National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Monkton IA Docs Reinforced by Rebar for iOS, version 1.0, Built on Monkton's Rebar Platform, Version 1.0

Report Number:	**CCEVS-VR-10825-2017**
Dated:	**12/7/2017**
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 Team

James Donndelinger

Meredith Hennan

The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Micciche

Zalman Kuperman

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Monkton IA Docs Reinforced by Rebar for iOS, version 1.0, Built on Monkton's Rebar Platform Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in December 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the Protection Profile for Application Software Version 1.2 (ASPP12) and the Extended Package for Software File Encryption Version 1.0 (ASFEEP10).

The Target of Evaluation (TOE) 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. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the APP PP and SWFE EP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 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 Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

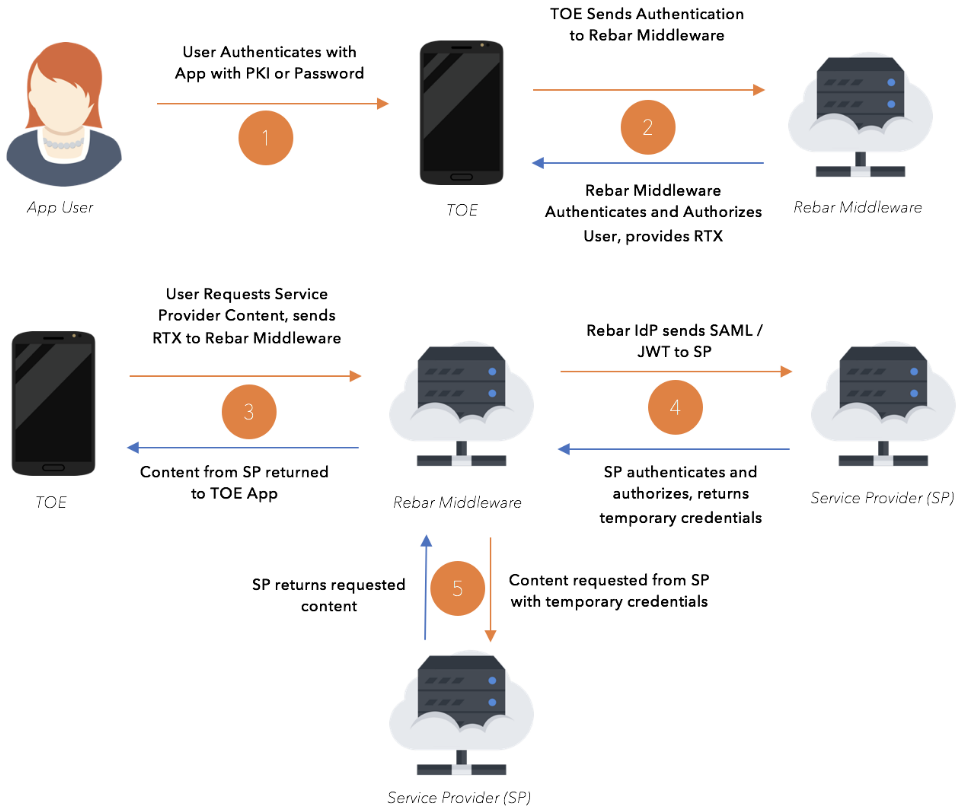
Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Monkton IA Docs Reinforced by Rebar for iOS, version 1.0, Built on Monkton's Rebar Platform
Protection Profile	tection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)
Security Target	Monkton IA Docs Reinforced by Rebar for iOS, version 1.0, Built on Monkton's Rebar Platform Security Target, version 1.0.11, December, 7, 2017
Evaluation Technical Report	Monkton IA Docs Reinforced by Rebar for iOS, version 1.0, Built on Monkton's Rebar Platform ETR, version 1.0.0
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Monkton, Inc.
Developer	Monkton, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	James Donndelinger, Meredith Hennan *The Aerospace Corporation*

