EUTRON INFOSECURITY

OTPSign

Overview version 1.0.1

This hardware key is in compliance with the following test specification:
CEI EN 61000-4-2; CEI EN 61000-4-3; CISPR22
as required by:
CEI EN 61000-6-1, CEI EN 61000-6-2, CEI EN 61000-6-3, CEI EN 61000-6-4
which are specified for the following test:

- “ESD Immunity test”
- “Radiated radio-frequency and electromagnetic field immunity test”
- “Radiated Emission Verification”

In compliance with the “Essential Requisites” for the EMC Directive 89/336/EEC.

FCC ID: TFC-AAE

EUTRON Infosecurity S.r.l.
OTPSign ([1])
Supply: 5V DC
Absorption: 30 mA

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.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to 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, if not 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 into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

[1] The models subjected to this mark are the following: OTPSign ITSEC-I, OTPSign ITSEC-P and OTPSign FIPS.

IMPORTANT REMARKS

Due to the limited space on the product shell, all FCC certification references are on this technical manual.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

1. *Introduction*

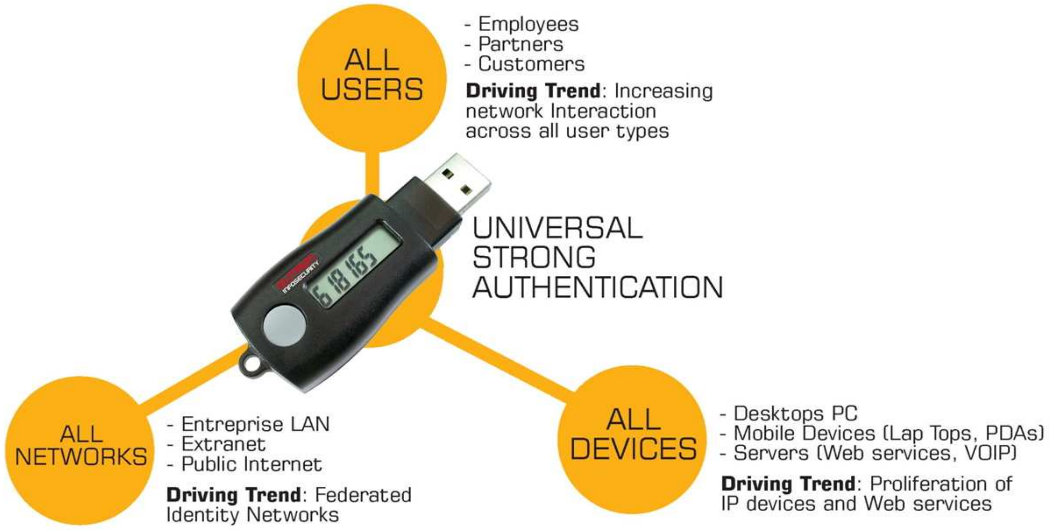
OTPSign is the new USB token realized by applying the innovatory EUTRON-VASCO hybrid technology that combines the advantages of OTP authentication with the potential offered by PKI technology.

OTPSign is a device that enables accessing the digital services quickly and safely through the telephone, mobile and Internet channels, besides allowing secure and non-repudiable transactions; it is therefore an extremely flexible, inexpensive and simple solution. This product is ideal for all those entities and organizations that intend to offer their customers secure multichannel accesses to corporate archives, bank data, financial services, health services et cetera.

OTPSign is an M2 secure device: multichannel and multipurpose:

- ***Multichannel***, thanks to the OTP USB hybrid technology that allows secure access from the fixed and mobile telephone network, from the Internet and via Internet through the USB token
- ***Multipurpose*****,** thanks to the EUTRON «all-in-one» technology which combines the OTP component with the smart card cryptography function and the smart card reader.

