Protexx Secure Office Server

Industrialized Security Solutions for Business Critical Applications

Protexx enables you with the ability to provide a "Secure Office Server" which is a turnkey solution for identity management and information protection.

- It includes our Protexx S.I.T.H data in motion security
- An enterprise firewall
- Secure mail services
- Secure file services
- Secure web back end services utilizing DCE (Distributed Computing Environment)
- Secure mysql
- Plus we can provide LDAP and single sign on capabilities.

Our HP server can be blind branded to you or your clients.

Many businesses today are connecting servers together into clusters, which are rapidly becoming the preferred configuration in demanding environments. You should consider clustering if your business requires any of the following:

- High application availability
- Data management and access to shared devices
- Improved performance
- Workload balancing and the ability to manage future growth incrementally
- Elimination of single points of failure
  For a smoother running business, Protexx secure clustering solutions give you one single point of control that integrates independent systems into a single, robust system achieving the highest level of scalability and availability.
  In many instances, the 'single system image' can be attained by simply consolidating multiple servers running the same application into one. This is even more feasible with the enhanced power and capacity of today's servers. Protexx will work with you to determine the best 'fit' for your operation.

Secure Office is a full spectrum of integrated security services implemented through a common interface to provide flexible, industrialized solutions of a scope and durability that is uncompromised by the limitations of integrating diverse products. Managed through any standard browser, Secure Office delivers a wide breadth of functionality and control ranging from primary certification services, VPN/firewall and PKI access control to workflow management tools for massive scale handling of users, certificates, network accesses, centrally managed encrypted storage, accountability auditing and directory services. Secure Office Server enables an organization to meet all U.S. federal guidelines for E-government initiatives, healthcare/insurance, nonrepudible digital commerce and the protection of confidential information in a full range of business/service environments.

The Protexx Secure Office Server is a flexible, industrialized solution for organizations that require high security with centralized administration to maintain the confidentiality and integrity of corporate data and personal information as well as to benefit from the advantages of connectivity with regard to cost savings, extended services to customers, and expanded business opportunities.

- Full spectrum, standard or customer-specific options for PKI authorities, certification profiles, data attributes, data input sources, publishing, auditing.
- Convenient end-user provisioning: smart card/role-based Single Sign On.
- Comprehensive audit history: users, cards, certificates, admin. accountability.
- Smart card authenticated, role-based encrypted file sharing.
- Centrally managed distributed partition encryption.
- Centrally managed distributed firewall: stateful inspection/packet filtering.
- Centrally managed IPSec VPN: Ethernet, Internet, modem, wireless.
- Smart card role-controlled administration through standard web browsers.
- Advanced management: role-based user provisioning, user self-service routines, and workflow definitions for massive scale operations.

Secure Office Server is provides comprehensive security services across a full range of heterogeneous computing topologies.

Secure Office Server avoids the inherent pitfalls of combining separate products with differing styles and limiting proprietary configurations by building the fundamental services into a single solution based on common component architecture to offer an uncompromised, integrated security system that is broad in scope and applicability.

Secure Office Server enables full compliance with all legal standards, recommended guidelines and legislated directives for the protection of

corporate data, non-repudible online transactions and confidential employee/customer information.

Secure Office Server is a full spectrum of integrated security services implemented through a common interface to provide flexible, industrialized solutions of a scope and durability that is uncompromised by the limitations of integrating diverse products. Managed through any standard browser, Secure Office Server delivers a wide breadth of functionality and control ranging from primary certification services, VPN/firewall and PKI access control to workflow management tools for massive scale handling of users, certificates, network accesses, centrally managed encrypted storage, accountability auditing and directory services. Secure Office Server enables an organization to meet all European Directive standards as well as U.S. federal guidelines for E-government initiatives, healthcare/insurance, nonrepudible digital commerce and the protection of confidential information in a full range of business/service environments.

Secure Office Server is the interface between the company's applications and the services that secure them. It provides a full range of security services, the support functions and administration system, and the interfaces to an organization’s business systems, work processes and computing environments. Simple menu choices accommodate a full spectrum of network / Internet topologies, central directories, PKI configurations and customer specific sources of data input such as mail servers, public directories or company databases containing information about employees, existing cards, certificates and status histories. Standard GUI operations are also provided for configuring factors that are specific to particular communities such as audit logging, warning flags, customized data attributes, custom certificate extension fields, etc. and for specifying the way that they are used within the PKI. Secure Office Server provides comprehensive, cost-effective manageability even in large scale applications by reducing routine administration with convenient user provisioning, user self service and workflow definitions for handling massive scale operations like company name changes or a dynamic turnover of keyholders and roles. Secure Office Server interoperates with other PKI-VPN installations by providing standard menu options for trust relationships, system subordination to existing PKI authorities, and automatic import of externally issued information about users, cards and certificate status. Secure Office gateway products do not require proprietary VPN clients and are interoperable with common gateways such as those provided by Cisco and Checkpoint. Secure Office Admin is protected by smart card role-based access control and invoked through a standard web browser from any location.