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

Figure 1: TOE Overview



User Authenticates with App with PKI or Password
1
TOE Sends Authentication to Rebar Middleware
2
Rebar Middleware Authenticates and Authorizes User, provides RTX
App User
TOE
Rebar Middleware
User Requests Service Provider Content, sends RTX to Rebar Middleware
3
Content from SP returned to TOE App
Rebar IdP sends SAML / JWT to SP
4
SP authenticates and authorizes, returns temporary credentials
TOE
Rebar Middleware
Service Provider (SP)
SP returns requested content
5
Content requested from SP with temporary credentials
Service Provider (SP)

The TOE is the Monkton IA Docs Reinforced by Rebar for iOS, version 1.0.0 mobile app. The TOE interacts with the Rebar Middleware ("Middleware"), a server component not under evaluation to serve up documents from a cloud storage provider, also known as a Service Provider (SP). The TOE is a composition of the application code (IA Docs) and the Rebar SDK (Also referred to as just "Rebar"), which provides the implementation of the included NIAP Protection Profiles in this Security Target. When "Rebar" is referenced in this document it references the TOE, it can be used in an interchanged method in referencing the TOE itself.

The TOE interaction with the "Middleware" leverages the "Middleware Identity Provider" ("IdP"), part of the Middleware Authentication and Authorization process. When a user initially authenticates the TOE with the Middleware via username / password, the app is granted a Rebar Token Context (RTX) for that user using the app on that specific device.

When the TOE wants to request a resource from a SP, the app invokes a web service method via the Rebar SDK. The Rebar SDK, leveraging the RTX, calls the Middleware (3). The Middleware authenticates and authorizes the user based on their RTX. If the RTX is valid and the user is allowed to access the resource, they will begin to authenticate with the Rebar IdP service.

The Middleware will begin the IdP process for the requested service provider. If the user is tied to an active directory account, the user's UPN value is leveraged to authenticate the user to the service provider (4). The Rebar IdP creates the SAML Response or JWT Assertion to present to the service provider. The Rebar IdP will send the request to the service provider endpoint for programmatic authentication.

If the IdP SAML Response or JWT Assertion is authenticated and authorized by the service provider, the provider will issue temporary tokens or credentials to perform operations against the service provider. Rebar will temporarily cache the credentials for the request avoiding multiple authentications for the individual user. Rebar will then return the resource with the temporary credentials from the service provider (5).

3.1 TOE Evaluated Platforms

The TOE is the Monkton IA Docs Reinforced by Rebar for iOS, version 1.0.0 mobile application installed on one of the following physical Apple device models:

Table 1: TOE Evaluated Platforms

Device	Software	Processor
Apple iPhone 7	iOS 10.3.2	A10 Fusion (64-bit)
Apple iPad Pro	iOS 10.3.2	A10X Fusion (64-bit)

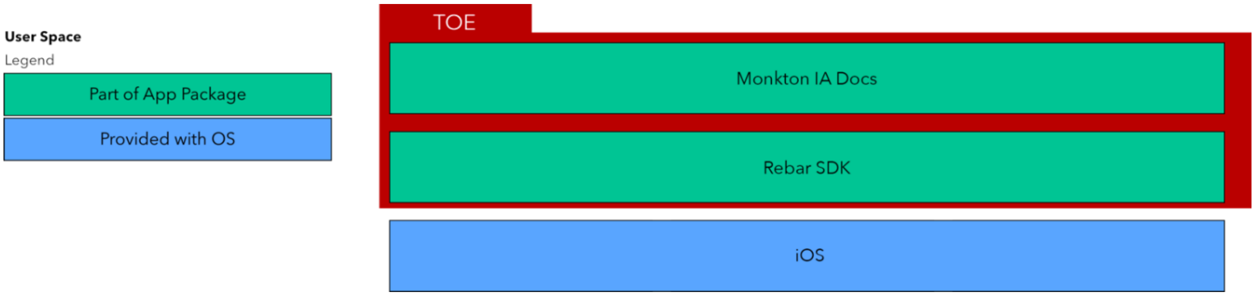
3.2 TOE Architecture

The section describes the TOE architecture including physical and logical boundaries.

