|  |  |  |
| --- | --- | --- |
|  | Document:  **Cypress Privacy & Security Requirements Verification By Analysis and Inspection** | Document #:  **CI6782-140-001** |

**Document Title**

# Cypress Privacy & Security Requirements Verification by Analysis and Inspection

**Project Number**

# CI6782

### Revision

«version\_label»

Page 1 of 7

Confidential & Proprietary to Beckman Coulter

|  |  |  |
| --- | --- | --- |
|  | Document:  **Cypress Privacy & Security Requirements Verification By Analysis and Inspection** | Document #:  **CI6782-140-001** |

## Introduction

### Purpose and Scope

The purpose of this document is to verify Cypress Software Requirements related to privacy and security by analysis and inspection.

### Definitions

### See CI6782-005 Cypress Project Glossary

### Reference Documents

* CI6782-058-001 Cypress Gradient Maker V&V Trace Matrix
* CI6782-081-002 Vulnerability Scan Reports
* CI6782-081-003 Cypress Gradient Maker Penetration Test Report build 0.3.0
* CI6782-081-004 Second Round Vulnerability Scan Reports
* CI6782-082 Cypress Gradient Maker Privacy and Security Risk Assessment
* CI6782-083 Cypress Gradient Maker Software Architecture and Design
* CI6782-149-003 Cypress Software Test Protocol Approve
  + Kiosk Mode Protocol
* CI6782-149-004 Cypress Software Verification - Round 1 Execution Results (for software version 1.0.0)
  + Kiosk Mode Protocol

## Design Inputs

### Design Inputs

The software module requirement in scope of this document are found in the Cypress Gradient Maker V&V trace matrix.

## Analysis and Inspection Detail

Page 2 of 7

Confidential & Proprietary to Beckman Coulter

|  |  |  |
| --- | --- | --- |
|  | Document:  **Cypress Privacy & Security Requirements Verification By Analysis and Inspection** | Document #:  **CI6782-140-001** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Software MR** | **Analysis and Inspection** | | **Pass/Fail** |
| [CI6782-101](https://lsjira.beckman.com/browse/CI6782-101)  The system shall encrypt data in transit across external connections. | External connections, i.e., that of software update and BeckmanConnect, originates from the instrument controller, and use HTTPS protocol. Inspection of *control/os-module.ss* and *beckman-connect/beckman-connect-module.ss* has confirmed this. | | Pass |
| [CI6782-102](https://lsjira.beckman.com/browse/CI6782-102)  The system shall run allow-listing software. | * AppArmor is used to allow list operations by the os operations by the software. OS operations are restricted to read the os-module.boot and read and execute the following system programs: last, systemd-id128, ip, hostname, netplan (via sudo) and its dependencies, rauc and its dependencies, fbi, cp, rm, reboot, and curl /app. Inspection of *install/Makefile*, *install/apparmor/os-module* are consistent with the above design. * Seccomp is used to allow list system calls used by each container, all containers are using the default seccomp policy at */usr/share/containers/seccomp.json.* Inspection of *install/Makefile* is consistent with the above design. | | Pass |
| [CI6782-121](https://lsjira.beckman.com/browse/CI6782-121)  The instrument shall have a firewall that only exposes one in bound and four outbound ports.  **Detailed Description**   |  |  |  | | --- | --- | --- | | **Port** | **Feature** | **Version** | | 443 - outbound | Software Update | v1.0 | | 123 - outbound | NTP | v1.0 | | 443 - outbound | BeckmanConnect | v1.0 | | 53 - outbound | DNS | v1.0 | | 67 - outbound | DHCP | v1.0 | | 54880 - inbound | Remote UI | v2.0 | | 636 - outbound | LDAP | v2.0 | | | The software uses *ufw (Uncomplicated Firewall)* and itexposes only four outbound ports by inspecting *install/Makefile*:   * DNS (53) * DHCP/bootp (67) * NTP (123) * HTTPS (443)   Cypress 1.0 does not include Remote UI nor LDAP. | Pass |

