Risk and threat analysis with security requirement

Deliverable D2.5

Editor Name:	M. des Noes
Type:	Report
Dissemination Level:	CO
Release Date:	10.02.2017
Version:	1.2
Status:	Final

This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
under Grant Agreement № 644962.
More information available at https://prismacloud.eu.

Copyright Statement

Executive Summary

Absolute security does not exist and, in any system, security definition has first to start with a threat analysis (attacker profiling) and a definition of the information to protect (and against what), second, to define security policies (how to protect the assets, which part of the system is in charge of protecting what) and third, to identify the security limitation of each component or subsystem and to implement counter measures at the component level or at the system level (adding security features at one upper level to counter weaknesses of the lower levels).

There are various methods supporting this kind of analysis, EBIOS at the system level (identifying risks) [1] [2], Common Criteria at the component level (rating the effective resistance) [3] [4]. The objective of this deliverable is to perform a risk analysis of two use cases which are typical of the cloud based services and then define security requirements to mitigate the identified risks. In the first one an application is hosted by a cloud service provider and sensitive personal data may be manipulated by a third party and in the second scenario the cloud service provider is the same entity that manages the application offered to customers. These risk analysis studies have been reported in deliverable D2.4 [1], which also proposes security requirements based on ISO/IEC standards. In this deliverable, security requirements are formalized in the language of Common Criteria standard [4][5][6] which will ease a future security evaluation.

Chapter 2: Smart Cities – European disable badge for public parking areas

The first use case is named "European Disable Badge for public parking areas". It offers a service helping disable persons to find dedicated park places in a city. It is based on a badge which can be read by a smartphone with the NFC technology. The badge ID is used to connect to the centralized application which is hosted by a cloud service provider [2]. The security of this service relies on the security of the implementation of the application in the smartphone and on the security of the cloud infrastructure provided by a third party. The implementation of this service should prevent illegal use of a badge and also must not leak personal data.

The risk analysis detailed in [1] identifies high risk level related to the availability, disclosure or modification of sensitive data. Security requirements are derived according to the Common Criteria methodology. It consists first in defining a Target of Evaluation (TOE), which clearly states what will be evaluated and certified. Then the security objectives for this TOE are defined, based on the outcomes of the risk analysis study. Eventually, security requirements that will mitigate these risks are formalized in the pre-defined structured language proposed by the Common Criteria standard. Finally, Security requirements implemented by PRISMACLOUD services are highlighted.

Chapter 3: E-Government

The second use case is named "E-Government". It implements a cloud service for public bodies in the Lombardia region [2]. The security of this service relies mainly on the security offered by the infrastructure controlled by LISPA. There is thus a difference compared to the previous use case, the cloud provider is also the service provider. The conclusions of the risk

analysis detailed in [1] are analogue to those derived for the European disable badge use case. Security requirements are proposed for this use case.

Document Information

Project Context

Work Package:	WP2
Task:	T2.4
Dependencies:	D2.3, D2.4

Author List

Organization	Name	E-mail
CEA	M. des Noes	Mathieu.desnoes@cea.fr

Reviewer List:

Organization	Name	E-mail
ETRA	Alberto Zambrano	azambrano.etraid@grupoetra.com
UNI PASSAU	Henrich Poehls/Marek Klein	hp@sec.uni-passau.de

Version History:

Version	Date	Reason/Change	Editor
1.0	07.10.2016	Creation	M. des Noes
1.1	20.01.2017	Final version for internal review	M. des Noes
1.2	03/02/2017	Modifications after comments from ETRA	M. des Noes

Abbreviations and Acronyms

CC	Common Criteria (ISO/IEC 15408)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OE	Operational Environment
TOE	Target of Evaluation
TSF	TOE Security Functions

Table of Contents

1. Introduction

1.1. Purpose and scope of the document

The goal of this report is to propose security functional requirements for two representative use cases that will be implemented in the project: Smart Cities (European disable badge for public parking areas) and E-government [2].

Security requirements are proposed for mitigating the identified risks, detailed in Deliverable D2.4 [1]. The methodology proposed by the Common Criteria standard [4][5][6] has been applied to formalize in a pre-defined structured language these security requirements. They could be used later on in a certification process to build a security target.

1.2. Relation to other project work

This document builds upon the risks identified in D2.4 to propose security functional requirements (SFRs) that will mitigate them. The outcome of this deliverable can be used to verify the specification of test-bed configurations (deliverable D8.1) take into account security requirements described in this document.

