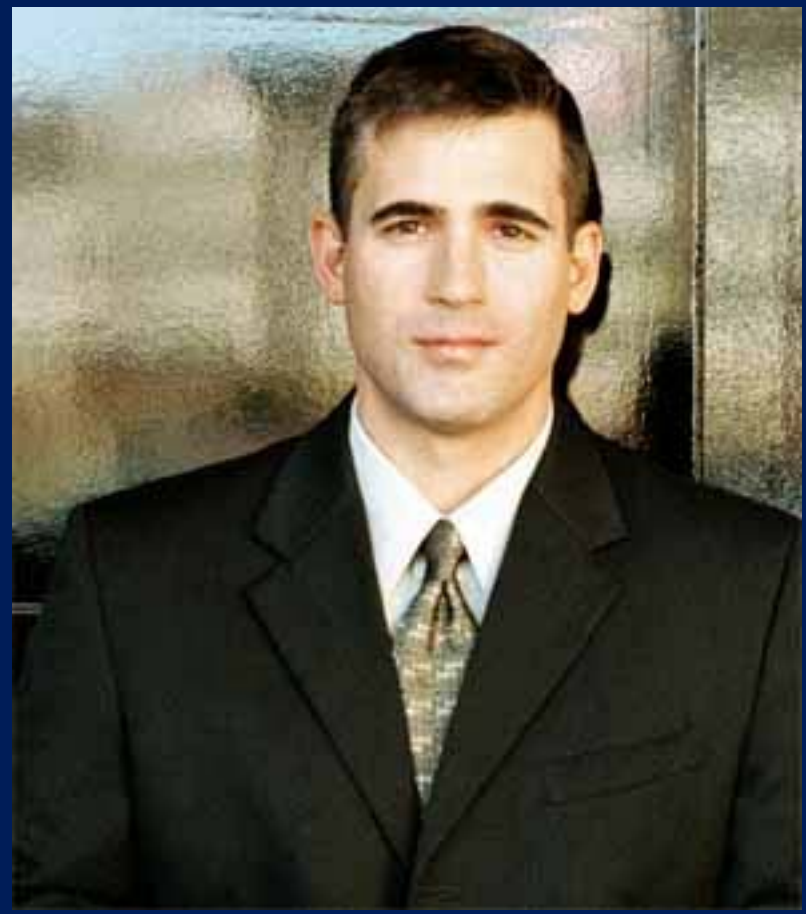
HP Instant Support Enterprise Edition (ISEE) Security overview

Advanced Configuration A.03.50

Mike Brandon
Interex
03 / 30, 2004

Executive summary

- To address the safety of our customers' networks and support data, HP has incorporated a number of security technologies into the design of our next generation remote support technology named HP Instant Support Enterprise Edition (ISEE).
- Encryption, authentication, and industry standard security protocols and best practices are integrated at the physical, network, application, and operational, levels of the ISEE architecture, providing a multi-level, layered security structure.



Presentation agenda

- Provide an overview of HP's next generation remote support solution with respect to the security technology used to deliver:
  - Hardware event management for remotely supported HP systems and devices.*
  - Remote execution of diagnostic support scripts (called MAPs) by HP support engineers for reactive support of hardware events.
  - Remote network access by HP support engineers for proactive or reactive hardware and software support.

*See ISEE marketing brief for supported systems and devices

HP ISEE support features

HP ISEE support features

- ISEE advanced configuration provides:
  - Remote hardware event management
  - Remote execution of diagnostic support scripts (MAPs)
  - Remote network access for HP support engineers
    - Installation of ISEE client software and onsite Support Point of Presence (SPOP) server required for hardware event management and MAP functionality
    - Installation of onsite VPN hardware required for remote network access functionality

Remote hardware event management

- Provides real-time hardware event detection for supported HP hardware, and sends notification of the event to the HP monitoring center.
  - Events are acted upon in accordance with customer's service level agreement.
- HP support engineers at HP's monitoring centers can view the incoming events (called incidents) and log support calls, if needed, into the HP workflow system.

What is a hardware event?

- Existing diagnostic software is used to monitor hardware status and generate notification events when certain predetermined conditions are detected.
- Notification events are received by event collectors running on the monitored system.
- The diagnostic data from the event is used to create an ISEE hardware incident, which is transmitted to HP for review by an HP support engineer.

Remote execution of support scripts (MAPs)

- A diagnostic engine installed on a monitored system or device allows for remote execution of “support scripts”, also known as “MAPs” which diagnose problems and provide timely information for resolving those problems.
- MAPs can perform a variety of operations related to collecting additional diagnostic data.

Types of MAPs

- Telemetry collection
  - Obtains a specific set of system or device configuration data
  - Does not modify system or device configurations
- ISEE management
  - Executed to maintain and update the customer side ISEE infrastructure
  - An example is updating hardware EMS diagnostic configuration files as new monitors become available
- HP provides a MAP script browser to allow the customer to view the contents of MAP scripts and commands that may be executed against their systems. Customers can review MAP script content in advance at the following URL:

  http://isee.americas.hp.com/isee/MAPscriptsBrowser/index.html

Remote network access

- Remote network access enables an HP support engineer located in HP's response center to remotely login to HP supported servers or devices located on the customer's enterprise network utilizing a secure IPSec VPN router installed in the customer's DMZ network, for the purpose of providing remote HP hardware or software support (only with prior customer authorization).
- HP support engineers are able to utilize additional support tools installed on the SPOP server that provide further local support capabilities in the customer's enterprise.
- Customer may designate a customer owned and managed "Customer Access System" or CAS to act as a point of control for HP remote access.
- Customer maintains security control over all HP access to customer systems and networks.

What is an SPOP?

- SPOP is an acronym for “support point-of-presence”, an HP provided workstation.
  - Intel based platform, Windows 2000 Advanced Server operating system
  - Customer can further harden to meet internal security standards.
- The SPOP provides:
  - An enterprise view of hardware events generated in the customer’s environment.
  - A centralized point in the customer’s environment for executing HP support tools and services.