Secure Office Client (SOC)

- VPN client
- Digital signature
- Remote Logon
- Boot Protection
- Smart card logon
- Personal firewall
- Encrypted Archive
- Card handling
- Session handling
- PKI client
- Crypto services
- Data Store
- Web client authentication
- Smart card secured e-mail
- Certification Authority
- PKI Validator
- Virtual Private Network
- Distributed Firewall
- Role-based Single Sign On
- Encrypted DataSafes
- OCSP/ Time Stamp servers
- Secure Office Server active inactive
- Internal PKI
- Data Store
- Role Authority
- Audit server
- Web server
- Comprehensive management
- Embedded firewall

Secure Office Server

- PKI services
- Centrally administration of:
- EA Encrypted Archive
- ED Encrypted Disk
- EW Encrypted Web Archive
- Certification Authority
- Card Issuing System
- Secure Office Directory
- Critical Path
- Active Directory
- Netware Directory Service
- Public domain
- Administration
- DataSafe (network based)

- Remote Signature Support
- Time Stamp Server
- Online Certificate Status Protocol
- Validator
- CA
- CIS
- Dir
- DS
- RSS
- TSS
- OCSP
- Val

Secure Office Server is the interface between the company's applications and the services that secure them. It provides a full range of security services, the support functions and administration system, and the interfaces to an organization’s business systems, work processes and computing environments. Simple menu choices accommodate a full spectrum of network / Internet topologies, central directories, PKI configurations and customer specific sources of data input such as mail servers, public directories or company databases containing information about employees, existing cards, certificates and status histories. Standard GUI operations are also provided for configuring factors that are specific to particular communities such as audit logging, warning flags, customized data attributes, custom certificate extension fields, etc. and for specifying the way that they are used within the PKI. Secure Office Server provides comprehensive, cost-effective manageability even in large scale applications by reducing routine administration with convenient user provisioning, user self service and workflow definitions for handling massive scale operations like company name changes or a dynamic turnover of keyholders and roles. Secure Office interoperates with other PKI-VPN installations by providing standard menu options for trust relationships, system subordination to existing PKI authorities, and automatic import of externally issued information about users, cards and certificate status. Secure Office gateway products do not require proprietary VPN clients and are interoperable with common gateways such as those provided by Cisco and Checkpoint. Secure Office Admin is protected by smart card role-based access control and invoked through a standard web browser from any location.

...a broadly-based, industrialized solution for securing commercial business, police, military, health care, or public services...
... advances in management commensurate to the task of securing nationwide IT systems.

Certification Authority. Secure Office CA is a federal class root certification authority (CA) solution for organizations and public CAs. It is designed for organizations that want to own and operate the technology either as an end user solution or to provide services as a trusted third-party CA. A truly scalable system, Secure Office handles massive PKI demands with comprehensive management of users, cards, certificates, auditable histories and large-scale certificate storage.

Card Issuing System. Secure Office Card Issuing system generates strong RSA keys and formats industry standard (PKCS#15) smart cards from blank cards within a secure module, isolated from any network connections. In addition to significant cost savings compared to public vendor prices, CIS enables the cost-effective re-use of old cards and keeps the generation of the critical private keys secure within company walls. In house production of smart cards puts the process on the schedule of the owner organization for timely temporary cards, replacement cards and routine re-keying. An organization can own and operate the Card Issuing System either for in-house production of smart cards or to provide commercial services to other organizations.

Encrypted Archives. Encrypted Archives enable multiple users to share network stored encrypted data. This is an easy, cost-effective means of securing collaboration around shared encrypted information with automatic key handling. Encrypted files can be stored on common file/web servers for easy access while maintaining high security standards to achieve simple solutions without a fully encrypted network. Encrypted Archives are created and managed centrally with access assigned according to roles.

Encrypted Disk. Centrally managed disk encryption. An entire hard disk partition is encrypted and dedicated for all confidential files while system files remain in clear text. Encrypted Disk enables an organization to protect all confidential information while leaving system files unaffected so that machines can be serviced by normal routines without special procedures such as hard disk removal to protect information. Keys are created centrally and linked to the user's smart card by a role. A key can be accessed by multiple, differing roles so that in an open working environment with shared workstations, any user having any of the roles can access the encrypted disk partition.

Remote Signature Support. Regulation digital signature actually includes a compressed version of the material being signed but these materials are often generated on the fly by servers that are remote to the signer. For example, when a physician submits a prescription, it may be from any location. The server at the pharmacy creates the requested order and fowards it to the Secure Office Server. Secure Office locates the signer, wherever logged on, and instructs him/her to sign with a valid smart card. All requests may be recorded in signed logs at both ends of the operation, providing auditable, non-reputable histories of the transactions.
Validation Authority. A 24/7 authority centralizing validation services for digitally signed materials e.g. certificates, payment authorizations, or any

recordable data from industrial devices. The Validator authenticates the signer's identity and provides notary services for the submitted materials. All operations can be signed, time stamped and logged to provide an audit trail of non-reputable transactions. The Validation Authority also contains a policy mapper for linking alternative validation policies to the issuing CAs, keyholder identity information or to other, auxiliary data.