1.3. Structure of the document

Chapter 2 implements the methodology proposed by CC standard to derive security functional requirements (SFRs) for the "European Disable Badge for public parking areas" Smart City use case. First of all, the target of evaluation (TOE) is defined. It specifies the scope of what will be evaluated. Then the security problem is stated. It splits the work between the TOE and the operational environment (OE) which is not concerned by the evaluation process. Based on the risk analysis performed in deliverable D2.4, the security objectives for the TOE and the OE are established. Eventually SFRs are selected in the list of pre-defined requirements proposed by CC standard [2]. Finally, the security objectives coverage by SFRs is analyzed.

Chapter 3 carries out the same work for the E-government use case.

2. Smart Cities - European Disable Badge for public parking areas

2.1. Description of the target of evaluation (TOE)

In the CC language [4], a Target of Evaluation (TOE) is defined as a set of software, firmware and/or hardware. The TOE may be an IT product, a part of an IT product, a set of IT products…etc. It is defined to clearly state what will be evaluated and certified. For instance, the TOE may contain only a part of an IT product, and its evaluation should not be misrepresented as the evaluation of the entire IT product (e.g. for marketing purpose).

In the context of the smart cities context, the TOE is the set of software used to run the SIMON SAYS application. The operational environment (OE) is defined by the set of IT products operated by the cloud service provider to manage its infrastructure (e.g. servers, communication between servers).

2.2. Security problem definition

This section shows the threats that are to be countered by the TOE and its operational environment. This information is extracted from deliverable D2.4 [1] that provides a detailed risk analysis.

2.2.1. Threats thwarted by the TOE

The residual risks faced by the TOE are listed in Table 1. While many risks can be mitigated with the application of standard good practices of the IT domain, others that are specific to cloud based application require additional cryptographic tools:

- Secure storage:
  - Encryption of personal data: TS16, TS17, TS18, TS22, TS25
  - Verification of data integrity : TS6 , TS14, TS15, TS21, TS24
- Secure distributed storage: TS9, TS10

The mitigation of threat scenarios 9 and 10 requires the services, reports and records provided by the cloud provider should be regularly monitored and reviewed, and audits should be carried out regularly.

Reference	Threat scenario	Countermeasure	Risk level
TS6	Data transmission Man in the middle attack – Modification of data or routing	Cryptographic mechanism for data integrity verification (MAC)	1. Negligible
TS9	Cloud provider declares bankruptcy	A mirror site is operated by a different cloud provider	1. Negligible

		(distributed storage).	
TS10	Servers are seized by justice	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS14	Data can be modified by another tenant	Cryptographic mechanism for data integrity verification (MAC)	2. Limited
TS16	Data stored in a server are not erased properly and are accessible to another tenant	Encryption of data	1. Negligible
TS17	Data are accessible to another tenant (*Trust Boundaries Overlapping)*	Encryption of data	1. Negligible
TS18	Servers are stolen and data can be retrieved	Encryption of data	1. Negligible
TS21-TS24	An employee under the influence of a hacker or motivated by revenge modifies data	Cryptographic mechanism for data integrity verification (MAC)	2. Limited
TS22-TS25	An employee under the influence of a hacker or motivated by revenge discloses some data	Encryption of data	1. Negligible

Table 1: Residual risks estimation.

2.2.2. Threats thwarted by the operational environment (OE)

Table 2 shows the risks thwarted by the OE. It is assumed the cloud service provider applies standard IT security measures defined by ISO/IEC 27001, 27002 [7] and 27018 [8] standards. In a certification process, the compliance with these standards should be audited. This will ensure the TOE is protected as expected.

Reference	Threat scenario	Countermeasure	Risk level
TS3	Denial of service attack (resources consumption)	Standard IT protections (ISO/IEC 2700x and 27018)	2. Limited

TS4	Blocking of IP addresses	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS5	Cloud's access network disruption	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS8	Cloud is over exploited	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS11	Data are lost or erased	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS12	Malicious modification of access rights of a legitimate user	Standard IT protections (ISO/IEC 2700x and 27018)	2. Limited
TS13	Connections between servers of the cloud provider's infrastructure are not available	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS15	Modification of data or routing	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS19	Eavesdropping of communications between cloud's servers	Standard IT protections (ISO/IEC 2700x and 27018)	1. Negligible
TS20-TS23	An employee under the influence of a hacker or motivated by revenge deletes data	Standard IT protections (ISO/IEC 2700x and 27018)	2. Limited

Table 2: Risks thwarted by the organisational environment.

