Implementing Secure Applications for e-business

Compaq NonStop™ eBusiness Solutions **White Paper**

Using Compaq's public key infrastructure solution to create a secure environment for your business applications

The Compaq Certificate Security Solution (CSS) products ensure the authenticity, privacy, and integrity of information routed over public and private IP networks. The CSS family includes software, hardware, and services for a certification authority, individual users, and business applications.

COMPAQ

Contents

The Compaq Certificate Security Solution (CSS) product family is an end-to-end management system that can provide a safe, secure environment for all of your organization's participants in electronic commerce, communications, and information access activities. The CSS product provides a public key infrastructure (PKI), which lets you establish a single, common security infrastructure for all your business applications. This common approach improves the operational effectiveness of your organization and reduces your overall information technology (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 and its constituents. To implement PKI, you must evaluate your security policies, operate or outsource a certification authority (CA), and enable your applications with PKI.

The CSS product ensures the authenticity, privacy, and integrity of information routed over public and private Internet Protocol (IP) networks. Based on partnerships with the leading PKI and security product vendors, the CSS family includes software, hardware, and services for a CA, individual users, and business applications.

Using a step-by-step example, this white paper leads you through the process of creating a secure environment for your business applications.

Implementing a secure application for electronic commerce, communications, and information access

Creating a secure environment for a global application requires careful planning and implementation.

As a leading provider of enterprise computing solutions, Compaq knows how to help you create a secure environment for doing business over the Internet. This white paper presents our suggested step-by-step process, which you can adapt to your own needs. To help you envision how this process might look in a real-world situation, we've described how a hypothetical company — Stargazer, Inc.—might implement this process.

StarGazer, Inc., our hypothetical corporation, is a global manufacturer of telescopic equipment with 10,000 employees in six countries. Terrance Talbot, CIO for StarGazer, needs to provide his employees with a secure way to access and make changes to their retirement accounts via the Internet. We'll observe how the company secures its application for this function.

Step 1: Identify the issues

What are your security issues? What do you want to do and how much security do you need to accomplish your goal? Most likely, you need a way to do the following:

- Guarantee the identities of those using your application
- Validate the form of payments, deposits, and withdrawals made against an employee account
- Promote mutual respect and trust between parties
- Prevent fraud and other malicious activity
- Leverage your existing network to do business 24 hours a day, 7 days a week, with little additional investment
- Continue operations after a disaster

What kinds of electronic transactions do you want to deploy?

Another step in identifying the issues is to determine the kinds of transactions you will be doing. These might include

- *Electronic data interchange (EDI):* business-to-business transactions involving invoices, payments, replenishment, and so on
- *Home shopping:* business-to-customer transactions involving the direct purchase of goods and services
- *Home banking:* banking services delivered directly to a corporate or retail customer using a graphical interface
- *Interoffice applications:* secure internal electronic mail, employee benefits management, corporate data transfer, and communication between remote offices

What are the requirements for a secure infrastructure?

Your requirements might include

- *Authentication:* confirming the identity of participants (individuals, organizations, and applications) and granting or denying access
- *Authorization:* defining the privileges (the application functions) an individual has access to
- *Privacy:* protecting the confidentiality of users and sensitive information
- *Data integrity:* ensuring that data is not modified, altered, corrupted, or tampered with during transmission
- *Evidence of nonrepudiation:* ensuring that the participants in a transaction cannot falsely deny later that it occurred or was authorized
- *Availability:* ensuring that services provided by the secure infrastructure are never disrupted for long periods of time, despite human error or natural disasters
- *Scalability:* ensuring that the infrastructure can scale as the numbers of individuals, applications, networks, and organizations grow over time

Can you be sure your applications are secure over the Internet?

The CSS products offer a complete system for cryptography, certificate management, and directory management services for enterprises and domains of all sizes. Our solution includes the software, hardware, and services for the CA, individual users, applications, and commercial organizations to process secure business transactions.

