MICROSEC LTD.

PASSBY[ME] SERVER SYSTEM V1.2

SECURITY TARGET

COMMON CRITERIA / ISO 15408
EAL2

2017

Version:	1.7
Date:	11.10.2017
Reference:	PassBy[ME] Server Security Target 1.7
Classification:	Unclassified

History of Changes

Version	Date	Author	Checked	Approved	Comments
1.0	31.03.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Initial version
1.1	18.04.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Correction of threats and objectives
1.2	21.04.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Additions to rationales
1.3	25.04.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Formal changes
1.4	03.07.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Observed anomalies corrected in: Chap. 1.5.1, sec. 27, Chap 1.4.3, sec 24, Chap. 3.1.1, 3.2 Table 7, 8, 9, Chap. 6.1.3.4, New FDP_DAU_CPD_EXT
1.5	20.07.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Chap 1.5.1, Chap 6.1 and Glossary upgraded according to ROA PASSBYME-016
1.6	27.07.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	Formal changes in: Chap. 4.3, 5.2, 6.1.5.3
1.7	11.10.2017	Gábor MOLNÁR	Sándor SZŐKE dr.	Gergely VANCZÁK	PBM version changed to v1.2

Table of Contents

Table of Contents 3

1 Introduction (ASE_INT.1) 6
1.1 ST Overview 6
1.2 ST Reference 6
1.3 TOE Reference 7
1.4 TOE Overview 7
1.4.1 TOE usage and major security features 8
1.4.2 TOE type 9
1.4.3 Non-TOE hardware/software/firmware 9
1.5 TOE Description 11
1.5.1 Physical scope of the TOE 11
1.5.2 Logical scope of the TOE 14
1.5.2.1 Security Audit 16
1.5.2.2 User Data Protection 16
1.5.2.3 Identification and Authentication 18
1.5.2.4 Security Management 18
1.5.3 TOE life cycle 19

2 Conformance Claims (ASE_CCL.1) 21
2.1 Common Criteria conformance Claim 21
2.2 Package conformance claim 21
2.3 Protection Profile conformance claim 21

3 Security Problem Definition (ASE_SPD.1) 22
3.1 Assets, users and threat agents 22
3.1.1 Assets 22
3.1.2 Users 23
3.1.3 Threat agents 23
3.2 Threats 23
3.3 Organizational Security Policies 24
3.4 Assumptions 24

4 Security Objectives (ASE_OBJ.2) 26
4.1 Security Objectives for the TOE 26
4.2 Security Objectives for the Operational Environment 27
4.3 Security Objectives Rationale 28
4.4 Security Objectives Sufficiency 29

5 Extended Component Definition (ASE_ECD.1) 32
5.1 FDP_DAU_CPV_EXT.1 Certificate Processing 32
5.2 FDP_DAU_CPI_EXT.1 Certificate Path Initialization 33
5.3 FDP_DAU_CPD_EXT.1 Certification path development 34
5.4 FDP_ITC_SIG_EXT.1 PKI Signature Verification 34
5.5 FDP_DAU_OCS_EXT.1 Basic OCSP Client 34
5.6 FDP_DAU_CRL_EXT.1 Basic CRL Checking 36
5.7 FIA_UAU_SIG_EXT.1 Entity Authentication 37

6 Security Requirements (ASE_REQ.2) 39
6.1 TOE Security Functional Requirements 39
6.1.1 Use of requirement specifications 40

6.1.2 Class FAU – Security Audit 41
6.1.2.1 FAU_GEN.1 Audit Data Generation 41
6.1.2.2 FAU_GEN.2 User Identity Association 41
6.1.2.3 FAU_SAR.1 Audit Review 41
6.1.3 Class FDP – User Data Protection 42
6.1.3.1 FDP_ACC.1 Subset access control 42
6.1.3.2 FDP_ACF.1 Security attribute based access control 42
6.1.3.3 FDP_DAU_CPD_EXT.1 Certificate path development 43
6.1.3.4 FDP_DAU_CPI_EXT.1 Certificate path initialization 43
6.1.3.5 FDP_DAU_CPV_EXT.1 Certificate processing 43
6.1.3.6 FDP_DAU_CRL_EXT.1 Basic CRL checking 44
6.1.3.7 FDP_DAU_OCS_EXT.1 Basic OCSP client 45
6.1.3.8 FDP_ITC_SIG_EXT.1 Signature Verification 46
6.1.4 Class FIA – Identification and Authentication 47
6.1.4.1 FIA_AFL.1 Authentication failure handling 47
6.1.4.2 FIA_ATD.1 User attribute definition 47
6.1.4.3 FIA_UAU.2 User Authentication Before any Action 47
6.1.4.4 FIA_UAU_SIG_EXT.1 Entity Authentication 47
6.1.4.5 FIA_UID.2 User Identification Before any Action 48
6.1.5 Class FMT – Security Management 48
6.1.5.1 FMT_MSA.1 Management of Security Attributes 48
6.1.5.2 FMT_MSA.3 Static Attribute Initialization 48
6.1.5.3 FMT_SMF.1 Specification of Management Functions 49
6.1.5.4 FMT_SMR.1 Security Roles 49
6.1.6 Class FPT - Protection of the TOE Security Functions 49
6.1.6.1 FPT_ITT.1 Basic Internal Transfer Protection 49
6.1.6.2 FPT_STM.1 Reliable time stamp 49
6.2 TOE Security Assurance Requirements 50
6.3 Security Functional Requirements Rationale 51
6.4 Dependency Rationale 56
6.5 Rationale for chosen security assurance requirements 59
7 TOE Summary Specification (ASE_TSS.1) 60
7.1 TOE Security Functions 60
7.1.1 Security audit (TSF.Audit) 60
7.1.2 User data protection (TSF.Data_Protection) 60
7.1.3 Identification and Authentication (TSF.Identification) 61
7.1.4 Security Management (TSF.Management) 62
7.2 Fulfilment of the SFRs 63
7.2.1 Correspondence of SFRs and TOE mechanisms 64
8 Glossary and Acronyms 65
9 Bibliography 68

List of Tables

1. Table ST Organization 6
2. Table Threats for the TOE 24
3. Table Organizational Security Policies 24
4. Table Assumptions for the IT Environment 25
5. Table TOE Objectives 26
6. Table Environment Objectives 27
7. Table Mapping of security problem definitions to security objectives 28
8. Table Assumptions – Objectives mapping 30
9. Table Threats – Objectives mapping 31
10. Table Extended Requirements 32
11. Table Security Functional Requirements 40
12. Table Security Assurance Requirements: EAL2 50
13. Table Mapping of functional requirements to security objectives of the TOE 51
14. Table Security Objective to Functional Requirements mapping 56
15. Table Functional Requirements Dependencies 59
16. Table Mapping of SRFs to mechanisms of the TOE 64

List of Figures

1. Figure PassBy[ME] working environment 9
2. Figure TOE Boundaries 11
3. Figure Authentication process flow 15

1 Introduction (ASE_INT.1)

1.1 ST Overview

1 This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

2 Throughout this document, the terms PassBy[ME] and PBM refers to the PKI based server system solution (a third-generation authentication solution) of Microsec Ltd.

Section	Title	Description
1	Introduction	Provides an overview of the TOE and defines the software that make up the TOE as well as the physical and logical boundaries of the TOE.
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions or Packages where applicable.
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Defines the security objectives for the TOE operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats.
5	Extended Components Definitions	Describes extended components of the evaluation.
6	Security Requirements	Contains the functional and assurance requirements for this TOE.
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and it identifies the assurance measures targeted to meet the assurance requirements.

1. Table ST Organization

1.2 ST Reference

3 Title: PassBy[ME] Server System v1.2 Security Target (EAL2)

4 TOE: PassBy[ME] Server System v1.2

5 Author: Microsec Ltd., Gábor MOLNÁR

6 Version number: v1.7

7 Date: 11.10.2017.

8 The Security Target defines the security requirements of PassBy[ME] Server System v1.2.

9 Keywords: Security Target, Common Criteria, Authentication Server, Second factor Authentication, Mobile ID solution.

1.3 TOE Reference

10 The Security Target refers to the product "PassBy[ME] Server System v1.2" for CC evaluation.

11 TOE Name: PassBy[ME] Server System

12 TOE short name: PassBy[ME] / PBM

13 TOE Version: v1.2

14 Evaluation Criteria: Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004 [4]

15 Evaluation Assurance Level: EAL 2

16 Developer: Microsec Ltd.

17 Evaluation Sponsor: Microsec Ltd. 1031 Budapest, Záhony utca 7. D building

18 Keywords: Authentication Server, PKI based system, Second factor Authentication, Mobile ID solution.

1.4 TOE Overview

19 The TOE Overview summarizes the usage and major security features of the TOE.

The Target of Evaluation (TOE) is the PassBy[ME] Server System v1.2 consisting of the following logical server components:

- PUBLIC Server,
- Second Factor Authentication Subsystem (2FA),

- User Interface Management (UI MGMT),
- Certificate Enrollment Server (SCEP),
- Timestamper Subsystem,

and the associated guidance documents.

20 PassBy[ME] Server System is the server part of mobile based 2 factor authentication system.
The main functions of the server system are:

- Second factor authentication,
- Organization, User and Device management,
- Proof and signature validation and storage,
- Time stamp preparation,
- Certificate management,
- Instrumentation of the Messaging Server,
- Secure and reliable notification and message delivery.

1.4.1 TOE usage and major security features

21 PassBy[ME] is a PKI based mobile ID solution. It provides future-proof user authentication, transaction signing and mobile digital signature via high level security. The system consists of two parts:

- server service, called PassBy[ME] Server System (TOE), involving User and Application administration, enrollment control and storage of data for authentication and audit.
- client application running on a mobile device (this is not scope of this ST).

