ioXt 2021 Base Profile

Version 2.0

Document C-03-25-01
Date 03/25/21
Document Status: Release

1. Notice of Use and Disclosure

Elements of ioXt Alliance documentation, specifications, and test plans may be subject to third party property rights, including without limitation copyrights and patents. The ioXt Alliance is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights.

This document and information contained herein are provided on a “AS IS” basis.

THE IOXT ALLIANCE DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD-PARTIES, OR ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR USE, TITLE, NON INFRINGEMENT, OR GUARANTEE OF PRODUCT SECURITY. IN NO EVENT WILL THE IOXT ALLIANCE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN.

The above notice must be included in all copies of this document.

2. Document Version Information

Version	Date	Author	Description
0.1	3/19/20	Brad Ree (ioXt)	1. Initial Draft
0.2	4/2/20	Brad Ree (ioXt)	1. Added introduction
0.3	4/2/20	Brad Ree (ioXt)	1. Updated abbreviations and definitions section.
0.4	4/2/20	Bridgette Roberts (ioXt)	1. Formatting for PC and AA.
0.5	4/2/20	Brad Ree (ioXt)	1. Editorial Edits.
1.00	4/16/20	Brad Ree (ioXt)	1. Release 1.00 Version
1.1	12/10/20	Brad Ree (ioXt)	1. Converted to Google Doc. 2. Added profile diagram 3. Converted test case list to include level info.
2.0	3/25/21	Brad Ree (ioXt)	1. Modified verified software stack to move Anti-rollback out of baseline

1. Introduction

1.1. Purpose

This document provides the specifications required to certify a device such that the manufacturer may use the ioXt Compliance mark. This specification defines which devices may be certified under the profile, along with the test plan which must be met. The test cases are defined in the ioXt Test Case Library document.

In general, a profile shall define the devices which may be certified using the profile, a threat model, and test plan. The ioXt 2020 base profile shall cover all devices which are not covered under another profile. Thus, the device definition is significantly different from other profiles. Further, there is not a threat model provided.

ioXt approved labs must be explicitly approved to execute this profile and shall be governed with the ioXt Lab Agreement.

1.2. Acronyms and Abbreviations

Acronym	Definition
VDP	Vulnerability Disclosure Program or Vulnerability Reporting Pledge
AA	Automatically Applied Update Pledge
SE	Security Expiration Date Pledge
VS	Verified Software Pledge
UP	No Universal Password Pledge
PC	Proven Cryptography Pledge
SI	Secured Interface Pledge

1.3. Definitions

Term	Definition
Anti-rollback	Preventing a device from accepting a software update which is older than the current version.
Manufacturer	The entity which is certifying the device. This may be the company which produces the device, or the company which is marketing the device to the end consumer.
ioXt Pledge	A single security principal which a manufacturer agrees to fulfil.
ioXt Yardstick	The definition of the core elements for each Pledge item which must be met to achieve a specific level for each pledge item.
ioXt Test Case Library	This document describes all test cases which are recognized by the ioXt Alliance.
Profile	A device specific test plan which must be met in order to be certified by the ioXt Alliance.

1.4. References

2. Profile Scope

This profile may be used for all devices which are not covered under another profile's device definition.

