Now, a SecureWay Software offering

IBM KeyWorks Toolkit and Key Recovery Service Provider

Highlights

Implements The Open Group Common Data Security Architecture

Helps accelerate the development of cryptographic and security functions essential to e-business

Allows customers to choose between different trust models, signing algorithms and encryption algorithms

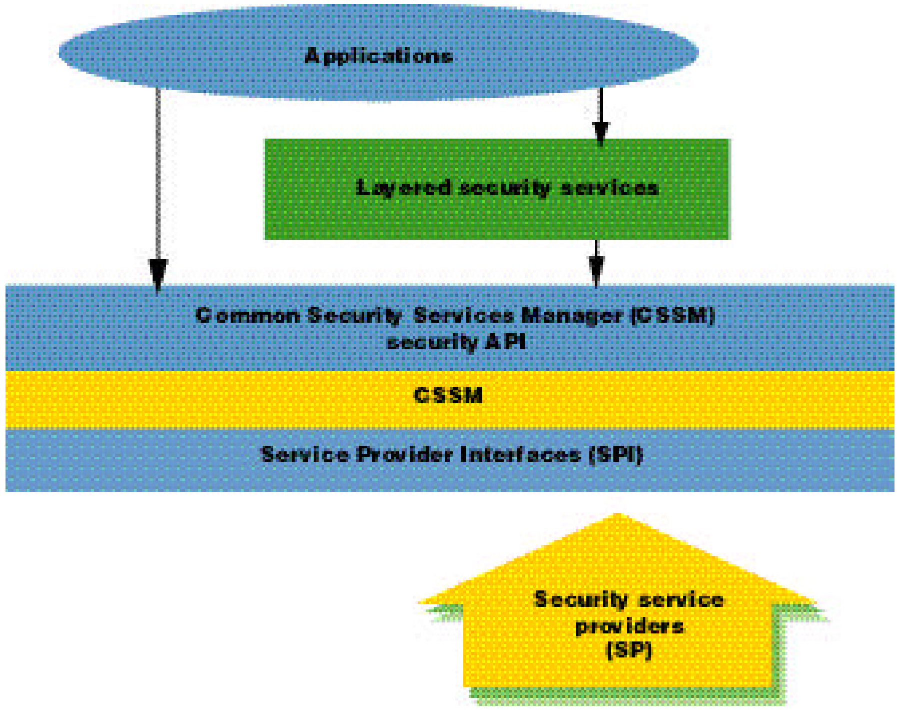
Can enhance programmer productivity by providing a standard way to access cryptographic and other security functions

Permits changes or substitutions to service provider modules without rewriting the solution

Provides support for hardware-based encryption and digital signatures

Helps accelerate development of applications that require cryptographic services, including key recovery and cryptographic backup

Provides public key certificate parsing and life cycle management


Applications
Layered security services
Common Security Services Manager (CSSM) security API
CSSM
Service Provider Interfaces (SPI)
Security service providers (SP)

The Common Data Security Architecture (CDSA) is an industry standard from The Open Group.

More than likely, your users and administrators already rely on the Internet to deliver services and to conduct routine business with customers and business partners. But like most business people today, they probably stop short of sending highly confidential, critical data and files across the Internet. Why? They're worried about security.

