OS/390 Websphere Security

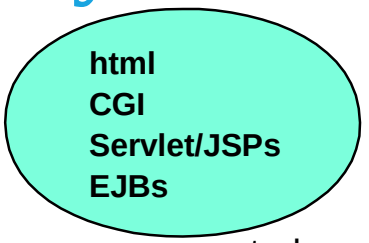
Paul de Graaff
Field Technical Sales Specialist
E-Mail : graaff@us.ibm.com

Agenda

- Websphere Security Parts
- Security Objectives
- Why Serving the Web from OS/390 Provides Better Security
- Serving Web Pages Securely from OS/390
- Protecting Communications with SSL
- Using Global Server Certificates
- Using the S/390 Cryptographic Coprocessor
- Improving Security with Client Certificates
- Certificate Name Filtering

Elements of Websphere Security

Websphere Resources



access control

Websphere Security

Websphere Security

EJB Security

CORBA Security

JAVA Security

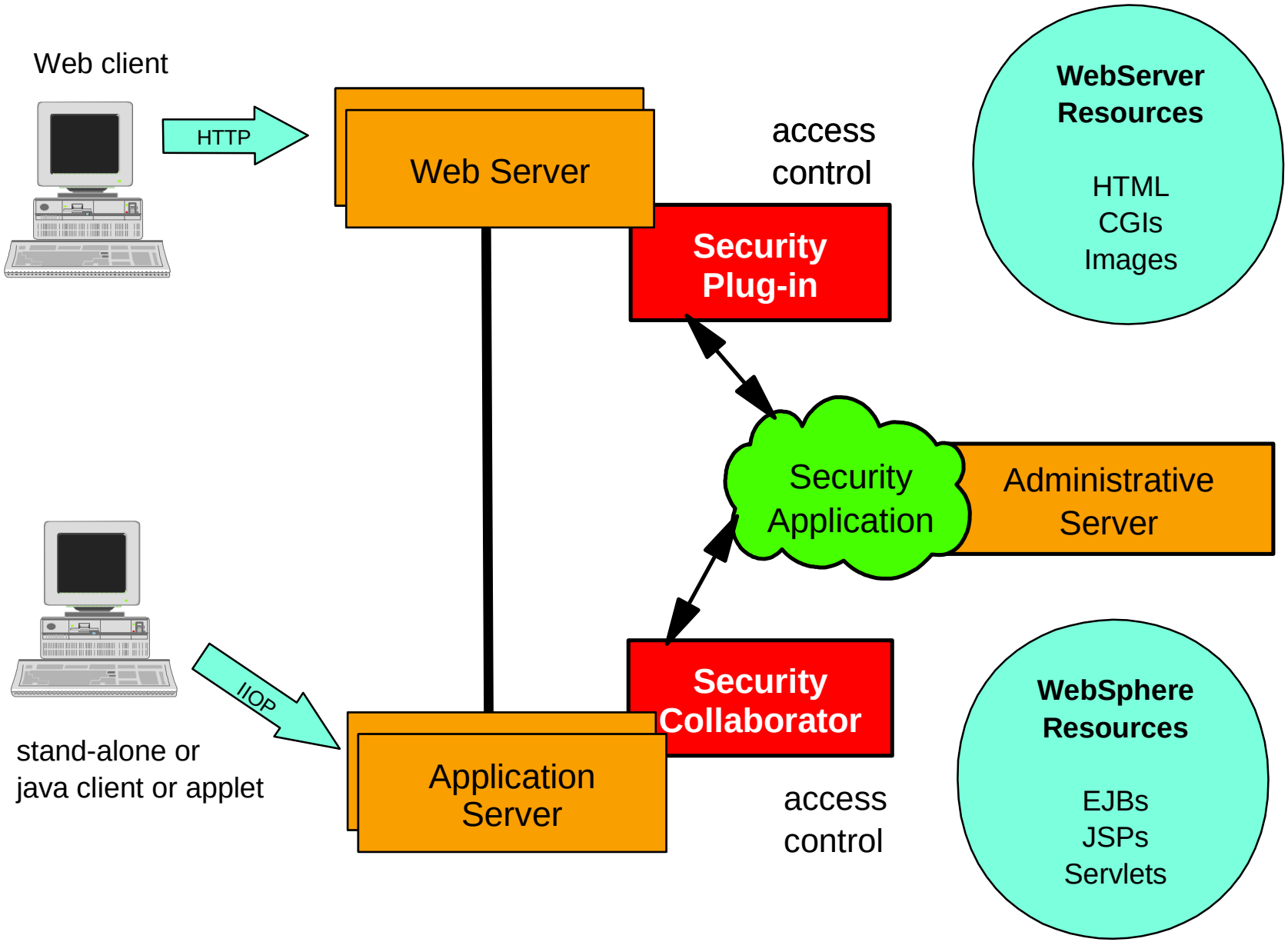
Java Security Classes

JVM

Platform Security

Operating System Security

Websphere Security Architecture



e-business

IBM

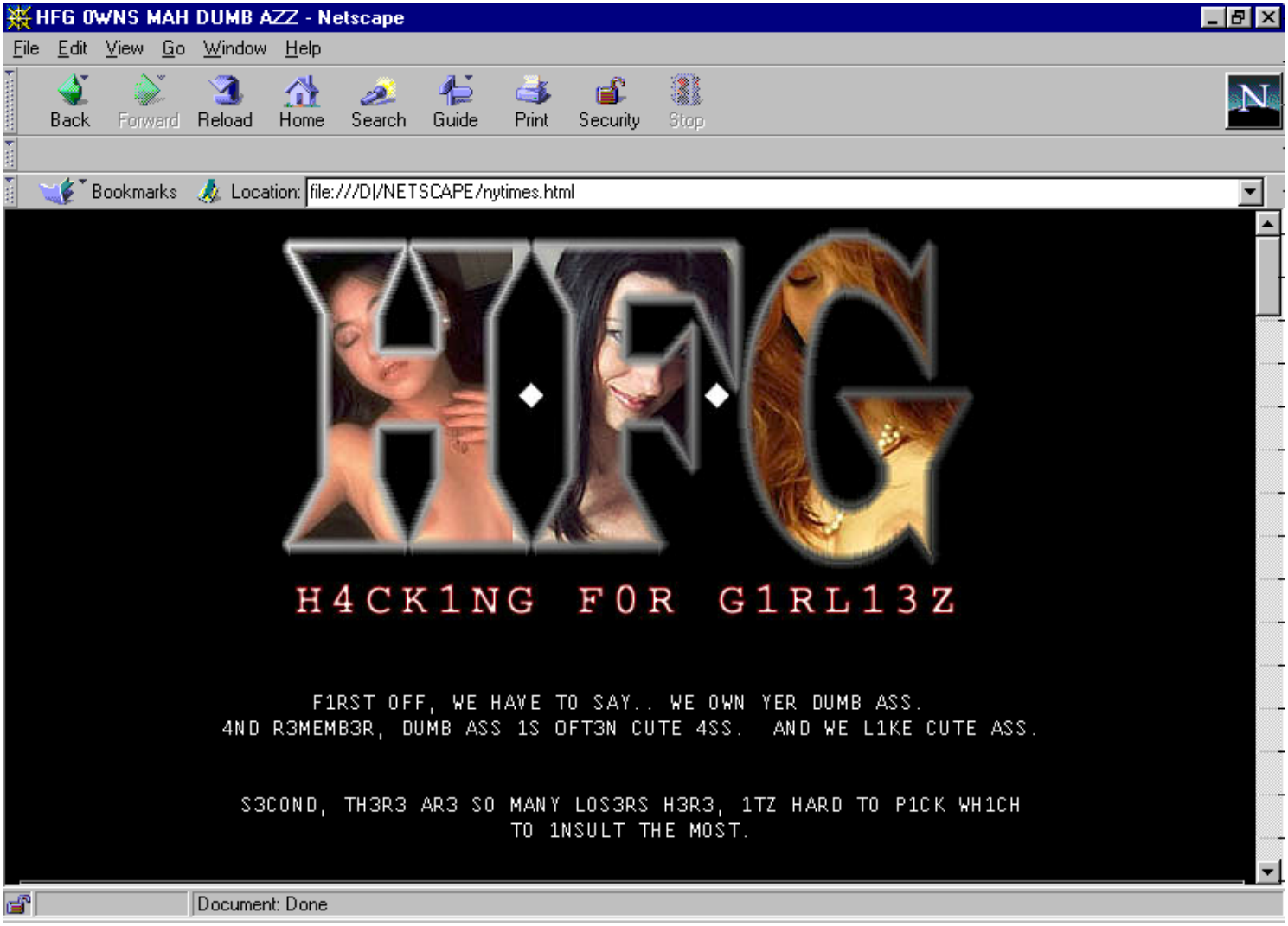
Security Objectives

Security Objectives, Risk Assessment

- Access Control
- Identification and Authentication
- Confidentiality (or Privacy)
- Data Integrity
- Non-Repudiation (or Accountability)

Security measures are dependent on risks and amount of possible damage, so a thorough risk assessment should always be performed and a security policy needs to be defined.

NY Times Website Hacked on 98/09/13



Why Serving the Web from OS/390 Provides Better Security

OS/390 Security Advantages

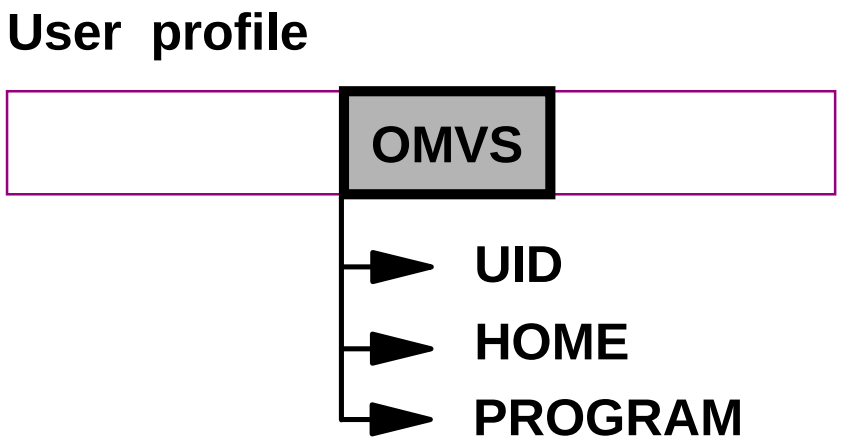
- Superior hardware and system integrity
- User Identification and Authentication through RACF
- RACF Control of Superuser functions
- RACF Control of user identity changes
- Protection of daemons against modification and misuse
- Thread-level security

Superior Hardware and System Integrity

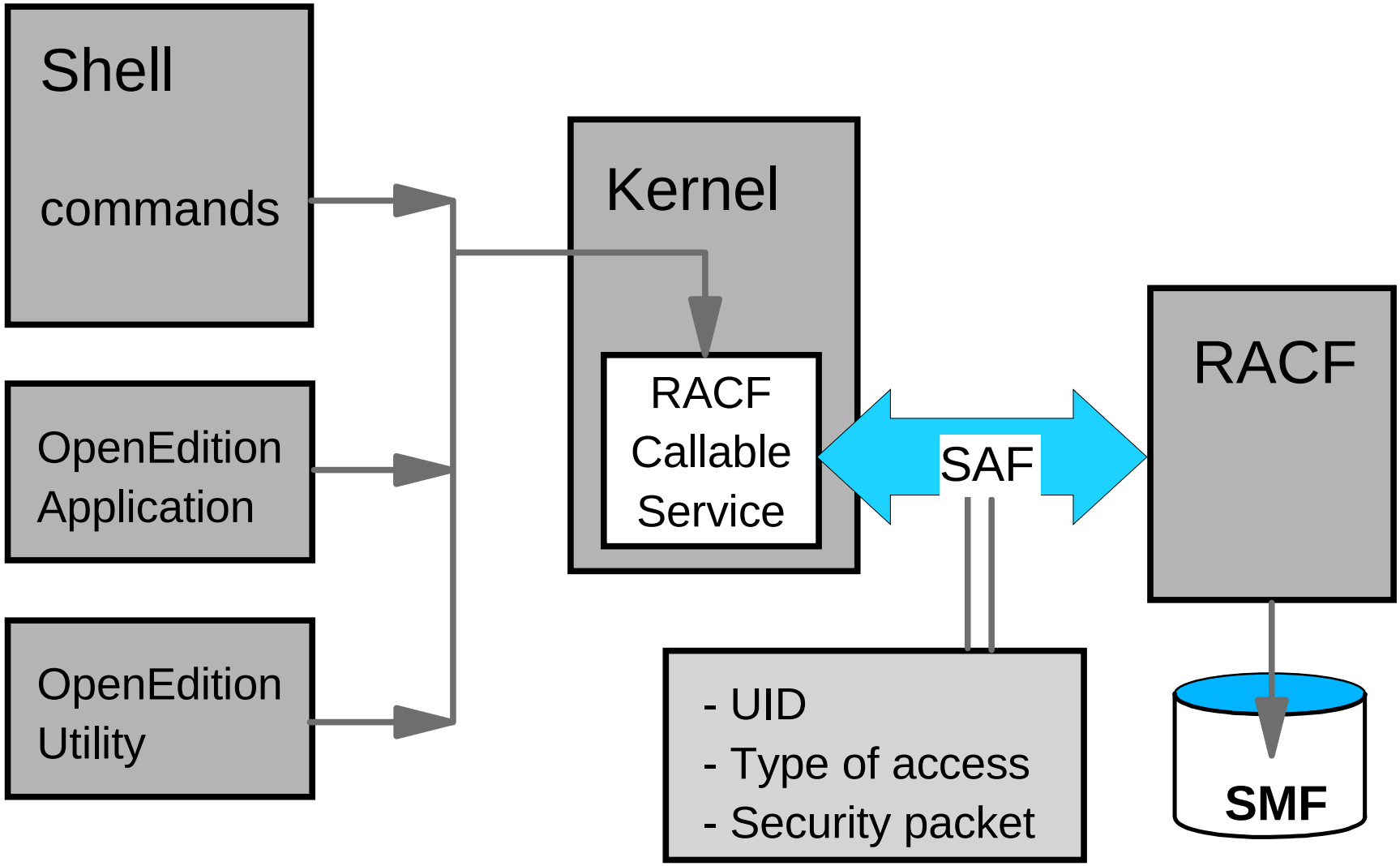
- S/390 LPAR function provides B2-level (ITSEC-E4) isolation between system images
- S/390 Supervisor/Program states and storage keys isolate Trusted Computing Base from applications
- Tight control of Authorized Program Facility (APF)
- Link Pack Area (LPA) is write protected even from privileged programs
- Address spaces are isolated from each other
- Fetch protected storage can only be read from programs with same storage key
- Formal commitment to System Integrity since 1973

