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

Grant agreement 688061

TagItSecure! Reference Architecture

Deliverable ID:	**D 1.1**
Deliverable Title:	TagItSecure! Reference Architecture
Revision #:	**4**
Dissemination Level:	**Public/Confidential**
Responsible beneficiary:	FINCONS GROUP AG
Contributing beneficiaries:	
Contractual date of delivery:	31/03/2018
Actual submission date:	17/05/2018

Start Date of the Project: 1 January 2016 Duration: 36 Months

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 - State of the Art 5

Section 3 - System Architecture 6

3.1 TIS components used by TagItSecure! 9

3.2 Demonstration use cases 10

Section 4 - Validation Scenario 11

4.1 KPIs to be used for evaluation 13

Section 5 - Conclusion 14

Section 6 - References 15

Section 7 - Glossary 16

List of tables

Table 1: Summary of KPIs 13

List of pictures

Figure 1: CP-ABE encryption process 6
Figure 2: CP-ABE decryption process 7
Figure 3: SeDEM Architecture & Interactions 7
Figure 4: Tag & Android App Interactions 8
Figure 5: SeDEM Browser 9
Figure 6: TagItSecure! overall picture 10
Figure 7: Policy definition tool 12

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	19/04/18	First draft version	FINCONS AG
2	24/04/18	Internally reviewed version	FINCONS AG
3	10/05/18	Update after first TIS feedback	FINCONS AG
4	17/05/18	Further internal review after first TIS feedback	FINCONS AG

Section 1 - Introduction

This document has been produced as output of the task 1.1, *Analysis and Technical Specifications*, with the objective to analyse the TIS platform and to design the architecture and infrastructure of the SeDEM integration, as well as the validation scenarios, reviewing also the KPI to be used for evaluation.
The present deliverable (D1.1), therefore, is structured as follows:

- Section 1 introduces the work done
- Section 2 reports the state-of-the-art of technological solutions tackling data protection issues, explaining the advantages of the FINCONS solution
- Section 3 describes the system architecture, the components that will be deployed, the main interactions among them and the functionalities offered, providing indication of TIS components used (section 3.1) and use cases supported (section 3.2).
- Section 4 elaborates the validation scenarios and reviews the KPIs to be used for evaluation
- Section 5 summarizes the conclusions drawn
- Section 6 provides bibliographic references
- Section 7 is the glossary

Section 2 - State of the Art

In IoT scenarios significant amount of data is collected and, usually, moved to the cloud for being processed or stored. These data is often of personal or confidential nature and, therefore, needs to be properly protected. Personal data, in particular, is subject to be managed in compliance to the privacy laws and, specifically, to the EU GDPR [5].
IoT contexts are quite dynamic and therefore characterized by a potentially variable number of subjects (i.e., people, services, devices) in need to gain access to the collected data [8]. Additionally, also the data time span is usually not known in advance. Therefore, the confidentiality of collected data have to be guarantee for the whole data life cycle not for specific steps of the life cycle, as happens, for example, using TLS/SSL which guarantees confidentiality only while the data is being transferred via TLS/SSL sessions.

Traditional access control mechanisms like RBAC and ABAC presents many issues in IoT contexts [6] like: scalability, effectiveness and usability in consumers' contexts, relevant management effort, difficulties in enforcing *least privilege* access principle. At the same time, pure access control mechanisms do not guarantee confidentiality of data along the whole life cycle (e.g., on backups, on dismissed hard disks).

In these years the *security/privacy-by-design* and *security/privacy-by-default* design principles are gaining relevance [9] especially for IoT contexts; principles that are also mandated or recommended by regulations like: EU GDPR, EU Article 29 Data Protection Working Party [10] and the US FTC [11].
Traditional encryption mechanisms, like symmetric or asymmetric key cryptography [7], even if potentially in line with these design principles present issues like: keys distribution, keys sharing, keys revocation.

A novel asymmetric cryptographic approach, known as Attribute Based Encryption (ABE) [1] [12], allows encrypting the data on the basis of user-defined access policies stating the conditions a subject has to satisfy to succeed in decrypting the information. In ABE systems each subject has a personal key to be used for decrypting the information. Subject's personal keys are generated based on specific subject's attributes (e.g., user's profile), and the decryption process will succeed only if these attributes are in line with the conditions in the access policy.
Therefore, ABE systems do not require sharing or distributing keys.

