Why Bluetooth® Low Energy (LE) is Secure for Mobile ID Verification

INTRODUCTION

When creating mobile identity applications, there are a number of technologies available that 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 technology. This white paper examines the threats and the mitigating actions that can be taken to reduce any risks presented by Bluetooth technology and render it safe for use in the 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 (LE). The latest market trend is Bluetooth Low Energy which is very popular 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 Bluetooth LE), 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!

WHY IS BLUETOOTH IMPORTANT IN MOBILE ID?

Bluetooth, or more accurately Bluetooth LE, is critical to mobile ID because it maximizes the reach and contributes to a consistent, enhanced user experience. The other transport technologies specified in the ISO standards result in inconsistent usage as they are only supported by a limited number of devices and/or inconvenient user experiences. (.g., Near Field Communication (NFC) which requires the users to be in very close proximity to the verifier during the entire duration of the data transfer and is not supported on all devices.) Bluetooth LE 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 IDS?

Bluetooth LE is mandated for the verification of ISO mobile driving license (mDL) (ISO18013-5) and ISO mobile electronic identity document (m-eID) (ISO23220-1). Verification of a standard mobile driving license and upcoming mobile eID relies first on a device engagement phase, where the information to establish a direct 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 data returned following user consent as follows:

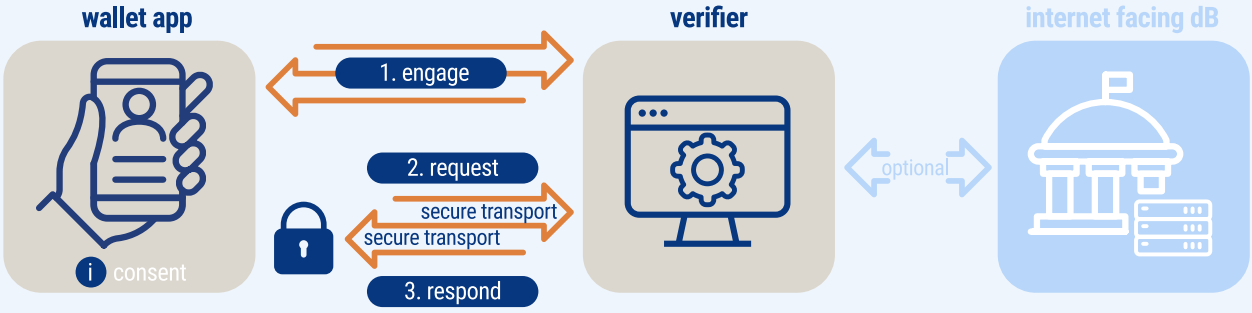

Figure 1: mDL & m-eID verification process

Step 1 – Engage. The holder establishes a connection with the verification device and shares a key. This is done through a channel other than Bluetooth LE and can even be done at the time that the m-eID is issued to the holder. In other cases, such as mDL, this happens by scanning a QR code. Because the process is done through a channel other than Bluetooth LE 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 device allows the verifier to derive an encryption key used for both the request and response on top of the security of the selected transport (e.g., Bluetooth LE).

Step 3 – Response. The holder's device returns the consented information, through an encrypted channel, to the verifier.

THE MDL & M-EID STANDARDS SPECIFICALLY ADDRESS THREATS TO BLUETOOTH LE.

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

- During engagement phase, an ephemeral public key is shared along with Bluetooth LE configuration information
- As part of the data retrieval phase, an ephemeral public key from the other party is shared and both Wallet app and 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 the Bluetooth LE 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 mobile app and verifier applications terminate the communication when decryption fails, thus securing the data.

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 a mobile phone to another device such as headphones or a car entertainment system, it may be an issue for the verification side.

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.

The most common Bluetooth attacks of concern attack Bluetooth BR/EDR/HS or dual-mode systems where Bluetooth LE is implemented alongside one of the other technologies. In these implementations, one Bluetooth technology cannot be enabled without the other, and therefore they are subject to both types of threats. However, implementation threats do exist for systems where only Bluetooth LE is deployed.

A more in-depth look at the known threats to these legacy systems can be found in our technical white paper on this subject.

MINIMIZING THE THREATS TO BLUETOOTH

The 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 mobile eID or mDL, it could be used to prevent unexpected connections over the Bluetooth BR/EDR/HS channels.	Favor implementations that enable Bluetooth LE without BR/EDR/HS. Solutions where both are turned on at once should be prohibited as it doubles the threat possibilities. Therefore, use 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 mDL/m-eID application-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 Bluetooth LE 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 good: 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 Bluetooth LE implementations, so that a hack only compromises a subset of all devices.

Conclusion

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

Find out more about implementing mobile identity with **HID goID**.

HID
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

2022-12-05-cid-ble-secure-mobile-id-wp-en PLT-05767
Part of ASSA ABLOY