2.3. Security objectives

The security objectives are a statement of the intended solution to the problem defined by the security problem definition. They are split according to the TOE and the OE. The coverage showing how threats are countered by the security objectives is detailed in deliverable D2.4 [1] (cf. Table 1 and Table 2).

2.3.1. Security objectives for the TOE

The security objectives for the TOE are presented in Table 3.

Security objective	Description	Prevention	Protection	Recovery
Secure wireless communication	The wireless communication between the remote user and the application is protected against data disclosure and modification.		x	
User authentication	The TOE shall ensure the authentication of the user before providing access to the application	x	x	
Confidentiality	The TOE shall ensure the confidentiality of the stored data with respect to any unauthorized user.		x	
Integrity	The TOE shall ensure the integrity of the stored data.		x	x
Availability	The TOE shall ensure the availability of the offered service.		x	
Audit	The TOE shall audit the critical events that inform about the correct functioning of the application	x		
Secure state	The TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal data or user data		x	x
Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	x		x
Security of system documentation	System documentation should be protected against unauthorized access.		x	
Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	x	x	
Administrator and operator logs	System administrator (Officer) activities should be logged.	x	x	

Fault logging	Faults should be logged, analyzed, and appropriate action taken.		x	x
User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	x	x	
Privilege management	The allocation and use of privileges (Officer and Auditor) should be restricted and controlled.	x	x	
Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	x		x
Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		x	

Table 3: security objectives for the TOE.

2.3.2. Security objectives for the OE

Table 4 presents the security objectives for the OE. They are taken from ISO 27002 standard [7]. The main security objective for the cloud service provider is to be compliant with ISO/IEC 27002 and 27018 standards [7][8]. This ensures that sate of the art security measures are enforced.

The client application on the smartphone and the application will provide an appropriate interface and communication path between users and the TOE. The TOE environment transmits identification, authentication and management data of TOE users correctly and in a confidential way to the TOE. This is ensured by using appropriate modes of wireless communication systems (3G, LTE…).

Security measure	**Description**	**Prevention**	**Protection**	**Recovery**
Information security awareness, education, and training	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and	x	x	

	regular updates in organizational policies and procedures.			
Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.	x	x	
Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	x		
Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	x	x	
Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	x	x	
Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	x	x	
Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	x	x	x
Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.		x	
Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	x	x	
Service delivery	It should be ensured that the security controls, service definitions and	x		

	delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.			
Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	x	x	
Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.	x	x	
Data localization	Cloud service provider must be able to inform the organization about the localization of data.	x		
Capacity management	The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance	x		

Table 4: security objectives for the OE.

2.4. TOE Roles

The TOE shall as a minimum support the following user categories (roles):

- **Officer** (authorized to install, configure, maintain and uninstall the TOE)
- **User** (authorized to access and use the services offered by the TOE)
- **Auditor** (authorized to read audit data generated by the TOE and exported for audit review)

The interface to the TOE may either be shared between the different user categories, or separated for certain functions, for example configuration.

Authentication of TOE users shall be identity-based.

Maintenance of the TOE are highly critical operations that need to be related to the individual users that performed the operation. It is therefore required that the individual users have to be known by the TOE as Auditor and Officer and the TOE needs to perform identity based authentication for those roles. The Officer role is very powerful including user and key management. Therefore the Auditor role is implemented to watch on Officer's actions and to detect misuse of Officer's authorization.

2.5. Security Functional Requirements

Security Functional Requirements (SFR) are a translation of the security objectives for the TOE into a predefined standardized language [5]. This is independent from implementation. SFRs do not concern security objectives for the operational environment, because it is not evaluated.

Those portions of a TOE that must be relied on for the correct enforcement of the SFRs are collectively referred to as the **TOE Security Functionality (TSF)**. It consists in all hardware, software, and firmware of a TOE that is relied upon for security enforcement.

2.5.1. Audit (FAU)

2.5.1.1. Audit data generation (FAU.1)

It shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- Initialization/ shutdown of the TOE;
- Authentication failure handling: the reaching of the threshold for the unsuccessful authentication attempts and the actions;
- Timing of authentication: all unsuccessful use of the authentication mechanism;
- Management of security attributes: all modifications of the values of security attributes;
- Static attribute initialization: modifications of the default setting of permissive or restrictive rules, all modifications of the initial values of security attributes;
- Management of audit data: export of audit data, clear of audit data;
- Failure with preservation of secure state: Failure detection of the TOE security functions and secure state.
- Notification of physical attack: detection of intrusion
- Execution of the self-tests during initial start-up, at the request of the authorized user (Officer), during installation and maintenance and the results of the tests, unsuccessful self-test operations.

