TagItSmart!
Smart Tags driven service platform for enabling ecosystems of connected objects

Grant agreement 688061

TagItSecure!
Dissemination and Evaluation Report

Deliverable ID:	**D 3.1**
Deliverable Title:	TagItSecure! Dissemination and Evaluation Report
Revision #:	**1**
Dissemination Level:	**Public/Confidential**
Responsible beneficiary:	FINCONS GROUP AG
Contributing beneficiaries:	FINCONS GROUP AG
Contractual date of delivery:	29/06/2018
Actual submission date:	25/07/2018
Start Date of the Sub-Project	01/02/2018
Duration:	5 Months
Reviewer 1	
Reviewer 2	

PROPRIETARY RIGHTS STATEMENT
This document contains information, which is proprietary to the TagItSmart! Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the TagItSmart! consortium.

Contents

List of tables 2

List of pictures 2

Section 1 - Introduction 4

Section 2 - Demonstration 5

2.1 Validation Results 10

2.2 KPIs evaluation result 10

Section 3 - Dissemination 12

Section 4 - Exploitation 13

Section 5 - Conclusion 14

Section 6 - Glossary 15

List of tables

Table 1: Results of the execution of the validation cases 10

Table 2: Summary of KPIs 11

List of pictures

Figure 1: Each of the stickers above (available at https://ibd-aws.finconsgroup.com:8080/TagItSecureKGS/stickers) provides QR code and NFC tag associated to a sensor of the publisher device and enables the TagItSecure! app to fetch the measures posted by that specific sensor to the TagItSmart! platform 5

Figure 2: The app asks the user to register on the website for the generation of the private key, necessary to decrypt the data fetched from TagItSmart platform, that will be stored on the mobile device as a configuration parameter, in such a way to have the key under the direct control and responsibility of the users. 6

Figure 3: according to the sticker scanned, the user is displayed, upon the indication of the period of interests, the measures produced by the associated sensor 7

Figure 4: The EVRYTHNG console that allows inspecting the 'THNGs' stored 8

Figure 5: TagItSecure! overall picture 9

PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the TagItSmart! Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the TagItSmart! consortium.

Document history

Revision	Date	Modification	Authors
1	05/07/18	First draft version	FINCONS AG
2	06/07/18	Internal review	FINCONS AG
3	25/07/18	Internal approval of graphic items	FINCONS AG

Section 1 - Introduction

This document has been produced as output of the WP 3, *Evaluation, Dissemination and Exploitation*, with the objective to evaluate the project results and outline possible exploitation strategy and further extensions, as well as reporting about the dissemination activities carried out in the frame of the project.

The present deliverable (D3.1), therefore, is structured as follows:

- Section 1 introduces the document
- Section 2 reports about the demonstration and validation activities performed with the prototype implemented and includes the conclusive evaluation of the related KPIs.
- Section 3 reports about the dissemination activities done
- Section 4 describes the worthwhile further extensions of the solution and outlines a possible exploitation strategy
- Section 5 draws the conclusions
- Section 6 is the glossary

Section 2 - Demonstration

The demonstration of the project achievements has been done focusing on the use case related to the protected management of information related to the monitoring of environment parameters collected by sensors deployed at the FINCONS's Bari office.

To enable the demonstration, a mobile Android application acting as a SmartTag reader has been developed. The SmartTags have been associated to specific sensors (i.e. temperature, humidity and presence) managed by a Raspberry Pi III board in the FINCONS's Bari premise that publishes, using the *TagItSecure!* Security features, the sensors' measures on the *TagItSmart!* platform.

For each sensor a sticker (see Figure 1) has been designed and produced. Scanning the sticker's QR Code or NFC tag, the app will fetch from the *TagItSmart!* Virtual Entity Database the data associated to the selected sensor and will display those data if the Android app's CP-ABE key is in line with the access policy with which the sensor's measures have been encrypted.