Due to the ABE processing needs, a pure ABE approach is not suitable for IoT contexts with a high rate or with devices having resource constraints.

The solution proposed by FINCONS aims to demonstrate the benefits derived from the use of advanced cryptographic techniques based on Attribute-Based Encryption (ABE), testing them in a highly-distributed environment (like TagItSmart! is). Specifically, it puts into practice the application of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE, [1]) in combination with the AES symmetric encryption scheme in order to enable information to be shared while confidentiality is preserved, combining the flexibility and granularity of CP-ABE with the efficiency and speed of AES in order to provide a security component capable to support requirements of different ICT (and IoT) solutions and the related applicative scenarios [2] [13] [14] [15].
FINCONS's approach constitutes a significant innovation as compared to traditional approaches in assuring end-to-end data confidentiality, *security/privacy-by-design* and *security/privacy-by-default*, flexibility and speed.

Section 3 - System Architecture

Objective of the TagItSecure! project is to strengthen the overall security level of the TagItSmart! ecosystem by integrating a new module, the Secure Data Exchange Management (SeDEM), to enhance the platform with encryption features able to provide end-to-end data protection, especially for privacy-related or confidential data.
The SeDEM module is designed to support compliance with the Security-by-Design, Privacy-by-Design and Security-by-Default and Privacy-by-Default principles. Security/Privacy-by-Design means that a system is designed taking into account the security and confidential data management needs, so the security and privacy (i.e., proper management of confidential data) are an essential element of the system. Security/Privacy-by-Default means that the security design and default configuration of the system ensures a minimum level (which means an acceptable level which can be increased only) of security and privacy (i.e., confidential data management) that: (1) cannot be lowered, (2) is configured by default.
One of the most relevant features of the system is the end-to-end protection of confidential data using new CP-ABE techniques, which are asymmetric encryption schemes where: (1) explicit access policies are used to control the encryption of the information, (2) subjects have their own personal key, (3) personal keys are generated based on subject's attributes and (4) the decryption process succeeds only if those subject's attributes meet the access policy. The CP-ABE approach, therefore, avoids issues related to keys distribution, keys sharing, etc.

