What To Look For in a CA: A Buyer's Guide

CyberGuard Corporation
2000 West Commercial Boulevard, Suite 200
Fort Lauderdale, Florida 33309
954.958.3900, 800.666.4273

It should not be any secret that the certification authority described in this buyer's guide is TradeWave's TradeAuthority CA. TradeAuthority meets every qualification for a total-solution, standards-based, easy-to-manage, industry-standard CA. In fact, TradeAuthority exceeds industry standards of today. But as the industry begins to understand its security needs, the TradeAuthority CA will define the evolving standards.

Introduction

If you are investigating the security requirements for public-key security technology, you know that you need a trusted third party known as the certification authority (CA). The CA distributes the electronic keys used to encrypt and decrypt user and server information and also distributes the electronic certificates used to authenticate user and server identities. Whether you contract with an outside vendor for CA services or purchase the products required to operate your own CA, you'll want to ensure that the CA can meet your needs.

In general, a CA should provide:

- **Comprehensive key management**, including issuing keys, updating keys, backing up and recovering keys, revoking and reissuing keys, and disabling and reenabling keys.

- **A standards-based architecture**, including support for X.509 certificate standards and X.500 directory standards, which include the Lightweight Directory Access Protocol (LDAP) for access to the public-key directory.

- **The strongest, most reliable system implementation and operation**, as proven by accreditation by the FIPS PUB 140-1 standard for secure, unclassified communications over the Internet.

- **A redundant site for the certificate directory service** and professional support by established experts in security.

- **Complete and detailed policies and procedures** that provide for the human aspects of CA services, such as who administers those services, who operates the CA site, and how these tasks are performed.

To choose a CA, follow the same methodology you would use to make any security decision: understand your requirements and assess the risk. The following checklist can guide your evaluation and selection process.

Key Management and Administration

Is a local registration agent (LRA) model employed?

In an LRA model, the CA handles certificate administration and the enterprise retains control over who is allowed to receive certificates. This frees the enterprise from the administrative overhead while it maintains local control over security.

Is there centralized support for encryption key management?

Managing keys is more than just issuing them. Keys also need to be updated, backed up, recovered, revoked, reissued, disabled, and reenabled. When these tasks are handled centrally, they can be implemented more quickly and more securely. For example, some systems require that the directory of public keys be maintained at the user or application level. This creates unnecessary overhead and might even involve manual delivery of the directories to the workstation.

Also, central key management helps maintain system integrity over time; there is less degradation due to employee turnover or business mergers that affect the list of authorized users. New names are added and the names of unauthorized users are deleted from the central list.

Does the CA's software comply with the Federal Information Processing Standards Publication (FIPS PUB) 140-1 standard?

The FIPS PUB 140-1 standard defines requirements for products used to protect sensitive information. By June 1997, government agencies will only be allowed to purchase products that have been validated to FIPS PUB 140-1. The Canadian government is also adopting FIPS PUB 140-1. This validation indicates the strength of the CA-related software.

Is a scalable key management system provided?

While you might initially need CA support for only several hundred users, you want CA services that can grow to meet your requirements, from hundreds to tens of thousands of users and beyond.

Does the CA support separate key pairs for encryption and digital signatures?

Using a pair of keys for encryption that is separate from the pair used for digital signatures enables the CA to keep a backup of the encryption key pair and thus to recover those keys as necessary. At the same time, this procedure minimizes the risk of possible electronic forgery. To forge a document requires gaining possession of the signing pair used for signatures. If this pair and the encryption key pair are the same pair, and if the backup of the encryption pair is compromised, forgery is possible. If the pairs are separate, and the backup is compromised, forgery is not possible because the backup does not include the signing pair.

Is a standards-based directory service available for providing public keys, certificates, and timely certificate revocation information?

To facilitate access to the public keys, a standards-based access method should be supported, such as the Lightweight Directory Access Protocol (LDAP).

Is any additional information provided as part of the directory service?

A basic directory service provides, at least, the public keys and certificates for valid users. However, a directory service can provide other information that users might find helpful. This additional information is made available based on company policy.

Are X.509 v3 certificates supported?

The X.509 v3 standard provides for additional information to be conveyed as part of the certificate. For example, the certificate might include the person's email address and a Web address. By supporting X.509 v3, a CA can provide you with more flexible services and greater support.

Is cross-certification supported? Does cross-certification comply with PKIX?

Cross-certification is the ability of one CA to validate certificates issued by another CA. Currently, cross-certification is only possible by CAs that use the same technology. However, there is an IETF (Internet Engineering Task Force) working-group effort to build industry consensus on how CAs with differing technology should cross-certify. This effort is known as PKIX (for X.509-based public-key infrastructure). If a CA supports PKIX, the CA will be able to cross-certify with a greater number of other CAs, including those located at other companies.

Can keys and certificates be obtained: (a) online, (b) securely, and (c) transparently both for initial registration and for updates?