Figure 1: Each of the stickers above (available at https://ibd-aws.finconsgroup.com:8080/TagItSecureKGS/stickers) provides QR code and NFC tag associated to a sensor of the publisher device and enables the TagItSecure! app to fetch the measures posted by that specific sensor to the TagItSmart! platform

The demonstration includes the following steps:

- The user scans the sticker of interest using any QR code or NFC tag reader with an Android smartphone (the NFC tags are only available on the stickers deployed at the FINCONS office, so, for a remote user it is necessary to scan the QR code).
- The reading of the QR / NFC code activates the TagItSecure! app; if the app is not already installed, the smartphone automatically pulls it down from Google Play, installs it (asking necessary permissions to the user) and activates it.
- In case of first activation, the TagItSecure! app invites the user to go to its web site (https://ibd-aws.finconsgroup.com:8080/TagItSecureKGS/) to generate a personal CP-ABE key.
- The generation of the CP-ABE personal key at the URL above requires the user to: (a) register by setting a password associated to the username (of the type "User001", "User002", etc.) automatically generated by the system, (b) login with the newly created

account, (c) ask for the key generation, (d) copy the key to the clipboard and (e) pasting it to the Android app by using the *Copy from Clipboard* button (see Figure 2).

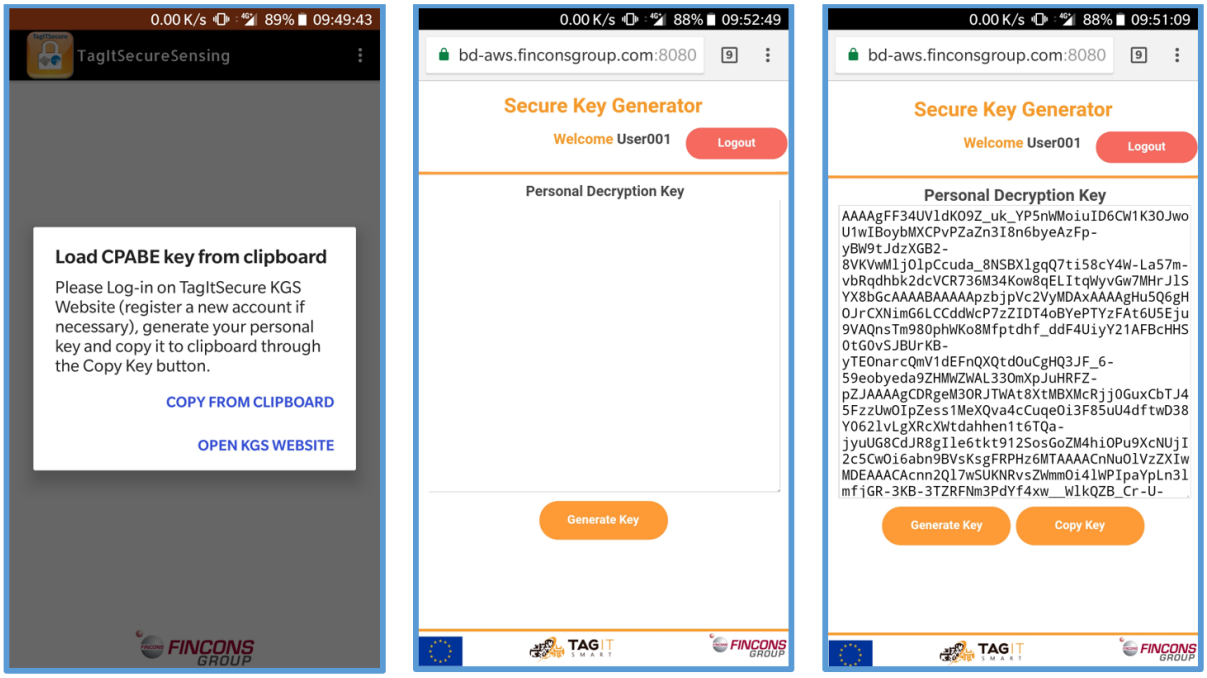

Figure 2: The app asks the user to register on the website for the generation of the private key, necessary to decrypt the data fetched from TagItSmart platform, that will be stored on the mobile device as a configuration parameter, in such a way to have the key under the direct control and responsibility of the users.