Implementing step 1

In our example, the chief security officer, Loren Gaine, identifies StarGazer's issues: "We need to provide a secure way for our employees, retirees, and vested former employees to access their accounts, process transactions, and make changes to their retirement portfolios. Because our application will be open to retirees and former employees, we need to make it available beyond our intranet. But by making the application available on the Internet, we run the risk of hackers breaking in. We need to prevent them from gaining entry and changing the data or emptying our accounts, by implementing tight security controls. Because of its combination of software and hardware cryptography, we think the Compaq Certificate Security Solution product family is the best way to secure an Internet application from unauthorized access."

Implementing step 2

In our example, Loren Gaine identifies those using the secured retirement application as follows: "Our employees in the United States, England, Japan, Brazil, Sweden, and Australia all need to access their retirement accounts to choose funds and change allocation percentages at their convenience. In addition to serving all of our current employees, we want to make this application available to our retired employees globally, 24 hours a days, 7 days a week, and 365 days a year."

Step 2: Define the user requirements

Who will use your secure application? Your employees? Trading partners? Local government? Customers? Suppliers?

Will it be used internally through an intranet or externally through the Internet or a virtual private network (VPN)? For which countries will you need to implement PKI-enabled applications? How often will users access your application? Do they need 24-hour global access?

Step 3: Evaluate the security of your existing application

When evaluating the security of your existing application, you need to answer questions such as

- Does the current application security align with your organization's security policies?
- Do you need to review and update your security policies?
- How is security currently implemented with respect to the application, 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 application going to change in an Internet, intranet, or extranet environment?
- What types of commerce, communications, and information access transactions must be secure?

After evaluating your existing security measures, you will be able to determine whether they meet your needs. If they do not, develop a plan to enhance your security based on the requirements you identified in step 2.

Step 4: Establish security policies and procedures

Develop 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 who will be granted access, and then decide which applications and information they will be authorized to access.

In addition to your own policies and procedures, you must be aware of your government's trading policies. They are intended to prevent individuals, organizations, and governments deemed to be untrustworthy from being granted access to sensitive information or conducting unauthorized electronic commerce and communications.

Implementing step 3

StarGazer's officers evaluate the security of their existing application by answering the following questions.

What type of security exists for our retirement application? **Currently, we have Internet access with firewalls. Our internal system is on a private network that provides security based on a user ID and a 10-character password. Our network is a heterogeneous environment consisting of open, standards-based computing platforms.**

What types of transactions must be secure? **We need to provide a secure mechanism for our employees to view their accounts and make deposits, withdrawals, and transfers between their accounts.**

What type of security do we need for the current application, including the database? **Our certificate directory is where we will store our digital certificates, lists of revoked certificates, and other data associated with our secure retirement application.**

What type of security do we need for the network? **We need to prevent unauthorized access to our retirement application and user accounts over the Internet. We need administrative software that can be accessed securely over a network or on the workstation that hosts the certificate management services. We need software that enables our administrators to add and delete users, enable and disable our users, revoke certificates, perform key recovery operations, and set default certificate and key lifetimes. We need a way to let multiple administrators simultaneously access the certificate management services over the network so administrators for our accounts in different countries can be close to the users they administer.**

Implementing step 3 (continued)

What type of security do we need for client machines? **We need to protect our employees' information and transactions by providing them with software that enables them to encrypt and decrypt their transactions, identify themselves with a digital signature, verify digital signatures of others, and receive key updates on a regular basis. To make it easy on our employees, we want these features to be transparent to them as well as easy to use.**

After evaluating their existing retirement application, StarGazer's officers realize that the existing security measures do not meet all of their needs. To secure its application, StarGazer decides to use public key technology provided by the Compaq CSS family of products to ensure that the company's retirement application meets its security requirements.

Implementing step 4

In our example, the chief security officer drafts the policies and procedures to set a standard for how the application can be used and how the certificates will be managed.