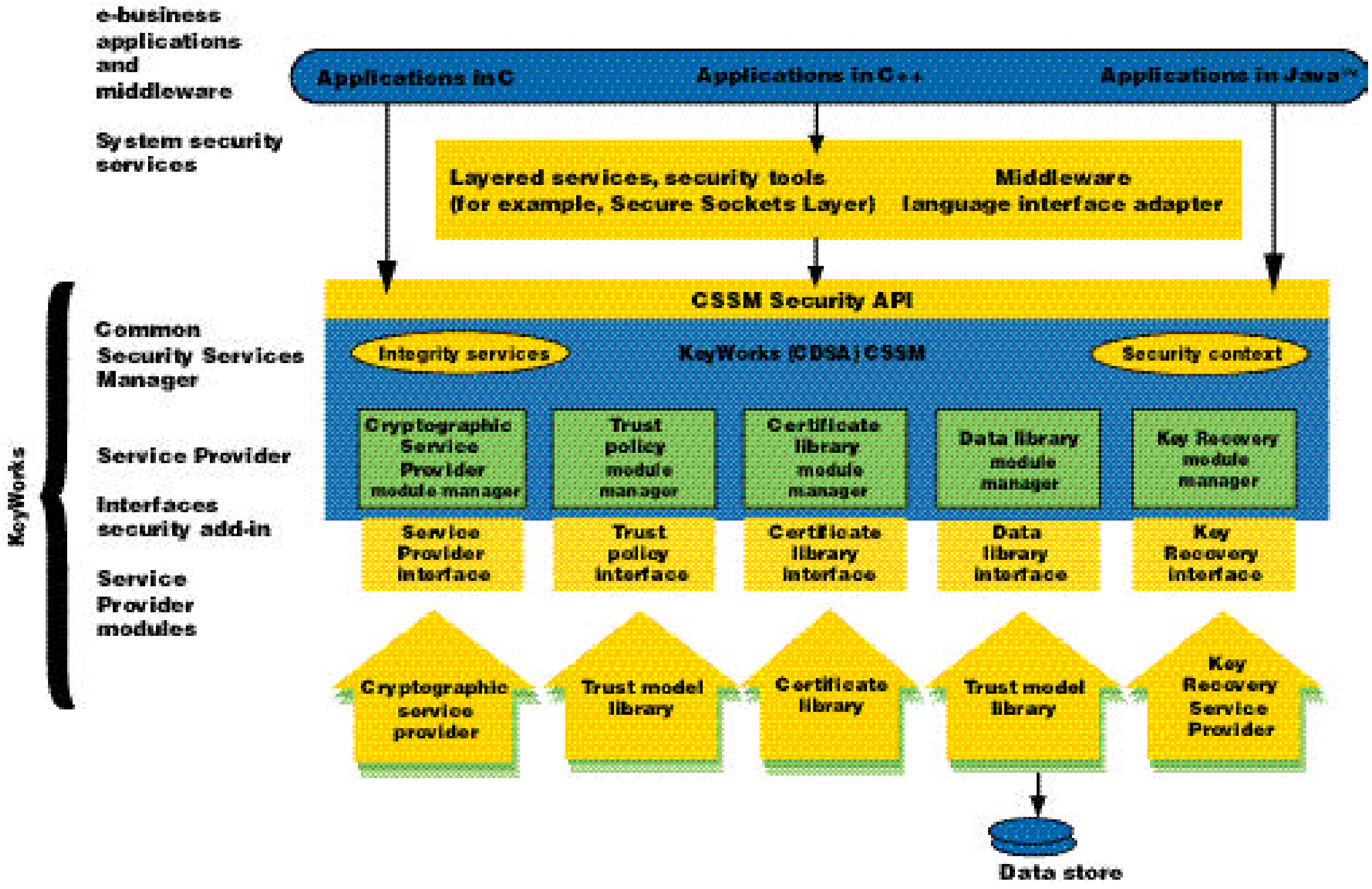
Accelerating security development to enhance your e-business

Faced with multiple application and solution changes, businesses often hesitate to devote large amounts of time and money to making each of their applications highly secure. Yet, in the world of e-business, companies that take full advantage of the Internet and its communication-enhancing technologies are the ones most likely to win.

As a system designer, engineer or programmer, you know all about the frustration of repeatedly redesigning and reprogramming proprietary cryptographic functions and algorithms into applications and middleware. You know your users need responsive, inexpensive and timely solutions. But in the past, your technical team was forced to solve security problems with vertical integration – one application at a time.

