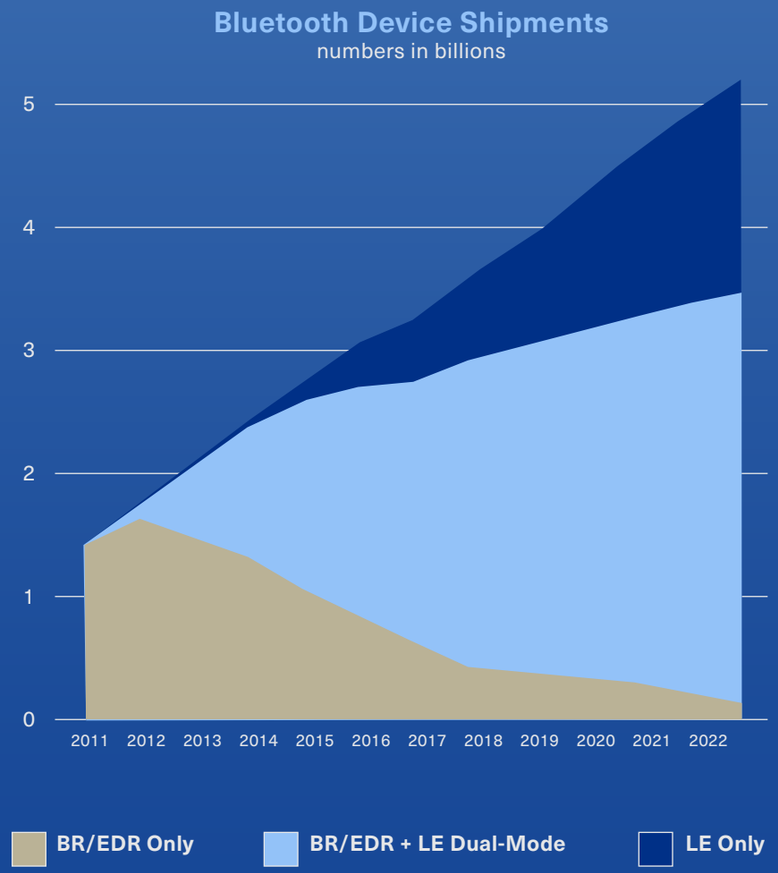
Why Bluetooth Low Energy (BLE) Is Secure to Use for Mobile ID Verification

EBOOK



Introduction

When creating mobile identity applications, there are several technologies available which can be used for securely handling the data transmission process between the holder's device and the verifying device. Despite industry confidence in the use of Bluetooth for this process, doubts remain in some quarters about the security of the implementation of the technology. This paper examines the threats and the mitigating actions that can be taken to reduce any risks presented by enabling Bluetooth technology and render it safe for use in verification of mobile identities.

What Is Bluetooth?

Bluetooth is a wireless technology specified by the Bluetooth Special Interest Group, a global community of more than 36,000 companies working to standardize and drive innovation in connected devices. Bluetooth has evolved over the years through different types of technology, Bluetooth Basic Rate (BR), Bluetooth Enhanced Data Rate (EDR), Bluetooth High Speed (HS) and Bluetooth Low Energy (BLE). Bluetooth Low Energy (BLE) is gaining in popularity because it consumes less energy compared to other Bluetooth versions, making it more suitable for devices that are battery powered such as mobile phones.

Boasting an impressive four billion devices on the market in 2020 (most supporting BLE), Bluetooth has easily become one of the most successful wireless technologies. Thankfully, Bluetooth popularity also means that security has been, and still is, under strict scrutiny. It is safe to say that no threat remains in the Bluetooth protocols and remaining security risks are typically implementation related. While implementation fixes are released before security becomes a problem, deployment typically involves new software, middleware, or firmware to be installed, which means that legacy systems could still be vulnerable today!

Typical Bluetooth Implementations

Before looking at the specific threats, its important to look at how Bluetooth can be implemented, particularly in respect to BLE. Figure 2 broadly depicts these implementations.

