Bit4id tokenME

User manual

Bit4id srl
Head Office Napoli:
Via Coroglio, 57
Città della Scienza
80124 Napoli – Italy
Tel. +39 081 7625600

Sales Office Milano:
Corso Vercelli, 11
20144 Milano - Italy
Tel. +39 024 547 42 59
info.it@bit4id.com

Bit4id Ibérica
C/ Marie Curie, 8-14
Forum Nord de Tecnología
08042 Barcelona - España
Tel. +34 935 35 35 18
info.es@bit4id.com

Oficina Lisboa
Alameda Bonifácio Lázaro
Lozano, 13 Ed. B 1ºE
2780-125 Oeiras- Portugal
Tel .+351 214 694 060
info.pt@bit4id.com

Bit4id UK:
2 London Wall Buildings
London Wall,
London EC2M 5UU - UK
Tel. +44 (0)2 03 3973166
info.uk@bit4id.com

Oficina Guatemala
15 avenida, 14-09 zona 10
Oakland - 01010
Guatemala
Tel: +502 22 21 91 63
aor@bit4id.com

Bit4id Perú
Mártil Olaya, nº 169
Oficina 406 - Miraflores
Lima
Perú
Tel: +51 1 242 9994
info.pe@bit4id.com

Support and Contacts

Bit4id and its partners provide high-end support. The first line of support is your reseller anyhow if you do require additional help and/or latest documents version you can contact Bit4id at:

Spain and Latino America	Rest of the countries
Sales support: comercial@bit4id.com Technical support: soporte@bit4id.com Website: www.bit4id.com Telephone:+34 935 35 35 18	Sales support: info@bit4id.com Technical support: support@bit4id.com Website: www.bit4id.com Telephone:+39 081 76 25 600

Author	GAM
Date of publication	17/09/2014
Revision author	MCU
Revision	5.0
Last update	27/02/2015

SUMMARY

1. Introduction

This document was written to illustrate the use of tokenME FIPS and tokenME CC (thereafter tokenME) and contains the documentation about the hardware specifications and special features.

tokenME has been implemented to be integrated into a large number of application and scenarios concerning digital signature and authentication into PKI infrastructures (Public Key Infrastructures). The device is totally driverless and needs no installation (on Microsoft platforms starting from Vista) to make it work.

Bit4id has made available a “configurator” that allow to use the digital identity into various applications just by following the simple wizard once started the application.

2. Inserting the Device

tokenME has to be inserted into the host PC as shown in Figure 1.

Figure 1

Once inserted the OS will recognise two devices that can be identified following the path “Start>Devices and Printers”. In this window two icons will be shown: Smart Card and TokenME (please refer to figure 2).