RACF User Identification and Authentication

- OS/390 UNIX user identification
  - RACF user profile with OMVS segment
  - RACF group profile with OMVS segment
- User authentication
  - RACF password
- OS/390 UNIX logon
  - TSO
  - r_login
- Resource access control
  - RACF



RACF Callable Services



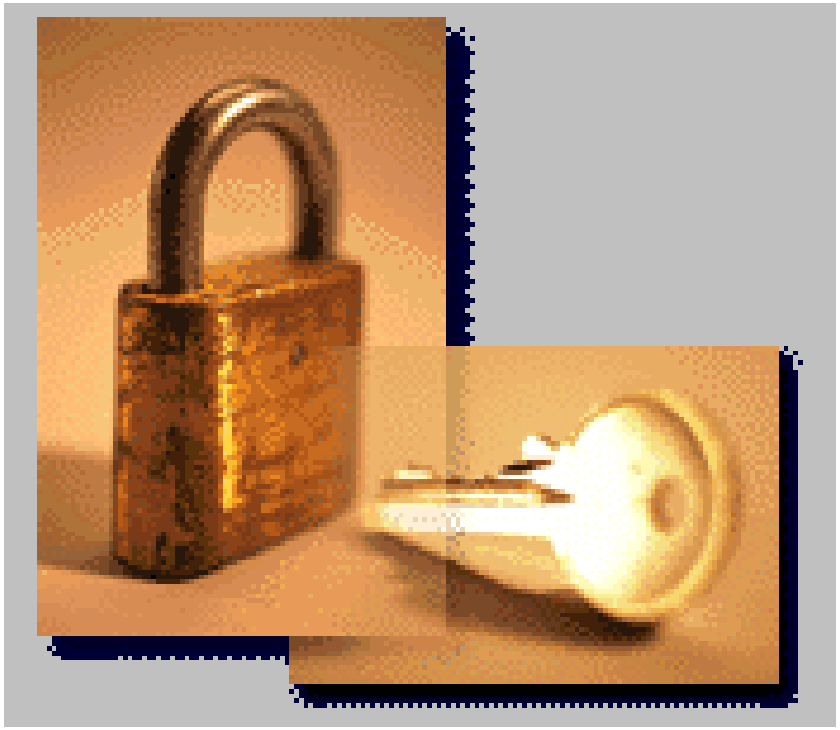
RACF Control of Superuser Functions

- BPX.SUPERUSER
  - authorized users can switch into Superuser mode
  - administrators do not need UID 0 user IDs
  - used by SMP/E (starting with OS/390 V2R7) instead of UID 0
- UNIXPRIV class partitions Superuser functions in OS/390 V2R8

- BPX.FILEATTR.APF, BPX.FILEATTR.PROGCTL
  - ability to set extended attributes for HFS files

RACF Control of User Identity Changes

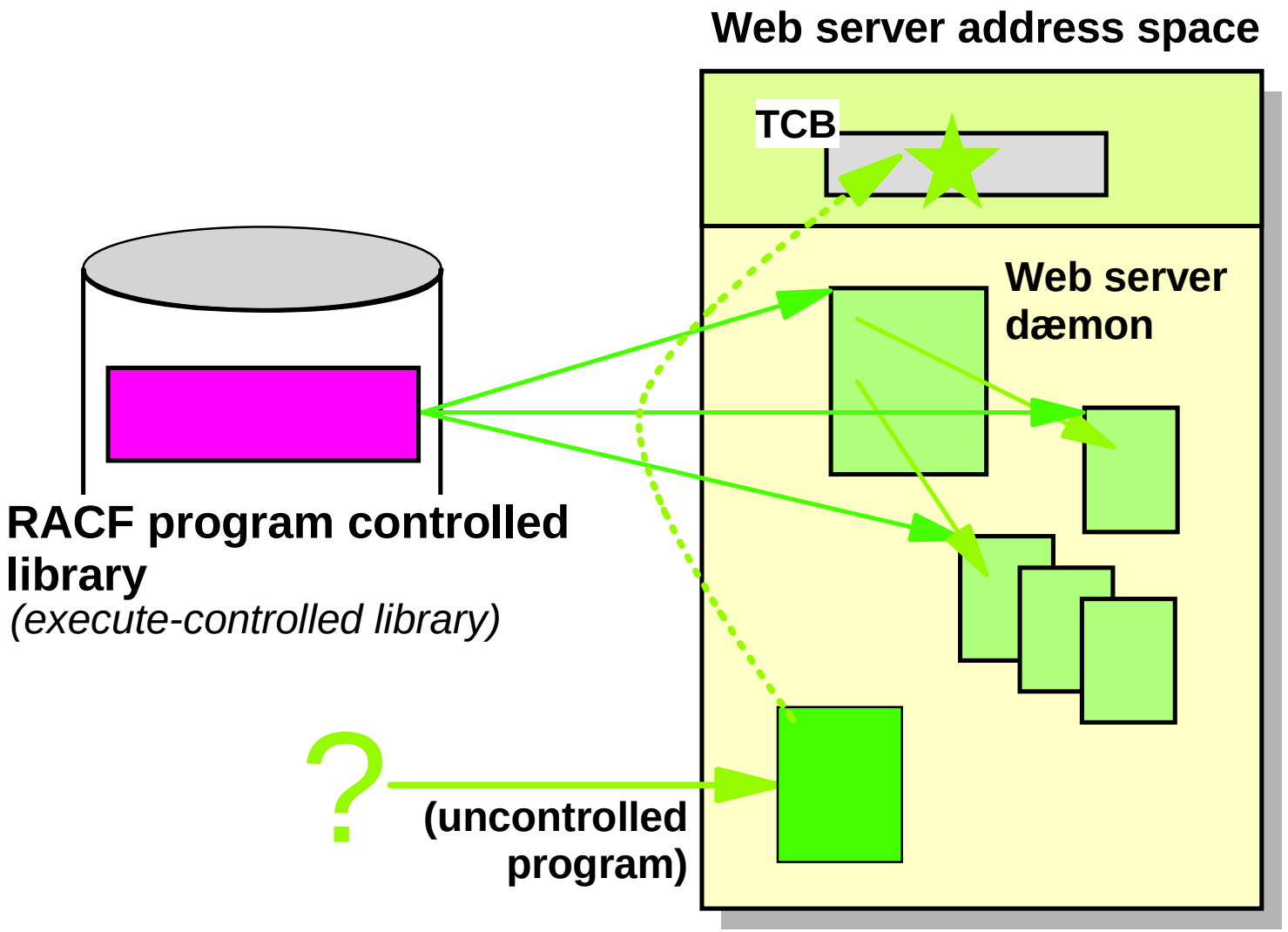
- BPX.DAEMON
  - ability to validate and assume RACF identities
  - dæmon programs can only change identity if authorized
- BPX.SERVER
  - surrogate assignment for POSIX threads
  - daemons can create threads with surrogate IDs if authorized:
    - UPDATE: client needs access authority to MVS resources
    - READ: client and server both need access authority



Protection of Daemons Against Modification and Misuse

- Dæmon programs typically run with UID 0 (Superuser)
  - Switch user IDs (UIDs) or authenticate user identities
  - Open TCP/IP ports below 1024
  - Invoke system commands of functions
- If code can be modified or modules can be replaced, daemons can be misused
- Modules are loaded from MVS search order (STEPLIB, LPA, LNKLSTxx, ...) if sticky bit is set in HFS executable
- Critical functions can only be performed if program environment is controlled:
  - Modules loaded from library defined with RACF Program Control
  - Modules loaded from HFS files with PROGCTL attribute set

Controlled Environment



Process and Thread Level Security Environment

- Platforms such as UNIX and Windows NT can assign different user identities to processes
  - Threads within a process all run under the same user identity
  - To change the identity, a child process must be forked
  - Process creation and deletion requires considerable overhead
- OS/390 can assign different user identities (UserIDs) to processes and threads
  - Processes are address spaces
  - Medium- and heavyweight threads run with their own TCB (Task Control Block)
  - Overhead for thread creation is much lower than for process
  - User Identities can be assigned at the task (thread) level
  - Access control is performed against the thread-level user

Serving Web Pages Securely from OS/390

Basic Web Server File Protection

- Protect & Protection directives in Websphere (all platforms):

```
Protection internal_only    {
    Authtype Basic
    PasswdFile /pw.file
    Mask All@150.2.*.*
    }

Protect   /intonlydata/*  internal_only
Pass  /*  /html/*
```

User Assignment and Access Control

- On other platforms, web server runs under a UserID, e.g. "Nobody"
  - This user needs access to all files served to users
  - User authentication against password file
  - Access control against mask (UserID, IP address)
- On OS/390, web server uses surrogate UserIDs
  - User authentication in RACF
  - Access control against surrogate or client UserID
  - Access control rules can be much more fine-grained
- Use OS/390 if user-based access control is needed

OS/390 Protection Setup Directives

```
Protection itso_only    {
Authtype Basic
ServerID ITSO_SERVER
PasswdFile %%SAF%%
Mask All
}

Protect   /itsodata/*  itso-only   %%CLIENT%%
```

Authtype Basic is the only valid value; indicates to encode (but not encrypt) passwords.

Unique identifier for server

Name of password file for authentication of client. %%SAF%% indicates to use RACF.

Server accepts only valid, authenticated UserIDs defined in the password file (RACF).

Server does SetUID to client's ID before serving request.

Web Server Extensions for RACF

- Web server for OS/390 allows the use of SAF authentication in place of the password file
  - specify %%SAF%% as password file
  - access to files (HFS and MVS) under normal RACF control
  - subsequent functions under control also (CGI, ICAPI, GWAPI,Servlet))
- Authority can be based on client UserID
- Can specify a surrogate User ID
  - surrogate IDs can have limited access
  - can be less administrational overhead than authorizing lots of users
- More effective access control within an enterprise network

HTTP Basic Authentication

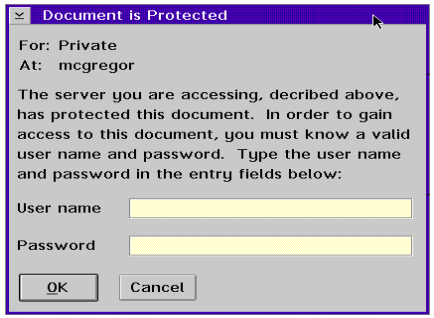
1. User clicks on link to protected page

Request: GET http://server/restricted.html

2. Server checks authority and rejects request

Response: Status 401 Realm "Private"

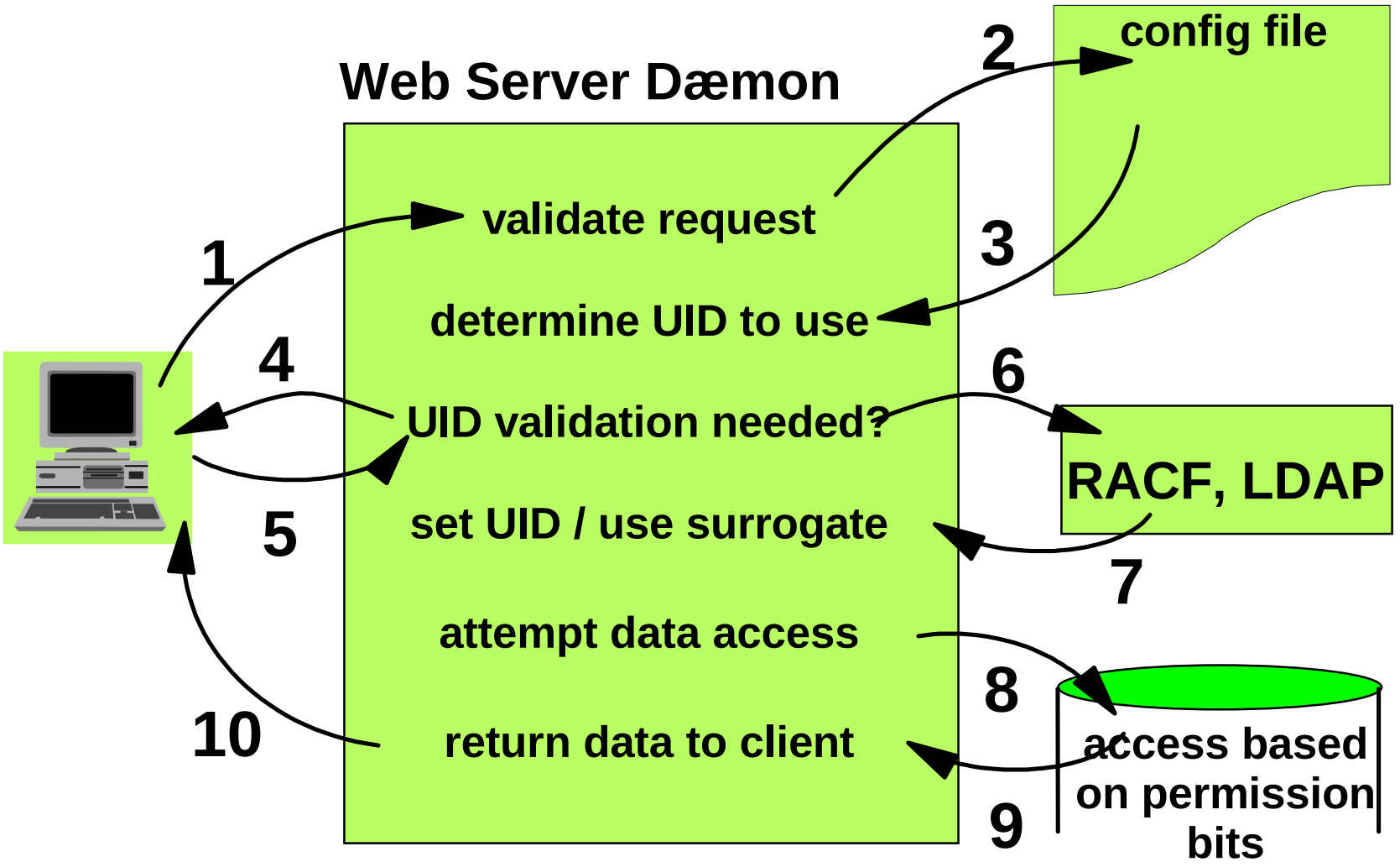
3. Browser pop-up window prompts user for user ID and password