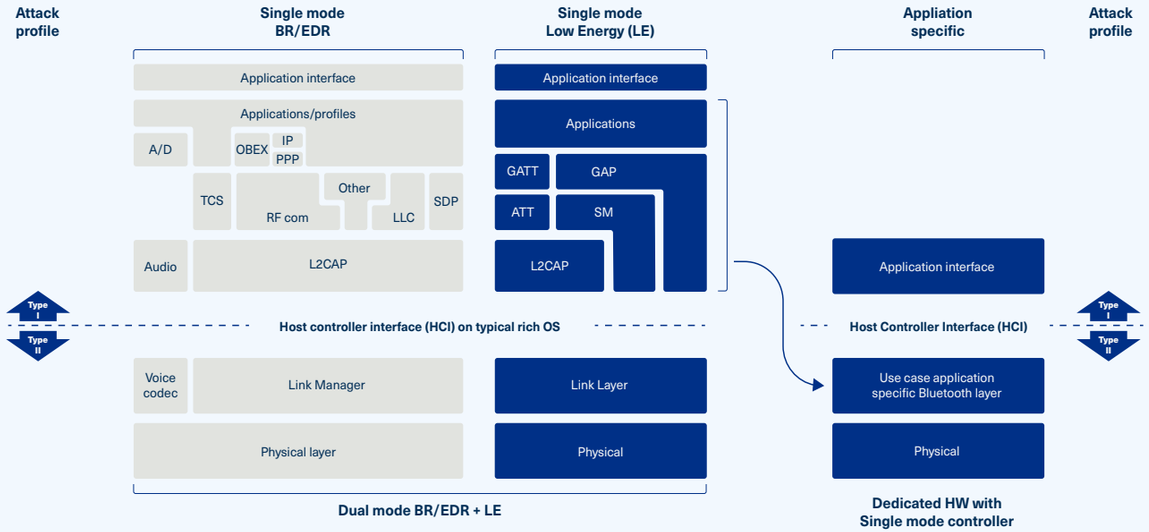
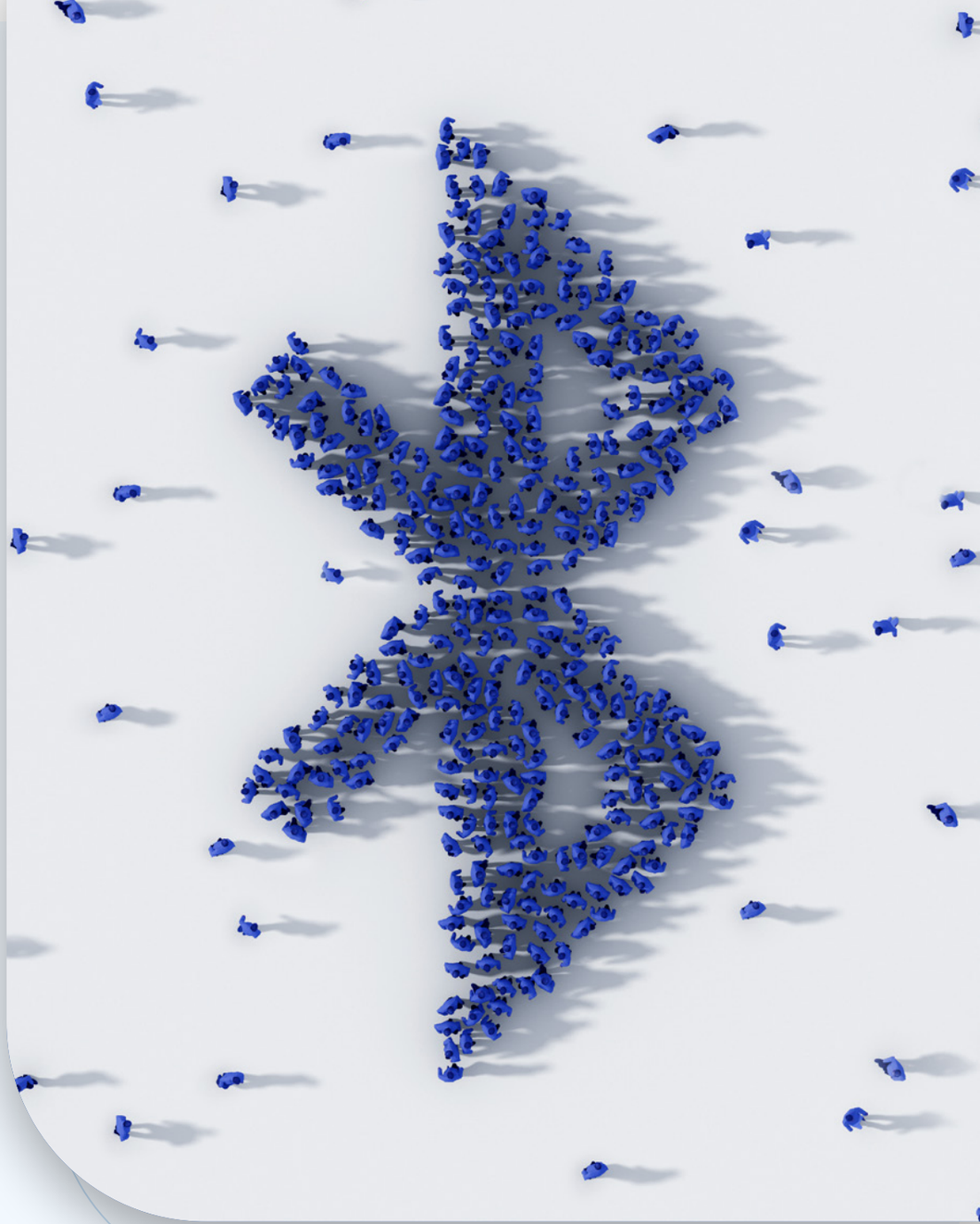