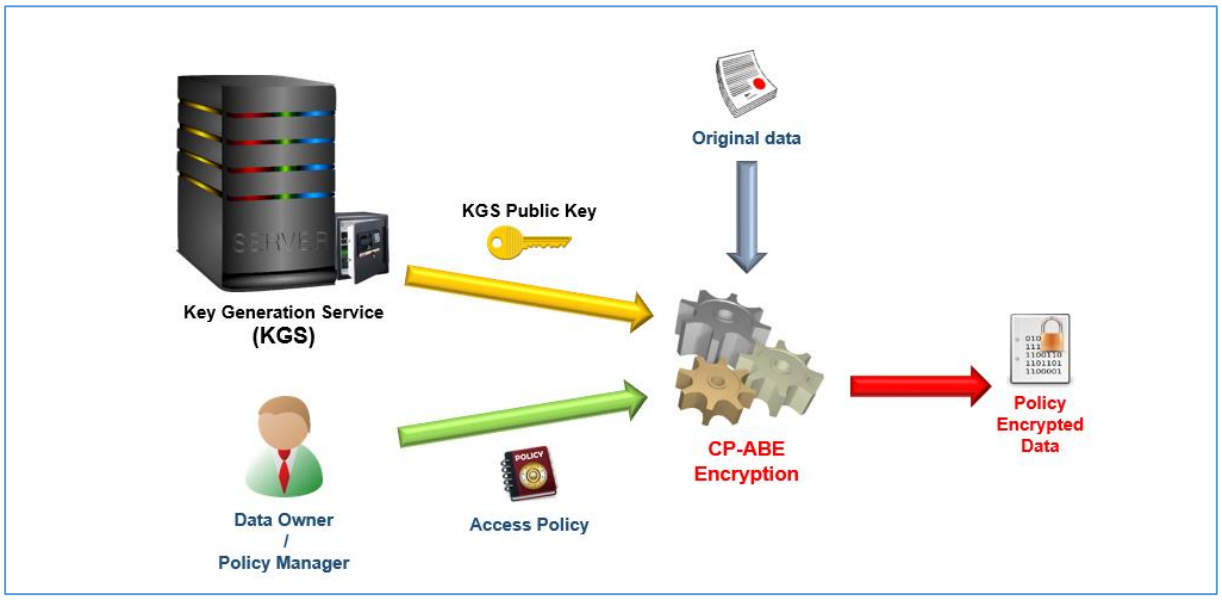

Figure 1: CP-ABE encryption process

The **Key Generation Service** is the entity responsible for generating CP-ABE private keys based on the attributes associated to the data consumer's profile. The ABE Key Generation Service at 1st start-up generates two keys: the *KGS public key* used to encrypt information in conjunction with an access policy (as shown in Figure 1), and a *KGS master key* used, on-request and in combination with the user's profile, to generate the user's *personal key*, used in the decryption process (as shown in Figure 2).

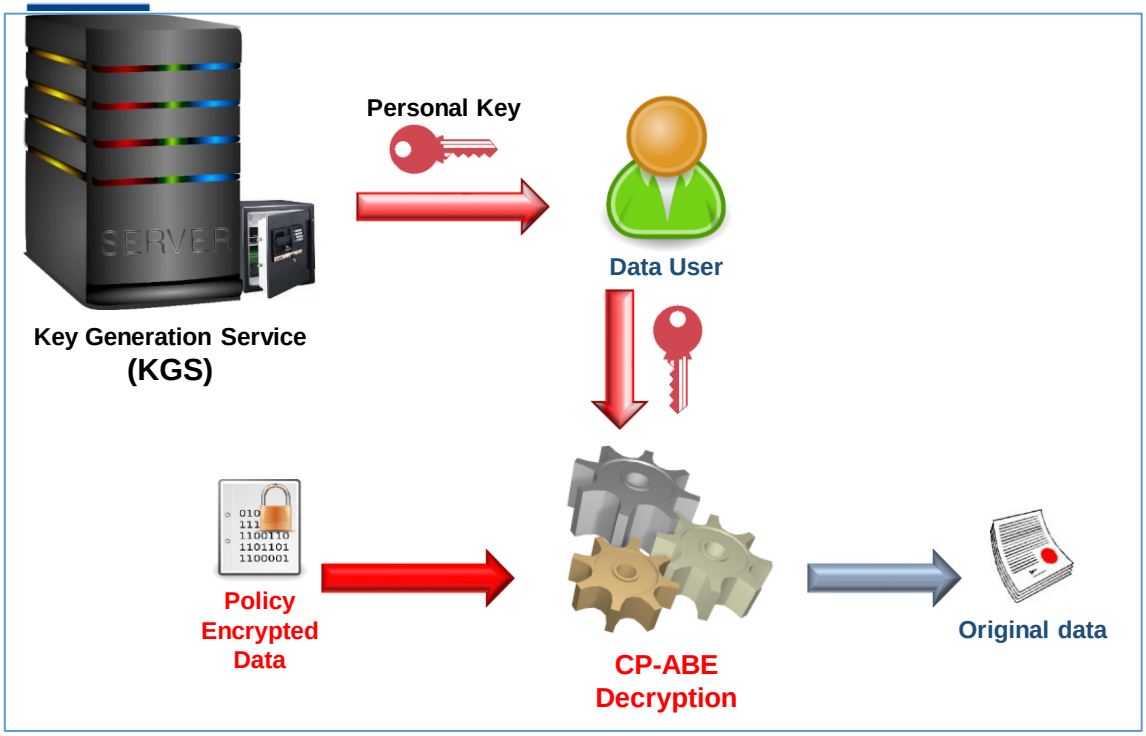

Figure 2: CP-ABE decryption process

The injection of the encryption / decryption functionalities in the information flow implemented for TagItSmart! is supported – thanks to the integration of the SeDEM client libraries - by clients acting as publishers and consumers of the MQTT messages handled by the Message Broker (i.e. the TagITSmart! Stream Processing component in the integration scenario), as shown in Figure 3. CP-ABE technology provided by the TagItSecure! component can be integrated in any user device able to run Java applications as well as in web browsers supporting the W3C WebCrypto API (smartphones, PCs, Raspberry Pi boards; some of these devices will be selected for the actual integration to be done for demonstration purposes). The CP-ABE client libraries included in the SeDEM solution, in fact, are available both in Java or in JavaScript.