- Once the app is activated, it fetches from TagItSmart! (i.e. from the Everything Virtual Entity DB) the measures produced by the sensor identified by the sticker in the timeframe specified by the user (see Figure 3).

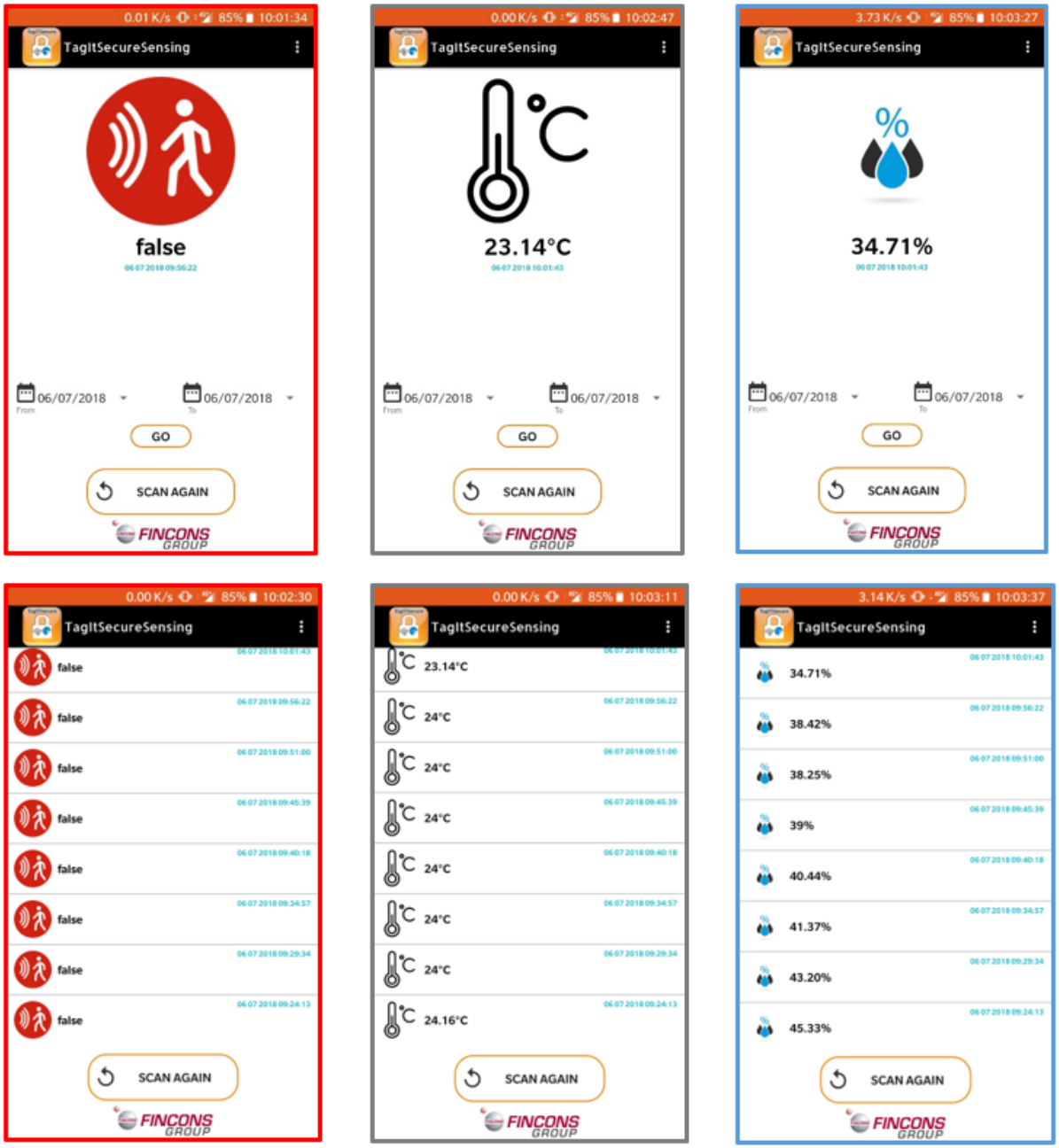

Figure 3: according to the sticker scanned, the user is displayed, upon the indication of the period of interests, the measures produced by the associated sensor

