Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 4/18

(Certification No.)

Prodotto: **PassBy[ME] Server System v1.2**
(Product)

Sviluppato da: **Microsec Ltd.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 8 maggio 2018

Common Criteria

SOGIS IT SECURITY CERTIFICATE

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

PassBy[ME] Server System v1.2

OCSI/CERT/SYS/03/2017/RC

Version 1.0

8 May 2018

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	08/05/2018

2 Table of contents

3 Acronyms

2FA	Second Factor Authentication Subsystem
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
RFV	Rapporto Finale di Valutazione (Evaluation Technical Report)
SAR	Security Assurance Requirement
SCEP	Certificate Enrollment Server
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
TDS	Traguardo di Sicurezza (Security Target)
TLS	Transport Layer Security

TOE	Target of Evaluation
TSA	Time Stamp Authority
TSF	TOE Security Functionality
TSFI	TSF Interface
UI MGMT	User Interface Management

4 References

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

[AGD] PassBy[ME] Server Administrator Guide, Version 1.3, 9 January 2018

[CMS] PassBy[ME] Server Configuration Management Scope, Version 1.1, 6 November 2017

[OPE] PassBy[ME] Server Operational User Guide, Version 1.2, 20 October 2017

[RFV] PassBy[ME] Server Evaluation Technical Report, v1, 12 March 2018

[SIM] PassBy[ME] Appliance System Installation Manual, Version 1.1.21, 29 November 2017

[TDS] PassBy[ME] Server Security Target, v1.7, 11 October 2017

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all assurance components selected.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “PassBy[ME] Server System v1.2”, developed by Microsec Ltd.

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

In particular, the TOE is a PKI based mobile ID solution, providing user authentication, transaction signing and mobile digital signature.

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 the TOE).

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "PassBy[ME] Server System v1.2" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	PassBy[ME] Server System v1.2
Security Target	PassBy[ME] Server Security Target, v1.7, 11 October 2017
Evaluation Assurance Level	EAL2
Developer	Microsec Ltd.
Sponsor	Microsec Ltd.
LVS	Systrans Software Laboratory - CCLAB
CC version	3.1 Rev. 4
PP conformance claim	No compliance declared
Evaluation starting date	10 May 2017
Evaluation ending date	12 March 2018

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

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

In particular, the TOE is a PKI based mobile ID solution, providing user authentication, transaction signing and mobile digital signature.

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 the TOE).

Each user receives his 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 service provider 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 payment service provider will only authorize the transaction if the customer authentication was successful and the customer confirmed the online transaction.

7.3.1 TOE Architecture

For a detailed description of the TOE, please refer to sect. 1.5 “TOE Description” of the Security Target [TDS]. The most significant aspects are summarized below (see Figure 1).

The components of the TOE (green boxes in Figure 1) are the following:

- PUBLIC Server (Apache), providing 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 a TLS channel, where the server is authenticated. The enrollment process serves to bind a mobile device to a user.