Figure 2 shows the relationship of the TOE to its operational environment along with the TOE boundary. The security functional requirements identify the libraries included in the application package. Part of the TOE is the Rebar SDK. The Rebar SDK provides compliance to the necessary NIAP protection profile SFRs being evaluated in this document. Rebar, Rebar SDK, are analogous with the TOE in terms of being referenced in this document. Any references to Rebar or the Rebar SDK should be considered the TOE.

Monkton IA Docs is a combination of the Monkton provided Rebar SDK. The IA Docs executable and Rebar SDK are specific parts of vendor provided elements of the TOE. The TOE executes on top of iOS and interacts with platform provides APIs to perform specific tasks that are provided by the platform.

Figure 2: TOE Architecture



3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (Apple iPhone or Apple iPad) on which the TOE resides.

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Cryptographic Support
2. User Data Protection
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. Privacy
7. Trusted Path

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the PP as necessary to satisfy testing/assurance measures prescribed therein.

4.1 Cryptographic Support

The TOE provides several functions for cryptographic support. The TOE, by virtue of being built on Rebar, implements DAR and DIT as a functional component. When HTTPS network connections are created, they are made over TLS 1.2 connections with the requisite cipher suites. The TOE uses OpenSSL 1.0.2L to provide its cryptographic support.

The TOE, through Rebar, provides all requisite cryptographic functions for hashing, signing, HMAC, random number generation, and symmetric encryption.

To protect the keys and data generated by the TOE, the TOE will aggressively and securely delete key data and files written to non-volatile memory. This leverages both platform implemented functions as well as functions integrated into Rebar.

The relevant CAVP certificates are listed below for the TOE and the platform provided DRBG.

Table 2: CAVP Certificates

	Algorithm	Length	CAVP
AES	CBC, GCM	128, 192, 256	4751
HMAC	HMAC-SHA-256, HMAC- SHA-384, HMAC-SHA-512	Key: 160, 256, 512; Digest: 160, 256, 512	3165
ECDSA	PKG, PKV	P-256 P-384 P-521	1245
	SigGen, SigVer	P-256 P-384 P-521 with SHA-256, SHA-384, SHA-512	1245
RSA	ANSIX9.31: SigGen, SigVer	2048, 3072 with SHA-256, SHA-384, SHA-512	2595
	RSASSA-PKCS1_V1_5: SigGen, SigVer	2048, 3072 with SHA-256, SHA-384, SHA-512	2595
	RSASSA-PSS: SigGen, SigVer	2048, 3072 with SHA-256, SHA-384, SHA-512	2595
SHS	SHA	SHA-1, SHA-256, SHA-384, SHA-512	3008
CVL/KAS /ECC	ECC/KPG/ EphemUnified	P-256, P-384, P-521	1388
DRBG	AES-256 CTR DRBG	256	1632

4.2 User Data Protection

The TOE requests no hardware or software resources during the use of the application. The TOE requires network access but this is not a request that is prompted to the user.

4.3 Identification and Authentication

The TOE, through Rebar, implements X509 certificate validation for all server certificates presented for TLS 1.2 connections. Additionally, Rebar implements SSL Pinning, validating certificates based on SHA512 hashes of the certificates.

For user authorization, the TOE leverages PBKDF2 with HMACSHA256 to validate user credentials based on a passcode. The conditioned key is used as the FEK for the RMD. The passcode can be configured by the administrator for complexity requirements.

4.4 Security Management

The TOE is, by default, configured to be secure whenever it is freshly installed on a device. The TOE, through Rebar, provides configuration settings available through the Managed App Configuration settings. Rebar implements a secure version of NSUserDefaults that ensures settings are stored in an AES256 encrypted database.

4.5 Protection of the TSF

The TOE leverages only approved iOS APIs and available libraries. The TOE includes several third-party libraries that provide specific functionality for the TOE. Each of these libraries leverage only approved iOS APIs.

The TOE leverages the iOS update manager (App Store) or enterprise distribution mechanisms (MDM/Enterprise App Store) to update and install approved apps.

