DoD Bluetooth Peripheral Device Security Requirements

(16 July 2010)

This document specifies requirements necessary for the secure use of unclassified Bluetooth peripheral devices in the U.S. Department of Defense.

1 Basic Requirements

1.1 For personal area network applications, Bluetooth devices must use low-power Class 2 or Class 3 Bluetooth radios without external amplifiers or high-gain antennas.

1.2 Devices must not use the Bluetooth 3.0 High Speed (3.0 + HS) alternate MAC and PHY or Bluetooth 4.0 Low Energy (LE) technology.

1.3 Devices must use easily-understandable connection, configuration, and link activity status indicators like LEDs or icons.

1.4 Devices must only support the minimum number of Bluetooth services required for operational use of approved Bluetooth peripherals. Services should be enabled only while needed. Devices or administrators must reliably disable or delete all unneeded Bluetooth services.

1.5 Devices or administrators must reliably disable or delete all unneeded Bluetooth user controls, drivers, application programming interfaces, executables, and applications.

1.6 Devices must use random number values and public/private key pairs that achieve maximum entropy for all cryptographic functions as mandated and defined in the Bluetooth specifications and based on applicable NIST guidelines.

1.7 Each Bluetooth device intended for use in the DoD should be subjected to an independent security implementation evaluation conducted by one or more qualified and objective individuals approved by DISA Field Security Operations. Evaluators must work with the vendor to mitigate any security deficiencies prior to approval for DoD use.

1.8 Once approved for DoD use, operational Bluetooth devices and piconets must be independently monitored for unauthorized Bluetooth activity.

1.9 Bluetooth devices must be transported and stored securely by users and administrators at all times.

2 Connectivity Requirements

2.1 Discoverability

2.1.1 Bluetooth devices must not be discoverable (responsive to inquiry messages from other Bluetooth devices) unless absolutely necessary. Ideally devices should never be discoverable.

2.1.2 Devices must never be discoverable for longer than two minutes at any one time.

2.2 Connectability

2.2.1 Bluetooth devices must not be connectable (responsive to incoming connection requests from other Bluetooth devices) unless absolutely necessary. Ideally devices should become unconnectable once the connection is established, or should never be connectable if operationally possible.

2.2.2 Devices should initiate Bluetooth connections only when absolutely necessary. Ideally only one device per Bluetooth piconet should initiate connections to other devices in that piconet.

2.3 Auto-Reconnect

2.3.1 Page frames from devices attempting to automatically re-establish Bluetooth links to peripheral devices must be transmitted periodically and not continuously.

2.3.2 Bluetooth devices must not transmit auto-reconnect frames longer than 30 seconds at any one time or more frequently than once every five minutes.

2.3.3 Bluetooth devices must never transmit auto-reconnect frames longer than 20 minutes total.

3 Authorization Requirements

3.1 Bluetooth devices must prompt the user to authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed.

3.2 Users must never accept connections, files, or other objects from unexpected, unknown, or untrusted sources.

4 Pairing and Authentication Requirements

4.1 General Pairing and Authentication Requirements

4.1.1 During initial Bluetooth connection requests, all Bluetooth devices must pair (mutually authenticate) and bond (store the resulting link key).

4.1.2 Devices must store link keys securely based on applicable NIST guidance.

4.1.3 Subsequent to pairing, all Bluetooth devices must again mutually authenticate each other during all connection requests.

4.1.4 Devices must not delete existing link keys until after a replacement link key is generated successfully.

4.1.5 All Bluetooth pairing should be done as infrequently as possible, ideally in a secure location (e.g., an indoor non-public area away from windows and behind physical access controls) where attackers cannot realistically observe entry of the passkey or intercept transmitted pairing messages.

4.1.6 Users or administrators must never enter or confirm pairing passkeys when unexpectedly prompted to do so.

4.1.7 Users or administrators must immediately remove unused, lost, stolen, or discarded Bluetooth devices from paired device lists.

4.1.8 Bluetooth devices must use either legacy pairing Security Mode 3 link level security or Secure Simple Pairing Security Mode 4 service level security. See Section 4.2 and 4.3 below for additional guidance on each.

4.2 Legacy Pairing Requirements

4.2.1 Bluetooth 2.0 and earlier devices must use Security Mode 3 link level security during legacy Bluetooth pairing.

4.2.2 Bluetooth devices using legacy pairing must not use or accept unit keys and must use combination keys for link key establishment.

4.2.3 Devices must use completely random Bluetooth passkeys at least eight digits in length that are newly generated for each pairing exchange. Ideally devices should use random 128-bit binary passkeys. Passkeys must not be valid indefinitely.

<u>4.3 Secure Simple Pairing (Security Mode 4) Requirements</u>

4.3.1 Ideally Bluetooth 2.1 and later devices should use the Passkey Entry SSP association model. Devices may also use Numeric Comparison association model if each digit of the passkey is confirmed individually. Devices may also use the Out of Band association model but only with a tethered, non-wireless interface. Devices must never use the Just Works association model and therefore must immediately discard all unauthenticated Just Works link keys after pairing to terminate such connections.

4.3.2 Bluetooth devices supporting SSP must use Elliptic Curve Diffie-Hellman (ECDH) public/private key pairs that are unique for each device and must originate from a trusted source.

4.3.3 Bluetooth devices must store SSP ECDH public/private key pairs securely.

4.3.4 Host protocol stacks in devices using Security Mode 4 must be sufficiently robust to prevent denial of service and other attacks based on anomalous frames.

5 Encryption Requirements

5.1 All Bluetooth links must use 128 bit Bluetooth encryption.

5.2 Devices must initiate Bluetooth encryption immediately after the successful completion of mutual authentication.

6 Additional FIPS-Certified Cryptography

6.1 Where practically feasible, all Bluetooth devices must use FIPS 140-2-certified key establishment and encryption layered atop the Bluetooth cryptography specified above for defense in depth.

6.2 Bluetooth smart card readers intended for DoD use must use FIPS 140-2 certified cryptography.

6.3 Public/private key pairs used in FIPS-certified cryptography must be unique to each device and must originate from a trusted source.

6.4 Bluetooth devices must store public/private key pairs and all keys used in FIPS-certified cryptography securely based on applicable NIST guidance.