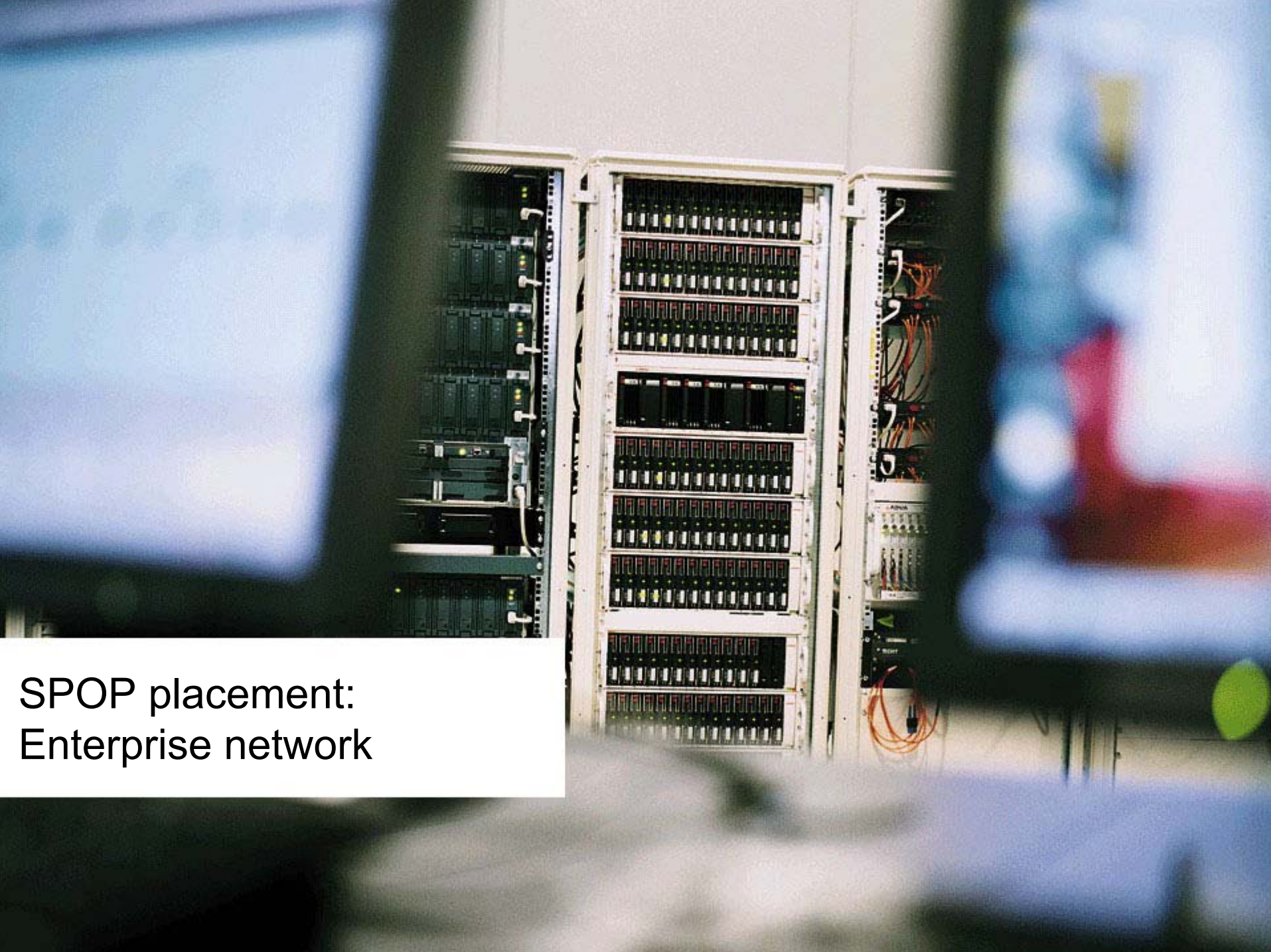
Security hardening SPOP

- SPOP is “security hardened” using the following tools to help ensure a secure HP remote support platform:
  - Microsoft Baseline Security Analyzer (MBSA) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsawp.asp
  - IIS Lockdown http://www.microsoft.com/technet/security/tools/locktool.asp
  - HFNetChk http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp
  - Norton Antivirus 8, with regular updates of antivirus definition files.
  - Regular remote software management updates of relevant security patches and hotfixes as identified by ISEE Support team.
  - Penetration and Security testing at each major ISEE release by external security consulting firm.

SPOP network placement

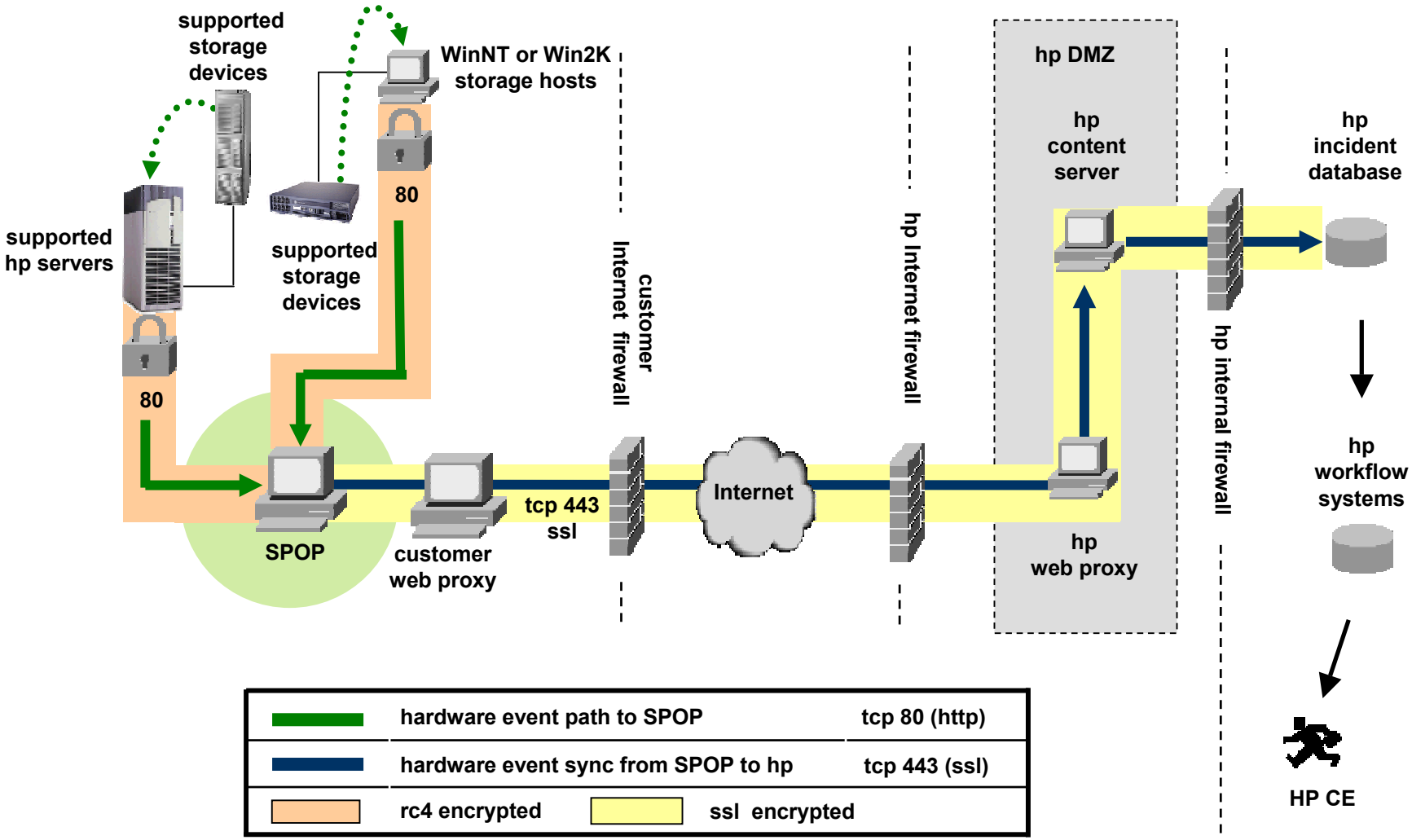
- ISEE supports placement of the SPOP in one of two locations in the customer's network environment:
  - Enterprise network
    - Placement of the SPOP directly on the customer's internal enterprise network, inside the customer's internal firewall
    - No firewall restrictions between SPOP and monitored clients
  - DMZ network *
    - Placement of the SPOP within the customer's DMZ network, inside the customer's external (Internet) facing firewall, but outside the customer's internal firewall
    - Internal firewall located between SPOP and monitored clients
    - External firewall located between SPOP and Internet (HP)

