Bluetooth & NFC Transport for FIDO U2F

July 22, 2015

Executive Summary

Universal 2nd Factor (U2F) is a Fast IDentity Online (FIDO) Alliance protocol that lets online applications and services augment the security of their existing password infrastructure by adding a strong second factor to user login based on public key cryptography. U2F Authenticators, including tokens and biometrics, have traditionally been connected to a computing device via a USB port.

In an increasingly mobile world, however, not every device has a USB port. And given the sorry state of today's passwords, it's become clear that every device at least should have access to FIDO U2F strong authentication to ensure security and privacy.

The U2F protocol was designed to accommodate multiple types of Authenticators, and to communicate over a range of transport protocols.

With that in mind, FIDO has added two new classes of transport protocols to the U2F 1.0 specification that support wireless communication.

The new U2F transport options are Bluetooth® Technology, including Bluetooth Smart (also known as Bluetooth Low Energy) and Bluetooth (also known as Bluetooth Classic), and Near Field Communication (NFC). These new classes are additions to the base FIDO U2F 1.0 specification and do not change the specification in any way. They are implemented as extensions and were developed to support U2F use on devices, including mobile phones, tablets and any other computing device that requires a secure login but do not support USB.

With U2F, the user logs into an application or service with a set of credentials, typically a username and password, then the application or service prompts the user to present a second factor device, also known as an Authenticator. With Bluetooth Technology and NFC extensions, transport of that communication is as varied as the number of Authenticator choices. These changes also highlight the flexibility, extensibility and the future-proof design of the U2F protocol.

What is Bluetooth Technology?

Bluetooth Technology is a global wireless standard enabling secure connectivity among a range of devices and services. It supports the exchange of data using radio transmissions between paired devices. Bluetooth Technology was created by Ericsson in 1994 and today support is built into billions of products, including smartphones and tablets. The technology is now owned by the Bluetooth Special Interest Group (SIG). There are over eight billion Bluetooth enabled devices in use today around the globe and over 10 billion are projected to ship in the next three years, according to the SIG. Research firm IHS Technology projects just over 3.6 billion Bluetooth Device Shipments in 2015 growing to a total of nearly 5 billion in 2019. (*See Chart 1 below*)

U2F Bluetooth Technology

The U2F Bluetooth Technology transport specification allows the creation of special-purpose, Bluetooth Smart U2F devices that require just the press of a button to authenticate to an online service. In addition, phones and peripherals, which consume more power, can be programmed to act as U2F devices using either Bluetooth Smart or Bluetooth.

FIDO's U2F support of Bluetooth Technology protocols is designed to work with multiple form factors. The U2F Bluetooth Technology extensions support either Bluetooth Smart or Bluetooth. The addition of Bluetooth Technology into U2F does not alter in any way the current 1.0 specification and its operations. The Bluetooth Technology extensions for FIDO U2F only define an additional transport.

U2F Bluetooth Smart

For Bluetooth Smart (also called Bluetooth Low Energy), the FIDO Alliance has created a U2F Primary Service that has been adopted by the Bluetooth SIG.. A Primary Service defines the primary functionality of a device. The SIG-approved U2F Primary Service can be used by any device manufacturer implementing Bluetooth Smart, and provides a standard way to implement transport for U2F Client and Authenticator. This standardization is important as it aligns with FIDO's overall standards mission.