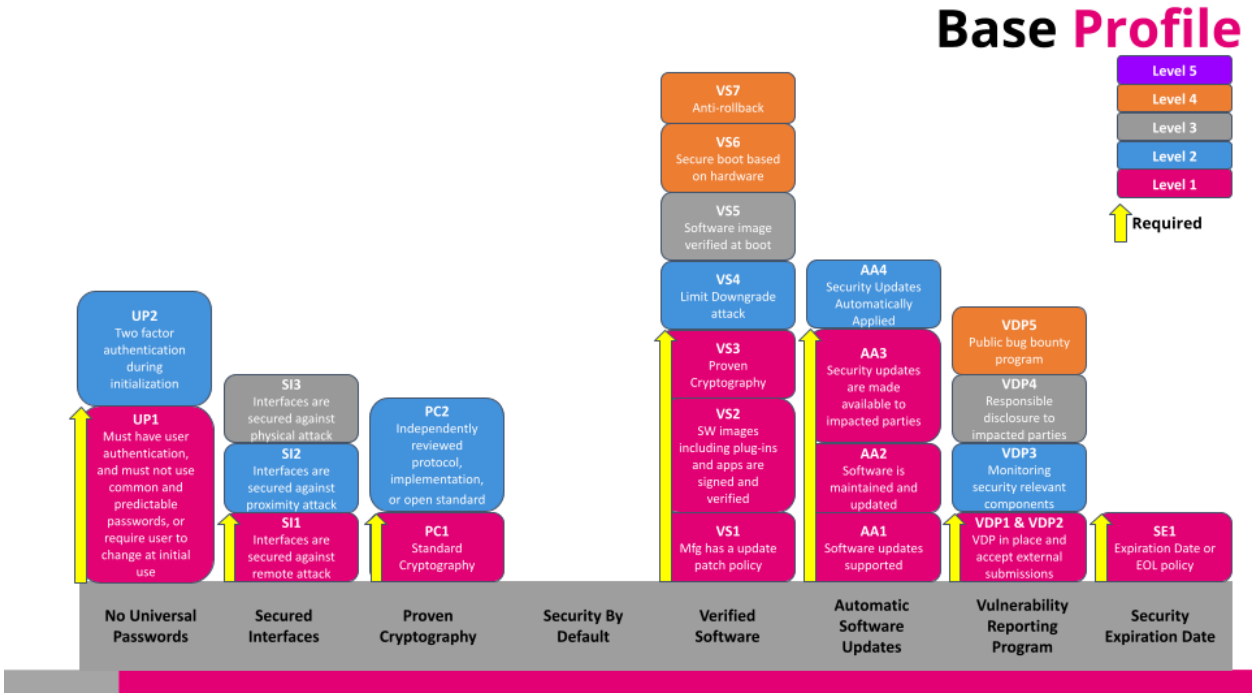
3. Requirements

3.1. Test Case Library Version

The profile requirement document only describes the test cases needed for certification by test case ID. The actual text of the test cases are located in the ioXt Test Case Library. As the test case library is a shared document used by all profiles, there may be newer versions of the library than was approved when this profile was created.

The ioXt 2021 Base profile version 2.0 shall only use the ioXt Test Case Library version 5.0.

3.2. Profile Summary



3.3. Proven Cryptography

3.3.1. Requirements

ID	Test Case
PC1	Standard cryptography
PC2	Independently reviewed protocol, implementation, or open standard

3.3.2. Security Levels

Security Level	Test Cases	Required For Certification
1	PC1	Yes
2	PC2	

3.4. No Universal Password

3.4.1. Requirements

ID	Test Case
UP1	User credentials shall not be common or predictable, or the credentials must be required to change at initial use.
UP2.1	Availability of two factor authentication for products which have a user facing interface during initialization
UP2.2	Availability of two factor authentication for products which have a user facing interface during management

3.4.2. Security Levels

Security Level	Test Cases	Required for Certification
1	UP1	Yes
2	UP2.1 UP2.2	

3.5. Verified Software

3.5.1. Requirements

ID	Test Case
VS1	Manufacturer has an update patch policy
VS2	Software images including plug-ins and apps are signed and verified
VS3	Proven Cryptography
VS4	Limit Downgrade Attack
VS5	Software images verified at boot time
VS6	Secure boot based on hardware root of trust
VS7	Anti-Rollback

3.5.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VS1 VS2 VS3	Yes
2	VS4	
3	VS5	
4	VS6 VS7	

3.6. Security by Default

3.6.1. Requirements

ID	Test Case
N/A	This profile does not have any test cases for this pledge item.

3.6.2. Security Levels

Security Level	Test Cases	Required for Certification
1	None	Yes

3.7. Secured Interfaces

3.7.1. Requirements

ID	Test Case
SI1.1	Remote Attack: All certifiable protocols used on the interfaces contained in the device shall be Certified
SI1.2	Remote Attack: Unused Services are disabled
SI1.3	Remote Attack: Authentication
SI1.4	Remote Attack: Secured Communications

SI2.1	Proximity Attack: Unused Services are disabled
SI2.2	Proximity Attack: Authentication
SI2.3	Proximity Attack: Secured Communications
SI3.1	Local Attack: Debug ports are disabled

3.7.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SI1.1 SI1.2 SI1.3 SI1.4	Yes
2	SI2.1 SI2.2 SI2.3	
3	SI3.2	

3.8. Automatically Applied Updates

3.8.1. Requirements

ID	Test Case
AA1	Software updates supported
AA2	Software is Maintained and Updated
AA3	Software updates are made available to impacted parties
AA4	Security Updates applied automatically, when product usage allows

3.8.2. Security Levels

Security Level	Test Cases	Required for Certification
1	AA1 AA2 AA3	Yes

2	AA4	

3.9. Vulnerability Reporting Program

3.9.1. Requirements

ID	Test Case
VDP1	VDP in place
VDP2	Accept external submissions
VDP3	Monitoring security relevant components.
VDP4	Responsible disclosure of defects to impacted parties that must take action.
VDP5	Public Researcher Rewards program

3.9.2. Security Levels

Security Level	Test Cases	Required for Certification
1	VDP1 VDP2	Yes
2	VDP3	
3	VDP4	
4	VDP5	

3.10. Security Expiration Date

3.10.1. Requirements

ID	Test Case
SE1.1	End of life notification policy is published
SE1.2	Expiration Date is published

3.10.2. Security Levels

Security Level	Test Cases	Required for Certification
1	SE1.1 or SE1.2	Yes