FORGING

INDUSTRY-ACADEMIA FORUM
TO UNCOVER THE POTENTIAL OF
EMERGING ENABLING TECHNOLOGIES

CO-CREATION WORKSHOP PRELIMINARY RESULTS

Novel Enabling Technologies For A Sustainable Future: Cyber Safe Data Technologies

Rome, Italy | June 13th-14th, 2024

Funded by the European Union

Group 1: Udayanto Dwi Atmojo, Luigi Briguglio, Adelino Correia, Ilja David

Use-case: TRULY

Facilitators: Maria Carmela Fierro (APRE), Francesca Foliti (APRE)

Healthcare is the sector that the group decided to focus the discussion on. More specifically, they wanted to tackle data management issues within public healthcare services. In this domain, an initial discussion highlighted an overall lack of efficient data sharing systems among medical care providers in European countries. With some country-specific exceptions (like Portugal) most healthcare national systems cannot really count on a structured, integrated, portable, easily accessible, and shareable data management system that allows an efficient use and transfer of citizens' medical data. Simply put, when it comes to people's medical data, there is a very limited (if not inexistent) communication between healthcare providers both in the private and the public sector. For instance, no hospital can access a patient's medical data gathered by another, no healthcare emergency operator has access to a patient's medical history, and so forth.

If health data is not accessible (or difficult to access) even for healthcare operators themselves, it means that there is a substantial lack of interoperability, which impacts the quality of healthcare systems at large, for a number or reasons: it makes it more difficult for citizens to access medical services, increases the risk to lose data, undermines the inclusivity of medical services, raises resource waste concerns, and might even expose citizens to physical risks. This affects a wide variety of actors - from patients (citizens) to doctors (directly), from third-party services (e.g., system integrators) to regulatory bodies and policymakers (indirectly).

According to the group, the root causes of such problem are found in obsolete processes (which often prevent healthcare systems from adapting to technological progress), in an active resistance to (and a mistrust in) new technology adoption shown by medical personnel, in digital illiteracy, and in policy and regulatory gaps.

So, how to efficiently storage and share personal health data to enhance more inclusive, agile, safe, and trustworthy healthcare systems? The solution envisaged by this group is the establishment of a secure and usable health data management service that is accessible anywhere, at any time, and by any (authorised) healthcare operator. The technology deemed to be the most appropriate to achieve this solution is zero trust: by tackling data accessibility issues, it builds trustworthy access to data, thus facilitating data sharing among relevant stakeholders.

This explains why the use-case was named "TRULY - Trustworthy Health Data Access & Share Anytime/Anywhere/by Anyone".

Such solution would enhance reliability, security, efficiency, resilience and inclusivity in the healthcare sector, all while building trust in healthcare institutions. It would also contribute to a smarter use of resources, allowing less medical waste, less papers, less medical examinations, and so forth. Therefore, it would bring both social and environmental benefits, even though the effects on energy consumption remain uncertain.

Group 2: Ângela Faria, Andrew Humphrey, Raj Rajarajan, Santiago Romeu Sala

Use-case: ZENCARE (Zero-Knowledge Enhanced Network for Confidential and Reliable Healthcare)

Facilitator: Livia Di Bernardini (APRE)

The group focused on the Healthcare sector starting the activity by identifying several critical issues such as: continuity of operations against attacks, lack of adequate certification and the security of sensitive data. The inadequate level of protection of personal data was then identified as the most crucial problem. This is because it affects various stakeholders, including healthcare workers who require secure access to patient data for effective treatment while ensuring confidentiality, and patients concerned about the privacy and security of their health information. A poor level of protection and the potential exposure of data leads to higher risk of breaches and a lack of trust on the part of patients.

The proposed solution involves a combination of Zero Knowledge Proofs and Zero Trust technologies. Zero Knowledge Proofs allow for data verification without exposing the data itself, enhancing privacy and security. The Zero Trust framework requires strict verification for every person and device trying to access resources, minimizing the risk of data breaches. This solution aims to create a user-centric privacy-preserving system where users have control over their data, preventing unauthorized access and ensuring that only necessary data is shared.

The value proposition of this solution includes empowering users with control over their data, thus ensuring they can check who accesses their information. The solution aims to foster transparency and trust ensuring that users are more confident in the secure handling of their data.

Implementing this solution faces several barriers. Regulatory challenges involve complying with lack of harmonise implementation of data protection regulations among countries. Ensuring all stakeholders adopt and effectively use the new technologies presents a technology adoption challenge. Overcoming resistance to change and gaining user trust is also crucial for social acceptance. Additionally, addressing gaps in the current IT infrastructure to support new security measures is necessary. Interoperability concerns also need to be addressed to ensure seamless integration with existing healthcare IT systems.

Key resources required for the successful implementation include education and training for healthcare workers, clinicians, and other stakeholders to effectively use new technologies.

Legal and regulatory frameworks need updating to support advanced data protection measures. Expertise in software engineering and ZKP is essential for developing and implementing secure solutions. A robust IT infrastructure capable of supporting these new security measures is also crucial.

The social impacts include increased user trust, improved service delivery, and job creation in cybersecurity and IT fields. The implementation of such solution may also cause a gap between those who are capable of using this technology and those who are under-educated in digital terms (inter-generational gaps, custodial problems etc.). For this reason, training and awareness campaigns are needed. More broadly, the implementation of such solution, may also lead to increased longevity of people (due to an improved healthcare service). In environmental terms, the digital approach reduces paper waste, but the high level of energy consumption needs to be considered.

The “ZENCARE” solution aims to enhance data protection in healthcare through user-centric privacy technologies, ultimately leading to a more secure, transparent, and trusted healthcare system. The solution's impact extends beyond security, fostering user's empowerment, inclusivity and improving the overall healthcare service.

Group 3: Nicolás Castellano Russo, Sefora Maria D'Aiera, Ricardo Rodrigues, Marcelo Viegas

Use-case: NEXT GEN P.A.

Facilitator: Brigita Jurisic (INL)

The group chose Public Administration as the sector of focus due to its vast distribution across different institutions such as courts, immigration office, municipalities, fiscal and social security services, national registry and other. All these different institutions deal with citizen (personal) data and use systems that often lack interoperability and run on old IT infrastructure. Another major issue identified was also lack of awareness of cyber threats that people working in the public administration have as well as citizens themselves. The main problem the group decided to address was personal data being treated as a commodity and not as a valuable asset enabling access to power. The issues identified result in lack of trust in the public administration and consequently government as well as in the increase in cybersecurity incidents.

The solution to this problem proposed was enforcement of security measures through a distributed data storage using a standardized data classification methodology as well as cyber aware database naming. The systems used need to be secure by design. Data integrity needs to be assured as well as continuous training and awareness raising at all levels of society and the public administration employees. In order to deliver on this solution, the group agreed it was important to have an international court dedicated to personal data protection that would enable citizens to enforce regulations in case of any personal data leaks.

The solution proposed by the group can be delivered using zero knowledge proof, a technology already being used in blockchain based systems. To implement this solution investments in cryptography infrastructure is needed as well as cybersecurity specialist knowledge. Major social benefit of this solution is seamless public service engagement and therefore trust in public services and the government. Further social impacts of this solution are recognition of the value of personal data by the citizens, knowledge-empowered citizens as well as citizens feeling safer (or not). Major environmental benefit stems from paperless, digitalised processes that may have impact on the environment through increased need for computer power.