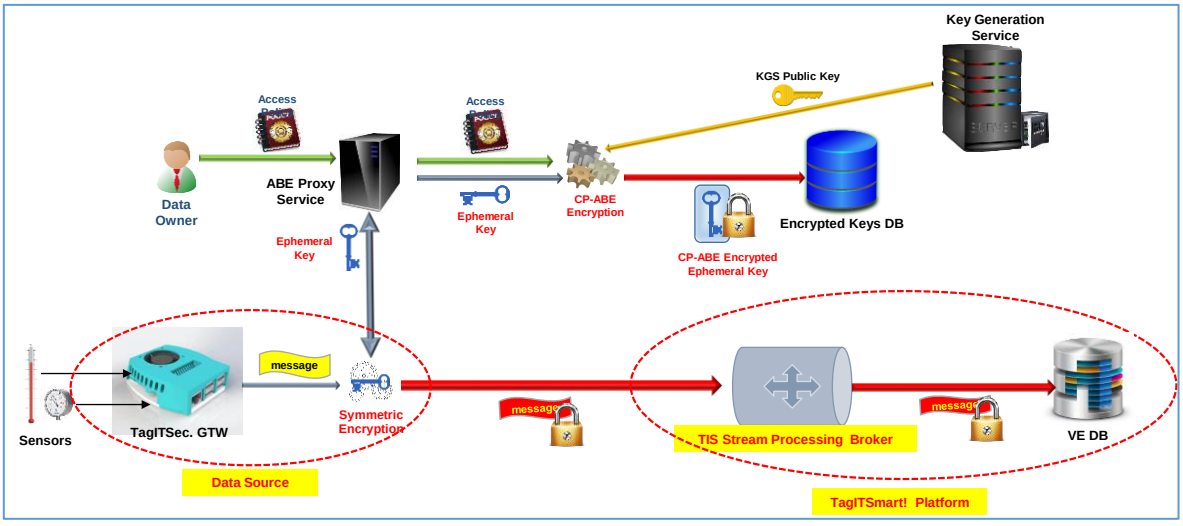

Figure 3: SeDEM Architecture & Interactions

The SeDEM client libraries, thus, enable the publishing of, or subscribing to, events in a secure way interacting with the CP-ABE supporting services, which are part of the SeDEM system, in particular, beyond the already described KGS, we have:

- **ABE Proxy Service**: the component responsible to perform the heavy ABE encryption operations;
- **Key Storage Service** (KSS): the service that manages the storage, with CP-ABE techniques, of the encrypted symmetric keys in the Encrypted Keys DB, so that these keys can be retrieved and used by data consumers.

At consumer side (see Figure 4) a mobile application acting as SmartTag reader will be developed. The SmartTags are associated to specific sensors of the publisher device's (e.g., the temperature sensor of the Raspberry Pi III) and, once scanned from the Sensor Stick, the mobile app will be enabled to fetch from the Virtual Entity Database the data associated to the sensor identifier and to display those data if the Android app's CP-ABE key is in line with the access policy.