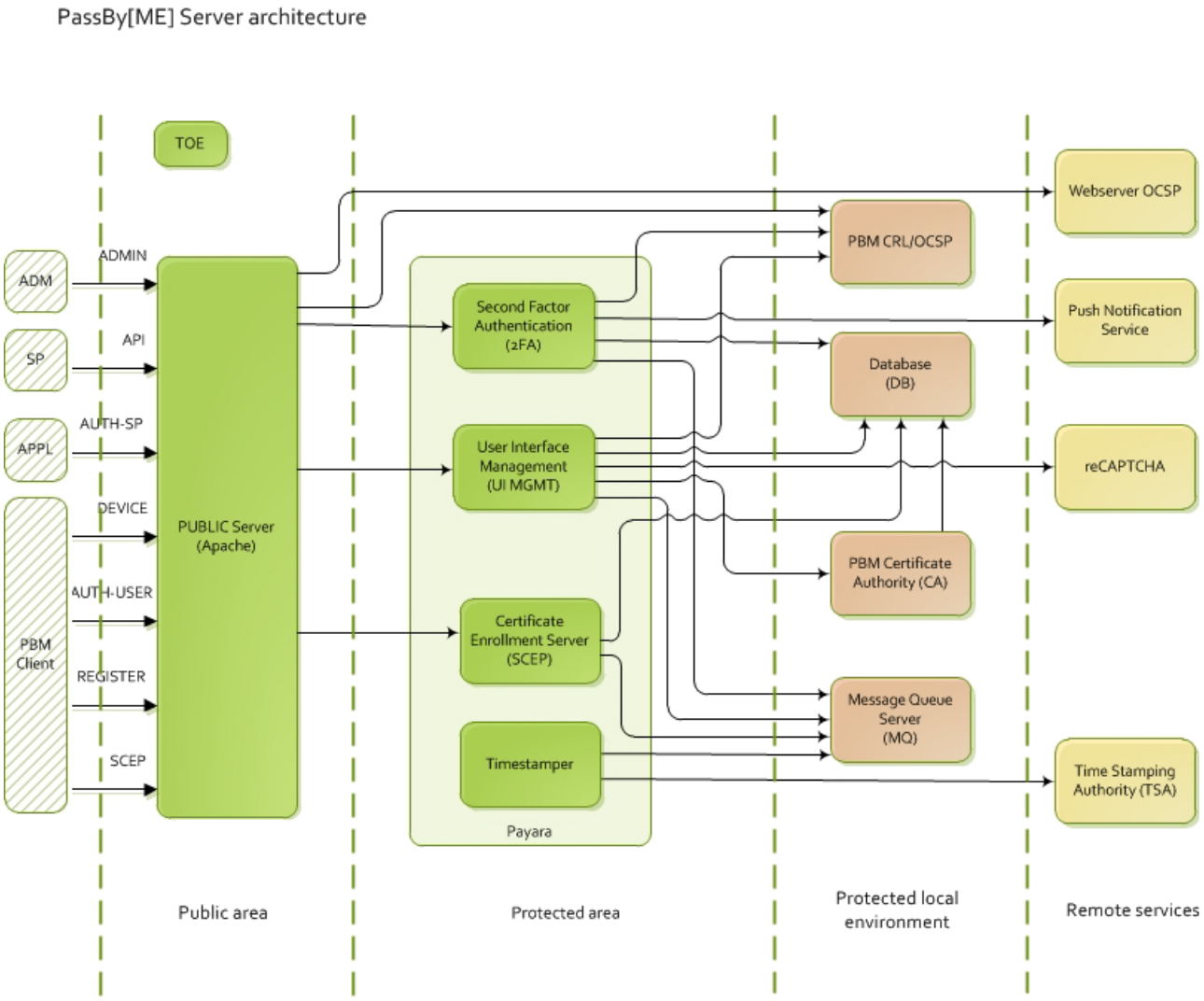

Figure 1 – TOE Boundaries

- 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 Time Stamp Authority (TSA).

All other components are needed for a complete working environment, but they are not parts of the TOE.

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.

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.

7.3.2 TOE security features

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 TSA will be used.

7.3.2.1 TOE security functions

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

- **Security Audit**. 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).

- **User Data Protection**. User data protection defines how users of the TOE can perform operations on objects. User data are to be found in messages, in database, in filesystem. 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. 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.

- **Identification and Authentication**. All the Users, mobile devices (Devices) and Service Providers are identified and authenticated by certificates, which have been issued by a configured Certification Authority (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. The PassBy[ME] system uses shared secrets to strengthen the security of processes where PKI is not applicable.

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

For more detail see sect. 1.5.2 of [TDS].

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customers together with the product. The guidance documentation contains all the information for secure installation, initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the security use of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, also the following extended components are included (see sect. 5 of the Security Target [TDS]):

- FDP_DAU_CPV_EXT.1 Certificate processing
- FDP_DAU_CPI_EXT.1 Certification path initialization
- FDP_DAU_CPD_EXT.1 Certification path development
- FDP_ITC_SIG_EXT.1 PKI Signature Verification
- FDP_DAU_OCS_EXT.1 Basic OCSP Client

- FDP_DAU_CRL_EXT.1 Basic CRL Checking
- FIA_UAU_SIG_EXT.1 Entity Authentication

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) Systrans CCLAB.

The evaluation was completed on 12 March 2018 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 17 April 2018. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [RFV] issued by the LVS Systrans CCLAB and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "PassBy[ME] Server System v1.2" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2.

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

Assurance classes and components		**Verdict**
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "PassBy[ME] Server System v1.2" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the Security Target are respected.

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([AGD] and [OPE]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The components of TOE, PassBy[ME] Server System v1.2, will be delivered in form of archive compressed file on a storage media (DVD or USB-token). The storage medium is written in standard format and is readable on Linux systems.

The delivered package can be accepted by the customer if it contains the following items:

- Installation package in compressed form
- Electronically signed Release notes with qualified signature by Microsec Ltd.
- Installation notes
- PassBy[ME] Server Operational User Guide [OPE]
- PassBy[ME] Server Administrator Guide [AGD]

The acceptance test of the delivered TOE will be performed by the System Administrator, following the instructions provided in the Administrator Guide [AGD].