Create a protected e-business environment

IBM answers many of your critical needs for creating a protected e-business environment with IBM® SecureWay® FirstSecure toolbox, a component of FirstSecure. The components in the toolbox are designed to help you address the risks, complexity and costs faced during e-business deployment.



e-business applications and middleware
System security services
KeyWorks
Common Security Services Manager
Service Provider
Interfaces security add-in
Service Provider modules
Applications in C
Applications in C++
Applications in Java™
Layered services, security tools (for example, Secure Sockets Layer)
Middleware language interface adapter
CSSM Security API
Integrity services
KeyWorks (CDSA) CSSM
Security context
Cryptographic Service Provider module manager
Trust policy module manager
Certificate library module manager
Data library module manager
Key Recovery module manager
Service Provider interface
Trust policy interface
Certificate library interface
Data library interface
Key Recovery interface
Cryptographic service provider
Trust model library
Certificate library
Trust model library
Key Recovery Service Provider
Data store

IBM KeyWorks Toolkit is the IBM implementation of The Open Group CDSA standard.

By using toolbox components, such as IBM KeyWorks Toolkit, you can:

- Securely deploy e-business applications that use appropriate encryption and digital signatures
- Parse certificates and manage certificate life cycles
- Strengthen the security of existing operations by requiring cryptographic authentication
- Integrate cryptographic and security solutions with the legacy IT environment

The first two components of FirstSecure toolbox are KeyWorks Toolkit and Key Recovery Service Provider. These components can help you better leverage your resources to address cryptographic and trust issues effectively across your enterprise – with the added assurance you get by using products from IBM, a proven name in the security industry.

Security services built on an industry standard

KeyWorks Toolkit is a comprehensive set of layered security services built in compliance with the Common Data Security Architecture (CDSA), an industry standard from The Open Group. CDSA is a middleware framework (it has no GUI) that supports multiple trust models, certificate formats, cryptographic algorithms and certificate repositories. KeyWorks Toolkit makes it easier for you to choose the prime cryptographic security implementation for your needs – without having to rewrite applications each time these needs change. Sophisticated IT departments, systems integrators and solution providers can all benefit from the flexibility of KeyWorks.

KeyWorks Toolkit enhances programmer productivity

KeyWorks Toolkit provides standard interfaces applications can use to invoke cryptographic and trust services. It also has standard interfaces that allow you to plug in additional cryptographic and trust modules you have purchased or developed. The toolkit can enhance programmer productivity by providing a standard way to access cryptographic and other security functions across different operating environments.

KeyWorks Toolkit is compatible with the following operating systems: Microsoft® Windows NT®, Windows® 95, Windows 98, AIX®, OS/390® and Sun Solaris (Version 2.6). KeyWorks Toolkit functions as middleware for applications needing to access security services.

KeyWorks Toolkit offers critical functions that:

- Protect against bypassing vital steps in a toolkit-supported process
- Verify that the service provider plug-in modules have not been tampered with
- Allow plug-in modules from service providers to be used only through the framework
- Support country and enterprise-specific cryptography and trust usage policies
- Help ensure that KeyWorks cannot be circumvented in any environment where this policy is chosen

KeyWorks Toolkit cryptographic and trust services

KeyWorks Toolkit offers several services that support enterprise security solutions, including:

- Cryptographic services: bulk encryption, digital signature and hash algorithms, secure key storage and support for PC cards (PKCS #11).
- Cryptographic backup and key recovery.
- Certificate management: creation, revocation, manipulation and validation.
- Authentication services: focused on internal and external uses. For internal uses, key recovery and integrity are addressed, and for external uses, access and interoperation are addressed.
- Trust policy services: actions on certificates, actions on certificate revocation lists (CRLs), read-only LDAP remote access and domain-specific actions. Provides services for certification and CRL life cycle management.
- Certificate library services: performs certificate and CRL syntactic operations, (with access to certificate and CRL fields).
- Data storage: includes native file systems, database systems and custom hardware storage devices.

How the toolkit works

KeyWorks Toolkit provides an insulating layer between application programs and cryptographic and trust functions.