The following TIS components, as envisaged and described in D1.1, have been used for the demonstration implementation (see Figure 5):

- **Stream Processing:** it is a Message Broker responsible to handle messages published / consumed by SeDEM clients in accordance to the MQTT protocol

- **Virtual Entity Database:** is the repository (EVRYTHNG database) where encrypted messages published by SeDEM clients are stored (see Figure 4) in order to be consumed by the Android App after scanning the SmartTag (tag that will provide to the App the sensor identifier in order to use it as key for the database query). The THNG configured for TagItSecure! includes the different measures published at a given time by the Data Source device as different properties. In the case of the Raspberry, in fact, the presence, humidity and temperature measures are three different properties.

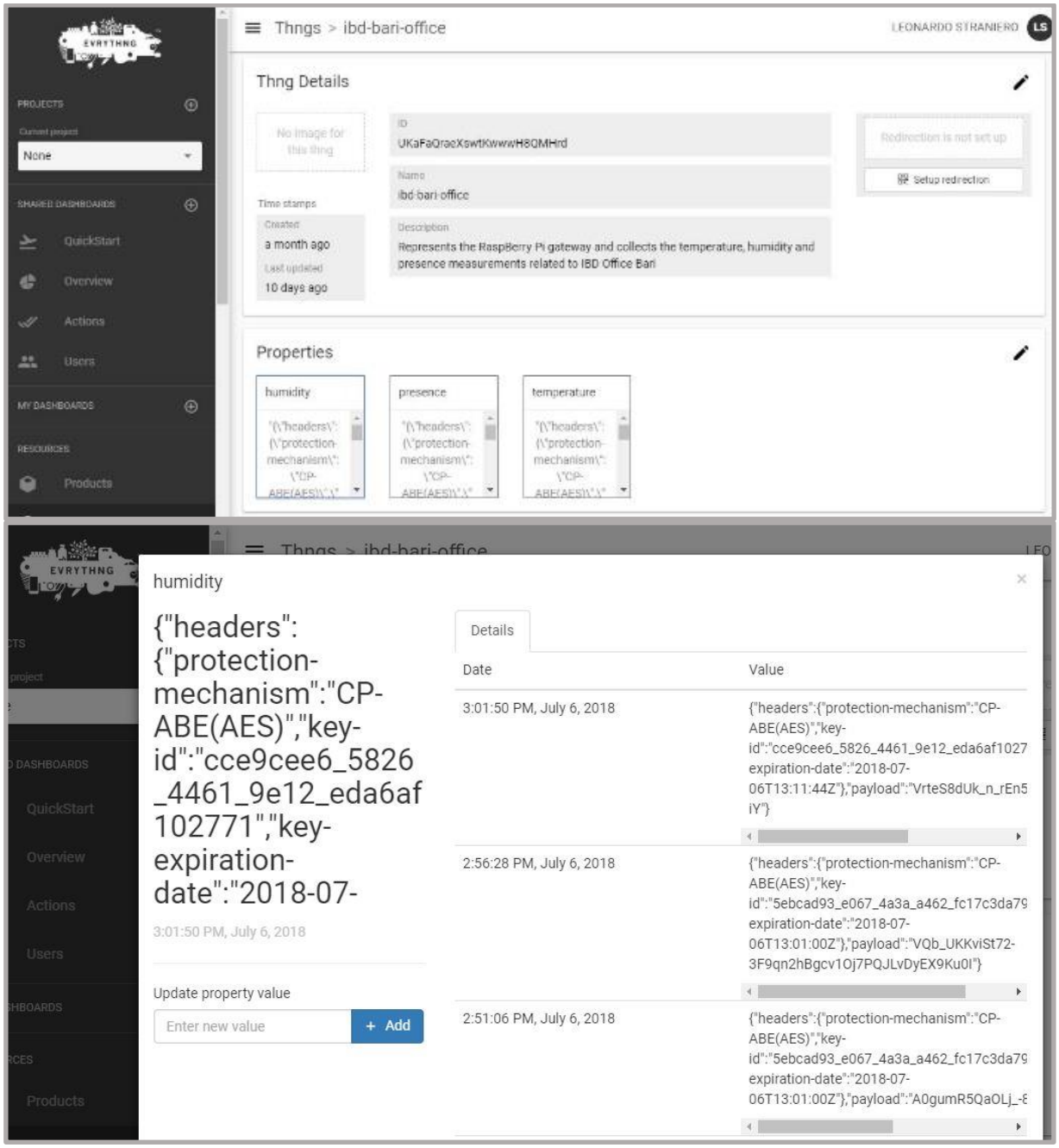

Figure 4: The EVRYTHNG console that allows inspecting the 'THNGs' stored

It was not possible, instead, to evaluate the feasibility of executing a similar demonstration with the FC-Scanner application, due to the lack of information necessary to integrate the TagItSecure! client components in it. A similar scenario will be considered, therefore, for the post project exploitation phase.

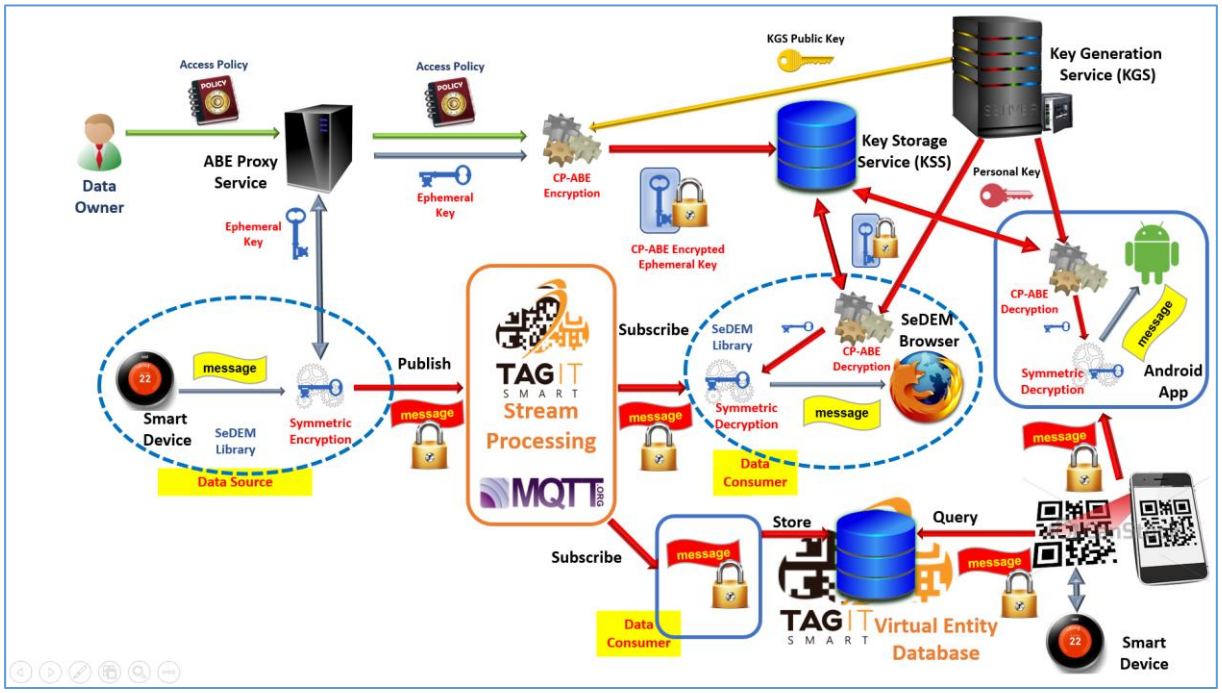

Figure 5: TagItSecure! overall picture

2.1 Validation Results

This section provides indication of the execution of the demonstration cases that addressing the main functional aspects of the component and selected as validation scenarios in D1.1.