4. Browser resends request with userid/password in request header

Request: GET http://server/restricted.html

Server Security Flow on OS/390



Basic Security - Improved

- Basic authentication is not secure
  - UserIDs and passwords are not encrypted
  - Base64 encoding is easy to decode (purpose is to avoid control characters in text, not encryption)
- Challenge mechanism causes password to be retransmitted regularly
- Improve by:
  - Wrapping messages in encrypted session
    - Use SSL (Secure Sockets Layer) if password is required
  - Avoid passwords altogether
    - OS/390 V2 R4 and later support the use of X.509 V3 certificates for RACF authentication

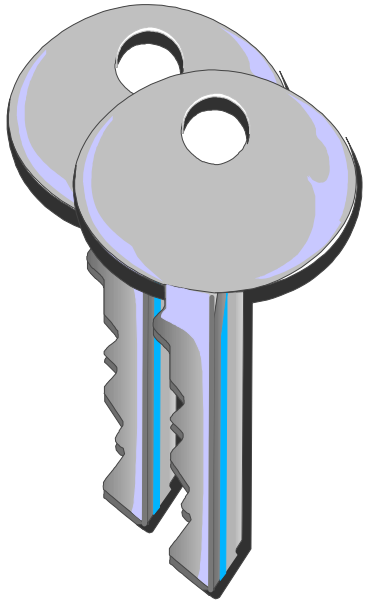
RACF Passwords

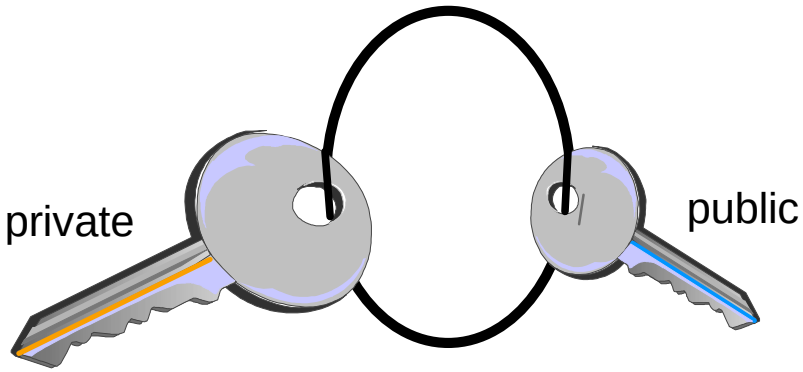
- User is prompted for RACF user ID and password with Basic Authentication dialog
- If password is expired, web server will pass an appropriate return code back to browser
  - A web server extension is available that makes changing expired RACF passwords from a web browser easy
    - Download: http://www.software.ibm.com/webservers/dgw/pwapi.c
  - Overcomes problem with HTML: password expiration and change not defined in protocol
- User can change RACF password at any time on a password prompt by typing in the password field:
  - old_password/new_password/new_password

Protecting Communications with SSL

Cryptographic Techniques for SSL

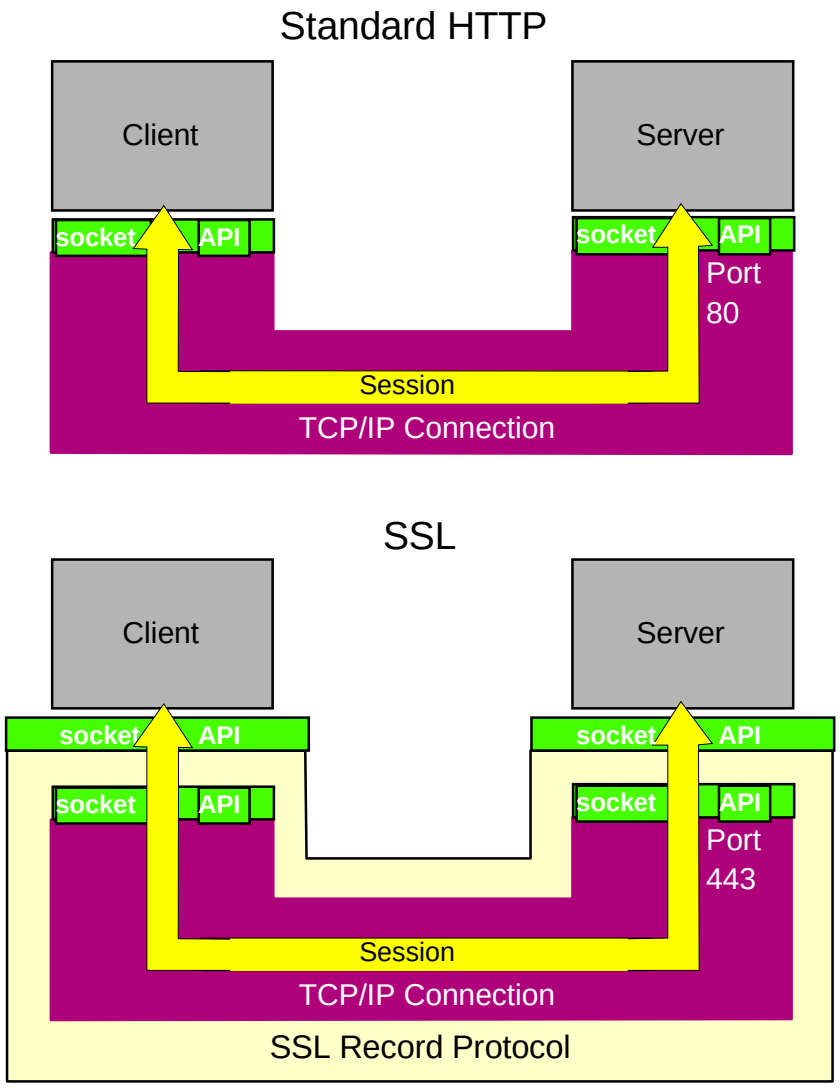
- Symmetric Encryption
  - Used to encrypt the data
  - DES, 3DES (Triple DES)
  - RC2, RC4
- Asymmetric Encryption
  - Used for key exchange and digital signatures
  - RSA
- Message Digest/ Hashing
  - For message integrity
  - MD5, SHA-1





The Secure Socket Layer Protocol

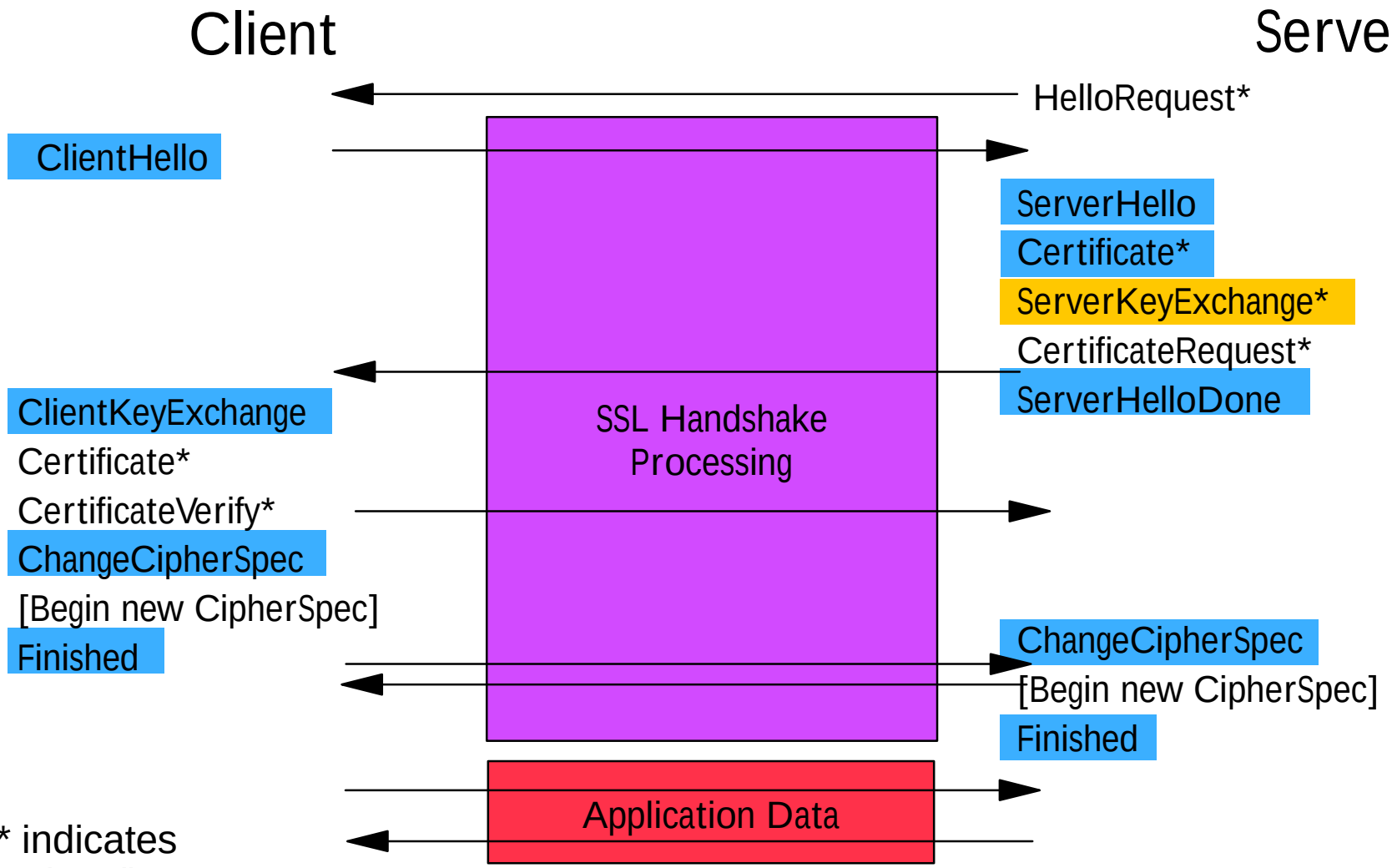
- Creates secure channel
  - Encryption, Integrity, Authentication
  - Entire session is encrypted
- Secure channel can be used for other protocols
  - TN3270E server and LDAP support SSL
- SSL request indicated by URL with https://
  - Triggers SSL handshake
  - Default port number: 443



SSL Version 3 Handshake (no Client Authentication)

- Browser starts with "Client hello"
  - Sends list of supported cipher suites in preference order
- Server sends "Server hello"
  - Selects cipher suite supported by both client and server
  - Sends server certificate
- Client verifies server certificate
  - Creates random "Pre Master Secret", encrypts with server's public key
  - Sends it in "Key exchange message"
- Client and Server generate keys
  - MAC secrets, write keys, IVs for client and server
- "Change cipher spec" and "Finished" messages
  - After these messages all data are encrypted and MACed

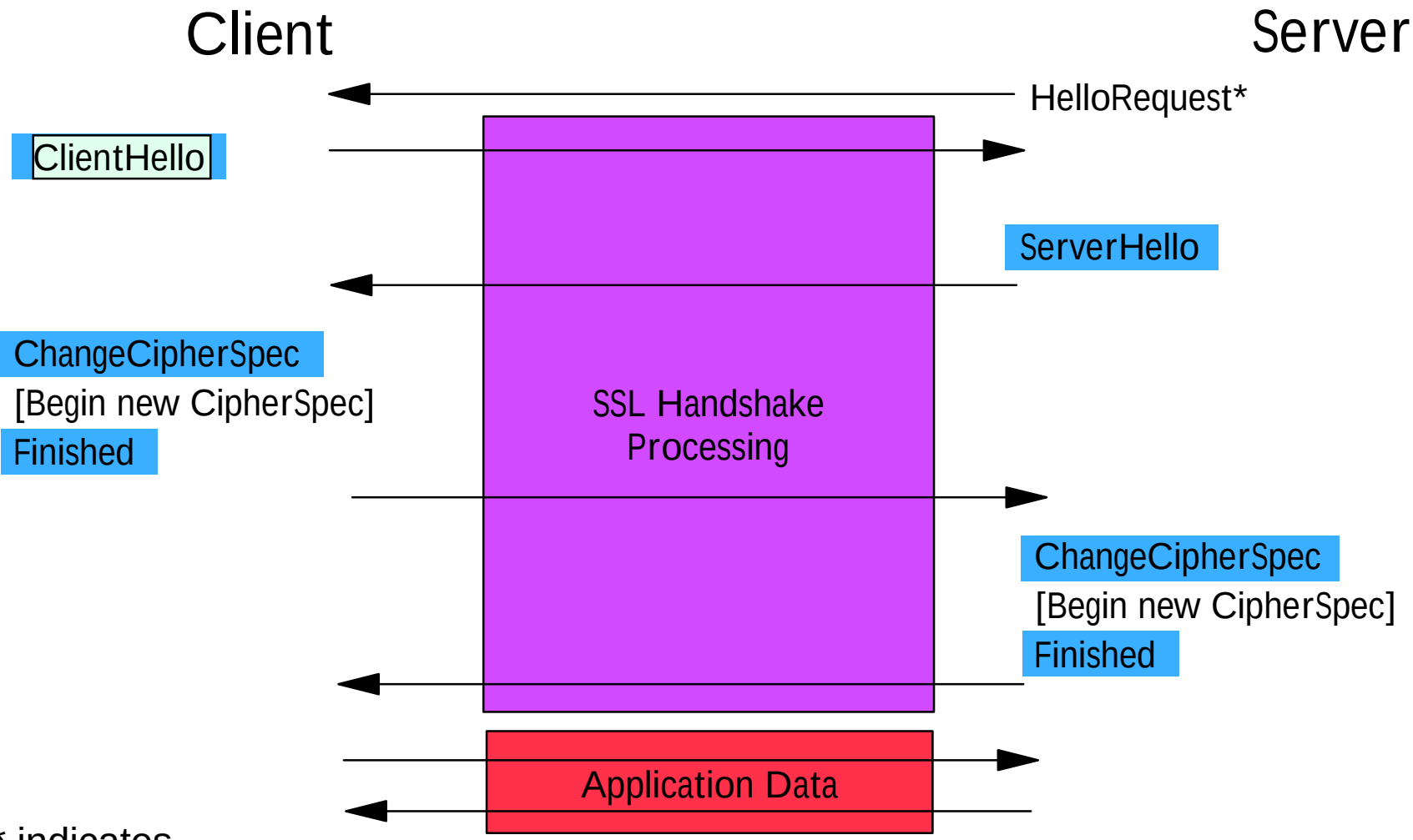
SSL Version 3 Handshake



Resuming an SSL Version 3 Session

- Browser starts with "Client hello"
  - Includes ID of previous session in message
- Server sends "Server hello"
  - Returns the same session ID to indicate that session will be resumed
  - Server caches session parameters until timeout reached
    - Default timeout for SSL Version 2: 100 seconds
    - Default timeout for SSL Version 3: 1000 seconds (ca. 15 mins.)
- No new encryption parameters for resumed session
  - Saves costly RSA decryption of "Pre-master secret"
  - New session keys are generated (different random values)
- "Change cipher spec" and "Finished" messages
  - Sent immediately after "Server hello"

