



CryptoKit™ - simplicity  
without compromising security

## A Powerful Versatile Toolkit for Developing Secure Applications

With the rapid growth of e-business today, companies are more concerned than ever to ensure that all sensitive transactions are absolutely safe. By enabling organizations to incorporate strong security, CryptoKit can help them to widen their e-business horizons.

CryptoKit is a flexible set of development tools that enable convenient integration of cryptographic-strength data security into any 3<sup>rd</sup> party application. CryptoKit functionality is based on the industry-wide PKCS#11 standard and can be easily incorporated even by developers with no cryptographic background.

CryptoKit version 3.0 contains SmartAdaptor™ technology that provides outstanding flexibility by enhancing interoperability between smart card readers and smart cards from different vendors. Moreover, SmartAdaptor enables automatic support for 3<sup>rd</sup> party

PKCS#11 libraries and provides an adaptation layer for Entrust applications, for MS-Crypto API and ports the PKCS#11 API to Java.

Using these features, developers can build an application today that uses one type of security token, including software token (for key storage etc.) and later, use CryptoKit to enable smooth integration of other smart card readers, smart cards, tokens and biometric devices, if a stronger implementation is needed.

Organizations can also use CryptoKit's Crypto API or Java PKCS#11 API to build their applications.

CryptoKit is an integral part of ARX's Security Architecture providing the underlying technology for all ARX products used by major e-businesses worldwide.



## ■ CryptoKit supports the following readers, smart cards and tokens:

- MiniKey USB token
- PrivateSafe smart card reader
- CryptoSafe smart card reader
- PrivateCard smart card
- Software token
- All CT-API readers (after brief registration)
- Readers with proprietary API (when an adaptation layer is provided)
- All PC/SC readers

## ■ Common CryptoKit Applications

- E-commerce
- On-line banking and trading
- Secure e-mail, S/MIME
- Secure login
- B2B commerce
- PKI client
- Secure and signed transactions
- Remote access
- Authentication and authorization
- Data encryption and integrity

## ■ Security Added to Any Application

CryptoKit can protect almost any application with features such as encryption, non-repudiation, authentication and data integrity verification. The toolkit has been successfully implemented to secure various applications such as remote banking, electronic purchasing, and processing of medical information and payroll accounts. CryptoKit also serves as the standard development toolkit for all products available from ARX.

## ■ Flexible Security Architecture

ARX Security Architecture (ARX-SA) provides a modular and flexible set of solutions addressing organizations' current and future security requirements. ARX-SA CryptoKit toolkit enables effective integration of data security functions into any application and transparent interoperability with ARX or 3<sup>rd</sup> party products.

## ■ PKCS#11 or CAPI Standard API

By implementing the PKCS#11 standard, CryptoKit enables vendor-independent access, through a standard API, to ARX advanced security services. In addition, a Crypto API layer is provided to allow developers to choose the SDK that best fits their needs. ARX's PrivateCard, PrivateSafe, CryptoSafe and MiniKey can be easily incorporated in new and existing financial, healthcare and government applications that rely on either industry-wide standard: PKCS#11 or Crypto API.

## ■ Cost-Effective and Flexible Software and Hardware Implementations

CryptoKit security functions can be executed in software only, or integrated with hardware for maximum security. CryptoKit's API provides easy and transparent access to AR's smart card solutions to perform advanced cryptographic processing in a

secure tamper-proof environment. ARX's smart card products include CryptoSafe and PrivateSafe smart card readers, PrivateCard, an advanced public/private key smart card and MiniKey, an advanced USB token.

Support is also scheduled for a combination smart card/biometric reader that checks a user's fingerprint against the fingerprint template stored on his PrivateCard smart card.

No changes to applications are required when using software or hardware. Full transparency ensures a cost-effective implementation with easy migration from software to hardware.

## ■ Advanced Cryptographic Capabilities

- RSA key generation (1024-2048 bit length)
- RSA digital signatures
- RSA encrypt/decrypt
- DSS key generation (1024-bit length)
- DSS digital signatures
- Diffie-Hellman key management
- Public key management and certification
- Random number generation
- DES, Triple-DES, RC4 and RC2 encryption/decryption
- Hash functions
- X.509v3 certificates and X.509v2 CRLs
- PKCS#11, PKCS#10, PKCS#8, PKCS#7, PKCS#1, MS Crypto API.

## ■ Simplicity without Compromising Security

The application developer need not be a cryptographic expert. Simple, high-level instructions are translated internally into complex cryptographic functions and protocols. Therefore, development can be performed easily by independent or in-house developers.

## ■ Platform Independence

CryptoKit supports multiple platforms and operating systems, including Windows 95, 98, NT and Windows 2000. Support for Unix platforms is scheduled in the next release. Additional platforms may be supported as required.

## ■ Communication Protocol Independence

Once CryptoKit security functions have been integrated into the application, there are no limitations on using any communication protocol supported by the application. CryptoKit integration into the application provides tight and true end-to-end security, independent of any network considerations.

## ■ Multiple Development Environments

CryptoKit provides both a unified and consistent API for all platforms and an open environment enabling integration in any software development environment supporting C or Java calls.

## ■ Multiple Options for Key Storage

CryptoKit supports storage of encryption/decryption keys on both software and hardware using a unified interface based on the PKCS#11 standard. Storage media include MiniKey, various smart cards, removable floppy diskettes and special files on a disk.

### ARX - The Cryptographic Specialists

ARX (Algorithmic Research) is a leading global supplier of cryptographic-strength data security solutions for financial, commercial, industrial and government applications. For over two decades, ARX has been providing advanced cryptographic security solutions for a wide variety of applications. This acquired experience in designing and implementing critical, large-scale security solutions and smart card based applications enables ARX to bring innovative, cutting-edge technologies to its entire range of data security products.



ARX (Algorithmic Research)  
855 Folsom St. Suite 939  
San Francisco, CA 94107  
Tel: (415) 839 8161  
Fax: (415) 723 7110  
www.arx.com