National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Protection Profile for Application Software, Version 1.1, November 5, 2014

Report Number:	**CCEVS-VR-PP-0026**
Dated:	**March 10, 2016**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Gossamer Security Solutions
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Application Software, Version 1.1 (PPAPP11). It presents a summary of the PPAPP11 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the PPAPP11 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the CyberReliant Corporation's (CRC) Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2). The evaluation was performed by Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, in the United States and was completed in October 2015. This evaluation addressed the base requirements of the PPAPP11, as well as a few of the optional, selection-based and objective requirements contained in the Appendices.

The information in this report is largely derived from the Assurance Activity Report (AAR), written by the Gossamer Security Solutions.

The evaluation determined that the PPAPP11 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the PPAPP11, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the PPAPP11 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the PPAPP11 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Data at Rest (DaR) Service (Native) Version 1.0.0 (Version Code 2), provided by CyberReliant Corporation's (CRC). Gossamer Security Solutions Common

Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, in the United States and was completed in October 2015.

The PPAPP11 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either optional, selection-based, or objective depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because these additional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the PPAPP11 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional requirements in the PPAPP11.

Protection Profile	*Protection Profile for Application Software, Version 1.1, November 5, 2014*
ST (Base)	CyberReliant Corp. Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target Version 0.6 October 21, 2015
ST (Additional)	Trivalent Data at Rest (DaR) Service (Inside) (ASPP11/FEEP10) Security Target Version 0.6, December 21, 2015
Assurance Activity Report (Base)	Assurance Activity Report (ASPP11/ASFEEP10) for CRC Data at Rest Service (Native) Version 1.0.0 (Version Code 2) Version 0.4, October 29, 2015
Assurance Activity Report (Additional)	Assurance Activity Report (ASPP11/ASFEEP10) for Trivalent Data at Rest Service (Inside) Version 0.6, December 23, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
CCTL (base and additional)	Gossamer Security Solutions, Catonsville, MD USA
CCEVS Validators (base)	Ken Elliott, Aerospace Corporation Herb Ellis, Aerospace Corporation Kelly Hood, Aerospace Corporation Jerome Meyers, Aerospace Corporation
CCEVS Validators (Additional)	Ken Elliott, Aerospace Corporation Herb Ellis, Aerospace Corporation Kelly Hood, Aerospace Corporation Jerome Meyers, Aerospace Corporation

3 PPAPP11 Description

The requirements in the PPAPP11 apply to application software which runs on mobile devices ("apps"), as well as on desktop and server platforms. Some application types are covered by more specific PPs, which may be expressed as Extended Packages of this PP. Such applications are subject to the requirements of both this PP and the Extended Package that addresses their special functionality. PPs for some particularly specialized applications may not be expressed as EPs at this time, though the requirements in this document should be seen as objectives for those highly specialized applications.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption Name	Assumption Definition
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Table 1: Assumptions

4.2 Threats

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

Table 2: Threats

4.3 Organizational Security Policies

The APP PP does not define organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

TOE Security Obj.	TOE Security Objective Definition
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom if ever shipped without errors, and the ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

Table 3: Security Objectives for the TOE

The following table contains objectives for the Operational Environment.

TOE Security Obj.	TOE Security Objective Definition
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

TOE Security Obj.	TOE Security Objective Definition
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the PPAPP11 are comprised of the "base" requirements and additional requirements that are either optional, selection-based, or objective depending on the requirement in question. The following are table contains the "base" requirements that were validated as part of the CyberReliant evaluation activity referenced above.

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_RBG_EXT.1: Random Bit Generation Services
	FCS_STO_EXT.1: Storage of Secrets
FDP: User Data Protection	FDP_DEC_EXT.1: Access to Platform Resources
	FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
FMT: Security Management	FMT_SMF.1: Specification of Management Functions
	FMT_MEC_EXT.1: Supported Configuration Mechanism
	FMT_CFG_EXT.1: Secure by Default Configuration
FPT: Protection of the TSF	FPT_AEX_EXT.1: AntiExploitation Capabilities
	FPT_API_EXT.1: Use of Supported Services and APIs
	FPT_TUD_EXT.1: Integrity for Installation and Update
	FPT_LIB_EXT.1: Use of Third Party Libraries
FTP: Trusted path/channels	FTP_DIT_EXT.1: Protection of Data in Transit

Table 5: Base Requirements

The following table contains the additional optional requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_TLSC_EXT.1: TLS Client Protocol	

The following table contains the additional selection-based requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_RBG_EXT.2: Random Bit Generation from Application	Trivalent Data at Rest (DaR) Service (Inside) (ASPP11/FEEP10) Security Target Version 0.6, December 21, 2015
	FCS_CKM_EXT.1: Key Encryption Key (KEK) Suppor	CyberReliant Corp. Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target Version 0.6 October 21, 2015
	FCS_CKM.1: Cryptographic Key Generation	
	FCS_CKM.2: Cryptographic Key Establishment	
	FCS_COP.1(1): Cryptographic Operation Encryption	CyberReliant Corp. Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target Version 0.6 October 21, 2015
	FCS_COP.1(2): Cryptographic Operation - Hashing	
	FCS_COP.1(3): Cryptographic Operation - Signing	
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)	CyberReliant Corp. Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target Version 0.6 October 21, 2015
	FCS_TLSC_EXT.1: TLS Client Protocol	
	FCS_DTLS_EXT.1: DTLS Implementation	
	FCS_HTTPS_EXT.1: HTTPS Protocol	
FIA: Identification and Authentication	FIA_X509_EXT.1: X.509 Certificate Validation	
	FIA_X509_EXT.2: X.509 Certificate Authentication	

Table 6: Selection-Based Requirements

The following table contains the objective requirements that specify security functionality that is desirable that are contained in Annex C. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this PP.

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_TLSC_EXT.1: TLS Client Protocol
FPT: Protection of the TSF	FPT_API_EXT.1: Use of Supported Services and APIs
	FPT_IDV_EXT.1 Software Identification and Versions

Table 7: Objective Requirements

6 Assurance Requirements

The following are the assurance requirements contained in the PPAPP11:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

Table 8: Assurance Requirements

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

Table 9: Evaluation Results

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the PPAPP11 Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Gossamer Security Solutions, Inc., *CyberReliant Corp. Data at Rest (DaR) Service (Native) (ASPP11/FEEP10) Security Target* Version 0.6 October 21, 2015

[7] Gossamer Security Solutions, Inc., *Trivalent Data at Rest (DaR) Service (Inside) (ASPP11/FEEP10) Security Target* Version 0.6, December 21, 2015

[8] Gossamer Security Solutions, Inc., *CRC Data at Rest (DaR) Service (Native) Validation Report* Version 0.3, October 29th, 2015

[9] Gossamer Security Solutions, Inc., *Trivalent Data at Rest (DaR) Service (Inside)Validation Report* Version 1.0, December 23, 2015

[10] Gossamer Security Solutions, Inc., *Assurance Activity Report (ASPP11/ASFEEP10) for CRC Data at Rest Service (Native) Version 1.0.0 (Version Code 2)* Version 0.4, October 29, 2015

[11] Gossamer Security Solutions, Inc., *Assurance Activity Report (ASPP11/ASFEEP10) for Trivalent Data at Rest Service (Inside)* Version 0.6, December 23, 2015

[12] Protection Profile for Application Software, Version 1.1, November 5, 2014