Each audit record should at least contain the following information: date and time of the event, type of event, subject identity, user identity (if relevant) and the outcome (success or failure) of the event.

2.5.1.2. User identity association (FAU.2)

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

2.5.1.3. Guarantees of audit data availability (FAU.3)

The stored audit records shall be protected from unauthorised modifications and deletion.

2.5.1.4. Secure audit event storage (FAU.4)

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail

2.5.2. User data protection (FDP)

2.5.2.1. Basic Data authentication (FDP.1)

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of stored personal information (i.e. badge ID, user ID).

2.5.2.2. Residual information protection (FDP.2)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource.

2.5.2.3. Stored data integrity monitoring and action (FDP.3)

The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects. This could be based e.g. on cyclic redundancy check or an error detecting code. Upon detection of a data integrity error, the TSF shall enter the secure state.

2.5.2.4. User data confidentiality transfer protection (FDP.4)

When user data are transferred using an external channel between the TSF and another trusted IT product (remote memory storage resource), the user data shall be transmitted/received in a manner protected from unauthorized disclosure.

2.5.2.5. User data integrity transfer protection (FDP.5)

When user data are transferred using an external channel between the TSF and another trusted IT product (remote memory storage resource), the user data shall be transmitted/received in a manner protected from modification, deletion, insertion and replay errors.

2.5.3. Identification and authentication (FIA)

2.5.3.1. Authentication failure handling (FIA.1)

The TSF shall detect when unsuccessful authentication attempts occur. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE shall block the identity for authentication.

2.5.3.2. User attribute definition (FIA.2)

The TSF shall maintain the following list of security attributes belonging to individual users: identity and role (Officer/User/Auditor).

2.5.3.3. User authentication (FIA.3)

The TSF shall require each user to be successfully authenticated before allowing any other actions on behalf of that user.

The TSF shall detect and prevent use of authentication data that has been forged by any user of the TOE.

The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TOE.

2.5.4. Privacy (FPR)

The TSF shall ensure that other users are unable to determine the real user name.

2.5.5. Protection of the TOE Security Functionality (FPT)

2.5.5.1. Fail secure (FPT.1)

The TSF shall preserve a secure state when self-tests failures are detected.

2.5.5.2. Inter-TSF detection of modification (FPT.2)

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product.

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform alarm indication to the Officer if modifications are detected.

2.5.5.3. Internal TOE TSF data transfer (FPT.3)

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

2.5.5.4. Trusted recovery (FPT.4)

After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided. This could be a manual or automated recovery.

2.5.5.5. TSF testing (FPT.5)

The TSF shall run a suite of self-tests during initial start-up, at the request of the authorised user, during installation and maintenance to demonstrate the correct operation of the TSF.

2.5.6. Resource utilisation (FRU)

2.5.6.1. Fault tolerance (FRU.1)

The TSF shall ensure the operation of [*list of TOE capabilities*] when the following failures occur: [*list of type of failures*]. The two lists are to be defined.

2.5.6.2. Resource allocation (FRU.2)

The TSF shall enforce maximum quotas of the critical resources that users can use simultaneously or over a specified period of time. This requirement allows the TSF to control the use of resources by users such that denial of service will not occur because of unauthorised monopolisation of resources.

2.5.7. Trusted path (FTP)

The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

The TSF shall permit remote users to initiate communication via the trusted path.

The TSF shall require the use of the trusted path for initial user authentication.

Practically, it is assumed the application selects a communication bearer that ensures both data confidentiality and integrity. These bearers are proposed by 3G and 4G networks.

2.5.8. Security objectives coverage by SFRs

Table 5 shows that each security objective is at least covered by one SFR.

