PrivyLink Cryptographic Key Server*

Tamper Resistant Protection of Key Information Assets for Preserving and Delivering End-to-End Trust and Values in e-Businesses

September 2003

E-commerce technology is today leading a paradigm shift, enabling companies to capture additional revenue, improve customer service, lower sales and customer acquisition costs, improve time to market, enhance distribution, and streamline communications among employees, customers and business partners.

Data security on a public network, such as the Internet and the Wireless Internet needs to be more stringent and sophisticated than those that has been used for the private network. However, the strength of all cryptographic algorithms is based on the secrecy of the keys. Anyone holding the keys will have complete access and knowledge to the secret protected.

Traditionally, cryptographic server-side secrets are stored within the web server or application server, either in clear or scrambled. As it is well known that the web server is the most often attacked component in the entire network. It is also known that a big percentage of the frauds are done from within, i.e. by the employees or associates of the organisation. This makes software-based solutions vulnerable, increasing the risks of businesses in such any undertaking relating to the electronic world.

With hardware-based approach, all cryptographic processing takes place within the safety of a physically secure environment. This hardware encasement safeguards all cryptographic algorithms and keys against unauthorised access, disclosure, alteration, duplication, and substitution.

A hardware-based cryptographic solution assures the high confidence and security that Internet commerce requires. Software-based security products

* The information contained in this document represents the current view of PrivyLink International Ltd, and is correct as of the date of publication. This document is for information purposes only. PrivyLink International Ltd makes no warranties, express or implied, in this document. Information in this document is subject to change without notice, and does not represent a commitment on the part of PrivyLink International Ltd. PrivyLink International Ltd cannot guarantee the accuracy of any information presented after the date of publication.

decrypt sensitive data in unsecured memory, displaying both keys and algorithms in readable form, which makes the data vulnerable to cyber-pirate attacks.

PrivyLink's Cryptographic Key Server adds hardware-based security functionality to Internet, Intranet, Extranet, and enterprise infrastructure applications. PrivyLink technology embedded in hardware safeguards sensitive private key information with strong physical and logical security, and offloads computationally intensive public key operations from the server. These products work with your application to eliminate the significant bottlenecks and risks associated with software security processing.

This white paper provides an overview on the Cryptographic Key Server, describing the architectural design, the features available and the scalability of the Key Server.

Overview

Cryptographic Key Server Architecture

The design of the Key Server (KS) adopts the approach of multi-segment architecture for handling key service operations and administration. All service operation calls are initiated from one segment and all administration calls are initiated from another segment. This creates a natural separation of in-band (production) and out-of-band (administrative) traffics. With such a separation, administrators can continue to perform administration of the key server even though the production segment might be congested with production traffics.

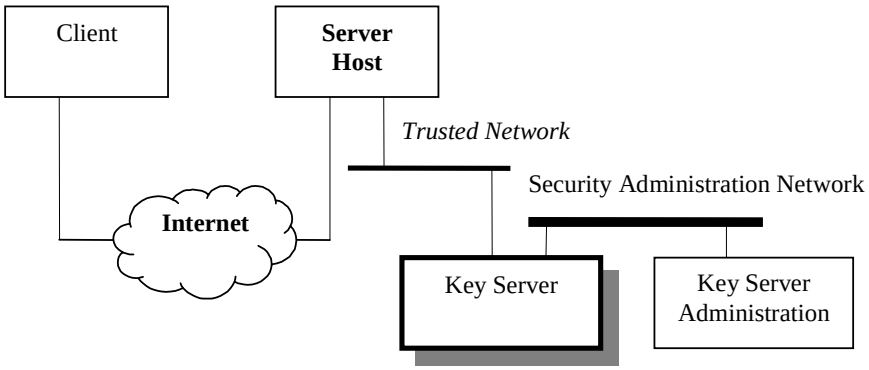

Figure 1: Overview of the Key Server architecture

With the multi-segment key server architecture, the KS is connected to the server host via a ***trusted network segment*** so that security management can be greatly simplified. In contrast to the traditional approach of serial connection between the server and the KS, the use of a trusted network segment simplifies maintenance and enhances scalability and performance of the key management system.

