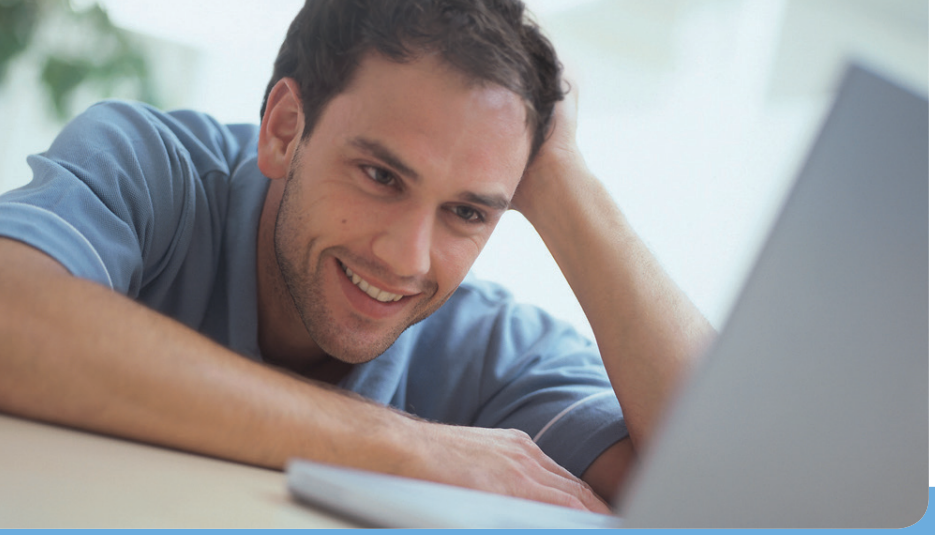

NXP IDProtect client middleware V6 & V7

The fast, secure way to deploy & manage multi-factor authentication

This standards-driven middleware supports multi-factor authentication on a single, secure cryptographic device, and uses broad-based compatibility, with support for the latest mobile applications, to speed deployment and simplify access management.

KEY FEATURES

- Mixed network topologies (Windows, Linux, Mac OS X, Android)
- Microsoft-certified CAPI/CAPI2/CNG/MD and PKCS#11 interfaces
- TokenD support for Mac OS X
- Biometric support
- ECC support
- Next-gen Android crypto apps (V7 only)
- Certified by Microsoft for all systems
- Multi-language operation
- Works with PC/SC compatible readers
- CMS systems support (integrates with MyID, FIMCM, OpenTrust, Versatile security, BlueX)
- Virtual environment support (Citrix, VMware)

KEY BENEFITS

- Secure, cross-platform operation
- Flexible form factors, fast deployment
- Simple lifecycle management

APPLICATIONS

- Logical access
- Mobile applications
- Biometric smartcards

NXP's IDProtect middleware provides a robust link between user credentials, stored on a secure device, and the client authentication system. Fully certified to protect mixed-network topologies and supporting multi-factor authentication, the software strengthens the steps involved in user authentication, signature, VPN logon, and encryption, and safeguards system integrity.

The IDProtect client works with a range of smartcard and/or token form factors, including contact, contactless, USB, MicroSD, Secure Bio Reader, or BLE. The client generates keys, matches biometric data, and stores PIN policies on the device. All sensitive communication between the host and device, including keys and PINs, is encrypted using secure messaging. The setup supports RSA cryptography up to 4096, SHA2 and ECC cryptography.

FLEXIBLE & INTEROPERABLE

The IDProtect client simplifies installation by providing full Windows client/server compatibility, along with support for Linux, Apple Mac OS X, and Android. For Windows, the middleware can be installed as either a CSP or a Minidriver. There are also APIs for PKCS#11. The OEM-ready, scalable architecture supports multi-language use and offers customizable MSI installation parameters.

Support for certified CAPI/CAPI2/CNG and PKCS#11 interfaces ensures the broadest interoperability, with hardware and software associated with Windows, Microsoft Outlook, Adobe, Checkpoint, Cisco, Citrix, Firefox, Lotus Notes, Novell, PGP, and many others.

For broad-based compatibility with the reader infrastructure, the IDProtect client is designed for use with PC/SC compliance card readers.

OPTIONAL BIOMETRICS

The IDProtect client offers full biometric support, with multiple finger templates, for use with Windows Logon authentication, ISO-standard biometric Match-on-Card algorithms, Minex II, Minex III. The middleware supports a comprehensive range of market sensors, including Crossmatch (Digital persona/UPEK/Authentec) optical, Validity, Nitgen optical, Precise Biometrics, NEXT Biometrics, and WBF-supported sensors.

FAST AND EASY

The IDProtect client eases issuance and lifecycle management. For large-scale deployments, the middleware is integrated with leading CMS systems, such as Microsoft FIMCM, MyID, OpenTrust, Versatile security, and 3DES challenge-response mechanisms. For small- and medium-scale deployments, the middleware is available with the IDProtect Admin Card tool. Either way, users have access to features like lifecycle management, remote unlocking, self-service portals, and multi-CA support.

VERSION 7

Version 7 builds on all the functionality of Version 6, adding support for next-generation mobile crypto apps on the Android platform, SSCD support, PKCS#15 file system support, and Light PKI for banking cards.

Technical highlights

OS support	Windows 32/64-bit clients (XP, Vista, 7, 8/8.1, 10 beta), Windows 32/64-bit servers (2003, 2008/R2, 2012/R2), Mac OS X 10.5 and above, most Linux distributions (deb and rpm formats), Android platform 4.x and above
Specification support	Windows Smart Card Minidriver Microsoft Log certified (Spec 7.06), Microsoft CAPI, CAPI2, and CNG support, PKCS#1, 7, 10, and 11 (2.20) specifications, X509 version 3 certificates, ISO/IEC 7816-3, 4, 5, 6, 8, 9, 11, and 15 for supported devices
Cryptographic support	ECC cryptography support for all key sizes (256, 384, and 521-bit keys) RSA up to 4,096 bits
Security features	PKCS#11 implementation does not export private keys, PIN policy enforced on card, not on host, extra layers of security protect PIN verification offline brute-force attacks, PIN history maintained on card, PIN can be changed on first use or after unlock (managed, tracked on-card), PIN can be set to expire after specific time periods (managed on-card)
Optional biometrics	Match-on-Card based on ISO 19794 or Precise Biometrics (V3.0), biometric only or biometric + PIN, XP with Graphical Identification and Authentication (GINA) change (Vista and above) via credential provider of OS
Applets	Laser PKI, ChipDoc (V7 only), Light PKI for banking (V7 only)
Version 7 add-ons	PKCS#11 (version 2.20) and JCA for Android, Secure Signature Creation Devices (SSCD) keys with signatory PIN/PUK, ISO/IEC 7816-15 (PKCS#15) file system

Date of release: October 2015
Document order number: 9397 750 17679
Printed in the Netherlands