Page 3 of 7

Confidential & Proprietary to Beckman Coulter

|  |  |  |
| --- | --- | --- |
|  | Document:  **Cypress Privacy & Security Requirements Verification By Analysis and Inspection** | Document #:  **CI6782-140-001** |

|  |  |  |
| --- | --- | --- |
| **Software MR** | **Analysis and Inspection** | **Pass/Fail** |
| [CI6782-122](https://lsjira.beckman.com/browse/CI6782-122)  The software shall include only the minimum necessary operating system components and utilities required for operation of the system. | The software uses a communize the container images to use the same *ubuntu:jammy (22.04)* base image  in order to reduce the number of different versions of supporting software baked into these images. Inspection of *src/Makefile* and *src/ubuntu/* folder confirmed that. | Pass |
| [CI6782-123](https://lsjira.beckman.com/browse/CI6782-123)  The instrument shall implement applicable security and hardening standards as defined by the Center for Internet Security's Linux Benchmarks and track the alignment to those standards through CI6782-086 Security and Hardening Checklist. | * Inspection of *install/Makefile* has confirmed that the software build process has integrated the OpenSCAP checklist to perform automated vulnerability assessment and policy compliance evaluation. The output is reported in CI6782-086 Security and Hardening Checklist. * Penetration testing is performed on the installed instrument. * Nessus scan is performed on the installed instrument. | Pass |
| [CI6782-60](https://lsjira.beckman.com/browse/CI6782-60)  As a user, I need the system to comply with data privacy and security standards. | The Cypress software handles Personally Identifiable Information (PII) in the form of customer name and email during BeckmanConnect enrollment. The software must ensure that the PII is protected. To do this, the BeckmanConnect Module uses OpenSSL for generating an asymmetric key pair. A new key pair is generated when the container starts up. The private key is an RSA key with 2048 bits. The key is generated on start up instead of having the key as part of the container to prevent an attacker from potentially extracting the private key from a software image, which anyone can download. Because the key is generated every time the container starts, the PII data in the Atlas logs are effectively destroyed. The public key is published by copying its string contents to Atlas state in modules/BeckmanConnect/key. The UI module can use it for encrypting the customer name and email. When the encrypted data is sent to Atlas to pass into a method, any logging done by Atlas will only capture the encrypted data. When finally passed into the BeckmanConnect Module to process, it decrypts with its private key. | Pass |

Page 4 of 7

Confidential & Proprietary to Beckman Coulter

|  |  |  |
| --- | --- | --- |
|  | Document:  **Cypress Privacy & Security Requirements Verification By Analysis and Inspection** | Document #:  **CI6782-140-001** |

|  |  |  |
| --- | --- | --- |
| **Software MR** | **Analysis and Inspection** | **Pass/Fail** |
| [CI6782-192](https://lsjira.beckman.com/browse/CI6782-192)  The *Gradient Maker* shall comply with items identified in CI6782-081 Cypress Gradient Maker Product Privacy and Security Plan. | Based on inspection and analysis from the rows above in this table, in addition:   * The software can check and fetch software update located at Microsoft Azure Storage using HTTPS, and install such software update. * By inspecting *install/Makefile* and *src/containers,* the software employs Chromium security policies and reduce the number of virtual terminals to one to prevent breaking out of the kiosk mode. It is verified by the Kiosk Mode verification protocol.   Therefore, the software fully complies with the items identified in CI6782-081 Cypress Gradient Maker Product Privacy and Security Plan. | Pass |

## Content Change Abstract

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Level** | **Date** | **Author Name** | **Change Description** |
| 1.1 | 11/5/2024 | Peng Wang | Initial Release |

1. **Approvals**

The following approvals are required for this document:

Development Quality

My signature confirms my review and approval of this document for its intended use.

**APPROVALS: APPROVED ON: *(mm-dd-yyyy)***

Page 5 of 7

Confidential & Proprietary to Beckman Coulter