* Requires additional firewall port openings



SPOP placement:
Enterprise network

Remote hardware event management
Enterprise SPOP placement



Internet firewall port requirement
Enterprise SPOP placement

Remote hardware event management & MAP execution functionality

Customer's Internet firewall				
Protocol	Port	Service	Direction	Function
TCP	443*	SSL	outbound	Hardware event management and MAP execution requests

* Can utilize customer web-proxy

Specific IP address information for HP servers will be provided to assist with firewall rules

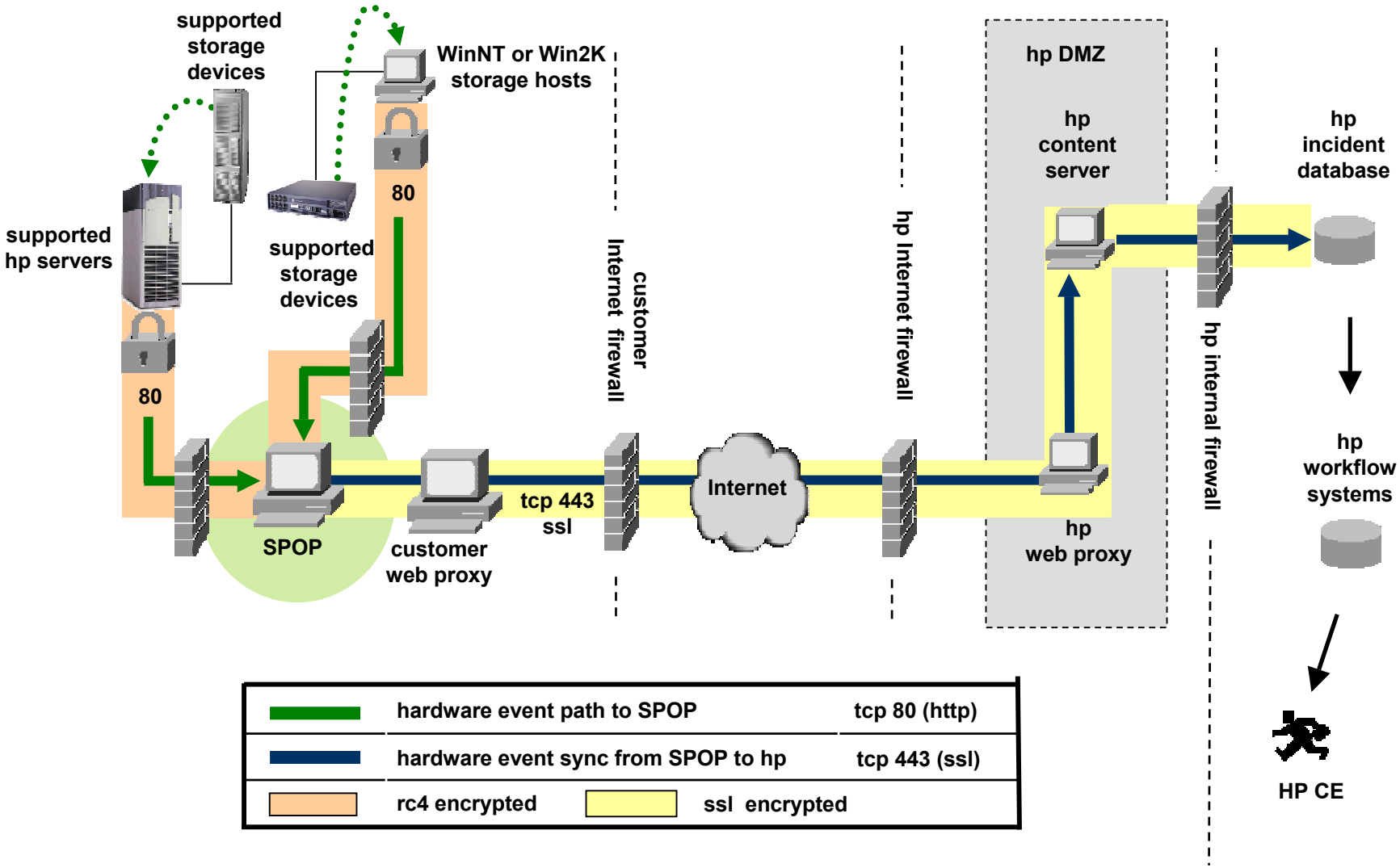
Internet firewall port requirement
Enterprise SPOP placement

- Placement of the SPOP on the customer's internal network requires the following Internet firewall port opening (with ack back) enabled between the SPOP and HP:
  - TCP 443

    SSL (https) protocol (128-bit RC4)
    - Transport of encrypted hardware events from SPOP to HP
    - Synchronization between HP and SPOP on status of hardware events transmitted to HP
    - Synchronization of MAP execution requests from HP to SPOP
    - Synchronization of MAP execution results from SPOP to HP
    - All network traffic can utilize local customer web-proxy


SPOP placement:
DMZ network

Remote hardware event management
DMZ SPOP placement



Internet firewall port requirement
DMZ SPOP placement

Remote hardware event management & MAP execution functionality

Customer's Internet firewall				
Protocol	Port	Service	Direction	Function
TCP	443*	SSL	outbound	Hardware event management and MAP execution requests

* Can utilize customer web-proxy

Specific IP address information for HP servers will be provided to assist with firewall rules

Internet firewall port requirement
DMZ SPOP placement

- Placement of the SPOP on the customer's DMZ network requires the following Internet firewall port opening (with ack back) enabled between the SPOP and HP:
  - TCP 443

    SSL (https) protocol (128-bit RC4)
    - Transport of encrypted hardware events from SPOP to HP
    - Synchronization between HP and SPOP on status of hardware events transmitted to HP
    - Synchronization of MAP execution requests from HP to SPOP
    - Synchronization of MAP execution results from SPOP to HP
    - All network traffic can utilize local customer web-proxy

