Encyclopedia of Information Systems and Technology

Phillip A. Laplante, Vladimir Stantchev, Jeff Voas, Anne-Marie Smith, Qiuming Zhu, Morris Chang, Irena Bojanova, David Alan Grier, Jia Zhang, Thomas Costello, San Murugesan, Jim Goldman, Joanna DeFranco

PKI: Public Key Infrastructure

Publication details

Harry B. DeMaio

Published online on: 29 Dec 2015

How to cite :- Harry B. DeMaio. 29 Dec 2015, PKI: Public Key Infrastructure from: Encyclopedia of Information Systems and Technology CRC Press
Accessed on: 20 Aug 2023

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
PKI: Public Key Infrastructure

Harry B. DeMaio
Cincinnati, Ohio, U.S.A.

Abstract
This entry discusses encryption as a form of security, mostly focusing on public key infrastructures (PKIs). After a detailed examination of encryption, public-key encryption, and PKI, the author discusses how well PKI satisfies the needs of today. Although PKI is viewed as a possible approach, the author discusses whether it is the best choice as well as how to actually make PKI a “cost-effective reality.”

In the history of information protection, there has been an ongoing parade of technologies that loudly promises new and total solutions but frequently does not make it past the reviewing stand. In some cases, it breaks down completely at the start of the march. In others, it ends up turning down a side street. Is public key infrastructure (PKI) just another gaudy float behind more brass bands, or is there sufficient rationale to believe that this one might make it? There are some very good reasons for optimism in this case, but optimism has been high before.

To examine PKI, one needs to know more than just the design principles. Many a slick and sophisticated design has turned embarrassingly sour when implemented and put into application and operational contexts. There are also the questions of economics, market readiness, and operational/technological prerequisites, all of which can march a brilliant idea into a blind alley.

APPROACH AND PRELIMINARY DISCUSSION
We’ll start with a short review of the changing requirements for security. Is there really a need, especially in networking, that didn’t exist before for new security technologies and approaches?

- We’ll (very) briefly describe encryption, public-key encryption, and PKI.
- We’ll see how well PKI satisfies today’s needs from a design standpoint.
- We’ll look at what’s involved in actually making PKI a cost-effective reality.
- Finally, we’ll ask whether PKI is an exceptional approach or just one of many alternatives worth looking at.

CHANGING WORLD OF NETWORKED SYSTEMS
First, a few characteristics of yesterday’s and today’s network-based information processing need to be considered. If the differences can be summed up in a single phrase, it is “accelerated dynamics.” The structure and components of most major networks are in a constant state of flux—as are the applications, transactions, and users that traverse its pathways. This has a profound influence on the nature, location, scope, and effectiveness of protective mechanisms.

Table 1 illustrates some of the fundamental differences between traditional closed systems and open (often Internet-based) environments. These differences do much to explain the significant upsurge in interest in encryption technologies.

Clearly, each network is unique, and most display a mix of the preceding characteristics. But the trends toward openness and variability are clear. The implications for security can be profound. Security embedded in or “hard-wired” to the system and network infrastructure cannot carry the entire load in many of the more mobile and open environments, especially where dial-up is dominant. A more flexible mode that addresses the infrastructure, user, workstation, environment, and data objects is required.

An example: envision the following differences:

- A route salesperson who returns to the office work station in the evening to enter the day’s orders (online batch)
- That same worker now entering on a laptop through a radio or dial-up phone link those same orders as they are being taken at the customer’s premises (dial-up interactive)
- Third-party operators taking orders at an 800/888 call center
- Those same orders being entered by the customer on a website
- A combination of the preceding
The application is still the same: order entry. But the process is dramatically different, ranging from batch entry to Web-based electronic commerce.

In the first case, the infrastructure, environment, process, and user are known, stable, and can be well controlled. The classic access control facility or security server generally carries the load.

In the second (interactive dial-up) instance, the employee is still directly involved. However, now there is a portable device and its on-board functions and data, the dial-up connections, the network, the points of entry to the enterprise, and the enterprise processes to protect if the level of control that existed in the first instance is to be achieved.

The third instance involves a third party, and the network connection may be closed or open.

The fourth (Web-based) approach adds the unknowns created by the customer’s direct involvement and linkage through the Internet to the company’s system.