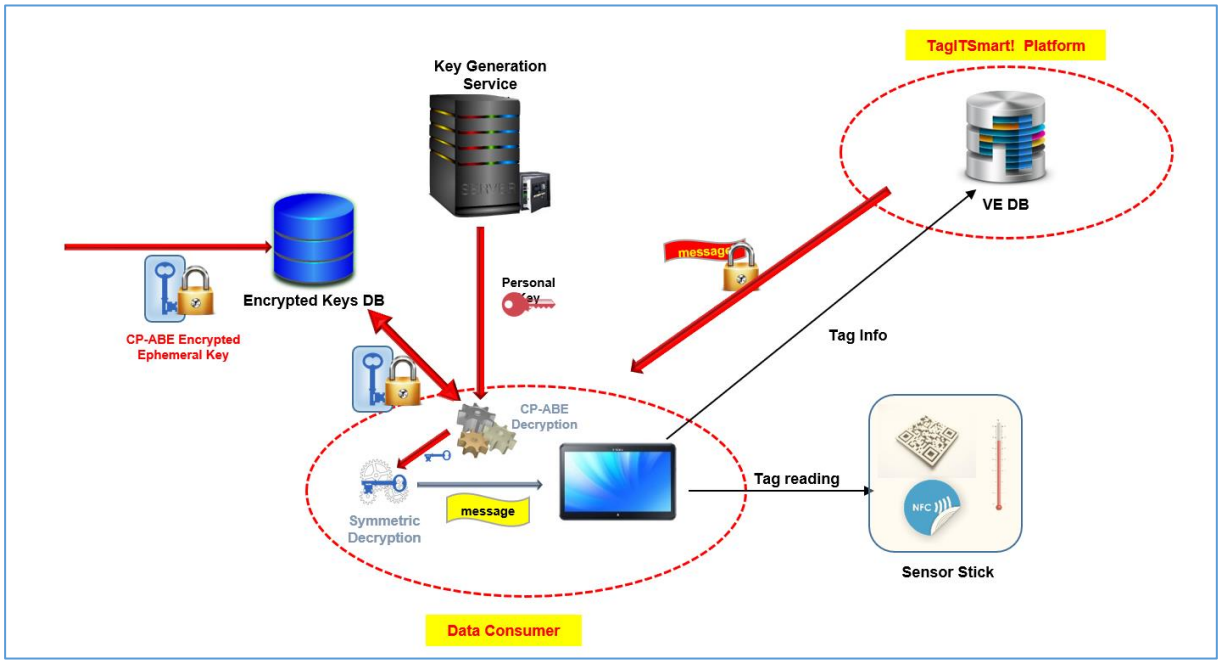

Figure 4: Tag & Android App Interactions

Finally, the SeDEM browser, a web application that, subscribed to the TagITSmart! Stream Processing event queue, uses the SeDEM libraries and displays each received event both in its encrypted and decrypted forms (see Figure 5), will be deployed as part of the solution. To this end the SeDEM Browser will use a CP-ABE key in line with the access policy provided by the data publisher.

