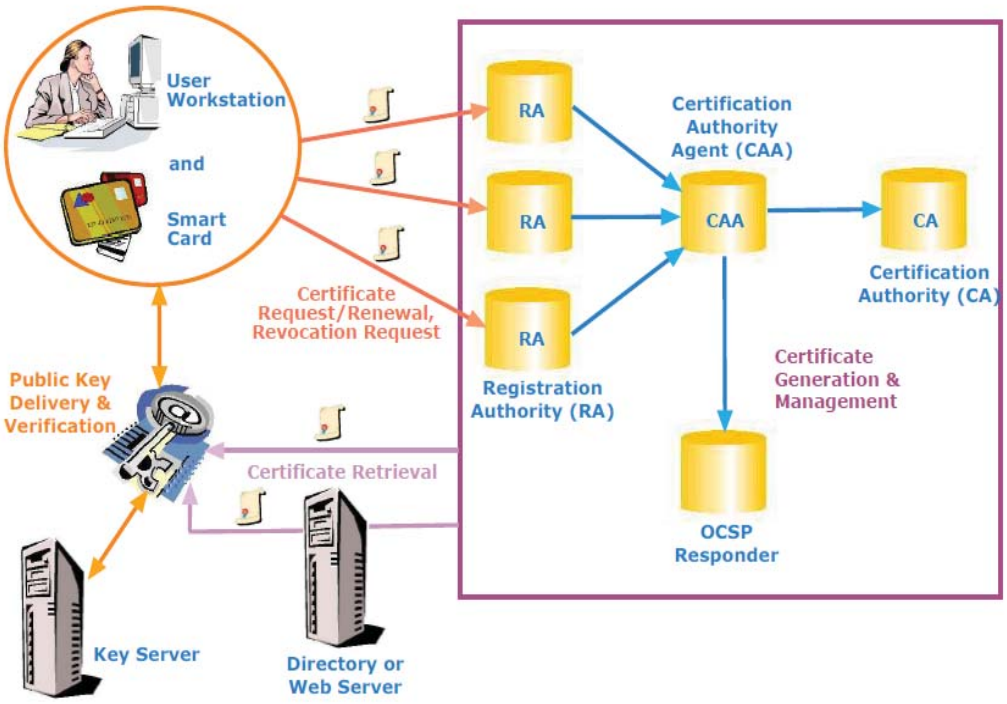
SecureAge

SA PKI

Internet has become an essential business tool for all organizations to conduct electronic communications and transactions internally as well as externally with their business affiliates, vendors and customers. But how can you make sure that all these communications and transactions are carried out securely? What can you do to ensure the confidentiality, integrity and non-repudiation of these communications and transactions? Your most trusted solution for resolving this is SA PKI which provides a highly reliable environment for protecting the confidentiality of communications, validating the user's identity via digital signature, verifying the data integrity and ensuring non-repudiation of electronic transactions. It has the technology capability to meet even the most demanding security environments required by banking, government and other electronic commerce (e-commerce) enterprises. On top of that, our SecureAge solution is able to comple ment SA PKI to further optimize the security strength that can best meet your business objectives.

Product Description

SA PKI is a Public Key Infrastructure System that follows the PKIX (Public Key Infrastructure X.509) standards proposed by Internet Engineering Task Force (IETF). It is the state-of-the-art Certificate Authority System that provides SSL (Secure Sockets Layer) and S/MIME enabled digital certification for establishing trustworthy identities and management services to administer the related encryption and signature keys for any security-enabled system used by e-businesses and enterprises. Since all the public key cryptography enabled security systems need a public key infrastructure, SA PKI serves as the foundation for any security-enabled systems used by technology savvy enterprises to safeguard the integrity and privacy of information exchanged over the Internet. This secures all online transactions by authenticating the users' iden tity, thereby enhancing their trust and confidence when engaging electronic commerce over the Internet.



SA PKI is made up of three components: Certificate Authority (CA), Registration Authority (RA) and Certification Authority Agent (CAA). In essence, all these components work interdependently whereby the CA controls all CA signing operations and handles all certificate and revocation requests from RA and CAA. RA basically handles all certificate issuing and new CA registration. SA CAA, on the other hand, acts as the security agent that controls new CA registration, profile creation, user account management, administration functions and granting of privileges to other modules and operators.

SA PKI fully supports X.509 Certificate Revocation Lists (CRLs). Once the related private key has been exposed, certificates will be revoked and listed in the CRLs which will then be published by CA. Alternatively, the validity of these certificates can be checked online using the OCSP support provided by SA PKI.

SA PKI also supports the Directory or Web Server which is a central repository of certificates and public keys made available for public accessing. It provides centralized, automated management of digital certificates which can be readily integrated into your existing applications. It also allows the developers to embed certificate creation and management in their solutions thereby offering innovative digital signature and encryption capabilities without having to buy additional PKI software. Administrators can manage user and security policy settings centrally, including standardized certificate revocation list checking and integrated management of multiple RAs. This ensures consistent certificate policies when multiple departments each host their own RA.

Key Server, another component of SA PKI, provides a safe way to store user private key as encrypted data package so that users can access proprietary corporate information from anywhere. It therefore saves you the trouble of having to copy user private key from one machine to another and the users will have the convenience of full access to PKI applica tions without having to carry the private keys with them.

Key Features

Compliance with certificate management standards of IETF PKIX.

Supports online web based certificate registration.

Full support for X.509 v3 certificate format.

Support SSL, S/MIME, SET certificates.

Full support for X.509 CRL based certificate revocation.

Provides OCSP support.

Automatic publication of certificates to LDAP Server and Microsoft Active Directory.

GUI based X.509 v3 certificate profile creation.

Full-strength cryptographic algorithms. Supports RSA (1024/2048/4096-bit), MD5/SHA-1.

Multi-level access control mechanisms.

Full audit log.

Support multiple CAs in a single installation .

Support PKCS #1, #5, #7, #8, #9, #10, #11, #12.

Support Hardware Security Module (HSM).

Java based multi-platform support.

Support RSA 1024/2048-bit smart card and USB token.

Full strength Secure Socket Layers (SSL) communication protection among all modules.

Certificate based authentication for both client and server to protect communication among CA, CAA and RA.

Provides Key Server support for roaming access.

Fully integrated with SecureAge software.

SecureAge Technology Pte Ltd
20 Ayer Rajah Crescent #09-13
Technopreneur Centre Singapore 139964
Tel: (65) 6873 3710 Fax: (65) 6234 4992
URL: http://www.secureage.com
Email: contactus@secureage.com

SecureAge