Internal firewall port requirements
DMZ SPOP placement

Customer's internal firewall				
Protocol	Port	Service	Direction	Function
TCP	80	HTTP*	outbound	Hardware event management
TCP	3389	RDP**	outbound	Centralized view of hardware events using terminal services from desktop to SPOP
TCP	25	SMTP**	inbound	MAP execution request approval (can utilize customer's DMZ mail gateway)

* HTTP encrypted with 128-bit RC4 (can utilize customer's outbound web-proxy)
** Optional functionality

Internal firewall port requirement
DMZ SPOP placement

- Placement of the SPOP in the customers DMZ network requires the following outbound port opening* from the customer's internal firewall to the SPOP in the DMZ, to enable hardware event management functionality:
  - TCP 80

    HTTP, incident data encrypted with 128-bit RC4
    - Transport of encrypted hardware event data from monitored clients on internal network to SPOP in DMZ
    - Can utilize customer's existing web-proxy to communicate with SPOP in DMZ

* Or use of a customer web-proxy

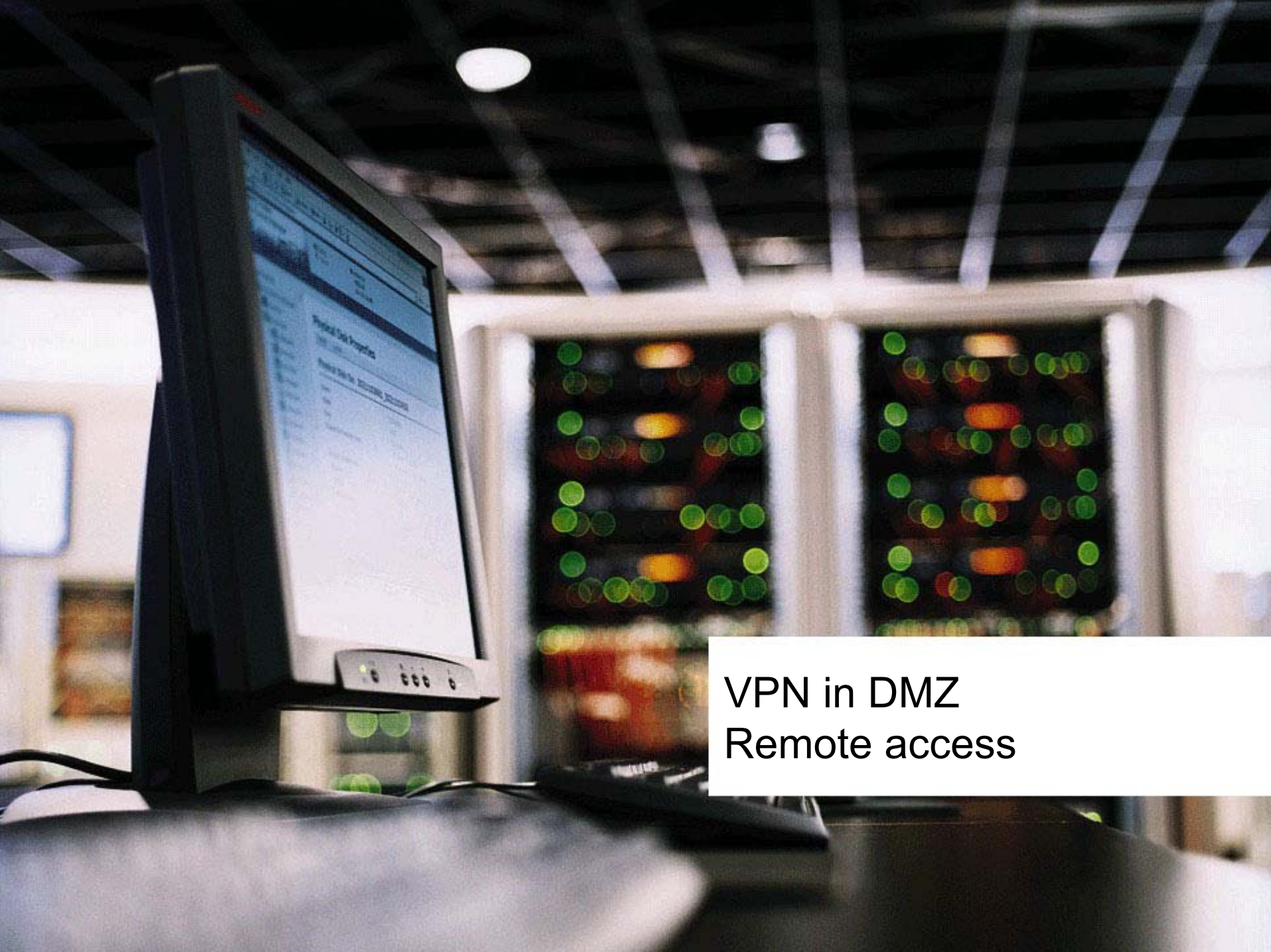
Internal firewall port requirement
DMZ SPOP placement

- Placement of the SPOP in the customers DMZ network requires the following outbound port opening from the customer's internal firewall to the SPOP in the DMZ:
  - TCP 3389