The fifth, hybrid scenario calls for significant compatibility adjustments on top of the other considerations. By the way, this scenario is not unlikely. A fallacious assumption in promoting web-based services is that one can readily discontinue the other service modes. It seldom happens.

Consider the changes to identification, authentication, and authorization targets and processes in each instance. Consider monitoring and the audit trail. Then consider the integrity and availability issues. Finally, the potential for repudiation begins to rear its ugly head. The differences are real and significant.

### EVOLVING BUSINESS NETWORK

Remember, too, that most network-based systems in operation today have evolved, or in many cases, accreted into their existing state—adding infrastructures and applications on demand and using the technology available at the time. Darwin notwithstanding, some of the surviving networks are not necessarily the fittest. In most of the literature, networks are characterized as examples of a specific class—open-closed, intranet-extranet, LAN-WAN-Internet, protocol-X or protocol-Y. Although these necessary and valuable distinctions can be used to describe physical and logical infrastructures, remember that when viewed from the business processes they support supply chain, order entry, funds transfer, and patient record processing. Most “business process” networks are technological and structural hybrids.

The important point is that today security strategy and architecture decisions are being driven increasingly by specific business requirements, not just technology. This is especially true in the application of encryption-related techniques such as PKI. Looking again at the earlier order entry example, the application of consistent protective mechanisms for a hybrid order entry scenario will undoubtedly require compatibility and interoperability across platform and network types unless the entire system is rebuilt to one specification. This seldom happens unless the enterprise is embarking on a massive reengineering effort or deploying major application suites such as the SAP AG R/3 or PeopleSoft.

### Disintegration and Reintegration of Security Mechanisms

To be effective, a protective mechanism must appropriately bind with the object and the environment requiring protection. In open networks, the connection, structure, and relationship of the components are more loosely defined and variable. Therefore, the protective mechanisms must be more granular, focused, and more directly linked to the object or process to be protected than was the case with legacy systems. Formerly, protection processes operated primarily at a “subterranean plumbing” level, surfacing only in password and authorization administration and log-ons. Now the castle moat is being supplemented with “no-go” zones, personal bodyguards posted at strategic spots, food tasters, and trusted messengers.

Encryption mechanisms fit this direct, granular requirement often ideally, since they can protect individual files, data elements (including passwords), paths (tunneling and virtual private networks), and manage access management requirements. (Identification and authentication through encryption is easier than authorization.) But saying that encryption is granular is not the
same as saying that a PKI system is interoperable, portable, or scalable. In fact, it means that most encryption-related systems today are still piece parts, although some effective suites such as Entrust are in the market and several others, such as IBM SecureWay and RSA/SD Keon, are just entering.

This “disintegrated” and specialized approach to providing security function creates a frustrating problem for security professionals accustomed to integrated suites. Now the user becomes the integrator or must use a third-party integrator. The products may not integrate well or even be able to interface with one another. At the 1999 RSA Conference in San Jose, CA, the clarion call for security suites was loud and clear.

**Encryption Defined**

Encryption is a process for making intelligible information unintelligible through the application of sophisticated mathematical conversion techniques. Obviously, to be useful the process must be reversible (decryption). The three major components of the encryption/decryption process are as follows:

1. **The information stream in clear or encrypted form.**
2. **The mathematical encryption process**—the algorithm. Interestingly, most commercial algorithms are publicly available and are not secret. What turns a public process into a uniquely secret one is the encryption key.
3. **The encryption key.** The encryption key is a data string that is mathematically combined with the information (clear or encrypted) by the algorithm to produce the opposite version of the data (encrypted or clear). Remember that all data on computers is represented in binary number coding. Binary numbers can be operated upon by the same arithmetic functions as those that apply to decimal numbers. So by combining complex arithmetic operations, the data and key are converted into an encrypted message form and decrypted using the same process and *same key*—with one critical exception.

Before explaining the exception, one more definition is required. The process that uses the *same key* to decrypt and encrypt is called symmetric cryptography. It has several advantages, including exceptional speed on computers. It has a serious drawback. In any population of communicating users (n), in order to have *individually unique* links between each pair of users, the total number of keys required is \( n(n + 1)/2 \). Try it with a small number and round up. If the population of users gets large enough, the number of individual keys required rapidly becomes unmanageable. This is one (but not the only) reason why symmetric cryptography has not had a great reception in the commercial marketplace in the last 20 years.

