OPERATIONAL DESCRIPTION

1.1. Description of the OTP TOKEN

Enterprises frequently deploy multiple authentication mechanisms to address diverse usage scenarios within and beyond the corporate network. The most common scenarios that need strong authentication are remote access, Windows® logon, and Wi-Fi access. However, in today's competitive business environment, the need to protect proprietary company information is ever increasing. And this risk increases as more and more mobile workers access company networks and move files to and from their home office or remote locations via a USB Flash Storage Device. Once these documents are removed from the network and placed on a mobile device, the vulnerability of these documents increases. USB Flash Storage Devices are convenient and small, and therefore, are subject to being lost, misplaced or even falling into the wrong hands. Therefore, the need to constantly protect company information, whether it is inside or outside the network, is becoming a problem for both small and large enterprises.

The OTP Token combines One-Time Password (OTP) and PKI authentication with Secure Storage and smartcard technology, enabling a variety of security-related applications. The token includes a USB Flash drive that connects to a computer's USB port to enable the transfer and encryption of files to and from the storage device. A user PIN is all that is required to quickly and easily access and decrypt files for removal from the device. This personal and versatile mobile device is the perfect solution for unifying authentication and encryption mechanisms to protect employee's credentials and sensitive information.

The OTP Token is an all-in-one personal mobile security device. The device enables you to strongly authenticate using OTP functionality and/or PKI, and allows you to safely store your digital certificate in the tamper resistant module as well as personal information and company documents on its storage unit. Secure mechanisms enable PIN reset, providing for an efficient and safe way for users to recover a lost or forgotten PIN. Recovery of encrypted data by administrators is also supported, paving the way for data recovery in the context of the enterprise.

1.2. Related Submittal(s) / Grant(s)

All host equipment used in the test configuration are FCC granted, when relevant.

1.3. Tested System Details

The FCC IDs for all equipment, plus description of all cables used in the tested system are:

Trade Mark – Model Number (Serial number)	FCC ID	Description	Cable description
OTP TOKEN * **(sn: none)** ***Without Flash memory***	**MESOTP**	**Personal Mobile Security device**	USB extension cord (1.1 standard): 1m
OTP TOKEN * **(sn: none)** ***With 128Mo Flash memory***	**MESOTP**	**Personal Mobile Security device (with secure storage)**	USB extension cord (1.1 standard): 1m
TOSHIBA T9000 PIII **Model: PT9000E-03SFH-FR** **(sn: Y1081087G ST900-0**	**CJ6PA3070WL**	**Laptop PC**	DC power supply cable, unshielded: 1.8m
TOSHIBA AC adaptor **Model: PA3215U-1ACA** **(sn: 03410994)**	**None**	**AC/DC adapter (100V-240V / 15Vdc)**	AC power cable, 2 wires: 2m

*: Equipment under test

1.4. Test Methodology

Radiated testing was performed according to the procedures in ANSI C63.4-2003, FCC Part 15 Subpart B.
Radiated testing was performed at an antenna to EUT distance of 10 meters. Radiated testing was performed at an antenna to EUT distance of 10 meters. During testing, all equipment's and cables were moved relative to each other in order to identify the worst case set-up.

1.5. Test facility

Tests have been performed on March 14th and 25th, 2005.

The test facility used to collect all the test data is the SMEE ***Actions Mesures*** facility, located ZI des Blanchisseries, 38500 VOIRON, France.
This test facility has been fully described in a report and accepted by FCC as compliant with the radiated and AC line conducted test site criteria in ANSI C63.4-2000 in a letter dated July 19, 2002 (registration number 94821).
This test facility has also been accredited by COFRAC (French accreditation authority for European union test lab accreditation organization) according to NF EN ISO/IEC 17025, accreditation number 1-0844 as compliant with test site criteria and competence in 47 CFR Part 15/ANSI C63.4 and EN55022/CISPR22 norms for 89/336/EEC European EMC Directive application. All pertinent data for this test facility remains unchanged.