Security objective	Description	SFRs
Secure wireless communication	The wireless communication between the remote user and the application is protected against data disclosure and modification.	FTP.1
User authentication	The TOE shall ensure the authentication of the user before providing access to the application	FDP.1, FIA.1, FIA.2 and FIA.3
Confidentiality	The TOE shall ensure the confidentiality of the stored data with respect to any unauthorized user.	FDP.2, FDP.4
Integrity	The TOE shall ensure the integrity of the stored data.	FDP.3, FDP.5
Availability	The TOE shall ensure the availability of the offered service.	FRU.2

Audit	The TOE shall audit the critical events that inform about the correct functioning of the application	FAU.1, FAU.2 and FAU.3
Secure state	The TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal data or user data	FPT.1, FPT.4, FPT.5
Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	FDP.2, FDP.3, FDP.4 and FDP.5
Security of system documentation	System documentation should be protected against unauthorized access.	FAU.4
Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	FAU.4
Administrator and operator logs	System administrator (Officer) activities should be logged.	FAU.4
Fault logging	Faults should be logged, analyzed, and appropriate action taken.	FAU.4
User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	FIA.1, FIA.3
Privilege management	The allocation and use of privileges (Officer and Auditor) should be restricted and controlled.	FIA.2
Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	FRU.1
Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	FPR

Table 5: Security objectives coverage by SFRs.

2.6. Security requirements implemented by PRISMACLOUD services

PRISMACLOUD services will implement the following security requirements: user authentication, confidentiality, and data protection and privacy of personal information. This will serve as countermeasures to threat scenarios 17, 18, 22 and 25 defined in Table 6.

Reference	Threat scenario	Countermeasure	Risk level
TS17	Data are accessible to another tenant (*Trust Boundaries Overlapping)*	Encryption of data	1. Negligible
TS18	Servers are stolen and data can be retrieved	Encryption of data	1. Negligible
TS22-TS25	An employee under the influence of a hacker or motivated by revenge discloses some data	Encryption of data	1. Negligible

Table 6: Threat scenarios thwarted by PRISMACLOUD services.

The Encryption Proxy Service [3] will allow the encryption of data at rest without modifying anything in the application being cloudified. Sensitive information from legacy applications are encrypted in a format/order preserving way when moved to the cloud.

The application will be redesigned in a privacy-by-design manner, in order to minimize the amount of sensitive data required to provide the service. The Privacy Enhancing Identity Management (PIDM) service [3] will support the redesign by providing the cryptographic features needed to avoid the processing of actual users identification in the process of validating and controlling parking lot uses. It enables users to delegate PIDM to the Selective Disclosure component. In particular, it allows users to store their attribute credentials obtained from some entity in this component and this component realizes a selective attribute-disclosure functionality. The application will be presented a redacted version of the credential (and potentially additional information) that it can verified. This verification will ensure the user is allowed to access the system.

3. E-Government

In this chapter, security functional requirements for the E-government use case are presented. Unlike the smart city use case, the cloud infrastructure is the service provided by LISPA to its customers (public bodies of Lombardia region). As a result, the operational environment of the smart city use case becomes the target of evaluation of the E-government use case.

Note that ANSSI and BSI have released in December 2016 a label for Cloud Security, named ESCloud [10][11]. It also defines security requirements for cloud service provider and reference to international standards [12].

3.1. Description of the target of evaluation (TOE)

In the context of the E-government use case, the TOE consists in all the software applications and hardware platforms that are used to build the cloud platform that will enable LISPA's customers (public bodies and authorities) to design and set-up their own IT infrastructure.

The operational environment (OE) is defined by the organization of information security, security policies and work instructions, personnel related security issue (e.g. training, disciplinary measures) and physical security. The related security requirements are detailed in section 5.1, 5.2 and 5.3 of [10].

3.2. Security problem definition

The residual risks are listed in Table 7. According to the security objectives defined in [1], the risks are kept below a level 2.
While many risks can be mitigated with the application of standard good practices of the IT domain, others that are specific to cloud based application requires additional cryptographic tools:

- Secure storage:
  - Encryption of data: TS14, TS15, TS16, TS17, TS20, TS23
  - Verification of data integrity and authenticity: TS4, TS5, TS13, TS19, TS22
- Secure distribute storage: TS1, TS2, TS3, TS9, TS10, TS12

Reference	Threat scenario	Countermeasure	Risk level
TS1	Denial of service attack (resources consumption)	A mirror site is operated by a different cloud provider (distributed storage).	2. Limited
TS2	Blocking of IP addresses	A mirror site is operated by a different cloud provider	1. Negligible

		(distributed storage).	
TS3	Cloud's access network disruption (e.g. "cut" the cable)	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS4-TS6	Man in the middle attack	Cryptographic mechanism for data integrity verification (MAC)	1. Negligible
TS5	Eavesdropping (access network)	Encryption of data	1. Negligible
TS9	Servers are seized by justice	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS10	Data are lost or erased	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS13	Data can be modified by another tenant	Cryptographic mechanism for data integrity verification (MAC)	1. Negligible
TS14	Data stored in a server are not erased properly and are accessible to another tenant	Encryption of data	1. Negligible
TS15	Data are accessible to another tenant (*Trust Boundaries Overlapping)*	Encryption of data	1. Negligible
TS16	Servers are stolen and data can be extracted	Encryption of data	1. Negligible
TS17	Eavesdropping (inside cloud infrastructure)	Encryption of data	1. Negligible
TS19-TS22	An employee under the influence of a hacker modifies data (personal or access rights)	Cryptographic mechanism for data integrity	2. Limited

		verification (MAC)	
TS20-TS23	An employee motivated by revenge discloses some data	Encryption of data	1. Negligible

Table 7: Residual risks estimation.