The salvation of cryptography for practical business use has been the application of a different class of cryptographic algorithms using asymmetric key pairs. The mathematics is complex and is not intuitively obvious, but the result is a *pair of linked keys* that must be used together. However, only one of the pair, the private key, must be kept secret by the key owner. The other half of the pair—the public key—can be openly distributed to anyone wishing to communicate with the key owner. A partial analogy is the cash depository in which all customers have the same key for depositing through a one-way door, but only the bank official has a key to open the door to extract the cash. This technique vastly reduces the number of keys required for the same population to communicate safely and uniquely.

**ENTER PKI**

If the public key is distributed openly, how do you know that it is valid and belongs with the appropriate secret key and the key owner? How do you manage the creation, use, and termination of these key pairs. That is the foundation of PKI. Several definitions follow:

The comprehensive system required to provide public-key encryption and digital signature services is known as the public-key infrastructure (PKI). The purpose of a public-key infrastructure is to manage keys and certificates.

—Entrust Inc.

A public-key infrastructure (PKI) consists of the programs, data formats, communications protocols, institutional policies, and procedures required for enterprise use of public-key cryptography.

—Office of Information Technology, University of Minnesota

In its most simple form, a PKI is a system for publishing the public-key values used in public-key cryptography. There are two basic operations common to all PKIs:

1. **Certification** is the process of binding a public-key value to an individual organization or other entity, or even to some other piece of information such as a permission or credential.
2. **Validation** is the process of verifying that a certificate is still valid.

How these two operations are implemented is the basic defining characteristic of all PKIs.

—Marc Branchaud
Digital Certificate and Certificate Authorities

Obviously, from these definitions, a digital certificate is the focal point of the PKI process. What is it? In simplest terms, a digital certificate is a credential (in digital form) in which the public key of the individual is embedded along with other identifying data. That credential is encrypted (signed) by a trusted third party or certificate authority (CA) who has established the identity of the key owner (similar to but more rigorous than notarization). The “signing key” ties the certificate back to the CA and ultimately to the process that bound the certificate holder to his or her credentials and identity proof process.

By “signing” the certificate, the CA establishes and takes liability for the authenticity of the public key contained in the certificate and the fact that it is bound to the named user. Now total strangers who know or at least trust a common CA can use encryption not just to conceal the data but also to authenticate the other party. The integrity of the message is also ensured. If you change it once encrypted, it will not decrypt. The message cannot be repudiated because it has been encrypted using the sender’s certificate.

Who are CAs? Some large institutions are their own CAs, especially banks (private CAs). There are some independent services (public CAs) developing, and the government, using the licensing model as a take-off point, is moving into this environment. It may become a new security industry. In the Netherlands, KNB, the Dutch notary service, supplies digital certificates.

As you would expect, there has been a move by some security professionals to include more information in the certificate, making it a multipurpose “document.” There is one major problem with this. Consider a driver’s license, which is printed on special watermarked paper, includes the driver’s picture, and is encapsulated in plastic. If one wished to maintain more volatile information on it, such as the existing make of car(s), doctor’s name and address, or next of kin, the person would have to get a new license for each change.

The same is true for a certificate. The user would have to go back to the CA for a new certificate each time he made a change. For a small and readily accessible population, this may be reasonable. However, PKI is usually justified based on large populations in open environments, often across multiple enterprises. The cost and administrative logjam can build up with the addition of authorization updates embedded in the certificate. This is why relatively changeable authorization data (permissions) are seldom embedded in the certificate but rather attached. There are several certificate structures that allow attachments or permissions that can be changed independently of the certificate itself.

To review, the certificate is the heart of the PKI system. A given population of users who wish to intercommunicate selects or is required to use a specific CA to obtain a certificate. That certificate contains the public-key half of an asymmetric key pair as well as other indicative information about the target individual. This individual is referred to as the “distinguished name”—implying that there can be no ambiguities in certificate-based identification—all Smiths must be separately distinguished by ancillary data.

Where Are Certificates Used?

Certificates are used primarily in open environments in which closed network security techniques are inappropriate or insufficient for any or all of the following:

- Identification/authentication
- Confidentiality
- Message/transaction integrity
- Nonrepudiation

Not all PKI systems serve the same purposes or have the same protective priorities. This is important to understand when one is trying to justify a PKI system for a specific business environment.

