Building a public key infrastructure - in-source or out-source?

by Dr. Tim Moses
Manager, Security Technology Group

Introduction

A public key infrastructure will become a critical weapon in every organization's armory in the fight to drive down information processing costs, and improve operational performance, by removing steps from its information processing chains and by eliminating wasteful duplication of data entry (rekeying). Automated information systems replace traditional business controls, and, unless implemented with care, they can increase the organization's exposure to loss due to errors and malicious actions by both insiders and outsiders. While these are serious concerns, mature product solutions do exist to address them. And, if operated with adequate administrative controls, these solutions can surpass the level of assurance provided by traditional business controls, without threatening the cost-savings and performance improvements expected from the use of automation. A public key infrastructure will be an essential part of any such solution.

Two main approaches exist for obtaining suitable infrastructure services: the necessary capital equipment can be procured and operated by the IT unit within the organization (in-sourcing), or services can be purchased from a public service provider (out-sourcing). In making this choice, a number of considerations come into play. Naturally, there are economic considerations, but these are relatively easy to deal with; the cost of owning and operating the public key infrastructure can be compared with the subscription cost of the service which is being contemplated. However, the economic aspect of the decision may turn out to be one of the more minor considerations. Other considerations that come into play include: the confidentiality and availability of critical corporate information; control over critical system resources; enforcement of the second party's obligations and the quality of service perceived by customers.

Take as an example a situation in which customers are allowed to enter order information directly into a supplier's order-entry system, thereby eliminating the need for clerks whose function is solely to re-key data that already exists in machine-readable form on

the customers' systems. The cost saving delivered by this shortened information processing chain comes at a price. It may be possible for a competitor to masquerade as a bona fide customer, and thereby insert orders that would be subsequently denied by that customer. It may be possible for a competitor to gain access to sensitive information, and thereby gain a competitive advantage. These issues are discussed in the following section.

Issues to Consider

The following issues should be considered when making the choice between in-sourcing and out-sourcing of a public key infrastructure service.

Confidentiality - The act of issuing a certificate is an assertion by a recognized authority of the privileges held by the subject. These privileges are generally implicit in the certificate and the practices under which it is issued. Alternatively, they may be explicitly coded in a *subjectDirectoryAttribute* extension or in a related attribute certificate. 'Registration' is the name given to the process by which the claimant demonstrates its entitlement to a particular privilege amongst all those recognized within the operating practices of the authority. This 'demonstration' may take several forms, but there are conventional business processes by which an employee's or trading partner's privileges are recognized, and these will have to be integrated with the operation of the public key infrastructure registration function. In cases where the registration function is out-sourced, this integration requires the opening up of those internal privilege management systems to the service provider. This is likely to disclose strategic corporate information about employees and trading partners to the third party. Agreements in place with these employees and trading partners may disallow such disclosure. In addition, a new and unnecessary point of vulnerability must be introduced into the corporate information system.

Availability - Critical corporate information which has been encrypted for long-term storage is vulnerable to loss in the event that the corresponding decryption key becomes lost or corrupted. Therefore, it is essential to ensure that a centrally-controlled method of decryption is available. Having this method under one's direct control provides the necessary assurance that this facility will be available, if and when required, at some point in the indefinite future, and that it will not be misused. In the case of an out-sourced service, documented and rigorously-enforced procedures and independent audits are required to achieve the necessary level of assurance. While it is true that one can seek redress in the courts for any breach that may occur, it is small consolation when the very ability of the organization to continue operating is at stake.

Control - Over time, the corporation's business systems will increasingly come to depend upon the availability and integrity of its public key infrastructure. As more of the corporation's business processes become ported to the paper-less medium, the public key infrastructure will play a more and more central role in the organization's operation. Therefore, there must be absolutely no doubt in its continuing and correct operation. Among the most critical operations for a public key infrastructure are the mechanisms for

revoking privileges, issuing CRLs, distributing CRLs[1] and auditing and archiving the record of the infrastructure's operations. These critical operations are discussed in a subsequent section from the point of view of determining whether in-sourcing or out-sourcing is the appropriate approach in a particular business situation.

Certificate Revocation Lists (CRLs)

A Certificate Revocation List (CRL) is a list of the serial numbers of those current certificates which have been issued by a CA and which have since been revoked. The list is signed by the CA, in order that it can be distributed to certificate verifying systems with integrity and authenticity over an unsecured channel. A certificate may be revoked for one of a number of reasons; most common amongst these are that the corresponding private key has been compromised or that the subject's privileges have been withdrawn, possible as a result of dismissal for cause. Using a CRL allows a relatively long life-time to be assigned to a certificate, in order to minimize the amount of network traffic and processing delay associated with renewing certificates, while acknowldging that privileges may have to be withdrawn unexpectedly.

