RSA® Digital Certificate Solution

Create and strengthen layered security

Trust is a vital component of modern computing, whether it is between users, devices or applications in today's organizations, strong public key authenticators in the form of digital certificates provide an excellent solution to validate the integrity and mutual identification of these elements. Certificates also provide the means to activate a strong cryptographic layer in many applications including secure E-mail, VPN and strong two-factor authentication.

The RSA Digital Certificate solution ensures the security and scalability of transactions by providing a flexible, scalable system for managing digital identities. Establishing the trust carried by certificates and managing the use of keys and certificates is critical to the proper deployment and maintenance of e-business applications.

The RSA Digital Certificate solution offers interoperable modules that allow organizations to better develop, deploy and scale secure applications and business services by automating and centralizing the management of cryptographic keys and digital certificates. Working off of the secure RSA Certificate Manager core, the complete Digital Certificate solution consists of four fully integrated products combined to provide a single, seamless system to solve a variety of business needs.

Interoperable modules for managing digital certificates offer a single, seamless system to solve a variety of business needs.

RSA Certificate Manager

RSA Certificate Manager is a digital-certificate-management system that enables organizations to develop, deploy, and scale secure applications and online services. RSA Certificate Manager helps manage digital identities and automate and centralize the management of cryptographic keys and digital certificates.

RSA Certificate Manager offers several key benefits:

- **Enhanced security.** RSA Certificate Manager is Common Criteria EAL4+ certified, the highest ranking ever achieved for commercial certificate-manager software. It is also built to fully support industry-standard certificate revocation lists (CRLs) formats to ensure revoked certificates are not deemed valid.

- **Scalability.** RSA Certificate Manager offers a streamlined user-enrollment process and has been independently tested to scale to more than eight million users, supporting massive demand for certificate signing operations, PKI queries, and large-scale certificate storage and management.

- **Interoperability.** RSA Certificate Manager offers support for multiple industry standards and is interoperable with more than 200 applications, including e-mail applications and directories.

- **Ease of deployment and administration.** RSA Certificate Manager provides local and remote web-based administration and a tight integration with Microsoft® Outlook® to simplify deployment.

Data Sheet

RSA Registration Manager

RSA Registration Manager streamlines the enrollment process for handling large volumes of end-user certificate requests by verifying the credentials of certificate requests and providing certificates to the requester.
RSA Registration Manager enables organizations to set up remote or local standalone enrollment centers for large user implementations at distributed geographic locations, thereby allowing organizations to scale their certificate management systems while moving the approval process closer to the users. This process significantly reduces the risk of approving certificates to unauthorized parties.

RSA Registration Manager offers the following key benefits:

- **Scalability**. RSA Registration Manager is scalable across multiple registration authorities (RAs) and supports the distribution of many RAs to provide easy deployment of certificates to hundreds or thousands of employees, partners, customers, systems, and devices.

- **Enhanced security**. RSA Registration Manager is a highly secure enrollment system that authenticates administrators using certificates and, if required, smart cards. It is designed for secure web-based administration and approval via authenticated, access-controlled SSL sessions.

- **Flexible enrollment**. RSA Registration Manager was designed to streamline enrollment by supporting high volumes of requests for certificates and is flexible to work within any trust model.

Set up remote or local standalone enrollment centers for large user implementations at distributed geographic locations.

RSA Validation Solution

RSA Validation solution enables immediate validation of digital certificates to ensure the integrity of electronic communications and transactions for organizations and government agencies.

RSA Validation offers several key benefits:

- **Enhanced security**. RSA Validation is a far more efficient and reliable method for checking the status of certificates than Certificate Revocation Lists (CRLs) by providing real-time certificate status checking. This minimizes the risk of revoked certificates being deemed valid.

- **Addresses enterprise certificate validation management requirements**. RSA Validation offers a highly scalable, industry-standards-based solution for validating digital certificates to meet the needs of today's demanding online environment.

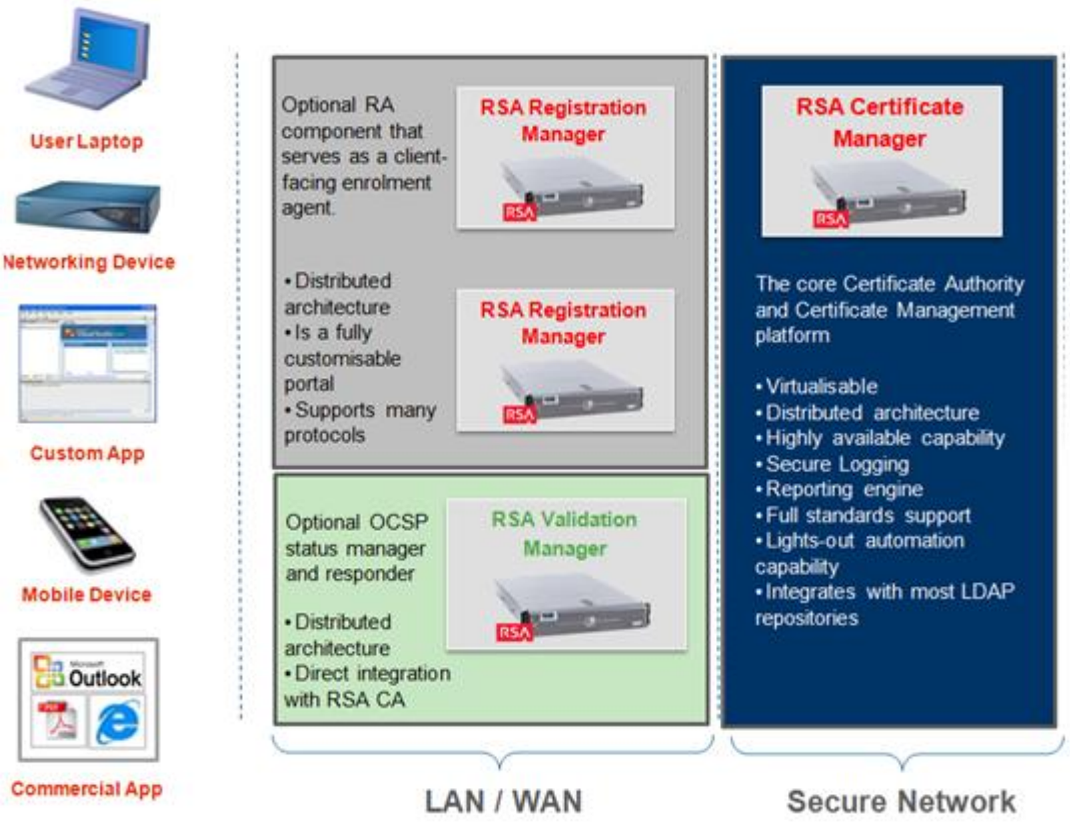
- **Seamless integration**. The RSA Validation Client enables seamlessly integrated real-time status-checking capabilities for Microsoft and other third-party applications using MS CAPI such as e-mail clients, web browsers, and web servers.

