National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Bluechip Systems LLC

MicroCloud X4

Report Number: CCEVS-VR-VID10740-2017
Dated: **August 29, 2017**
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

Validation Panel

Jim Donndelinger

MITRE Corporation, Bedford, MA

Patrick Mallett, PhD

MITRE Corporation, McLean, VA

Common Criteria Testing Laboratory

Brad Mitchell

Ryan Day

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the MicroCloud X4 v1.0.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE is intended to be used in mobile devices. The TOE is a microSD card that provides data at rest (DAR) protections for user data stored on the TOE.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Handset	Samsung Galaxy S5 SM-G900F host running Android v4.6 - v6.0

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	MicroCloud X4
Protection Profile	cPP FDE AA, cPP FDE EE
Security Target	MicroCloud X4 Security Target v1.0
Dates of Evaluation	June 2016 - June 2017
Conformance Result	Pass
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	17-3546-R-0015 V1.2
Sponsor/Developer	Bluechip Systems LLC
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Brad Mitchell
CCEVS Validators	Jim Donndelinger, Patrick Mallett

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before March 9, 2017.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE.

4.1 Cryptographic Support

The TOE performs cryptographic operations using CAVP validated algorithms. The TOE performs random number generation, ECDSA signature verification, key derivation, and encryption/ decryption to support full drive encryption functions.

4.2 User Data Protection

The TOE encrypts all user data using AES XTS with a 256 bit key.

4.3 Security Management

The TOE allows users to change the data encryption key (DEK), cryptographically erase the DEK, and initiate firmware updates.

4.4 Protection of the TSF

The TOE protects itself by running a suite of self-tests at power-up and by authenticating firmware updates by verifying a digital signature. The TOE does not store plaintext submasks in non-volatile memory.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

Table 3: Assumptions

Assumption	Description
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
A. INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in “bad” sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may

Table 3: Assumptions	
Assumption	Description
	use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, unpartitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE preauthentication software) contain no protected data.
A.TRAINED_USER	Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
A.POWER_DOWN	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off. This properly clears memories and locks down the device, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., Lockscreen or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.
A.SUCURE_STATE	Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
A.SINGLE_USE_ET	External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
A.PASSWORD_STRENGTH	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
A.PLATFORM_I&A	The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the Operating system's login interface, but it will not change or degrade the functionality of the actual interface.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

Table 4: Threats	
Threat	Description
T.UNAUTHORIZED_DATA_ ACCESS	The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a

Table 4: Threats	
Threat	Description
	host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
T.KEYING_MATERIAL_ COMPROMISE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash, or TPMs.
T.AUTHORIZATION_GUESSIN G	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release DEKs or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.KEYSPACE_EXHAUST	Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to brute force exhaust the key space and give them unauthorized access to the data.
T.KNOWN_PLAINTEXT	Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with known plaintext could allow an attacker to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.CHOSEN_PLAINTEXT	Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file A poor choice of encryption algorithms, encryption modes, and initialization vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software and/or firmware that bypasses the intended security features and provides them unauthorized to access to data.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

There are no organizational security policies addressed by this cPP.

6 Architectural Information

The TOE is classified as Full Drive Encryption for Common Criteria purposes. The TOE is made up of Hardware and Software components.

6.1 Architecture Overview

The TOE consists of the following components:

6.1.1 TOE Hardware

- MCX4-004 or MCX4-008
- InvenSense MPU-6500 Accelerometer (part of the host device)

6.1.2 TOE Software

- MicroCloud Linux 3.4.110.1 (running on the MCX4-004 or MCX4-008)
- MicroCloud Manager 1.9 (running on the MCX4-004 or MCX4-008)
- GreenFiles v1.8.0 (running on the host device)
- Bluechip DataHub Service v1.8.0 (running on the host device)

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is shipped to the end user via commercial carrier. The guidance documents are provided in the shipment and available online, and apply to the CC Evaluated configuration:

7.1 Design Documentation

Document	Revision	Date
MicroCloud X4 Key Management Description	2.3	February 27, 2017
MicroCloud X4 Entropy Essay	1.2.6	March 22, 2017