The toolkit contains a framework and service provider plug-in modules. At the application end (the top of the framework), the framework provides a standard application programming interface (API). The API is the functionally rich Common Security Services Manager (CSSM) API as defined in the CDSA standard from The Open Group; IBM has extended the API with the addition of key recovery functions.

At the service provider end (the bottom of the framework) is the standard Service Provider Interface (SPI) from CDSA, with the addition of key recovery support. The SPI provides an interface to pluggable service provider modules from the CSSM framework.

Plug-in service provider modules included with KeyWorks Toolkit are PKCS #11, RSA cryptographic functions, X.509V3 certificates, the trust policies of Entrust and VeriSign, and LDAP. The framework provides seamless integration of the security functions provided by each independent service provider module.

Toolkit users integrate KeyWorks Toolkit libraries with applications and middleware to produce KeyWorks-enabled client and server applications, and middleware runtimes. A number of original equipment manufacturers and systems integrators currently offer KeyWorks-enabled runtime client and server solutions.

Key Recovery Service Provider supports enterprise solutions

Key Recovery Service Provider is a plug-in module for KeyWorks that creates key recovery blocks. Encrypted information can be recovered without escrowing private keys or parts of any key with a third party. Use of this module with KeyWorks and key recovery services allows you to produce solutions that support enterprise or individual policies for key recovery.You can provide secure solutions that implement strong encryption and still effectively manage your corporate data by allowing cryptographic backup and recovery of encrypted information when keys may be unavailable.

IBM KeyWorks Toolkit for AIX at a glance

Hardware requirements	• 4.2x or 4.3.2 operating system • At least 32MB of memory (RAM) • 50MB available disk space
Software requirements	• AIX Version 4.2 or higher • AIX x1C compiler

IBM KeyWorks Toolkit for Windows 95, Windows 98 and Windows NT at a glance

Hardware requirements	• At least 16MB of memory (RAM) • 45MB available disk space on a long filename partition
Software requirements	• Microsoft Windows NT 4.0 with SP3 • Microsoft Windows 95 or Windows NT with TCP/IP (recommended) • Microsoft Visual C++, Version 4.2 • Microsoft Visual C++ Runtime Library, Version 4.2

IBM KeyWorks Toolkit for OS/390 at a glance

	• IBM KeyWorks Toolkit has been designed to run under the UNIX® service environment and requires OS/390 Version 2, Release 7 (hardware and software) to operate

IBM KeyWorks Toolkit for Sun Solaris, Version 2.6 at a glance

Hardware requirements	• Sun Solaris 2.7 operating system • SunSparc workstation
Software requirements	• Sun Visual Workshop 4.2 with 5.0 compiler

Key Recovery Server helps recover encrypted information

In addition to KeyWorks Toolkit and Key Recovery Service Provider, IBM offers Key Recovery Server to assist in recovering encrypted information for which key recovery blocks were generated by KeyWorks-enabled application and middleware runtimes. Key Recovery Server is an application built on the KeyWorks framework, which has a well-defined GUI and communications interface. Key Recovery Server is available for separate purchase from IBM under several programs.

Part of the total IBM integrated security solution

IBM KeyWorks Toolkit and IBM Key Recovery Service Provider are components of IBM SecureWay FirstSecure toolbox, delivering comprehensive security solutions that enable e-business. KeyWorks Toolkit and Key Recovery Service Provider can be purchased separately or as part of SecureWay FirstSecure. You may also work with one of our qualified original equipment manufacturers or solution providers to gain the advantages of KeyWorks and its standards-based approach to cryptographic and trust services.

For more information

To learn more about KeyWorks Toolkit and Key Recovery Service Provider, visit the Web site at:

www.ibm.com/security/cryptoproducts

For more information about IBM SecureWay integrated security solutions, visit the IBM Security Web site at:

www.ibm.com/software/secureway

IBM Corporation
Department VK4A
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in the United States of America
4-99
All Rights Reserved

Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.

For Position Only

G325-3886-00