PKI NOTE

April 2002

PKI Basics - A Business Perspective

This Note examines the use of Public Key Infrastructure (PKI) in a business environment, starting from the current security concerns of businesses and then reviewing the necessary components of information security. It also delineates the key security services that enable risk mitigation in digital environments, and explains how PKI cohesively enables the systematic approach to information security that businesses need.

The Business Environment Today

As e-business[1] evolves, new business models are bringing about a plethora of changes. Interconnectivity between vendors, suppliers, customers, and employees has gained a new level of importance as a way to achieve a competitive edge. The value of intellectual property has skyrocketed and the need to protect it has become more critical. In the financial, healthcare, and education markets, government regulation has made compliance with privacy and security rules an imperative.

Accompanying these changes are e-business related risks. One of the primary concerns identified by both businesses and consumers in establishing and participating in e-business is the potential loss of assets due to security breaches of commercial transactions and corporate computer systems. A security breach not only erodes confidence in the business but also affects the organization's reputation capital. Case studies demonstrate risks that include sabotage, vandalism, loss of data confidentiality and integrity, theft, fraud, and breaches of privacy.

Privacy of information is on high center in many environments. When an enterprise is responsible for the safe keeping of third party personal information, the burden of care goes up and the risks go up with it. Providing for the ready availability of information to authorized constituents amidst these risks requires thorough and thoughtful planning.

In the brick and mortar world, responsibility to mitigate these risks is well understood and so the infrastructure, in the forms of legal, financial and physical controls, has been developed to meet those organizational obligations. To sustain an equivalent level of risk management under new business models that rely on the electronic flow of sensitive information, new infrastructure and trust models must be established.

Information Security

Most electronic communications today are not private nor are they secure unless explicitly protected. Digital media are susceptible to substitution, modification, and replication. Data that is stored on a network, or that is passed from one user to another, must be protected from fraudulent access and misdirection. As a result, network security is paramount to every organization that has chosen to enter the digital domain. Information security typically requires three approaches that are all essential to providing the modern environment with adequate levels of electronic risk mitigation. They are commonly categorized as:

[1]For the purposes of this discussion, e-business refers to any business conducted over electronic channels. It includes, but is not limited to, government, finance, healthcare, and all commercial vertical market applications.

Acknowledgements

"PKI Basics - A Business Perspective" is a deliverable from the PKI Forum's Business Working Group (BWG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Principal Author:

Patricia Lareau
Chair, PKI Forum Business Working Group

Contributor:

Bryta Schulz
RSA Security

Reviewers:

Andy Churley
nCipher, Inc.

Steve Lloyd
Chair, PKI Forum Technical Working Group

Jeff Stapleton
KPMG LLP

1) enablement,
2) intrusion detection and response, and
3) perimeter control.

Digital signatures and the Public Key Infrastructure (PKI) being discussed here fall under the first of these efforts. Enablement implies that a cohesive plan has been put in place (a security policy) and that an infrastructure to support the successful execution of the plan has been developed. Broadly speaking, this security plan must consider people, business processes, and technologies and structure how they will interact to conduct business in a secure and trusted fashion. The infrastructure must provide services such as data confidentiality and integrity, user authentication, non-repudiation of transactions, and legitimate availability of services and information. These security services enable risk mitigation in a digital environment.

Enablement also means that new business opportunities can be exploited, that the implementation of the security plan allows the adoption of processes that were previously too risk laden.

Public key cryptography allows a private secret to have a public counterpart that can be used to provide secure communications without jeopardizing the secret. Each entity protects its own private key (secret) while allowing its public key to be widely disseminated for all to use when conducting business with it.

Public Key Infrastructure (PKI)

For years PKI has advocated, through its intrinsic design, a systematic approach to information security. Rather than addressing the security service needs individually, PKI builds an infrastructure that cohesively provides these enablers. One of the long-term returns on investment in such a system is that future applications can be added without modifying the basic structure. After all, the return on investment for any infrastructure is tied to the applications that use it and as the list in the Appendix suggests, the potential benefits are substantial. Like electricity and telephone infrastructures, a security infrastructure has become an essential enabler of business objectives, be they increasing revenue, reducing costs, meeting compliance mandates, or reducing risk.