Resuming an SSL Session



(* indicates Optional)

RSA CipherSuites Supported with SSL

SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
SSL_RSA_WITH_IDEA_CBC_SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

Notes:

red - exportable cipher suites

green italicized - not supported by Webspshere

Most web browsers support only a subset of these cipher suites. The cipher suites shown are for SSL V.3

SSL and US Export Regulations

- US web servers support strong encryption
  - RSA: 1024-bit keys for key exchange and signatures
  - DES: 56-bit keys; 3DES: 168-bit keys; RC2, RC4: 128-bit keys
- Export web servers support weak encryption
  - RSA: 512-bit or 1024-bit keys for key exchange, 1024-bit keys for signatures
  - DES: 56-bit keys, RC2, RC4: 40-bit keys
- Special rules exist for some industries
  - Banks, insurance companies, health industry and e-commerce in many countries can get a license for US strength encryption

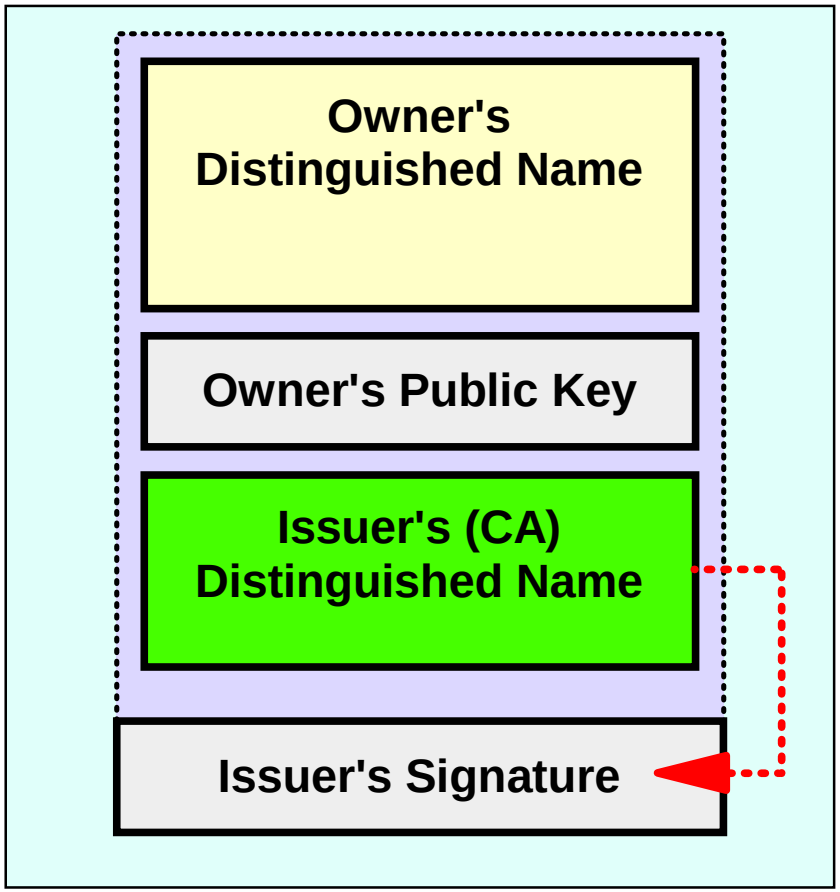
Note: This new, more relaxed export policy was announced on Sept. 16,1998 by the US Government.

US Export Regulations (Web Browsers)

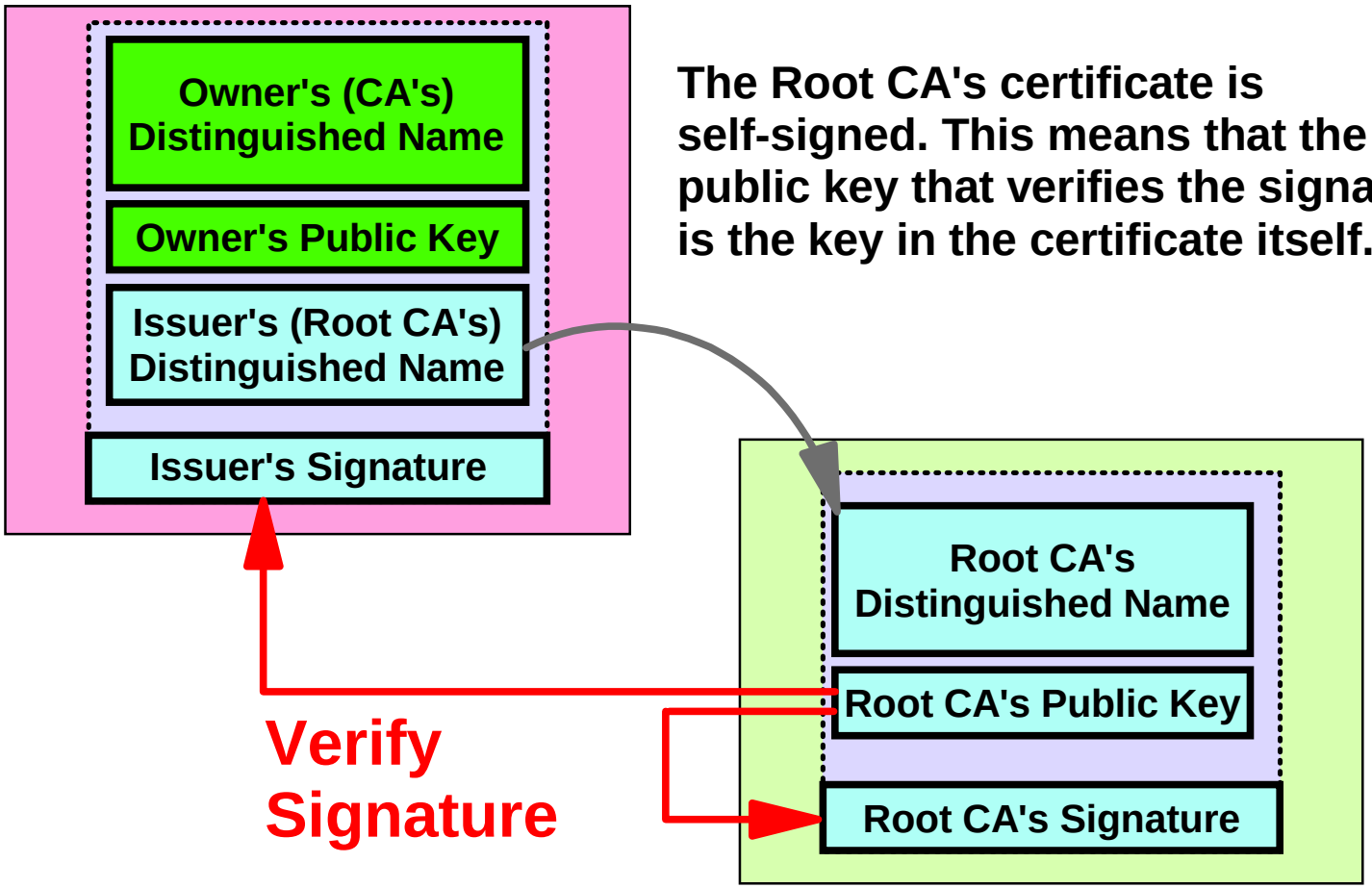
- US Versions of Web Browsers
  - Netscape Navigator/Communicator, Microsoft Internet Explorer
  - RSA: 1024-bit keys for key exchange and signatures
  - DES: 56-bit keys; 3DES: 168-bit keys; RC2, RC4: 128-bit key
- Export (International) Versions of Web Browsers
  - Netscape Navigator/Communicator, Microsoft Internet Explorer
  - RSA: 512-bit keys for key exchange, 1024-bit keys for signatures
  - RC2, RC4: 40-bit keys
  - Netscape Communicator 4.6 and Microsoft Internet Explorer 5.1 support 1024-bit keys for key exchange together with DES with 56-bit keys

Digital Certificates

- Certificate identifies its owner
- Main purpose is to publish the owner's public key
- Issuer is a Certification Authority (CA)
- Issuer's digital signature certifies the owner's identity and public key
  - Allows anyone who has CA certificate to verify the validity of the certificate



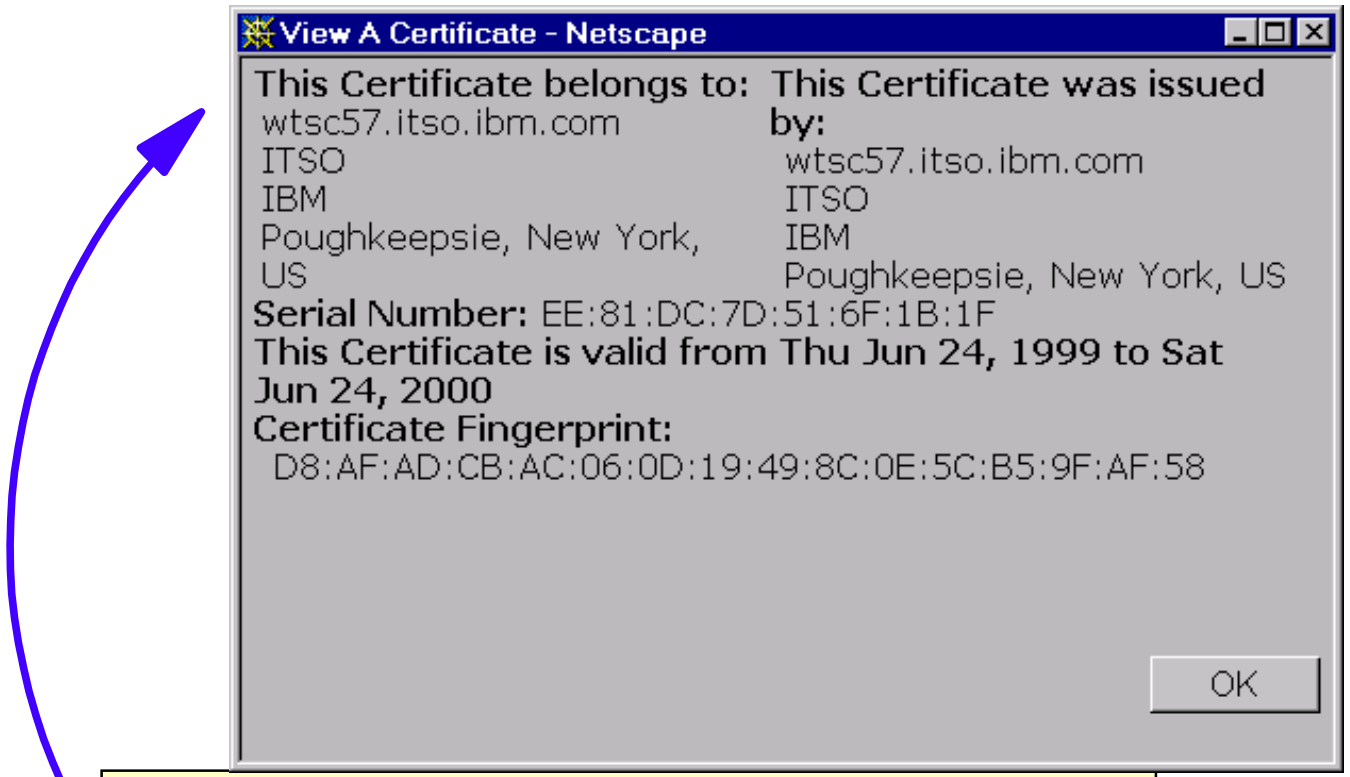
Certificate Hierarchy



The Root CA's certificate is self-signed. This means that the public key that verifies the signature is the key in the certificate itself.

Certificates can only be verified if the Root CA's certificate has been received in a trusted manner (e.g. pre-installed with the web browser)

Server Certificate Example



Address in URL must match address in certificate or browser will display warning message.

Using Global Server Certificates

Why Global Server Certificates?