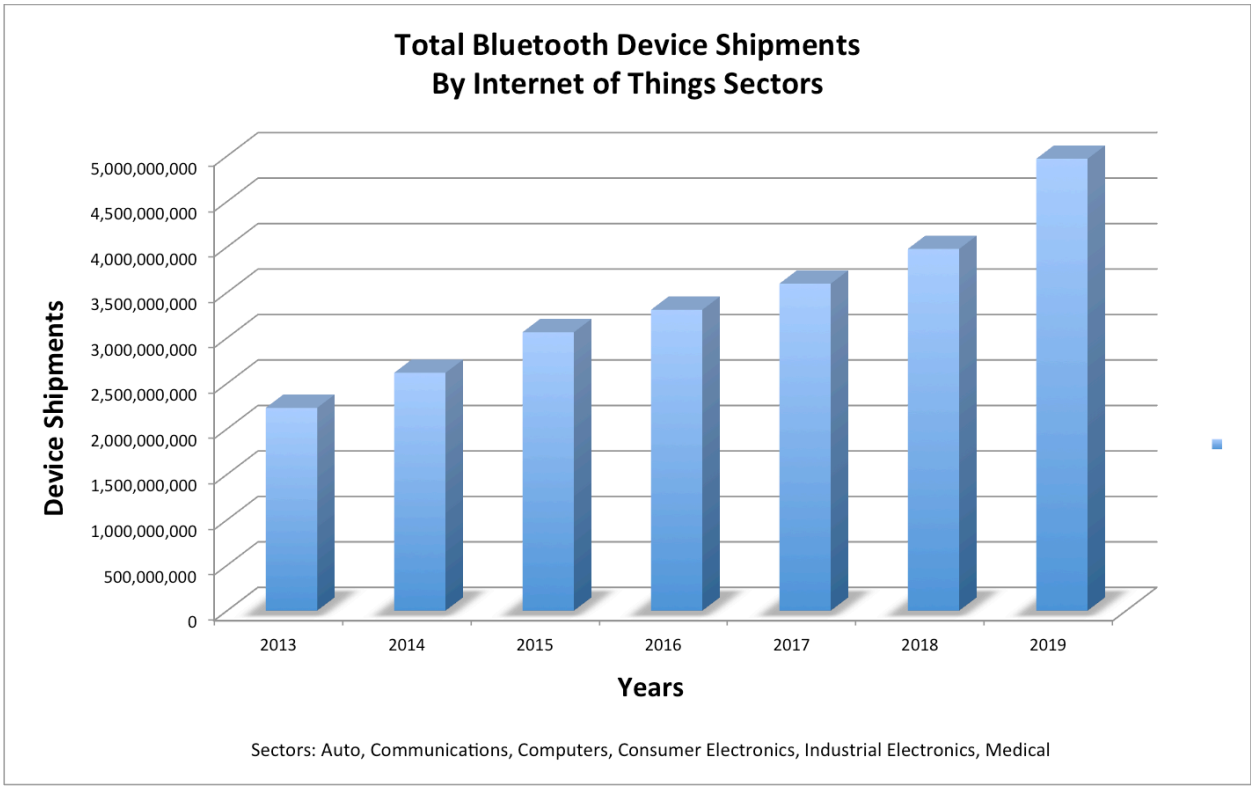
In U2F Bluetooth Smart, the Authenticator advertises its FIDO U2F Primary Service expressed as a Universally Unique Identifier (UUID) and the Client scans for such services. Both the Authenticator and Client devices must conform to Bluetooth Technology Core Specification 4.0 or later. When the Client locates an Authenticator, it performs a characteristic, or attribute type, discovery to find Bluetooth Smart devices with a unique U2F Service UUID, which is stipulated by the U2F Primary Service.

If the two devices have not been previously paired, the user must explicitly put the Authenticator into pairing mode in order to complete a Bluetooth Smart pairing and create a long-term link key. This encryption key prevents monitoring, injection, and other network-level attacks that are known vulnerabilities for wireless communication.

The U2F Bluetooth Smart protocol calls for encryption before any U2F messages are sent between devices.

If the pairing is made, the Client connects to the Authenticator and begins writing a request, such as Enrollment, into the Authenticator's Control Point characteristic. The Authenticator evaluates the request and responds with a notification over the Status characteristic. The connection is then closed by either the Client or the Authenticator or if the connection times out.

If the request was for Authentication, the Authenticator calculates the U2F cryptographic response and transfers results back to the Client, which collects all the packets and sends them back to the U2F Server.



