

**Connected X Cyber Security**

**Bluetooth Security Requirements**

Version 1.0

**UNCONTROLLED COPY IF PRINTED**

**FORD CONFIDENTALF**

# Version History & Table of Contents

## Table of Contents

[1 Version History & Table of Contents 2](#_Toc519072904)

[1.1 Table of Contents 2](#_Toc519072905)

[1.3 Revision History: 3](#_Toc519072906)

[2 Requirements 4](#_Toc519072907)

[2.1 Functional Requirements 4](#_Toc519072908)

[2.1.1 4](#_Toc519072909)

[2.1.2 4](#_Toc519072910)

[2.1.3 5](#_Toc519072911)

[2.1.4 5](#_Toc519072912)

[2.1.5 6](#_Toc519072913)

[2.1.6 6](#_Toc519072914)

[2.1.7 6](#_Toc519072915)

[2.1.8 7](#_Toc519072916)

[2.1.9 7](#_Toc519072917)

[2.1.10 7](#_Toc519072918)

## 

## Revision History:

| **Version** | **Revision Date** | **Description of Change** | **Affected Sections** | **Author** |
| --- | --- | --- | --- | --- |
| V0.1 | 7/15/2018 | Initial Version | N/A | Matt Burris |
| V0.2 | 9/25/2018 | Feedback changes | 2, 2.1.9, | Matt Burris |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Requirements

All security requirements must be met. However, specific features and applications may require additional security constraints not addressed in this document.

## Functional Requirements

### 

###BT\_SEC\_00001### Bluetooth Security Modes

Devices allowing Bluetooth connections shall use the strongest Security Mode that is available. The latest Bluetooth version should be used, but if unavailable the following list defines Security Modes that shall be used for each applicable version:

* Bluetooth 1.4 devices that support BR, EDR and High Speed (HS) shall use Security Mode 4, Level 4
* Bluetooth 2.1 through 4.0 devices shall use Security Mode 4, Level 3
* Bluetooth 2.0 and older devices shall use Security Mode 3
* Security Mode 1 shall never be used
* For Low Energy Bluetooth, devices shall use Security Mode 1 Level 4 when available, 4.0 and 4.1 devices shall use Security Mode 1 Level 3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00001###** | | | | | | |
| **Rationale** | | | | | | |
| Using the highest level Security Mode possible protects Bluetooth devices from known exploits and vulnerabilities. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Bluetooth device uses correct security mode | | | | | | DV Testing and Review |
| **Notes** | | | | | | |
| Not all security modes are supported by each version of Bluetooth. Security modes define how well the device protects Bluetooth communications, and how well the device is protected from potential attacks. Security Mode 1 devices do not initiate any security and should not be used. NIST Special Publication 800-121. | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00002### Bluetooth Configuration Settings

Bluetooth devices shall not use default configuration settings including the default PIN code. Each device shall be configured to use a randomly-generated PIN code, and PINs shall be unique per module.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00002###** | | | | | | |
| **Rationale** | | | | | | |
| Bluetooth devices using the default settings, including the default PIN code, are susceptible to eavesdropping and unauthorized access to data. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Device is not using default PIN code * Device name should be changed to something non-descriptive to avoid revealing the platform type * Device is using separate, randomly-generated PIN code for each connection | | | | | | DV Testing and Review |
| **Notes**  NIST Special Publication 800-121. | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00003### Security Mode 4 Compatibility

Bluetooth devices in Security Mode 4 can fall back to a lower Security Mode when connecting to devices that do not support Security Mode 4. Devices shall not use Security Mode 1 even in circumstances where Security Mode 4 is not available. If a Bluetooth device in Security Mode 4 must fall back to a lower level for backward compatibility, Security Mode 3 shall be used

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00003###** | | | | | | |
| **Rationale** | | | | | | |
| Bluetooth Security Mode 1 offers no security and is susceptible for man-in-the-middle attacks. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Device uses appropriate Security Mode * Device does not allow lower Security Mode | | | | | | DV Testing |
| **Notes**  NIST Special Publication 800-121. | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00004### Link Keys