STRONGLY AUTHENTICATING, EVERYONE AND EVERYTHING-EVERYWHERE


ALL USERS
- Employees
- Partners
- Customers
Driving Trend: Increasing network Interaction across all user types
UNIVERSAL STRONG AUTHENTICATION
ALL NETWORKS
- Entreprise LAN
- Extranet
- Public Internet
Driving Trend: Federated Identity Networks
ALL DEVICES
- Desktops PC
- Mobile Devices (Lap Tops, PDAs)
- Servers (Web services, VOIP)
Driving Trend: Proliferation of IP devices and Web services

2. *Main functionalities*

OTP Functionalities

- One-Time-Password authentication
- Button-operated OTP generation
- OTP Encryption: Time synchronous / Time and Event synchronous
- Compatibility with the whole Digipass VASCO family

PKI Functionalities

- Signature and on-board generation of the 1024 bit RSA key pair
- X 509 v3 certificates and secure key storage
- PIN for private key protection

3. Models

- **ITSEC-I** with 32K EEPROM, RSA 1024 bit cryptography, INFINEON SLE66CX322P cryptographic chip, CardOS 4.01A (ITSEC E4 High certified) or CardOS M4.2B (CC EAL 4+certified) or CardOS M4.3B (CC EAL 4+ certified) Siemens - chip CC EAL 5+ certified
- **ITSEC-I-64** with 64K EEPROM, RSA 2048 bit cryptography, INFINEON SLE66CX642P cryptographic chip, CardOS M4.3B Siemens mask – Chip CC EAL 5+ certified and mask CC EAL 4+ certified
- **ITSEC-P** with 32K EEPROM, RSA 1024 bit cryptography, PHILIPS P8WE5032 cryptographic chip, G&D StarCOS SPK 2.3 mask – Chip and mask ITSEC E4 High certified
- **FIPS** with 32K EEPROM, RSA 1024 bit cryptography, PHILIPS P8WE5032 cryptographic chip, G&D StarCOS SPK 2.4 mask

4. Specifications

Standard

ISO 7816 3-4, PKCS#11 v2.11, PC/SC, Microsoft CAPI, S/MIME, IPSec/IKE, X.509 v3

Operating systems

Microsoft Windows 98/ME/2000/XP and LINUX

Interoperability

Microsoft Internet Explorer, Microsoft Outlook, Lotus Notes 6.0x, Adobe Acrobat, VPN clients and with all applications using the reported standards

5. Technical specifications

OTP section

- 8 character LCD Display
- Real time clock on board
- Battery life: 5 years minimum
- Compatibility with the Digipass VASCO family

USB PKI section

- Transfer rate of cryptographic component: up to 115Kbps
- Power supply: from USB bus (4.5V - 5.5V)

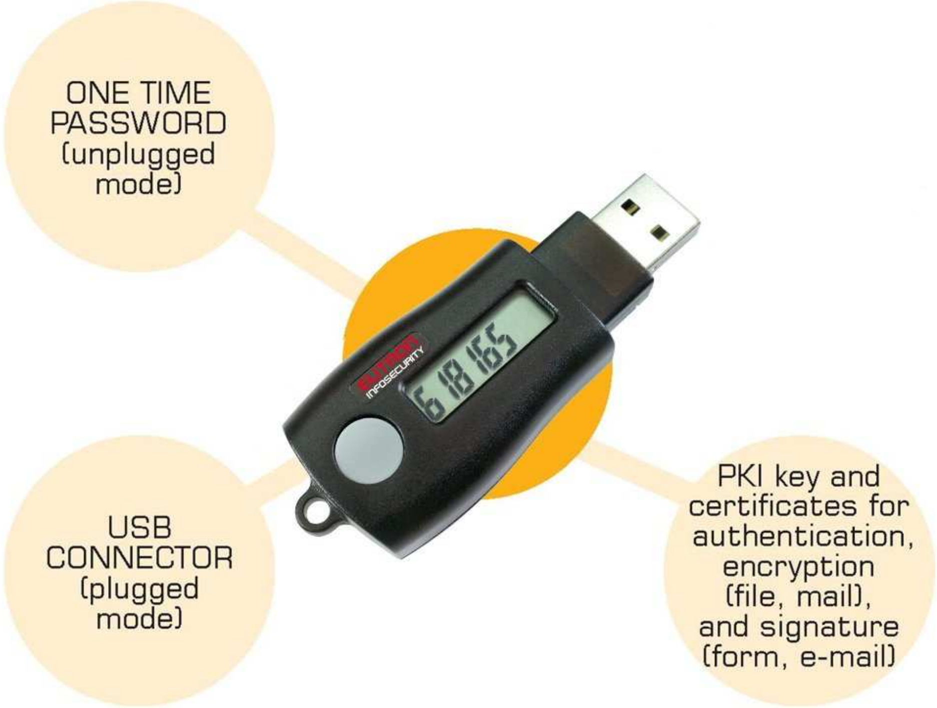
Minimum hardware requirements

- Pentium 100MHz or higher
- 1 USB 1.1 port or higher

6. Activation and setup of OTP-PKI services

Integrating the OTP component in the existing networks is simple and easy. Any static password can be replaced instantly with the more secure OTPSign-generated dynamic password. You simply start the programming procedure.

