Open Issues and/or Actions

No open issues

|  |  |
| --- | --- |
| **Open Issue** | **Issue description** |
|  |  |
|  |  |

Table of Contents

[1 Document Introduction 3](#_Toc488301653)

[1.1 Purpose 3](#_Toc488301654)

[1.2 Scope 3](#_Toc488301655)

[1.3 References 3](#_Toc488301656)

[1.4 Terminology & Abbreviations 3](#_Toc488301657)

[2 Overview 5](#_Toc488301658)

[3 Requirements 5](#_Toc488301659)

[3.1 CommLib 5](#_Toc488301660)

[3.1.1 Interface Requirements 5](#_Toc488301661)

[3.1.2 General Requirements 9](#_Toc488301662)

[3.1.3 Function/Feature Requirements 9](#_Toc488301663)

[4 Revision History 13](#_Toc488301664)

[5 Approval 13](#_Toc488301665)

[6 <Appendices> 14](#_Toc488301666)

# Document Introduction

## Purpose

This document describes the requirements.

## Scope

This document describes the requirements for work completed in PI 17.3 for components as marked in below diagram with CommLib.



Figure 1: Bundling of documents for BlueLib and CommLib

## References

| **Reference** | **Identification** | **Title / additional remarks** |
| --- | --- | --- |
| DICOMM | JohSun-20160115-04V01 | Software Interface Specification  DiComm |
|  |  |  |
|  |  |  |

## Terminology & Abbreviations

| **Terminology & Abbreviations** | **Description/Definition** |
| --- | --- |
| Appliance | A device which includes a DI Comm connectivity node and allows communication over a supported channel. |
|  |  |

# Overview

The components in scope together provide a technical component for connecting with connectivity nodes which implement the DI Comm protocol (see [DICOMM]).

# Requirements

## CommLib

### Interface Requirements

#### Technical Interfaces

|  |  |
| --- | --- |
| **The component must provide certain properties of a discovered peripheral** | ID: 22226, POF: -, Safety: -, Security: -  State: Approved, 2017-Jul-17 09:11 |
| Description:   The iOS connectivity components must provide the following properties of a discovered peripheral:   * CppId * ModelId   The Android connectivity components must provide the following properties of a discovered peripheral:   * ModelId | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **Passthrough of pairing parameters from CommLib to peripheral** | ID: 26124, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:08 |
| Description:   A pairing call must be available on CommLib containing the same parameters as specified on the dicomm pairing port. | |
| Acceptance Criteria:   A pairing call for user pairing is available on CommLib | |

|  |  |
| --- | --- |
| **Firmware Port provide a canUpgrade property** | ID: 32852, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:09 |
| Description:   * The Firmware Port shall expose a 'canUpgrade' property, indicating if the device can do Firmware upgrade or not. This must reflect the state of the same property in the  connectivity node's firmware port. * It's up to the app developers to read this property when attempting a firmware upgrade | |
| Acceptance Criteria:   1. The app developer can access a firmware port property to check if the device can do firmware upgrade or not 2. The value of this property is the same as the value of the canUpgrade property on the connectivity node's REST or BLE interface. 3. Release notes is updated | |

|  |  |
| --- | --- |
| **The component must pin an encountered TLS certificate for a persistently stored DiComm appliance when a first DiComm response is received.** | ID: 35799, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 08:57 |
| Description:   A pinned certificate is called a "pin". | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **Pins shall have infinite lifetime for managed DiComm appliances** | ID: 35800, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 08:58 |
| Description:  Pins for managed DiComm appliances must not expire.  Pins must be persisted for connected managed DiComm appliances. | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component shall refuse to connect to a managed connected appliance via DiComm over the LAN if the certificate does not match the pin.** | ID: 35801, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 09:06 |
| Description:  When no pins match the certificate of the managed connected appliance, a callback or error must be given on the public interface of the component. This fact must be available to the caller even after the moment it occurred. | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component must allow the caller to add the non-matching certificate as a pin.** | ID: 35804, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 09:05 |
| Description:  When the non-matching certificate is added as a pin, this must re-establish the possibility for connection with the managed appliance. | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component must still allow DI Comm communications over LAN HTTPS with App Transport Security enabled on iOS. The component is allowed to require exceptions to App Transport Security for local networking.** | ID: 37176, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 09:07 |
| Description: | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component must use HTTPS to communicate over LAN with connectivity nodes which support HTTPS.** | ID: 37177, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 09:09 |
| Description:   The component must use HTTPS to communicate over LAN with connectivity nodes which support HTTPS.  The component must allow models to be configured to support either HTTP or HTTPS. If a model is not configured, the component must treat the model as configured to support HTTPS.  The component must not use HTTP to connect to connectivity nodes which are configured to support HTTPS.  The component must not use HTTPS to connect to connectivity nodes which are configured to support HTTP.  The component must accept connections with connectivity nodes which have self-signed certificates, except where other requirements state otherwise.  The component must communicate with the connectivity node in accordance with [DICOMM] (SwIS DIComm Protocol) as intended for HTTPS and HTTP. | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component must support LAN DIComm ChangeIndications** | ID: 37178, POF: -, Safety: -, Security: -  State: Approved, 2017-Jul-17 09:10 |
| Description:   When connecting with a connectivity node through LAN, the component must listen for, receive and decrypt DIComm ChangeIndication UDP packets from the connectivity node in accordance with [DICOMM] (SwIS DIComm Protocol). | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **The component must provide its version number on a public interface.** | ID: 60027, POF: -, Safety: -, Security: -  State: Approved, 2017-Jul-17 09:10 |
| Description: | |
| Acceptance Criteria: | |

