Simplifying management of digital certificates for trusted e-business

IBM SecureWay Trust Authority

Highlights

Provides secure authentication for all parties involved in e-business transactions

Handles digital certificates for multiple uses, such as e-commerce or identification of remote employees

Uses digital signing to ensure confidence that transferred data has not been altered

Offers the scalability needed for your growing e-business

Uses a virtual smart card interface to ease migration to smart cards

Simplifies administration of digital certificates within large organizations and across organizational boundaries

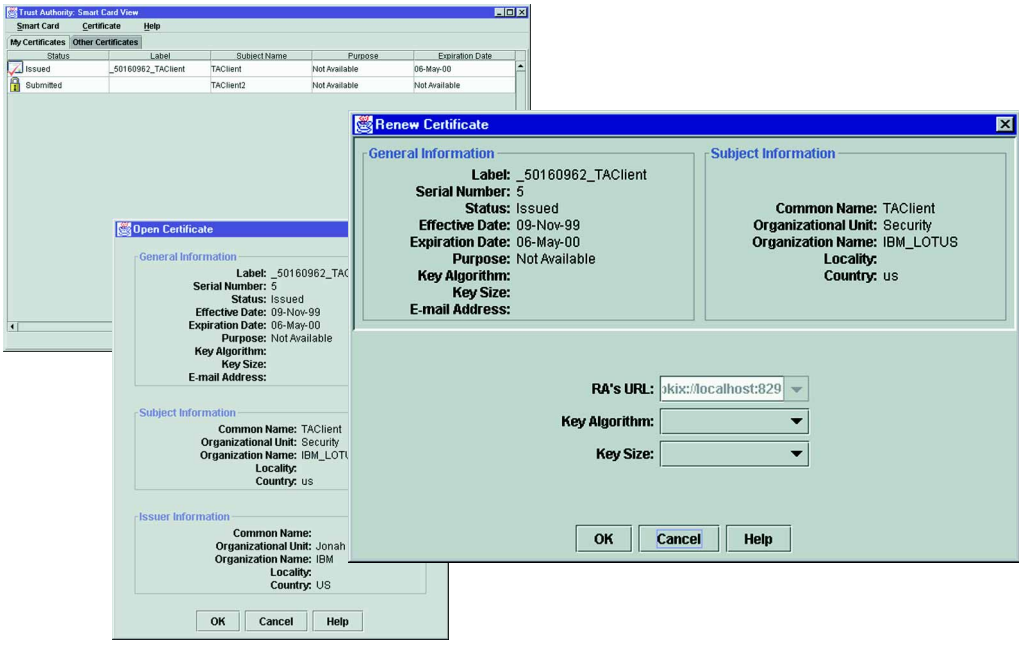
Automates the registration process to speed digital certificate administration

Helps you to build the levels of trust appropriate for your business needs into the registration process

Integrates authentication with access control through SecureWay Policy Director or user-defined extensions to your digital certificates

Build trust into e-business

Trust. It's one of the most critical elements required to conduct successful e-business. In dealing with someone face to face, it's not that difficult to establish a high level of trust. But when the people you're conducting business with are virtually invisible, there is a critical need to establish a trustworthy method for assuring identity of users, authenticity of data and privacy. It's also important to protect against tampering and unauthorized interceptions and to have an audit trail of all your transactions.



The SecureWay Trust Authority client makes it easy for users to obtain and manage digital certificates.

e-business

Conducting e-business across boundaries without compromising privacy and security

IBM SecureWay® Trust Authority enables you to establish security and trust in your business communications according to your needs—based on the policies you have established for your e-commerce transactions. Digital certificates—or electronic identities—are the preferred means for authentication and access control over unsecured networks, such as the Internet. The registration and certification process determines the degree of trust in the certificates. With Trust Authority, you can use digital certificates to identify and authenticate your e-business users and tailor the automatic registration process according to the level of trust you need.

Trust Authority infuses trust into the extended enterprise by allowing e-business transactions to travel across organizational boundaries without compromising privacy, security or confidence.

A flexible, easy-to-use PKI solution

SecureWay Trust Authority is an easy-to-use, multiplatform public key infrastructure (PKI) solution for handling electronic registrations and certifications. Because Trust Authority is based on PKI, you can enable applications to use certificates to grant access, maintain transaction privacy, protect data integrity, provide authentications and reduce the risk of repudiation. Trust Authority helps you register customers, employees and authorized users, and it integrates with your existing databases to support automatic verification of registration data—all in accordance with your established registration and certifications policies.

To promote vendor interoperability, Trust Authority supports several open industry standards, including Secure Sockets Layer, Version 2 and Version 3 (SSL), IPsec, S/MIME, Lightweight Directory Access Protocol (LDAP), PKI for X.509, Version 3 (PKIX) and Common Data Security Architecture (CDSA). Trust Authority provides browser- and client-based registration capabilities for maximum flexibility. Trust Authority has advanced features that support hierarchies and cross-certification at any level.

Trust Authority components

Trust Authority focuses on simple installation and includes a directory, database, Web server, certificate authority and registration application. Trust Authority uses IBM SecureWay KeyWorks for cryptographic and key store functions.

Registration facility

Trust Authority registration facility (RF) handles the administrative tasks behind user registration, supporting both browser- and client-based requests. The RF ensures that only certificates that support business activities are issued, and that they are issued only to authorized users. Administration can be handled through automated processes, or users can handle administration manually.