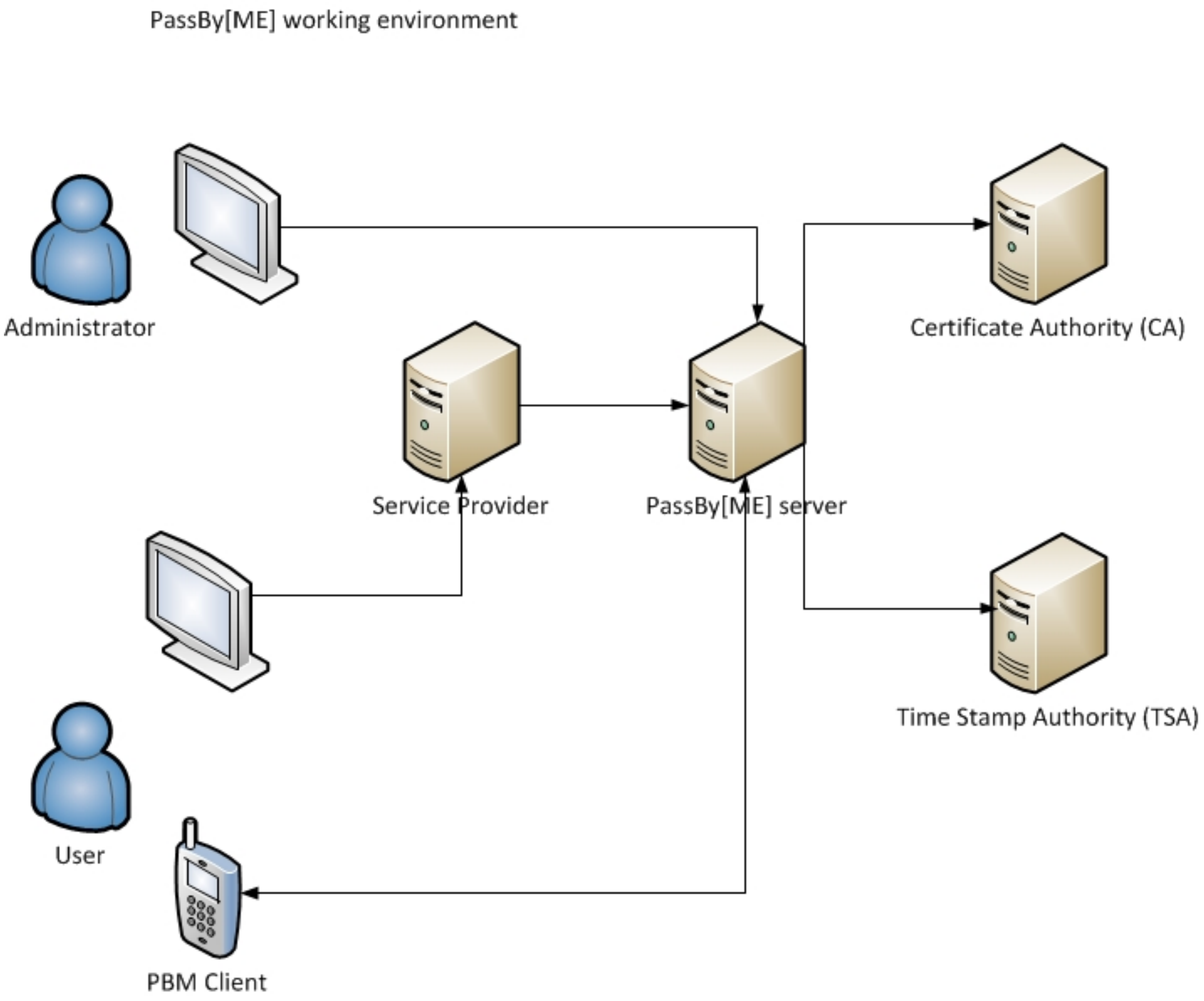
22 The characteristic features of the system are:

- Secure communication (TLS – RFC 5246),
- Certificate based authentication,
- 2 factor authentication for Organization administrators,
- User and Device management,
- Transaction authorization by electronic signature (XAdES),
- Trusted messaging, signed receipts of messages as proof of delivery,
- Timestamped evidences,
- auditing.

It provides the mobile- based second factor leg of an authentication scheme already implemented by an online service provider (e.g. online banking or cloud service login).

The client application running on the mobile device is not scope of this ST.

The Figure 1. illustrates the working environment of PassBy[ME].


PassBy[ME] working environment
Administrator
Certificate Authority (CA)
Service Provider
PassBy[ME] server
Time Stamp Authority (TSA)
User
PBM Client

1. Figure PassBy[ME] working environment

1.4.2 TOE type

23 The TOE is an authentication server system for mobile based second factor authentication.

1.4.3 Non-TOE hardware/software/firmware

24 The next software elements are required by the TOE to perform its claimed security features:

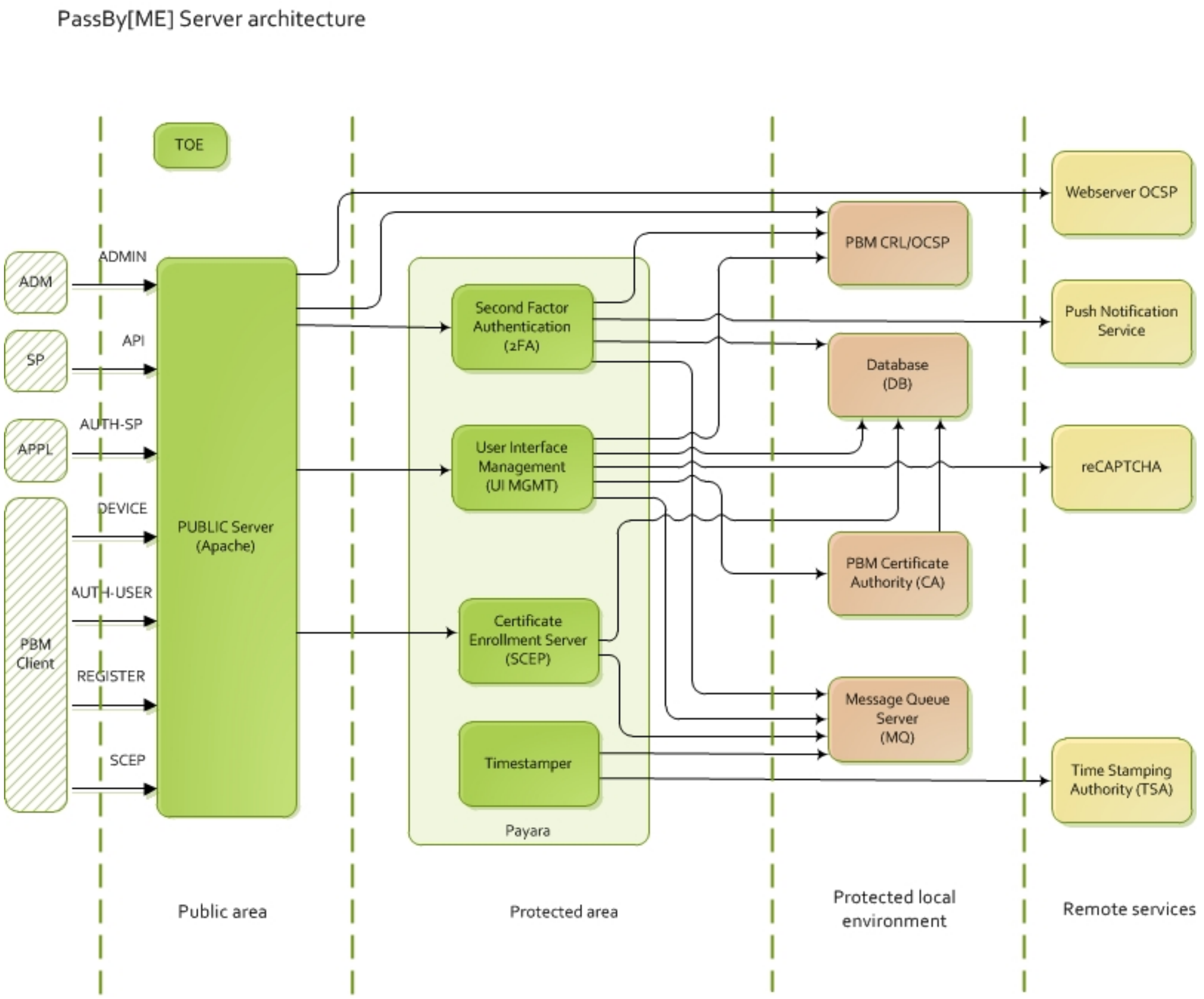
- Apache HTTP Server Version 2.4 (Apache)
  - The HTTP server with 7 virtual hosts builds the external interface of PBM.
- Payara Application Server Version 4.1.2 (Payara)
  - This application server wraps the PBM subsystems UI MGMT, 2FA, SCEP and Timestamper subsystems.
- Operating System Linux (RedHat, CentOS)
  - All the PBM server modules are running under the operating system Security Enhanced Linux.
- Relational Database (DB)
  - A relational database is used to store audit events, user's data, enrollment data and mobile messaging states.

- Certificate Authority (CA)
  - The Certificate Authority is responsible for issuing and administration of digital certificates.
- OCSP Responder (OCSP)
  - The Online Certificate Status Protocol server is used for obtaining the revocation status of digital certificates.
- Time Stamping Authority Server (TSA)
  - A Time Stamping Authority is issuing a trusted time stamp. The time stamp is used to prove the existence of certain data before a certain point without the possibility that the owner can backdate the time stamps.
- Message Queue Server (MQ)
- Push Notification Service (Apple, Google, Microsoft)
- Smartphone device (Apple IOS, Android, Windows)
- reCAPTCHA Human user check service

1.5 TOE Description

1.5.1 Physical scope of the TOE

25 The Figure 2. illustrates the physical scope and the physical boundary of the overall solution.


PassBy[ME] Server architecture
TOE
ADM
SP
APPL
PBM Client
ADMIN
API
AUTH-SP
DEVICE
AUTH-USER
REGISTER
SCEP
PUBLIC Server (Apache)
Second Factor Authentication (2FA)
User Interface Management (UI MGMT)
Certificate Enrollment Server (SCEP)
Timestamper
Payara
PBM CRL/OCSP
Database (DB)
PBM Certificate Authority (CA)
Message Queue Server (MQ)
Webserver OCSP
Push Notification Service
reCAPTCHA
Time Stamping Authority (TSA)
Public area
Protected area
Protected local environment
Remote services

2. Figure TOE Boundaries

26 Components of the TOE:

- PUBLIC Server (Apache)
  - The PUBLIC Server provides the external interface for the following services:
    - Web-based management interface: Accessible through HTTPS connection, it requires second factor, PassBy[ME] authorization to provide full functionality.
    - Authentication and Management service API: Accessible after mutual certificate based authentication (RFC 5246).

        - Authorization interface for the mobile applications: Accessible after mutual certificate based TLS authentication.

- Second Factor Authentication Subsystem (2FA)
    - This subsystem controls the process of the second factor authentication. It accepts the requests from the Service Provider and based on the delivered user-id communicates with the user's mobile device. The user's decision is signed and sent back using a mutually authenticated channel.
- User Interface Management (UI MGMT)
    - All the external administration requests arriving through the PUBLIC Server will be processed in this subsystem. Its main task is the management of Users and Organization administrators (organization management), signature validation, certificate management, instrumentation of the Messaging Server, as well as storing the audit relevant data.
- Certificate Enrollment Server (SCEP)
    - Mobile devices use the Simple Certificate Enrollment Protocol (SCEP) to request certificates for their on-board generated keys. In addition to the original SCEP specification the communication is tunneled through an TLS channel, where the server is authenticated. The enrollment process serves to bind a mobile device to a user.
- Timestamper
    - To provide long-term validity of the generated proofs, the PassBy[ME] system applies time stamps on the signed proofs. The Timestamper Subsystem creates the time stamps using the service of a TSA.