3.3. Security objectives

3.3.1. Security objectives for the TOE

The security objectives for the TOE are presented in Table 8.

Security objective	Description	Prevention	Protection	Recovery
Secure wireless communication	The wireless communication between the remote user and the application is protected against data disclosure and modification.		x	
User authentication	The TOE shall ensure the authentication of the user before providing access to the application	x	x	
Confidentiality	The TOE shall ensure the confidentiality of the stored data with respect to any unauthorized user.		x	
Integrity	The TOE shall ensure the integrity of the stored data.		x	x
Availability	The TOE shall ensure the availability of the offered service.		x	
Audit	The TOE shall audit the critical events that inform about the correct functioning of the application	x		
Secure state	The TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal data or user data		x	x
Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	x		x

Security of system documentation	System documentation should be protected against unauthorized access.		x	
Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	x	x	
Administrator and operator logs	System administrator (Officer) activities should be logged.	x	x	
Fault logging	Faults should be logged, analyzed, and appropriate action taken.		x	x
User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	x	x	
Privilege management	The allocation and use of privileges (Officer and Auditor) should be restricted and controlled.	x	x	
Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	x		x
Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		x	

Table 8: security objectives for the TOE.

3.3.2. Security objectives for the OE

Table 9 presents the security objectives for the OE. They are taken from ISO 27002 standard [7][8]. Compliance with the new ESCloud label [10][11] promoted by ANSSI and BSI could be of valuable interest.

Security measure	Description	Prevention	Protection	Recovery
Information security awareness, education, and training	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures.	x	x	
Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.	x	x	
Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	x		
Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	x	x	
Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	x	x	
Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	x	x	
Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	x	x	x
Cabling security	Power and telecommunications cabling carrying data or supporting information services should be		x	

	protected from interception or damage.			
Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	x	x	
Service delivery	It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	x		
Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	x	x	
Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.	x	x	
Data localization	Cloud service provider must be able to inform its customers about the localization of data.	x		

Table 9: security objectives for the OE.

3.4. TOE Roles

The TOE shall as a minimum support the following user categories (roles):

- **Officer** (authorized to install, configure, maintain and uninstall the TOE)
- **User** (authorized to access and use the services offered by the TOE)
- **Auditor** (authorized to read audit data generated by the TOE and exported for audit review)

The interface to the TOE may either be shared between the different user categories, or separated for certain functions, for example configuration.

Authentication of TOE users shall be identity-based.

Maintenance of the TOE are highly critical operations that need to be related to the individual users that performed the operation. It is therefore required that the individual users have to be known by the TOE as Auditor and Officer and the TOE needs to perform identity based authentication for those roles. The Officer role is very powerful including user and key

management. Therefore the Auditor role is implemented to watch on Officer's actions and to detect misuse of Officer's authorization.

3.5. Security Functional Requirements

3.5.1. Audit (FAU)

3.5.1.1. Audit data generation (FAU.1)

It shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- Initialization/ shutdown of the TOE;
- Authentication failure handling: the reaching of the threshold for the unsuccessful authentication attempts and the actions;
- Timing of authentication: all unsuccessful use of the authentication mechanism;
- Management of security attributes: all modifications of the values of security attributes;
- Static attribute initialization: modifications of the default setting of permissive or restrictive rules, all modifications of the initial values of security attributes;
- Management of audit data: export of audit data, clear of audit data;
- Failure with preservation of secure state: Failure detection of the TOE security functions and secure state.
- Notification of physical attack: detection of intrusion
- Execution of the self-tests during initial start-up, at the request of the authorized user (Officer), during installation and maintenance and the results of the tests, unsuccessful self-test operations.

Each audit record should at least contain the following information: date and time of the event, type of event, subject identity, user identity (if relevant) and the outcome (success or failure) of the event.