How Does PKI Satisfy Those Business Environment Needs?

Market expectation

As PKI becomes interoperable, scalable, and generally accepted, companies will begin to accept the wide use of encryption-related products. Large enterprises such as government, banks, and large commercial firms will develop trust models to easily incorporate PKI into everyday business use.

Existing reality

It is not that easy. Thus far, a significant number of PKI projects have been curtailed, revised, or temporarily shelved for reevaluation. The reasons most often given include the following:

- Immature technology
- Insufficient planning and preparation
- Underestimated scope
- Infrastructure and procedural costs
- Operational and technical incompatibilities
- Unclear cost–benefits

Apparent Conclusions about the Marketplace

PKI has compelling justifications for many enterprises, but there are usually more variables and pitfalls than
anticipated. Broadside implementation, though sometimes necessary, has not been as cost-effective. Pilots and test beds are strongly recommended.

A properly designed CA/registration authority (RA) administrative function is always a critical success factor.

CERTIFICATES, CA, AND RA

How do they work and how are they related?

First look at the PKI certificate lifecycle. It is more involved than one may think. A digital certificate is a secure and trustworthy credential, and the process of its creation, use, and termination must be appropriately controlled.

Not all certificates are considered equally secure and trustworthy, and this is an active subject of standards and industry discussion. The strength of the cryptography supporting the certificate is only one discriminating factor. The degree to which the certificate complies with a given standard, X.509, for example, is another criterion for trustworthiness. The standards cover a wide range of requirements, including content, configuration, and process. The following is hardly an exhaustive list, but it will provide some insight into some of the basic requirements of process.

- **Application**—How do the “certificate owners to be” apply for a certificate? To whom do they apply? What supporting materials are required? Must a face-to-face interview be conducted, or can a surrogate act for the subject? What sanctions are imposed for false, incomplete, or misleading statements? How is the application stored and protected?

- **Validation**—How is the applicant’s identity validated? By what instruments? By what agencies? For what period of time?

- **Issuance**—Assuming the application meets the criteria and the validation is successful, how is the certificate actually issued? Are third parties involved? Is the certificate sent to the individual or, in the case of an organization, some officer of that organization? How is issuance recorded? How are those records maintained and protected?

- **Acceptance**—How does the applicant indicate acceptance of the certificate? To whom? Is non-repudiation of acceptance eliminated?

- **Use**—What are the conditions of use? Environments, systems, and applications?

- **Suspension or Revocation**—In the event of compromise or suspension, who must be notified? How? How soon after the event? How is the notice of revocation published?

- **Expiration and Renewal**—Terms, process, and authority?

Who and What Are the PKI Functional Entities That Must Be Considered?

Certification authority

- A person or institution who is trusted and can vouch for the authenticity of a public key
- May be a principal (e.g., management, bank, or credit card issuer)
- May be a secretary of a “club” (e.g., bank clearing house)
- May be a government agency or designee (e.g., notary public, Department of Motor Vehicles, or post office)
- May be an independent third party operating for a profit (e.g., VeriSign®)
- Makes a decision on evidence or knowledge after due diligence
- Records the decision by signing a certificate with its private key
- Authorizes issuance of certificate

Registration authority

- Manages certificate life cycle, including Certificate Directory maintenance and Certificate Revocation List(s) (CRL) maintenance and publication.
- Thus can be a critical choke point in PKI process and a critical liability point, especially as it relates to CRLs.
- An RA may or may not be CA.

Other entities

- **Other Trusted Third Parties**—These may be service organizations that manage the PKI process, brokers who procure certificates from certificate suppliers, or independent audit or consulting groups that evaluate the security of the PKI procedure.
- **Individual Subscribers**.
- **Business Subscribers**—In many large organizations, two additional constructs are used:

1. **The Responsible Individual (RI)**—The enterprise certificate administrator.
2. **The Responsible Officer (RO)**—The enterprise officer who legally assures the company’s commitment to the certificate. In many business instances, it is more important to know that this certificate is backed by a viable organization that will accept liability than to be able to fully identify the actual certificate holder. In a business transaction, the fact
that a person can prove he or she is a partner in Deloitte & Touche LLP who is empowered to commit the firm usually means more than who that person is personally.

