

Čipová karta Gemalto IDPrime MD 840/940

Technické parametry

Podporované operační systémy:	Windows, MAC, Linux (podporované jejich výrobci)
Middleware:	SafeNet Authentication Client (SAC)
Standardy:	BaseCSP minidriver v7 (IDGo 800 Minidriver) PKCS#11 & CSP (SafeNet Authentication Client)
Certifikace:	CC EAL 5+
Šifrovací algoritmy:	RSA: up to RSA 2048 bits, RSA OAEP & RSA PSS, elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH, generování klíčů v hardware karty (RSA & Elliptic) 3DES (ECB, CBC), AES (128, 192, 256 bits)
Hashovací funkce:	Hash: SHA-256, SHA-384, SHA-512
Velikost paměti:	80 kB; až 15 kontejnerů pro uložení šifrovacích klíčů (RSA, elliptic curves)
Uchování dat v paměti:	nejméně 25 let
Přepisování paměti:	nejméně 500 000 cyklů
Komunikační protokol:	T=0, T=1, PPS, with baud up to 230 Kbps
Velikost:	standardní čipová karta
Záruka:	12 měsíců