Public-Key Infrastructure Q&A

Public-key infrastructure security has failed to achieve widespread adoption, mostly because enterprises rarely need all of its benefits. Nonetheless, it has value when properly implemented.

What lessons can enterprises learn from Gartner's public-key infrastructure (PKI) case studies?

Gartner research shows that most real-world PKI implementations have been disappointments, and many have been scaled back or abandoned altogether. Nonetheless, some PKI projects show promise. These case studies highlight enterprises' complex experiences with PKI:

- "Kaiser-Permanente's Public-Key Infrastructure Rollout" — Kaiser-Permanente, a major U.S.-based healthcare provider, is using its large-scale PKI for identification, authentication and access control for its clinical information system. A major driver for this project was Kaiser-Permanente's belief — which proved to be unfounded — that PKI would be required by federal healthcare security and privacy laws.

- "State of Illinois Moves Public-Key Infrastructure Forward" — Government officials in Illinois salvaged a stalled project and are driving the use of PKI in state e-government initiatives.

- "Washington State Adopts Common Security Infrastructure" — Many state governments that are struggling with the technical, legal and policy difficulties associated with shared security infrastructure have dropped their PKI projects. The State of Washington has successfully resolved these issues, although the number of PKI users is low.

- "PKI Case Study: Lawrence Livermore National Laboratory" — This national research laboratory is using PKI for secure e-mail and encryption of sensitive files, but it has not yet succeeded in leveraging PKI to other applications.

Other enterprises have derived significant benefits from PKI:
• A pharmaceutical manufacturer is using PKI to protect intellectual property on laptops and desktops as well as in secure e-mail. PKI also is enabling the company to fulfill Food and Drug Administration requirements for digital signatures on regulatory filings.

• A nuclear-waste disposal facility is using PKI — in conjunction with "smart cards" — to track containers more effectively than possible with paper-based systems. Digital signatures are required on the electronic forms that must be filed whenever a container is moved or its condition is evaluated. Thus, audit results are more accurate and radioactive material is less likely to be lost in the system. However, the PKI project has only 200 users, and no other applications are leveraging the PKI investment.

Overall, however, enterprises' experiences with PKI have been negative. For example, a major Canadian bank that was an early adopter of digital certificates for its retail consumers now is essentially discouraging their use. The bank's Web site states that Secure Sockets Layer (SSL) — which uses a server-side digital certificate to encrypt a session — offers more-flexible protection because it enables customers to perform banking transactions from any PC, not just those that hold their digital certificates.

Governments' experiences in implementing PKI also have been revealing. For example, the United Kingdom's Office of the e-Envoy, which drives the development of online technologies, has stated, "To date, and generally in the absence of a PKI, the majority of transactional services requiring a degree of confidentiality have been successfully implemented using SSL technology in conjunction with passwords" (see www.e-envoy.gov.uk/oeo/oeo.nsf/sections/index/$file/index.htm). A study by the General Accounting Office (GAO), the U.S. federal government's budget oversight body, also has identified several obstacles to PKI deployment in government (see "U.S. GAO Raises Red Flags With Federal PKI").

**What are the major inhibitors to PKI adoption?**

Enterprises that implement PKI without first performing an in-depth needs analysis typically find that few of their applications require PKI or PKI cannot be easily integrated with applications that require it. Moreover, PKI can be complex and expensive to implement. Many planners, when they understand that PKI requires user identifications (IDs) and passwords, begin to question the additional benefits offered by digital certificates. Despite the problems associated with user ID/password-based security, it is adequate for many applications, particularly when only identification and authentication are required.
Other key inhibitors to PKI adoption are:

- **Liability and enforceability**: An enterprise-issued certificate that is used improperly can lead to potential legal liability, just as is the case when an employee contracts for products or services without the necessary authority. A related issue is the enforceability of IDs or signatures that are created using certificates. Proof of identity depends to a considerable degree on the quality of the registration process and protection of the private key (which frequently is unprotected or protected only with a password). It is unclear whether a cryptographically applied digital signature is better than an electronic signature — perhaps using password and user ID — if the signing parties’ only goal is to enter into an agreement. Cryptography-based signatures offer other benefits, notably providing message integrity by binding to a hash of the message (a hash is a mathematically generated message digest, or "digital fingerprint"). Any change to the message causes the signature to be invalidated — if it is checked. However, applications do not necessarily check the validity of certificates. Another benefit of cryptography-based signatures is nonrepudiation, because the public key that is used to verify the signatures' registration delivers increased certainty of signers’ identities — that is, if the private key's owner takes the necessary steps to protect it.