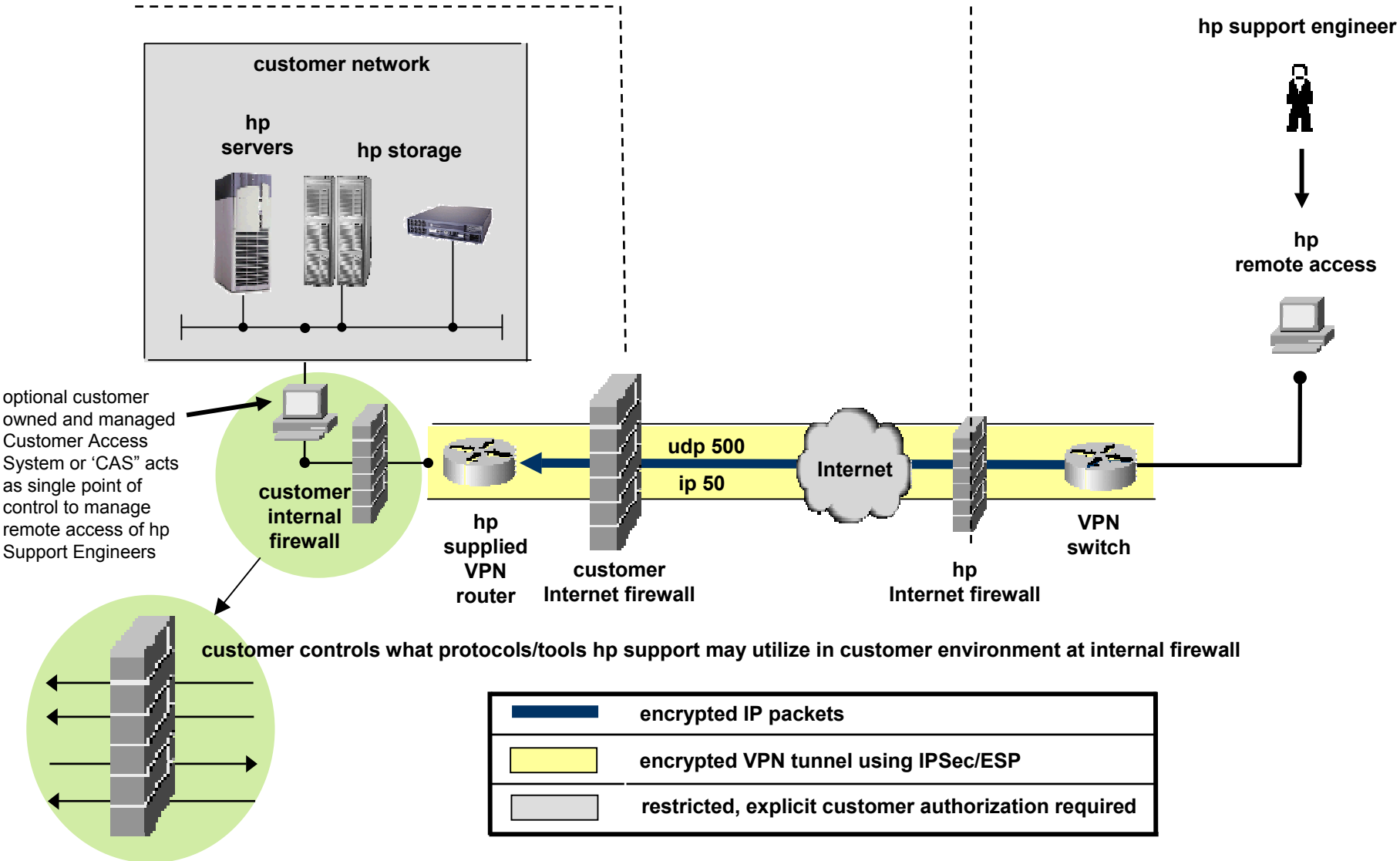
    Microsoft Terminal Services
    - Provides the ability to obtain an enterprise view from one desktop of all open hardware events in the enterprise
    - Uses terminal services installed on users desktop to view SPOP desktop, then launch ISEE UI on SPOP for enterprise view of all hardware events
    - Optional functionality

Internal firewall port requirement
DMZ SPOP placement

- Placement of the SPOP in the customers DMZ network requires the following inbound port opening from the SPOP in the DMZ to the customer's internal firewall, to enable e-mail communication from SPOP:
  - TCP 25 SMTP
    - Customer can configure all MAP execution requests to be pre-approved by customer
    - An e-mail request is sent to customer from SPOP in DMZ requesting approval to execute the MAP
    - Optional functionality if customer does not require MAP execution by HP to be pre-approved
    - Can utilize a customer's existing DMZ mail relay


VPN in DMZ
Remote access

Remote access via IPSec VPN



Internet firewall port requirements
Remote access IPSec VPN

DMZ placement of VPN hardware

Customer's Internet firewall				
Protocol	Port	Service	Direction	Function
UDP	500	IKE	Bi-directional	VPN key exchange
IP 50	None	IPSec/ESP	Bi-directional	IPSec VPN

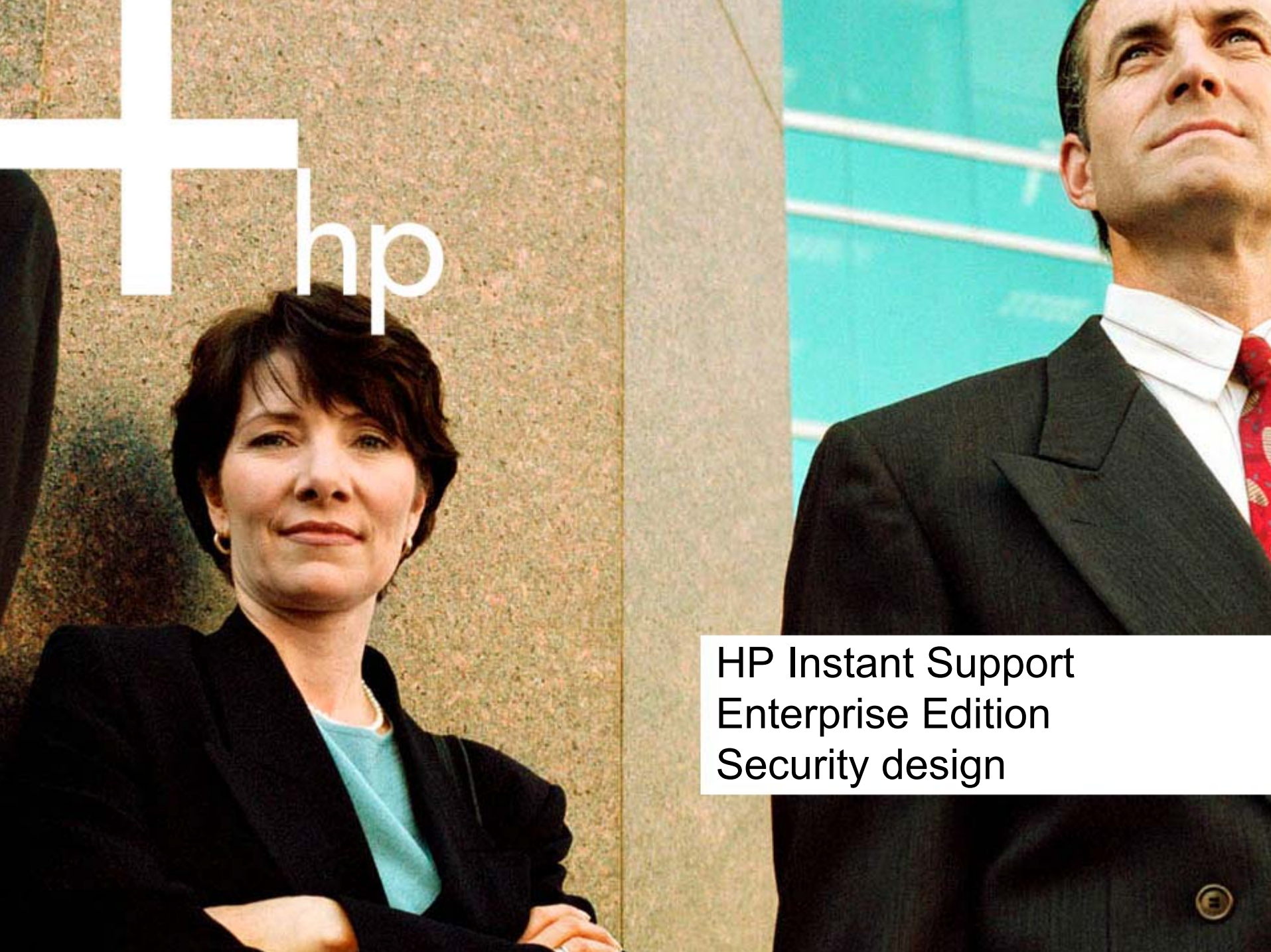
* Can use customer web-proxy

Specific IP address information for HP servers will be provided to assist with firewall rules