Figure 2: Bluetooth Implementations

There are four kinds of Bluetooth implementations:

- Implementations that feature a **single mode Bluetooth BR/EDR** controller
- Implementations that feature a **single mode Bluetooth LE** controller
- Implementations that feature a **dual mode** Bluetooth controller (BR/EDR +LE)
- **Application specific** implementation with a dedicated HW featuring a single mode controller

Three kinds of implementation may apply to the verification of mobile driving licenses (mDL) and mobile electronic identity documents (m-eID).



Most systems running a rich OS (Windows, Linux, MacOS, Android, iOS, etc.) feature an implementation with a dual mode Bluetooth BR/EDR+LE controller and an extensive Bluetooth software stack running on the rich OS as represented in figure 2.

Single-mode, low-energy implementations are typically found in dedicated devices implementing off-the-shelf generic controllers. This is typical for headphones, medical devices, activity trackers, etc.

An example of application specific implementation is the HID Global Omnikey reader which features a Bluetooth implementation specific to Seos®, a very popular solution for physical access control.

Why Is Bluetooth Important in Mobile ID?

Bluetooth, or more accurately BLE, is critical to mobile ID because it maximizes the reach of and contributes to a consistent enhanced user experience. The other transport technologies specified in the mobile e-ID and mobile driving license (mDL) ISO standards result in inconsistent usage as they are only supported by a limited number of devices and/or inconvenient user experiences (e.g., NFC which requires the users to be in very close proximity to the verifier during the entire duration of the data transfer). BLE allows data transfer at a distance which has many benefits: it is safer for law enforcement officers approaching a potential suspect and it quickens the passage of individuals through gates, doors or checkouts by engaging as the person approaches rather than waiting until the person is within a few centimeters of the verification device.

How Is Bluetooth Covered in the Standards for Mobile e-ID's?

BLE is mandated for the verification of ISO mobile driving license (ISO18013-5) and ISO mobile electronic identity document, m-eID(ISO23220-1). Verification of a standard mobile driving license and upcoming mobile e-ID relies on a first-device engagement phase, where the information to establish a secure communication channel between the holder's phone and the verifying device is exchanged, followed by a data retrieval phase composed of a request from the verifier and finally, a response with returned data following user consent as follows:

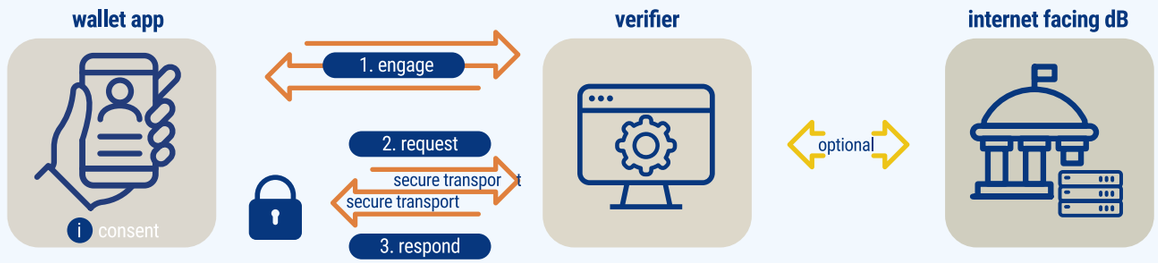


Figure 1: mDL & m-eID verification process

STEP 1

Engage. The wallet app and verification device shares keys. This starts through a channel other than BLE and can even be started at the time that the m-eID is issued to the holder. In other cases, such as m-DL this happens by scanning a QR code. Because this step is done through a channel other than for data retrieval it is often referred to as "Out of Band" (OOB).