Appointing security personnel

Security begins with the appointment of highly capable and trusted individuals to be the security officers and administrators. You need to decide how many people are needed and who will be named to the security staff. These people will have access to the CA facilities that you will establish. They will be responsible for the certificate, key, and directory management services and for maintaining the trust in your CA's operation. (See step 9 for more about CA establishment.) Your key personnel will probably include

- *A security site planner:* This person is responsible for all aspects of the setup and installation of the CA as well as some post-installation activities.
- *Security officers:* We suggest having at least two people who are responsible for maintaining the security of the CA system and setting the security policies. They are also responsible for keeping the directory up to date, safeguarding it from unauthorized access, performing regular backups, and maintaining user entries.
- *Administrators and registration agents (RAs):* These people are responsible for registering new users and deleting and maintaining user accounts.

The security officers and administrators will determine the level of security needed, evaluate liability and risk, and determine who will be granted access. Here are some questions your security officers need to consider:

- What levels of security are needed?
- Who will be granted access?
- Which applications need to be secured?
- What procedures are necessary to provide sufficient authentication?
- What are the security requirements for CA facilities?
- Who will receive certificates?
- What does the certificate guarantee?
- What is the limit of liability?
- How do you protect yourself from liability and prove due diligence?
- What are the security policies? How are the policies enforced?
- How do you secure the components of the security system?
- How many officers are required to approve certain activities?
- How do you authenticate users? Are there levels of authentication?
- How do you distribute credentials to the user?
- Do you need to cross-certify with other CAs? What is the implication of cross-certification?
- What functions require multiple approvals?

- How important is availability? Define the business cost in terms of dollars per unit of service downtime. Define the business cost of rebuilding the secure infrastructure in the event it is compromised.
- How important is scalability?
- What contract issues need to be considered?
- Are confidentiality agreements needed? At what level?
- What other legal issues exist?
- How will you educate your users about security practices and policies?

Establishing your certificate policy

Security officers select or develop and maintain your certificate policy. This policy, as defined in the X.509 standard, is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

In the future, industry forums will establish certificate policies for their respective business sectors. This will allow security officers to simply adopt or modify a model certificate policy from an industry association. Until then, Compaq and our partners can help you develop a certificate policy for your company or organization.

The certificate policy must be approved at the appropriate level of the organization. For example, the officers of the corporation should approve a corporate certification policy, and department managers should approve departmental certificate policies.

The certificate policy will be used by external organizations required to process certificates issued by your CA as well as by those engaged in a cross-certification agreement based on a certification practice statement (CPS).

Step 5: Define a certification practice statement

Any organization establishing a secure application and a CA must publish a CPS. The purpose of this document is to provide a detailed explanation of what the CA's practice will be, including service offerings and certificate life-cycle management.

The CPS describes the measures that the CA will employ 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, your employees, customers, suppliers, and trading partners can use it to assess the trustworthiness of your CA.

The certificate policy generally states *what* is to be adhered to, while the CPS states *how* it is adhered to.

Currently, there isn't a standard format for either a certificate policy or a CPS. However, a framework has emerged. This framework includes the following list of policy components that you need to consider when developing a certificate policy and CPS for your organization's CA.

Implementing step 5

In our example, the chief security officer, Loren Gaine, drafts the CPS, covering all of the relevant issues.

Community and applicability

The CPS identifies the

- Certificate policies to which it applies
- Order of magnitude of the user community that it serves, including the number of CAs and RAs
- Standards to which its external interfaces conform
- Name form used in its certificates
- Name space (for example, X.500 subtree) in which the CA intends to issue the certificates
- Applications for which the issued certificates can be used (for example, electronic mail, retail transactions, contracts, travel orders, and employee benefits)
- Applications for which use of the issued certificates is restricted
- Applications for which the issued certificates cannot be used

Contact details

The CPS includes the name and mailing address of the CA responsible for the registration, maintenance, and interpretation of the certificate policy or CPS. It also includes the name, e-mail address, telephone number, and fax number of the CA contact person.