Liability - In general, the issue of liability does not arise when one operates one's own public key infrastructure and trusts only one's own certificates. There may however be situations in which one elects to trust certificates issued to end-users by one's trading partners. In such cases, a cross-certification agreement is the vehicle by which the assignment of liability can be controlled, in very much the same way that conventional trading partner agreements address this issue.

The fiduciary relationship between the issuer and the subject is material to the enforceability of the certificate (and its implicit privileges) in the case where the CA is discovered to have operated entirely within its operating practices, but due to some fraudulent act on the part of the certificate's subject, the certificate misrepresents the subject's authority to act on behalf of the organization (see the example in the coloured box). In such a situation, if the issuer CA is owned and operated by the organization, then the organization bears a fiduciary responsibility and the certificate may be enforceable against the issuer as well as the certificate holder. If, on the other hand, an out-sourced service is used, then there is no redress against the issuer, as it has committed only to operate within its published practices, and therefore bears no responsibility for fraudulent representations of the certificate holder. So, the only available course of action is against the certificate holder.

If the certification service is out-sourced, then the question of what happens if the service provider withdraws its service, for whatever reason, either due to business failure or due to a change of strategic direction, must be addressed. The corporation can at that point

[1] In a system which provides confidentiality services, the distribution of certificates is also a critical operation. However, if the same mechanism is used for distributing both certificates and CRLs, then the ensuing discussion of CRLs is equally relevant to certificates.

seek a new service provider, but unlike more conventional data processing services, the concerns long outlive the issuance of the original certificate. In the event that a dispute arises far in the future, it may be necessary to locate archive records associated with the issuance of the certificate, and to demonstrate that their integrity has been preserved throughout the intervening period. If this fails, there will be no organization in existence against which redress can be sought.

Quality of service - Where the subject of the certificate is a client or customer of the organization, the quality of the service by which the certificate is issued and subsequently managed reflects directly on that organization. Where the public key infrastructure is operated by the organization itself, the quality of that service is entirely under the organization's own control, and any problem with service quality that endangers the client relationship can be given the immediate attention that it deserves. On the other hand, where the service is out-sourced, direct control is lost. Therefore, it is essential to obtain service quality guarantees and to demand a periodic and independent audit of those guarantees.

Critical Operations

The most critical operations for a public key infrastructure are discussed below.

Registration - Registration is the process of identifying a candidate subject for a certificate and confirming their entitlement to that certificate. The very issuance of a certificate for an individual makes a statement about that individual and his or her privileges within the context of the issuing organization's operating practices. Generally, registration involves reference to sensitive corporate information, and in the case of an out-sourced service, the issuing service must be able to confirm the details of this information. In order to do this, it must have access to sensitive data on the corporation's employees and those of its trading partners.

Privilege Revocation and CRL issuance - A cross-certification agreement is the vehicle by which the assignment of liability between partners is controlled. The issuance of a cross-certificate is the tangible expression of acceptance by one organization of certificates issued by the other organization. A cross-certification agreement should clearly define the apportionment of liability in the event that the assertion represented by a certificate turns out to be false or misleading. Generally, organizations will agree to accept liability if and only if it can be demonstrated that they deviated from the practices documented in their Certification Practice Statement. If they are unable to present credible audit records which demonstrate their adherence to those practices, then liability is likely to be apportioned to them. If they adhered to their practices, but things went wrong nonetheless, then they are likely to be held blameless. This vulnerability is comparable to that commonly assumed in traditional business relationships, so it represents no abnormal liability for the corporation in the case where the service is in-sourced.

Timeliness of CRL issuance is also an issue. In the event that a trusted employee is dismissed for cause, or in the event that he or she is hired by a competitor, it must be possible to revoke their privileges rapidly by integrating the certificate revocation process into the associated human resource procedures. If an out-sourced service is chosen, then there must be adequate and credible guarantees of timely response. Such guarantees are of little consolation if they are discovered not to have worked after the fact.

CRL distribution - CRLs must be distributed with acceptable latency and response times. Low latency is required so that notification of all applicable revocations is made available to verifiers rapidly, and low response time is required so that no unacceptable delays are introduced into the information process. Latency and response guarantees offered by the service provider must be evaluated and audited.