27 The hatched boxes (ADM, SP, APPL, PBM Client) are the clients, communicating with the PassBy[ME] Server. The notations mean:

- ADM – Organization administrator using Administration GUI,
- SP – Service Provider of an Organization using the Management API,
- APPL – Application of an Organization performing the messaging,
- PBM Client – PassBy[ME] client application on a mobile device.

28 Parts of the TOE are some shell scripts and configuration files forming the guidance:

- Initialization scripts of the PUBLIC Server,
- Configuration files of the PUBLIC Server,
- Initialization scripts of the Apache web server wrapping the Payara application server,

- Configuration files of the Apache web server wrapping the Payara application server,
- Initialization scripts of Payara application server,
- Configuration files of Payara application server,
- Trusted certificates for Apache web servers,
- Intermediate certificates for Apache web servers,
- Configurations files for subsystems 2FA, UI MGMT, SCEP, and Timestamper.

29 The following components are needed for a complete working environment, but they are not parts of the TOE:

- Message Queue Server (MQ)
    - The PassBy[ME] system uses the OpenMQ software as a queue broker. It decouples the consumer modules (e.g. Timestamper) from the producers (e.g. 2FA subsystem).
- Relational Database (DB)
    - A relational database is used to store configuration- and dynamic-data of PBM, such as enrollment, messaging and certificate information.
- Certificate Authority (CA)
    - The Certificate Authority is responsible for issuing and administration of active and revoked digital certificates.
- Apache Web Server (Apache)
    - The Web Server is the communication interface for the PassBy[ME] Server System.
- Payara Application Server Version 4.1.2 (Payara)
    - This application server wraps the PBM subsystems UI MGMT, 2FA, SCEP and Timestamper subsystems.
- Operating System Linux (RedHat, CentOS)
    - All the PBM server modules are running under the operating system Security Enhanced Linux.
- OCSP Responder (OCSP)
    - The PassBy[ME] system relies on the Online Certificate Status Protocol service (OCSP Responder) of the used CA infrastructure, its task is to check the revocation state of certificates.
- Time Stamping Authority Server (TSA)
    - A trusted third party (TTP) acting as a Time Stamping Authority (TSA) may issue a trusted time stamp.
- Push Notification Service (Apple, Google, Microsoft)
    - The PassBy[ME] system uses external push notification services to notify mobile devices about messages. These services are not required, they only complement it to enhance the user experience.
- Smartphone device (Apple IOS, Android, Windows)

    - Smartphone devices are needed to run the client application of PassBy[ME].
- reCAPTCHA Human user check service
    - reCAPTCHA protects the Administration GUI interface against spam and other types of automated abuse.

30 The external interface of the TOE is the PUBLIC Server. This interface makes possible for the mobile device and service provider to communicate with the PassBy[ME] server. For the communication, secure HTTPS channels will be used. The PUBLIC Server contains more virtual hosts, which are specialized for a given message type or task. Depending on the required task the message will be passed to the subsystem UI MGMT, 2FA or SCEP. To validate the certificate of the users OCSP or CRL service will be used.

31 The messages of the Users, which contain answer or decision will be timestamped and stored in the system. For the PKI functions OCSP, CA, Time stamping external services will be used. For internal PKI functions, like SSL and certificate handling the Java built-in functions and libraries of OpenSSL and BouncyCastle will be used.

32 Additional external services, as database and message queue server, will be needed to fulfil the required functionality. To improve the communications with the mobile device a push notification service expands the list of external services.

1.5.2 Logical scope of the TOE

33 As introduction to logical functions of the TOE let's see a typical use case:

Each user receives his or her private key generated on the smartphone device. This guarantees that the private key exists in only one copy. In an e-Commerce scenario, when making an online purchase the payment provider bank will then validate the transaction by requesting a second authentication through the smartphone. The customer will receive an alert on his mobile device and a request to authorize the transaction. The customer will be able to confirm or reject the transaction. The bank or the payment provider will only authorize the transaction if the customer authentication was successful and the customer confirmed the online transaction.

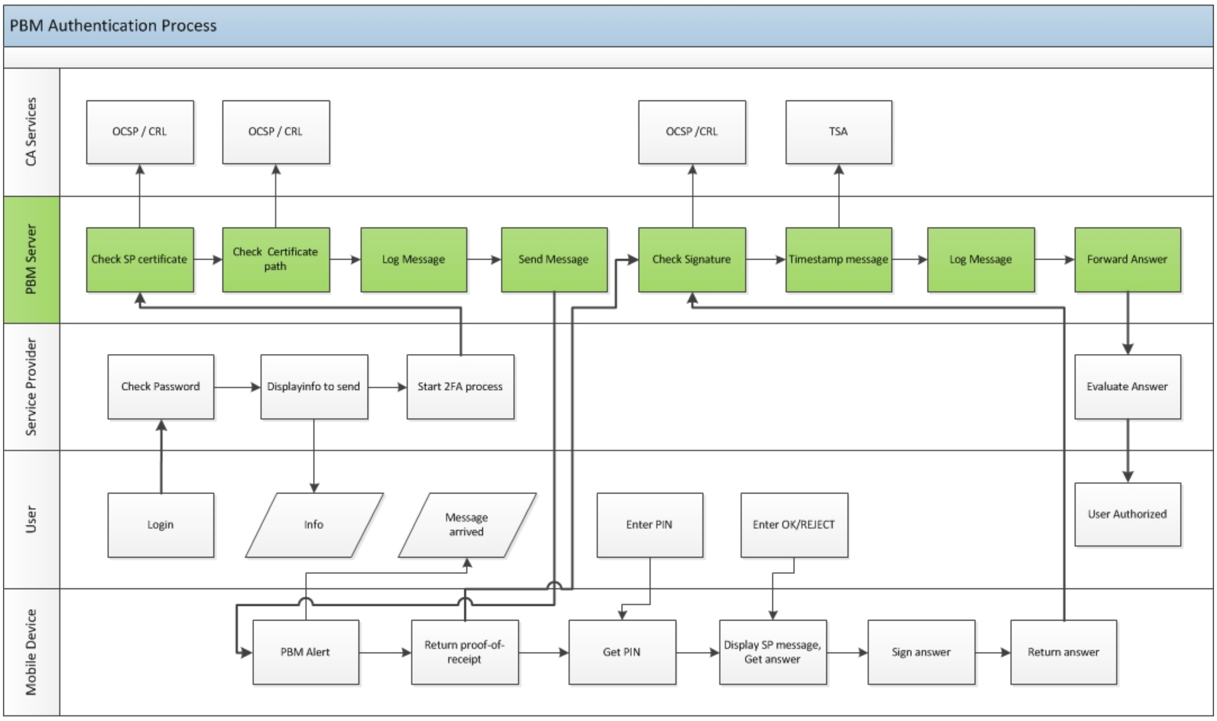
34 Life-cycle of a User
A User is the real customer of the PassBy[ME] system. He is always member of an organization. The activities of a User within PBM can be divided in four phases, which mean four processes:

- registration: the User will be entered in the system (in the Service Provider and in the PassBy[ME] server),
- enrollment: a mobile device will be assigned to the User, with a private key generated on board,

- authorization: The Service Provider asks the User for her/his acceptance or rejection in a given subject,
- deletion: the certificate of the User will be revoked, and her/his data on the server will be deleted.

The main operational task of PBM is to provide service for the second factor authentication.

The Figure 3. shows the process flow in the case of a by User initiated authentication.



3. Figure Authentication process flow

35 In the operational use of the TOE the following security features will be applied:

- PKI Based Entity Authentication
  - Every incoming connection to the TOE uses TLS to protect the communication. Mutual certificate based TLS authentication is used where applicable to provide strong client authentication.
- PKI Signature Verification
  - Transaction authorization relies on digital signatures. The User's mobile device receiving a message sends automatically a signed proof-of-receipt to the server. Then the User's decision about accepting or rejecting a transaction will be signed by the private key stored in the mobile device and will be sent to the server too.
- Certificate Path Validation

  - All the used certificates must be checked in the server for authenticity. A certificate may be accepted only if the whole path to the root certificate can be validated. For validation, the services OCSP or CRL will be used.
- Online Certificate Status Protocol Client
  - To get the actual status of a certificate the service of an OCSP responder will be used. It is configurable which method (OCSP or CRL) for certificate check will be applied.
- Certificate Revocation List (CRL) Validation
  - CRL Validation is one of the possibilities to check the state of a certificate.
- Audit
  - It generates audit log about the activities of the Organization administrators, about the communication events, and about the User signed transactions. To extend the validity of the user-signed proofs, the TOE time stamps all the signed proofs. Creating time stamp the external service of a Time Stamp Authority (TSA) will be used.

36 The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management.

1.5.2.1 Security Audit

37 The TOE keeps track about all the important events occurred in the system. The activities of the Organization administrators will be logged in the database with a time marker. The User's transactions will be timestamped and stored in PKCS#7 form (Cryptographic Message Syntax Standard).

1.5.2.2 User Data Protection

38 User data protection defines how users of the TOE can perform operations on objects.

User data are to be found:

- in messages
  - Outside of PassBy[ME] the message channels are protected by TLS. Inside the PassBy[ME] no secure channels will be used, but the whole system is physically protected and so it is running in secure environment.

- in database
    - The user data are stored in the database and they may be accessed by Organization administrators with limited scope.
- In filesystem
    - The transaction data signed by the User and timestamped by PBM server are stored in filesystem and so they are protected against any modifications.

39 *Access of administrators*

The System administrator has a trusted role, and is responsible for the whole system. Each Organization administrator can manipulate only the data of her/his organization.

40 *Types of user data*

PassBy[ME] handles only a minimal amount of user related data and requires no confidential data to operate. Most of the data used during the operation is generated within the system and has no meaning outside the PassBy[ME] systems context. PassBy[ME] processes the external data below.

Items in **bold** are validated and must be meaningful outside the PassBy[ME] system.

External data of PBM:

- user related data
    - username
    - full name
    - email
    - phone number
    - phone name
    - aliases
- organization related data
    - name
    - **email**
- service provider related data
    - application name
- data in messages
    - user-id
    - text from SP

1.5.2.3 Identification and Authentication

41 *Use of certificates*

All the Users, mobile devices (Devices) and Service Providers are authenticated and identified by certificates, which have been issued by a configured CA of PassBy[ME].

Online Certificate Service Provider or CRL is used to check the validity of certificates.

The Organization administrators use username/password and they must pass a second factor authentication using PassBy[ME] to access the web based administration interface.

Only Service Providers holding a valid authentication certificate can perform management operations through the API.

42 *Use of shared secrets*

The PassBy[ME] system uses shared secrets to strengthen the security of processes where PKI is not applicable.

In the following cases shared secrets, generated by PassBy[ME], will be used:

- Organization administrator invitation code,
- Organization administrator activation code,
- Device enrollment ID,
- SCEP challenge password,
- Device deactivation code.