STEP 2

Request. The verifying device requests information from the holder's device and optionally shares a key when engagement information is presented from the wallet app. Using keys from both the wallet app and the verifier's device allows an encryption key to be used for both the request and response on top of the security of the selected transport (e.g., BLE).

STEP 3

Response. The holder's device returns the consented information encrypted with the derived key and through an encrypted channel, to the verifier.

The mDL & m-eID standards specifically address threats to BLE.

The process depicted in Figure 1 ensures data encryption on top of the BLE transport by the following steps:

- During engagement phase, an ephemeral public key is shared along with BLE configuration information
- As part of the data retrieval phase, an ephemeral public key from the other party is shared and both the wallet app and the verifier compute the derived key used to encrypt the request and response

This results in prevention and detection of attacks such as:

- **Eavesdropping** – because the identity data is encrypted on top of BLE transport
- **Man-in-the-Middle** – because of the encryption and out of band sharing of the encryption key
- **Data injection or fake data** – because of the encryption and out of band sharing of the encryption key

Detection means that the wallet App and/or verifier application terminates the communication when decryption fails, thus preventing the above attacks.

The mobile ID standards do not address implementation threats. While transactions are short in time and the verifier can keep Bluetooth off when not involved in a verification, a sophisticated Bluetooth attack with a lot of automation may still be able to take advantage of implementation flows to succeed. While for the holder, the mDL or m-eID app verification process presents no more risk than enabling Bluetooth to pair the mobile phone to another device such as headphones or a car entertainment system, it may be an issue for the verification side in particular when on a computer connected to a network with access to sensitive data.

Known Bluetooth Threats

Software attacks are generally, either financially driven or related to disrupting a service (e.g., denial of service attacks). Nowadays, most attacks are financially driven, and the real money is to be found by stealing data. This is accomplished by taking advantage of faulty implementations of Bluetooth protocols to run malicious code on the host which intercepts sensitive communications. There remain a number of known attacks which are not mitigated by the measures in the standards.

Popular attacks are related to Bluetooth BR/EDR/HS. Bluetooth BLE is also subject to many attacks on faulty implementations. These attacks are also applicable to dual mode systems where both technologies are implemented alongside each other. In these implementations, one Bluetooth technology cannot be enabled without the other, and therefore they are subject to both families of threat.

Common Attacks

Attacks on Bluetooth BR/EDR/HS

Attack Name	Year	Information	Profile
Bleedingbit	2018	TI chip (WiFi routers)	Type I
Bluebornе	2017	Android, windows, Linux, iOS	Type I
Bluebugging	2006	OBEX protocol	Type I
Bluejacking	2001	OBEX protocol	Type I
Bluesnarfing	2003	OBEX protocol	Type I
Bluesmacking	2006	RF	**Type II**
Cabir	2004	Symbian	Type I
EternalBlue	2017	Windows SMB	Type I

Attacks on Bluetooth BR/EDR/HS

Attack Name	Year	Information	Profile
CVE-2019-2102	2019	Android Fido key and Feitian key	paring/LTK - Type I
CVE-2019-5014	2019	Winco firework	
CVE-2019-13953	2019	Camera	
SweynTooth	2019	Medical device	

The most common Bluetooth BR/EDR/HS attacks exploit the Bluetooth stack to execute a malicious application on the host device. It is not surprising to see that the type I profile (as illustrated on Fig 2) is prevalent because most are money driven attacks.

Many of the current exploits on BLE are related to the long-term key (LTK). In many cases it relates to such keys being embedded, extracted, or discovered thus allowing any kind of attack, even when the BLE transport layer uses cryptography.

While all these threats have countermeasures, it is worth noting that many are still amongst the most common attacks in 2020 , even old ones: bluebugging, bluejacking, bluesnarfing, blueborne, etc.

Attacks From Exploiting Poor Implementation Choices

Bluetooth defines four security modes (1 to 4) and five security levels (0 to 4). Poor implementation choices (e.g., fallback to unsecure level instead of disconnecting) may result in insecure pairing and unencrypted communication.

