SHAPES Secure Cloud Platform for HealthCare Solutions and Services

Jyri Rajamäki[1, 2] and Aarne Hummelholm[2]
[1] Laurea University of Applied Sciences, Espoo, Finland
[2] University of Jyväskylä, Finland
jyri.rajamaki@laurea.fi
aarne.hummelholm@elisanet.fi
DOI: 10.34190/EWS.20.047

Abstract: The SHAPES project is an ambitious endeavour that gathers stakeholders from across Europe to create, deploy and pilot at large-scale a EU-standardised open platform incorporating and integrating a broad range of solutions, including technological, organisational, clinical, educational and societal, to enable the ageing population of Europe to remain healthy, active and productive, as well as to maintain a high quality of life and sense of wellbeing for the longest time possible. Not only each digital solution will be ethical, legal and appropriate for users, but also the results will align with the full and ethically responsible end-to-end exploitation of the new functionalities empowered by the secure cloud platform. Relevant EU and national legal or regulatory frames, ethical principles and fundamental rights will be considered, not only to guarantee due alignment with the development and use of the secure cloud platform but also to determine how to contribute to the reinforcement of the legal and policy frames to strengthen the deployment of large-scale cyber-secure digital solutions and the sustainability of the digital transformation of health and care delivery in Europe. This work in progress paper presents the project's findings so far with regard to privacy and cybersecurity issues of the SHAPES secure cloud platform.

Keywords: cloud services, cross-border healthcare, eHealth, healthy aging, SHAPES project, well-being

1. Introduction

Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project (European Commission, 2019) that supports the well-being of the elderly at home. This work in progress paper discusses the project's finding during first three months with regard to privacy and cybersecurity issues.

2. From Hospitals to Home

Europe is ageing. Good health is not only of value to the individual as a major determinant of quality of life, well-being and social participation; it contributes to general social and economic growth (Eurostat, 2018). Accessibility to healthcare is thus one of the key priorities of the EU health policy. Integrated care focuses on the needs of the recipient on coordination between diagnosis and treatment and between primary care and secondary care, and between different therapeutic areas and specialties. Benefits of integrated care models are clear; still, the complexity of healthcare systems in individual countries and regions adds to the challenge. The redesign requires shifting care from hospitals to home. While individuals with chronic conditions need regular care and/or support that can often be delivered at home by community nurses, or others, potentially using information and communication technologies. Regular, reliable homecare ensures changes in the condition and treatment, resulting in better-managed conditions and fewer hospitalizations. New digital solutions include assistive robots, eHealth sensors and wearables, Internet of Things (IoT)-enabled devices and mobile applications. Cyber security is a prerequisite for the launch of these services.

Figure 1 shows the process of Intelligent Information Management for eHealth environments and it gives possibilities of how to follow and verify that patient sensor and IoT device data are going to the right place and are accessible only by authorized healthcare individuals. A system called 'IIMP' monitors patients' IoT-devices and sensors' information flow to hospital healthcare systems to provide healthcare personnel with a rapid analysis of the information. IIMP ensures that medical staff can find information about patients even in critical situations. This type of system can also help to find anomalies or data changes, or identify if someone has attempted to penetrate or use data in an undesirable way. The user can create specific action groups for this system. Members of the user group can follow the progress and changes of situations, data resources and reports in real time.