1.5.2.4 Security Management

43 In the PassBy[ME] system all the important security parameters are adjustable to comply with the requirements of the hosting environment.

As a main security component of the PassBy[ME] system is the underlying PKI infrastructure. All parameters of a typical PKI infrastructure are configurable like:

- Key length of CA certificates,
- Key length of TLS certificates,
- Key length of API authentication certificates,
- Key length of the mobile client certificates,
- Certificate validity periods.

The PassBy[ME] system applies validity periods on several processes to protect them. These timeouts depend on the supplied configuration or input parameters:

- Validity of enrollment sheets and SCEP challenges,
- Validity of Organization administrator invitation codes,

- Validity of Organization administrator activation codes,
- Validity of authentication sessions.

The PassBy[ME] system uses shared secrets to strengthen the security of processes where PKI is not applicable. The key-length of these secrets is configurable by System administrator, namely:

- The length of Organization administrator invitation codes,
- The length of Organization administrator activation codes,
- The length of enrollment ID-s,
- The length of SCEP challenges,
- The length of Device deactivation codes.

1.5.3 TOE life cycle

44 In the life-cycle of the TOE there are the following phases and their steps:

- Development (performed by Developer):
    - TOE Development,
    - Developer test,
- Manufacturing (performed by System Administrator):
    - Packaging,
    - System test,
    - Documentation of the version,
    - Delivery,
- Deployment (performed by System administrator):
    - TOE installation,
    - Integration (connections with the environment),
    - System configuration,
    - Key pair generation (for authentication),
- Personalization (performed by Organization administrator):
    - Configuration of organizations,
    - Creating keys and certificates for users, and Applications (Service Providers),
- Operation (used by Organization administrator, Application and Users):
    - Providing authentication service,
    - Adding and removing Users,
    - Renewing, revoking certificates,

- Termination (performed by Organization administrator):
    - Revoking all certificates,
    - Deleting all Users.

2 Conformance Claims (ASE_CCL.1)

2.1 Common Criteria conformance Claim

45 This Security Target is conforming to the Common Criteria Part 1 version 3.1 Revision 4 ([1]).

46 This Security Target is conforming to Common Criteria Part 2 version 3.1 Revision 4 extended ([2]).

47 This Security Target is conforming to the Common Criteria Part 3 version 3.1 Revision 4 ([3]).

2.2 Package conformance claim

48 This Security Target claims strict conformance to the following package:

- Evaluation Assurance Level EAL2.

2.3 Protection Profile conformance claim

49 The TOE does not claim conformance to any registered Protection Profile.

3 Security Problem Definition (ASE_SPD.1)

50 This section describes the security aspects of the environment in which the TOE will be used and the way the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment,
- Organizational security policies with which the TOE must comply,
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.1 Assets, users and threat agents

51 The main task of the TOE is to assure a second factor authentication (2FA) for organizations. In this process, the TOE must be able to prove what was the User's answer for a given question sent by an organization (Service Provider). The answer is authenticated by the private key of the User, but timestamped in the TOE. The signing of the answer takes place in the mobile device, so out of scope of this ST.

The real asset of the TOE is the signed and timestamped answer of the User.

Performing the authentication service for customer the TOE should identify the communication parties (Applications, Users, Devices, Organization administrators) mainly based on certificates. Therefore, it is important the management of certificates and their validation.

3.1.1 Assets

52 **Timestamped signed evidences**

All the messages authenticated by User’s signature will be timestamped and stored by PBM. There are two types of messages coming from the User. The first type is a proof-of receipt signed by the client application, which means, that the message has arrived in the User’s Device. The second type is the User’s answer, also signed by the private key stored in the Device. These are the proofs of the performed transactions.

53 **Organization administrator’s password**

The Organization administrators need a password to log in.

54 **Configuration files**

The configuration files of the PUBLIC Server enforce the client certificate based authentication and controls its work.

55 **CA certificates**

Authentication certificates are allowed only from configured CAs. The allowed CA certificates (root and intermediate) are stored in a protected area, set up at installation by System administrator.

3.1.2 Users

56 **System administrator**

The System administrator can manage the configuration and the environment of PBM.

57 **Organization administrator**

The Organization administrator manages all the Users and other Organization administrators of the organization via the web-based administrator interface.

58 **User**

The User is a member of an organization willing to use PassBy[ME] as a second factor for authentication while accessing an Application. The Users communicate via messages with the PBM server.

3.1.3 Threat agents

59 **Attackers**

They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.

It is assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE.

3.2 Threats

60 This chapter lists the threats of the TOE caused by threat agents.

Threat Name	Description
T.Audit_Compromise	An attacker may cause audit records to be lost or modified, thus masking a User’s action. Threat agent: attacker, asset: evidence document, adverse action: denial of an executed action.

T.Crypto_Compromise	An attacker may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms. Threat agent: attacker, asset: CA certificates, adverse action: replace or add CA certificates allowing illegal API access.
T.Masquerade	An attacker may masquerade as another entity to gain unauthorized access to data or TOE resources. Threat agent: attacker, asset: password, adverse action: illegal access as Organization administrator.
T.Wrong_Certificate	A revoked or expired certificate of an attacker could be used as valid, resulting in security compromise. Threat agent: attacker, asset: configuration files, adverse action: illegal access to an organization data.

2. Table Threats for the TOE

3.3 Organizational Security Policies

61 An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

OSP Name	Description
P.Accountability	The authorized users of the TOE shall be held accountable for their actions within the TOE.

3. Table Organizational Security Policies

3.4 Assumptions

62 This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Assumption Name	Description
A.Configuration	The TOE will be properly installed and configured.
A.Physical	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.
A.No_Evil	Authorized System and Organization administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain the TOE and follow all guidance.
A.Database	The TOE needs a secure and reliable database service to store the audit logs and to manage the needed activities.
A.Private_Key	The private keys inside and outside of the TOE are well protected, it can be used only by its owner.
A.OCSP	An authorized source for OCSP delivers accurate and current OCSP responses, which will be stored locally with the expiration date.
A.CRL	An authorized source for CRL delivers accurate and current revocation information, which will be stored locally with the expiration date.
A.Systemtime	A reliable system time will be provided by the environment.

4. Table Assumptions for the IT Environment

4 Security Objectives (ASE_OBJ.2)

63 Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition above. The set of security objectives for a TOE form a high-level solution to the security problem. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

64 The specific security objectives for the TOE are as follows:

Security Objective Name	Description
OT.Audit	The TOE must record the actions taken by Organization administrators and provide the authorized System and Organization administrators with the ability to review and sort the audit trail.
OT.Admin	The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users may exercise such control.
OT.Auth_OCSP	The TOE shall accept the revocation information from an authorized source for OCSP transactions.
OT.Auth_CRL	The TOE shall accept the revocation information from an authorized source for CRL.
OT.Certificates	The TSF shall only accept certificates, which are verifiable, not expired and not revoked.
OT.Availability	The TSF shall continue to provide security services even if revocation information is not available.
OT.Trusted_Keys	The TSF shall use trusted public keys in certification path validation.
OT.Path_Find	The TSF shall be able to find a certification path from a trust anchor to the subscriber.
OT.I&A	The TSF shall uniquely identify all entities, and shall authenticate the claimed identity before granting an entity access to the TOE facilities.

5. Table TOE Objectives

4.2 Security Objectives for the Operational Environment

65 The following IT security objectives are to be satisfied by the environment:

Security Objective Name	Description
OE.Audit_Generation	The IT Environment will provide the capability to detect and create records of security-relevant events associated with users.
OE.Audit_Protection	The IT Environment will provide the capability to protect audit information.
OE.Configuration	The TOE will be installed and configured properly for starting up the TOE in a secure state.
OE.Timestamp	The TOE Environment must provide reliable time stamps for the TOE's use.
OE.No_Evil	The TOE environment will ensure that System and Organization administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.Physical	The non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks.
OE.TOE_Access	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

6. Table Environment Objectives

4.3 Security Objectives Rationale

66 The following table presents the coverage of security objectives.

Objectives	OT.Admin	OT.Auth_OCSP	OT.Auth_CRL	OT.Certificates	OT.Trusted_Keys	OT.Path_Find	OT.I&A	OE.Audit_Generation	OE.Audit_Protection	OE.Configuration	OE.Timestamp	OE.No_Evil	OE.Physical	OE.TOE_Access
Threats, Policy, Assumptions														
T.Audit_Compromise							X		X				X	
T.Crypto_Compromise		X	X		X		X			X	X		X	
T.Masquerade	X	X	X				X						X	X
T.Wrong_Certificate				X	X	X	X			X	X		X	
P.Accountability								X	X		X			
A.Configuration										X				
A.Physical													X	
A.No_Evil												X		
A.Database									X					
A.Private_Key										X			X	
A.OCSP										X				
A.CRL										X				
A.Systemtime											X			

7. Table Mapping of security problem definitions to security objectives

4.4 Security Objectives Sufficiency

67 The following discussion provides detailed evidence of coverage for each assumption, policy and threat,

Assumptions	Objectives	Rationale
A.Configuration	OE.Configuration	For correct and reliable work of the TOE it is necessary, that it is properly installed and configured. The OE.Configuration objective ensures, that the TOE will be properly installed and configured.
A.Physical	OE.Physical	The TOE and its coupled components (e.g. Database) need a physically secure environment. The OE.Physical ensures, that the TOE resides in a protected environment and under physically controlled access.
A.No_Evil	OE.No_Evil	Authorized System and Organization administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain the TOE and follow all guidance.
A.Database	OE.Audit_Protection	The TOE needs a secure and reliable database service to store the audit logs and to manage the needed activities. The TOE environment shall protect all the audit data including the database.
A.Private_Key	OE.Configuration, OE.Physical,	The physical protection of the whole system and the controlled access to it ensures, that the stored and transferred private data can be used only by its owner.
A.OCSP	OE.Configuration	Accurate and current revocation information is the basis for revocation checks. The System administrator configures trusted and authorized OCSP responder, which completes the assumption A.OCSP.

Assumptions	Objectives	Rationale
A.CRL	OE.Configuration	Accurate and current revocation information is the basis for revocation checks. The System administrator configures trusted and authorized CA for CRL service, which completes the assumption A.CRL.
A.Systemtime	OE.Timestamp	The IT Environment will provide reliable time for the TOE, which will be used at checking the certificate expiration and revocation information.
P.Accountability	OE.Audit_Generation, OE.Audit_Protection, OE.Timestamp	The P.Accountability policy is fulfilled by the generation and preservation of audit logs, timestamped based on the reliable time provided by the environment.