7.2 Guidance Documentation

Document	Revision	Date
Bluechip Systems MicroCloud X4 Operation Manual	7e4	N/A

7.3 Configuration Management and Lifecycle

Document	Revision	Date

7.4 Test Documentation

Document	Revision	Date
16-3546-R-0072 V1.3 Bluechip FDE-EE + AA Test Report	1.3	August 3, 2017

7.5 Vulnerability Assessment Documentation

Document	Revision	Date
16-3546-R-0072 V1.4 Bluechip FDE-EE + AA Test Report	1.4	August 3, 2017

7.6 Security Target

Document	Revision	Date
MicroCloud X4 Security Target	1.0	August 28, 2017

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Developer Testing

The vendor performed initial functional testing of the TOE to ensure that it performed all functions correctly and bug-free.

8.2 Evaluation Team Independent Testing

The evaluation team performed all required assurance activities for this cPP, and verified that the TOE achieved correct results for all tests.

8.3 Vulnerability Analysis

As part of the functional testing, the evaluation team performed a vulnerability assessment of the TOE, and determined that the TOE contained no known exploitable vulnerabilities.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation,

Version 3.1 Revision 4.

UL has determined that the TOE meets the security criteria in the Security Target. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed on June 5, 2017.

10 Validator Comments/Recommendations

None.

11 Security Target

MicroCloud X4 Security Target v1.0, August 28, 2017

12 Terms

12.1 Acronyms

Table 5: cPP Glossary	
Term	Description
Authorization Factor	A value that a user knows, has, or is (e.g. password, token, etc) submitted to the TOE to establish that the user is in the community authorized to use the hard disk and that is used in the derivation or decryption of the BEV and eventual decryption of the DEK. Note that these values may or may not be used to establish the particular identity of the user.
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
Border Encryption Value	A value passed from the AA to the EE intended to link the key chains of the two components.
Key Sanitization	A method of sanitizing encrypted data by securely overwriting the key that was encrypting the data.
Data Encryption Key (DEK)	A key used to encrypt data-at-rest.
Full Drive Encryption	Refers to partitions of logical blocks of user accessible data as managed by the host system that indexes and partitions and an operating system that maps authorization to read or write data to blocks in these partitions. For the sake of this Security Program Definition (SPD) and cPP, FDE performs encryption and authorization on one partition, so defined and supported by the OS and file system jointly, under consideration. FDE products encrypt all data (with certain exceptions) on the partition of the storage device and permits access to the data only after successful authorization to the FDE solution. The exceptions include the necessity to leave a portion of the storage device (the size may vary based on implementation) unencrypted for such things as the Master Boot Record (MBR) or other AA/EE pre-authentication software. These FDE cPPs interpret the term “full drive encryption” to allow FDE solutions to leave a portion of the storage device unencrypted so long as it contains no protected data.
Intermediate Key	A key used in a point between the initial user authorization and the DEK.
Host Platform	The local hardware and software the TOE is running on, this does not include any peripheral devices (e.g. USB devices) that may be connected to the local hardware and software.
Key Chaining	The method of using multiple layers of encryption keys to protect data. A top layer key encrypts a lower layer key which encrypts the data; this method can have any number of layers.
Key Encryption Key (KEK)	A key used to encrypt other keys, such as DEKs or storage that contains keys.
Key Material	Key material is commonly known as critical security parameter (CSP) data, and also includes authorization data, nonces, and metadata.
Key Release Key	A key used to release another key from storage, it is not used for the direct derivation or decryption

Table 5: cPP Glossary	
Term	Description
(KRK)	of another key.
Operating System (OS)	Software which runs at the highest privilege level and can directly control hardware resources.
Non-Volatile Memory	A type of computer memory that will retain information without power.
Powered-Off State	The device has been shutdown.
Protected Data	This refers to all data on the storage device with the exception of a small portion required for the TOE to function correctly. It is all space on the disk a user could write data to and includes the operating system, applications, and user data. Protected data does not include the Master Boot Record or Pre-authentication area of the drive – areas of the drive that are necessarily unencrypted.
Submask	A submask is a bit string that can be generated and stored in a number of ways.
Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.