Audit - An audit procedure is required to ensure that the certificate issuer continues to adhere to its published practices. So, before considering the use of a service provider, it should be verified that they have identified an independent audit organization who can be trusted and who publishes, uninfluenced, the results of their periodic audits. Despite the fact that it is their client that is the subject of the audit, the ability of the auditor to act independently must be carefully considered. It may take several consecutive years of stable operation and several issues of the audit report before one can make a complete assessment of the auditor's thoroughness and independence.

Archive - In the event of a dispute, it will be necessary to reconstruct the state of the applicable certificate at various points in the past. Therefore, the required records must be reliably archived. The archive must record all the state changes in the certificate's life-cycle and the identities of those responsible for authorizing each state change. This record must be accessible into the indefinite future. The skills required to do this are no different from those required to operate a corporate distributed information system, but the audit must confirm that archive procedures are properly enforced.

Summary

Because of the criticality of the service associated with a public key infrastructure, the competence of the organization to perform the critical operations correctly should be carefully considered. However, if the organization's IT unit has successfully demonstrated its ability to operate mission-critical systems, such as an accounting, billing or corporate email systems, then the issues encountered in operating a public key infrastructure, in support of inter-organizational business processes, should be familiar and represent no unusual risk.

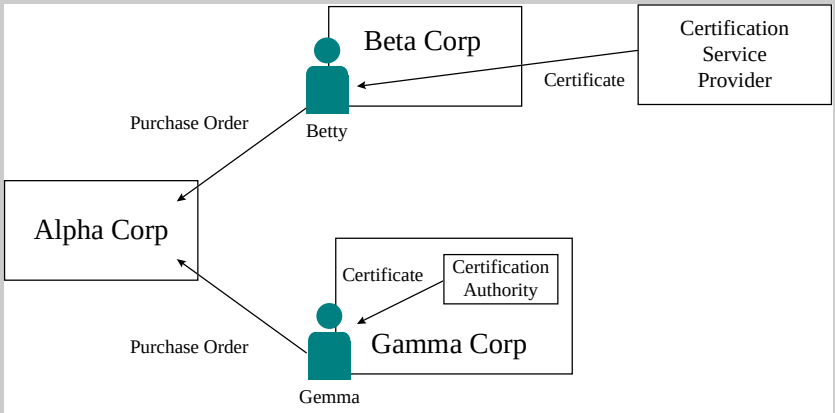
Consequential damage resulting from a failure by the certificate issuing body can far outweigh any direct costs. Therefore, if the certification service is out-sourced, the service provider must be covered by credible insurance for consequential damages, and it must be able to demonstrate that the insurance is continuously in-place. Simply entering into a contract with a provider which places liability on them is not sufficient, because it does not guarantee their ability to assume that liability for consequential damages in the

event of failure. Causing the service provider to go out of business brings no satisfaction when the corporation's critical systems have been compromised.

On the other hand, if a public key infrastructure is required only to support confidentiality, integrity and authenticity services for the organization's own employees, then the considerations are much more relaxed, and there is no reason not to in-source the service.

For further information on suitable products and advice on how to establish a public key infrastructure for your organization, contact Entrust Technologies at **613-765-5607**, or by e-mail at **entrust@entrust.com**.

Example comparing assignment of liability for in-sourced and out-sourced services



Alpha Corp is a supplier to both Beta Corp and Gamma Corp. Beta Corp uses a service provider to issue certificates to its procurement officers, and Gamma Corp runs its own Certification Authority. Betty is an employee of Beta Corp, but she is not a qualified procurement officer. Nonetheless, by presenting fraudulent credentials, she obtains a certificate from the service provider which identifies her as a procurement officer of Beta Corp. Betty uses this certificate to authorize a purchase order on Alpha Corp. The fraud is later discovered and Beta Corp repudiates the purchase order. Note that the sevice provider has acted entirely within its published practices.

Gemma is an employee of Gamma Corp, but she is not a qualified procurement officer either. Nonetheless, by the presentation of fraudulent credentials, Gemma obtains a certificate from Gamma Corp which identifies her as a procurement officer. Like Betty, Gemma uses this certificate to authorize a purchase order on Alpha Corp, and, as in the previous case, the fraud is discovered and Gamma Corp repudiates the purchase order.

In both cases, Alpha Corp incurs costs and seeks redress. Alpha Corp has a case against both Betty and Gemma, but the probability of adequately enforcing these cases is small. It has a stronger case against Gamma Corp than it does against Beta Corp, and it has no case whatsoever against the service provider. Therefore, Alpha Corp is more likely to obtain compensation when there is a fiduciary relationship between the certificate issuer and the certificate holder.