Internet firewall port requirements
Remote access IPSec VPN

- Requires the following bi-directional* port openings at the customer's Internet firewall for communication between HP VPN switch and customer side VPN router installed in the customer's DMZ network, to enable secure HP remote network access:
  - UDP 500 Internet key exchange protocol
    - Exchange of encryption keys and negotiation of encryption ciphers for IPSec VPN tunnel
  - IP 50 protocol IPSec/ESP protocol
    - Secure branch VPN tunnel between HP VPN concentrator and customer side VPN router for remote support access

* UDP and IP protocols are stateless, and must be explicitly configured each direction



HP Instant Support Enterprise Edition Security design

Security design issues

- ISEE is a support technology that involves the delivery of remote customer support using a public network infrastructure (Internet).
- HP faced security concerns and public perception issues similar to other e-business vendors who conduct security sensitive transactions using the Internet.
- In business today, many security sensitive transactions such as e-commerce, stock trades, and online banking, are executed securely over the Internet using the same industry standard security technologies utilized by ISEE.

Security design requirements

- ISEE is designed to meet the following security requirements:
  - Data privacy
  - Data integrity
  - Authenticity and integrity of content (MAPs)
  - Access logs and audit trails
  - Comprehensive operational security

Security implementation

- ISEE implements transaction security in two key areas:
  - Security of client-server network communications:
    - Secure communications between client-server components is implemented using http encrypted with RC4 private-key encryption and machine to machine X.509v3 digital certificate authentication.
  - Security for content (MAPs):
    - Content security is implemented using X.509v3 digital certificates and MD5 message digest to digitally sign content to verify integrity and authenticate origin.

HP ISEE security technology

- SSL (protocol 3.0)
- IPSec/ESP virtual private network
- RC4 private-key encryption cipher with 128-bit key
- RSA public-key encryption cipher with 2048-bit key
- 3DES private-key encryption cipher with 168-bit key
- X.509v3 digital certificate standard
- MD5 message digest
- RADIUS authentication

Security objectives vs. controls

- Privacy of data:
  - SSL with RSA and RC4 encryption ciphers
  - IPSec/ESP VPN with 3DES encryption cipher
- Integrity of data:
  - MD5 message digest with X.509v3 digital certificate standard
- Authenticity of data:
  - SSL with X.509v3 certificate standard
  - MD5 message digest with X.509v3 digital certificate standard
- Authenticity of users:
  - RADIUS authentication
  - PKI authentication (X.509v3 digital certificate standard)
  - NT domain authentication

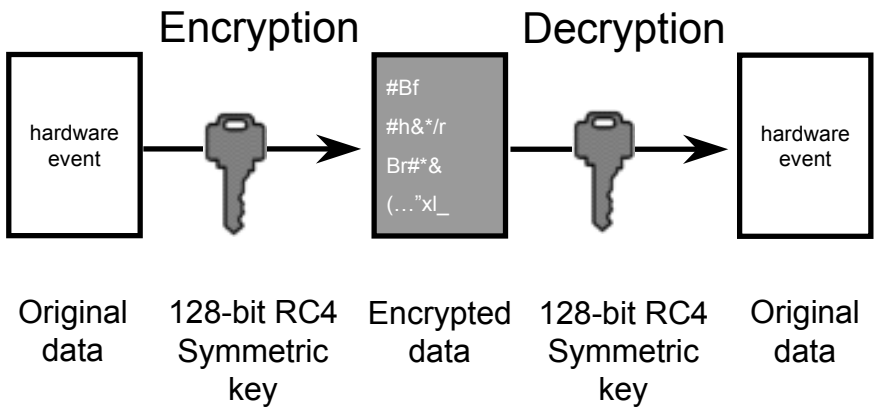
Frequently asked questions

How is my hardware event data secured during transport to HP?

- Before the transmission of hardware event data occurs between servers, the network communications channel is authenticated using X.509v3 digital certificates.

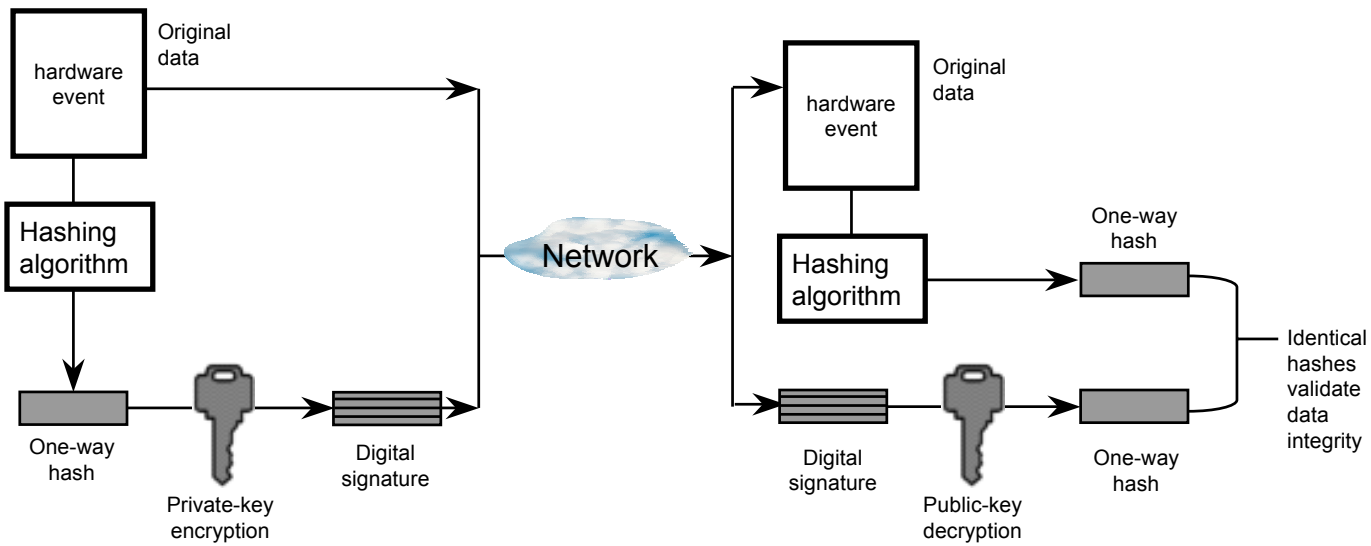
How is my hardware event data secured during transport to HP?