While the role of the KS is to provide a secure environment for cryptographic operations needed by server hosts, the administration of keying information is controlled by the Key Server Administrator (KSA) module. KSA is connected to KS securely via ***another trusted segment***

dedicated for security administration. With the multi-segment approach for key server administration, more than one key servers can be managed by KSA; hence allowing transparent installation of back-up or concurrent key servers to serve a cluster of hosts.

Cryptographic Key Server Applications

This section briefly illustrates the deployment of the Cryptographic Key Server in some typical application environment.

Banking and e-Banking

In the banking environment, the Cryptographic Key Server can be used to generate the Personal Identification Number (PIN) necessary for customer identification for ATM. It supports PIN Authentication and PIN Change meant for Electronic Banking and other banking applications too.

Credit Card and Smart Card Production

The Cryptographic Key Server is suitable for use for card production. It provides the secure means of generating cryptographic card values, as well as securely generating PINs and PIN mailers. The cryptographic values required for Smart Cards can also be generated by the Key Server for loading into the cards.

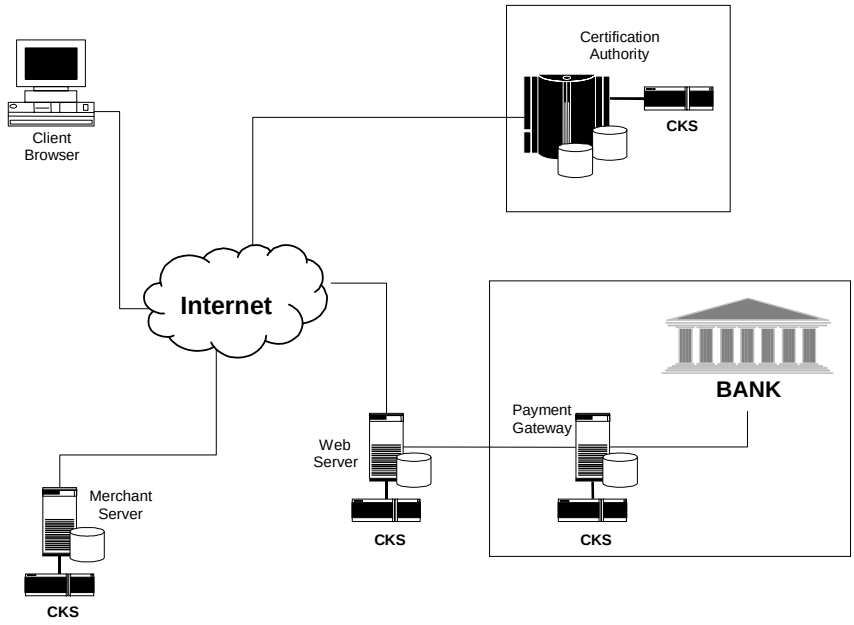

Figure 2: The Cryptographic Key Server in a typical electronic commerce environment

Figure 2 illustrates the roles of the Cryptographic Key Server in a typical electronic commerce environment.

Public Key Management for Electronic Commerce

The Cryptographic Key Server brings the most advanced security and the fastest processing speed to Certificate Authority (CA) applications for trusted third parties and CA solution providers. The Cryptographic Key Server reduces server bottlenecks by functioning as a cryptographic co-processor for key generation, certificate generation, certificate and signature verification, signing, and hashing. It physically and logically isolates cryptographic operations from the server system applications, ensuring the integrity of data, keys, and algorithms.

Secure Electronic Transaction (SET)

The Cryptographic Key Server is the superior solution for Internet credit card transactions, offering the fastest processing available, strong security and a direct bridge to the bank payment network. It easily isolates private customer information intended solely for the bank from information intended solely for the merchant, to meet the demanding requirements of the Secure Electronic Transaction (SET) protocol.