8. Table Assumptions – Objectives mapping

Threats	Objectives	Rationale
T.Audit_Compromise	OT I&A, OE.Audit_Protection, OE.Physical	The generated audit records of the TOE will be stored in a protected and secure database. Only the Organization administrators may read these data, modifications or deletes are not allowed.
T.Crypto_Compromise	OT.Trusted_Keys, OT.I&A, OT.Auth_OCSP, OT.Auth_CRL, OE.Configuration, OE.Timestamp, OE.Physical	The proper installation and configuration of trusted public keys and cryptographic libraries ensures that the system starts in a reliable state. The physical protection and the controlled access of the TOE prevents it against attacks of cryptographic functionalities.
T.Masquerade	OT.Admin, OT.I&A, OT.Auth_OCSP, OT.Auth_CRL, OE.Physical, OE.TOE_Access,	To prevent the TOE against unauthorized access there are mechanisms of the environment and that of the TOE. All the connected entities (Users, Organization administrators, Applications) will be secure authenticated and identified. To authenticate the Users and Applications certificates will be used. The Organization administrators use id/password and a second factor authentication based on PBM. The identified entities get access only to facilities according to their identity.
T.Wrong_Certificate	OT.Certificates OT.Trusted_Keys, OT.Path_Find, OT I&A, OE.Configuration, OE.Physical, OE.Timestamp	Certificates used for authentication and signature checking will be proofed using trusted public keys and reliable revocation information. The steps are: - certificate expiration - certificate path validity - certificate revocation

9. Table Threats – Objectives mapping

5 Extended Component Definition (ASE_ECD.1)

68 Requirements are drawn from the CC Parts 2 and 3 where possible. Extended requirements have been added for some needed requirements.

Extended requirements are identified as “Part 2 extended” and their name ends with "EXT" interpretation tag.

Requirement	Name	Extension
FDP_DAU_CPV_EXT.1	Certificate processing	Part 2 extended
FDP_DAU_CPI_EXT.1	Certification path initialization	Part 2 extended
FDP_DAU_CPD_EXT.1	Certification path development	Part 2 extended
FDP_ITC_SIG_EXT.1	PKI Signature Verification	Part 2 extended
FDP_DAU_OCS_EXT.1	Basic OCSP Client	Part 2 extended
FDP_DAU_CRL_EXT.1	Basic CRL Checking	Part 2 extended
FIA_UAU_SIG_EXT.1	Entity Authentication	Part 2 extended

10. Table Extended Requirements

5.1 FDP_DAU_CPV_EXT.1 Certificate Processing

69 Hierarchical to: No other components.

Dependencies: [FDP_DAU_CRL_EXT.1 or FDP_DAU_OCS_EXT.1].

FDP_DAU_CPV_EXT.1.1	The TSF shall reject a certificate if any of the following checks fails: a) Use parent-public-key, parent-public-key-algorithm-identifier, and parent-public-key-parameters to verify the signature on the certificate; b) notBefore field in the certificate < = TOI; c) notAfter field in the certificate > = TOI; d) issuer field in the certificate = parent-DN; or

	e) TSF can process all extensions marked critical.
FDP_DAU_CPV_EXT.1.2	The TSF shall bypass the revocation status check if the certificate contains no-check extension.
FDP_DAU_CPV_EXT.1.3	The TSF shall bypass the revocation check if the revocation information is not available and [selection of one or more by the ST author: *none, User, Organization administrator,* [assignment by the ST author*: other role(s) defined*]] overrides revocation checking.
FDP_DAU_CPV_EXT.1.4	The TSF shall reject a certificate if the revocation status using [selection of one or more by the ST author: *CRL, OCSP*].

5.2 FDP_DAU_CPI_EXT.1 Certificate Path Initialization

70 Hierarchical to: No other components.

Dependencies: FPT_STM.1.

FDP_DAU_CPI_EXT.1.1	The TSF shall use the trust anchor provided by [selection of one or more by the ST author: *User, Organization administrator,* [assignment by the ST author*: other role(s) defined*]].
FDP_DAU_CPI_EXT.1.2	The TSF shall obtain the time of interest called "TOI' from a reliable source [selection of one by the ST author: *local environment,* [assignment by ST author: *other sources defined by ST author*]].
FDP_DAU_CPI_EXT.1.3	The TSF shall perform the following checks on the trust anchor [selection of one or more by the ST author: • *None;* • *Subject DN and Issuer DN match;* • *Signature verifies using the subject public key and parameter (if applicable) from the trust anchor;* • *notBefore field in the trust anchor <= TOI;* • *notAfter field in the trust anchor => TOI*]

5.3 FDP_DAU_CPD_EXT.1 Certification path development

71 Hierarchical to: No other components.

Dependencies: None.

FDP_DAU_CPD_EXT.1.1	The TSF shall develop a certification path from a trust anchor provided by [selection of one or more by the ST author: *User; Organization administrator,* [assignment by the ST author*: other role defined*]] to the subscriber using matching rules for the following subscriber certificate fields or extensions: [selection of one or more by the ST author: *distinguished name, subject alternative names, subject key identifier, subject public key algorithm, certificate policies,* [assignment by the ST author*: other certificate fields or extensions*]].
FDP_DAU_CPD_EXT.1.2	The TSF shall bypass any matching rules except [selection of one or more by the ST author: *distinguished name, subject alternative names, subject key identifier, subject public key algorithm, certificate policies,* [assignment by the ST author*: other certificate fields or extensions, none*], *none*] if additional certification paths are required.

5.4 FDP_ITC_SIG_EXT.1 PKI Signature Verification

72 Hierarchical to: No other components.

Dependencies: None.

FDP_ITC_SIG_EXT.1.1	The TSF shall use the following information from the signed data [selection of one or more by the ST author: *hashing algorithm, signature algorithm, signer public key certificate, signer DN, signer subject alternative name, signer subject key identifier,* [assignment by the ST author*: other information*]] during signature verification.

5.5 FDP_DAU_OCS_EXT.1 Basic OCSP Client

73 Hierarchical to: No other components.

Dependencies: None.

FDP_DAU_OCS_EXT.1.1	The TSF shall formulate the OCSP requests in accordance with PKIX RFC 2560.
FDP_DAU_OCS_EXT.1.2	The OCSP request shall contain the following extensions: [selection of one or more by the ST author: *none, nonce,* [assignment by the ST author: *other extensions*]].
FDP_DAU_OCS_EXT.1.3	The TSF shall obtain the public key, algorithm, and public key parameters of the OCSP Responder from [selection of one by the ST author: *trust anchor, certificate signing CA, OCSP responder certificate,* [assignment by ST author: *other sources*]].
FDP_DAU_OCS_EXT.1.4	The TSF shall perform the following additional function [selection of one by the ST author: *1. none; or* 2. *establish trust in OCSP responder certificate using* [selection of one or more by the ST author: *certification path validation – basic, certification path validation – basic policy, certification path validation –policy mapping, certification path validation – name constraint*]]
FDP_DAU_OCS_EXT.1.5	The TSF shall invoke the cryptographic module to verify signature on the OCSP response using trusted public key, algorithm, and public key parameters of the OCSP responder.
FDP_DAU_OCS_EXT.1.6	The TSF shall verify that if the OCSP responder certificate contains extendedKeyUsage extension, the extension contains the PKIX OID for ocsp-signing or the anyExtendedKeyUsage OID.
FDP_DAU_OCS_EXT.1.7	The TSF shall match the responderID in the OCSP response with the corresponding information in the responder certificate.
FDP_DAU_OCS_EXT.1.8	The TSF shall match the certID in a request with certID in singleResponse.

FDP_DAU_OCS_EXT.1.9	The TSF shall reject the OCSP response for an entry if all the following are true: 1. time checks are not overridden; 2. [selection of one by the ST author: always, TOI > producedAt + x where x is provided by [selection by the ST author: *User, Organization administrator,* [assignment by the ST author: *other role(s) defined*]]]; 3. [selection of one by the ST author: *always, TOI > thisUpdate for entry + x where x is provided by* [selection by the ST author: *User, Organization administrator,* [assignment by the ST author: *other role(s) defined*]]]; and 4. [selection of one by the ST author: *always, TOI > nextUpdate for entry + x if nextUpdate is present and where x is provided by* [selection by the ST author: *User, Organization administrator,* [assignment by the ST author: *other role(s) defined*]]].
FDP_DAU_OCS_EXT.1.10	The TSF shall permit [selection of one or more by the ST author: *User, Organization administrator,* [assignment by the ST author: *other role(s) defined*], *none*] to override time checks.
FDP_DAU_OCS_EXT.1.11	The TSF shall reject OCSP response if the response contains “critical” extension(s) that TSF does not process

5.6 FDP_DAU_CRL_EXT.1 Basic CRL Checking

74 Hierarchical to: No other components.

Dependencies: None.

FDP_DAU_CRL_EXT.1.1	The TSF shall obtain the CRL from [selection of one or more by the ST author: *local cache, repository, location pointed to by the CRL DP in public key certificate of interest, User*, [assignment: *other locations defined by the ST author*]].

FDP_DAU_CRL_EXT.1.2	The TSF shall obtain the trusted public key, algorithm, and public key parameters of the CRL issuer.
FDP_DAU_CRL_EXT.1.3	The TSF shall invoke the cryptographic module to verify signature on the CRL using trusted public key, algorithm, and public key parameters of the CRL issuer.
FDP_DAU_CRL_EXT.1.4	The TSF shall verify that if a critical keyUsage extension is present in CRL issuer certificate, cRLSign bit in the extension is set in the certificate.
FDP_DAU_CRL_EXT.1.5	The TSF shall match the issuer field in the CRL with what it assumes to be the CRL issuer.
FDP_DAU_CRL_EXT.1.6	The TSF shall reject the CRL if all the following are true: a) Time checks are not overridden; b) [selection of one by the ST author: *always, TOI > thisUpdate + x where x is provided by* [selection by the ST author: *User, Organization administrator,* [assignment by the ST author: *other role(s) defined*]]]; and c) [selection of one by the ST author: *always, TOI > nextUpdate + x if nextUpdate is present and where x is provided by [selection by the ST author: User, Organization administrator, [assignment by the ST author: other role(s) defined*]]]
FDP_DAU_CRL_EXT.1.7	The TSF shall permit [selection by the ST author*: User, Organization administrator,* [assignment by the ST author*: other role(s) defined*]*, none*] to override time checks.
FDP_DAU_CRL_EXT.1.8	The TSF shall reject CRL if the CRL contains “critical” extension(s) that TSF does not process

5.7 FIA_UAU_SIG_EXT.1 Entity Authentication

75 Hierarchical to: No other components.

Dependencies: None.

FIA_UAU_SIG_EXT.1.1	The TSF shall invoke the cryptographic module with the following information from Certification Path Validation to verify signature on response from the entity to the challenge from the TSF: subject public key algorithm, subject public key, subject public key parameters.
FIA_UAU_SIG_EXT.1.2	The TSF shall verify that the keyUsage output from Certification Path Validation contains digitalSignature bit set.
FIA_UAU_SIG_EXT.1.3	The TSF shall apply the following additional checks [selection of one or more by the ST author: *a) Match the subject DN from the Certification Path Validation with the entity being authenticated.* b) *Match the subject alternative name from the Certification Path Validation with the entity being authenticated.* c) [assignment by the ST author: *other checks defined*]]

6 Security Requirements (ASE_REQ.2)

6.1 TOE Security Functional Requirements

76 This section specifies the SFRs for the TOE organized by CC class.

The TOE is part 2 extended. All functional requirements included in this Security Target are listed in Table 14. below. Extended requirements are identified as “Part 2 extended.” And their name ends with "EXT".