Identification and authentication

The CPS describes the procedures used to authenticate the identity of all principals, including the security officers, administrators, registration agents, end users, applications, and network devices. It also provides information on the security privileges given to each of the principals.

Key/certificate management

This component describes how the key/certificate life cycles of each of the principals are managed. Additional components in the area of key management may include

- Certificate signature/verification algorithm
- Certificate validity periods
- Data signature/verification algorithm
- Data encryption/decryption algorithm

Local security practices

Local security practices are those that relate to the environment in which the major components of the PKI operate, including

- Physical controls
- Personnel controls
- Procedural controls

Technical security practices

Technical security practices deal with the required technical standards for the components of the system, including

- Computer security controls
- Network security controls
- Cryptographic module engineering controls
- Facility security controls

Operational practices

These describe the operating procedures for the security officers, administrators, registration agents, and end users that include

- Registration of unique "distinguished" names
- De-registration and revocation
- Key compromise
- Dismissal for cause
- Certificate update
- Disaster recovery
- Private key recovery
- Audit practices
- Nondisclosure of personal information

Legal provisions

The certificate policy may explicitly identify the statutes to which the PKI must conform, including data protection, privacy, access to information, and legal wiretap legislation. The certificate policy also states the purpose and constraints for use of the private and public keys or certificates.

Legal provisions must be included for each of the following:

- CA obligations
- Certificate user obligations
- Principal obligations
- Acceptance of limitations
- Informed consent

Cross-certification agreements

Independent organizations that wish to use one another's certificates should establish cross-certification agreements. An agreement between organizations should formally commit both parties to adhere to the CPS and clarify how disputes will be arbitrated in the event that loss is incurred as a result of failure to comply.

Certificate and certificate revocation list profile

The CPS includes a profile of the certificates, the certificate revocation lists (CRLs), and the directory schema. The profile should indicate which certificates and CRL extensions are present, whether they are marked critical or noncritical, which optional fields are included, what value ranges are allowed, and what action is expected of verifiers in response to any nonstandard extensions. The location of these attributes in the directory should be described.

CPS administration

The CPS describes the procedures for development and maintenance of the CPS document. These should include the procedures for approving the CPS and the nature of changes that will lead to the issuance of a new policy identifier.

Step 6: Hire and train your security personnel

Most likely, each region in which your security system is deployed (for example, Asia-Pacific or Europe) will have its own administrators who will perform background checks in several countries. The number of officers and administrators needed depends on your company's practices, as well as the mandates of the individual countries.

First, establish clear lines of authority and responsibility among your security personnel. Also, implement employee background checks and clearance procedures, training requirements, sanctions for unauthorized actions, and bonding requirements for contract personnel.

In addition to hiring and training your administrators, decide how you are going to handle the departure of your officers and administrators, including firings, workforce reductions, deaths, and retirements. Similarly, if an individual user becomes a security threat, you will need to revoke that person's passwords and certificates immediately. Make sure these processes are covered in your CPS. Also, carefully audit any changes made to your applications, to ensure compliance with corporate practices.

Document the tasks that each officer and administrator must do on a daily basis. For example, your personnel should know the standard backup and recovery procedures.

Plan to train your security officers and administrators in both full-scale and limited disaster-recovery procedures. A full-scale recovery procedure is necessary, for example, if the CA computer room burns down or is flooded.

A limited recovery procedure is necessary when only part of the network's trust is broken. For example, you would need a plan of action if a particular subset of certificates were to become compromised. In that situation, you might limit the damage by selectively shutting down only a portion of the network.

As another example of limited recovery procedures, what if there is a problem with a bank's transactions in a particular country? Its security officers and administrators must know what to do. Most likely, they would disable all of the bank's credit card transactions in that country while allowing its transactions in all other countries to proceed.

Step 7: PKI-enable your applications

An application developer must modify existing applications so that they can use certificates and cryptographic services. This type of modification is referred to as PKI-enabling applications.

