MobilePKI Office

On-the-go connectivity with Bluetooth Smart devices

Mobile devices are changing the way we work. Employees are increasingly demanding to use mobile devices, such as laptops, smartphones and tablets for business activities. Studies show employees use three or more different devices for work on a daily basis and 89% of mobile users access business applications with their personal devices. The bring your own device (BYOD) trend is pervasive and not going to slow down. Gartner predicts by 2017, half of employers will require employees to supply their own device for work purposes.

The rapid increase in mobile usage has many IT teams scrambling to get enterprise mobile security in line with current corporate standards. Many of these enterprises already use corporate badges, with certificate-based PKI, the question is how to extend this security to mobile devices, most of which lack embedded card readers or USB ports.

MobilePKI Office: PKI Security on Mobile Devices

MobilePKI Office uses Bluetooth Smart technology to enable connectivity for roaming users, integrating with desktop and mobile devices for anytime, anywhere PKI security on PCs, tablets and smartphones.

MobilePKI Office enables secure mobility by integrating seamlessly with existing ecosystems and extending typical PKI-based corporate badge solutions and PKI security to mobile devices. For enterprises that have already deployed PKI, the same credentials can be used to validate the identity of users on all Windows enabled desktops and mobile devices. This allows enterprise users to log onto corporate resources, and sign documents or email on their mobile devices and PCs using a token or badge that communicates via Bluetooth with all PKI applications.

MobilePKI Office

On-the-go connectivity with Bluetooth Smart devices

CT1100

Solution components

Offering a choice of form factors, the MobilePKI Office solutions consists of the SafeNet Reader CT1100, a Bluetooth Smart enabled smartcard badge holder, and the SafeNet Reader K1100, a Bluetooth Smart enabled USB token. The devices are compatible with all Windows PKI applications and act as a standard reader for PKI credentials. Also, for MAC desktops and laptops, MobilePKI Office is compatible with any PKI credential.

Both devices are extremely lightweight with up to a two month battery life and Gemalto's managed pairing provides secure, quick and easy connection with devices. The devices also feature multi-host support so users can connect to more than one device at the same time. The devices are supported by the IDGo800 middleware which is available on Windows desktop and MacOS Operating Systems. They can also be used with the Base CSP / Minidriver and PKCS#11 libraries.

For iOS and Android devices, the Bluetooth devices are compatible with IDGo 800 for Mobile*, Gemalto's Mobile SDK, which allows the development of custom applications for these platforms. IDGo 800 for Mobile includes a PKI API, an OTP API, a PC-SC API and a range of drivers to interface with a larger range of secure elements, such as Bluetooth Smart, Micro-SD, USB, NFC and smart card readers.

K1100

BENEFITS OF GEMALTO BLUETOOTH SMART DEVICES

Enhanced battery usage time

- **Enhanced battery usage time** —The low consumption of the BT 4.0 standard, combined with the Gemalto smart power management protocol, Bluetooth Smart devices will last 10 times longer between charges (compared to previous Bluetooth versions)
- **Secure pairing**—Gemalto's managed pairing provides secure, quick and easy connection with devices
- **Secure communication**—The security protocol of Gemalto's Bluetooth products were built to overcome all known security issues related to the Bluetooth protocol

Supported Operating Systems

- Android, iOS, Windows 7+ desktop, MacOS

Gemalto's Identity Protection 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: **www.gemalto.com/identity.**

SUPPORTED USE CASES

- Smart Card logon
- Strong two-factor authentication
- Secure remote access (VPN/ Web)
- Digital signature
- Email encryption

GEMALTO.COM

gemalto
security to be free