Security Functional Class	Security Functional Components	Origin
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation	Part 2
	FAU_GEN.2 User Identity Association	Part 2
	FAU_SAR.1 Audit Review	Part 2
User Data Protection (FDP)	FDP_ACC.1 Subset Access Control	Part 2
	FDP_ACF.1 Security Attribute Based Access Control	Part 2
	FDP_DAU_CPD_EXT.1 Certification path development	Part 2 Extended
	FDP_DAU_CPI_EXT.1 Certification path initialization	Part 2 Extended
	FDP_DAU_CPV_EXT.1 Certificate processing	Part 2 Extended
	FDP_DAU_CRL_EXT.1 Basic CRL Checking	Part 2 Extended
	FDP_DAU_OCS_EXT.1 Basic OCSP Client	Part 2 Extended
	FDP_ITC_SIG_EXT.1 PKI Signature Verification	Part 2 Extended
	FIA_AFL.1 Authentication Failure Handling	Part 2

Security Functional Class	Security Functional Components	Origin
Identification and Authentication (FIA)	FIA_ATD.1 User Attribute Definition	Part 2
	FIA_UAU.2 User Authentication Before any Action	Part 2
	FIA_UAU_SIG_EXT.1 Entity Authentication	Part 2 Extended
	FIA_UID.2 User Identification Before any Action	Part 2
Security Management (FMT)	FMT_MSA.1 Management of Security Attributes	Part 2
	FMT_MSA.3 Static Attribute Initialization	Part 2
	FMT_SMF.1 Specification of Management Functions	Part 2
	FMT_SMR.1 Security Roles	Part 2
Protection of the TOE Security Functions(FPT)	FPT_ITT.1 Basic internal TSF data transfer protection	Part 2
	FPT_STM.1 Reliable time stamps	Part 2

11. Table Security Functional Requirements

6.1.1 Use of requirement specifications

77 Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

78 **Refinement**.

The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions.~~

79 **Selection**.

The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

80 **Assignment**.

The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

81 **Iteration**.

The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b

6.1.2 Class FAU – Security Audit

6.1.2.1 FAU_GEN.1 Audit Data Generation

82 Hierarchical to: No other components.

Dependencies: FPT.STM.1 Reliable time stamps

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***minimum***] level of audit; c) [**none**]
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

6.1.2.2 FAU_GEN.2 User Identity Association

83 Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit Data Generation, FIA_UID.1 Timing of identification

FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2.3 FAU_SAR.1 Audit Review

84 Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1	The IT environment shall provide [**Organization administrator**] with the capability to read [**basic information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.3 Class FDP – User Data Protection

6.1.3.1 FDP_ACC.1 Subset access control

85 Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table below**].

Notes:

Subject	Object	Operation
System administrator	Organization administrators	Create/enable/disable
Organization administrator	Organization administrators, Users, Devices, Applications	Create/enable/disable
Application (SP)	Organization administrators, Users, Devices, Applications	Create/enable/disable

6.1.3.2 FDP_ACF.1 Security attribute based access control

86 Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset Access Control,
- FMT_MSA.3 Static Attribute Initialization.

FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**Organization administrator, Application**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

	a) Organization administrators will be identified by the OID of their certificate, sent with acknowledgement at 2FA, **b) Applications, Users and Devices will be identified by the OID in their authentication certificate**].

6.1.3.3 FDP_DAU_CPD_EXT.1 Certificate path development

87 Hierarchical to: No other components.

Dependencies: None

FDP_DAU_CPD_EXT.1.1	The TSF shall develop a certification path from a trust anchor provided by [***Organization administrator***] to the subscriber using matching rules for the following subscriber certificate fields or extensions: [***distinguished name, subject key identifier,*** [**none**]].
FDP_DAU_CPD_EXT.1.2	The TSF shall bypass any matching rules except [***distinguished name***] if additional certification paths are required.

6.1.3.4 FDP_DAU_CPI_EXT.1 Certificate path initialization

88 Hierarchical to: No other components.

Dependencies: FPT_STM.1.

FDP_DAU_CPI_EXT.1.1	The TSF shall use the trust anchor provided by [***Organization administrator***].
FDP_DAU_CPI_EXT.1.2	The TSF shall obtain the time of interest called “TOI’ from a reliable source [***local environment*****, NTP server**].
FDP_DAU_CPI_EXT.1.3	The TSF shall perform the following checks on the trust anchor [***Subject DN and Issuer DN match; notBefore field in the trust anchor <= TOI; notAfter field in the trust anchor => TOI***].

6.1.3.5 FDP_DAU_CPV_EXT.1 Certificate processing

89 Hierarchical to: No other components.

Dependencies: [FDP_DAU_OCS_EXT.1 or FDP_DAU_CRL_EXT.1].

FDP_DAU_CPV_EXT.1.1	The TSF shall reject a certificate if any of the following checks fails: 1. Use parent-public-key, parent-public-key-algorithm-identifier, and parent-public- key-parameters to verify the signature on the certificate; 2. notBefore field in the certificate < = TOI; 3. notAfter field in the certificate > = TOI; 4. issuer field in the certificate = parent-DN; or 5. TSF can process all extensions marked critical.
FDP_DAU_CPV_EXT.1.2	The TSF shall bypass the revocation status check if the certificate contains no-check extension.
FDP_DAU_CPV_EXT.1.3	The TSF shall bypass the revocation check if the revocation information is not available and [[***Organization administrator***]] overrides revocation checking.
FDP_DAU_CPV_EXT.1.4	The TSF shall reject a certificate if the revocation status using [***CRL or OCSP***] demonstrates that the certificate is revoked.

6.1.3.6 FDP_DAU_CRL_EXT.1 Basic CRL checking

90 Hierarchical to no other component.

Dependencies: None.

FDP_DAU_CRL_EXT.1.1	The TSF shall obtain the CRL from [***local cache***].
FDP_DAU_CRL_EXT.1.2	The TSF shall obtain the trusted public key, algorithm, and public key parameters of the CRL issuer.
FDP_DAU_CRL_EXT.1.3	The TSF shall invoke the cryptographic module to verify signature on the CRL using trusted public key, algorithm, and public key parameters of the CRL issuer.
FDP_DAU_CRL_EXT.1.4	The TSF shall verify that if a critical keyUsage extension is present in CRL issuer certificate, cRLSign bit in the

	extension is set in the certificate.
FDP_DAU_CRL_EXT.1.5	The TSF shall match the issuer field in the CRL with what it assumes to be the CRL issuer.
FDP_DAU_CRL_EXT.1.6	The TSF shall reject the CRL if all the following are true: 1. Time check are not overridden; 2. [***TOI > thisUpdate + x where x is provided by*** [[***Organization administrator***]]]; and 3. [***TOI > nextUpdate + x if nextUpdate is present and where x is provided by*** [[***Organization administrator***]]]**.**
FDP_DAU_CRL_EXT.1.7	The TSF shall permit [***Organization administrator***] to override time checks.
FDP_DAU_CRL_EXT.1.8	The TSF shall reject CRL if the CRL contains “critical” extension(s) that TSF does not process.

6.1.3.7 FDP_DAU_OCS_EXT.1 Basic OCSP client

91 Hierarchical to: No other component.

Dependencies: None.

FDP_DAU_OCS_EXT.1.1	The TSF shall formulate the OCSP requests in accordance with PKIX RFC 2560.
FDP_DAU_OCS_EXT.1.2	The OCSP request shall contain the following extensions: [[***none***]].
FDP_DAU_OCS_EXT.1.3	The TSF shall obtain the public key, algorithm, and public key parameters of the OCSP Responder from [***OCSP responder certificate***].
FDP_DAU_OCS_EXT.1.4	The TSF shall perform the following additional function [***establish trust in OCSP responder certificate using*** [***certification path validation – basic***].
FDP_DAU_OCS_EXT.1.5	The TSF shall invoke the cryptographic module to verify signature on the OCSP response using trusted public key, algorithm, and public key parameters of the

	OCSP responder.
FDP_DAU_OCS_EXT.1.6	The TSF shall verify that if the OCSP responder certificate contains extendedKeyUsage extension, the extension contains the PKIX OID for ocsp- signing or the anyExtendedKeyUsage OID.
FDP_DAU_OCS_EXT.1.7	The TSF shall match the responderID in the OCSP response with the corresponding information in the responder certificate.
FDP_DAU_OCS_EXT.1.8	The TSF shall match the certID in a request with certID in singleResponse.
FDP_DAU_OCS_EXT.1.9	The TSF shall reject the OCSP response for an entry if all the following are true: 1. time checks are not overridden; 2. [***TOI > producedAt + x where x is provided by*** [[***Organization administrator***]]***;*** 3. [***TOI > thisUpdate for entry + x where x is provided by*** [[***Organization administrator***]]***;*** and 4. [***TOI > nextUpdate for entry + x if nextUpdate is present and where x is provided by*** [[***Organization administrator***]]***.***
FDP_DAU_OCS_EXT.1.10	The TSF shall permit [***Organization administrator***] to override time checks.
FDP_DAU_OCS_EXT.1.11	The TSF shall reject OCSP response if the response contains "critical" extension(s) that TSF does not process.

6.1.3.8 FDP_ITC_SIG_EXT.1 Signature Verification

92 Hierarchical to no other component.

Dependencies: None.

FDP_ITC_SIG_EXT.1.1	The TSF shall use the following information from the signed data [***hashing algorithm, signature algorithm, signer public key certificate, signer DN, signer subject***

	key identifier] during signature verification.

6.1.4 Class FIA – Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication failure handling

93 Hierarchical to no other component.

Dependencies: FIA_UAU.2 User Authentication Before any Action

FIA_AFL.1.1	The TSF shall detect when [[**10**]] unsuccessful authentication attempts occur related to [**connection or login to the TOE**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**log the event with the data of the party**].

6.1.4.2 FIA_ATD.1 User attribute definition

94 Hierarchical to no other component.

Dependencies: None.

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password, Role, Certificate, Device**]**.**

6.1.4.3 FIA_UAU.2 User Authentication Before any Action

95 Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

.

6.1.4.4 FIA_UAU_SIG_EXT.1 Entity Authentication

96 Hierarchical to: No other components.

Dependencies: None.