Source: IHS Technology

Chart 1

U2F Bluetooth

A U2F Bluetooth Authenticator acts in a specific way when it encounters a Bluetooth Client. If the two are not yet paired, the Authenticator goes into a Discoverable Mode. This mode allows the authenticator to speak to new Clients.

This "conversation" allows the Client to connect to the Authenticator. If the two have not previously been paired the Client and Authenticator bond, creating a long-term link key and enabling a connection. This encryption key prevents monitoring, injection, and other network-level attacks that are known vulnerabilities for wireless communication.

The two devices must be paired initially in order for the Authenticator to allow subsequent connections without need for user intervention.

After the bond is completed, the Client, if it is not a dual-mode device, performs a service discovery on the Authenticator and then connects to the FIDO U2F service. The Client then makes a request that is evaluated by the Authenticator, which then issues a response. To end the interaction, the Client closes the connection. If the connection times out, the Authenticator closes the connection. While Bluetooth support is a meaningful design point, many devices and PCs manufactured after 2010 have migrated to Bluetooth Smart.

Bluetooth Connection Best Practices

The U2F Bluetooth Technology protocol stipulates that if one or both devices support only Bluetooth that the Authenticator and the Client must communicate over RFCOMM, which emulates the serial cable line settings and status of an RS-232 serial port. If both devices support dual mode, the devices must communicate using Generic Attribute Profile (GATT) over Logical Link and Adaptation (L2CAP), which enables multitasking, segmentation and reassembly, on a Basic Rate/Enhanced Data Rate (BR/EDR) connection. EDR enhancements help reduce power consumption and improve security.

Because they are wireless and can potentially transmit over a sizeable distance, Bluetooth and Bluetooth Smart must use a long-term encryption key. This also improves the end-user experience by ensuring only paired devices can exchange critical data and alleviating privacy concerns. Depending on the class of Bluetooth Technology device, the wireless signal can extend approximately from 3 to 300 feet.

What is NFC?

Near Field Communication (NFC) technology enables simple and secure two-way interactions between electronic devices, allowing contactless transactions, access to digital content, and to connect electronic devices. Because it operates only within a short range, it is often used for high-security operations, such as payment systems and building access. The technology uses electromagnetic induction between two loop antennae within NFC devices to exchange information. Devices must be within close proximity of each other at a distance typically 10 cm or less. NFC is derived from a sub-set of Radio-Frequency Identification (RFID) technology, and was standardized by ISO/IEC and the NFC Forum, a non-profit industry association founded in 2004 by Nokia, Philips Semiconductors (became NXP Semiconductors in 2006) and Sony.

NFC-enabled cellular handset shipments will increase by 70% in 2015 to 756 million, up from 444 million in 2014, according to IHS Technology. In 2020, handset shipments will hit 2.2 billion, IHS forecasts (See Chart 2).