- Prior to leaving the customer's network, all hardware event data is encrypted using 128-bit RC4 symmetric-key encryption cipher.
- This provides data confidentiality while hardware event data is in network transit to HP.



How is my hardware event data secured during transport to HP? (continued)

- Further, all hardware event data is digitally signed prior to transmission using MD5 message digest hash and X.509v3 digital certificates.
- This provides data authenticity and data integrity for hardware event data transmitted to HP.



How is my hardware event data secured while at HP?

- Access to customer hardware event data is restricted within HP to a subset of authorized HP support engineers with a support business need to access such data.
- HP support engineers accessing customer hardware event data are individually authenticated prior to data access.

How is my company protected from unauthorized access to my network by HP?

- Only HP support engineers with a verified business need to support your company are issued the required RADIUS database entries necessary to authenticate the engineer and allow remote access to the customer side VPN router.
- Customer may designate a customer owned and managed “Customer Access System” or CAS through which all HP support engineers are required to login prior to accessing other systems in the customer’s network. Customer provides and manages all login credentials to the CAS.
- All HP support engineers are required to adhere to an “ISEE acceptable use policy” which outlines required behavior when accessing customer networks for the purposes of providing remote support.

How is access to the SPOP secured?

- The SPOP is securely positioned behind your company firewall, inside your enterprise network or DMZ.
- SPOP is “security hardened” using a number of security tools including MBSA, IIS Lockdown, HfNetChk, and Norton Antivirus.
- Authentication is achieved using X.509v3 certificates for server to server authentication, and RADIUS for user authentication.

How is remote access to the customer network secured?

- Access to the customer's network from inside HP is highly restricted.
- Each HP support engineer's access is individually authenticated.
- Only HP support engineers with a support business need are granted the RADIUS database entries required for remote support access.
- Access logs and audit trails help maintain individual accountability, enabling customers to determine which support engineers at HP accessed the customer's network, and when the access occurred.

Why are support scripts (MAPs) secure?

- All MAPs undergo a thorough testing and validation process before being digitally signed to validate authenticity and integrity.
- The diagnostics engine uses “sandbox technology” to contain support scripts based on established security parameters.
- Customer has the option to allow all MAPs to run automatically, or may approve each request to run a MAP.

HP

- Technical information in this document is specific to the A.03.50 releases of HP Instant Support Enterprise Edition (ISEE), and is subject to change without notice.
-

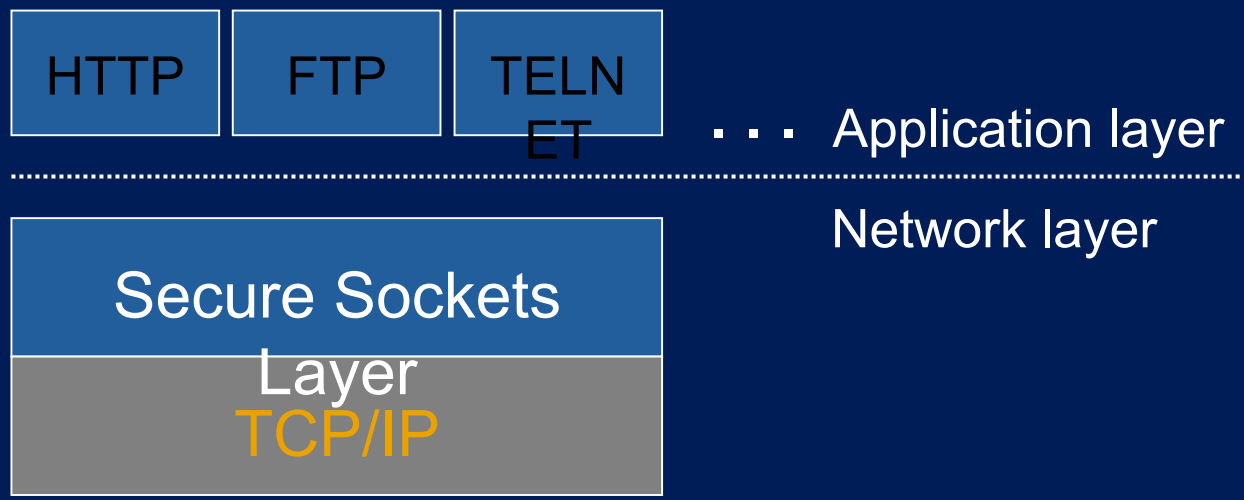

hp
invent

Secure Sockets Layer (SSL)

- De facto industry standard for delivering secure online services to business and financial sector
- Powerful session-level security
- Also known as transport layer security, or TLS as defined in RFC 2246
- Uses public-key certificate based system to establish identity and trust relationship between clients and servers