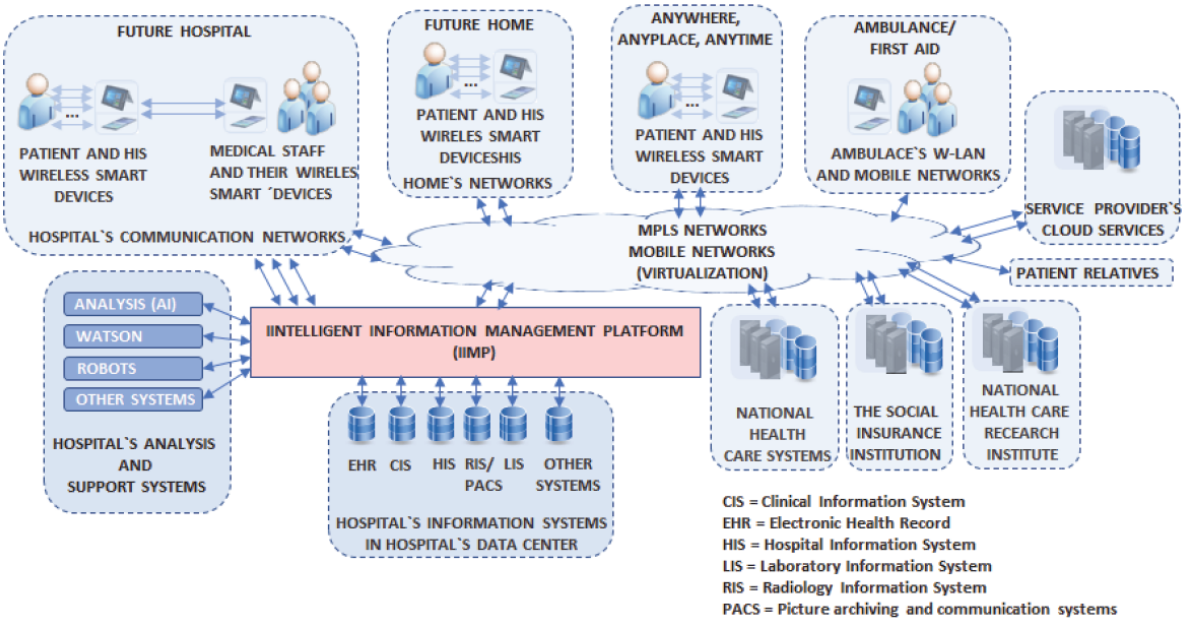

Figure 1: eHealth operating environment (Hummelholm, 2019)

SHAPES leverages the outcomes of an open interoperability framework (symbIoT, 2018) that empowers the interconnection of different IoT-based platforms, devices, digital solutions and services. symbIoT middleware supports controlled and secure exchange of information, sharing of resources and best practices and delivering of services to third-parties, thus enabling the building of a true ecosystem of digital solutions and services that may be selected and tailored to the specific individuals' needs, interests and contextual environment, fostering SHAPES' large-scale pan-European deployment and market scale-up. symbIoTe including open software development kits and application programming interfaces provides an interoperable mediation framework that enables the discovery and sharing of connected devices across existing and future IoT-platforms for development of cross-platform IoT-applications.

3. Authentication and Security Assessment as a Service in SHAPES

SHAPES manages a high degree of sensitive information pertaining to older individuals thus it is critical that high standards for security and privacy (fully adopting GDPR) are implemented, resulting in a trusted platform among its users and stakeholders. User authentication considers mechanisms that are seamless, noticing that seniors may lack technological skills or have unreliable memory to recall strong passwords. So, SHAPES implements user authentication mechanisms based on Multimodal Biometrics using several physiological or behavioural human characteristic for enrolment, verification, authentication or identification. SHAPES demonstrates capabilities (face recognition and fingerprint) applying multi-factor authentication in a seamless way. Concerning device and component authentication, SHAPES brings a twofold approach:

1. SHAPES implements an authentication mechanism that is able to take into consideration state-of-the-art protocols (end-to-end encryption, PKI, web-based using secure API call and token-based authentication) and IoT-friendly lightweight protocols, such as the Constrained Application Protocol (CoAP) for message exchanges. Most IoT-devices allow re-use of existing Enrolment over Secure Transport (EST) functionality for energy-efficient certification management and secure bootstrapping operations.
2. SHAPES implements a state-of-the-art authentication mechanism based on secure stateless tokens 'Paseto' (Platform-Agnostic SEcurity Tokens) that enables a distributed mechanism for token-based authentication achieving inter-module authentication.