Link keys shall not be reused, and shall not be based on unit keys. Instead, pairing shall use combination keys, which are generated at each device pairing.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00004###** | | | | | | |
| **Rationale** | | | | | | |
| Using shared, static unit keys can leave communications open to spoofing, eavesdropping and man-in-the-middle attacks from previously trusted devices. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Link keys shall not be based on unit keys | | | | | | DV Testing |
| **Notes**  Unit keys are generated in a single device during the installation process and reused for future pairings. Link keys should be derived from a non-static key based on information from both parties, such as a combination key. NIST Special Publication 800-121. | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00005### Devices shall be undiscoverable

Bluetooth devices shall be configured to be undiscoverable by default and remain undiscoverable outside of pairing.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00005###** | | | | | | |
| **Rationale** | | | | | | |
| Leaving a device discoverable outside of needed pairing leaves it unnecessarily exposed to outside threats. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Bluetooth device shall not be discoverable outside of pairing process | | | | | | DV Testing |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00006### Link Encryption

Link encryption shall be used to secure all data transmissions over Bluetooth. Encryption key sizes shall be configured to be the maximum allowable.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00006###** | | | | | | |
| **Rationale** | | | | | | |
| Unencrypted data sent over Bluetooth transmission is vulnerable to eavesdropping. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Bluetooth devices shall invoke link encryption for communications | | | | | | DV Testing |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00007### Mutual Authentication

Except in cases where PIN pairing is not available Mutual authentication shall be required for all device connections. Exceptions may be made in cases where PIN pairing is not available, such as BLE.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00007###** | | | | | | |
| **Rationale** | | | | | | |
| Mutual authentication provides assurance that devices connecting via Bluetooth are legitimate. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * PIN verification shall be required on both the Bluetooth device and the device being paired. * Bluetooth devices shall prompt the user to authorize all incoming pairing requests before any connection is allowed to proceed | | | | | | DV Testing and Review |
| **Notes**  Not all Bluetooth pairing modes support mutual authentication, such as “Just Works” mode which allows for connections without verifying via PIN on one of the devices. | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

### 

###BT\_SEC\_00008### Broadcast Disabled When Not in Use

All Bluetooth capabilities shall be disabled when not in use except for BLE applications.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00008###** | | | | | | |
| **Rationale** | | | | | | |
| Disabling Bluetooth except when specifically needed by the user minimizes exposure to potential malicious activities. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Bluetooth radio/streaming disabled when no device is connected | | | | | | DV Testing and Review |
| **Notes**  An example would be a vehicle that has no Bluetooth devices paired should not allow audio streaming over Bluetooth. | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 7/15/2018 | Mburris6 | Initial version | | | |

###BT\_SEC\_00009### Fuzz Testing

All Bluetooth devices shall undergo fuzz testing using a tool approved by Ford.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00009###** | | | | | | |
| **Rationale** | | | | | | |
| Fuzz testing provides random data to a system’s inputs. This technique is useful on all systems, especially when they can accept inputs from other interfaces. Fuzz testing is also useful for testing the stability of a system. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * System does not become unresponsive * System does not perform abnormally | | | | | | DV Testing and Review |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** | NIST Guide to Bluetooth Security Revision 2 | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 8/7/2018 | Mburris6 | Initial version | | | |

###BT\_SEC\_00010### Bluetooth MAC

Bluetooth MAC addresses shall not be the same as or within one digit of the corresponding WLAN MAC address.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Requirement ID: ###BT\_SEC\_00010###** | | | | | | |
| **Rationale** | | | | | | |
| Bluetooth devices using the default settings, including the default PIN code, are susceptible to eavesdropping and unauthorized access to data. | | | | | | |
| **Acceptance Criteria** | | | | | | **V&V Method** |
| * Bluetooth MAC is not sequential to WLAN MAC * Bluetooth MAC is not the same as the WLAN MAC * Bluetooth MAC is not within one digit of the WLAN MAC | | | | | | DV Testing and Review |
| **Notes** | | | | | | |
|  | | | | | | |
| **Type** | | Functional | | **Source** |  | |
| **Priority** | | High (Mandatory) | | **Source Req.** | <Put any parent requirement trace link here> | |
| **Status** | | Draft | | **Owner** | Matt Burris | |
| **Change Log** | | | | | | |
| **Version** | **Date** | **Author** | **Change** | | | |
| 1.0 | 11/1/2018 | Mburris6 | Initial version | | | |