SOTER

Cybersecurity Optimization and Training for Enhanced Resilience in Finance

D2.3 – PIA+ Report (I)

[WP2 – General cybersecurity aspects. Human factor as internal threats]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Lead Contributor	Robin Renwick (TRI)
	robin.renwick@trilateralresearch.com
Other Contributors	Alan Mackenna (TRI)
	Charlotte Kelly (InAuth)
	James Palmer (InAuth)
	Alexa Mackenzie (TRUNOMI)
	Shawn Brown (TRUNOMI)
	Kartik Venkatesh (TRUNOMI)
	José Manuel Panizo Plaza (FNMT)
	Manuel Abiega Vizcaya (EVERIS)
	Miren Karmele Garcia Garcia (EVERIS)
	Laura Rodríguez Carlos-Roca (EADS)
	Su Anson (TRI IE) [Internal Review]
	Paul Rabel (UNIGRAZ) [External Review]

Due Date	31.08.2020
Delivery Date	31.08.2020
Type	Report
Dissemination level	PU = Public

Keywords	SOTER, cybersecurity, privacy, data protection, impact assessment, ethics, privacy by design, societal concerns

Document History

Version	Date	Description	Reason for Change	Distribution
V01r01	23.03.2020	Draft	NA	23.03.2020
V01r02	21.05.2020	Revision	TRI IE added contributions	21.05.2020
V01r03	10.06.2020	Revision	TRI IE change of structure	10.06.2020
V01r04	24.06.2020	Revision	Contributions added by TRI IE	24.06.2020
V01r05	01.07.2020	Revision	Contributions added by TRI IE	01.07.2020
V01r06	17.07.2020	Revision	Contributions by InAuth and EADS	17.07.2020
V01r07	28.07.2020	Revision	Contributions by EVERIS and TRUNOMI	28.07.2020
V01r08	07.08.2020	Revision	Contributions by FNMT and TRI IE	07.08.2020
V01r09	16.08.2020	Revision	Contributions by TRI IE	16.08.2020
V01r10	19.08.2020	Revision	Contributions by TRI IE	19.08.2020
V01r11	20.08.2020	Review	Sent for internal review (TRI IE)	20.08.2020
V01r12	25.08.2020	Revision	Integrated internal review (TRI IE)	25.08.2020
V01r13	28.08.2020	Review	Sent for external review (UNIGRAZ)	29.08.2020
V01r14	31.08.2020	Revision	Integrated external review	31.08.2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

V02r00	31.08.2020	Final Version	V02	31.08.2020
V02r01	04.11.2020	Review	Integrating comments from InAuth and TRUNOMI	04.11.2020
V02r02	12.11.2020	Revision	Preparation of Public Version	12.11.2020
V02r03	12.11.2020	Consensus	Request from beneficiaries for consensus	12.11.2020
V02r04	xx.11.2020	Public Version	Public Submission	xx.11.2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Abstract

This deliverable represents the Public Summary of a document entitled D2.3 – PIA+ Report (I). It provides a Public Summary of work undertaken so far, as part of the Privacy Impact Assessment and Privacy-by-Design task (T2.3] within the SOTER project, Grant Agreement No.833923. It provides the Public Summary of the operationalisation of Privacy-by-Design methodology, and complementary Privacy Impact Assessment reporting for the SOTER project. The process considers privacy, ethical, legal, and societal concerns. The document also provides an outline of the identification and mitigation of risk moving forward. It should be seen as a monitoring tool used to demonstrate necessity, proportionality, accountability and transparency in the operationalisation of Privacy-by-Design in the development of the SOTER technology. The SOTER technology is a biometric identification and authentication digital onboarding platform intended for deployment into the financial services sector. The Public Summary is a redacted version of D2.3 – PIA+ Report (I), which was submitted to the European Commission in M12 [August 2020] of the SOTER project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Public Summary

SOTER is a European Commission H2020 funded project, entitled *'cyberSecurity Optimization and Training for Enhanced Resilience in finance'* (SOTER). This deliverable is part of requirements agreed with the European Commission, with respect to Grant Agreement No.833923. The document is the Public Summary of the deliverable *entitled D2.3 - PIA+ Report (I)*, which was submitted to the European Commission in August 2020 [M12]. The Public Summary is a redacted version of *D2.3 – PIA+ Report (I)*. It has been redacted due to legal concerns.