The location of the source code determines who will PKI-enable the application. Some applications are developed in-house; others are developed by vendors. Whoever has control of the source code is the one responsible for PKI-enabling the application.

Make your programming staff aware of any software modifications that will be taking place on the system. You can also begin training them on how to make changes to an application using any available toolkits and how to integrate your directory. After modifying your application, you may need to revise your security policies, practices, and procedures to reflect and align with those changes.

Step 8: Integrate your directory

PKI components (such as the CA, RA, 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 LDAP/X.500-compatible directory or extend the schema of your existing directory. You will need a directory structure that supports certificates (X.509 v3) and certificate revocation lists (x.509 v2) for authentication and authorization of participants; it must also provide for the collection of information that provides evidence for nonrepudiation.

Implementing step 6

StarGazer has already identified Loren Gaine as chief security officer and Emilia Edwards as security site planner. Next, StarGazer must identify the administrators who will register new users and delete and maintain user accounts. The company decides to appoint Jean Moore and John Chen as security administrators.

Implementing step 7

Since the retirement application in our example was developed in-house, StarGazer's developers will make the modifications. If necessary, a security officer will then revise the security policies and procedures as well as the CPS.

Implementing step 8

In our example, Loren Gaine assigns John Chen, one of the security administrators, the task of extending the current directory to support certificates. Because the existing directory is X.500-compatible, John easily integrates LDAP access, the schema for X.509 v3 certificates, and X.509 v2 certificate extensions with StarGazer's existing directory.

Step 9: Set up a certification authority

Third-party trust refers to a situation in which two individuals implicitly trust each other although they have not previously established a business or personal relationship because they each share a relationship with a third party. That third party vouches for the trustworthiness of the two people or enterprises.

The element of trust begins with a third-party certification agency—the CA. The trusted agency's central responsibility is certifying the authenticity of users. The CA is a critical component of PKI because it provides assurance that the participants involved in electronic commerce, communications, or information access activities 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

Before setting up a CA, you need to decide whether to establish an in-house CA (that is, a department responsible for buying and operating the necessary hardware and software) or outsource these services to a trusted third party. When choosing between using an in-house CA or outsourcing to a third party, consider the following issues:

- *Confidentiality.* When outsourcing, you may have to provide the third party with access to sensitive information about employees, suppliers, and trading partners. However, you may already have agreements with your employees, suppliers, and trading partners that do not allow for such disclosure.
- *Availability.* Critical encrypted information is vulnerable to loss if the corresponding decryption key becomes lost or corrupted. You need to be sure that a method for decryption is always available. Keeping this method in-house gives you more control and assurance that decryption will be possible and that it won't be misused.
- *Control.* Because your PKI-enabled application depends upon the availability and integrity of the public key infrastructure, you need to be sure that it continues to operate correctly. Some of the most critical operations for a PKI are its mechanisms for revoking privileges, issuing and distributing CRLs, and auditing and archiving records of operations. You need to pay careful attention to these critical operations when determining whether to establish a CA in-house or outsource to a third party.
- *Liability.* When using an in-house CA, normally the issue of liability does not arise. However, if you elect to trust the issuing of certificates to one of your trading partners, you can control the assignment of liability with a cross-certification agreement. If you have outsourced your certification services to a third party, you must address what will happen if the service provider withdraws its service for some reason (for example, should they go out of business).
- *Quality of service.* When using an in-house CA, you have direct control over the quality of the service through which the certificate is issued and managed. You can immediately deal with any problems that arise. In contrast, if the service is outsourced, you lose direct control. Therefore, it is imperative that you obtain service quality guarantees and that you demand periodic, independent audits of those guarantees.

Implementing step 9

In our example, since StarGazer's retirement application is used for current and former employees and retirees—a finite number of persons well known to the corporation—it is relatively easy for the company to be its own CA. Therefore, StarGazer has decided to set up an in-house CA.

