

Technická specifikace tokenu TokenME EVO 3



TokenME EVO 3 je nejnovější zařízení od firmy Bit4ID, které je schválené jako kvalifikovaný prostředek pro vytváření elektronických podpisů a elektronický pečetí v souladu s nařízením eIDAS a slouží k vytváření kvalifikovaných elektronických podpisů a pečetí. Je to PKI token postavený na kryptografickém mikroprocesoru s certifikací Common Criteria EAL5+ a FIPS 140-2 level 3.

Technické vlastnosti:

Paměť: 144KB

DES, 3DES, AES: 128, 192, 256bits

RSA: Cipher/Decipher, (SFM&CRT) from 512 up to 2048 bits (step of 32bit) RSA Key Generation: up to 4096 bits

ECC: P-256, P-384, P-521

EC Key Generation: up to 521 bits

SHA: SHA1, SHA-224, SHA-256, SHA384, SHA512

EC-DSA SHA-1, SHA-256,

SHA-224, SHA-384 and SHA-512

Supported signing, encryption schemes

PKCS#1 version 1.5 and 2.1 RSAES-OAEP for encryption and RSASSA-PSS for signing

Umístění zařízení na seznamu eIDAS

Seznam: Certifikované zařízení SSCD a QSCD

CC EAL5+ SmartCard on JCOP3 SECID P60 (OSB) Security IC Platform Protection Profile for SSCD z 14.1.2020

CC EAL5+ ChipDoc P60 on JCOP3 in ICAO SSCD configuration, verze v7b4_2 z 20.11.2017

Podporované operační systémy Windows

Microsoft Vista, 7, 8, 8.1, 10 server 2003, 2008(R2) 2012(R2), 2013, 2016