3.5.1.2. User identity association (FAU.2)

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

3.5.1.3. Guarantees of audit data availability (FAU.3)

The stored audit records shall be protected from unauthorised modifications and deletion.

3.5.1.4. Secure audit event storage (FAU.4)

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail

3.5.2. User data protection (FDP)

3.5.2.1. Basic Data authentication (FDP.1)

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of stored personal information.

3.5.2.2. Residual information protection (FDP.2)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource.

3.5.2.3. Stored data integrity monitoring and action (FDP.3)

The TSF shall monitor user data stored in containers controlled by the TSF for integrity errors on all objects. This could be based e.g. on cyclic redundancy check or an error detecting code. Upon detection of a data integrity error, the TSF shall enter the secure state.

3.5.2.4. User data confidentiality transfer protection (FDP.4)

When user data are transferred using an external channel between the TSF and another trusted IT product (remote memory storage resource), the user data shall be transmitted/received in a manner protected from unauthorized disclosure.

3.5.2.5. User data integrity transfer protection (FDP.5)

When user data are transferred using an external channel between the TSF and another trusted IT product (remote memory storage resource), the user data shall be transmitted/received in a manner protected from modification, deletion, insertion and replay errors.

3.5.3. Identification and authentication (FIA)

3.5.3.1. Authentication failure handling (FIA.1)

The TSF shall detect when unsuccessful authentication attempts occur. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE shall block the identity for authentication.

3.5.3.2. User attribute definition (FIA.2)

The TSF shall maintain the following list of security attributes belonging to individual users: identity and role (Officer/User/Auditor).

3.5.3.3. User authentication (FIA.3)

The TSF shall require each user to be successfully authenticated before allowing any other actions on behalf of that user.

The TSF shall detect and prevent use of authentication data that has been forged by any user of the TOE.

The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TOE.

3.5.4. Privacy (FPR)

The TSF shall ensure that other users are unable to determine the real user name.

3.5.5. Protection of the TOE Security Functionality (FPT)

3.5.5.1. Fail secure (FPT.1)

The TSF shall preserve a secure state when self-tests failures are detected.

3.5.5.2. Inter-TSF detection of modification (FPT.2)

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product.

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform alarm indication to the Officer if modifications are detected.

3.5.5.3. Internal TOE TSF data transfer (FPT.3)

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

3.5.5.4. Trusted recovery (FPT.4)

After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided. This could be a manual or automated recovery.

3.5.5.5. TSF testing (FPT.5)

The TSF shall run a suite of self-tests during initial start-up, at the request of the authorised user, during installation and maintenance to demonstrate the correct operation of the TSF.

3.5.6. Resource utilisation (FRU)

3.5.6.1. Fault tolerance (FRU.1)

The TSF shall ensure the operation of [*list of TOE capabilities*] when the following failures occur: [*list of type of failures*]. The two lists are to be defined.

3.5.6.2. Resource allocation (FRU.2)

The TSF shall enforce maximum quotas of the critical resources that users can use simultaneously or over a specified period of time. This requirement allow the TSF to control the use of resources by users such that denial of service will not occur because of unauthorised monopolisation of resources.

3.5.7. Trusted path (FTP)

The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.

The TSF shall permit remote users to initiate communication via the trusted path.

The TSF shall require the use of the trusted path for initial user authentication.

Practically, it is assumed the plaform selects a communication technology that ensures both data confidentiality and integrity.

3.5.8. Security objectives coverage by SFRs

Security objective	Description	SFRs
Secure communication	The communication between the remote user and the application is protected against data disclosure and modification.	FTP.1
User authentication	The TOE shall ensure the authentication of the user before providing access to the application	FDP.1, FIA.1, FIA.2 and FIA.3
Confidentiality	The TOE shall ensure the confidentiality of the stored data with respect to any unauthorized user.	FDP.2, FDP.4
Integrity	The TOE shall ensure the integrity of the stored data.	FDP.3, FDP.5
Availability	The TOE shall ensure the availability of the offered service.	FRU.2

Audit	The TOE shall audit the critical events that inform about the correct functioning of the application	FAU.1, FAU.2 and FAU.3
Secure state	The TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal data or user data	FPT.1, FPT.4, FPT.5
Information back-up	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	FDP.2, FDP.3, FDP.4 and FDP.5
Security of system documentation	System documentation should be protected against unauthorized access.	FAU.4
Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	FAU.4
Administrator and operator logs	System administrator (Officer) activities should be logged.	FAU.4
Fault logging	Faults should be logged, analyzed, and appropriate action taken.	FAU.4
User registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	FIA.1, FIA.3
Privilege management	The allocation and use of privileges (Officer and Auditor) should be restricted and controlled.	FIA.2
Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	FRU.1
Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	FPR

Table 10: security objectives for the TOE.