Step 10: Secure your certification authority facilities

For CA operations, your computer facilities must be kept in a highly secure environment. Carefully select the 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.

Determine what security controls are necessary for network and client machines. Since the certificate manager system is the nerve center of the Certificate Security Solution, it is critical to isolate it from unauthorized access, both physical and electronic.

Decide where to house the computer that contains the CA software. Isolation of physical access requires a secure location. The CA systems should be housed behind locked doors that are restricted to all but a few select and highly trusted people—the security officers, the administrators who are assigned to this function, and the system administrator. Any personnel accessing the area housing the CA systems should always be accompanied by one of the security officers.

Isolation of electronic access requires that steps be taken to prevent unauthorized people from logging onto the system. Additionally, take the following steps to improve electronic security:

- Configure the operating system to restrict all remote system logons.
- Protect the cables that connect the certificate manager system to the other system components from unauthorized access.
- Grant root access to only a very few trustworthy people.
- Restrict access to system password files.
- Install routers or firewalls between the network and the certificate manager system.
- Use Atalla cryptographic processors from Compaq for secure hardware encryption support.

Implementing step 10

In our example, Loren Gaine assigns Emilia Edwards, the security site planner, the task of securing physical and electronic access to the CA systems and facilities.

Implementing step 11

In our example, after successfully implementing the PKI-enabled retirement application, the auditors confirm that the security objectives have been met.

To protect your internal computer network from hackers and eavesdroppers, you should implement the latest firewall and/or VPN technology.

Acting as a security gateway, a firewall can be used to limit internal network systems from establishing connections to the Internet and 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 detect attempted security breaches.

Most importantly, consider creating backup CA facilities that you can deploy should the primary facilities be destroyed or compromised for any reason.

Step 11: Run preliminary tests and a pilot

Once you have set up your system, you are ready to run a preliminary test to make sure everything is operating properly. First, have your quality control team test the hardware to make sure it is functioning properly and securely. Test the CA systems, networks, security, and the PKI-enabled application for several weeks.

Test the software to ensure the integrity of the transactions. Analyze and report any glitches. Include disaster-recovery procedures in your test.

Implementing step 12

Terrance Talbot, CIO, says to Loren Gaine: "I'm really pleased with how you've implemented the retirement application. The end users are extremely happy, and you did it all on time and within budget. Now that we have that system set up, we can start looking at PKI-enabling our medical, dental, and salary administration accounts. And marketing has been after us to implement electronic commerce...."

After you have thoroughly tested the system and verified that both the hardware and software are operational and your auditors have confirmed that the system is secure, you should run a pilot test with a small group of users, preferably employees. Let them know this is a pilot. Allow approximately three to nine months for the pilot program to run.

Step 12: Train users and launch your secure application

Once you have successfully completed the pilot stage you will be ready for full production mode. You may want to do a review of the pilot and assess any changes you want to make at this time. The rollout of the complete system can be made available to your entire user group or any subset that you deem appropriate.

Before final launch of your application, you need to fully train or provide tutorials for the following people:

- End users
- Customer care staff (those responsible for handling customer inquiries and complaints)
- Technical support (those responsible for handling technical questions when problems with the system arise)
- Public relations
- Marketing

You'll want to develop different training courses to address the requirements for each department.

Once your staff is fully trained, you can begin registering end users and issuing keys and certificates. Begin by registering only a small subset of end users, perhaps in one city. Then analyze the results of your implementation to make sure everything is working properly and securely.

What's next?

After your first PKI-enabled application is up and running smoothly, you can think about adding other PKI-enabled applications. Or, if it is appropriate, you can begin to plan broader deployment of the application or expansion to users in other countries.

The Compaq CSS advantage

The CSS product family provides an infrastructure that makes it possible to implement security for a wide range of applications that use certificates to authenticate users, including electronic commerce, communications, and information access over the Internet.