- **High reliability, availability, and performance**. The RSA Validation Solution can support multiple certificate authorities and millions of users and offers accelerated performance with FIPS Level 3-certified Hardware Security Modules (HSMs).

RSA Key Recovery Manager

RSA Key Recovery Manager securely archives and recovers users' encryption keys to reduce the risk of data loss in the event an encryption key is lost, misplaced, or corrupted. RSA Key Recovery Manager is offered as an optional package as part o RSA Certificate Manager. RSA Key Recovery Manager features a hardware-based key-generation process handled through a hardware security module, offering a more secure key-generation technique than software-based generation. HSMs provide secure management of private keys in that the keys never leave the module unencrypted; they are in dedicated hardware while in use and encrypted with triple DES (Digital Encryption Standard) when idle. The use of an integrated HSM enables RSA Key Recovery Manager to deliver the highest standard for security and data integrity while providing key recovery services. RSA Key Recovery Manager also helps organizations address various storage requirements based on their varying regulatory needs and is completely configurable to meet different storage-period requirements. Private encryption keys are kept strongly encrypted in secure storage on the hardware security module so that even compromises to the server's operating system will not jeopardize the security of the key database.

An Overview of the RSA Digital Certificate Solution Components


User Laptop
Networking Device
Custom App
Mobile Device
Outlook
Commercial App
Optional RA component that serves as a client-facing enrolment agent.
RSA Registration Manager
• Distributed architecture
• Is a fully customisable portal
• Supports many protocols
RSA Registration Manager
Optional OCSP status manager and responder
• Distributed architecture
• Direct integration with RSA CA
RSA Validation Manager
RSA Certificate Manager
The core Certificate Authority and Certificate Management platform
• Virtualisable
• Distributed architecture
• Highly available capability
• Secure Logging
• Reporting engine
• Full standards support
• Lights-out automation capability
• Integrates with most LDAP repositories
LAN / WAN
Secure Network

Technical Specifications

Platform	Solaris (Sparc), Linux, Windows and VMware
Server Operating System	Windows 2003 R2 Service Pack 2 Windows 2003 Service Pack 2 Windows 2008 32 bit Service Pack 1 Windows 2008 R2 64 bit Service Pack 1 Sun SolarisTM 10 Red Hat Enterprise Linux 5.5 32 bit Red Hat Enterprise Linux 5.5 64 bit SUSE Linux Enterprise Server 11 SP1 32 bit SUSE Linux Enterprise Server 11 SP1 64 bit VMware ESX Server 4.1
Server Memory Requirement	Windows: 1 GB RAM Minimum Solaris: 512 RAM Minimum Linux: 512 MB RAM Minimum
Server Disk Requirement	Windows NT: 250 MB Minimum Solaris: 250 MB Minimum Linux: 250 MB Minimum
Server CPU Speed	Windows NT: Intel Pentium IV 2.66 GHz or better Solaris: Sparcv9 1280MHz or better Linux: Intel Pentium IV 2.66 GHz or better
Certificate Standards	X.509 v3 (including all standard extensions) - PKIX - SSL - S/MIME - IPSec - SET - Extended Validation
Industry Certifications:	Common Criteria EAL4+, Federal Bridge CA (FBCA), and IdenTrust Certification
Directory Features	Includes integrated LDAP certificate repository Publishes to LDAP v2/v3 and X.500 Directories Seamless S/MIME certificate lookup via LDAP/SSL-LDAP Certificate status checking via SSL-LDAP SSL-LDAP between all PKI components
PKI Features	X.509 CRLs and CRLs with extensions Unlimited sub-CA certificate chaining (hierarchical PKIs)
Certificate Features	X.509 v1, v3 certificates RSA, DSA and ECDSA certificates Up to 4096-bit keys for authentication Flexible DN configuration for certificates S/MIME certificates Object signing (Java, ActiveX) certificates PKIX v3 extensions SET extensions Firefox and Microsoft Internet Explorer Certificates
Cryptographic Support	RSA DSA P-256, P-384, and P-521 ECDSA SHA-1 and SHA-2
Encryption Hardware	Storage of CA private keys on Hardware Security Module (HSM) and Hardware-based CA key cloning/archiving with PKCS #11 devices. FIPS 140-1 level 1 through 3 key security (via SafeNet, Thales, AEP and/or other PKCS#11 devices)

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.