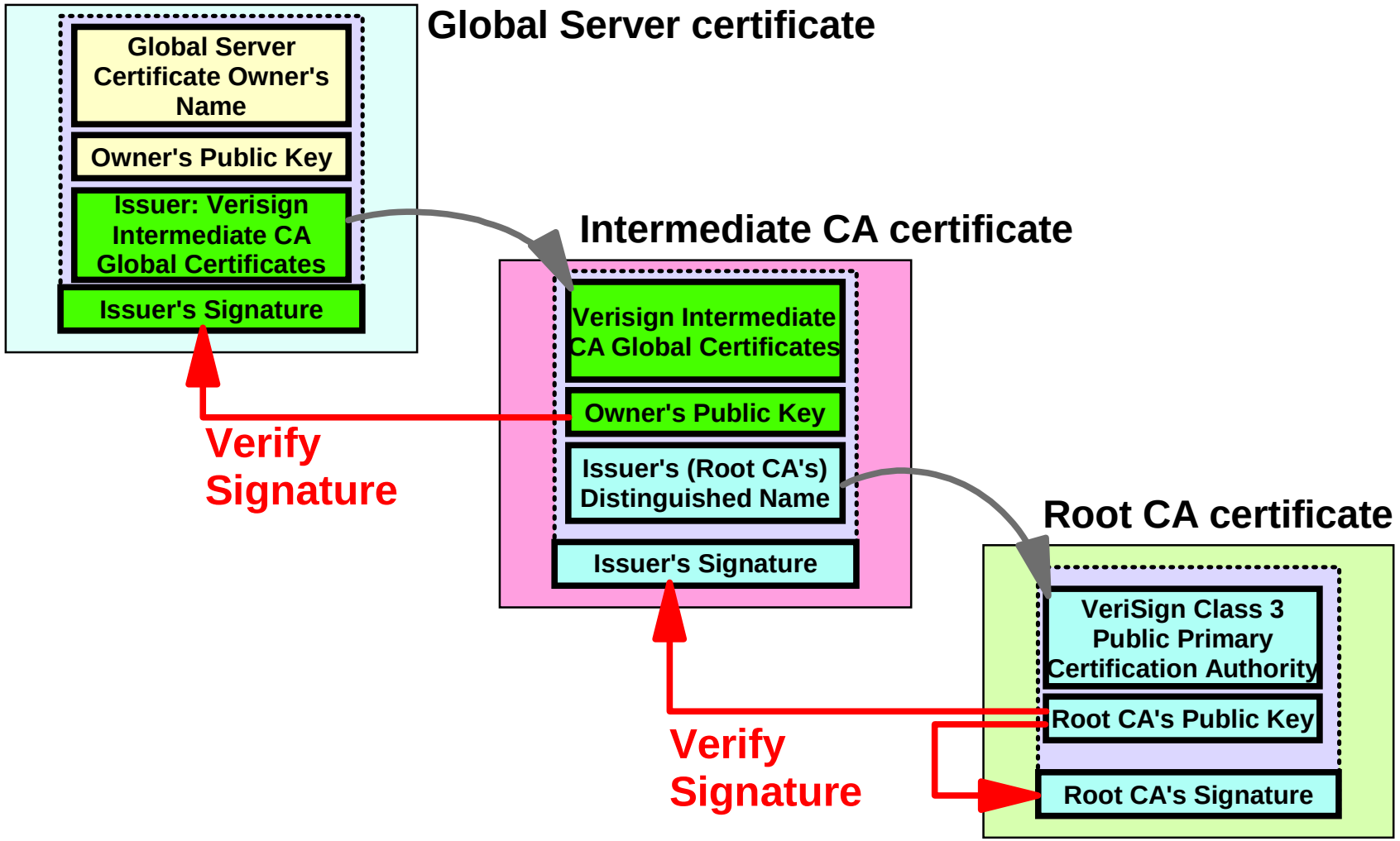
- Banks, insurance companies, health care industry and e-commerce providers can obtain US strength cryptographic products
- Users outside the US and Canada cannot obtain US strength web browsers
- Strong encryption can only be used in SSL sessions if supported by both web server and browser
- Companies with US strength cryptographic products can obtain Global Server Certificate
- Export web browsers recognize Global Server Certificate and "step up" to US strength encryption
  - RC2 128-bit, RC4 128-bit, 3DES 168-bit

Obtaining a Global Server Certificate

Obtaining a Global Server Certificate...

- Certificate must be requested from provider in USA
  - VeriSign Inc. is authorized by US Government
  - Thawte Certification also claims to be authorized
- Proof of eligibility is required
  - Proof can be through D-U-N-S number
  - If not available, appropriate legal documents must be provided (translated to English, if required)
- Companies should get a D-U-N-S number from Dun & Bradstreet
- ITSO Poughkeepsie has published a Redbook that explains how to obtain and install the certificate

Global Certificate Hierarchy



Using the S/390 Cryptographic Coprocessor

Hardware Crypto Prerequisites

- Cryptographic Coprocessor must be activated with Hardware Enablement Diskette
- Cryptographic Coprocessor must be initialized with master keys, using TKE or ICSF panels
- Integrated Cryptographic Service Facility (ICSF) must be active
- Appropriate cryptographic algorithms (DES or TDES) must be supported by Hardware Enablement Diskette
- TDES is not supported for G3 servers, only G4 and higher

Use of Cryptographic Coprocessor

- DES algorithm and Triple DES algorithm are implemented in cryptograhic hardware
  - Hardware used by Websphere automatically if ICSF is active
- DES algorithm used is DES-CBC
  - Cipher Block Chaining mode, keylength 56 bits
- Triple DES algorithm used is 3DES-EDE-CBC
  - Encrypt with key 1, decrypt with key 2, encrypt with key3
  - Cipher Block Chaining mode, equivalent key length 168 bits
- RC2 and RC4 algorithms are implemented in software (proprietary algorithms of RSA Inc.)
- MD5 and SHA-1 hash functions are implemented in software

APAR PQ22108 for DGWS 5.0

- Introduces additional use of the S/390 Cryptographic Coprocessor during SSL handshake
- RSA decryption of pre-master secret with server's private key now done in hardware
  - Independent of use of cryptographic hardware for symmetric encryption (DES, Triple DES)
  - Also done if symmetric encryption is done with software routines (RC2, RC4)
- Accounts for up to 70% of CPU usage during server's part of SSL handshake
  - Performance improvement especially important if Global Server Certificate is used
- Requires OS/390 V2R6 or later for ICSF support

APAR PQ19981 for DGWS 5.0

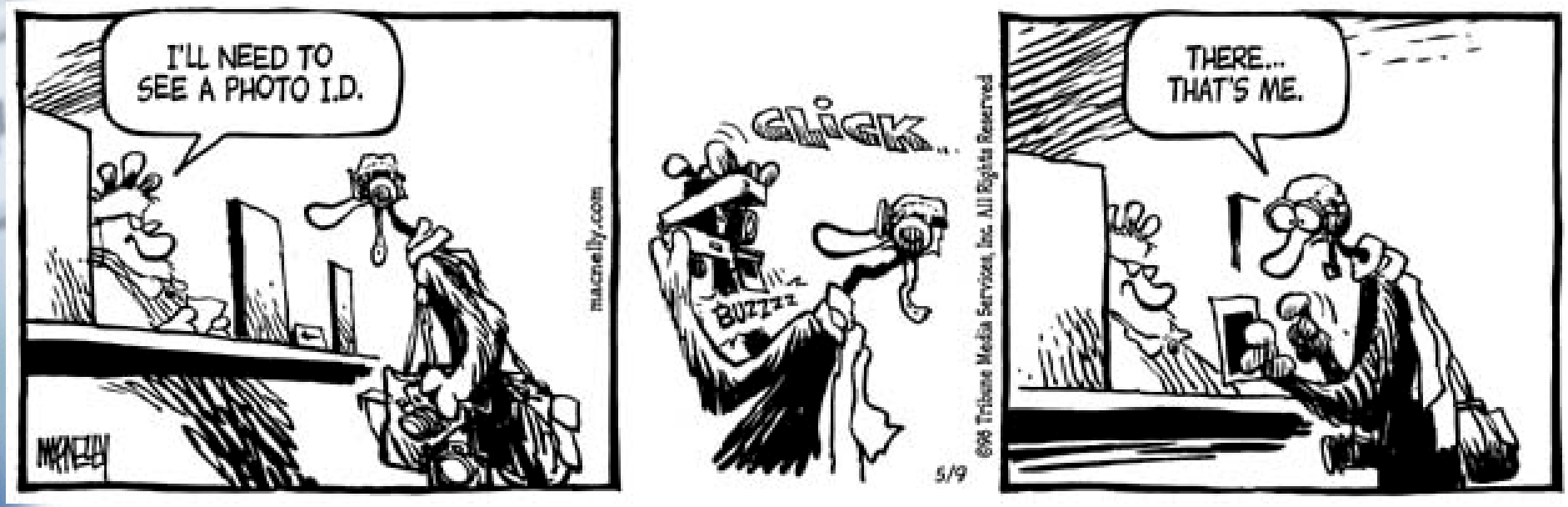
- Additional performance improvements for SSL handshake processing
  - Eliminates serialization problems
- Independent of use of S/390 Cryptographic Coprocessor
  - Problems solved are unrelated to cryptography
- Users of IBM HTTP Server 5.1 should install the PTF for APAR PQ23829

Any installation using a webserver on OS/390 with SSL should have at least OS/390 V2R6 with DGWS 5.0 and both PTFs installed (if good SSL performance is required).

Improving Security with Client Certificates

e-business

Get the idea (ID)...

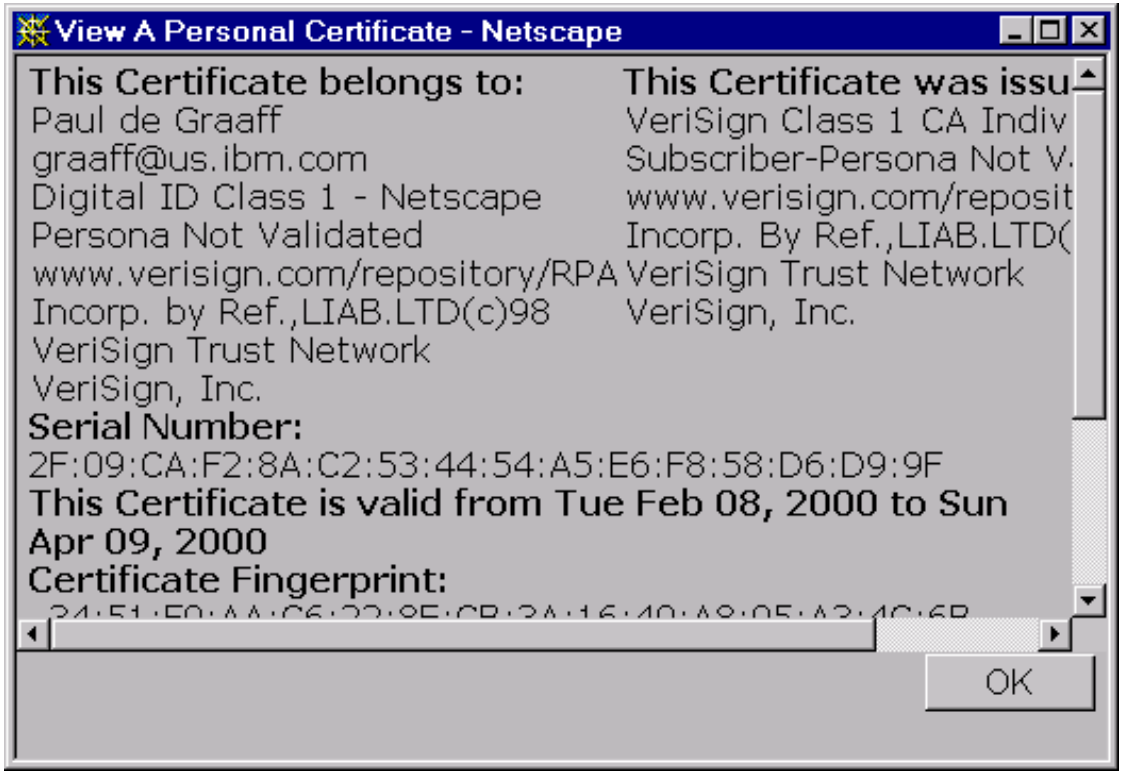


IBM

Client Certificate Advantages

- UserID/password prompts in an Internet environment allow for denial-of-service attacks
  - Use of certificates can eliminate password prompts
- Expired passwords cause usability problems
- Passwords can be shared with others, spied out, or guessed
  - Certificates are unique (specifically on SmartCards)
  - No attack other than brute force is known against RSA private key
- Certificates expire after a pre-determined time
  - After expiration, new certificate must be acquired
  - Certificate Revocation List (CRL) processing system handles unexpired certificates that have become invalid (LDAP)

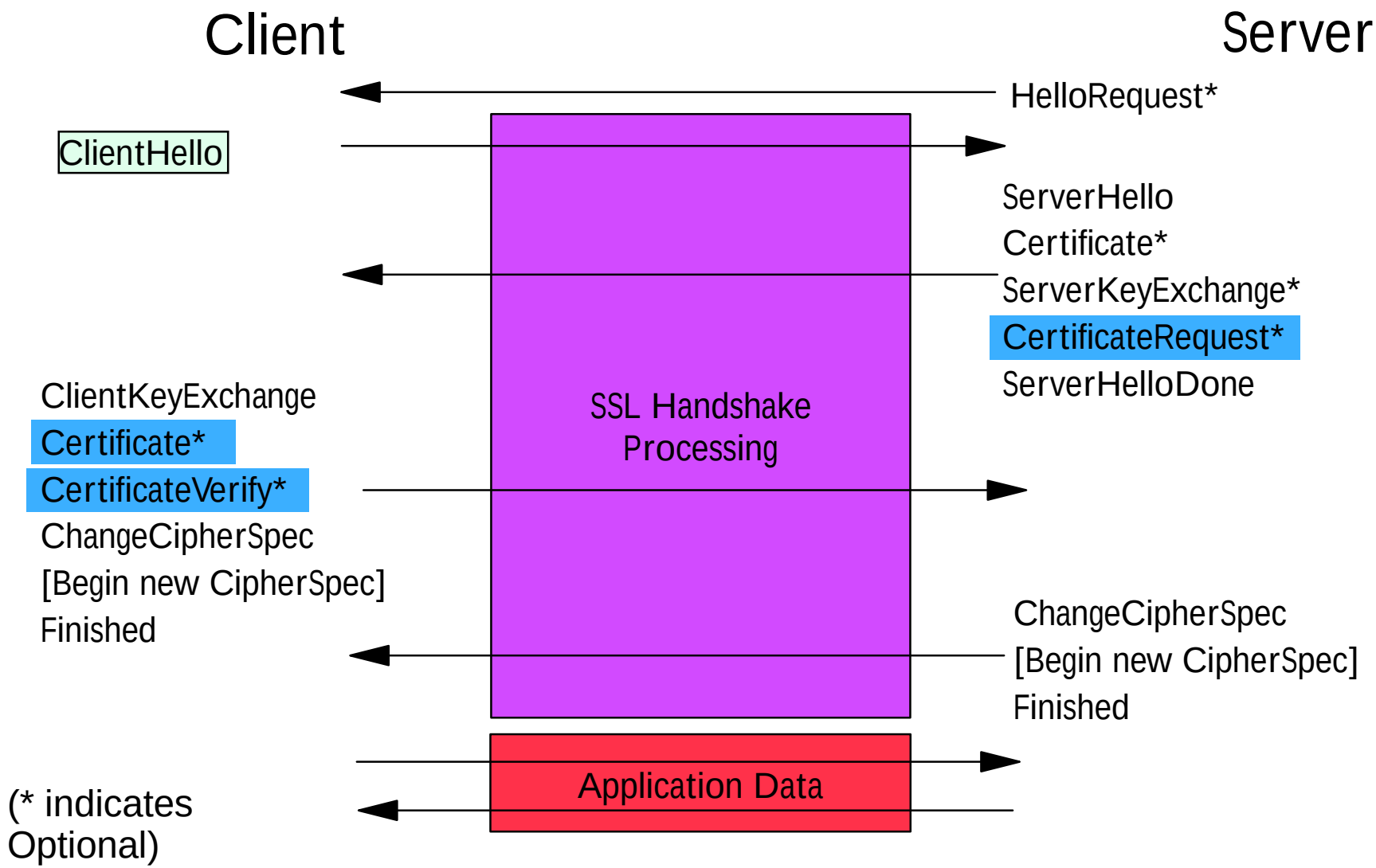
Digital Client Certificate



SSL Version 3 Handshake with Client Authentication

- If client authentication is required, server sends "Certificate request" after sending its own certificate
- Client sends client certificate
  - If no certificate is available, client sends a "no_certificate alert"
- After Key exchange message, client sends "Certificate verify" message
  - Message is non-replayable and signed with the private key that belongs to the public key in the certificate
  - Server can verify that the certificate belongs to the client (ownership of private key is proof)
- Handshake continues with "Change cipher spec" and "Finished" messages

SSL Version 3 Handshake with Client Authentication...