Smart card/role-based Single Sign On. Secure Office combines smart card security with role-based Single Sign On to provide secure, cost-effective user provisioning. Secure Office centralizes a company policy of smart card security, Single Sign On and role based access control across a full range of diverse systems and applications such as central directory networks, including Active Directory, Novell e-Directory, Windows NT, Terminal Servers, application/web servers, and customer specific business processes.

Encrypted networking. Secure Office VPN converts any combination of network / dialup / broadband / Internet / wireless connections to a private encrypted network, securing company portals (Intranets, Extranets) and remote access to inner company resources from PCs, mobile laptops and wireless PDAs. Secure Office VPN security includes smart card / role-based access control, 24x7monitoring for attempted intrusions and fine-grained configuration options. Multiple, simultaneous encrypted tunnels can be configured broadly (from router-to-router) or as finely as one laptop to one application.

Distributed Firewall. The Secure Office firewall operates from a centrally managed access control list, automatically distributing filtering and stateful inspection profiles to the client machines to establish a centrally controlled, personal firewall at every server, PC, laptop or PDA. Administration of the firewall supports broad (router-to-router) or narrow configurations (one machine-to-one application) as well as drag and drop security grouping to simplify management in even the most complex of networks.

OCSP Server. OCSP is an alternative to CRLs for handling certificate status information (verifying that a certificate is not revoked). An OCSP server is a central gathering point of revocation information from any number of certificate issuers. It generates a signed response to certificate status queries from PKI applications. Organizations can own and operate the OCSP server for in-house services or as a commercial provider of OCSP/non-repudiation services.

Time Stamp Server. Time-stamping records the point in time at which electronic materials exist for situations where they are legally binding or will become so in due course. Secure Office can log inbound requests and outbound time stamps in an auditable history. Organizations can own and operate the Time Stamp Server for in-house purposes or as an ASP to provide commercial time stamp/non-repudiation services to other organizations.

Hewlett Packard Secure Office Server Options

HP dl360

HP dl380

HP rx1620

HP rx2620

Protexx Secure Office Server Architecture and Implementation

I. Introduction

Protexx mission is to provide network security on both the internet and intranet. By using various components in its arsenal of security tools, Protexx has combined these tools to provide a secure environment for the various office servers in an organization.

The servers could be multiple machines, partitions in a virtual server or combination of these.

II. Components

The components of the secure office server are:

A. Firewall(s)

The Firewall is required to secure the environment. Protexx can provide a software firewall in a LINUX, HPUX or AIX virtual partition or small appliance server, or help the customer configure their own firewall for use in the Protexx secure office server environment.

The customer could choose to have multiple Firewalls for redundancy and/or capacity.

B. Tunnel Server(s)

The Tunnel Server is a software component that secures the communication between the clients and the application servers. This needs to reside either in its own virtual partition, its own appliance or in the Protexx Firewall appliance server.

For redundancy and capacity multiple Tunnel Servers could be configured.

C. Sub-Certificate Authority

The Sub-Certificate Authority is a mini Trust Center, used to provide the PKI (public/private key infrastructure). This component is crucial to the secure office server environment, because it supplies the credentialing of the clients for authorization.

This piece can reside in its own partition, server, housed at Protexx Trust Center or use any reliable Certificate Authority (must be

configurable for appropriate information in the X509 or PKCS#12 certificate.

D. Application server(s)

The application servers are the individual or grouped computers or virtual partitions that make up the application services that are being protected. Examples of these services are email, web-server, account receivables, account payables, general ledger, and these servers could be in a virtual partition or individual servers or combinations of both.

III. Theory of Operation

The secure office server works on the principal that users only need access to certain information and applications. While someone on the accounting staff might need access to accounts payable, he / she may and most likely will not need access to the payroll system. By establishing secure tunnels to the various applications, and routing the users based on their certificate, the system administrator creates and environment where the user can not even get to the logon screen of the application. In addition to blocking access to a server, all of the information flowing from the client system to tunnel server is sent encrypted, therefore it is blocked from the prying eyes of an unauthorized user who might be watching the network traffic.

IV. Defining and Building Policy and Procedures

We now to decide:

1 Who will have the Authority to Issue certificates

A decision needs to be made as to who has final authority on issuing and modifying a user access to the network.

2 Default life of certificate

What should the life cycle of a certificate be?

3 How many standard groups will be needed and who will be in them

Need to decide on the type of groups for access, an example might be the payroll department having two clerks and a supervisor.

4 Which applications are in each group

Payroll users might need access to email, time clock application, the payroll system and the general ledger system.

5 Exception Policy for expanding or compressing application for a user in a group

6 Documenting the Policies and Procedures for Trust

Now the hardest part is documenting and implementing the policy and procedures and getting signoff.

V. Network Layout

Now that we have all the information required, a logical network map needs to be produced so that the secure routings can be created

VI. Implementation of Test Environment

VII. Final Test

VIII. Go Live