Creating a Secure Environment for e-business

Compaq NonStop™ eBusiness Solutions **White Paper**

Recognizing the issues that affect the building of a secure foundation for e-business

As organizations turn to the Internet as a medium for communications and for marketing products and services, providing security for users and IT assets is essential. However, establishing a safe, secure environment is not a simple task. Many issues must be carefully considered: establishing security policies and procedures, securing your facilities, selecting security personnel, setting up a certification authority, and more.

COMPAQ

Contents

As organizations turn to the Internet as a medium for communications and for marketing products and services, providing security for users and information technology (IT) assets is essential. However, establishing a safe, secure environment is not a simple task. Many issues must be carefully considered: establishing security policies and procedures, securing your facilities, selecting security personnel, setting up a certification authority, and more.

The purpose of this white paper is to identify key issues that you should consider when establishing security goals and objectives and when implementing a security infrastructure.

Online security: new challenges, new requirements

As the Internet undergoes explosive growth as a medium for conducting business globally, providing a safe, secure environment for all participants is essential.

The Internet is undergoing explosive growth as a medium for doing business on a global basis. As businesses have begun tapping the enormous potential of the Internet, security has become a strategic component for deploying online e-business applications.

Conducting business over the Internet poses a unique set of security challenges because the parties involved are often faceless and voiceless, known only to each other through their presence on the network. To provide a safe environment for all participants, an infrastructure for electronic commerce, communications, and information access must satisfy the following security requirements:

- *Authentication:* confirming the identity of participants (employees, customers, suppliers, partners, applications, and network devices)
- *Authorization:* granting or denying access to a participant
- *Privacy:* protecting the confidentiality of participants and sensitive information
- *Data integrity:* ensuring that data is not modified, altered, corrupted, or tampered with during commerce, communications, and information access activities
- *Evidence for nonrepudiation:* ensuring that the participants in a commerce transaction cannot later falsely deny that it occurred or was authorized

Public key infrastructure (PKI) is an end-to-end management system that provides a safe environment and satisfies the security requirements for all participants involved in electronic commerce, communications, and information access. PKI enables you to establish a single, common security infrastructure for all your e-business applications. This approach improves the operational effectiveness of your organization and reduces your overall IT costs, providing an excellent return on your security investment.

PKI makes it possible to implement public key cryptography and manage keys and digital certificates for an entire organization—including employees, customers, suppliers, and trading partners. Businesses have the opportunity to implement PKI as a highly effective way to reduce the risk of fraud and minimize IT costs.

Public key cryptography is ideally suited to ensure a secure environment for doing e-business over the Internet. Using a pair of keys—one public and one private—public key cryptography makes it possible to authenticate and authorize users on virtual private networks (such as intranets and extranets) and on public networks (such as the Internet). Public key cryptography can also satisfy the security objectives of privacy, data integrity, and nonrepudiation.

Digital certificates augment public key cryptography by providing a means of validating a user's public key and, thereby, verifying the individual's identity. A trusted party, called a certification authority, is responsible for issuing and managing certificates, vouching for the authenticity of each key and the identity of its owner.

To implement PKI, you must evaluate and modify your security policies, establish operation of a certification authority, and enable your applications with PKI.

As a leading provider of enterprise computing solutions, Compaq knows what it takes to create a secure environment. In subsequent sections of this document, we will address the key issues that you need to consider when implementing PKI to create a secure e-business environment.

Establishing security policies and procedures

When implementing PKI, it is important to develop security policies and procedures for accessing and using your IT assets.

As you begin the process of implementing PKI, you should develop (or reevaluate) the security policies and procedures associated with the access and use of your IT assets (such as applications, databases, servers, and clients) by your employees, customers, suppliers, and trading partners.

You need to establish levels of security: determine which individuals will be granted system access, then decide which applications and information they will be authorized to access. Based on the nature of the application, you may decide to grant access only to employees or you may choose to broaden access privileges to include trading partners and customers. You may need to limit user access to certain kinds of information; for example, allowing customers to view product information, but not pricing data; or permitting trading partners to view information, but not modify it.

In addition to your own policies and procedures, you must be cognizant of your government's trade policies. They are intended to prevent individuals, organizations, and governments deemed untrustworthy from being granted access to sensitive information or conducting electronic commerce. You must understand how to coordinate and implement your policies and procedures with existing domestic and international laws.

Setting up a certification authority

A certification authority (CA) is a trusted party who provides assurance that the participants involved in electronic commerce, communications, and information access are really who they claim to be.

You need to establish CA services in order to maintain the trust upon which secure electronic commerce, communications, and information access depend. The CA is a critical component of PKI because it provides assurance that the participants involved in electronic commerce, communications, and information access are really who they claim to be. To accomplish this, the CA performs many critical tasks, including

- Evaluating and registering users
- Creating and issuing keys and certificates
- Renewing and revoking certificates
- Maintaining lists of revoked certificates
- Establishing security policies

Establishing a CA requires operational facilities, security officers and administrators, directory integration and implementation, cross-certification procedures and processes, and the publication of a certification practice statement. Early on, you need to determine who will administer your CA services. Will it be your IT department or should you outsource the CA services? When making this decision, it is important to consider the costs, security trade-offs, risks, and liability of each option.