Unique Technology

The primary purpose of this note is to discuss PKI in a business environment and how it addresses the trust issues inherent in business models, but first two aspects of the technology itself require a short explanation. PKI is built on mathematical constructions that are designed to address cohesively all of the requirements noted above. The mathematical underpinnings of public key cryptography fortuitously allow a secret (there is no security without secrets!) to be assigned uniquely to each entity and individual in a system. Prior to this development, secure communications required the secret to be known by all parties to the information exchange. One party always had to worry about the care taken by the other parties to maintain the secret. In addition, the difficulty of distributing the secrets to multiple parties in a secure manner becomes impractical for large-scale deployments. Public key cryptography allows a private secret to have a public counterpart that can be used to provide secure communications without jeopardizing the secret. Each entity protects its own private key (secret) while allowing its public key to be widely disseminated for all to use when conducting business with it. This is called Public key cryptography has been well vetted in the scientific community since the mid-70s.

Core to many of the security services of a PKI is the notion of a "digital signature". Designed to duplicate the value of a hand written signature in the brick and mortar world, it is based on the use of the unique private key (secret) described above. The "signing" process involves the use of the private key in a mathematical formula that ties the secret to the data being signed. The widely disseminated public counterpart, in the form of a digital certificate, can be used to verify that data is strongly associated with the sender of the data. We will see later how this construct can be indispensable in establishing and conducting business relationships. The use of digital signatures is supported by recent legislative actions that provide credibility to the concept of electronic signatures and recognition to the need for such a capability. The U.S. E-Sign Law, passed in 2000, and the EU Digital Signature Law, passed in 2001, are examples of this trend.

The use of digital signatures is supported by recent legislative actions that provide credibility to the concept of electronic signatures and recognition to the need for such a capability. The U.S. E-Sign Law, passed in 2000, and the EU Digital Signature Law, passed in 2001, are examples of this trend.

The I in PKI

As was discussed before, information security relies on a framework or infrastructure to deliver its promise. The infrastructure is the big picture, the blanket that ensures the interoperability of the parts. For example, a user's secret is of little value in establishing the identity of a business partner if there is not an infrastructure in place to provide assurances that the user and his secret are bound together in a trusted manner. Dependence upon the secret to determine the identity of the user is only prudent where the infrastructure guarantees (up to the risk threshold) that the binding is still valid. The backbone must also make the services useful by assuring that they are conducted in a trusted way. In a well-constructed infrastructure, the services are available, reliable, and unobtrusive. As with the service of electricity, the user does not need to understand how it is provided but rather that it can be relied upon to deliver.

Although PKI derives its name from Public Key Cryptography, some of the services it provides have their technical roots in techniques that are outside this branch of cryptography. PKI embodies the best of these well-understood techniques. It represents the integration of public key cryptography used for digital signatures and key management, and symmetric key[2] cryptography used for encryption.

All security infrastructures must meet these obligations. A Public Key Infrastructure uses the basic Public-Private key-pair relationship to build not only many of the services it provides but also the trusted infrastructure that provides the services. There is a consistency of methodology that augments the trust in the system. A public key infrastructure is, by design, a cohesive set of services built on a trusted architecture. The well conceived combination of services, communications methods and protocols available to applications programs comprises the infrastructure of a PKI.

A Public Key Infrastructure uses the basic Public-Private key-pair relationship to build not only many of the services it provides but also the trusted infrastructure that provides the services.

Secure Business Services

Each of the security services defined earlier is specifically designed to meet the challenges of mitigating the risks associated with conducting business over networks. Even networks that have no external connectivity have risks that need to be addressed. Insider attacks today are considered by many to present the most significant threats to assets. Each security service can be described in the context of the business objective it is designed to support.

- **Entity Authentication**: In a business environment, the single most important basic need is certainty regarding the identity of the person, corporate entity, application server, customer, or supplier with whom business is being transacted. In the electronic environment this security service is referred to as entity authentication. For example, users sending their credit card number across a network to make a purchase want to be certain that they are dealing with a trustworthy merchant rather than a fraudulent impersonator who wishes to steal their credit card number for a private spending spree. If users can verify the identity of the merchant, they will send their credit information with greater confidence. Today, a public key infrastructure almost ubiquitously provides this service for on-line retail purchases and on-line banking. Through protocols such as SSL and TLS, a customer is provided additional assurance that the retail or banking service provider is authentic. These protocols can be used to provide assurances in both directions. In applications like remote employee access to a corporate network, email and messaging services, supplier and customer access to databases through industry web portals, where identity authentication is critical, the use of digital signatures is a natural. The Infrastructure makes it happen by assuring the binding of the signature to the individual requesting access, and by providing the way to verify that binding.