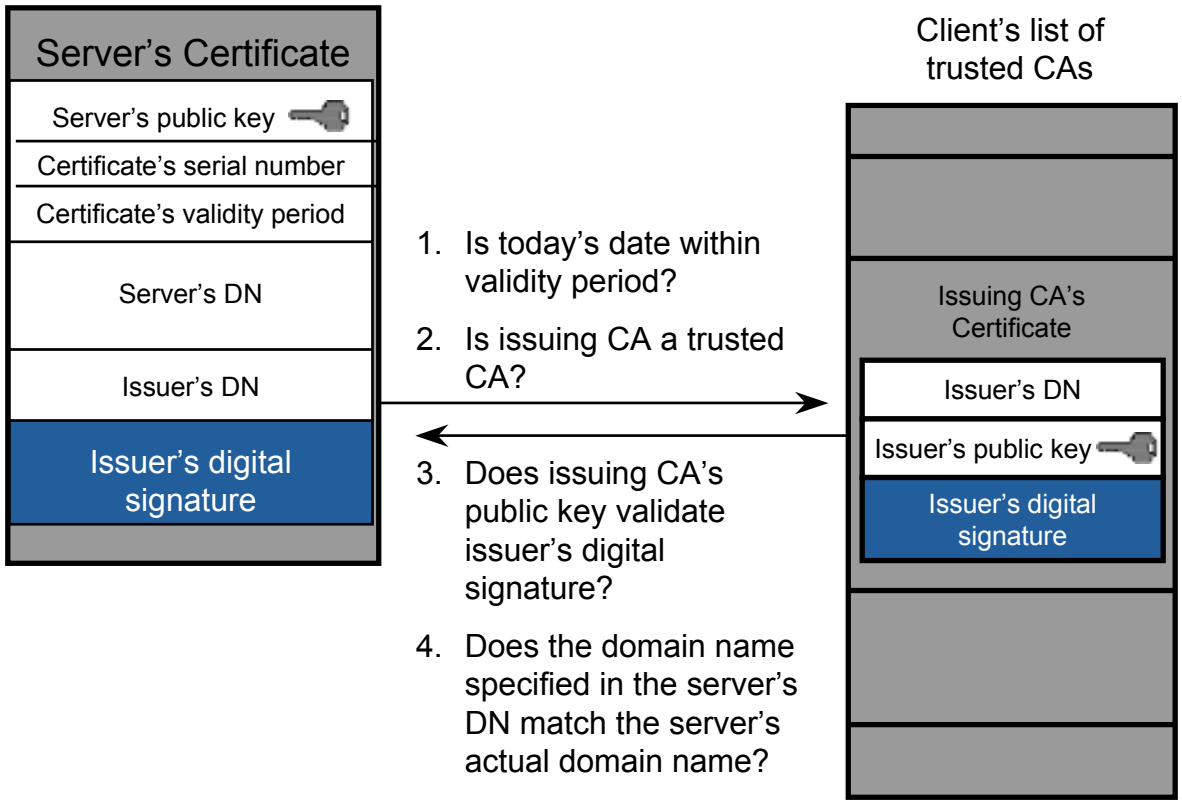
Secure Sockets Layer

- SSL runs above TCP/IP and below high-level application protocols like http:



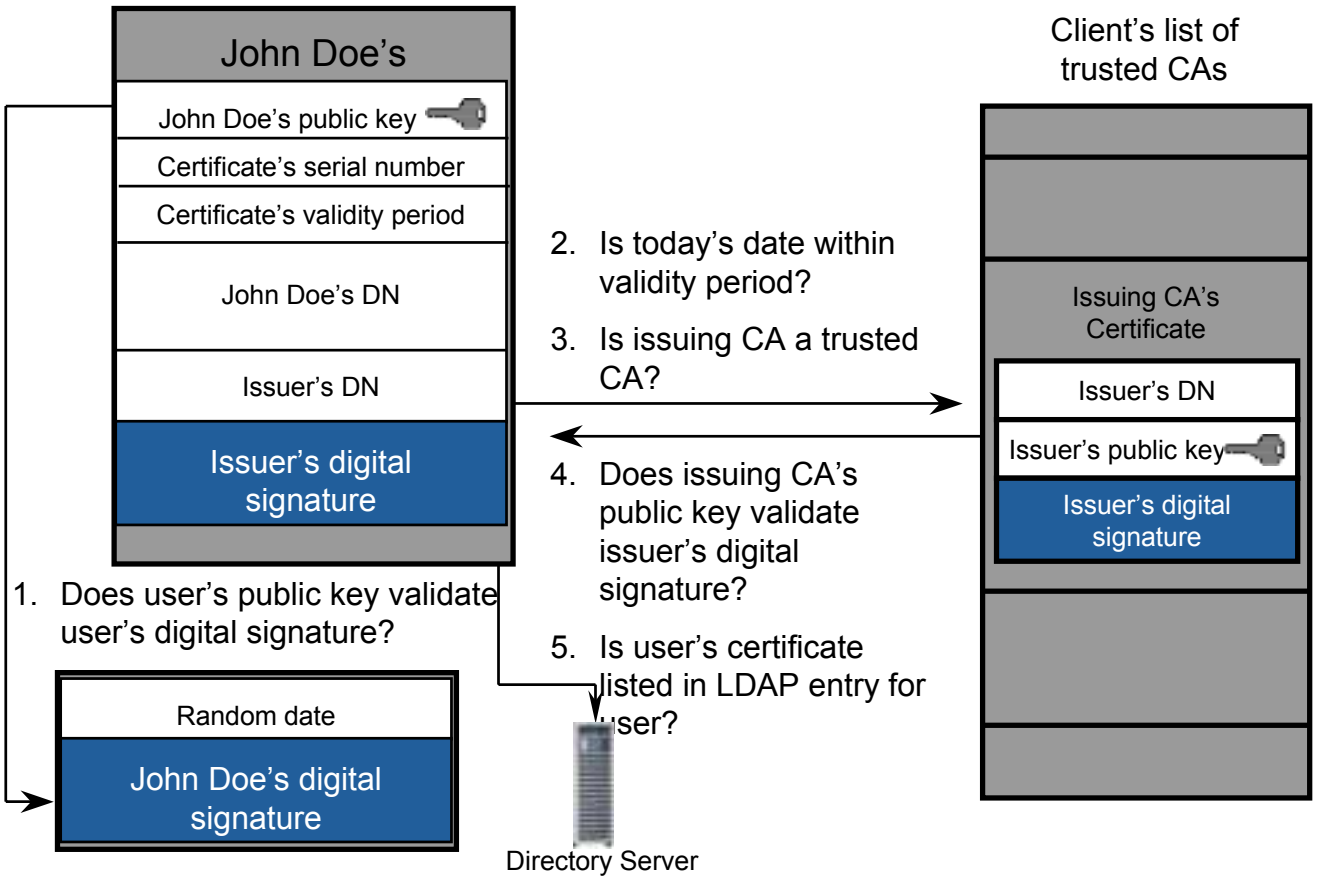
Secure Sockets Layer

- X.509v3 digital certificates and SSL server authentication allows a client to confirm a server's identity.



Secure Sockets Layer

- X.509v3 digital certificates and SSL client authentication allows a server to confirm a client's identity.



IPSec

- IPSec secures data by creating a virtual tunnel from point A to point B that “looks” like a direct connection with no infrastructure [routers/hops] in between.
- To protect the payload, IPSec utilize a suite of IP security protocols that include an authentication header (AH) and an encapsulating security payload (ESP) to encrypt many of the network stack information items.

MD5 message digest

- MD5 (message digest) is a hashing algorithm used in generating digital signatures.
  - The output of MD5 is a message digest, which can be used to authenticate the owner of a private key.
- If the signature verification is successful, the recipient is notified of the data's authenticity, and that data integrity has been preserved.

X.509v3 public-key certificates

- Provides strong authentication (two factor) of a user's identity
- Based on public-key cryptography
- Uses a certificate authority (CA) to bind a user or system to a public-key/private-key pair

RC4 private-key encryption

- RC4 private-key (symmetrical) stream cipher is used for high performance encryption of data transported between a customer's network and HP's network.
- HP uses a 128-bit key size, which is classified as strong encryption.

RSA public-key encryption

- RSA public-key (asymmetrical) encryption is used to encrypt the session private-key for hardware incidents transmitted between a customer's network and HP's network.
- HP uses a configurable 1024 or 2048-bit key size, classified as strong encryption.

Additional Internet technical references

- Introduction to SSL:
  - http://developer.netscape.com/docs/manuals/security/sslin/contents.htm
- The SSL protocol:
  - http://home.netscape.com/eng/ssl3/ssl-toc.html
- Introduction to IPSec:
  - http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver23f/ipsec/ch01.htm
- Introduction to Public-Key Cryptography:
  - http://developer.netscape.com/docs/manuals/security/pkin/contents.htm
- Digital Signatures Illustrated:
  - http://www.aci.net/kalliste/digsig.htm