Introduction

Gemalto’s Bluetooth Smart solutions combine the unparalleled security of PKI with the anywhere, anytime convenience of mobile, using a single credential. This allows organizations of all types to realize the benefits of allowing mobile connectivity, while ensuring integrity and trust in their PKI environments.

Gemalto’s Bluetooth Smart enabled solutions extend the use of PKI credentials to mobile devices such as iOS, Android and legacy Windows & Mac devices.

The purpose of this document is to review the various security mechanisms that are designed to ensure security for solutions based on Gemalto’s Bluetooth Smart products.
Technical Specifications

The following sections cover the technical specifications for Gemalto’s Bluetooth Smart solution components.

**SafeNet Reader CT1100**

The CT1100 badge reader is a lightweight device, with one click-simple and secure encrypted pairing. The reader has automatic detection within proximity of the designated mobile device, laptop or desktop and no physical connection is needed. SafeNet Reader CT1100 has more than three months standby battery life, more than 20 working days in standard use case and charges through a USB port.

**SafeNet Reader K1100**

SafeNet Reader K1100 is a lightweight, smart card-enabled Bluetooth reader. It has one-click simple and secure encrypted pairing and carries a replaceable smart card in SIM form factor. SafeNet Reader K1100 has more than three months standby battery life, more than 15 working days in standard use case and charges through a USB port.

**Ezio Bluetooth Reader**

The Ezio Bluetooth Reader is a personal smart card reader that can operate in both unconnected (standalone) and connected (through USB or Bluetooth) mode.

The major functionalities in connected mode comply with:

- MasterCard SecureChannal 2010
- Gemalto proprietary “See What You Sign” functionality
- PSCS 2.0 Part10: Secure PIN Entry

The device can be equipped with a Secure Element that can be used to store a secret device key for generating a “Terminal Signature” which provides evidence that a certain transaction has been performed with this unique device.

Please refer to the table below for additional technical specifications for CT1100, K1100 and Ezio Bluetooth Reader.
### Technical Specifications

<table>
<thead>
<tr>
<th></th>
<th>CT1100</th>
<th>KI1100</th>
<th>Ezio Bluetooth Reader</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host interface</strong></td>
<td>Bluetooth Low Energy 4.0/4.1 and USB2.0</td>
<td>Bluetooth Low Energy 4.0/4.1 and USB2.0</td>
<td>Bluetooth Low Energy 4.0 and USB2.0</td>
</tr>
<tr>
<td><strong>Operating Systems</strong></td>
<td>Android, iOS, Windows 7, 8 and 10, Mac OS</td>
<td>Android, iOS, Windows 7, 8 and 10, Mac OS</td>
<td>Android, iOS, Windows Phone, Windows Vista, 7, 8 and 10, Mac OS</td>
</tr>
<tr>
<td><strong>Smart card electrical interface</strong></td>
<td>Class B, short circuit protection, card insertion/extraction detection</td>
<td>Class B, short circuit protection, card insertion/extraction detection</td>
<td>Smartcard sensor to detect card insertion/removal</td>
</tr>
<tr>
<td><strong>Human interface</strong></td>
<td>2 LEDs (battery and Bluetooth activity), 1 button to manage the different modes</td>
<td>2 LEDs (battery and Bluetooth activity), 1 button to manage the different modes</td>
<td>4 row 17 positions Liquid Crystal Display 102x48 pixel (WxH) display Character table ISO/IEC 8859-15 and ISO/IEC 8859-5 Status row indicates the battery level, the Bluetooth and USB status.</td>
</tr>
<tr>
<td><strong>Operating temperature</strong></td>
<td>0°C/+50°C</td>
<td>0°C/+50°C</td>
<td>0°C/+50°C</td>
</tr>
<tr>
<td><strong>Environmental and security certifications</strong></td>
<td>RoHS, REACH, WEEE marking, CE, UL, FCC</td>
<td>RoHS, REACH, WEEE marking, CE, UL, FCC</td>
<td>WEEE, CE, UL, RoHS</td>
</tr>
<tr>
<td><strong>Supported smart cards</strong></td>
<td>ID1, ISO7816-1/2/3/4, T=0 and T=1 protocols, PPS, up to 500Kbs</td>
<td>ID0, ISO7816-1/2/3/4, T=0 and T=1 protocols, PPS, up to 500Kbs</td>
<td>T=0 and T=1 protocols, EMV-Compliant, ISO 7816-Compliant</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>101mm x 63mm x 9mm</td>
<td>69mm x 22mm x 8mm</td>
<td>107 mm x 66 mm x 14 mm</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>45grs</td>
<td>15grs</td>
<td>77grs</td>
</tr>
</tbody>
</table>

Table 1: Technical Specification
IDGo800 Mobile

IDGo800 Mobile includes a PKI API, an OTP API, a PC-SC API and a range of drivers to interface with a large range of secure elements, such as Bluetooth Smart devices (badge holder, token and Ezio Reader), MicroSD and SIM. The IDGo800 Mobile library support iOS and Android.

Please refer to the IDGo800 Mobile product page for all product related and security related information here.

Gemalto’s Bluetooth Device Manager

The Gemalto Bluetooth Device Manager (GBDM) application for Windows 7, 8.1 and 10, as well as Mac, use the native PC/SC layer to communicate transparently with the SafeNet Reader CT1100, SafeNet Reader K1100 and Ezio Bluetooth Reader.

