Nubo Software
Thin Client v2.0 Security Target

Prepared for:
Nubo Software LTD
1 Hayaeden Street
Airport City, Israel

Prepared by:
Common Criteria Consulting LLC
15804 Laughlin Ln.
Silver Spring, MD 20906

REVISION HISTORY

Rev	Description
1.0	November 14, 2017, Initial release
1.1	February 8, 2018, Updated to address validator comments
1.2	May 31, 2018, Updated based on evaluation results and internal review
1.3	June 2018, Updated based on ECR comments
1.4	July 2018, Updated based on ECR round 2 comments

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

CA ..... **Certificate Authority**
CC ..... **Common Criteria**
CM ..... **Configuration Management**
CN ..... **Common Name**
CRL ..... **Certificate Revocation List**
DNS ..... **Domain Name System**
DRBG ..... **Deterministic Random Bit Generator**
HTTPS ..... **HyperText Transfer Protocol Secure**
IP ..... **Internet Protocol**
NIAP ..... **National Information Assurance Partnership**
NISP ..... **National Institute of Standards and Technology**
OCSP ..... **Online Certificate Status Protocol**
OID ..... **Object IDentifier**
PII ..... **Personally Identifiable Information**
PP ..... **Protection Profile**
RFC ..... **Request For Comments**
SAN ..... **Subject Alternative Name**
SFR ..... **Security Functional Requirement**
ST ..... **Security Target**
TD ..... **Technical Decision**
TLS ..... **Transport Layer Security**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
VMI ..... **Virtual Mobile Infrastructure**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Nubo Software Thin Client v2.0 TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Nubo Software Thin Client v2.0 Security Target, version 1.3, June 2018.

1.2 TOE Reference

Nubo Software Thin Client v2.0

1.3 Keywords

Software, thin client, Virtual Mobile Infrastructure (VMI)

1.4 TOE Overview

The Target of Evaluation (TOE) is the Nubo Software Thin Client v2.0. The TOE is an application from the Google Play store installed and executing on a mobile device.

With VMI, virtual applications execute on a user's behalf on VMI servers. No executable code associated with the virtual applications is downloaded to the user's device. Instead, the Thin Client displays the output from the virtual applications, and forwards input from the user to the virtual applications.

The Thin Client transparently controls all communication with the VMI servers and ensures that all communication occurs over trusted channels. All network connections are initiated by the TOE. Direct connections are established to two VMI server components. The Nubo Management Server processes user activation and login. The Nubo Gateway provides the real-time connection for access to virtual applications. The traffic for any number of virtual applications is multiplexed over a single trusted channel with the Thin Client.

When the Thin Client is first installed, the user is required to activate the Thin Client with the Nubo Management Server. The user specifies his/her password to the Management Server during activation. Once activated, the user may establish sessions and execute virtual applications. Each session requires that the user provide his/her password, which is transparently forwarded to the Management Server for validation. Upon successful login, the Management Server provides a session id to both the Thin Client and Gateway. The Thin Client then established a trusted channel to the Gateway, specifying the session id, enabling the user to activate his/her authorized applications.

1.5 TOE Description

The TOE is the thin client executing on mobile devices that provides the user interface to virtual mobile applications executing on Nubo Software's VMI servers. The TOE runs on evaluated Samsung Galaxy S7 and S7 Edge devices running Android 6.0.1.

1.5.1 Physical Boundary

The physical boundary of the TOE is the Thin Client application installed and running on a supported platform. Note that Android and the hardware devices are outside the TOE boundary.

The physical scope of the TOE also includes the following guidance documentation:

1. *Nubo End User Guide*

1.5.1.1 Logical Boundary

The TOE supports the security functions documented in the following sections.

1.5.1.2 Cryptographic Support

The TOE relies on underlying cryptographic functionality provided by the platform for all of its cryptographic operations.

In the evaluated configuration the TOE will be running on the following CC validated platforms.

- Samsung Galaxy S7 and S7 Edge (VID10739)

1.5.1.3 User Data Protection

The TOE does not store sensitive data in local files. The TOE can access physical resources on the mobile device, but does not access any of the logical data repositories.

