



Standardisation Activities in Curex H2020 project

Outline

CUREX H2020 Project
CUREX's standardisation strategy
CUREX Innovation Potential
CUREX innovations at a glance
Standards Identified relevant to Cyber Hygiene
Other activities on ICT standardisation



CUREX H2020 project

CUREX is working towards the protection of the confidentiality and integrity of health data by producing a novel, flexible and scalable situational awareness-oriented platform.

It allows a healthcare provider to assess the realistic cybersecurity and privacy risks they are exposed to and suggest mathematically optimal strategies for addressing these risks with safeguards.

At the core of the CUREX platform, a decentralised architecture enhanced with a private blockchain infrastructure ensures the integrity of the risk assessment process and of all data transactions that occur between the diverse range of stakeholders involved.

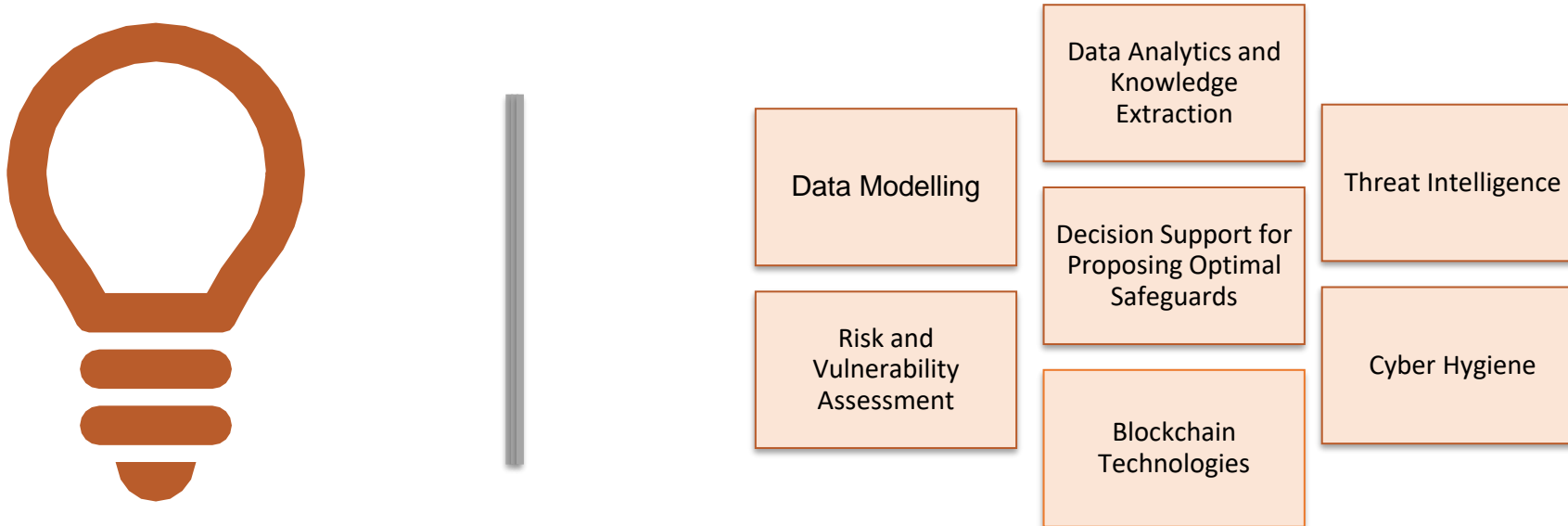


CUREX's standardisation strategy

- To reach the maximum impact on standardisation and relevant bodies, CUREX has defined a **four-step strategy**:
 - 1) Observation and monitoring of the available standards
 - 2) Derivation of required standards from the CUREX use cases
 - 3) Identification of gaps (technical, but also commercial, operational, business, regulatory, etc.) / improvements introduced by the **CUREX's key innovations**
 - 4) Recommendation to corresponding standard body

CUREX Innovation Potential

- The seven (7) key innovation aspects of CUREX



CUREX innovations at a glance



Legend

- ADT: Asset Discovery Tool
- VDM: Vulnerability Discovery Manager
- TIE: Threat Intelligence Engine
- KEA: Knowledge Extraction and Analytics
- CAT: Cybersecurity Assessment Tool
- PAT: Privacy Assessment Tool
- OST: Optimal safeguards Tool
- CH: Cyber Hygiene
- PrB: Private Blockchain

Standards Identified relevant to Cyber Hygiene



Information technology — Security techniques — Information security management systems — Overview and vocabulary [ISO/IEC 27000:2018]

Status: Published (Available in EN, FR)

Scope: Provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization.

The terms and definitions provided in this document:

cover commonly used terms and definitions in the ISMS family of standards;

do not cover all terms and definitions applied within the ISMS family of standards; and

do not limit the ISMS family of standards in defining new terms for use.

Approved by: ENISA

Preview: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

Security and Privacy Controls for Information Systems and Organizations [NIST SP 800-53 rev. 4]

Status: Published (Available: EN)

Scope: Provides a catalogue of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyber-attacks, natural disasters, structural failures, and human errors.

The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk and addresses a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs from both a functionality perspective and an assurance perspective. It also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or operating environments.

Approved by: ENISA

Preview: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf>



Cyber Hygiene Standards - ENS Standard

Status: Published (Available in ES)
Spanish version: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantacion-del-ens/file.html>

Approved by: ENISA



Other activities on ICT standardisation



ICT Verticals and Horizontals for Blockchain Standardisation Roundtables

The European Commission was organising roundtable discussions “ICT Verticals and Horizontals for Blockchain Standardisation” which allowed H2020 projects to present the work done and explore more active involvement in blockchain standardisation activities bodies.

Roundtables involved distinguished standardisation experts working with INATBA, ETSI, CEN-CENELEC, ISO TC307, IEEE, ITU-T and other respective entities.

Approximately 200 Horizon 2020 projects related to the blockchain identified.

More than 60 Horizon 2020 projects, including CUREX, participated by delivering a presentation.



Leveraging data protection goals in CUREX H2020 project

On February 10th, 2021, the eHealth roundtable of the “ICT Verticals and Horizontals for Blockchain Standardisation” took place, during which ALRS delivered on behalf of the CUREX consortium a short presentation.

In this short presentation discussed the six data protection goals and how the CUREX project worked to accomplish them based on lessons learned from collaborations with other projects. As an example, one of the CUREX project's Use Cases was illustrated. Furthermore, were proposed possible interesting topics in the context of blockchain technologies and GDPR legislation that may benefit from standardization efforts.



The six data protection goals as identified by the Conference of the Independent Data Protection Authorities of the Bund and the Lander in Germany. (Privacy&Us, 2017)

StandICT.eu 2023 & CUREX Project Collaboration to Support Evolution of Cybersecurity Standards in eHealth

Both StandICT.eu 2023 and CUREX are supported by the European Commission in the framework of Horizon 2020 Program, and they contribute to shaping Europe's digital future with a shared focus in cybersecurity, Big Data, and eHealth.

This collaboration will benefit the entire StandICT.eu 2023 Community and the European policymakers in standardisation, having the contribution of CUREX experts to the Technical Work Group (TWG) on Cybersecurity on the EUOS. Specific insights in the secure health data exchange are crucial for digital transformation of European healthcare services. Moreover, this collaboration will result in recommendations unlocking the EU Digital Single Market in that field





This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404