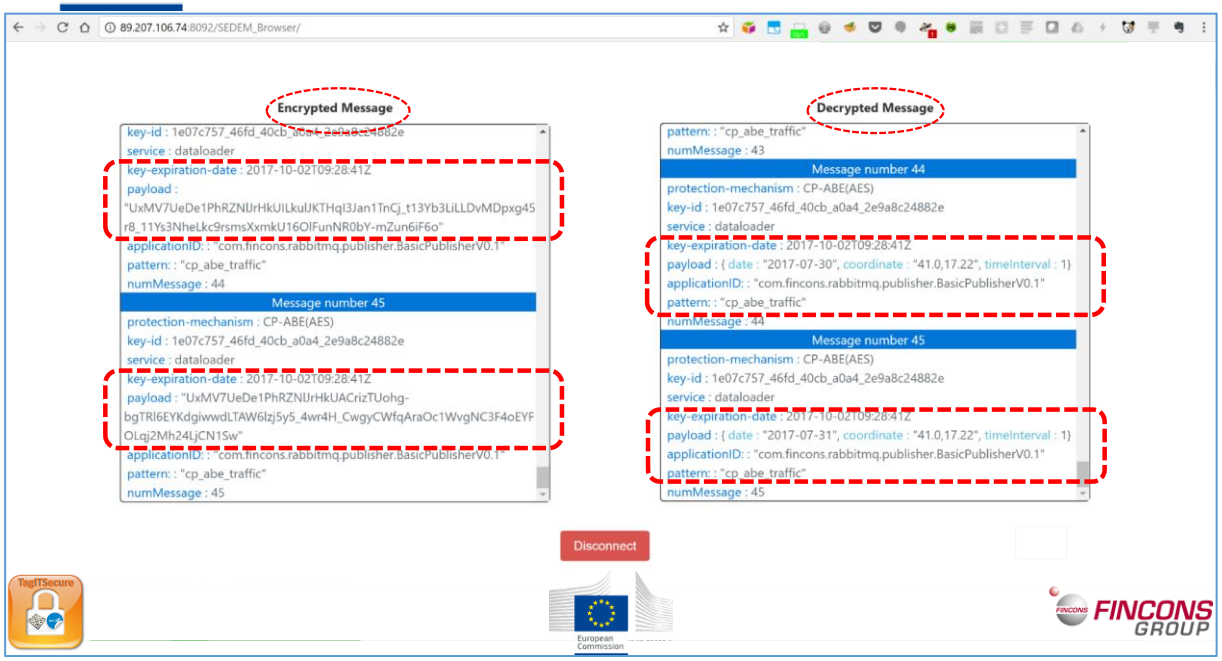

Figure 5: SeDEM Browser

Due to the ABE processing needs, a pure ABE approach is not suitable for environments in which data are generated at a high rate or by devices with resource constraints (thing that happens in IoT environments). The SeDEM module, therefore, has introduced a new approach for privacy-preserving data sharing that combines attribute-based cryptography along with symmetric key cryptography, thus obtaining the flexibility and expressiveness of the first one and the efficiency of the second one.
Therefore, the SeDEM system combines the CP-ABE and AES symmetric encryption schemes. Indeed, instead of directly encrypting the data with CP-ABE, data sources can encrypt the information they provide by using the AES symmetric algorithm and ephemeral AES keys that are CP-ABE encrypted by using data owner's provided access policies. In the end, thus, just the AES symmetric keys' encryption are CP-ABE protected.
From the security point of view, in addition to the CP-ABE encryption techniques, the component employs Elliptic Curve Cryptography (ECC) and Elliptic Curve Diffie–Hellman (ECDH) [3] algorithms for generating the ephemeral keys, as well as the new W3C Web Crypto API [4] for security management within web-browser-based applications.

3.1 TIS components used by TagItSecure!

The following TIS components will be used for the project implementation (see Figure 6):

- **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:** it will be the repository where encrypted messages published by SeDEM clients will be stored 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). An ad-hoc Virtual Entity template will be defined to easy the storage of sensor's data into the Virtual Entity Database
- **FC-Scanner:** the use of this component is still under evaluation; if feasible, it could be used, with proper integration of the SeDEM libraries, to encrypt and publish information linked to the scanned SmartTags.