All key material used within the TOE is protected and destroyed as part of the cryptographic support. The password conditioned FEK is never stored in non-volatile memory.

4.6 Privacy

The TOE does not transmit PII.

4.7 Trusted Path/Channel

All data in transit for the TOE is sent with TLS 1.2.

5 Assumptions, Threats & Clarification of Scope

5.1 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	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.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	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.

Threat	Threat Definition
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
T.KEYING_MATERIAL_COMPROMISE	Attacks against the encryption product could take several forms; for example, if there is a weakness in the random number generation mixing algorithm or the data sources used in random number generation are guessable, then the output may be guessable as well. If an attacker can guess the output of the pseudorandom number generator (PRNG) at the time an encryption key is made, then the output may be used to recreate the keying material and decrypt the protected files. As the encryption program runs, it will store a variety of information in memory. Some of this information, such as random bit generation (RBG) inputs, RBG output, copies of the plaintext file, and other keying material, could be very valuable to an attacker who wishes to decrypt an encrypted file. If the encryption product does not wipe these memory spaces appropriately, an attacker may be able to recreate the encryption key and access encrypted files.

Threat	Threat Definition
T.KEYSPACE_EXHAUST	The protection of the data involves encrypting said data assuming an attacker may have significant computing resources at their disposal. Several ciphers have already been broken through brute-force attacks because the length of the keys used in those ciphers was too short to provide protection against a concerted computing effort to discover those keys. Because protection of the data may rely on a chaining of keys and encryption mechanisms, there are many opportunities for brute force attacks against each potential key in the chain, such that the weakest link in the chain of factors/keys will determine the overall strength against a brute force attack.

Threat	Threat Definition
T.PLAINTEXT_COMPROMISE	Unlike full disk encryption, selectable encryption products also need to protect against data leaks to other applications on the machine. Many file creators and editors store temporary files as the user is working on a file, and restore files if the machine experiences an interrupt while a file is open. Any of these files, if not properly protected or deleted, could leak information about a protected file to an attacker. Other applications might also access volatile or non-volatile memory released by the file encryption product, and the software used to create files prior to encryption may retain information about the file even after it has been encrypted. As the user creates and saves a new document, the plaintext will be stored on the machine's hard drive. An attacker could then search for the plaintext of the sensitive, encrypted information. An attacker may not even have to access the encrypted file for the protected information to be compromised. When the user wishes to encrypt the document, this plaintext file should be replaced with the new encrypted version. For non-mobile devices, it is expected that if the volatile and/or non-volatile memory space where the plaintext file was stored is merely released back to the machine without being first wiped clean of the data that was stored there, then the information the user wishes to protect will still be accessible. While protection of the encryption algorithm itself is vital, memory must also be properly managed by the file encryption product or the TOE platform in order for security to remain intact. For mobile devices, it is assumed that the File Encryption product will not be responsible for providing memory management cleanup and the environment's platform has met the Mobile Device Fundamentals Protection Profile.

Threat	Threat Definition
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.
T.UNAUTHORIZED_DATA_ACCESS	The central functionality of the TOE is the protection of resources under its control through encryption. In a shared resource environment, users on a system may have access to administrative-level tools that are capable of over-riding a system's access control protections. Further, if the system were to be lost or the system's storage device stolen, the attacker could then look directly at the storage device using low-level forensic tools in an attempt to access data for which they are not authorized. However, the need to protect the data in these scenarios should not interfere with the data-owner's (or another user that has been granted access to those data) ability to read or manipulate the data.
T.UNSAFE_AUTH FACTOR_VERIFICATION	When a user enters an authorization factor, the TOE is required to ensure that the authorization factor is valid prior to providing any data to the user; the purpose of verification is to ensure the FEK is correctly derived. If the data is decrypted with an incorrectly derived FEK (the FEK is conditioned from the password/passphrase or is decrypted by the KEK), then unpredictable data will be provided to the user. If verification is not performed in a secure manner, keying material or user data may be exposed or weakened.