### General Requirements

|  |  |
| --- | --- |
| **The component must log pinning, re-pinning and pin mismatch events.** | ID: 36191, POF: -, Safety: -, Security: Yes  State: Approved, 2017-Jul-17 09:06 |
| Description: | |
| Acceptance Criteria: | |

### Function/Feature Requirements

|  |  |
| --- | --- |
| **Up to date list of discovered BLE peripherals** | ID: 15920, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:09 |
| Description:   If enabled to do so, the mobile connectivity components must update the list of discovered BLE peripherals.  A discoverable peripheral must be added to the list within at most 120 seconds.  A discoverable peripheral that is already in the list, must stay in the list.  A non-discoverable peripheral must be removed from the list within at most 120 seconds. | |
| Acceptance Criteria:   All tests in tab "links" must pass | |

|  |  |
| --- | --- |
| **Filter NetworkNodes based on a filter of ModelId's** | ID: 17381, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:10 |
| Description:  For the purpose of discovering connected products, the mobile components must provide the ability to filter on specified ModelIds.  Providing an unfiltered list must also be possible. | |
| Acceptance Criteria: | |

|  |  |
| --- | --- |
| **Firmware Upgrade deployment timeout must be configurable** | ID: 17821, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:10 |
| Description:   The mobile connectivity components must accommodate its clients to set the value of the deployment timeout.  In case of the timeout running out,  the mobile connectivity components must send  a 'deployment failed with timeout' error to its clients. Otherwise, the mobile connectivity components must send  a 'deployment successful' message to its clients.  Note: deployment timeout here means the maximum time is allowed for the peripheral to go from running the old version to running the new version of the firmware.  Note: The mobile connectivity components have no way of knowing if the actual deployment succeeded if the timeout occurs because the device is out of range. | |
| Acceptance Criteria:   If a timeout is set shorter than a successful deployment then a 'deployment failed with timeout' error must be sent.  If a timeout is set longer than a successful deployment then  a 'deployment successful' message must be sent. | |

|  |  |
| --- | --- |
| **Firmware Upgrade push timeout must be configurable** | ID: 17830, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:11 |
| Description:   The mobile connectivity components must accommodate its clients to set the value of the push timeout.  In case of the timeout running out,  the mobile connectivity components must send  a 'push failed with timeout' error to its clients.  Note: Push timeout here means the maximum time is allowed for the peripheral to go from one firmware upload related state to the next. See the state diagram in JohSun-20160115-04V01 Software Interface Specification DiComm. | |
| Acceptance Criteria:   If a timeout is set shorter than a successful internal state transition then a 'push failed with timeout' error must be sent.  If a timeout is set longer than a successful deployment then no error must be sent. | |

|  |  |
| --- | --- |
| **Firmware Upgrade cancel timeout must be configurable** | ID: 17833, POF: -, Safety: -, Security: -  State: Approved, 2017-May-10 13:11 |
| Description:   The mobile connectivity components must accommodate its clients to set the value of the cancel timeout.  In case of the timeout running out,  the mobile connectivity components must send  a 'cancel failed with timeout' error to its clients.  Note: Cancel timeout here means the maximum time is allowed for the peripheral to go from one firmware upload related state to the 'cancel' state. See the state diagram in JohSun-20160115-04V01 Software Interface Specification DiComm. | |
| Acceptance Criteria:   If a timeout is set shorter than a successful internal state transition to the 'cancel' state then a 'cancel failed with timeout' error must be sent.  If a timeout is set longer than a successful deployment then a 'cancel successful' message must be sent. | |

# Revision History

| **Version** | **Date** | **Author** | **Description of Change** | **Reason for Change** |
| --- | --- | --- | --- | --- |
| 0.1 | 2017-05-10 | Matthijs Piek | Initial version |  |
| 1.0 | 2017-05-12 | Matthijs Piek | Version changed | Review yielded no remarks, so version put to 1.0 for approval\* |
| 1.1 | 2017-07-13 | Jaime Visser | Updated requirements from TFS | Platform release 2.2.0 |
| 2.0 | 2017-07-20 | Jaime Visser | Fix footer, update TOC and version change | Fix review remarks, version 2.0 for approval |

\* Approval of 1.0 document will be given after approval date for Verification Reports and Test Protocol. This was possible because individual requirements have been approved earlier.

# Approval

| **Name** | **Role / Function** | **Date** (YYYY-MON-DD) | **Signature** |
| --- | --- | --- | --- |
| Ernest Angles Isern | Chapter Architect |  |  |
|  |  |  |  |

# <Appendices>

Not applicable: no appendices.