Table 1: Results of the execution of the validation cases

Validation Scenario	Successful execution	Notes
Possibility to define access policies based on the users' profile (attributes)	YES	For the implementation of the demonstration the access policies have been defined off-line with the policy management tool and configured at the Data Source side (see Figure 5) in order to protect accordingly the generated data
Possibility to encrypt data-stream with a policy chosen according to the data access requirements	YES	Data access requirements for the demonstration case have been set in order to as wide as possible (the profile of all the users proposed by the web site at registration time include attributes that match the policy used for the encryption of data stream). However, it is easy to enable selective access to the data generated: it is sufficient to change the access policy configured on the Data Source device, and to modify accordingly the attributes of one of the users: from that moment on just that user will access the data.
Successful decryption of a data-stream for users whose attributes match the policy used in the encryption	YES	This is the basic case demonstrated as explained in Section 2 -
Acquisition of private key to be used by a publisher /subscriber for encryption / decryption operation	YES	In the demonstration scenario the acquisition of the private key has been implemented as a functionality of the web site; the private key is generated upon user login, on the basis of the user's attributes stored in the LDAP; it has then to be stored on the mobile app (see Figure 2) in order to enable the decryption of the data to which the user is authorized to access.
Unsuccessful decryption of a data stream for users whose attributes do not match the policy used in the encryption	YES	Being the private key copied to the mobile app generated on the basis of the users' attribute, in order to reproduce the case described in this validation scenario it is sufficient to modify it on the smartphone clipboard before using the *Copy from Clipboard* button.

2.2 KPIs evaluation result

The achievement of the project technical objectives has been measured through the evaluation of the KPIs identified in D1.1 and reported in the following table:

Table 2: Summary of KPIs

#	KPI name	Way of measurement	Goal	Achieved	Notes
1	**Increased level of security**	Number of security threats addressed	5	YES	Identified as: • CWE-319: Cleartext Transmission of Sensitive Information • CWE-312: Cleartext Storage of Sensitive Information • CWE-313: Cleartext Storage in a File or on Disk • CWE-315: Cleartext Storage of Sensitive Information in a Cookie • CWE-316: Cleartext Storage of Sensitive Information in Memory and referred to the validation scenario 2
2	**Enhancement of data protection functionalities**	Number of new test cases introduced (and passed) related to data protection issues	5	YES	The validation test cases described in 2.1
3	**Privacy impact**	Number of types of sensitive information protected against disclosure in the demonstration scenario (e.g., sensors' data like: presence sensor, room temperature, room lighting).	≥ 3	YES	**N.B.:** the actual number of data items protected using the TagItSecure! solution will be much higher being, for example, related to sensors' data acquired with continuity in a home/office environment
4	**User's roles**	Number of roles to demonstrate the capability of the proposed system to control access to protected information according to user's attributes and access policies	3	YES	Consumer: is enabled to access data streams if the access policy linked to those data matches with his profile Producer: is enabled to publish sensor data to the TagItSmart! platform encrypted according to a defined access policy Operator: is enabled to define access policy
5	**Involved users**	Number of users to which a personal CP-ABE key will be provided and which will be able to test the capability of the system to actually control accessibility to the protected information. The idea is to provide personal keys to both FINCONS people, as well as people identified by the TagITSmart project.	≥ 10	YES	**N.B.:** the number provided here is related to FINCONS people only! **NN.BB.:** being the sensor's stickers[1] and user registration service[2] accessible via internet and the Android app available through the Google Play service the number of involved users is much higher as can be easily checked registering as new user on the registration service

[1] https://ibd-aws.finconsgroup.com:8080/TagItSecureKGS/stickers
[2] https://ibd-aws.finconsgroup.com:8080/TagItSecureKGS/

Section 3 - Dissemination

The project results have been disseminated in the context of the workshop “IoT & Security Issues” that had place at Bari University, on the 9th May 2018.