Features and Benefits

The Cryptographic Key Server is a tamper-resistant cryptographic device designed and developed to meet key requirements for providing host-side cryptography and managing server-side secret keys used for online transaction. While the standard functions available in the Key Server satisfy the needs of most clients, the Cryptographic Key Server can also be

customized to meet unique requirements. The following highlights some of the Key Server features:

FIPS PUB 140-1 Compliant

The Cryptographic Key Server is built according to the FIPS PUB 140-1 standards. The tamper resistant features ensure that all secrets stored within this hardware security box are safe and secure. The Cryptographic Key Server can provide higher level of security much needed by organization for their mission-critical operations.

Built-in RSA Public Key Support

The Cryptographic Key Server built-in RSA Public Key Support enables any host system to perform Public Key Cryptography and the "Key-Select" option enable you to select RSA key lengths from 512bits up to 2048bits. This feature allows the Cryptographic Key Server to cater to different key lengths and different functions. In addition, it protects your technology investment as the industry increases key length requirements to keep up with increased threats.

Flexible Key Management

The Cryptographic Key Server supports Flexible Key Management to meet diverse application's security requirements. In practice, the security offered by any application is only as good as the key management designed for it. The Cryptographic Key Server offers a variety of strong key management schemes such as Master/Session Key Management, Derived Key Management and Public Key Management.

The Cryptographic Key Server supports the generation and management of PIN used in most ATMs and Credit Card too.

Secure Key Storage

The Cryptographic Key Server maintains a table of cryptographic keys in its main memory and all keys stored within are encrypted by a master key. The master key in return, is stored in a PIN-protected smart card under the custodian of the security administrator. Any sign of illegal access will render the key table useless and the keys non-retrievable.

Key Escrow

The Cryptographic Key Server supports Key Escrow. This feature enables organization to perform key recovery, in the event of disaster, if required.

Key Server Administration

The Cryptographic Key Server provides several administrative capabilities that allow different level of security to be installed for administrating of the Key Server. It also provides capabilities for tailoring the administrative interface to the unique needs of each environment and for accommodating future upgrades to the Key Server.

Key Server Administration Module

The Cryptographic Key Server administration is done via the Key Server Administration (KSA) Module over a trusted and dedicated security administration channel. Communication between the Key Server and the KSA are based on proprietary protocols and requires some form of physical authentication to be carried out before and during the administration session. Any attempts to probe the Key Server without the proper authority will activate the security mechanism in-placed and render the information stored useless. The build-in enhanced authentication mechanism ensures that only authenticated administrator can perform the respective administration functions.

The available functions can be categorize under the followings areas:

- Administrative Services.
- Operation Services.
- Account Management.
- Shutdown Services.

The following diagram shows the KSA Interface for Administering the Key Server Operation Policy under the Administrative Services.