3.6. Security requirements implemented by PRISMACLOUD services

PRISMACLOUD services will implement the following security requirements: user authentication, confidentiality, and data protection and privacy of personal information. This will serve as countermeasures to threat scenarios 3, 9, 10, 13, 14, 15, 16, 19, 20, 22, 23 defined in Table 11. The PRSIMACLOUD service secure archiving is an instantiation of the PRSIMACLOUD Secure Object Storage Tool and tailored to fulfill the backup and archiving requirements in the e-Government use case [3].It provides the following features:

- Availability: backups are outsourced to n different cloud providers. Therefore, availability is increased since information will be reachable as k (being k < n) servers are reachable. The Secure Archiving service [3] allows the customization of the k and n values to the needs of the organization.
- Privacy: the information stored in at least k servers needs to be disclosed in order to gain access to the original data. This way, privacy of the information is enhanced when compared to traditional single-server backups.

Reference	Threat scenario	Countermeasure	Risk level
TS3	Cloud's access network disruption (e.g. "cut" the cable)	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS9	Servers are seized by justice	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS10	Data are lost or erased	A mirror site is operated by a different cloud provider (distributed storage).	1. Negligible
TS13	Data can be modified by another tenant	Cryptographic mechanism for data integrity verification (MAC)	1. Negligible
TS14	Data stored in a server are not erased properly and are accessible to another tenant	Encryption of data	1. Negligible
TS15	Data are accessible to another tenant (*Trust Boundaries Overlapping)*	Encryption of data	1. Negligible

TS16	Servers are stolen and data can be extracted	Encryption of data	1. Negligible
TS19-TS22	An employee under the influence of a hacker modifies data (personal or access rights)	Cryptographic mechanism for data integrity verification (MAC)	2. Limited
TS20-TS23	An employee motivated by revenge discloses some data	Encryption of data	1. Negligible

Table 11: Threat scenarios thwarted by PRISMACLOUD services.

4. Conclusion

This document proposes security functional requirements for two typical scenarios using cloud infrastructures. The first scenario implements a parking management system dedicated to disabled persons. The application is hosted by a cloud service provider. Sensitive personal data may thus be manipulated by a third party. The second use case implements a service devoted to public bodies. The difference is that the cloud service provider is the same entity that manages the application offered to customers (public bodies).

The risk analysis related to these two scenarios were detailed in deliverable D2.4. This document builds upon these identified risks to propose security functional requirements (SFRs) that will mitigate them. The lists of SFRs are derived from the ISO/IEC 15408 standard (Common Criteria).

References

[1] PRISMACLOUD D2.4, "Progress report on threat analysis and security requirements", H2020 PRISMACLOUD, https://prismacloud.eu/, 2016.

[2] PRISMACLOUD D2.3, "Use Case Specification", H2020 PRISMACLOUD, https://prismacloud.eu/, 2016.

[3] PRISMACLOUD D6.4, "Selection and Specification of Tools for Software Implementation", H2020 PRISMACLOUD, https://prismacloud.eu/, 2016

[4] Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), "Part I – Introduction and General Model", September 2012.

[5] Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), "Part II – Security Functional Components", September 2012

[6] Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), "Part III – Security Assurance Components", September 2012

[7] ISO/IEC 27002:2013, "Information Technology - Security Techniques - Code of practice for information security management", International Organization for Standardization ISO, Genève, 2013.

[8] ISO/IEC 27018:2014, "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors", International Organization for Standardization ISO, Genève, 2014.

[9] SP 800-57, "Recommendations for Key Management", National Institute of Standardization and Technology (NIST)", 2007.

[10] Bundesamt für Sicherheit in der informationstechnikle (BSI), "Cloud Computing Compliance Controls Catalogue (C5)", https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html.

[11] Agence nationale de la sécurité des systèmes d'information (ANSSI), "Prestataires de services informatique en nuage (SecNumCloud) – Référentiel d'exigences – Niveau essentiel", 8th december 2016.

[12] Bundesamt für Sicherheit in der informationstechnikle (BSI), "Referencing Cloud Computing Compliance Controls Catalogue (C5) to International Standards", version 1.0, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/Referencing_Cloud_Computing_Compliance_Controls_Catalogue.pdf?__blob=publicationFile&v=2, 2016