1.5.1.4 Identification and Authentication

The TOE utilizes Androids functionality to authenticate certificates for the Management Server and Gateway.

1.5.1.5 Security Management

The TOE does not come with any default credentials, and no user credentials are stored by the TOE.

1.5.1.6 Privacy

The TOE requests PII including, first and last name when creating a new Nubo account. A warning is displayed on the page indicating that this information will be transferred over the network. The user may additionally supply PII when interacting with applications in the Nubo VMI, but the TOE simply transparently transmits this data and is unaware of the nature of the data.

1.5.1.7 Protection of the TSF

The TOE implements anti-exploitation measures to protect against compromise during execution. The Android platform also provides protection for the TOE. Secure delivery of the TOE is accomplish through delivery via the Google Play store.

1.5.1.8 Trusted Channels

The TOE establishes trusted channels using HTTPS/TLS to the Management Server and Gateway.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 5

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Protection Profile Conformance

This Security Target claims exact conformance to the Protection Profile for Application Software [ASPP], version 1.2, dated 2016-04-22.

All NIAP Technical Decisions (TDs) issued to date that are applicable to [ASPP] have been addressed. The following table identifies all applicable TD:

Table 1 TDs

Identifier	Applicable	Exclusion Rationale (if applicable)
0327 – Default file permissions for FMT_CFG_EXT.1.2	Yes	
0326 – RSA-based key establishment schemes	No	This TD addresses FCS_CKM.1, FCS_CKM.2, and FCS_TLSS_EXT.1.3. The TOE does not include any of these SFRs.
0305 – Handling of TLS connections with and without mutual authentication	No	This TD address the Assurance Activities associated with FCS_TLSS_EXT.2. The TOE does not include FCS_TLSS_EXT.2.
0304 – Update to FCS_TLSC_EXT.1.2	Yes	
0300 – Sensitive Data in FDP_DAR_EXT.1	Yes	
0296 – Update to FCS_HTTPS_EXT.1.3	Yes	
0295 – Update to FPT_AEX_EXT.1.3 Assurance Activities	Yes	
0293 – Update to FCS_CKM.1(1)	No	This TD addresses FCS_CKM.1. The TOE does not include FCS_CKM.1. Additionally, this TD has been archived.
0283 – Cipher Suites for TLS in SWApp v1.2	Yes	
0269 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on Android. Additionally, the TD has been archived.
0268 – FMT_MEC_EXT.1 Clarification	Yes	
0267 – TLSS testing - Empty Certificate Authorities list	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0244 – FCS_TLSC_EXT - TLS Client Curves Allowed	Yes	
0241 – Removal of Test 4.1 in FCS_TLSS_EXT.1.1	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0238 – User-modifiable files FPT_AEX_EXT.1.4	Yes	
0221 – FMT_SMF.1.1 - Assignments moved to Selections	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP.
0218 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on Android. Additionally, the TD has been archived.

0217 – Compliance to RFC5759 and RFC5280 for using CRLs	No	This TD modifies the conformance options available when using CRLs for revocation. The TOE does not support the usage of CRLs for revocation.
0215 – Update to FCS_HTTPS_EXT.1.2	No	This TD modifies a selection which is not claimed by the TOE.
0192 – Update to FCS_STO_EXT.1 Application Note	Yes	
0178 – Integrity for installation tests in AppSW PP	No	This TD modifies the Assurance Activity for Apple iOS platforms. The TOE runs on Android.
0177 – FCS_TLSS_EXT.1 Application Note Update	No	This TD addresses the usage of FCS_TLSS_EXT.1 as it related to FTP_DIT_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0174 – Optional Ciphersuites for TLS	No	Superseded by TD283
0172 – Additional APIs added to FCS_RBG_EXT.1.1	No	This TD modifies the Assurance Activity for Windows Platforms. The TOE runs on Android.
0163 – Update to FCS_TLSC_EXT.1.1 Test 5.4 and FCS_TLSS_EXT.1.1 Test	No	This TD is only needed when the TOE does not support DHE or ECDHE.
0131 – Update to FCS_TLSS_EXT.1.1 Test 4.5	No	This TD addresses the Assurance Activity for FCS_TLSS_EXT.1. The TOE does not include FCS_TLSS_EXT.1.
0122 – FMT_SMF.1.1 Assignments moved to Selections	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP. Additionally, the TD has been archived.
0121 – FMT_MEC_EXT.1.1 Configuration Options	No	This TD addresses the SWFE EP. The TOE is not claiming conformance to the SWFE EP.
0119 – FCS_STO_EXT.1.1 in PP_APP_v1.2	Yes	
0107 – FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation	No	This TD address key generation (FCS_CKM.1). The TOE does not include key generation.