Online support for key management provides for fast and simple registration. Users should be able to fill out and submit online forms so time isn't lost trying to find the correct paper document, get it signed, and figure out who to send it to. Approval of the request and issuance of the keys and certificate should also be done online to speed the process.

All online key management--registration requests, revocation, and the distribution of keys and certificates--should be fully encrypted and authenticated. It should also be transparent to the user so that the user isn't interrupted and doesn't have to perform additional tasks.

Can key updates be forced--according to company policy--securely and transparently?

For certain positions, overall risk can be reduced by setting policies that govern how often keys and certificates must be updated (that is, how often a new key must be obtained to replace the current key). For example, because your purchasing agents can perform monetary transactions, you might want to force an update of their keys and certificates on a monthly basis. These updates should be performed automatically based on your policy and be transparent to the user.

Are secure key backup and recovery supported?

In the event that a user's key information is accidentally deleted or the user forgets his or her password, you should be able to recover the keys. This requires that the keys be backed up, which should be done securely.

Are keys and certificates time-stamped and archived so that digital signatures can be verified over the long term?

If the CA maintains a time-stamped history of keys and certificates, you can verify documents that have been signed and encrypted in the past.

Is revocation supported? Is that support online and centralized? Is CRL v2 supported?

You might need to revoke security privileges for a user when the user leaves the company or the user's private key or certificate is suspected of being compromised. Revocation needs to be easy to perform and absolute.

Centralization can reduce the time involved in revoking the certificate. Most CAs perform revocation through the use of a certification revocation list (CRL). Administrators place certificates that are revoked on the CRL. No user whose certificate is on the CRL should be able to access secure resources.

Some CAs, however, support only manual revocation; that is, an administrator or service must manually check the CRL to determine if a certificate is valid. If they don't check the CRL, they might unknowingly accept a certificate that has been revoked. Much tighter security is maintained if checking the CRL is performed automatically at preset intervals. In addition, automatic checking of the CRL is faster than manually checking it.

Also, if the CA supports the CRL v2 (the second version of the standard governing CRLs), you are assured the CA is implementing the current standard.

Is disabling and reenabling supported? Is that support centralized?

In some cases, you need to be able to immediately curtail use of a user's security credentials, such as when a security breach is suspected. Disabling, as compared to revocation, immediately prevents use of the security credentials. (Revocation takes place the first time a user or service checks the CRL after the certificate has been placed on the list.)

CA Security and Administration

Does the CA provide a redundant site for the certificate-directory service?

Reliability is increased by providing a redundant site for all certificate-directory services.

How secure is the CA's operation?

Any breach of the CA compromises your enterprise, so it is important that the CA implements stringent host, network, and physical site security. The CA should also employ vigorous security policies, procedures, and auditing controls.

Are the CA's security measures certified by an independent third party that performs a risk analysis?

Periodic risk assessments by an independent third party validate the security of the CA's environment and operations.

Is CA operation role-based?

For example, is the task of setting security policies handled by a person who is different from the one who administers keys and certificates? Role-based operation increases security by providing a check-and-balance situation that reduces the potential for internal compromise.

Does the CA maintain secure audit records of security-relevant events?

A secure audit trail is integral to reducing the risk of compromise and also helps contain any damage should there be a security breach.

Support Services

What level of support is provided? Is that support scalable to prevent bottlenecks?

When you have a problem that requires CA support, you often can't afford to wait hours, much less overnight, to get help. A CA's support operations should be available when you need it, down to the level that you need it.

Is there an online backup so that the CA is always available?

Even if the CA server goes down, you still need a way to validate certificates and obtain public keys. A CA should provide for the ongoing availability of these services.

Other Considerations

Does the CA provide complete and detailed policies and procedures?

Technology alone does not ensure security. Traditional controls--proper documentation of policies, procedures, standards, and guidelines; technical education; security awareness; and management approval--are still important. How well a CA documents and implements these operational controls greatly affects the security of its services.

Is the implementation and use of the CA services easy and seamless?

Do you need to obtain your certificates from one vendor and the software that uses the certificates from another vendor? If so, who provides the support to ensure that the two work together? Is the integration seamless or are extra, even manual, steps required of the user?

Are CA services available as a part of a total security solution?

Some vendors offer only CA services; you must deal with other vendors for the other parts required for a secure system, including the software to perform the actual encryption and decryption, authentication, and access control. In general, CA services that are provided as part of a comprehensive security solution are more fully integrated, so the system is easier to use and requires less set up and administration.

Does the CA have a Certification Practice Statement to meet the requirements of pending legislation for accreditation of CAs?

Legislation is pending in many states that provides for the accreditation of CAs. In some states this accreditation will be a legal requirement. To apply for accreditation, the CA publishes a Certification Practice Statement (CPS) that details the responsibilities and operations of the CA and controls the provision and use of the CA's services.

You can be assured you are dealing with a legitimate CA if it is publishing a CPS by which to apply for state accreditation.