9.2 Installation, initialization and secure usage of the TOE

TOE installation consists of two steps.

1. Preparation of the operational environment, consisting in the installation of the Linux operating system (RHEL or CentOS), with installed Web Server (Apache) and with working network connection. The delivered, checked and accepted TOE package contains scripts to check and set up the needed environment. All the preparation works, from uncompressing, up to the execution of install scripts will be performed by the System Administrator. Useful instructions to install the operational environment (switches, routers, servers) can be found in the public document:
    - PassBy[ME] Appliance System Installation Manual [SIM]
2. TOE installation and configuration should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer, and in particular in:
    - PassBy[ME] Server Administrator Guide [AGD]

10 Annex B – Evaluated configuration

The TOE is identified in the Security Target [TDS] with the version number 1.2. The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The subsystems of the evaluated configuration are listed in detail in the Configuration List, provided by the developer to the Evaluators in the document [CMS].

10.1 TOE components

The TOE subsystems, with their version number, are summarized in Table 2. Note that all the subsystems have the same version number, which corresponds to the delivered release version of the TOE.

For more details, please refer to sect. 1.5.1 of the Security Target [TDS].

Name	Reference	Version	Date
2FA subsystem	microsec-pbm-2nd-factor-web-1.2.war	1.2	November 2017
UI MGMT subsystem	microsec-pbm-ui-web-1.2.war	1.2	November 2017
Timestamper subsystem	microsec-pbm-timestamper-web-1.2.war	1.2	November 2017
SCEP subsystem	microsec-pbm-scep-web-1.2.war	1.2	November 2017

Table 2 – TOE subsystems

10.2 TOE operational environment

In Table 3 are summarized the minimal requirements of the operational environment of the TOE to allow its correct working.

For more details, please refer to sect. 1.5.2 of the Security Target [TDS].

Name	Developer	Version	Date
Operating System CentOS x86_64	The CentOS Project	7.4.1708	December 2016
Operating System RHEL	Red Hat Inc.	7.4.x	July 2017
Apache HTTP Server	The Apache Software Foundation	2.4.6	July 2017
Payara Application Server	Payara Services Ltd.	4.1.2.173	August 2017
Java Standard Edition for Linux x64	Oracle Corporation	1.8.0_152	July 2017
OpenSSL *(part of Linux operating system)*	OpenSSL Software Foundation	1.0.1efips	February 2013
PostgreSQL	The PostgreSQL Global Development Group	9.6.6	November 2017
OpenMQ Server	Oracle Corporation	5.1	September 2017
Online Certificate Status Protocol (OCSP)	Microsec Ltd.	1.2.15	November 2017
Certification Authority (CA)	Microsec Ltd.	1.2	November 2017

Table 3 – TOE operational environment components

11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL2 such activities include the following three steps:

- evaluation of the tests performed by the developer in terms of coverage;
- execution of independent functional tests by the evaluators;
- execution of penetration tests by the evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been arranged at the LVS site with the support of the developer, which provided the necessary resources.

The installation of the test environment was in accordance with the guidance documentation ([AGD], [OPE], [SIM]), as indicated in Annex A – Guidelines for the secure usage of the product.

After configuration of the TOE the evaluators checked the status and found that the TOE was installed properly, and the needed services were running.

The test environment is the same as the developer used for testing the TSFI.

11.2 Functional tests performed by the developer

11.2.1 Test coverage

The evaluators have examined the test plan presented by the developer and verified the complete coverage of the functional requirements SFR and the TSFIs described in the functional specification.

11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

They did not used testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.3.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE. In this research the Linux operating system has been also considered, part of the operational environment, but needed for the correct operation of the TOE. Several potential vulnerabilities have thus been identified.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation) and used automatic scanning tools (Nessus, Acunetix and BurpSuite Pro), to identify any additional potential vulnerabilities of the TOE. From this analysis, the evaluators have actually determined the presence of other potential vulnerabilities.

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify some actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with Basic attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves.

The execution of the penetration tests confirmed the presence of vulnerabilities potentially exploitable by an attacker with a potential of attack Basic. These results were promptly reported to the Developer, via an Observation Report. The Developer has replied, accepting the evaluators' observations and releasing a new version of the TOE. The evaluators installed such a new version of the TOE in the test environment, and were able to verify that the solutions proposed by the Developer have solved all the problems raised with the previous observations.

On the basis of such results, the evaluators concluded that no attack scenario with potential Basic can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. They have not identified residual vulnerabilities, i.e. vulnerabilities that, although not exploitable in the operating environment of the TOE, could be exploited only by an attacker with attack potential beyond Basic.