RACF Certificate Support

- Protection directive using certificate verification:

```
SSLClientAuth   On
.....
Protection confidential   {
   Authtype Basic
   ServerID Conf_Server
   PasswdFile %%SAF%%
   UserID   %%CERTIF%%
   Mask   Anybody
   }
```

Enables client authentication for all SSL sessions

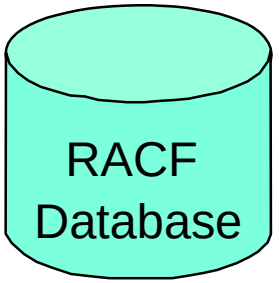
Name of password file for authentication of client. %%SAF%% indicates to use RACF.

Tells web server to ask RACF for UserID associated with client certificate

If "Mask All" is used, user is prompted for UserID/password additionally

Traditional Authentication on OS/390

RACF UserID/Password

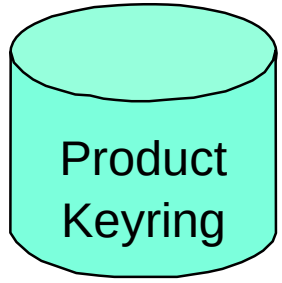


1. Validate if Userid exists ?
2. Password o.k. ?
3. UserID not revoked ?

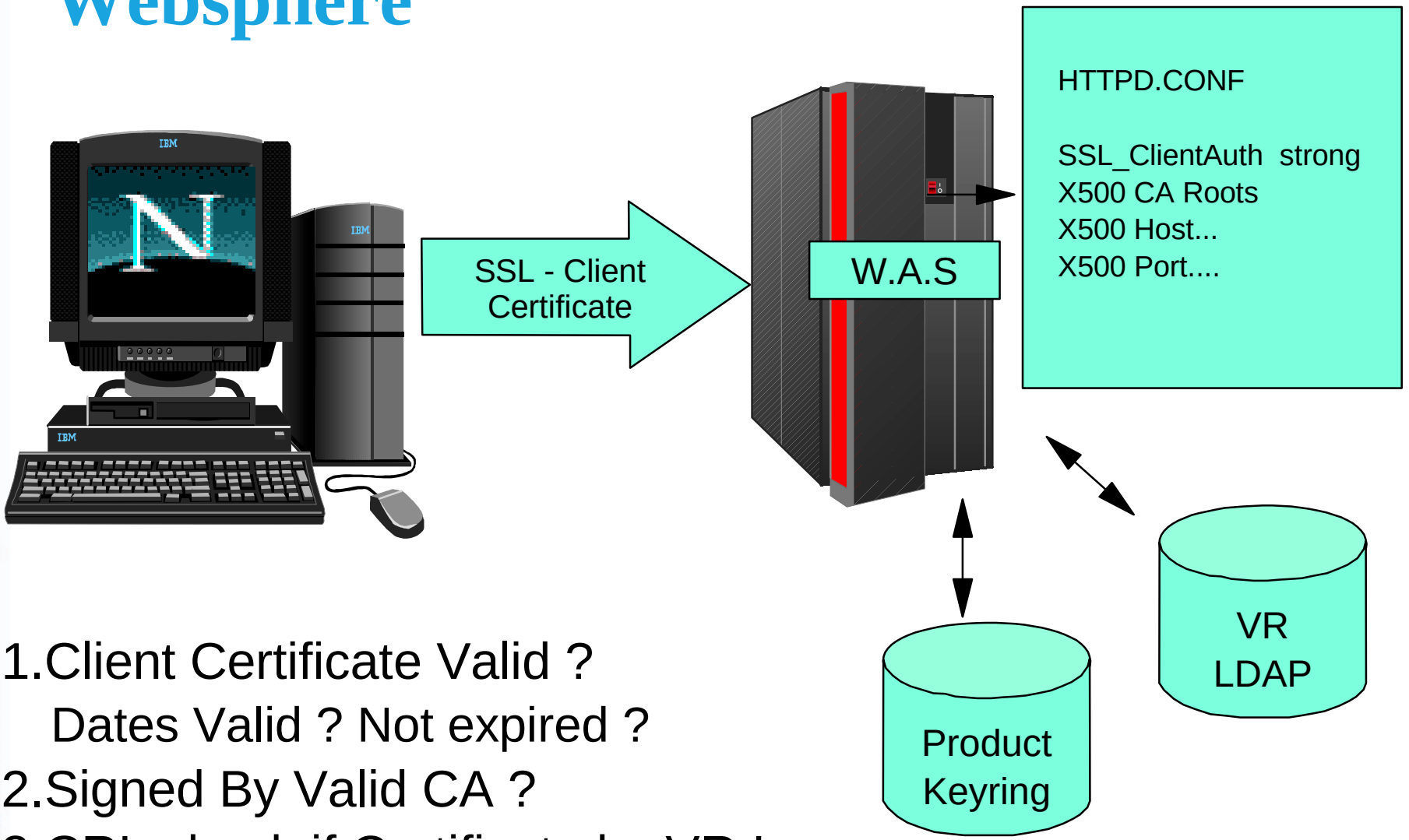
PKI Authentication

SSL - Client Certificate

1. Client Certificate Valid ?
   Dates Valid ? Not expired ?
2. Signed By Valid CA ?
3. Standard no check for revocation !



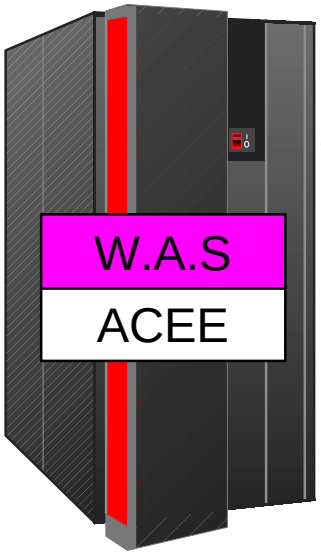
PKI Strong Authentication using Websphere



1. Client Certificate Valid ?
   Dates Valid ? Not expired ?
2. Signed By Valid CA ?
3. CRL check if Certificate by VR !

PKI Authentication beyond Websphere

SSL - Client Certificate



HTTPD.CONF

Userid %%CLIENT%%
Userid %%CERTIF%%
Userid %%SERVER%%

CICS

IMS

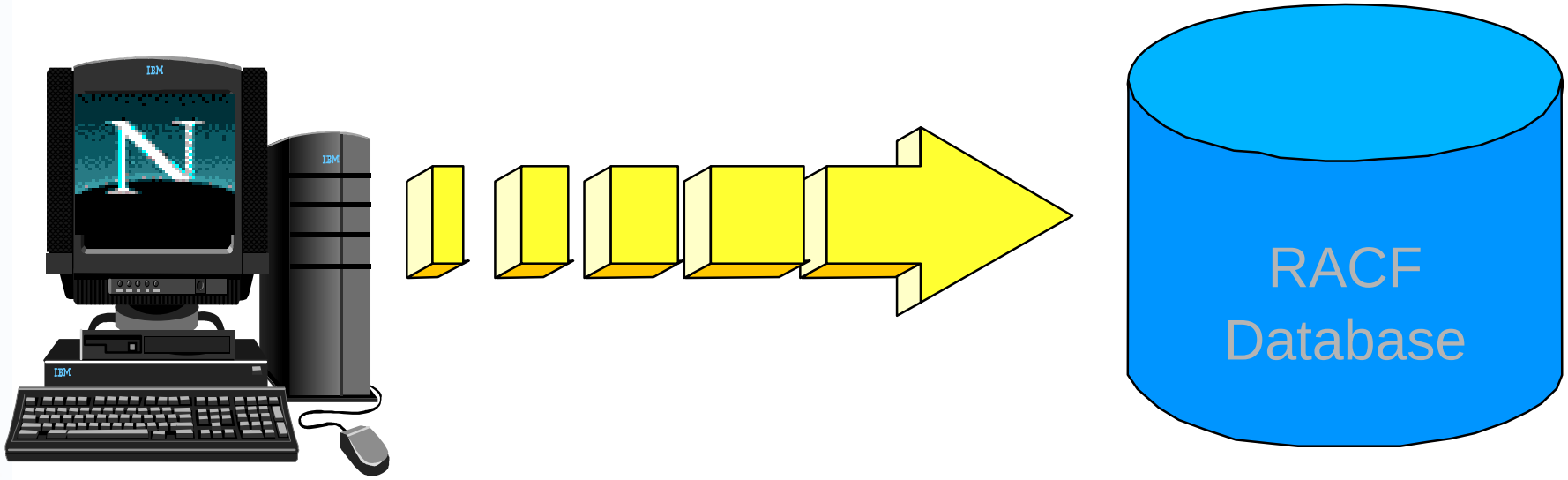
DB2

etc..

RACF Database

%%CERTIF%% means map certificate to a RACF Userid to access any application or data

How to get your certificate into RACF ?



Certificate is stored in the Browser on the Workstation or a smartcard !

Certificate stored in RACF through a new TSO command called RACDCERT !

Overview of the Self registration process

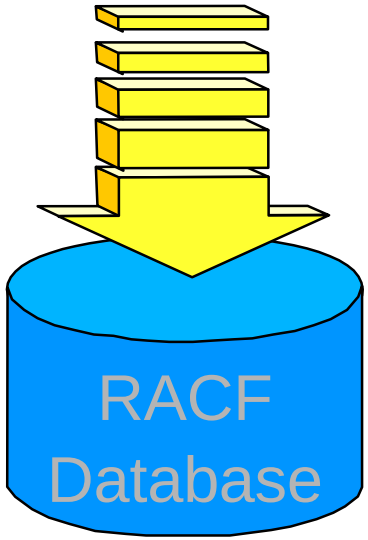
SSL V3

RACF
USERID/PASSWORD

OS/390 WEBSERVER

Webpage calls the initACEE callable service to register certificate

1.Client needs to have a certificate
2.Client presents it's certificate
3.Client needs to know his RACF userid/password.
4.Client needs read access to IRR.DIGTCERT.function profile



The problem with one on one approach

- To enable e-business
  - Every user must be identified
  - Every user's certificate must be installed into RACF
  - Each user can have many certificates
  - Certificates expire

The solution ...

- Certificate name filtering
  - Allows the grouping of many certificates to one user ID
  - Certificates are not stored by RACF
    - more users can be identified
    - eliminates expiration problems
  - Accountability is maintained
  - Access by shared user IDs can be restricted

Grouping user certificates

- RACDCERT is used to create a filter and map it to a RACF user ID
- Filtering is based on the subject's-name and the issuer's-name from a certificate (the X500 name)
  - subject's-name || issuer's-name
- RACDCERT command or ISPF panels can be used
  - DIGTNMAP class contains the mapping
- Each filter must be unique
- Other criteria such as application ID or system name can be used in determining the user ID
  - DIGTCRIT class is used for additional criteria

RACDCERT examples

- A customer's certificate
  - Subject: CN=Sid Shopper.OU=Customer.O=Ohio.C=US
  - Issuer: OU=BobsMart Subscriber.O=Verisign,Inc.L=Internet

- Map all customers in Ohio to a state user ID
  - RACD ID(OHIOUSER) MAP SDNFILTER(OU=Customer.O=Ohio.C=US) IDNFILTER(OU=BobsMart Subscriber.O=Verisign,Inc.L=Internet)
- Map this certificate to Sid's user ID
  - RACD ID(SIDS) MAP SDNFILTER(CN=Sid Shopper.OU=Customer.O=Ohio.C=US) IDNFILTER(OU=BobsMart Subscriber.O=Verisign,Inc.L=Internet) WITHLABEL('Cert for Sid')
- Map all BobsMart certificates to a general ID
  - RACD ID(ALLB) MAP WITHLABEL('General Bobs cert') IDNFILTER(OU=BobsMart Subscriber.O=Verisign,Inc.L=Internet)
- Map other company's certificates to PUBLIC
  - RACD ID(PUBLIC) MAP IDNFILTER(O=Verisign,Inc.L=Internet)

CNF criteria in action

Websphere
A

CICS
A

because criteria include application
id websphere A, userid WEBA assigned

because criteria include application
id CICS A, userid CICSA assigned

Subject: CN=Sid Shopper.OU=Customer.O=Ohio.C=US
Issuer: OU=BobsMart Subscriber.O=Verisign,Inc.L=Internet