2.3 Conformance Rationale

This Security Target provides exact conformance to [ASPP] version 1.2. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

3. Security Problem Definition

The following Security Problem Definition is reproduced from [ASPP].

3.1 Threats

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.

3.2 Assumptions

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.

3.3 Organizational Security Policies

There are no Organizational Security Policies for the application.

4. Security Objectives

The following Security Problem Definition is reproduced from [ASPP].

4.1 Security Objectives for the TOE

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. This also includes providing control to the user regarding disclosure of any PII.

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. This also includes unnecessary network communications whose consequence may be the loss of 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.

4.2 Security Objectives for the Operational Environment

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.

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.

5. Security Requirements

This section contains the requirements that are provided by the TOE.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations completed in this Security Target.

Assignment: indicated in underlined text

Selection: indicated in italics

Assignments within selections: indicated in italics and underlined text

SFR operation completed or partially completed in the PP: Bold

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by letters in parentheses following the component or element (e.g., FAU_ARP.1(A)).

5.1 TOE Security Functional Requirements

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

Table 2 SFRs

SFR	Description
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.4	TLS Client Protocol
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_TUD_EXT.1	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

5.1.1 Cryptographic Support (FCS)

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The application shall implement HTTPS using TLS in accordance with [*FCS_TLSC_EXT.1*].

FCS_HTTPS_EXT.1.3 The application shall [*not establish the connection*] if the peer certificate is deemed invalid.

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [*invoke platform-provided DRBG functionality*] for its cryptographic operations.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [*invoke the functionality provided by the platform to securely store [X.509 certificates with associated keys]*] to non-volatile memory.

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The application shall [*invoke platform-provided TLS 1.2*] supporting the following cipher suites:

[

TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
TLS_ECDHE_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289
TLS_ECDHE_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289].

And no other cipher suites.

FCS_TLSC_EXT.1.2 The application shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The application shall establish a trusted channel only if the peer certificate is valid.

FCS_TLSC_EXT.4 TLS Client Protocol

FCS_TLSC_EXT.4.1 The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*secp256r1, secp384r1, secp521r1*].

5.1.2 User Data Protection (FDP)

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [*leverage platform-provided functionality to encrypt sensitive data*] in non-volatile memory.

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [
camera,
microphone,
location services,
[media stored in non-volatile memory]].

FDP_DEC_EXT.1.2 The application shall restrict its access to [*no sensitive information repositories*].

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [
user-initiated communication for [the Nubo Management Server]].

5.1.3 Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The application shall [*invoked platform-provided functionality*] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The application shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 2560*].
- The application shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kpcmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*HTTPS, TLS*].

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall [*not accept the certificate*].

5.1.4 Security Management (FMT)

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged user.

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [*no management functions*].

5.1.5 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [*require user approval before executing [user account creation]*].

5.1.6 Protection of the TSF (FPT)

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [no exceptions].

FPT_AEX_EXT.1.2 The application shall [*not allocate any memory region with both write and execute permissions*].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be compiled with stack-based buffer overflow protection enabled.

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [

- libOpenglRender.so
- librender.so
- com.afollestad.materialdialogs.internal
- com.crashlytics.android
- com.google.android.gms
- com.google.common
- com.google.firebase.iid
- com.google.firebase.messaging
- com.google.firebase.provider
- com.google.gson.internal.bind
- com.google.gson.reflect
- com.google.gson.stream
- com.google.j2objc.annotations
- com.google.thirdparty.publicsuffix
- me.zhanghai.android.materialprogressbar

- org.apache.commons.net
- org.apache.http.client.methods
- org.apache.http.entity
- org.apache.http.message
- sun.misc].