Securing your facilities

For CA activities, your computer facilities must be in a highly secure environment. You need to carefully select the type of building and room where your CA's systems and operations will reside. During this process, you should consider implementing multiple layers of security within your facilities, including locked doors, video monitoring, round-the-clock guards, tamper-proof enclosures, password security, and security systems equipped with biometric access controls.

To protect your internal computer network from hackers and eavesdroppers, it is advisable to implement the latest firewall technology. Acting as a security gateway, a firewall can be used to limit internal network systems from establishing connections to the Internet and to prevent incoming Internet traffic from connecting to internal network systems. In addition, you should consider implementing an intrusion detection and analysis system to analyze data packets and to detect attempted security breaches.

Selecting security officers and administrators

Without a doubt, the selection of your security personnel (such as officers, administrators, and operators) is one of the most important decisions involved in setting up a CA. You need to decide how many people you will require and who they will be. Your candidates will have the highest levels of authority, with full access to the CA facilities. They will also be responsible for certificate and key management, and for maintaining the trust in your CA's operation. Therefore, they must be highly trusted individuals.

Establishing operational practices and procedures

Operational practices and procedures play a significant role in how the CA functions. There are many issues to consider.

For example, it is important to establish clear lines of authority and responsibility among your security personnel. You should implement employee background checks and clearance procedures, training requirements, sanctions for unauthorized actions, and bonding requirements for contract personnel. As part of this process, you need to develop procedures that prevent users and security personnel from engaging in fraudulent activities.

In addition, there must be policies and procedures describing the conditions that permit security administrators to register users and issue, renew, and revoke certificates. You need to consider life-cycle issues, such as for how long certificates and keys are valid and for how long your organization will maintain copies of revoked and expired keys and certificates.

Ensuring directory integration

PKI components (such as the registration authority, certificate manager, and PKI-enabled applications) rely on a directory to store, distribute, find, and retrieve certificates. To implement PKI components, you must create a new directory or extend the schema of your existing directory to support certificates and certificate revocation lists for authentication and authorization of participants, and to collect information that provides evidence for nonrepudiation.

Extending trust to other CAs via cross-certification

When setting up a CA, cross-certification may be a necessary function for your application environment. Cross-certification allows two or more CAs to expand their relationship of trust by exchanging certificates. You and your trading partners, for example, may choose to cross-certify each other to facilitate commerce and communication between your respective companies and employees.

Publishing a certification practice statement

Any organization establishing a CA must publish a certificate practice statement (CPS). The purpose of this document is to provide a detailed explanation of the CA's practices, including service offerings and certificate life-cycle management.

The CPS describes the measures taken by the CA to authenticate certificate users and to protect its operational environment. In addition, the document describes underlying technical, procedural, and legal foundations contributing to the trustworthiness of the CA. Because the CPS contains details pertaining to CA practices and functions, it can be used by employees, customers, suppliers, and trading partners to assess the trustworthiness of your CA.

PKI-enabling your applications

Existing applications must be modified to use certificate and cryptographic services.

When implementing PKI, you must modify your existing applications so they can use certificate and cryptographic services. Before modifying them, you need to understand the architecture of your current applications. There are several issues that you should consider:

- Does your current application security align with your organization's security policies?
- How is security currently implemented with respect to the client, server, database, and transactions?
- What kind of security is implemented on the applications server? On the database server? On the client?
- What kind of network security do you currently employ?
- How is the security of your business applications going to change in an Internet, intranet, or extranet environment?

As part of this process, you need to determine who will comprise your user community and the privileges that users will be granted. For example, the user community could be composed of only your employees or it could include suppliers, trading partners, and customers as well. Your decision will affect the measures required to minimize risk.

After redesigning the security of your applications, you will have the information needed to modify them to use PKI. Once the modifications are finished, you will need to evaluate and revise your security policies, practices, and procedures to ensure alignment with the current instance of your PKI-enabled applications.

Conclusion

At Compaq, we offer a breadth of products and solutions for secure electronic commerce, communications, and information access. We have extensive knowledge and practical experience to help you meet your security goals and objectives.

Compaq can help you plan and implement PKI to support your strategic security goals and objectives. We have extensive experience in the most demanding business environments where critical applications must be secure and available around the clock.

Compaq offers a full range of professional services, including risk assessment, logical and physical design, development, and implementation of security solutions.

In addition, we offer a comprehensive set of products and solutions for secure electronic commerce, communications, and information access including

- The Compaq Certificate Security Solutions (CSS) product family for enterprise, universal, service provider, and virtual CA deployments
- Security services (client and server toolkits) to PKI-enable business applications
- Firewalls, proxy servers, and remote access servers
- Virtual private networks
- Intrusion detection and analysis
- Secure transactions and communications using Secure Socket Layer (SSL), Secure Electronic Transaction™ (SET), Internet protocol security (IPSec), and others
- Virus protection software
- Smart cards and biometrics

Whether you are establishing a CA or PKI-enabling applications, Compaq can help you with every aspect of your security solution.

For More Information WEBSITE: **www.compaq.com**

99-0719

COMPAQ