RACDCERT command enhancements

```
RACDCERT [ID(user-id) | MULTIID]
   MAP [('cert-dsn')]
     [SDNFILTER('subject-dist-name-filter')]
     [IDNFILTER('issuer-dist-name-filter')]
     [CRITERIA('criteria-profile-name-template')]
     [WITHLABEL('label-name')]) [TRUST | NOTRUST]

   LISTMAP (LABEL('label-name'))

   ALTMAP (LABEL('label-name'))
     [NEWCRITERIA('criteria-profile-name-template')]
     [NEWLABEL('label-name')] [TRUST | NOTRUST]

   DELMAP (LABEL('label-name'))
```

Restricting user access

ADDUSER user-ID RESTRICTED
ALTUSER user-ID [RESTRICTED | NORESTRICTED]
LISTUSER user-ID
Output for a restricted user shows RESTRICTED attribute

Restricted access attribute means:
Global access checking is bypassed
UACC cannot be used to allow access
ID(*) on access list will not allow access

Indicated by bit in ACEE (ACEERAUI)
Supported by panels, R_admin, and DBunload
Satisfies customer requirement REQ00064015

Installation

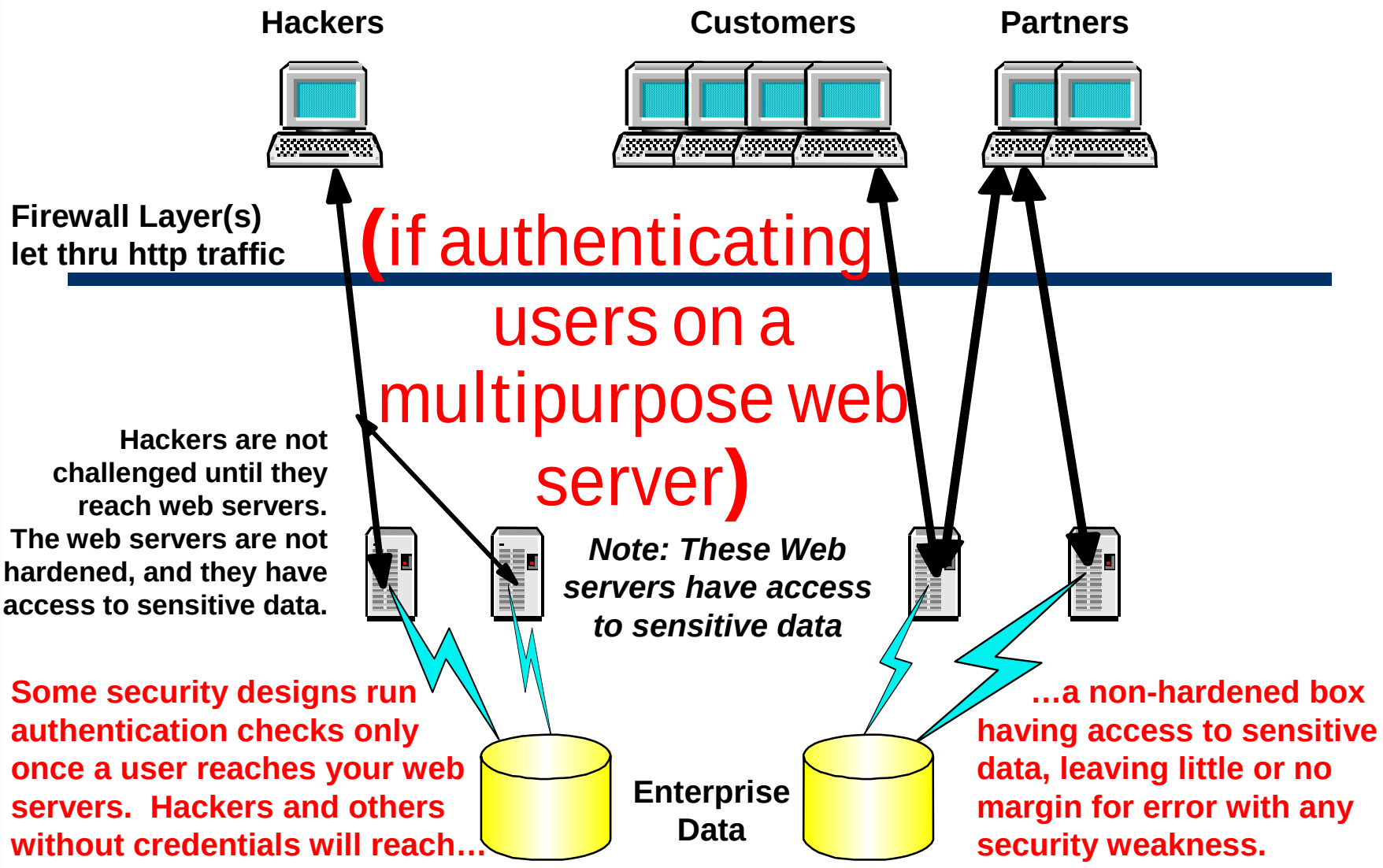
- Apply PTFs for these APARs
  - OW40129 for RACF
  - OW40130 for SAF
- Function will be available for both OS/390 R8 and OS/390 R9

Web Security Architecture Choices

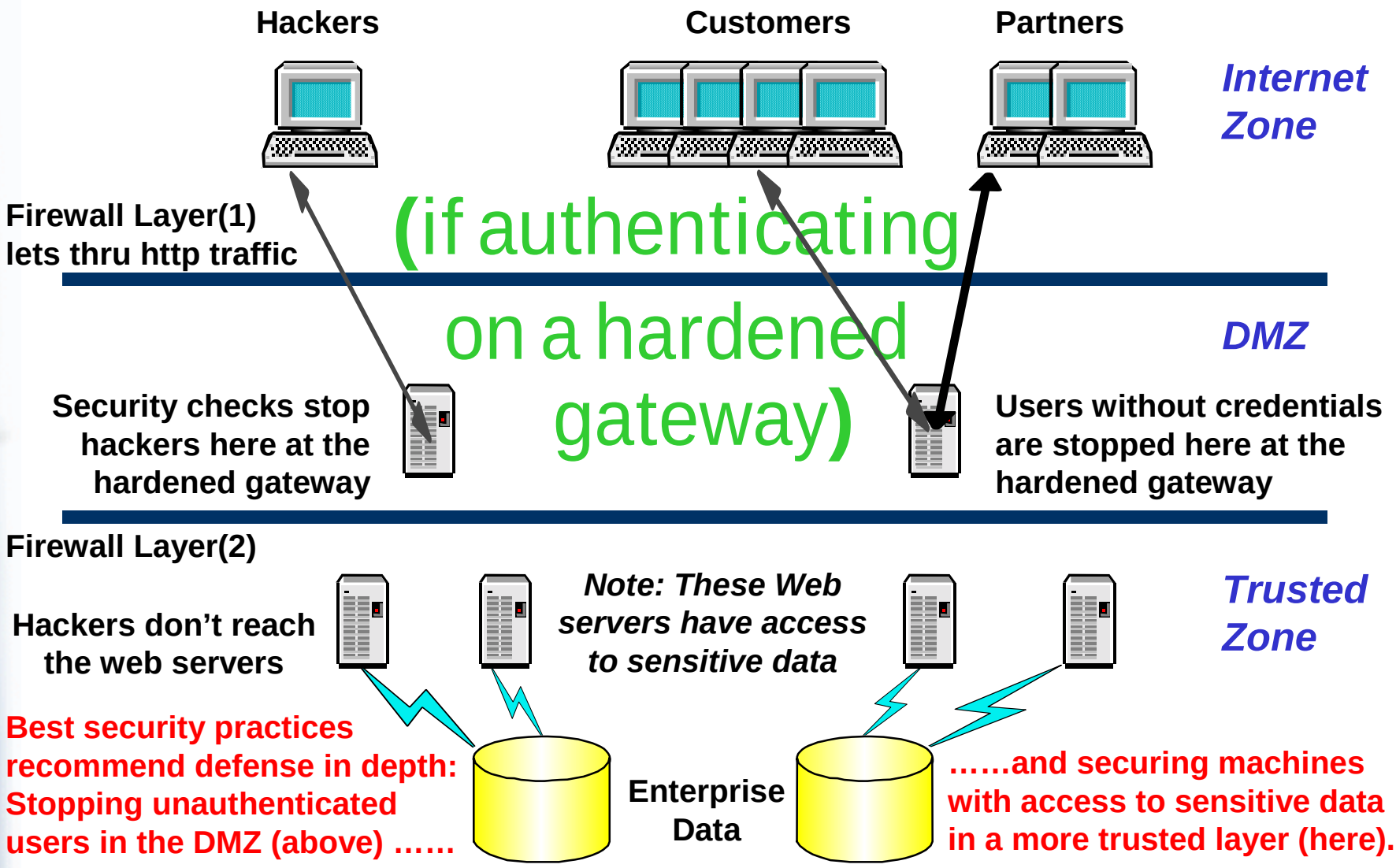
Architecture Choices for Web Security

- Where to authenticate: On a multipurpose web server, or a hardened gateway?
- Where to place web servers: in a DMZ, or in a trusted zone?
- How many entry points to your secured network - many or f
- How many software distribution points - many or few?
- Entry-point security only, or End-to-End security?

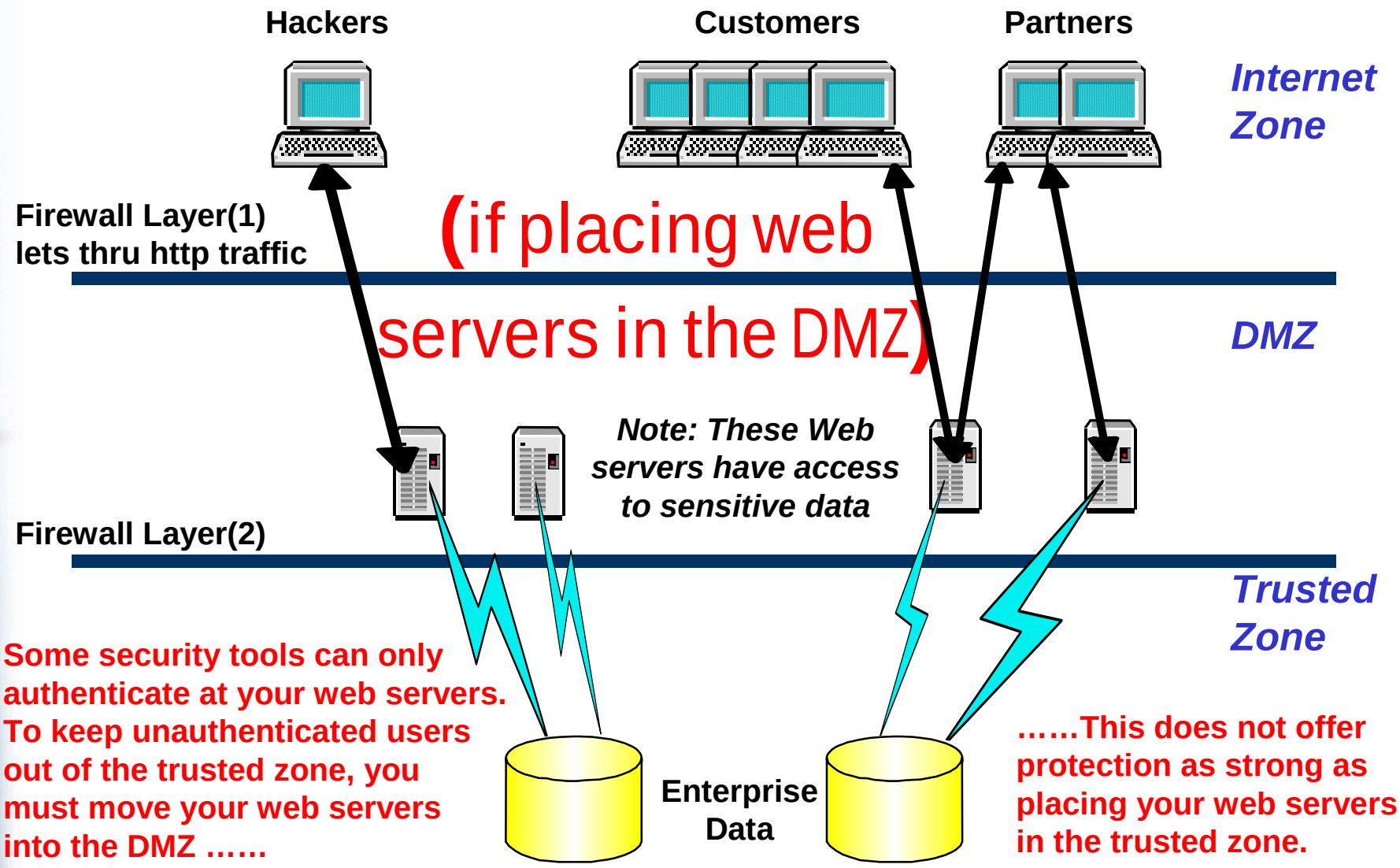
Where to Authenticate: on a multipurpose web server, or on a hardened gateway? (scenario 1)