FIA_UAU_SIG_EXT.1.1	The TSF shall invoke the cryptographic module with the following information from Certification Path Validation to verify signature on response from the entity to the challenge from the TSF: subject public key algorithm, subject public key, subject public key parameters.
FIA_UAU_SIG_EXT.1.2	The TSF shall verify that the keyUsage output from Certification Path Validation contains digitalSignature bit set.
FIA_UAU_SIG_EXT.1.3	The TSF shall apply the following additional checks [***match the subject DN from the Certification Path Validation with the entity being authenticated***].

6.1.4.5 FIA_UID.2 User Identification Before any Action

97 Hierarchical to: FIA_UID.1 Timing of identification.

Dependencies: None.

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Class FMT – Security Management

6.1.5.1 FMT_MSA.1 Management of Security Attributes

98 Hierarchical to: No other components

Dependencies:

- [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify***] the security attributes [**timeouts**] to [***Organization* administrators**].

6.1.5.2 FMT_MSA.3 Static Attribute Initialization

99 Hierarchical to: No other components

Dependencies:

- FMT_MSA.1 Management of Security Functions,
- FMT_SMR.1 Security Roles

FMT_MSA.3.1	The TSF shall enforce the [**access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

6.1.5.3 FMT_SMF.1 Specification of Management Functions

100 Hierarchical to: No other components.

Dependencies: None.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**organization management, administrator management, application management, user management, mobile device management**].

6.1.5.4 FMT_SMR.1 Security Roles

101 Hierarchical to: No other components.

Dependencies: FIA_UID.2 User Identification Before any Action.

FMT_SMR.1.1	The TSF shall maintain the roles [**User, Application, Organization administrator, System administrator**].

6.1.6 Class FPT - Protection of the TOE Security Functions

6.1.6.1 FPT_ITT.1 Basic Internal Transfer Protection

102 Hierarchical to: No other components

Dependencies: None.

FPT_ITT.1.1	The TSF shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE

6.1.6.2 FPT_STM.1 Reliable time stamp

103 Hierarchical to: No other components

Dependencies: None.

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

6.2 TOE Security Assurance Requirements

104 This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3. Table 13. – Security Assurance Requirements summarizes the requirements.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification

12. Table Security Assurance Requirements: EAL2

6.3 Security Functional Requirements Rationale

Objectives	OT.Audit	OT.Admin	OT.Auth_OCSP	OT.Auth_CRL	OT.Certificates	OT.Availability	OT.Trusted_Key	OT.Path_Find	OT.I&A
SFRs									
FAU_GEN.1	X								
FAU_GEN.2	X								
FAU_SAR.1	X								
FDP_ACC.1		X							X
FDP_ACF.1		X							X
FDP_DAU_CPD_EXT.1								X	
FDP_DAU_CPI_EXT.1							X		
FDP_DAU_CPV_EXT.1					X	X			
FDP_DAU_CRL_EXT.1				X					
FDP_DAU_OCS_EXT.1			X						
FDP_ITC_SIG_EXT.1									X
FIA_AFL.1									X
FIA_ATD.1									X
FIA_UAU.2									X
FIA_UAU_SIG_EXT.1									X
FIA_UID.2									X
FMT_MSA.1		X							X
FMT_MSA.3		X							
FMT_SMF.1		X							
FMT_SMR.1		X							X
FPT_ITT.1		X							X
FPT_STM.1	X								

13. Table Mapping of functional requirements to security objectives of the TOE

105 The mapping of all security objectives to functional requirements (components) with rationale is provided in Table 15.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations.

Security Objective	Mapped SFRs	Rationale
OT.Audit	FAU_GEN.1 Audit Data Generation	OT.Audit objective means, that the TOE must record the actions taken by Organization administrators and provide the authorized Organization administrators with the ability to review and sort the audit trail. The FAU_GEN.1 requirement ensures, that all activities of the Organization administrators will be logged with time, event type, subject identity and result.
	FAU_GEN.2 User Identity Association	The FAU_GEN.2 requirement ensures, that all the audit events are associated with the initiator (Organization administrator).
	FAU_SAR.1 Audit review	The FAU_SAR.1 requirement ensures, that the TOE provides the ability to review logs for the Organization administrators.
	FPT_STM.1 Reliable time stamps	Audit records need a reliable time stamps.
OT.Admin	FDP_ACC.1 Subset Access Control	Organization administrators are enforced to use login name and password. System administrators are controlled by the IT system, Organization administrator by the TOE.
	FDP.ACF.1 Security Attribute Based Access Control	Identification of Organization administrators is based on the enforced second factor authentication.
	FMT_MSA.1 Management of Security Attributes	OT.ADMIN objective specifies, that the TOE must include a set of functions that allow management of its functions and data. The FMT_MSA.1 requirement ensures, that only Organization

Security Objective	Mapped SFRs	Rationale
		administrators can modify the security attributes, such as key length.
	FMT_MSA.3 Static Attribute Initialization	The security attributes are configured by the System administrators. Some values are modifiable by the Organization administrator
	FMT_SMF.1 Specification of Management Functions	The required management tasks of the Organization administrator are specified by this requirement, such as organization management, administrator management, user management and mobile device management.
	FMT_SMR.1 Security Roles	This requirement ensures, that the TOE uses roles and only the Organization administrator role can perform management tasks.
	FPT_ITT.1 Basic internal TSF data transfer protection	Configuration values are stored in configuration files and database. Reading or modifying these values protected transfer is needed.
OT.Certificates	FDP_DAU_CPV_EXT.1 Certificate processing	The OT.Certificates claims, that only valid and not revoked certificates will be accepted by the TOE. This can be reached by a correct certificate processing specified by FDP_DAU_CPV_EXT.1.1. This objective is supported by the assumptions A.Configure, A.OCSP and A.CRL to ensure a reliable certificate validation.
OT.Availability	FDP_DAU_CPV_EXT.1 Certificate processing	OT.Availability claims, that TOE shall continue to provide security services even if revocation information is not available. The requirement FDP_DAU_CPV_EXT.1.2 expresses the

Security Objective	Mapped SFRs	Rationale
		same need. The revocation information will be stored and used from cache.
OT.Trusted_Keys	FDP_DAU_CPI_EXT.1 Certification path initialization	OT.Trusted_Keys states, that the TOE shall use trusted public keys in certification path validation. To complete this aim a proper certification path initialization is needed, which requires that the TSF use only trusted public keys in the certification path validation. The fulfilment of the objective is assisted by the assumption A.Configure.
OT.Path_Find	FDP_DAU_CPD_EXT.1 Certification path development	OT.Path_Find objective, which claims, that the TOE shall be able to find a certification path from a trust anchor to the subscriber, is covered by a correct certification path development requirement of FDP_DAU_CPD_EXT.1.1.
OT.I&A	FDP_ACC.1 Subset Access Control	The Organization administrators are enforced to authenticate and identify themselves.
	FDP.ACF.1 Security Attribute Based Access Control	The Applications and User should use certificates to authenticate and identify themselves.
	FDP_ITC_SIG_EXT.1 PKI Signature Verification	In the identification process of a signed evidence, the signature will be verified and the signer subject key identifier checked.
	FIA_AFL.1 Authentication Failure Handling	Detecting authentication failure in a connection or login, the process will be aborted and after a given number the event will be logged.

Security Objective	Mapped SFRs	Rationale
	FIA_ATD.1 User Attribute Definition	For identification purposes, some data about the Organization administrators and Users will be stored.
	FIA_UAU.2 User Authentication Before any Action	OT.I&A claims, that the TOE shall uniquely identify all entities, and shall authenticate the claimed identity before granting an entity access to its facilities. The FIA_UAU.2 requirement contains, that the user should be authenticated before allowing any action.
	FIA_UAU_SIG_EXT.1 Entity Authentication	To reach a secure authentication, the TOE should use certificate based authentication. This additional requirement enhances the security of the authentication process.
	FIA_UID.2 User Identification Before any Action	After the authentication, the users should be identified before allowing any actions, according to FIA_UID.2.
	FMT_MSA.1 Management of Security Attributes	Only administrators can change the security attributes. The System administrator can change the attributes stored in configuration files, and the Organization administrator some changeable attributes.
	FMT_SMR.1 Security Roles	All the users of the TOE have an assigned role.
	FPT_ITT.1 Basic internal TSF data transfer protection	In the authentication –identification process the request data will be transferred between PUBLIC Server and UI Management, which is protected.
OT.Auth_OCSP	FDP_DAU_OCS_EXT.1 Basic OCSP Client	OT.Auth_OCSP claims, that the TOE shall accept the revocation information from an authorized source for OCSP

Security Objective	Mapped SFRs	Rationale
		transactions. This aim will be reached by an OCSP client specified by FDP_DAU_OCS_EXT.1, which works in accordance with PKIX RFC 2560. The authorized source of OCSP responder will be configured by the System administrator according to OE.Configuration.
OT.Auth_CRL	FDP_DAU_CRL_EXT.1 Basic CRL Checking	OT.Auth_CRL claims, that the TOE shall accept the revocation information from an authorized source for CRL. It is covered by Basic CRL checking, which requires that the TSF accept revocation information from an authorized source. The authorized source of CRL will be configured by the System administrator according to OE.Configuration.

14. Table Security Objective to Functional Requirements mapping

6.4 Dependency Rationale

106 The following table provides an overview how the dependencies of the security functional requirements are solved and a justification why some dependencies are not being satisfied.

SFR	Required Dependencies	Inclusion
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	This dependency is met by the TOE Environment, which provides the time stamps for the TOE's use, as defined by OE.TIMESTAMP.
FAU_GEN.2 User Identity Association	FAU_GEN.1 Audit data generation	FAU_GEN.1

SFR	Required Dependencies	Inclusion
	FIA_UID.1 Timing of Identification	FIA_UID.2 is hierarchical to FIA_UID.1
FAU_SAR.1 Audit Review	FAU_GEN.1 Audit data generation	FAU_GEN.1
FDP_ACC.1 Subset Access Control	FDP.ACF.1 Security Attribute Based Access Control	FDP.ACF.1.
FDP.ACF.1 Security Attribute Based Access Control	FDP_ACC.1 Subset Access Control	FDP_ACC.1.
	FMT_MSA.3 Static Attribute Initialization	FMT_MSA.3.
FDP_DAU_CPD_EXT.1 Certification path development	None.	-
FDP_DAU_CPI.EXT.1 Certification path initialization	FPT_STM.1 Reliable time stamps	The dependencies related to this requirement are satisfied by the environment.
FDP_DAU_CPV.EXT.1 Certificate processing	[FDP_DAU_OCS_EXT.1 or FDP_DAU_CRL_EXT.1]	FDP_DAU_OCS_EXT.1 , FDP_DAU_CRL_EXT.1
FDP_DAU_CRL_EXT.1 Basic CRL Checking	None.	-
FDP_DAU_OCS_EXT.1 Basic OCSP Client	None.	-
FDP_ITC_SIG_EXT.1 PKI Signature Verification	None.	-