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [*leverage the platform*] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.1.3 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.1.4 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.5 The application shall [*leverage the platform*] to query the current version of the application software.

FPT_TUD_EXT.1.6 The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.1.7 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [*encrypt all transmitted data with [HTTPS, TLS]*] between itself and another trusted IT product.

5.2 TOE SFR Dependencies Rationale

[ASPP] contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.3 Security Assurance Requirements

The TOE assurance requirements for this ST are taken from [ASPP] which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 3 TOE Assurance Components Summary

Assurance Classes	Assurance Component	Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives
	ASE_REQ.1	Security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Lifecycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
	ALC_TSU_EXT.1	
Test	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

5.4 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Nubo Software to satisfy the assurance requirements. The table below lists the details.

Table 4 TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The

SAR Component	How the SAR will be met
	description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_TSU_EXT.1	Users of the Nubo Software Thin Client should report any security related issues via the Nubo Support web page, which provides a secure channel. Software updates/fixes are provided via the Google Play store. Public availability of an update for a publicly disclosed vulnerability is typically 90 days or less and a maximum of 180 days.
ATE_IND.1	Nubo Software will provide the TOE for testing.
AVA_VAN.1	Nubo Software will provide the TOE for testing.

6. TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 5 TOE Summary Specification SFR Description

SFR	Rationale
FCS_HTTPS_EXT.1	The TOE supports HTTPS using platform provided APIs. The functionality provided by the platform complies with RFC 2818 and uses TLS 1.2 (also provided by the platform). Therefore, the functionality described for FCS_TLSC_EXT.1 also applies.
FCS_RBG_EXT.1	The TOE uses the DRBG functionality provided by the Android platform. The platform's java.security.SecureRandom class is used for this functionality. The TOE itself does not use random numbers for any functions addressed by SFRs. Any random numbers used in SFR-related functions are initiated by the OS itself.
FCS_STO_EXT.1	The TOE stores one credential, as follows, • Credential: X509 Digital Certificates (and associated keys) for the Nubo Management Server • Usage: Authentication of the Nubo Management Server • Storage: Within the Android Key Store This is the only credential stored with the TOE. Additionally, the user of the TOE is prompted for a password on each login, but this information is passed transparently to the Nubo Management Server and is not stored on the Android platform or in the TOE.
FCS_TLSC_EXT.1	TLS support is provided by the platform that the TOE runs on. TLS support is restricted to v1.2 The following cipher suites are supported: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289 The TOE uses the underlying Android platform for all certificate validation. Android supports Common Name (CN) and Subject Alternative Name (SAN) (IP address and DNS) as reference identifiers. The TOE supports the use of wildcards in X.509 reference identifiers (CN and SAN). The TOE does not utilize certificate pinning.
FCS_TLSC_EXT.4	Android supports the following Elliptic Curve extensions (no configuration required): • secp256r1 • secp384r1 • secp521r1