Threat	Threat Definition
T.PLAINTEXT_DATA_SPOOFING	For certain modes of encryption, it is possible for a malicious person to modify ciphertext data to force unintended modification to the underlying plaintext data, without the user being notified. There are various failures that may occur on the part of the TOE, to include: failure to verify the integrity of the data prior to decryption, failure to provide integrity on the sensitive data, failure to use a cryptographic or secure hashing code and failure to differentiate the File Authentication Key (FAK) from the FEK; the FAK is any secret value used as input to a keyed hashing function or as part of an asymmetric authentication process

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile with File Encryption Extended Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP12/ASFEEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Monkton IA Docs Reinforced by Rebar for iOS version 1.0.0 User Guide, version 1.0
- Rebar Platform Administrative Guide, version 1.0

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation, and hence should not be relied upon when using the products as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE was evaluated on Apple’s iPhone 7 with iOS 10.3.2 (A10 Fusion with 64-bit architecture) and iPad Pro 10” with iOS 10.3.2 (A10X Fusion with 64-bit architecture).

To use the product in the evaluated configuration, the product must be configured as specified in the Monkton IA Docs Reinforced by Rebar for iOS version 1.0.0 User Guide, version 1.0 and the Rebar Platform Administrative Guide, version 1.0.

7.2 Excluded Functionality

- Authentication by means other than username and password

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the Evaluation Test Report for Monkton IA Docs Reinforced by Rebar for iOS, which is not publicly available. The *Common Criteria SWAPP Assurance Activity Report for Monkton IA Docs Reinforced by Rebar for iOS Version 1.0.0, version 1.3, dated November 27, 2017*, provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

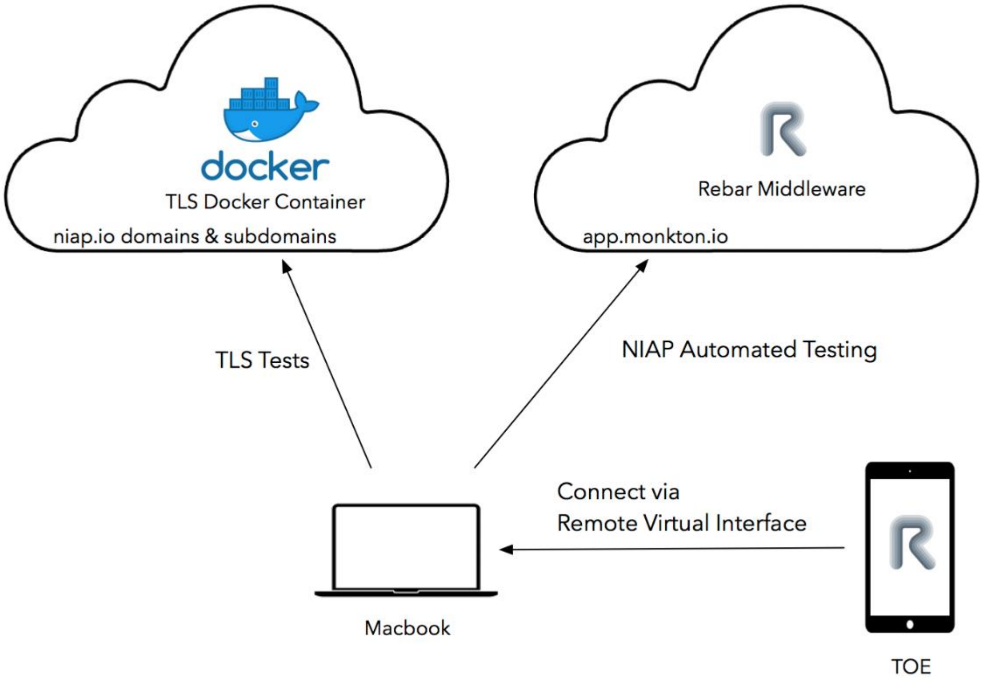
8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the ASPP12/ASFEEP10. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

8.2.1 Test Infrastructure

Below is a visual representation of the components included in the test bed. The TOE, as identified in the diagram, includes the iPad and iPhone devices. As these two devices were tested separately but against the same environment, the Test Diagram did not change.