Certificate management system
A trusted certificate authority (CA) manages the complete life cycle of digital certification. Cryptographic hardware, such as IBM SecureWay 4758 PCI Cryptographic Coprocessor, can be used to protect the CA's signing key.

Trust Authority client
The Trust Authority client, a Windows® application, allows users to obtain and manage certificates without using a Web browser. A virtual smart card is included to simplify migration to the use of real smart cards.

Administration interface
A Web-based administration interface, the RA desktop enables authorized registrars to approve or reject enrollment requests and administer certificates after they have been issued.

Audit subsystem
An audit subsystem computes a message authentication code (MAC) for each audit record. If audit data is altered or deleted after it has been written to the database, the MAC can detect the intrusion.

WebSphere Application Server
IBM WebSphere® Application Server combines the control and portability of server-side business applications with the performance and manageability of the Enterprise JavaBeans™ model. It offers a comprehensive, Java™-based Web application platform that supports deployment of e-business applications and components, including JavaBeans™, Java servlets, JavaServer™ Pages and Enterprise JavaBeans applications for transactions, enterprise system access and dynamic Web content. From design to development to deployment, Application Server Advanced Edition helps you build Web sites capable of handling your most advanced e-business applications. It supports medium- to high-level transactional environments and runs on Microsoft® Windows NT®, IBM AIX® and Sun Solaris™ operating environments.

DB2 Universal Database
As the foundation for e-business, IBM DB2® Universal Database™ is the industry's first multimedia, Web-ready relational database management system strong enough to meet the demands of large corporations and flexible enough to serve medium-sized and small businesses. DB2 Universal Database combines power for business intelligence (data warehousing and data mining) with industry-leading performance and reliability to drive the most demanding industry solutions. Industry-leading application vendors like SAP, PeopleSoft and Siebel Systems support DB2® in a wide variety of applications from ERP to Supply Chain Management to Customer Relationship Management.

SecureWay Directory
IBM SecureWay Directory provides a common directory for customers to address the proliferation of application-specific directories, a major driver of high costs. IBM SecureWay Directory is a LDAP cross-platform, high-performance, robust directory server for security and e-business solutions. The SecureWay Directory can support millions of entries to provide one of the most scalable PKI solutions available today.

Extending security with S/MIME and VPN support

Trust Authority extends the reach of your business applications with the added support of Secure Multipurpose Internet Mail Extensions (S/MIME), a specification for electronic messaging, and virtual private networks (VPNs), a technology that supports tunneling protocols for encrypting data transported over the Internet.

With Trust Authority, you can easily integrate e-mail and messaging products that implement S/MIME. Trust Authority also allows you to register and issue certificates for VPNs, providing your business with a framework for converting a public network into a VPN.

Integration with Policy Director

To fully integrate your registration and certification processes with your e-business functions, Trust Authority-issued certificates are used by IBM SecureWay Policy Director, the central control point for IBM SecureWay FirstSecure components. With Policy Director, you can unite your core security technologies around common security policies—reducing total cost of ownership and the likelihood of security breaches.

Trust Authority is one of the primary offerings that is part of IBM SecureWay FirstSecure, an integrated, policy-driven security solution built on open industry standards.

Open for trusted e-business with SecureWay FirstSecure

IBM SecureWay FirstSecure enables companies to build and operate secure and trusted environments to conduct e-business. FirstSecure offers an integrated, policy-driven solution for your IT security needs, including digital identities, network boundary protection, detection of viruses and intrusions, and tools for developing secure applications. Trust Authority can be purchased separately or as a component of FirstSecure.

For more information

For more information about Trust Authority, visit:
www.ibm.com/software/security/trust

To learn more about IBM SecureWay FirstSecure, visit:
www.ibm.com/software/security/firstsecure

Standards for Trust Authority

Component	*Digest and MAC (message authentication code) Algorithms used*	*Signing/Verification Algorithm, Length*	*Symmetric encryption Algorithm, Length*
Audit	SHA-1, HMAC (SHA-1)	RSA	None
RA server	SHA-1, MD2, MD5, HMAC (MD5)	RSA	DES-56, 128
Enrollment servlets	None	None	DES-56
Approval servlets	HMAC (MD5)	None	DES-56
CA	SHA-1, MD2, MD5, HMAC (SHA-1)	RSA	None
Certificate validation	SHA-1, MD2, MD5	RSA	None
Startup	None	None	3DES-128 (passwords only)
KeyStore	None	None	3DES-128 (keys only)
Install/configuration	None	None	

Trust Authority at a glance

IBM SecureWay Trust Authority, Version 3.1 can be installed on:

- IBM RS/6000® systems with IBM AIX, Version 4.3.2
- Intel®-based systems with Microsoft Windows NT 4.0 (with Service Pack 5)

IBM SecureWay Trust Authority, Version 3.1 also requires the following prerequisite products, which are included in Trust Authority:

- IBM SecureWay Directory, Version 3.1.1.
- IBM DB2, Version 5.2 Fix Pack 10 (Enterprise Edition)
- IBM WebSphere Application Server, Version 2.02 Standard Edition including IBM HTTP Web Server, Version 1.3.3. and JDK, Version 1.1.6

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

Produced in the United States of America
10-99

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

G325-3934-00