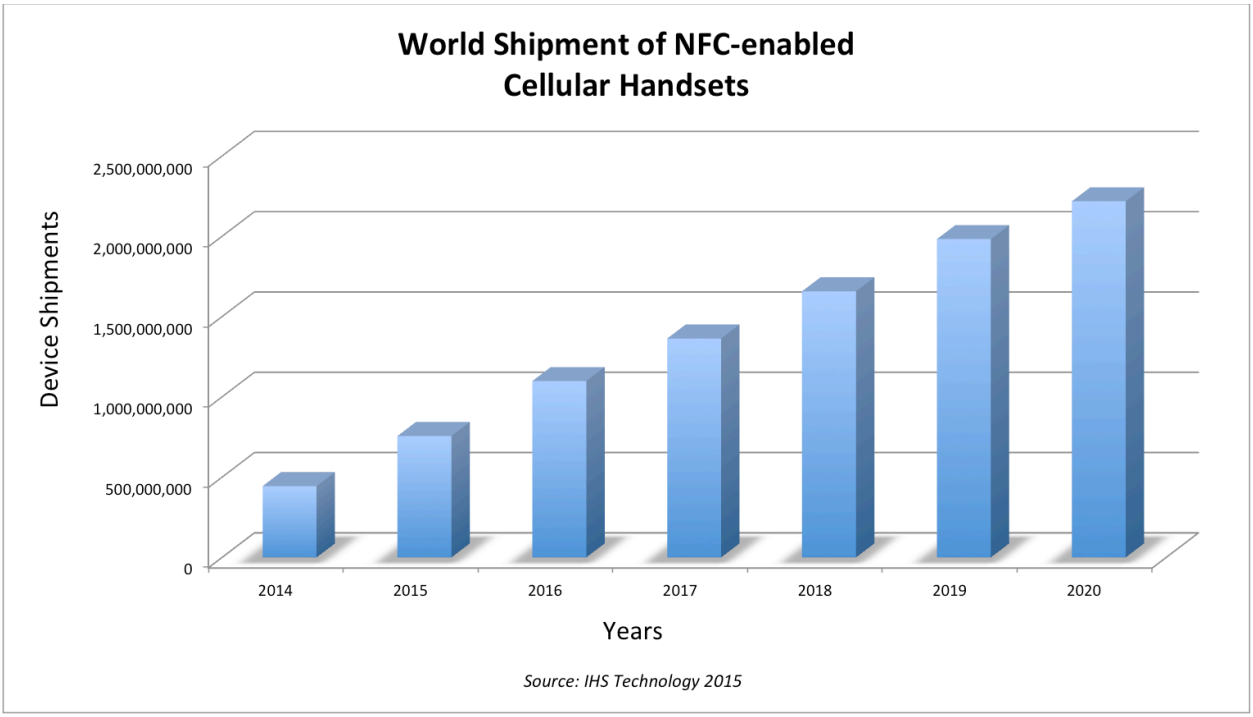


Chart 2

U2F NFC

The U2F NFC transport specification allows the creation of portable U2F devices such as credit cards, keyfobs, watches and other devices that are simply tapped against the target device to authenticate to an online service. These devices can be battery-less and passive. Alternately, a mobile phone with NFC capability can be programmed to act as an NFC U2F device. The user taps the mobile phone onto a target device to authenticate.

FIDO's U2F support of NFC protocols is designed to work with multiple FIDO-enabled Authenticators, which may include smartphones, tablets, laptops or keyboards. The addition of NFC into U2F does not alter in any way the current 1.0 specification and its operations. The NFC extension for FIDO U2F only defines transport. NFC's wireless operation is an industry-standard method to pair Clients and Authenticators.

The U2F public key cryptography is initiated when a U2F NFC Client is in proximity of a U2F NFC Authenticator. The Client sends an applet selection command to an Authenticator that returns a reply confirming receipt. The FIDO applet can be part of a multi-function device and does not have to be a dedicated FIDO Authenticator. Next, the Client sends a command for an operation, such as "authenticate," and the Authenticator replies by sending a signed assertion (and completing a U2F authentication) or an error message and then returns to a passive state.

Today's U2F NFC Clients can be embedded in devices such as smartphones so there is nothing that an end-user needs to add to the device. The Authenticator does not require a

battery, unlike a Bluetooth Authenticator. The NFC Authenticator must follow the U2F raw message format.

Conclusion

Bluetooth and Near Field Communication support provide additional transport modes for the FIDO U2F protocol. The new extensions do not change the U2F 1.0 protocol they only stipulate a number of steps and parameters for the way U2F Authenticators connect to new types of U2F Clients, and the way in which the two U2F components communicate with one another. Most important, is that Bluetooth and NFC provide a way for devices that do not have a USB port, namely mobile and wireless devices, to leverage FIDO U2F strong authentication that protects logins using a second-factor based on public key cryptography. Lastly, these transport extensions highlight the flexibility, extensibility and the future-proof design of the U2F protocol.