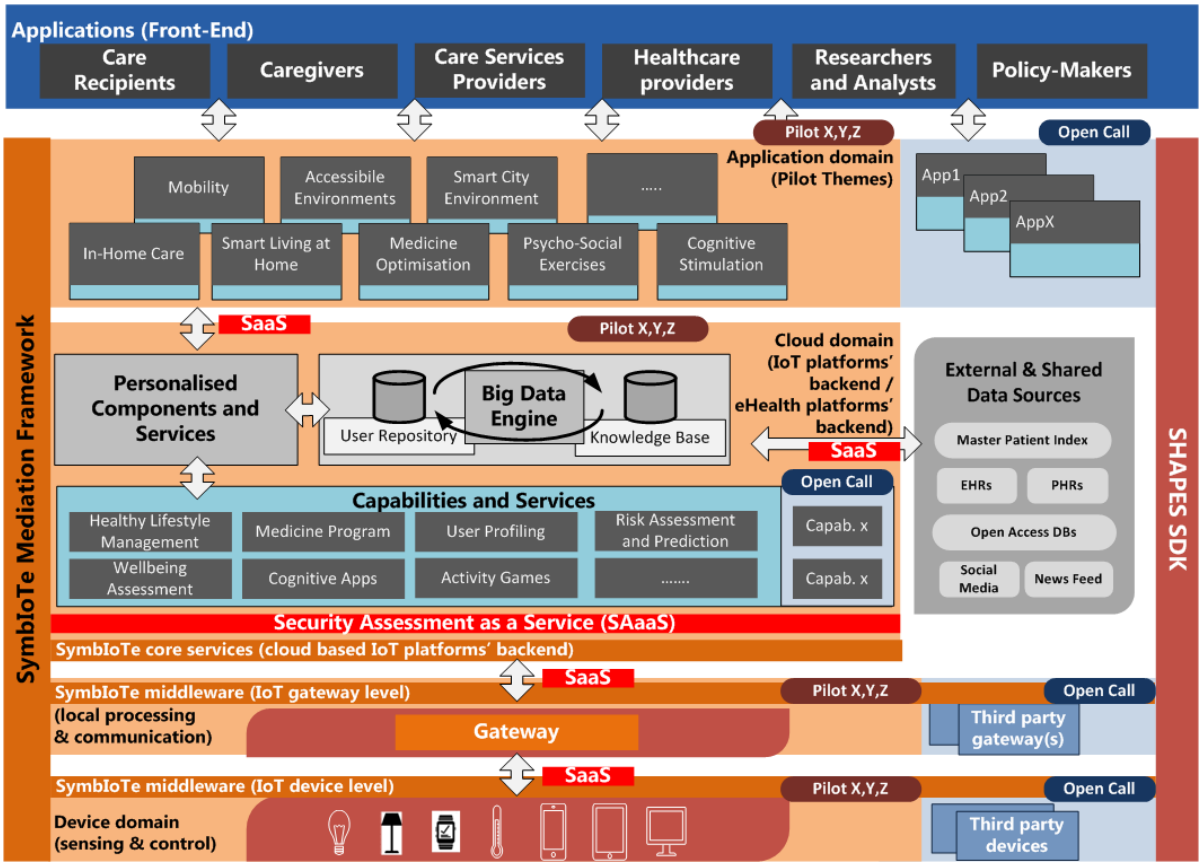

Figure 2: SHAPES high level architecture (SHAPES, 2019)

Considering the likelihood of operating in a not secured environment, SHAPES creates over-the-top secure environment (Virtual Local Area Network) enforcing security best practices. Moreover, it integrates a Security Assessment as a Service (SAaaS) cross-layered system to dynamically detect any existing and newly introduced network device, perform vulnerability assessments, certify the device against a standardised CVSS, assign it to a connectivity-appropriate VLAN and authenticate the service or device. Figure 2 presents SHAPES' high-level diagram.

4. Empowering

Health literacy, technology and individual involvement in care make healthcare more user-friendly and empowering, meaning that citizens (including seniors) must be seen as custodians of their own health (International Alliance of Patients' Organisations, 2014). Citizens continue to take a more central role in decisions about their own healthcare, and new technologies enable and facilitate this trend. New patients are evolving, similar to retail consumers. These former patients – new healthcare consumers – are driven by desire to take control over own health records and want to take active part in choosing healthcare providers and services. They are driven by the desire for more trustworthy, secure and timely healthcare information. Due to this changing role of patients, their empowerment has become a key priority for policy makers, professionals and service providers. Citizens' role is transforming from passive receivers of healthcare to active decision-makers; and managing own health data. Security is important aspect to empowering and creating the trust (Lettieri, et al., 2015).

As an example, activity-trackers enable to collect data from individuals' physical activities and health. A qualitative study (Lehto & Lehto, 2017) regarding the user perception on the privacy and sensitivity of health information collected with activity-tracker explored the user perception on health information sensitivity in general, and their willing, ness to share such information to other parties. Privacy calculus model (Laufer & Wolfe, 1977; Dinev & Hart, 2006) was the theory throughout the study. Table 1 summarize the results. Individuals do not perceive the information collected by activity-trackers as private or sensitive. But, information in medical records is considered to be very sensitive and private, as they include text written by doctors about procedures and discussions that are considered to be the most sensitive type of information.