OTPSign is fully interoperable with the entire Vasco Digipass product family; it works hand-in-hand with Vacman Controller or Vacman Server applications and with other 50 software programs by the main world vendors, thus allowing quick commissioning with low development costs.


ONE TIME PASSWORD (unplugged mode)
USB CONNECTOR (plugged mode)
PKI key and certificates for authentication, encryption (file, mail), and signature (form, e-mail)
618165
EUTRON INFOSECURITY

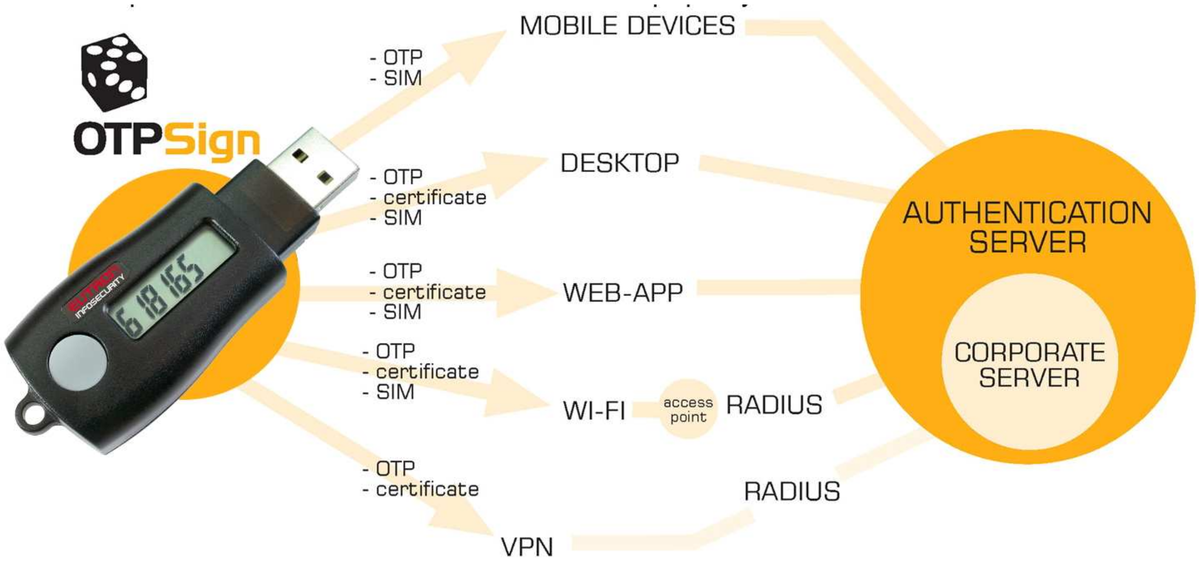
7. Operation scope and usability

OTPSign is especially suitable for managing any various secure authentication needs, in particular within the Corporate and Banking ambit. The device flexibility makes it suited for handling Web access, remote access, login-LAN, VPN access and PKI authentication in total security.

OTPSign is handy, pocket-sized, light and user-friendly. By pressing the button a univocal one-time-password is displayed on the LCD screen, enabling the multichannel authentication.

The user can therefore be service authenticated instantly through the OTP password, besides carrying out any cryptographic operations required by the service: digital signing, secure data encrypting, non-repudiability and integrity guarantee of data exchanged through the SSL protocol.

OTPSign is also the ideal token for home banking: it provides the fulfilment, longed-for by banking services in particular, which are under various informational attacks and risks (“phising” especially), of the need for simple, effective and really secure authentication and transactions; it also meets the wish of the most important banks to offer their Clients on-line top-quality services.


OTPSign
- OTP
- SIM
MOBILE DEVICES
- OTP
- certificate
- SIM
DESKTOP
- OTP
- certificate
- SIM
WEB-APP
- OTP
- certificate
- SIM
WI-FI
access point
RADIUS
- OTP
- certificate
RADIUS
VPN
AUTHENTICATION SERVER
CORPORATE SERVER
618165