Any application using the Microsoft Windows native PC/SC layer can communicate with a smart card via the Gemalto Bluetooth reader as easily as a USB reader.
Gemalto’s Bluetooth Smart Authentication Process Security Features

The standard Bluetooth Smart protocol is known for having several security vulnerabilities. In order to overcome these limitations and in order to increase the security assurance level of devices and applications that are using Gemalto’s solutions, Gemalto has implemented its own security protocol as an additional layer on top of the Bluetooth Smart standard. This proprietary security protocol is called BCCID.

The figure below depicts the architecture of a Gemalto Bluetooth Smart solution.

![Bluetooth Smart Solution Architecture](image)

**Figure 1 Bluetooth Smart Solution Architecture**
Gemalto’s BCCID

Gemalto’s BCCID provides a similar interface towards PC/SC as CCID provides for USB. This enables customers to use existing smart card middleware solutions.

Due to limited packet size and data rate of Bluetooth Smart, the BCCID protocol is optimized to transfer as much data as possible in each payload (20 ~ 300 bytes) and each CCID frame has a redundancy check (CRC8) in order to increase integrity and reliability.

Gemalto’s BCCID service mitigates the security issues that are present in Bluetooth Smart 4.0 and Bluetooth Smart 4.1 since it requires a separate pairing process that uses a “Password-Based Key Exchange” method.

BCCID’s Password-Based Key Exchange

The “Password-Based Key Exchange” method is based on PACE V2, which is a password based key exchange protocol that uses Elliptic Curve Diffie Hellman (ECDH). The passkey is used to create a new shared base point on the elliptic curve used for ECDH key exchange. ECDH provides a 192 bit shared secret that is used as a Long Term Key (LTK) between the devices for future connections.

On each connection occurrence a new subset of keys is generated based on the LTK. The subset of keys is then used to encrypt and perform an integrity check on each command transported via the BCCID protocol. Each command also includes a 32 bit counter to track the assigned commands. By doing so, it protects against replay attacks.

Please Note:

- For every new connection a new key set is derived from the LTK. This key set is only used during its active session.
- In order to insure confidentiality and integrity all of BCCID’s data exchange is encrypted with AES-128 and hashed with SHA256.

BCCID’s Bonding Whitelist

In order to support instant reconnection with previously paired clients, BCCID includes a bonding whitelist.

The list stores up to 10 connected device IDs. If the list reaches its maximum number of devices and a new device pairing takes place then the list gets updated. The update process involves removing the ID of the least used device (i.e. the device that has not been active the longest) and then adding the device ID of the most recent connection.

Please Note:

- For iOS and Android devices, BCCID provides application level bonding and not system level bonding. This prevents unauthorized applications on the mobile device from accessing the information that is exchanged via the Bluetooth Smart protocol.
Security Mechanisms per Device

**SafeNet Reader CT1100, SafeNet Reader K1100, Ezio Bluetooth Reader**

SafeNet Reader CT1100, SafeNet Reader K1100 and Ezio Bluetooth Reader use Bluetooth Smart 4.1. Gemalto’s BCCID service mitigates the security issues that are present in both Bluetooth Smart 4.0 and 4.1.

The Bluetooth Smart profile in Gemalto devices contains these services:

- BCCID service
- Battery service
- Device information service

The battery service and device information service are implemented according to the Bluetooth Smart standard. Additional information can be found [here](#).

Each Gemalto device holds a 128 bit storage key that is used to encrypt the local white list in the device. The key seed is produced during device manufacturing and it is unique per device. The key itself is stored in ROM.

**Ezio Bluetooth Reader Notes:**

- The Ezio Bluetooth Reader requires that the smart card PIN is entered directly on the device’s PIN pad. This means that the PIN is not sent over the Bluetooth communication channel.

- Another code, a 6 digit code “PASSKEY” that needs to be entered during the pairing sequence will only be used to define a common start position, between the Ezio Bluetooth Reader and the HOST device, of the ECDH key generation. This means that it will not have any impact on the security of the key generation itself. Using this PASSKEY will prevent unwanted HOST devices to connect with the Ezio Bluetooth Reader.

- The Ezio Bluetooth Reader provides additional security functionalities:
  - Protection against Denial of Service attacks (DoS)
  - Secure PIN Entry

These two functionalities are detailed in the [Ezio Bluetooth Reader Product Specification](#).
Summary

In order to mitigate Bluetooth Smart security limitations, Gemalto adds an additional security layer on top of the existing Bluetooth Smart infrastructure in the form of a proprietary protocol called BCCID.

BCCID provides a secure way to pair the Bluetooth Smart devices, a way to protect the key exchange and a way to protect the data exchange that is taking place during the operation of a Bluetooth Smart solution.

The security measures that enable security for Gemalto’s Bluetooth Smart solutions include:

**Pairing Protection:**
- Gemalto secure mode ECDH pairing (BCCID)
- ECC Diffie-Hellman with 192 bits keys
- Bonding white list

**Key Exchange Protection**
- For every new connection a new key set is derived from the LTK

**Data Protection**
- All data exchange is encrypted with AES-128 and hashed with SHA256

About Gemalto Identity Protection and eBanking Solutions

Gemalto’s Identity Protection and eBanking solutions enable enterprises, financial organizations and service providers to protect the daily digital interactions of employees, partners and customers by ensuring secure access to online resources and securing financial transactions. Gemalto’s flexible management platforms and broad range of strong authentication technologies and form factors, allow organizations to adopt a forward-looking identity management strategy, ensuring that their security needs are met as new threats and use cases evolve.

To learn more about Gemalto’s complete portfolio of authentication solutions, visit our website at:

http://www.gemalto.com/