- **Interoperability and cross-certification**: In theory, standards-compliant PKI solutions should work together. In practice, however, mostly because of the broad range of vendors and the unsettled state of standards, delivering interoperability and cross-certification has been difficult. Testing has shown that successful PKI deployments usually require technical adjustments because of differences in the way that standards are interpreted. (A particularly important factor is the flexibility that is offered by extension fields.) Policy issues related to cross-certification may be even more significant than technical challenges because enterprises must map their policies to other enterprises’ electronic business systems. Industry conventions and policy authorities have been proposed, but none have yet emerged.

**What are the major drivers of PKI adoption?**

We believe that the primary factor that is driving PKI adoption is the influence of IT professionals, who are encouraged by PKI vendors. The discipline of a solid credential registration process holds some appeal, although it can be accomplished without PKI. Some regional activities, such as e-government initiatives and national identity-card projects, have been promoting PKI. The increasing use of smart cards, which typically carry a digital certificate, can push PKI adoption. Government smart-card
programs, such as the U.S. Department of Defense's Common Access Card initiative, will influence PKI adoption to some degree; however, the use of smart cards for authentication varies greatly by region, and smart-card readers are not ubiquitous. PKI also will become more important as Web services develop (see "Code Signing: A Small Step Toward Software Security"), and as more-sensitive information, such as medical records, moves across the Internet in the form of electronic data interchange transactions. In addition, PKI that is used in conjunction with Wireless Transport Layer Security (WTLS) will prove useful in some areas of mobile commerce (see "Wireless Authentication via PKI: WTLS Is Enough for Now").

How are national governments influencing PKI adoption in their countries?

National governments' experience with PKI has been mixed: Some have promoted government-to-business and government-to-citizen applications of PKI. (Australia's Tax Office's use of one-time certificates for tax filings is an example of an active government-to-citizen application.) Some countries have championed more-general PKI adoption with projects such as Canada's Pathfinder awards program and Australia's Gatekeeper initiative. The governments of Singapore and China are pushing PKI as part of their smart-card-based national ID-card programs. By contrast, however, the U.S. government's Access Certificates for Electronic Services program remains highly lethargic, with individual agencies struggling to integrate their applications appropriately with PKI.

How are enterprises implementing PKI — and how should they be implementing it?

Most enterprise PKI projects begin with user identification and authentication, but PKI is excessive and unnecessary when used only for those purposes. PKI becomes a more-realistic and justifiable solution when applications use cryptography to ensure message privacy and protect stored data, and when enterprises identify the need for cryptographically applied digital signatures. The original vision for PKI — as part of a centralized service that provides key management across applications — is flawed. Most successful implementations will be tightly bound to the individual applications that they support. The public infrastructure originally conceived by the promoters of PKI has not materialized, and may never do so. Thus, the development of hierarchical PKIs also will be fairly limited. Hierarchies may develop within enterprises and agencies, with cross-certification creating webs of trust among entities by using digital certificates. Even within enterprises that choose to implement a central PKI based on one certificate authority or a limited number of authorities, registration will be
distributed to application owners. Key management can be handled as part of a provisioning system.

**What is the overall outlook for PKI?**

PKI generally has failed to deliver on its promise; therefore, the predominant authentication technology is password/user ID. Gartner believes that PKI adoption will continue a near-term decline, followed by a modest increase in use beginning in 2005. Most PKI vendors will need to move beyond PKI or they will go out of business. Gartner believes that PKI remains a useful tool. However, it will be most valuable for enterprises that focus not on PKI, but rather on the applications that PKI supports. In general, PKI will “disappear” into the applications that can benefit from the use of public and private keys. For example, e-mail systems will provide internal management of keys for digital signatures or encrypted messages, and virtual private network systems will manage keys without the use of external PKI.