In applications like remote employee access to a corporate network, email and messaging services, supplier and customer access to databases through industry web portals, where identity authentication is critical, the use of digital signatures is a natural.

[2]Symmetric key cryptography requires all communicating parties to know the same secret key. Public key cryptography makes it possible to efficiently distribute this shared secret. Secret key cryptography is a more efficient technique for the encryption of large amounts of data.

• **Data confidentiality** plays a major role within any transaction framework. Sensitive data, including, but not limited to, business plans, financial transactions, intellectual property, personnel records, third party information, etc. must be safeguarded from prying eyes. This is true whether the data is:

- in transit, e.g. over a network to a business partner, customer, or constituent, or the data is:
- at rest, e.g. stored on an application server.

Encryption is the mathematical mechanism that is used to provide confidentiality. As noted earlier, this is usually accomplished using symmetric key techniques, as opposed to asymmetric public key techniques, because it is more efficient to do so. For wide-spread use of encryption, it is essential to have a key distribution system that is as contemporary as the systems that will employ it. Public key cryptography is the only scaleable alternative for the secure delivery of keys. A PKI embraces both of these optimal techniques to support confidentiality.

Confidentiality can be more broadly construed than just the encryption of data. Confidentiality further implies no unauthorized access to information. In this broader context, data confidentiality services, along with authentication services, form part of an organization's strategic plan to meet legal, regulatory, and industry requirements regarding the **privacy** of individuals and their personal information. PKI is well suited to help meet these requirements.

Using a system that provides non-repudiation, the service or data provider can produce irrefutable evidence that the request was in fact made and establish the legitimacy of the bill.

• **Data integrity** is a service to detect whether information, either stored or being transmitted, has been accidentally or maliciously altered. Consider the case of an electronic business proposal. A proposal to purchase 50 units at US $50 each should not, in the course of transmission, be altered (or alterable) to 50,000 units. PKI uses a digital signature to assure the receiving party that the data has not been changed since it left the attention of the known sender. Even in the absence of malicious attacks, being positively informed about the accuracy of information is a critical business need and a well-suited application for public key technology.

• **Non-repudiation** is data integrity and entity authentication **provable to a third party**. It gives a recipient the confidence that the sender cannot successfully deny having authored, signed, or originated a given document or transaction. This is quite important in financial transactions where someone may wish to refuse a bill claiming that they hadn't requested the service in the first place. Using a system that provides non-repudiation, the service or data provider can produce irrefutable evidence that the request was in fact made and establish the legitimacy of the bill. Remembering that, in accordance with the principles of public key cryptography, the private key (and therefore the digital signature) is only known by one person, non-repudiation is achievable when coupled with the appropriate policies and procedures. Using digital signatures to sign binding contracts, is therefore achievable as well. Digital signatures do not provide non-repudiation but rather enable it. Technology is only one of several ingredients necessary to achieve non-repudiation. As with handwritten signatures, the appropriate policies and procedures must be in place, and human intervention can be required in some circumstances to establish non-repudiation.

A digital certificate, which is provided and managed by a PKI, can be used to bind an identity to a set of privileges, thus becoming a valuable tool in access management.

• **Privilege Management** is a service that securely administers the policies that govern access to sensitive data stored on a network. This could be important in guaranteeing the privacy of healthcare or financial information or in protecting access to intellectual property and competitive business plans. A digital certificate, which is provided and managed by a PKI, can be used to bind an identity to a set of privileges, thus becoming a valuable tool in access management. An administrator can thereby ascertain access privileges of an entity before allowing them access to the data, or even before verifying the existence of the data.

The Backbone of the Infrastructure

Recalling that the responsibility of the Infrastructure is to deliver the services in a trusted fashion, all kinds of questions should now come to mind. Who binds the identity of the secret to the individual? How is the entity's identity established in the first place? How do

I know if an individual's secret has been compromised? Most of these questions go back to the basic business need for trust.

To build trust, the Public Key model for an infrastructure centers on the Certification Authority, the Registration Authority, and their relationship to the applications they serve, to the individuals they subscribe, and the policies that they support.

