www.fte.com
frontline
+1 (434) 984-4500 | Fax: +1 (434) 984-4505
PO Box 7507 | Charlottesville, VA 22906-7507
337 W. Rio Rd. | Charlottesville, VA 22901 USA

# *Bluetooth*® Secure Simple Pairing, Simple Pairing Debug Mode, and Interoperability Testing

## Introduction

Secure Simple Pairing (SSP), a feature of the *Bluetooth*® Core Version 2.1 specification, was created to address two major concerns among the *Bluetooth* user community: *security* and *simplicity of the pairing process*. Prior to SSP, there was some apprehension that a knowledgeable hacker, using commercially available equipment, could intercept communication between *Bluetooth* devices. Though the chances of this happening were slight, the fact that it was possible at all caused some concern in the *Bluetooth* community. In addition to the security unease, some users found the process for pairing devices at times challenging. The *Bluetooth* Special Interest Group (SIG) reacted to these concerns by creating Secure Simple Pairing.

With SSP, pairing two *Bluetooth* devices can be as simple as turning them on and setting them next to each other. The idea of SSP is to "maximize security while minimizing complexity from the end user's point of view." This quote is taken from the **Core Specification v2.1 + EDR**, which can be found at: http://www.bluetooth.com/NR/rdonlyres/F8E8276A-3898-4EC6-B7DA-E5535258B056/6545/Core_V21__EDR.zip

During the development of SSP, the *Bluetooth* SIG determined that to be able to debug devices and do interoperability testing, engineers would have to have access to a **debug mode.** By using a debug mode, engineers could analyze and debug data without exposing any information that was intended to be kept secret. This determination brought us **Simple Pairing Debug Mode**.

## Simple Pairing Debug Mode

Simple Pairing Debug Mode uses a different Link Key for encryption than is used during normal operation. As a component of the Host Controller for any 2.1 compliant *Bluetooth* device, Simple Pairing Debug Mode can be turned on so engineers can analyze *Bluetooth* data. Once the analysis is complete, Debug Mode can be switched off so that further communication between the devices cannot be compromised. The main point here to remember is that a different Link Key is used when in Simple Pairing Debug Mode, thereby maintaining the enhanced 2.1 security process.

As an additional security feature, the Link Key generated during debug mode is clearly identified as having been created during the debug process. This allows the *Bluetooth* Host to recognize that the current Link Key is not secure. The Host can choose to initiate the pairing process again, which results in the generation of a new Link Key.

## Implications of Secure Simple Pairing for Device Manufacturers

In the 2.1 specifications, Simple Pairing Debug Mode is required to be a component of any Host Controller. *Bluetooth* chip manufacturers must modify their Host Controllers in order

+1 (434) 984-4500 | Fax: +1 (434) 984-4505
PO Box 7507 | Charlottesville, VA 22906-7507
337 W. Rio Rd. | Charlottesville, VA 22901 USA

for their chips to be certified as 2.1 compliant. While chip manufacturers are obligated to support Simple Pairing Debug Mode, no such obligation currently exists for device manufacturers.

But what happens if a manufacturer chooses not to integrate SSP, if a *Bluetooth* device does not provide a developer with the ability to enable or disable Simple Pairing Debug Mode? The best answer is that there will be no efficient way for device developers to do interoperability testing with that device. With no access to Simple Pairing Debug Mode, engineers will be unable to decrypt data for analysis and diagnostics. A device that has a low interoperability rate leads to poor customer experience. In addition, devices risk not being certified as 2.1 compliant.

## Conclusion

- Secure Simple Pairing (SSP), *Bluetooth* Core Version 2.1, was established to make devices easier to use and more secure.
- Support for Simple Pairing Debug Mode is mandatory in all 2.1 compliant Host Controllers.
- Secure Simple Pairing Debug Mode support is not currently mandated for device manufacturers; however, strong support for Debug Mode by device manufacturers is essential for interoperability testing and device debugging.
- In the field, engineers use sniffing to capture data for analysis on the spot or to take back to a controlled testing environment for analysis.
- Debug Mode allows analysis of any issues that arise after a device is deployed.
- **Debug mode enables interoperability testing, debugging, and analysis at all stages of development, decreasing time to market.**