The following is a summary of the key features that the CSS product offers:

- Complete, integrated, end-to-end solution
- Reliable, scalable, and high-availability certificate management services
- Reliable, scalable, and continuously available LDAP/X.500 directory management services
- Toolkits to PKI-enable applications (for Microsoft® Windows NT®, UNIX®, and *Compaq NonStop™ Himalaya* systems)
- Support for smart cards and biometrics
- Ability to use root, hierarchical, and peer-to-peer certificate structures
- Use of standard instead of proprietary cryptographic software with inclusion of encryption and decryption capabilities (for example, RSA BSAFE)
- Hardware encryption support, such as with the Compaq Internet Security Processors (ISPs)
  - Security (root key is stored in the hardware)
  - Performance (off-load cryptographic processing from host)
- Applications
  - X.509 certificates: multiapplication certificates (MACs), Secure Sockets Layer (SSL), Secure Electronic Transaction™ (SET), and VPNs
  - Multiple security levels
  - Transparent key recovery with due process

Complete, integrated, end-to-end solution

More often than not, you will need a complete solution that includes hardware security and services as well as cryptographic software. With the CSS product family, you can choose a complete solution rather than just a software product.

The CSS product allows secure exchange of information among Compaq *NonStop*™ systems and Windows NT and UNIX–based systems. Large organizations with multiple operating systems can use the CSS product seamlessly.

The CSS product also works with Atalla cryptographic coprocessors from Compaq, making certificates even more resistant to tampering or modification than when used with only software cryptography.

Compaq has many service plans to choose from and offers upgrade licenses so you can add more users as your business grows.

Reliable, scalable, high-availability certificate management services

The administrative environment must be an accessible and reliable environment that can scale over time and support the following operational functions:

- Register users, applications, and network devices
- Issue, renew, or revoke keys and certificates
- Publish certificates in a directory

The CSS Certificate Manager is designed to handle these functions in the most rigorous CA service provider environments ever deployed.

Running on Windows NT, CSS Certificate Manager ensures the highest levels of performance, reliability, scalability, and data integrity for your CA operational environment.

Reliable, scalable, continuously available LDAP/X.500 directory management services

Your solution must be easily scalable to handle the number of users you need in today's environment and beyond, with hardware and software reliability.

The CSS Certificate Directory is an LDAP/X.500-compliant directory that contains the names and other information associated with people in an organization. By supporting the LDAP/X.500 recommendations, CSS Certificate Directory can store information from other directories that comply with the standard.

Ideally suited for organizations that issue and manage certificates for a large number of users, CSS Certificate Directory can support millions of people. No other directory service based on a PKI can match the scalability of CSS Certificate Directory.

Running on Compaq *NonStop™ Himalaya* servers, CSS Certificate Directory ensures the highest levels of performance, reliability, scalability, and data integrity for your critical applications. You also have the option of choosing a Windows NT Server or Tru64 UNIX-based LDAP/X.500 directory.

Toolkits for Windows NT, UNIX, and Compaq *NonStop™ Himalaya* systems

Toolkits allow application developers to develop or enhance their applications with PKI security services. The CSS family offers several toolkits as part of its Security Services for Applications product suite. These toolkits provide high-level application programming interfaces (APIs) to user applications for encryption and decryption, digital signatures, verification, key management (automatic and transparent), and certificate management services.

The CSS product offers a generic S/MIME toolkit that allows application developers to incorporate S/MIME functionality within existing or planned applications. Major mail systems such as Microsoft Exchange, cc:Mail, Eudora, and Lotus Notes are supported by the CSS product via third-party plug-ins.

The CSS product also offers generic session and file toolkits that allow application developers to enable an organization's business applications with PKI security services. CSS file and session toolkits are supported on the following platforms: Windows NT, UNIX system, and Compaq *NonStop™ Himalaya* servers.

Applications that can be PKI-enabled include government services; Internet banking, shopping, and payments; insurance applications and claims; contracts and deeds; notary services; medical services and records; purchasing contracts; EDI; secure e-mail and messaging; and securities trading.