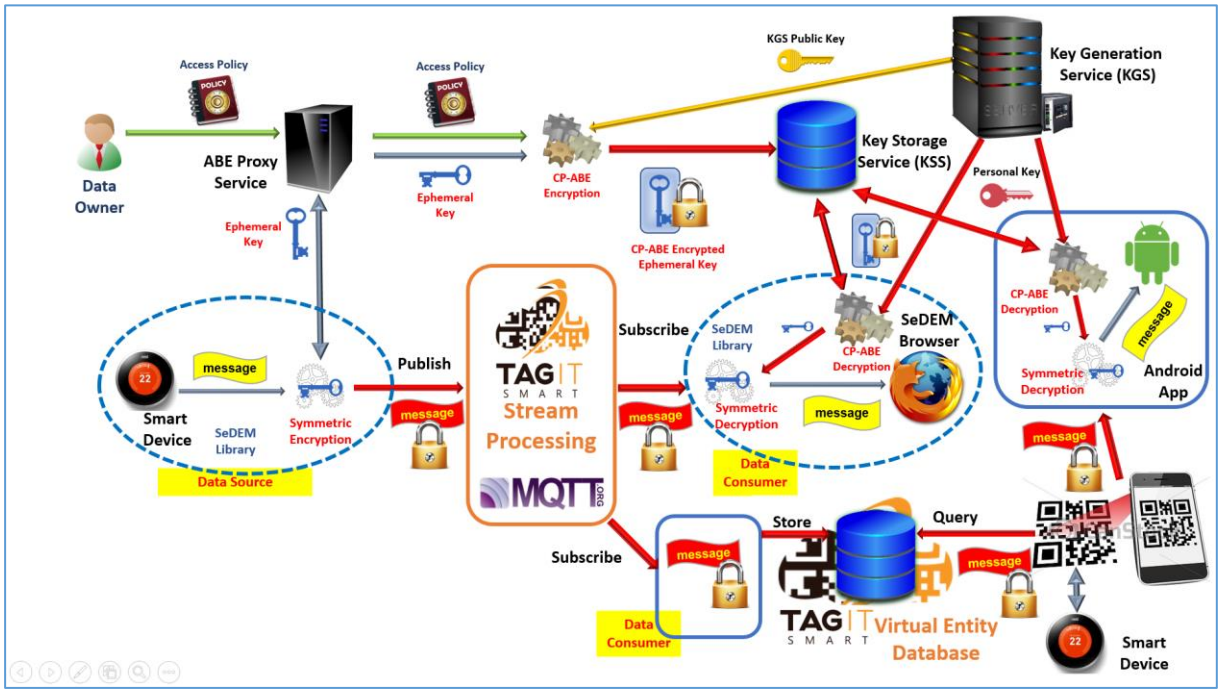

Figure 6: TagItSecure! overall picture

3.2 Demonstration use cases

The following use cases will be implemented for the demonstration of the project achievements:

- Protected management of information related to the monitoring of energetic parameters collected by sensors deployed in a school located in Palo del Colle (Italy)
- Protected management of information related to the monitoring of environment parameters collected by sensors deployed at the FINCONS Bari office
- Protected management of information acquired through the use of the FC-Scanner, upon the evaluation of the actual feasibility of the FC-Scanner integration, as described in 3.1.

Section 4 - Validation Scenario

This section aims to give evidence of the added value that the availability of the component brings to the TagItSmart! Platform mainly from the functional point of view.
Some validation scenarios are therefore described in the form of a set of demonstration cases that address the main functional aspects of the component.

1 **Possibility to define access policies based on the users' profile (attributes)**

***Actions*:**

- Access the TagItSecure! policy management tool (see Figure 7) by logging in with the credential of a user configured with rights to create policies.
- Move to the Create Policy tab and select in the left panel some of the blocks related to the attributes of the users as defined in the schema of the LDAP server used to manage users and drag them on to the main panel.
- Set the value of the attributes through the input / select box available on the attribute block
- Select in the left panel some of the blocks representing the logical operators and drag them in the main panel so that they surround the attributes which are subject to the logical condition.

***Result*:**

- The 'Text Policy' box shows the text of the policy to be used for encrypting those data intended to be accessed from users whose profiles match with the policy so defined
- The user can save the policy in the policy database, selecting or creating a particular folder

2 **Possibility to encrypt data-stream with a policy chosen according to the data access requirements**

Actions:

- Select a policy available or define a new policy (as described in scenario1) on the basis of the access requirements for a given dataset
- Configure the TagItSmart! Data Stream publisher client in order to use that policy for data encryption
- Activate the publisher so that it streams its events to the TagITSmart platform

Result:

- The events are published via the DataStream component correctly encrypted with the policy assigned (to verify that it is 'correctly' encrypted it is possible to check if the attributes of the users enabled to decrypt it match with the encryption policy, as done, for example, in the following TC)

3 **Successful decryption of a data-stream for users whose attributes match the policy used in the encryption**

Actions:

- Configure the mobile application that acts as reader of events from the Virtual Entity Database with a CP-ABE personal key matching the policy used for the encryption of data stream published via the Data Stream component
- Scan the QR code, or NFC tag, associated to a device previously used to generate the encrypted events

Result:

- The smartphone will acquire the sensor's data from VE Database, decrypt the data and display the sensor's value to the user

4 Unsuccessful decryption of a data stream for users whose attributes do not match the policy used in the encryption

Actions:

- Configure the mobile application that acts as reader of events from the Virtual Entity Database with a CP-ABE personal key that does not match the policy used for the encryption of data stream
- Scan the QR code, or NFC tag, associated to a device previously used to generate the encrypted events

Result:

- The smartphone will not succeed in decrypting the data acquired from the VE Database and will therefore display garbage text (or a decryption failed message)to the user

5 Acquisition of private key to be used by a publisher /subscriber for encryption / decryption operation

Actions:

- Access the TagItSecure! policy management tool (see Figure 7) by logging in with a publisher or subscriber credentials
- Move to the *Generate Key* tab and click the *Generate Key* button
- Copy the text of the generated key displayed and save it in the file referred as holder of the private key in the configuration of the publisher application (e.g. the Raspberry Pi III board) or on the subscriber one (e.g., the Android app or SeDEM Browser)
- report the acquired personal key into the publisher or subscriber configuration settings and start the application.