Table 1: Research findings from activity tracker users' study (Lehto & Lehto, 2017)

Perceived privacy risks	**Perceived privacy concerns**	**Willingness to provide personal health data**
Information stolen	Being tracked or followed	Not on social media
Information lost	Banks deny loan applications	For medical research
Information misused	Employers won't hire	For healthcare purposes
Information goes to third parties	Insurance companies deny payments	For improving wearable products and services
Unauthorized access to the information	Information used for marketing	For occupational health services

The study extends earlier study information by presenting a new context to utilize the Privacy Calculus theory. The study's benefit is knowledge that activity-trackers users are ready to share their information that can be utilized in research and development of public services.

5. Cross-border Healthcare

The EU Directive on the Application of Patients' Rights in Cross-Border Healthcare is a starting point, delivering a legal framework for individuals willing to gain greater access to information related to healthcare available across Europe. However, in order to secure above-mentioned rights and unleash the potential of cross-border healthcare exchange, new solutions are needed to secure the storage and cross-border exchange of health data.

SHAPES cross-border implementation will be in line with modular strategy and related specifications and initiatives of epSOS (Smart Open Services for European Patients) project. In addition to the epSOS, the related and furthered projects are:

1. OpenNCP (Open Source Components for National Contact Points) as base realization starting point for SHAPES which includes a novel framework to foster cross-border eHealth services and which is base into the epSOS specifications;
2. current DECIPHER project which creates a mobile health care solutions and enables secure cross-border access to existing patient healthcare portals; and
3. STORK (Secure idenTity acrOss borders linked) which establishes a European eID Interoperability Platform that will enable citizens and businesses to use their national electronic identities in any participant Member State for public eGovernment services.

The designed contribution is that SHAPES can improve security and resiliency elements to related mechanisms and transactions, which are already established in the related projects.

Based on technological, integration and system readiness levels (Pirinen, 2015), SHAPES should develop new security readiness level (SecRL) metrics that supports the development of European operational standards for secure cross-border data exchange and patient privacy protection. Based on these metrics and prior open-source solutions (such as the OpenNCP suite (OpenNCP, 2015)), SHAPES could realise secure node platforms and components that enables the secure sharing and exchange of eHealth related data among countries.

6. Discussion

The rights of ageing individuals and their ability to live a good life at home or in a home-like environment are at the heart of the services designed in the SHAPES project. Privacy and security competence play a key role in the project, from planning to implementation and assessment. However, according to an ongoing Horizon 2020 cybersecurity project, health care sector can be identified as the most far from the ideal cybersecurity situation (ECHO, 2019).

The future complex environments present many challenges because the standards are not yet set at the international level. IoT products and sensors are mainly used at proprietary-based standards and getting them work at the same platforms in the smart devices will be a really big challenge.

Acknowledgements

This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 857159.

References

Dinev, T. & Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), pp. 61-80.

ECHO, 2019. Health Care Sector. [Online] Available at https://www.youtube.com/watch?v=X9ViO1w_9ko

European Commission, 2019. Smart and healthy ageing through people engaging in supportive systems. [Online] Available at: https://cordis.europa.eu/project/id/857159

Eurostat, 2018. Sustainable development in the European Union: Monitoring report on progress towards the SDGs in an EU Context, European Union.

Hummelholm, A., 2019. E-health systems in digital environments. 18th European Conference on Cyber Warfare and Security, pp. 641-649.

International Alliance of Patients' Organisations, 2014. Patient empowerment: for better quality, more sustainable health services globally, London: All Party Parliamentary Group.

Laufer, R. S. & Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of social Issues, 33(3), pp. 22-42.

Lehto, Miikael & Lehto Martti, 2017. Health information privacy of activity trackers. 16th European Conference on Cyber Warfare and Security, pp. 243-251.

Lettieri, E. et al., 2015. Empowering patients through eHealth: a case report of a pan-European project. BMC Health Serv Res, 15(309).

OpenNCP, 2015. OpenNCP Installation. [Online] Available at: https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Installation

Pirinen, R., 2015. Towards common information sharing: Study of integration readiness levels. 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 355-364.

SHAPES, 2019. Grant Agreement ID: 857159. European Commission.

symbIoT, 2018. symbIoTe project. [Online] Available at: https://www.symbiote-h2020.eu/