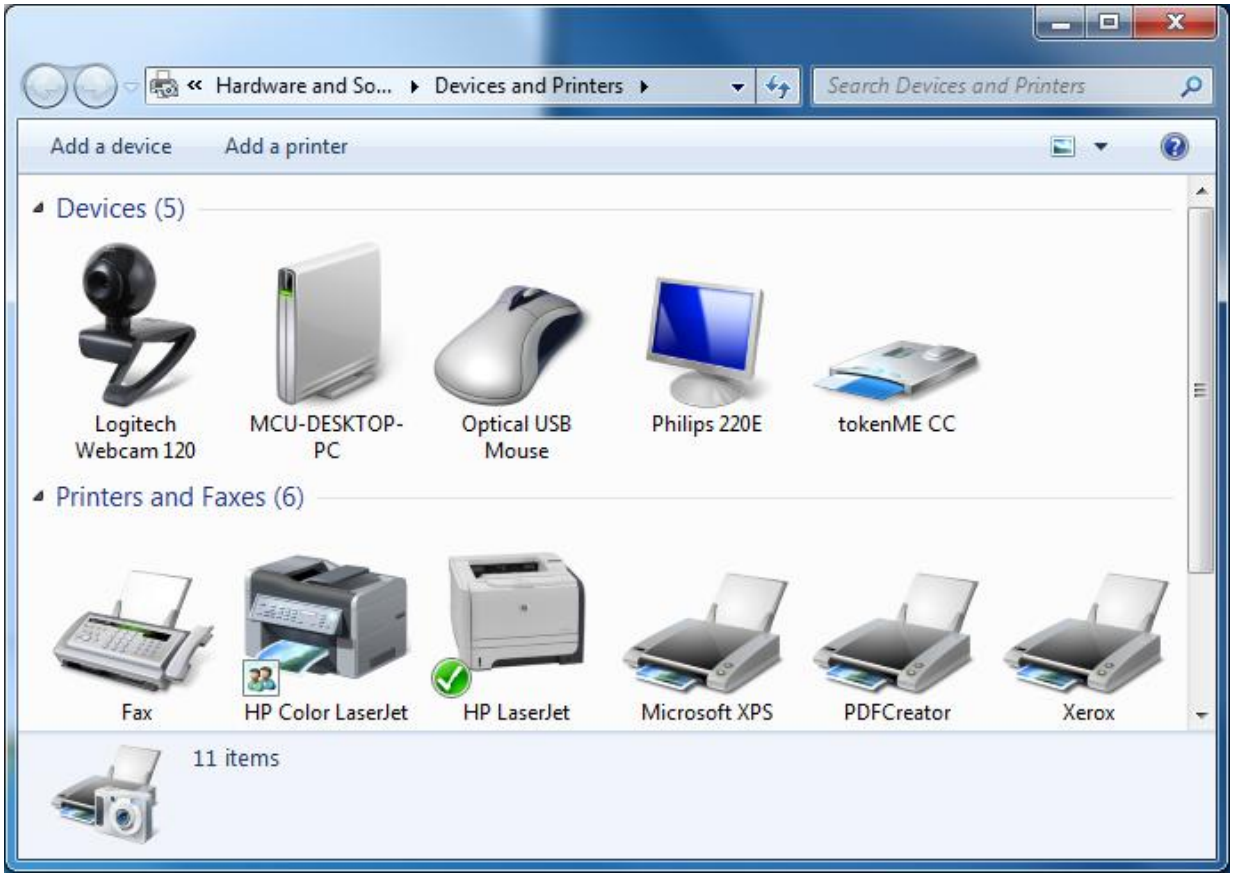

Figure 2

Once the OS has recognised the tokenME it is possible to run the “configurator” software.

3. Device Specification

Cryptographic Services

- Public Key Pair Generation
- Digital Signature
- Encryption / Decryption
- True Random Number Generation

Cryptographic Algorithms

- RSA up to 2048 bits
- Communication
- USB 2.0 Full Speed
- USB CCID compliant
- HID/driverless working mode (*)

Certifications and standards:

- FIPS 140-2 Security Level 3 (tokenME FIPS)
- Common Criteria EAL4+, SSCD Type 3 protection profile (tokenME CC)
- EN 60950/IEC 60950, EMV 2000 Level 1, PC/SC, CCID, CE, FCC, VCCI, RoHS Compliant, USB Full Speed

(*) optional on tokenME CC

4. Installing tokenME

tokenME is a USB 2.0 dongle implementing standard CCID specification. It appears to the operating system as a Smart Card Reader.

To use it you should use the PCSC/PCSCLite resource manager and a CCID driver.

On Microsoft Windows, starting from Windows Vista, the Microsoft CCID driver is integrated in the Operating System. On Microsoft Windows XP and Windows Server 2003, the Microsoft CIID driver can be downloaded automatically from Windows Update or, for your convenience it's located in the directory “utilitiesccidxp"

Note: PLEASE DO NOT install the XP CCID driver on Vista, Windows 7 or later versions.

On OSX versions up to 10.9 you need to install a specific driver in order to add tokenME to the PCSCLite resource manager. The OSX driver is located in the directory “utilities/ccid/osx".

Starting from OSX 10.9.2 tokenME is supported out of the box by Apple's CCID driver.

On Linux you may need to install, on certain distributions, the pcsc-lite and the libccid driver packages. Please refer to your distribution documentation to install such a packages.

Note: on Linux make sure the libccid driver version is 1.4.7 or later.

5. Using tokenME

To use tokenME you need to use one of the Interface libraries: PKCS#11 on all supported platforms, CSP/Crypto API on Microsoft Windows, TokenD and Apple's CDSA.

That libraries are able to access transparently both version of tokenME (CC and FIPS).

Please refer to CSP, PKCS#11 and TokenD documentation included in this SDK for more information.

Note: starting from OSX 10.7 the CDSA (and therefore TokenD) has been deprecated by Apple. Support it's still included in recent OSX distributions, but Apple discourage to develop new applications using CDSA.

6. FCC Statement

This equipment has been tested and found to comply with the limits for Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency

energy and, ifnot installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Notice per 47CFR15.21 Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

7. Disposal Information

The device should not be disposed with other household/commercial wastes disposal, separate it from other types of waste and recycle them to promote the reuse of material/resources. Please follow the indication provided by local authorities for electronic equipment disposal.