Result:

The subscriber application decrypts (i.e. displays in clear text) the event data.

Figure 7: Policy definition tool

4.1 KPIs to be used for evaluation

The achievement of the project technical objectives will be measured through the evaluation of specific KPIs, preliminary identified in the following table:

Table 1: Summary of KPIs

#	KPI name	Way of measurement	Goal	Notes
1	**Increased level of security**	Number of security threats addressed	5	Preliminary 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
2	**Enhancement of data protection functionalities**	Number of new test cases introduced (and passed) related to data protection issues	5	The validation test cases described in Section 4 -
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	**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 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	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	**N.B.:** the number provided here is related to FINCONS people only!

Section 5 - Conclusion

The present deliverable, D1.1, describes the technical architecture of the proposed module, and the integration scenario within the TIS ecosystem.
Some validation scenarios are also described in order to highlight what can be expected in a demonstration of the integrated solution.
Being 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 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*", which do not address issues tackled by TagItSecure!, i.e. the protection of data at transmission and storage level.

Section 6 - References

[1] J. Bethencourt, A. Sahai, B. Waters, " Ciphertext-policy attribute-based encryption", In: IEEE Symposium on Security and Privacy, SP 2007, pp. 321–334, 2007

[2] S. Pérez, J. L. Hernández-Ramos, D. Pedone, D. Rotondi, L. Straniero and A. F. Skarmeta, "A digital envelope approach using attribute-based encryption for secure data exchange in IoT scenarios", 2017 Global Internet of Things Summit (GIoTS), Geneva, 2017, pp. 1-6. doi: 10.1109/GIOTS.2017.8016281

[3] L. C. Elaine Barker, NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". Retrieved on May 2018, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

[4] M. Watson, "Web Cryptography API", Retrieved on May 2018, from https://www.w3.org/TR/WebCryptoAPI/

[5] http://ec.europa.eu/justice/data-protection/reform/index en.htm

[6] D. Rotondi, S. Gusmeroli, S. Piccione, "A capability-based security approach to manage access control in the Internet of Things", Mathematical and Computer Modelling Journal, ISSN 0895-7177, 10.1016/j.mcm.2013.02.006

[7] A. Kahate, "Cryptography and Network Security", Tata McGraw-Hill Education (2013)

[8] R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Comp. Netw. 57(10), 2266–2279 (2013)

[9] A. Cavoukian, M. Chanliau, "Privacy and security by design: a convergence of paradigms", Ontario, Canada: Office of the Privacy Commissioner (Ontario), 2013

[10] European Commission: Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", September 2014

[11] FTC Staff Report, "FTC: Internet of things - Privacy & Security in a Connected World", January 2015

[12] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine grained access control of encrypted data", in: Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98. ACM (2006)

[13] S. Pérez, D. Rotondi, D. Pedone, L. Straniero, M.J. Núñez, F. Gigante, "Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts", in: L. Barolli, T. Enokido (eds) "Innovative Mobile and Internet Services in Ubiquitous Computing". IMIS 2017. Advances in Intelligent Systems and Computing, vol 612. Springer, Cham (https://doi.org/10.1007)

[14] S. Pérez, D. Rotondi, D. Pedone, L. Straniero, "Data Confidentiality and Smart Energy", 3rd Italian Conference on ICT for Smart Cities & Communities; Bari, September 27-29 2017

[15] S. Pérez, J. L. Hernández-Ramos, S. N. Matheu-García, D. Rotondi, A. F. Skarmeta, L. Straniero, D. Pedone, "A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios", in IEEE Access, vol. 6, pp. 11738-11750, 2018.doi: 10.1109/ACCESS.2018.2801383

Section 7 - Glossary

Term	Definition
ABAC	Attribute Based Access Control
ABE	Attribute Based Encryption
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ATS	Access Token Service
CP-ABE	Ciphertext Policy Attribute Based Encryption
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
EU	European Union
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IoT	Internet of Things
JWT	Java Web Token
KPI	Key Performance Indicator
KGS	Key Generation Service
KSS	Key Storage Service
LDAP	Lightweight Directory Access Protocol
RBAC	Role-Based Access Control
SeDEM	Secure Data Exchange Middleware
TC	Test Case
TIS	TagItSmart!
W3C	World Wide Web Consortium