Support for smart cards and biometrics

The CSS product makes it possible to implement smart-card technology to enhance security. A smart card can securely store the private key, which can never be viewed by an intruder. By securely storing keys on a smart card instead of on a desktop, you offer end users even more protection against unauthorized access. Additionally, smart cards provide portability of keys so that users can move from system to system. Biometrics (fingerprints) can also be used to authenticate a user's access to a client device.

Ability to use both root, hierarchical, and peer-to-peer certificate structures

The CSS product family offers the flexibility for you to use one CA (root), two or more different CAs (peer-to-peer), or a combination of both models to form hierarchical structures. If your application serves a known, limited community of users, you will only need one CA. The SET protocol is an example of a CA with a hierarchical structure (root, brand, geopolitical, and end-entity CA). However, if you have several applications that need different types of certificate support, you may want to use different CAs for each application.

A peer-to-peer certification authority model is a standalone CA that uses cross-certification to create multiple CA domains. These peers could be within a corporate entity (for example, a department or division) or between totally unrelated CAs.

Cross-certification enables unrelated, distributed certification authorities to communicate with one another and check private information about certificates for secure electronic commerce, communications, and information access. For the successful operation of a peer-to-peer model, it is assumed that the various standalone CAs adhere to similar proprietary or open management standards and operating policies, so that each CA can "trust" the certificates issued by the other CAs.

Standard instead of proprietary cryptographic software

It's important that your security system use industry standards so it can interoperate with other vendors' products. The CSS solution components use many of the existing security industry standards, including

- RSA and DSA public key algorithms
- DES, 3DES, CAST, and RC2 symmetric key algorithms
- MD5 and SHA message digest algorithms
- RSA BSAFE software (used in Atalla hardware units configured for the CSS product)

Hardware encryption support

The CSS product is tightly integrated with the Compaq ISPs—high-performance, hardware-based cryptographic devices designed to handle large volumes of certificate-based transactions. Using the CSS product with Compaq hardware provides improved security as well as higher performance than software-alone cryptography.

The high-speed Compaq ISP encryption engines are built for the cycle-consuming task of data encryption. This frees up your application server so that you do not have to add costly server capacity.

The Compaq ISPs do all cryptographic processing within the safety of their physically and logically secure casing, preventing anyone from ever seeing your data in readable clear-text form. The CA root key is stored in the Compaq hardware.

Applications

The CSS product family supports

- X.509 certificates (MAC, SSL, SET, and VPNs)
- Security levels (four)
- Transparent key recovery with due process
- ISV applications enabled with PKI

The CSS Administrative/Registration Agent software registers new users. However, the activities involved with recording registered information on the CSS product are securely under control of the software.

If a user forgets his or her password, the security administrator can easily provide a new identification number and authorization code. The CSS Security Service for Applications software recovers a user's encryption key pairs and automatically creates a new signing key pair.

Conclusion

When you choose the CSS product familiy, Compaq provides you with everything you need to implement your PKI-enabled applications securely.

Once you have identified your important issues, defined your requirements, and evaluated your security needs, you are ready to establish your security policies and procedures, draft the CPS, and select and train your security officers and administrators. You can then PKI-enable your applications, integrate your directory, and physically secure your facilities. Finally, you can run a preliminary test using test data.

After using test data to establish that your hardware and software are operational and secure, you launch your application on a subset of your end users. Your post-test analysis will determine whether you are ready for the next step. At that time, you can broaden the deployment of your system to other users and PKI-enable other applications on your system.

Compaq specialists 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. These include

- PKI-enabled solutions (in-house, private label, and virtual CA certificate and directory management functions)
- Client and server toolkits to PKI-enable applications
- Firewalls, proxy servers, and remote access servers
- VPNs
- Secure transactions and communications (using SSL and SET standards)
- Intrusion detection and analysis
- Smart cards and biometrics
- Virus protection software

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

99-0718

COMPAQ