The related presentation is accessible at the following URL https://drive.google.com/open?id=19oMCaeE99V52VGM9QkZdsfCMxSBlYYoY

A further dissemination activity has been done in the NEM-SB ECSO SWG3.8: Telecom, media and content workshop, held on 17th July, 2018 in Brussels.

The related presentation is accessible at the following URL https://drive.google.com/open?id=1lchN5es_0lh7b-NEhqMeXJbvV_eENvMo

Section 4 - Exploitation

The developments activities done in the context of the TagItSecure! project have been planned taking into account on the one hand the needs of demonstrating the benefits of the solution, on the other hand the limited temporal extension of the project and the consequent impossibility to deepen the analysis of some technical aspects and components of the TagItSmart! platform.

Therefore, some possible further developments of the solution have been identified as potential extension since the design phase of the project. In particular it is worth mentioning, as development activities that would clearly add value to the solution, the following ones:

- The integration of the client TagItSecure! components into the FC-Scanner application.
- The integration of the TagItSecure! user management functionalities into the TagItSmart! User Management component.

It is worth making evidence of the fact that the TagItSecure! features appear as absolutely complementary with respect to the security features linked to the usage of the FC-Scanner application and described in the TagItSmart! deliverable D3.2 "*Secure and reliable FC-scanner usage*", because the FC-Scanner does not address some issues tackled by TagItSecure!, i.e. the protection of data at transmission and storage level.

It has to be remarked, also, that thanks to the integration of the SeDEM module, the TIS ecosystem will be enabled to deal with any data without concerns about the potential privacy issues by which those data may be affected, and without risking to violate privacy regulations (as explained in section 2.2 of D1.1). With a full integration of the TagItSecure! module, thus, the TIS ecosystem could be also used as test-bed to support the certification of SmartTag-enabled applications as GDPR compliant, as this has recently become an essential requirement to be fulfilled by IoT solutions before their roll-out in production environment, and therefore, an essential condition for the marketability of a solution, beyond contributing to increase the level of trustiness in using the solution for the involved actors.

Section 5 - Conclusion

The present deliverable, D3.1, describes the demonstration activity performed by FINCONS AG to show the functionalities of the proposed module and how it was integrated within the TIS ecosystem. The demonstration is described step-by-step so that it is easy to follow its plot and to reproduce the related demonstration cases.

The document also describes how the validation scenarios have been implemented within the demonstration performed.

Being TagItSecure! a component that provides features related to the safe handling of sensitive information and confidential data in compliance with the GDPR directive, it has cross-use case validity, but of course is more valuable for those use cases that more than others imply the access to confidential data. It can be, therefore, of significant interest for other applications proposed in the frame of subsequent TIS calls, which might exploit the TagItSecure! functionalities, or, in general, for future developments done within the TIS ecosystem.

The document, in this perspective, indicates the developments suggested for the achievement of a smoother integration of the component in the TIS platform, and outlines possible exploitation scenarios.

Section 6 - Glossary

Term	Definition
ABE	Attribute Based Encryption
AES	Advanced Encryption Standard
CP-ABE	Ciphertext Policy Attribute Based Encryption
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
KPI	Key Performance Indicator
KGS	Key Generation Service
KSS	Key Storage Service
LDAP	Lightweight Directory Access Protocol
NFC	Near Field Communication
QR	Quick Response
RBAC	Role-Based Access Control
SeDEM	Secure Data Exchange Middleware
TIS	TagItSmart!
W3C	World Wide Web Consortium