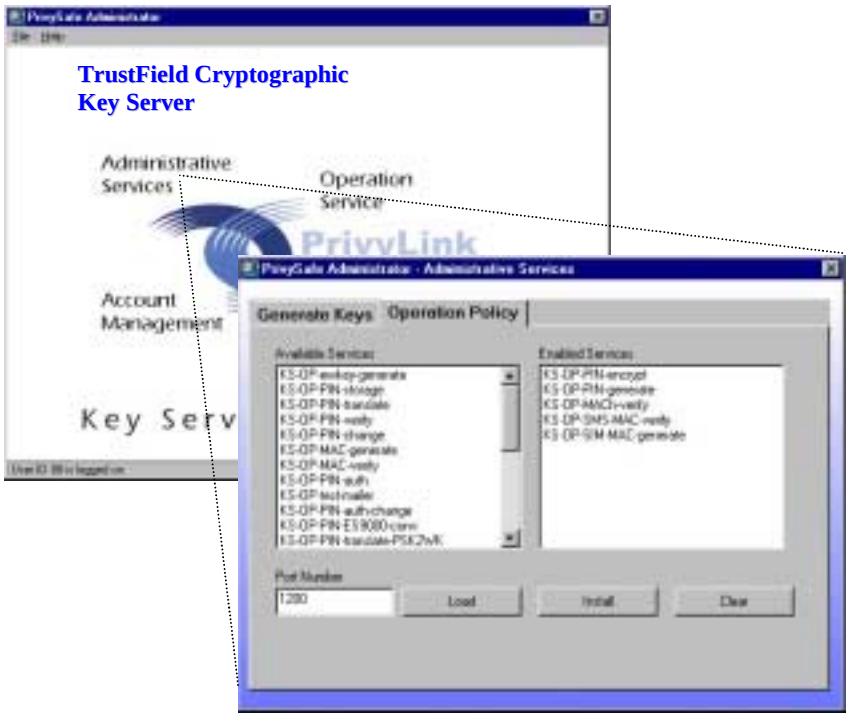

Figure 3: A look at the User Interface for the Key Server Administration Module

Role-based Administration

The default administration mode is Role-based. In the Role-based authenticated mode, any administration commands before execution requires the super user and the administrator keys to be in the correct position for the commands to be properly administered. With the right key inserted in the right position, the Key Server will recognize that the key holder is the authorized administrator and thus allowing the administrative commands to be carried out.

ID-based Administration

The Cryptographic Key Server also supports ID-based administration. In the ID-based authenticated mode, any administration commands before execution will requires the operators to enter their user identity and PIN for each administrative requests beside having the required keys in-placed. This "two-factor" based authentication mechanism enforces higher level of protection to satisfy organization's needs for higher security.

The ID-based authentication policy is compliant to FIPS PUB 140-1 level 4 standards.

Privileged Commands

The administration instructions are grouped into non-privileged and privileged commands. Non-Privilege commands are available to both the operators and super user and whereas the Privilege commands are available only to the super user. This hierarchy of privilege enables different levels of administration to be granted over a distributed system

and ensures that only the designated person can have access to the Key Server Administration. This also enhanced the manageability of the Key Server.

Scalability

The multi-segment architecture enhances the scalability of the Cryptographic Key Server by allowing flexible configuration of key servers to server hosts. One such configuration can be one server host connected to multiple key servers as shown in **Figure 4**. Another configuration can be multiple server hosts connected to a trusted network segment to share one key server as shown in **Figure 5**.

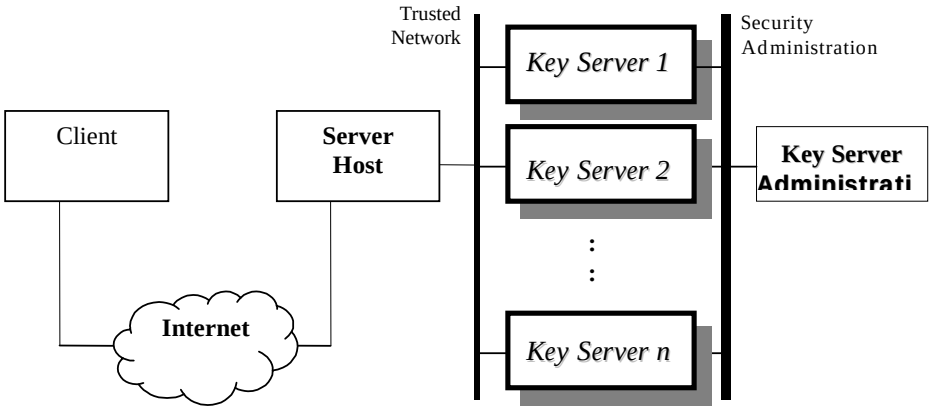

Figure 4: One Server Host connected to multiple Key Servers

Alternatively, there can be multiple hosts connected to multiple key servers as shown **Figure 6**.