Figure 3: Test Configuration Diagram



8.2.2 Test Configuration Information

8.2.2.1 Apple iPhone 7

- Software Version: 10.3.2
- IP Address: 192.168.128.167
- UDID: 4b80f0fb88ea308cf9a5ded318ca64a11ae46364

8.2.2.2 Apple iPad Pro

- Software Version: 10.3.2
- IP Address: 192.168.128.168
- UDID: 859634daed7aa795e5a8a8132ec580fb9c647000

8.2.2.3 Testing Workstation

- Hardware: Apple Macbook 12-inch
- Operating System: MacOS Sierra Version 10.12.5
- Purpose: Used for running the below tools and communicating with TOE
- Tools:
  - **Wireshark**: Version 2.2.7 for MAC OS X
  - **Rvictl**: MAC OS X tool that allows for remote virtual interface from Laptop to TOE device to allow packet capture
  - **NMAP**: Version 7.60 on MAC OS X for port scanning
  - **Visual Studio Code**: Version 1.13.1 for static code analysis
  - **Apple iTunes**: Version 12 for extracting output files from the TOE application
  - **Acumen-TLS TLS Test Tool**: Used for execution of the TLS bit modification tests and X509 certificate modification tests (IP for this test was set to 10.1.2.114)

8.2.2.4 NIAP.IO Test Domain and Subdomains

- Appache httpd Version 2.4.25
- Root CA: http://test-ocsp.niap.io:8881
- Intermediate One CA: http://test-ocsp.niap.io:8891
- Intermediate One – No OCSP Signing Purpose CA: http://test-ocsp-no-signing.niap.io:8894
- Intermediate Two CA: http://test-ocsp.niap.io:8892
- Intermediate Three CA: http://test-ocsp.niap.io:8893
- Purpose: See Section 5 for explanation of the port configuration for TLS automation tests

8.2.2.5 Rebar Middleware Server for automation tests

- Microsoft .NET Framework 4.7
- Purpose: Automation testing access to secure files

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 4. The evaluation determined the Monkton IA Docs Reinforced by Rebar for iOS to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Monkton IA Docs Reinforced by Rebar for iOS that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the PP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the PP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the PP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the PP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/

Public searches were performed against all keywords found within the Security Target and IA Docs for iOS User Guide that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware.

The list of keywords searched include:

- Monkton, Inc.
- IA Docs Reinforced by Rebar
- Apple iOS 10.3.2
- TLS 1.2
- Monkton Rebar
- Apple iPhone 7
- Apple iPad Pro

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, no issues were found for the TOE, and any issues found for the underlying platform, were not relevant to the evaluation, mitigating the risk factor.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the PP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the PP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

It may be possible for the consumer to configure authentication with an external factor, such as PKI, via the use of Monkton's Derived mobile application. This configuration will take the TOE out of the evaluated configuration, and no assertions can be made about its security compliance or effectiveness.

11 Annexes

Not applicable.

12 Security Target

Monkton IA Docs Reinforced by Rebar for iOS, version 1.0.0, Built on Monkton's Rebar Platform Security Target, version 1.0.11, December 7, 2017.

13 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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **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.

14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12).
6. Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10).
7. Monkton IA Docs Reinforced by Rebar for iOS, version 1.0.0, Built on Monkton's Rebar Platform Security Target, version 1.0.11, December, 7 2017.
8. Common Criteria SWAPP Assurance Activity Report for Monkton IA Docs Reinforced by Rebar for iOS Version 1.0.0, version 1.3, November 27, 2017.
9. Evaluation Technical Report for a Target of Evaluation Monkton IA Docs Reinforced by Rebar for iOS Version 1.0.0, version 1.0.
10. Monkton IA Docs Reinforced by Rebar for iOS version 1.0.0 User Guide, version 1.0
11. Rebar Platform Administrative Guide, version 1.0