PKI policies and related statements include the following:

- Certificate policy
- Named set of rules governing certificate usage with common security requirements tailored to the operating environment within the enterprise
- Certificate practices statement (CPS)
- Detailed set of rules governing the CA’s operations
- Technical and administrative security controls
- Audit
- Key management
- Liability, financial stability, due diligence
- CA contractual requirements and documents
- Subscriber enrollment and termination processes

Certificate Revocation List

Of all the administrative and control mechanisms required by a PKI, the CRL function can be one of the more complex and subtle activities. The CRL is an important index of the overall trustworthiness of the specific PKI environment. Normally it is considered part of the RA’s duties. Essentially, the CRL is the instrument for checking the continued validity of the certificates for which the RA has responsibility. If a certificate is compromised, if the holder is no longer authorized to use the certificate, or if there is a fault in the binding of the certificate to the holder, it must be revoked and taken out of circulation as rapidly as possible. All parties in the trust relationship must be informed. The CRL is usually a highly controlled online database (it may take any number of graphic forms) at which subscribers and administrators may determine the currency of a target partner’s certificate. This process can vary dramatically by the following:

- Timing/frequency of update. Be careful of the language here. Many RAs claim a 24 hours update. That means the CRL is refreshed every 24 hours. It does not necessarily mean that the total cycle time for a particular revocation to be posted is 24 hours. It may be longer.
- Push-pull. This refers to the way in which subscribers can get updates from the CRL. Most CRLs require subscribers to pull the update. A few private RAs (see the following text) employ a push methodology. There is a significant difference in cost and complexity and most important the line of demarcation between an RA’s and the subscriber’s responsibility and liability. For lessened liability alone, most RAs prefer the pull mode.
- Up link/down link. There are two transmissions in the CRL process: the link from the revoking agent to the CRL and the distribution by the CRL to the subscribing universe. Much work has been exerted by RAs to increase the efficiency of the latter process, but because it depends on the revoking agency, the up link is often an Achilles’ heel. Obviously, the overall time is a combination of both processes, plus file update time.

- Cross-domain. The world of certificates may involve multiple domains and hierarchies. Each domain has a need to know the validity status of all certificates that are used within its bounds. In some large extranet environments, this may involve multiple and multilayer RA and CRL structures. Think this one through very carefully and be aware that the relationships may change each time the network encompasses a new environment.

- Integrity. One major way to undermine the trustworthiness of a PKI environment is to compromise the integrity of the CRL process. If the continued validity of the certificate population cannot be assured, the whole system is at risk.
- Archiving. How long should individual CRLs be kept and for what purposes?
- Liabilities and commitments. These should be clearly, unambiguously, and completely stated by all parties involved. In any case of message or transaction compromise traceable to faulty PKI process, the RA is invariably going to be involved. Make very sure you have a common understanding.

As you might expect, CAs and RAs come in a variety of types. Some of the more common include the following:

- Full-service public CA providing RA, certificate generation, issuance, and life-cycle management. Examples: VeriSign, U.S. Postal Service, TradeWave
- Branded public CA providing RA, certificate issuance, and lifecycle management
- Certificates generated by a trusted party, e.g., VeriSign, GTE CyberTrust. Examples: IDMetrix/GTE CyberTrust, Sumitomo Bank/VeriSign
- Private CAs using CA turn-key system solutions internally. Examples: ScotiaBank (Entrust), LexisNexis (VeriSign On-Site)
- IBM Vault Registry

There are also wide variations in trust structure models. This is driven by the business process and network architecture:
Hierarchical trust (a classical hierarchy that may involve multiple levels and a large number of individual domains)
- VeriSign, Entrust
- X.509v3 certificates
- One-to-one binding of certificate and public key
- Web of Trust (a variation on peer relationships between domains)
- PGP
- Many-to-one binding of certificates and public key
- Constrained or Lattice of Trust structures
- Hybrid of hierarchical and web models
- Xcert

There are several standards, guidelines, and practices that are applicable to PKI. This is both a blessing and a curse. The most common are listed in the following text. Individual explanations can be found at several websites. Start at the following site, which has a very comprehensive set of PKI links—http://www.cert.dfn.de/eng/team/ske/pem-dok.html. This is one of the best PKI link sites available.

