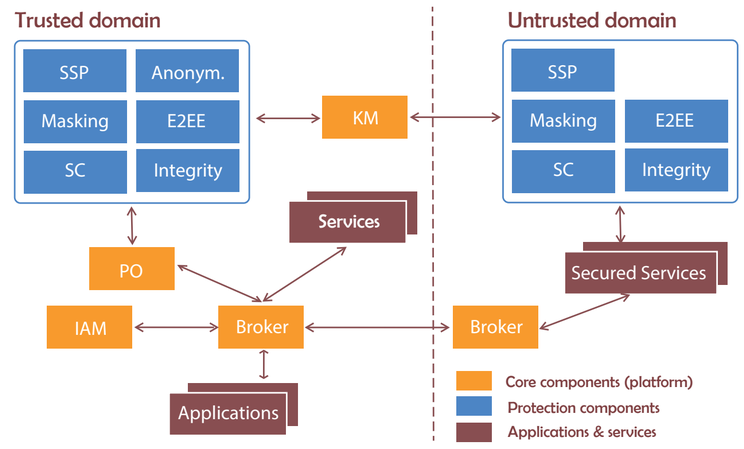
Financial Services

Protection of large-scale outsourced financial data storage and processing (e.g., financial risk calculation or fraud detection).



Initial Architecture

- Service-oriented architecture
- Applicable to multiple scenarios
- Modular, extensible and flexible
- Complex service composition by successive calls to individual services
- Services can be securely deployed in the trusted and untrusted domain



Outcomes

General Outcomes

Framework

- Methodology for analysis and assessment of end-to-end privacy/security.
- Objective privacy metrics and quantifiable evaluation mechanisms
- Analysis and formalization guidelines and methods for the analysis of security requirements and trust relationships
- Privacy and security by design and user-empowered architectures for outsourced/ distributed environments

Implementation Level

Toolkit and prototypes

- Privacy-preserving toolkit implementing privacy-preserving primitives, protocols, privacy-enhancing techniques (PETs) and formalized preferences for user-centric verifiable outsourced processing
- Multidisciplinarily assessed prototypes for eHealth and Banking scenarios, making use of the toolkit and showcasing the net advance and impact of the general and practical outcomes in two privacy-aware scenarios

Practical Level

Platform

- Definition and enforcement of user-centric privacy-preferences
- Security and privacy analysis for outsourced/ distributed eHealth and Financial services scenarios, instantiated architectures
- Resource-efficient cryptographic primitives, protocols and PETs for outsourced processing of sensitive data (addressing the trade-off between good performance and strong cryptographic protection)
- Efficient cryptographic verifiability mechanisms for user-empowered outsourced processing
- Evaluation of the developed primitives, quantitative assessment of the net advances in utility, efficiency and privacy/security

CONTACT

Project Coordinator:
Elsa Prieto
elsa.prieto@atos.net

Project Scientific Coordinator:
Juan Ramón Troncoso
troncoso@gts.uvigo.es

www.witdom.eu

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The work described in this poster has been conducted within the project WITDOM, started in January 2015. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 64437. This work was supported in part by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0098. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government or of the European Commission.