The methodology implemented over the SOTER project lifecycle is based on ISO/IEC 29314:2017, an international standard developed by the International Standards Organisation (ISO). The method is supplemented by Privacy Impact Assessment guidance from organisations such as the United Kingdom's Information Commissioner's Office (ICO), and France's Commission Nationale de l'Informatique et des Libertés.

This document **does not constitute the formal legal requirements of a Data Protection Impact Assessment (DPIA)** for the Digital Onboarding Platform, but may be used to demonstrate that efforts have been taken by the SOTER consortium towards achieving that legal requirement, as laid out in Art.35 of the GDPR.

The above process considers risks associated with nine types of privacy. Seven of these are laid out within ISO/IEC 29314:2017 (bodily privacy, communicational privacy, location and space privacy, behavioural privacy, privacy of data and image, privacy of thoughts and feelings, privacy of association). It is further supplemented by identification of risks concerning financial privacy and transactional privacy, which is especially important given the context of use.

There are six core components of the SOTER platform:

- EVERIS Mobile Application and API Hub
- InAuth Device Fingerprinting and Malware Detection
- Trunomi Consent and Permissions Management Platform
- EADS Document Verification and Biometric-based Identification
- FNMT Trust Service Provider Services and Technologies
- EVERIS and ALASTRIA Blockchain Technologies

This PIA+ process has so far identified 27 privacy and data processing related risks from analysis of the SOTER technologies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

There are also 4 risks identified from a high level overview of legal considerations for the SOTER platform. This entails formal outline of the lawful basis for processing of data, and the legal obligations of parties involved in the processing, and the proposed impacts this shall have on the individual or data subject as they engage with the SOTER platform. The risks are summarised as:

- The data controllers and processor relationships are undefined for the SOTER platform
- It is unclear what the correct level of legislative balance for the SOTER platform is
- It is not clear if AES is the correct level of signatory assurance required for the SOTER platform
- There is potential that the SOTER platform will not interoperate with EC initiatives regarding digital identity such as EBSI and ESSIF

The process has also outlined the ethical and social considerations of the SOTER platform, basing its analysis on ethical guidelines detailed by the Institute of Electrical and Electronics Engineers (IEEE), through their Global Initiative for Ethically Aligned Design. This section has identified 4 core ethical and societal risks:

- Well-being, Inclusion and Equality:
  - Regarding the mobile platform, its usability, and its accessibility for the vulnerable, elderly, or marginalized.
- Accountability, Transparency and Awareness of Misuse:
  - Concerning the data stored within the distributed ledger, and the governance agreement that legally binds the entities that have access to it (whether read or write access)
- Data Agency and Competency:
  - Surrounding control, access and security of the digital identity of the data subject, including their credentials, their interactions within the distributed ledger, and any transactions that are stored within the data structure
- Human Rights, Dignity, and Awareness of Misuse:
  - Concerning the levels of ‘safeness’ of the methods and protocols used to share information within the data structure, and applicable parties

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- especially as they relate to the balance of power between citizen, state, and corporation, including the potential harms that may befall the individual if the SOTER platform were to be deployed.

The proposed plan moving forward is an iterative PIA+ and Privacy-by-Design process led by Trilateral Research Ireland.

Trilateral Research Ireland have also created a PIA+ Issue Tracker, which will be used to demonstrate accountability and transparency regarding the Privacy-by-Design methodology, as well as details regarding the PIA+ Workshop and the Stakeholder Consultation tasks - viewed as key steps in realising the successful integration of the risks and recommendations into specific user-requirements.

The second formal deliverable within *T2.3 - Privacy Impact Assessment and Privacy-by-Design* will be delivered to the European Commission in M27 (September 2021).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.