D5.3 Trust and security software components – v1

Grant Agreement nr	856879
Project acronym	PRESENT
Project start date (duration)	September 1st 2018 (36 months)
Document due:	February 28th 2021
Actual delivery date	March 3rd 2021
Leader	ICERT
Reply to	roberto.deprisco@etuitus.it
Document status	Submission Version

Project funded by H2020 from the European Commission

Project ref. no.	856879
Project acronym	PRESENT
Project full title	**P**hotoreal **RE**altime **S**entient **ENT**ity
Document name	Trust and security infrastructure design
Security (distribution level)	Confidential
Contractual date of delivery	February 28th 2021
Actual date of delivery	March 3rd 2021
Deliverable name	D5.3 Trust and security software components – v1
Type	Report
Status & version	Submission Version
Number of pages	35
WP / Task responsible	ICERT
Other contributors	eTuitus
Author(s)	Roberto De Prisco
EC Project Officer	Ms. Adelina Cornelia DINU - Adelina-Cornelia.DINU@ec.europa.eu
Abstract	This document provides details about the implementation of the security module of PRESENT. Detailed explanations about the tools used to implement it and descriptions about the different capabilities and functionalities of the module are provided. The design of the security module is described in Deliverable 5.2 which should be read before reading this document. Deliverable 5.1 also is relevant since it discusses the general approach that we use to manage verifiable credentials in a distributed setting.
Keywords	Security module, authentication, registration.

Sent to peer reviewer	Yes
Peer review completed	Yes
Circulated to partners	No
Read by partners	No
Mgt. Board approval	No

Document History

Version and date	**Reason for Change**
0.0 20-01-2021	Document created by ICERT/eTuitus
1.0	Version for internal review
2.0	Submission Version

Table of Contents

1. EXECUTIVE SUMMARY 5

2. INTRODUCTION 6

3. TECHNOLOGIES 10

4. SOFTWARE COMPONENTS 12

4.1 Open source components 13

4.2 Code being developed 17

5. THE FLOW OF INTERACTIONS 17

5.1 Initial authentication 18

5.2 Optional subsequent authentications 20

6. SECURITY CREDENTIAL CONTROLLER 21

7. VIRTUAL AGENT CLOUD WALLET 23

8. USER WALLET APP 23

8.1 Wallet app 23

8.2 Flutter 24

8.3 App features 24

8.4 App design 25

9. BIOMETRIC MODULE 29

10. REST API Gateway 30

10.1 REST API Gateway 30

10.2 Authentication invite (first authentication, with wallet access) 32

10.3 Authentication check (optional subsequent authentications, no wallet access) 32

10.4 Authentication result 33

11. CONCLUSION 34

12. REFERENCES 35

1. EXECUTIVE SUMMARY

PRESENT is a three-year EU Research and Innovation project involving 8 companies and research institutions that are collaborating to create virtual digital humans (virtual agents) that look entirely naturalistic, demonstrate emotional sensitivity, establish an engaging dialogue, add sense to the experience, and act as trustworthy guardians and guides in the interfaces for AR, VR, and more traditional forms of media. These virtual agents can be used for interaction with human users in several scenarios.

The project includes a security component whose goal is that of authenticating the parties. Human users are equipped with digital identities (basically a digital identity card) and can use such identities to prove who they are through a face recognition authentication that compares the face of the user with the face stored in the digital identity card.

The design of the security module has been described in deliverable D5.2 *Trust and security infrastructure design*. The key technology that is used to implement the module is the Sovrin Blockchain, which allows us to handle credentials (digital identities) in a decentralized manner. The motivations for the use of the Sovrin framework have been discussed in the deliverable D5.1 *Blockchain Privacy Report*.

Among the features exposed by the security module, there are the release and verification of credentials that will allow users to be registered and virtual agents to authenticate users by validating their credentials.

To allow easy integration of the secure module functions, all services will be accessible via a REST API. This document provides all the necessary details about the REST services offered by the security module and about their integration with other components of the system.

The document also describes the current status of the implementation (version 1).

2. INTRODUCTION

The security module of the PRESENT project allows mutual authentication of the parties involved which can be the virtual characters of PRESENT (called virtual agents) and the users (human) of the service offered through the PRESENT infrastructure. Deliverable D5.1 *Blockchain Privacy Report*, has discussed the general strategy to manage digital identities in distributed settings such as the ones envisioned by the PRESENT project. Deliverable D5.2 *Trust and security infrastructure design* has provided the overall design of the security module. These documents should be read before reading this one; however, all the necessary information is summarized in this document. This document, proceeding in the path paved in D5.1 and D5.2, provides details about the implementation strategy and about the current status of the software development (version 1). Deliverable D2.2 *First Report on Modular Architecture*, Protocols and APIs, provides a description of the overall system. Figure 1 embeds an updated description of the security module into the overall picture outlined in Deliverable D2.2.