- X.500 Directory Services and X.509 Authentication
- Common Criteria (CC)
- American National Standards Institute (ANSI) X9 series
- Department of Defense Standards
- Trusted Computer System Evaluation Criteria (TCSEC), Trusted Software Development Methodology (TSDM), Software Engineering Institute Capability Maturity Model (SEI CMM)
- Internet Engineering Task Force (IETF) RFC—PKIX, PGP
- S/MIME, SSL, IPSEC
- SET
- ABA Guidelines
- Digital Signatures, Certification Practices
- FIPS Publications 46, 140-1, 180-1, 186

CA/RA targets of evaluation

To comprehensively assess the trustworthiness of the individual CA/RA and the associated processes, Deloitte & Touche developed the following list of required evaluation targets:

- System level (in support of the CA/RA process and certificate usage if applicable)
- System components comprising a CA/RA environment
- Network devices
- Firewalls, routers, and switches
- Network servers
- IP addresses of all devices

How Well Does PKI Satisfy Today’s Open Systems Security Needs?

In a nutshell, PKI is an evolving process. It has the fundamental strength, granularity, and flexibility required to support the security requirements outlined. In that respect, it is the best available alternative. But wholesale adoption of PKI as the best, final, and global solution for security needs is naïve and dangerous. It should be examined selectively by business process or application to determine whether there is sufficient “value-added” to justify the direct and indirect cost associated with deployment. As suites such as Entrust become more adaptive and rich interfaces to ERP systems such as the SAP R/3 become more commonplace, PKI will be the security technology of choice for major, high-value processes. It will never be the only game in town. Uncomfortable or disillusioning as it may be, the security world will be a multi-solution environment for quite a while.
What Is Involved in Making PKI a Cost-Effective Reality?

The most common approach to launching PKI is a pilot environment. Get your feet wet. Map the due diligence and procedural requirements against the culture of the organization. Look at the volatility of the certificates that will be issued. What is their life expectancy and need for modification? Check the interface issues. What is the prospective growth curve for certificate use? How many entities will be involved? Is cross-certification necessary? Above all else, examine the authorization process requirements that must co-exist with PKI. PKI is not a full-function access-control process. Look into the standards and regulations that affect your industry. Are there export control issues associated with the PKI solution being deployed? Is interoperability a major requirement? If so, how flexible is the design of the solutions being considered?

CA PILOT CONSIDERATIONS

Type of Pilot

- Proof of concept—May be a test bed or an actual production environment.
- Operational—A total but carefully scoped environment. Be sure to have a clear statement of expectations against which to measure functional and business results.
- Inter-enterprise—Avoid this as a start-up if possible. But sometimes it is the real justification for adopting PKI. If so, spend considerable time and effort getting a set of procedures and objectives agreed upon by all of the partners involved. An objective third-party evaluation can be very helpful.
- Examine standards alternatives and requirements carefully—especially in a regulated industry.

- Check product and package compatibility, interoperability, and scalability very carefully.
- Develop alternative compatible product scenarios. At this stage of market maturity, a Plan B is essential. Obviously not all products are universally interchangeable. Develop a backup suite and do some preliminary testing on it.
- Investigate outsourced support as an initial step into the environment. Although a company’s philosophy may dictate an internally developed solution, the first round may be better deployed using outside resources.
- What are the service levels explicitly or implicitly required?
- Start internally with a friendly environment. You need all the support you can get, especially from business process owners.
- Provide sufficient time and resources for procedural infrastructure development, including CA policy, CPS, and training.
- Do not promise more than you can deliver.

Is PKI an Exceptional Approach or Just One of Many Alternatives Worth Looking At?

The answer depends largely on the security objectives of the organization. PKI is ideal (but potentially expensive) for extranets and environments in which more traditional identification and authentication are insufficient. Tempting as it may be, resist the urge to find the single solution. Most networked-based environments and the associated enterprises are too complex for one global solution. Examine the potential for SSL, SMIME, Kerberos, single sign-on, and virtual private networks (VPNs). If you can make the technical, operational, and cost-justification case for a single, PKI-based security approach, do so. PKI is a powerful structure, but it is not a religious icon. Leave yourself room for tailored multi-solution environments.