SFR	Rationale
FDP_DAR_EXT.1	No user data is stored by the TOE. Configuration data is stored by the TOE in /data/data/package/shared_prefs/ with the MODE_PRIVATE flag set.
FDP_DEC_EXT.1	The TOE can access the camera, microphone, location services, and media stored in non-volatile memory resources of the platform. This access is to support the user's access of applications in the Nubo VMI. No sensitive information repositories are accessed.
FDP_NET_EXT.1	The TOE opens connections to the Nubo Management Server. No incoming connections are accepted.
FIA_X509_EXT.1	All certificate validation is performed by the underlying Android platform. The TOE relies upon Android for HTTPS/TLS; it also relies upon the platform for validation of X.509v3 certificates and checking the revocation status of the certificate. The presented Nubo Management Server certificates are validated against each certificate chain in the Android Trust Store. If a matching certificate chain is present, it is used for validation. This is done in a manner compliant with RFC 5280. The Android platform is used to verify fields within certificates related to usage, validity periods, revocation status and all other flags of a certificate. The Android platform supports OCSP. No configuration beyond installing the certificates in the Android Trust Store are required. The only functionality that leverages certificate validation are the connections with the Nubo Management Server.
FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 for server authentication for HTTPS/TLS connections. Presented Nubo Management Server certificates are validated against each certificate chain in the Android Trust Store. If a matching certificate chain is present, it is used for validation. When revocation status cannot be determined, certificates are not accepted as valid.
FMT_CFG_EXT.1	There are no default credentials within the TOE. Users of the TOE must activate with the Nubo Management Server before any applications in the Nubo VMI can be accessed. This involves providing the IP address for the Nubo Management Server. Subsequently, users of the TOE must login to the Nubo Management Server on each session (not the TOE); credentials collected from the user are passed transparently to the Nubo Management Server for processing.
FMT_MEC_EXT.1	Configuration data is stored by the TOE in /data/data/package/shared_prefs/ with the MODE_PRIVATE flag set. Configuration data stored by the TOE includes the user's First Name and Email address (specified by the user during activation) as well as the URL for the Nubo Management Server.
FMT_SMF.1	The TOE does not provide any management functions.
FPR_ANO_EXT.1	The TOE requests PII including, first and last name when creating a new Nubo account (note this account information is not stored on the TOE). A warning is displayed on the page indicating that this information will be transferred over the network. This information is sent to the Nubo Management Server. The user may additionally supply PII when interacting with applications in the Nubo VMI, but the TOE simply transparently transmits this data and is unaware of the nature of the data.
FPT_AEX_EXT.1	The TOE is a Java application; memory mapping and permissions on memory regions are not functions applicable to a Java application. Third party libraries are incorporated into the TOE; none of those map code to specific locations or include memory regions with both write and execute permissions. Third party libraries are compiled with the "-fstack-protector-all" flag.
FPT_API_EXT.1	The following Android Java APIs are invoked: • android.animation

SFR	Rationale
	• android.app.job • android.content.pm • android.content.res • android.database.sqlite • android.graphics.drawable • android.hardware • android.location • android.media.session • android.net • android.os • android.security • android.security.keystore • android.support.a.a • android.support.design.internal • android.support.design.widget • android.support.v13 • android.support.v4 • android.support.v7 • android.text • android.transition • android.util • android.view.accessibility • android.view.animation • android.view.inputmethod • android.webkit • android.widget • java.io • java.lang • java.math • java.net • java.nio.channels • java.nio.charset • java.security • java.security.spec • java.text • java.util.concurrent.atomic • java.util.concurrent.locks • java.util.jar • java.util.logging • java.util.regex • java.util.zip • javax.annotation.meta • javax.crypto • javax.crypto.spec • javax.net.ssl • javax.security.auth.x500 • org.json
FPT_LIB_EXT.1	The following libraries are packaged with the TOE:

SFR	Rationale
	• libOpenglRender.so • librender.so These are libraries from the OpenGL foundation and part of OpenGL ES 3.2 The following 3rd party java libraries were used: com.afollestad.materialdialogs.internal – Aidan Follestad, https://github.com/afollestad/material-dialogs, v 0.9.6.0 com.crashlytics.android Produced by http://fabric.io, v1 Google APIs: https://developers.google.com/android/reference/packages com.google.android.gms com.google.common com.google.firebase.iid com.google.firebase.messaging com.google.firebase.provider com.google.gson.internal.bind com.google.gson.reflect com.google.gson.stream com.google.j2objc.annotations com.google.thirdparty.publicsuffix me.zhanghai.android.materialprogressbar - https://github.com/DreaminginCodeZH/MaterialProgressBar v1.4.2 The Apache Software Foundation hc.apache.org, v4.5.6 org.apache.commons.net org.apache.http.client.methods org.apache.http.entity org.apache.http.message sun.misc - This package is part of android, but isn't listed as a package for developers because it is only called through other packages, v895bba
FPT_TUD_EXT.1	Users may use the Android platform to access Google Play store for updates/patches to the TOE. All releases are packaged in APK format and are signed with a Nubo Software certificate. Updates and fixes are obtained directly from the Google play store. Users of the Nubo Software Thin Client should report any security related issues via the Nubo Support web page, which provides a secure channel. Software updates/fixes are provided via the Google Play store. Public availability of an update for a publicly disclosed vulnerability is typically 90 days or less and a maximum of 180 days.
FTP_DIT_EXT.1	All external communications are protected by HTTPS/TLS.

End of Document