Buggy implementations of BLE		Poor implementations of Bluetooth		
Attack Name		**Attack Name**	**Information**	**Profile**
CVE-2017-8403, CVE-2018-10825,	CVE-2018-20957, CVE-2018-20958, Etc.	Car whisperer	BR	Predictable PIN
		- LTK exploits -	BLE < v4.2	

When it is not a buggy implementation the threats are mostly related to compromised pairing either through predictable PIN code or long-term key exploit.

[1] https://www.signils.com/types-of-bluetooth-attacks-in-2020/

Minimizing the Threats to Bluetooth

The mDL and m-eID standards go a long way to addressing privacy and data authenticity threats, yet other measures can be taken to reduce the threat from the known attacks described above due to faulty implementations.

Reducing Bluetooth Threats for the Verifier

Most of the known attacks discussed target the Bluetooth stack in order to inject malicious code on the host. There are differing levels of mitigation which are applicable to minimize this risk:

Basic	Good	Better	Great
Bluetooth profiles allow filtering of devices that may connect. While not applicable to m-eID or mDL, it could be used to prevent unexpected connections over the Bluetooth BR/EDR/HS channels	Favor implementations that enable BLE without BR/EDR/HS. Solutions where both are turned on at once should be prohibited as it doubles the threat possibilities. Therefore, favor solutions with single mode Bluetooth controller(s) instead of the default Rich OS configuration of the Bluetooth stack.	Use single mode Bluetooth, where the Bluetooth stack can run with limited rights. For example, the verifier application and the Bluetooth stack both run with limited rights. This is a better practice than using the default configuration of the Bluetooth stack delivered by the rich OS.	Use m-eID/mDL specific implementations of the Bluetooth stack running on dedicated hardware and featuring single mode Bluetooth. This leaves little risk of compromising the host. Furthermore, the host application and driver may additionally run with limited rights when possible.

Contribution From the mDL/m-eID Issuers

Mobile credential issuers can play a role in reducing risk by selecting mDL apps that only run as BLE peripheral. Having the verifier running in central mode reduces the threats because the verifier scans for the presence of devices running in peripheral instead of exposing its own information.

Planning for Recovery

It is also wise to implement good practice around security policies, to ensure systems can be recovered or protected in case of compromise or a new threat.

Good	Better	Great	Exceptional
Security policies shall enable updates and bug fixes. Ideally a specific account shall be used to control who can update and for tracking and audit purposes.	In addition to good: the selected solution shall not have embedded keys or predictable key generation mechanism.	In addition to better: the selected solution shall not have embedded keys or predictable key generation mechanism.	In addition to great, the hardware (HW) device also serves as root of trust for signer certificates. Furthermore, rely on different HW to ensure a multiplicity of BLE implementations, so that a hack only compromises a subset of all devices.

It is worth noting that having removable hardware presents a threat related to opening a connection port on the host device. This threat can be easily addressed by turning off plug-and-play and enforcing that ports are only open for specific hardware (HW).

Conclusion

The mDL and m-eID standards will mandate BLE interactions for verification of the mobile credentials. While the standards go a long way to mitigating the risks presented by using Bluetooth, threats still remain, mainly due to outdated devices and faulty implementations. However, by implementing best practices in solution design, security policy and app delivery, these risks can be minimized allowing for the use of BLE with confidence.

Acronyms Definitions

BLE: Bluetooth Low Energy
Bluetooth SIG: Bluetooth special interest group managing the Bluetooth specification
Bluetooth BR: Bluetooth Basic Rate
Bluetooth EDR: Bluetooth Enhanced data rate increases throughput up to 2.1Mpbs
Bluetooth HS: Bluetooth high speed
GATT: Bluetooth Generic attribute profile built on top of attribute protocol (ATT)
HW: Hardware
ISO: International Standard Organization
QR Code: Quick Response code
mDL: Mobile driving license
m-eID: Mobile identity
NFC: Near Field Communication
OOB: Out of Band
Rich OS: Windows, MacOS, Linux, Android, iOS, etc
SDK: Software development kit
SoC: System on chip
UUID: Bluetooth Universal Unique identifier
Wallet App: The mobile application that contains the mDL and/or m-eID

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-03-04-cid-ble-secure-mobile-id-eb-en
PLT-05765

Part of ASSA ABLOY