Certification Authority (CA)

The Certification Authority (CA) is the heart of the PKI, responsible for creating the certificate that binds a subscriber's identity to their public key. The evidence required to assure the accuracy of the binding depends on the applicable security policies. These policies are based on an enterprise's risk assessment of their business environment. The end-user registration process may require in-person interviews or it may rely solely on information publicly available and provided such as an email address. The value of the binding is determined by this procedure (as is true with any binding of an entity to a secret in any infrastructure). One of the strengths of a PKI is that it can be used to support multiple registration models, including the most restrictive requirements.

The CA also bears responsibility for the revocation of certificates. Although most certificates are issued and remain valid for their lifetime, there are occasions when the privileges associated with the certificate become invalid. This can be a result of normal activities, like the closing of an account or changing jobs. It can also be necessitated because of the potential compromise of the private key component. There are a number of models for how this activity can be carried out, but they are beyond the scope of this paper.

To build trust, the Public Key model for an infrastructure centers on the Certification Authority, the Registration Authority, and their relationship to the applications they serve, to the individuals they subscribe, and the policies that they support.

Registration Authority (RA)

A Registration Authority (RA) can be used to offload many of the administrative functions from the CA, including end-user registration. This is especially useful in large, geographically dispersed organizations that require their end-users to register in person. Rather then forcing all end-users to a centrally located registration site, RAs can be distributed so that personal travel and inconvenience is minimized.

PKI Policies

In order to implement a PKI effectively, a series of policies to govern the PKI must be in place. These are spelled out in documents such as the Certification Practice Statement (CPS) and the Certificate Policy (CP). A CPS describes the practices employed in issuing and managing certificates – it governs the management of the PKI. It may include a description of service offerings, detailed procedures for life-cycle management, operational information, etc. Furthermore, the CPS provides a legal framework describing the obligations and liabilities of the CA. By contrast, a CP consists of a set of rules that indicate the applicability of the certificate to a particular community and/or class of applications with common security requirements. The CP generally addresses the higher-level policy requirements whereas the CPS tends to be a fairly detailed and comprehensive technical and procedural document regarding the operation of the supporting infrastructure.

PKI presents a cohesive framework within which business applications can be conducted with the trust they require.

Conclusion

Business models today are driving security models to support them. All organizations face the pressures to increase revenue, reduce costs, comply with government and industry regulations, or reduce risk. These issues are compounded by the desire to conduct business electronically. Once the need for security services like authentication, data confidentiality and integrity, and non-repudiation are established as critical enablers to meet those objectives, the focus must turn to an implementation plan that can best support the success of the (security-enabled) business processes. PKI presents a cohesive framework within which business applications can be conducted with the trust they require. It is based on the best cryptographic techniques available and is comprehensive in its approach to enabling models that address today's business demands. A PKI keeps the horse before the cart and provides the environment and services within which an evolving business model can prosper.

Appendix 1: PKI-enabled Applications List

Market	Application Category	PKI-enabled Application Examples
Financial Services	Payment authentication	§ Stock purchases § Student loan funds transfer
	Access control (physical access and system access)	§ Online banking
	Secure messaging / e-mail	§ SEC filings
	Secure document storage / retrieval	§ Electronic mortgages § Applications § Storage
	Digital notary	§ Title documents § Loans
	Letters of Guarantee	§ Securing transactions / information against economic loss
Insurance	Digital signature	§ Online o Quotes o Application o Approval
	Payment authentication	§ Online payments o Premiums o Claims reimbursement
	Document management	§ Access control, version management, etc.
	Access control	§ Permissions-based access to patient records
Healthcare	Payment authentication	§ Claims reimbursement
	Secure messaging / e-mail	§ Claims filings
	Secure document storage / retrieval	§ Patient records o Processing o Retrieval o Transfer
	Physician ID	§ Identification for physician-only applications
	National ID	§ Passport § Emergency healthcare info.
Government	Access control	§ Building access
	Payment Authentication	§ Social Security benefits
	Bid Management	§ RFP response
	Transport	§ Contact-less smart card with access, payment / fee information
	Administration	§ Secure message / e-mail of benefit status
Vertical Market	**Application Category**	**PKI-enabled Application Examples**
	Secure document storage / retrieval	§ Legal briefs
	Government Services	§ Drivers License
B2B	Access control	§ Allowing only online partners to participate / view selected items
	Payment authentication	§ Securing electronic payment transfers upon purchase
	Procurement	§ NDA § MOU, MOI § RFP § Bids § Contracts
	Digital signature	§ Electronic contracts execution

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to understand and exploit the value of PKI in their e-business applications.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810