D5.2 Trust and security infrastructure design

Grant Agreement nr	856879
Project acronym	PRESENT
Project start date (duration)	September 1st 2018 (36 months)
Document due:	August 31st 2020
Actual delivery date	August 7th 2020
Leader	UPF
Reply to	vanesa.daza@upf.edu
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	August 31st 2020
Actual date of delivery	August 7th 2020
Deliverable name	D5.2 Trust and security infrastructure design
Type	Report
Status & version	Submission Version
Number of pages	15
WP / Task responsible	UPF
Other contributors	InfoCert
Author(s)	Vanesa Daza, Sergi Rovira
EC Project Officer	Ms. Adelina Cornelia DINU - Adelina-Cornelia.DINU@ec.europa.eu
Abstract	This document details the infrastructure design 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.
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 02-07-2020	Document created by UPF
1.0 31-07-2020	Version for internal review
2.0 07-08-2020	Submission Version

Table of Contents

1 EXECUTIVE SUMMARY

PRESENT is a three-year EU Research and Innovation project between 8 companies and research institutions to create virtual digital humans (sentient 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.

This document details the infrastructure design of the security module of PRESENT. We explain the tools used to implement it and provide descriptions about the different capabilities and functionalities of the module.

The main idea behind the security module is to use virtual identities to identify the parties interacting with the system. The design goal is to build a highly dynamic and decentralized system that allows the participants to be in control of their credentials.

There are two types of parties that can participate in the system: users and virtual agents. Both types will have verifiable credentials which will be used to validate their identity. For example, we will use name, surname and a front-facing image as part of the credential forming the identity of a user. Once the identity of a party is created, the security module will make use of different cryptographic tools and facial recognition to validate it.

The key technology that is used to implement the module is the Blockchain, which allow us to handle credentials in a decentralized manner. A description of this fundamental tool is out of the scope of this document and has been given in deliverable *D5.1 Blockchain Privacy Report.*

The security module can perform two functions. The first one is to register the credentials of the parties and the second one is to validate their identity from those credentials. All the other modules of the project will have access to these functionalities via a REST API.