SFR	Required Dependencies	Inclusion
FIA_AFL.1 Authentication Failure Handling	FIA_UAU.2 User Authentication Before any Action	FIA_UAU.2
FIA_ATD.1 User Attribute Definition	None.	-
FIA_UAU.2 User Authentication Before any Action	FIA_UID.1 User Identification Before any Action	Included by FIA_UID.2, because it is hierarchical to FIA_UID.1.
FIA_UAU_SIG_EXT.1 Entity Authentication	None.	-
FIA_UID.2 User Identification Before any Action	None.	-
FMT_MSA.1 Management of Security Functions	FDP_ACC.1 Subset Access Control	FDP_ACC.1.
	FMT_SMF.1 Specification of management function	FMT_SMF.1 .
	FMT_SMR.1 Security Roles	FMT_SMR.1.
FMT_MSA.3 Static Attribute Initialization	FMT_MSA.1 Management of Security Functions	FMT_MSA.1.
	FMT_SMR.1 Security Roles	FMT_SMR.1
FMT_SMF.1 Specification of management function	None.	-
FMT_SMR.1 Security Roles	FIA_UID.1 User Identification Before any Action	FIA_UID.2 is hierarchical to FIA_UID.1

SFR	Required Dependencies	Inclusion
FPT_ITT.1 Basic internal TSF data transfer protection	None.	-

15. Table Functional Requirements Dependencies

6.5 Rationale for chosen security assurance requirements

107 EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices.

108 The chosen assurance level is appropriate with the threats defined for the environment. While the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2 the system will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

7 TOE Summary Specification (ASE_TSS.1)

109 This chapter gives the overview description of the different TOE Security Functions composing the TSF.

7.1 TOE Security Functions

7.1.1 Security audit (TSF.Audit)

110 The TOE Security audit functions cover the requirements FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FPT_STM.1 and FIA_UID.2.

111 The TOE keeps track of auditable events through database entries. Such events are all the activities of the Organization administrators (e.g. management of Users), the transactions of Applications (Service Providers are requesting second level authentication) and Users (responding to authentication requests). All the audited events are bound to an entity and marked with a time stamp. The Organization administrators can read the audited events of their own organization.

112 The TOE audit records contain the following information:

- Date/Time - Date and time the event occurred.
- Origination User - Username of the user that caused the event.
- Category - Category of the event.
- Description - Description of the event.

7.1.2 User data protection (TSF.Data_Protection)

113 The user data protection functions of the TOE implement the requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3 and FPT_ITT.1.

114 The TOE is running under virtual machine VMware ESXi 6.0 platform. The system is accepting external connection by means of Apache web-server. From outside not accessible are running the application servers and databases. The configuration and user data can be accessed only by the System administrator and by PBM server processes.

115 The user data protection is based on the secure communication with the connected entities. TLS channels with certificate based authentication are used for connections with Users, Organization administrators and Applications.

116 The Users and Applications will be authenticated with certificates, the Organization administrators with username/password and mobile device (as second factor authentication).

117 The certificate based authentication will be performed using trusted data, configured by the System administrator. The Apache server terminates the incoming requests and performs the certificate validation. There are 4 different ports with 4 different groups of certificates (issued by 4 different Sub-CAs) according to the different tasks to be performed. The authenticated connection will be forwarded to the application processes, where the entity will be identified.

118 The management of Users or organization data can be performed only by Organization administrators. They can create, modify or delete the Users of their own organization.

119 The transactions between Applications and Users will be certified by signed evidences. The User's Device sends a signed proof-of-receipt at receiving a message. This signed proof will be timestamped by a Time Stamping Authority and stored in the filesystem. The signed answer of a User will be timestamped and stored as evidence before forwarding it to the requesting Application.

7.1.3 Identification and Authentication (TSF.Identification)

120 The Identification and Authentication functions cover the requirements FDP_ACC.1, FDP_ACF.1, FDP_DAU_CPD_EXT.1, FDP_DAU_CPI_EXT.1, FDP_DAU_CPV_EXT.1, FDP_DAU_CRL_EXT.1, FDP_DAU_OCS_EXT.1, FDP_ITC_SIG_EXT.1, FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU_SIG_EXT.1, FIA_UID.2, FMT_MSA.3.

121 The basic authentication method of the TOE is certification based. A connected Application or User will be authenticated by its certificate. The expiration, validity and revocation of the certificate will be checked. This checking will be performed in the Apache server by using trusted anchor certificates. The method of certificate revocation checking is configured by the System administrator. According to the configuration, the server uses either OCSP or CRL connection of an authenticated CA to check the certificate status.

122 There are 4 different entry points for 4 different tasks of the PUBLIC Server to accept external connections. There are 4 groups of certificates which can be used for authentication. The certificate groups are identified by 4 different issuing Sub-CAs. The groups are:

- Messaging API for Service Providers (Applications)
- Management API for Service Providers (Application Management)
- Device connections (proof-of-receipt)

- User connections (user transactions)

123 In the case of certificate validity, the PUBLIC Server forwards the request to the core server, where the OID of the certificate will be used for identification. No activity of the entity will be allowed before finishing these steps.

124 In the case of Organization administrators, username and password will be used for authentication, extended with mobile device based second factor authentication. When an Organization administrator is logging in, after entering the correct username and password, receives an alert message in her/his mobile device application with an identification code, displayed also on the login screen. After having acknowledged this message the access will be allowed to the organization management.

125 The identification of the sending party will be performed either based on a checked certificate or after a two-factor authentication.

126 At User's transactions, the signature of the evidences will be validated to identify the User and to check her/his legitimacy.

7.1.4 Security Management (TSF.Management)

127 The Security Management functions cover the requirements FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1.

128 There are four roles within the PassBy[ME] system:

- System administrator,
- Organization administrator,
- Service provider (Application),
- User.

The System administrator is responsible for the installation and maintenance of the system and for the security configuration of the TOE stored in property files and database. The security attributes will be set at installation. The System administrator supervises the other Organization administrators and can review the system logs.

129 The Organization administrator can manage the organization-specific data, e.g. can manage the Users, can enable or disable Devices. Organization specific data are the timeout values for Device enrollment and Organization administrator invitation.

130 The Service Providers have access through Management API to organization data, they can perform similar activities as the Organization administrators.

131 The users are in position to receive and send messages via the PassBy[ME] system.

7.2 Fulfilment of the SFRs

Objectives	TSF.Audit	TSF.Data_protection	TSF.Identification	TSF.Management
SFRs				
FAU_GEN.1 Audit data generation	X			
FAU_GEN.2 User Identity Association	X			
FAU_SAR.1 Audit Review	X			
FDP_ACC.1 Subset Access Control		X	X	
FDP_ACF.1 Security Attribute Based Access Control		X	X	
FDP_DAU_CPD_EXT.1 Certification Path Development			X	
FDP_DAU_CPI_EXT.1 Certification Path Initialization			X	
FDP_DAU_CPV_EXT.1 Certificate Processing			X	
FDP_DAU_CRL_EXT.1 Basic CRL Checking			X	
FDP_DAU_OCS_EXT.1 Basic OCSP Client			X	
FDP_ITC_SIG_EXT.1 PKI Signature Verification			X	
FIA_AFL.1 Authentication Failure Handling			X	
FIA_ATD.1 User Attribute Definition			X	
FIA_UAU.2 User Authentication Before any Action			X	
FIA_UAU_SIG_EXT.1 Entity Authentication			X	
FIA_UID.2 User Identification Before any Action	X		X	
FMT_MSA.1				X

Management of Security Functions				
FMT_MSA.3 Static Attribute Initialization		X	X	X
FMT_SMF.1 Specification of Management Functions				X
FMT_SMR.1 Security Roles				X
FPT_ITT.1 Basic internal TSF Data Transfer Protection		X		
FPT_STM.1 Reliable time stamp	X			

16. Table Mapping of SRFs to mechanisms of the TOE

7.2.1 Correspondence of SFRs and TOE mechanisms

132 Each TOE security functional requirement is implemented by at least one TOE mechanism. In section 7.1 the implementing of the TOE security functional requirement is described in form of the TOE mechanism.

8 Glossary and Acronyms

133 **Abbreviations**:

2FA	**Second Factor Authentication** or Two-factor authentication is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication.
API	**Application Programming Interface**
CA	**Certificate Authority**
CAP	**Composed Assurance Package**
CC	**Common Criteria**
CM	**Configuration Management**
CRL	**Certificate Revocation List**
CRL DP	**Certificate Revocation List Distribution Point** A distribution point is either a directory path that identifies the location where the CRLs are published, or a fully qualified HTTP URL.
DAC	**Discretionary Access Control**
DB	**Database**
DN	**Distinguished Name** A subject DN is a unique name given to an X.509 certificate. It consists of several attribute-value pairs called Relative Distinguished Names (RDNs).
EAL	**Evaluation Assurance Level** of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation.
GUI	**Graphical User Interface**
HSM	**Hardware Security Module**
HTTP	**Hypertext Transfer Protocol**

	is an application protocol for distributed, collaborative, and hypermedia information systems.
HTTPS	**HTTP over Transport Layer Security** is a communications protocol for secure communication over a computer network. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security.
IETF	**Internet Engineering Task Force**
IOCTL	**Input Output Control**
IP	**Internet Protocol**
IT	**Information Technology**
MQ	**Message Queue**
OCSP	**Online Certificate Status Protocol (RFC 2560)**
OID	**ISO Object Identifier** for X.509 certificates (unique for the given CA)
OSP	**Organizational Security Policy**
Payara	**Payara Application Server** is derived from GlassFish Application Server, with 24/7 Production Support and with quarterly releases containing enhancements, bug fixes and patches.
PBM	**PassBy[ME]**
PKCS	**Public Key Cryptography Standards**
PKI	**Public Key Infrastructure**
PKIX	**Working Group of IETF to support X.509 based Public Key Infrastructure**
PP	**Protection Profile**
SAR	**Security Assurance Requirement**
SCEP	**Simple Certificate Enrollment Protocol**

	is an Internet Draft in the Internet Engineering Task Force (IETF). It is designed to make the issuing of digital certificates as scalable as possible. The idea is that any standard network user should be able to request their digital certificate electronically and as simply as possible.
SFR	**Security Functional Requirement**
SFP	**Security Function Policy**
SP	**Service Provider**
SPD	**Security Problem Definition**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TLS	**Transport Layer Security Protocol (RFC 5246)**
TOE	**Target of Evaluation**
TOI	**Time of Interest**
TSA	**Time Stamp Authority (NTC 3161)**
TSF	**TOE Security Functionality**
VPN	**Virtual Private Network**
URL	**Uniform Resource Locator** is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
X.509	
XAdES	**XML Advanced Electronic Signatures (ETSI 101903)**

9 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

[5] PassBy[ME] Guide of administrators, Version 1.1.22, October 2017.

[6] PassBy[ME] API Documentation, Version 1.1.22, October 2017.

[7] PassBy[ME] Management API Documentation, Version 1.1.22, October 2017.