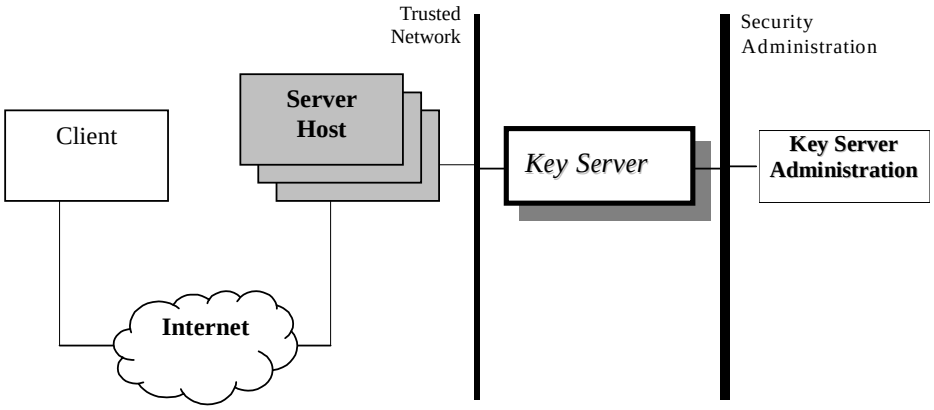

Figure 5: Multiple Server Hosts connected to one Key Server

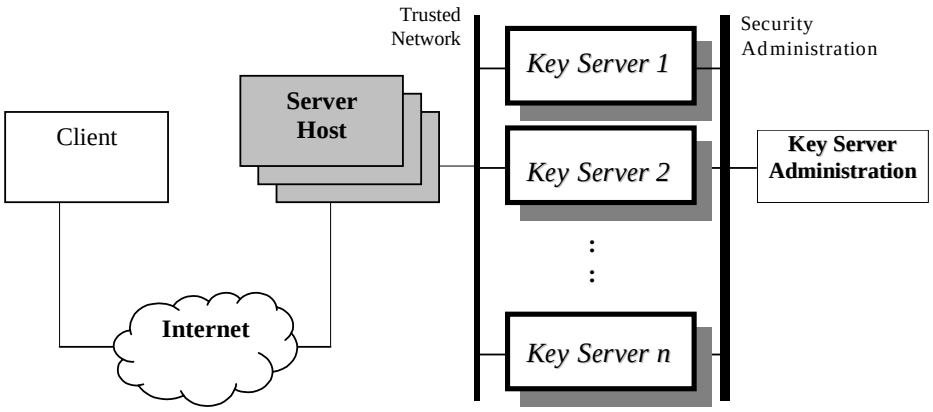

Figure 6: Multiple Server Hosts connected to multiple Key Servers

Administration Scalability

Administration Scalability refers to how easily the Cryptographic Key Server can be administered. From the above figures, only one unit of the Key Server Administration module is required for all possible deployment of the Cryptographic Key Server – Multiple-Hosts-to-Multiple-Key Servers, Single-Host-to-Multiple-Key Servers and Multiple-Hosts-to-Single-Key Servers.

Highlight on New Releases

The followings highlight some of the features that will be made available in the new release of the Cryptographic Key Server.

Hardware Crypto Card

The latest version of the Cryptographic Key Server featured a dedicated hardware crypto card that enhances the performance of all cryptographic operations, including all Public Key Cryptography supported such as digital signature, signature verification and others, e.g. RSA Key generation.

Summary

In order for organizations to compete effectively in today's business environment it is essential that they increase their use of networks, such as Internet, Intranet and Extranet. However, the increasing use of networks brings with it-increased vulnerability to network break-ins. Traditional software based security solutions protects the systems to a large degree, but hackers still manage to penetrate. Once compromised – whether internal or external – the break-ins can be costly.

The Cryptographic Key Server is a Secure Key Management Server that can greatly improve the security and manageability of the cryptographic functions for host-side components. With the use of the Cryptographic Key Server, organizations can continue to expand their use of networks

and better manage their risk, reducing the cost and development effort necessary to secure their electronic exposure and their investment in technology, thus maintaining their competitive edge.

About PrivyLink

Founded in 1997, PrivyLink is a response to strong industrial demands for high assurance delivery channel for electronic transactions, especially in the government and financial sectors. PrivyLink offers a comprehensive suite of software and hardware solutions to address end-to-end e-Security of today and tomorrow's businesses in the e-Commerce, e-Business, and e-Marketplace arenas.