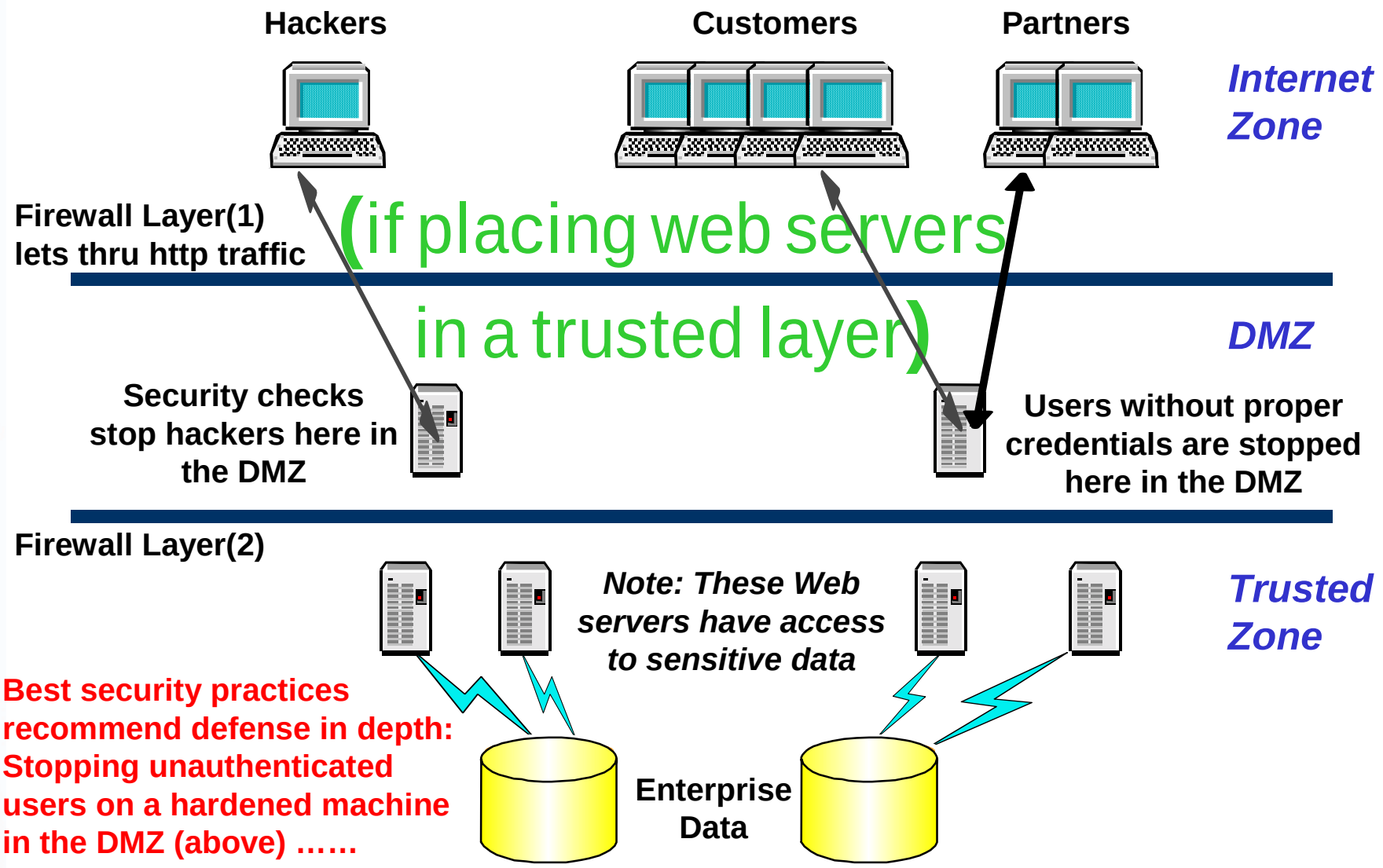
Where to Authenticate: on a multipurpose web server, or on a hardened gateway? (scenario 2)



Where to place web servers: in a DMZ, or in a trusted layer? (scenario 1)

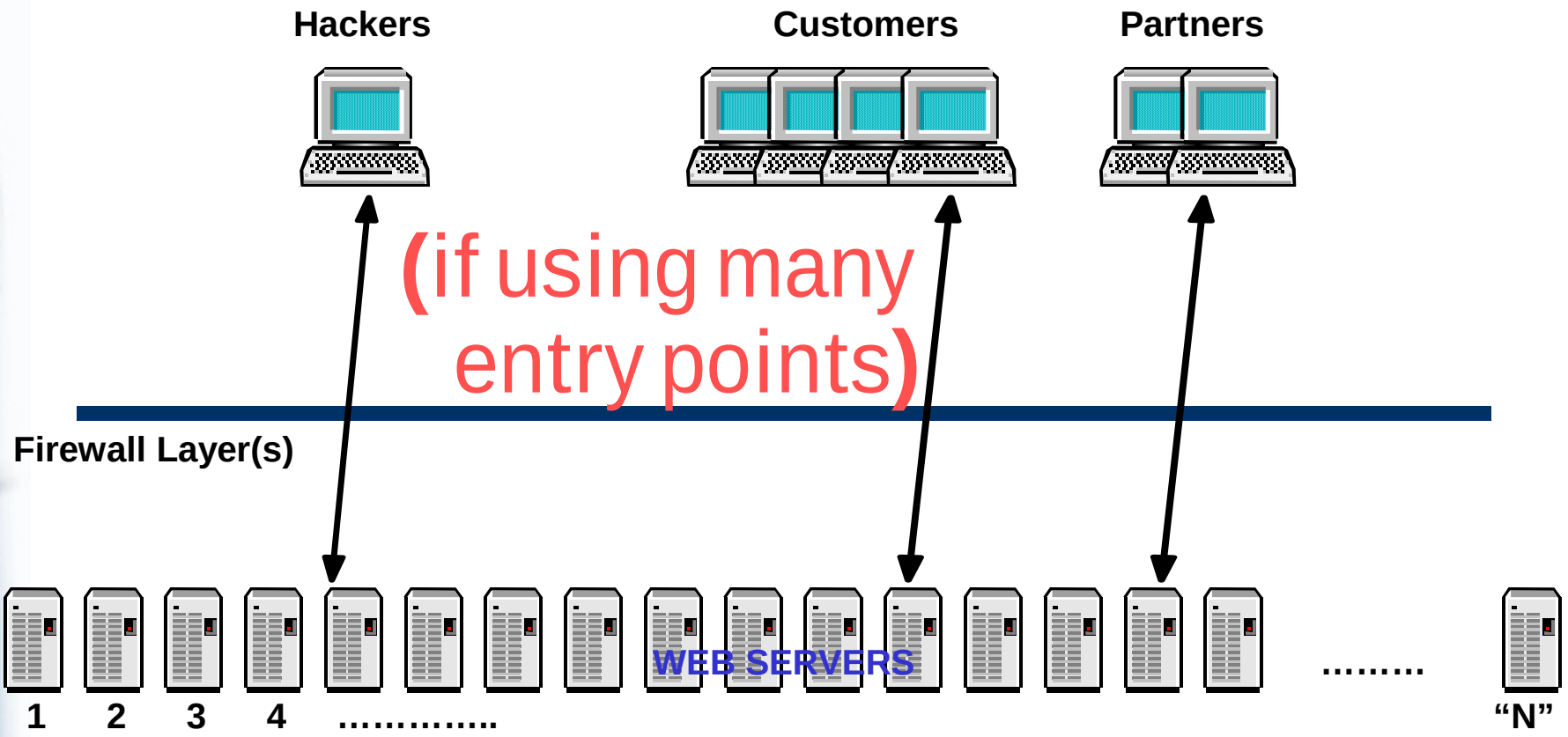


Where to place web servers: in a DMZ, or in a trusted layer? (scenario 2)

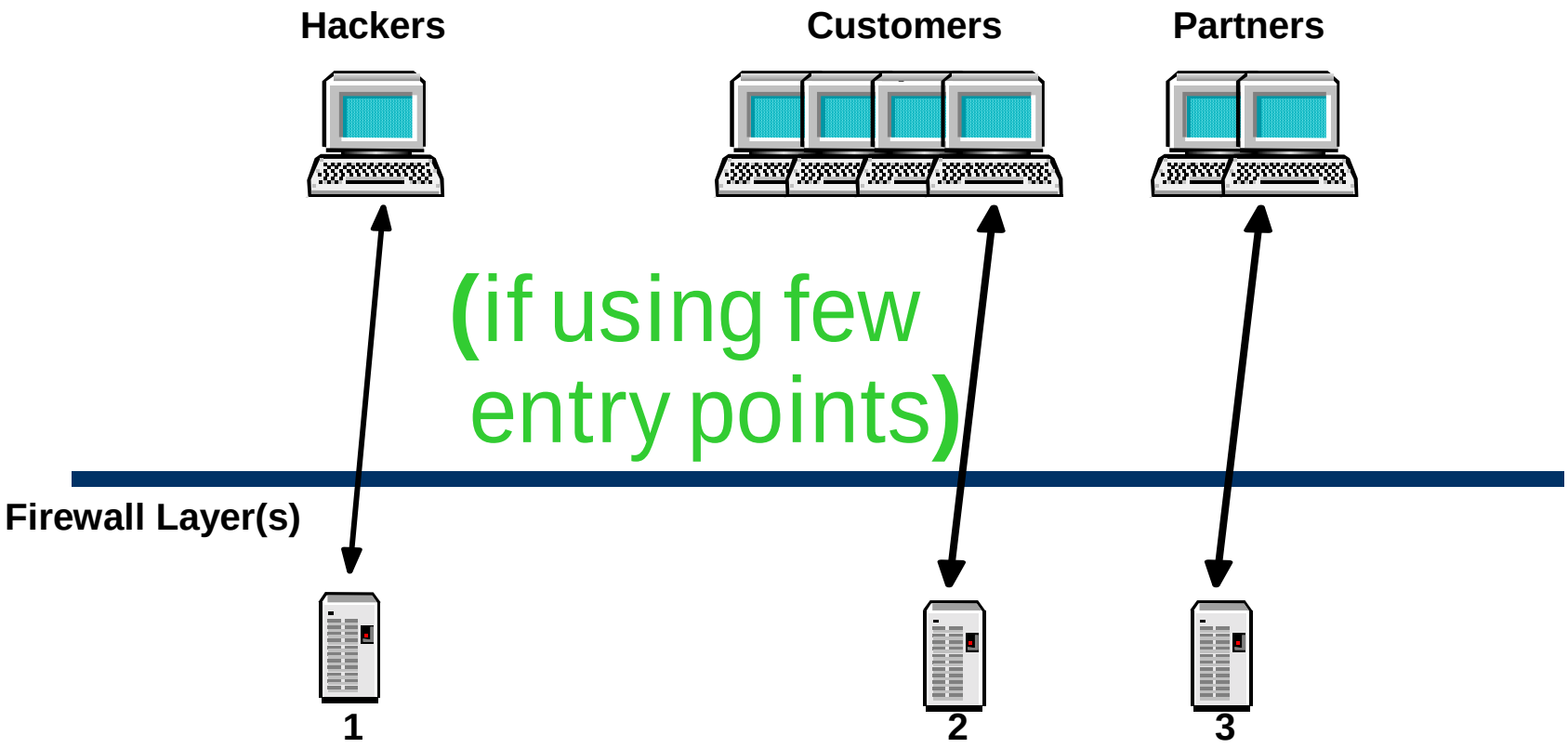


Best security practices recommend defense in depth: Stopping unauthenticated users on a hardened machine in the DMZ (above) ……

How many entry points to your secured network: many or few? (scenario with "many")

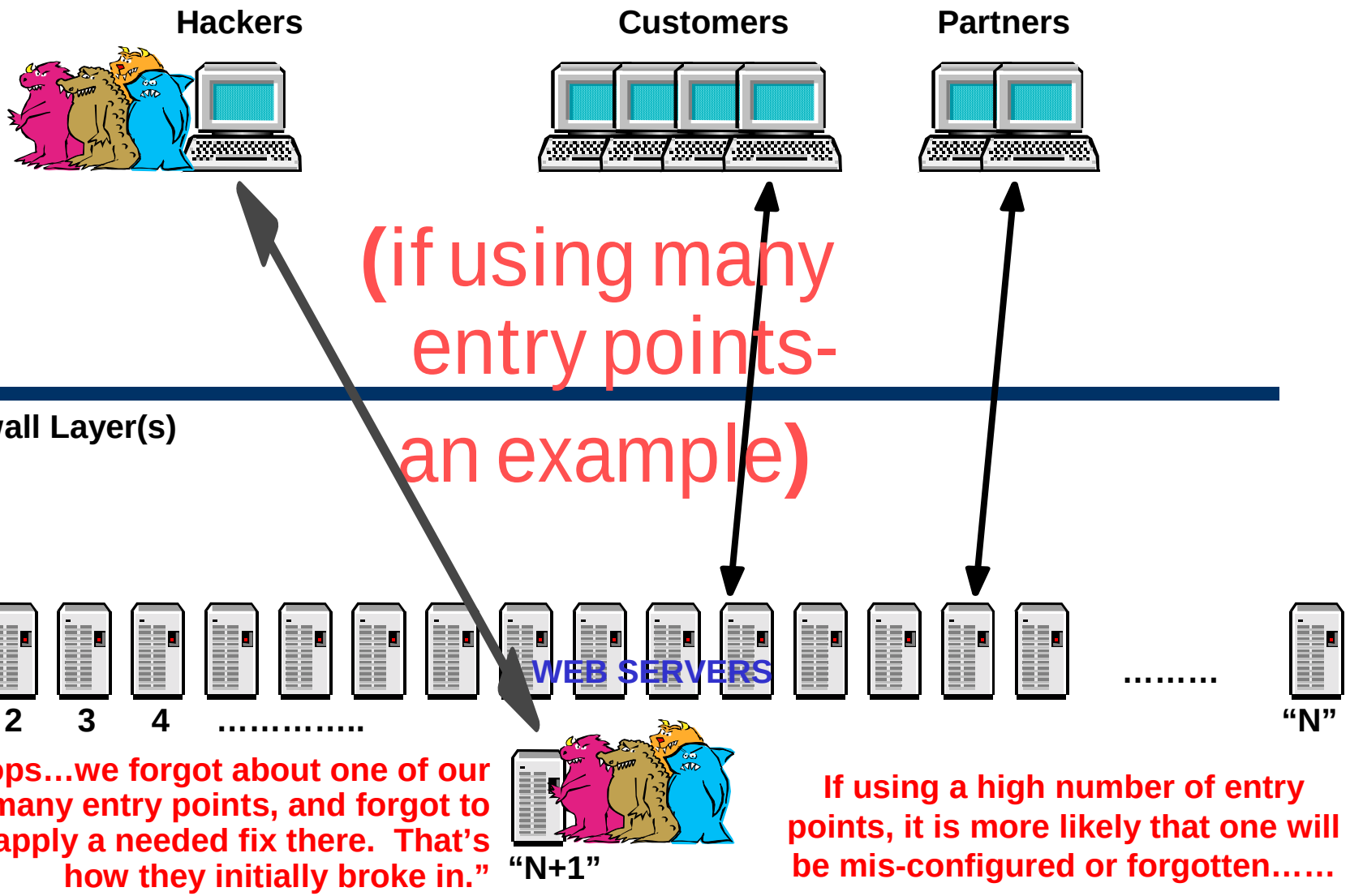


How many entry points to your secured network: many or few? (scenario with "few")

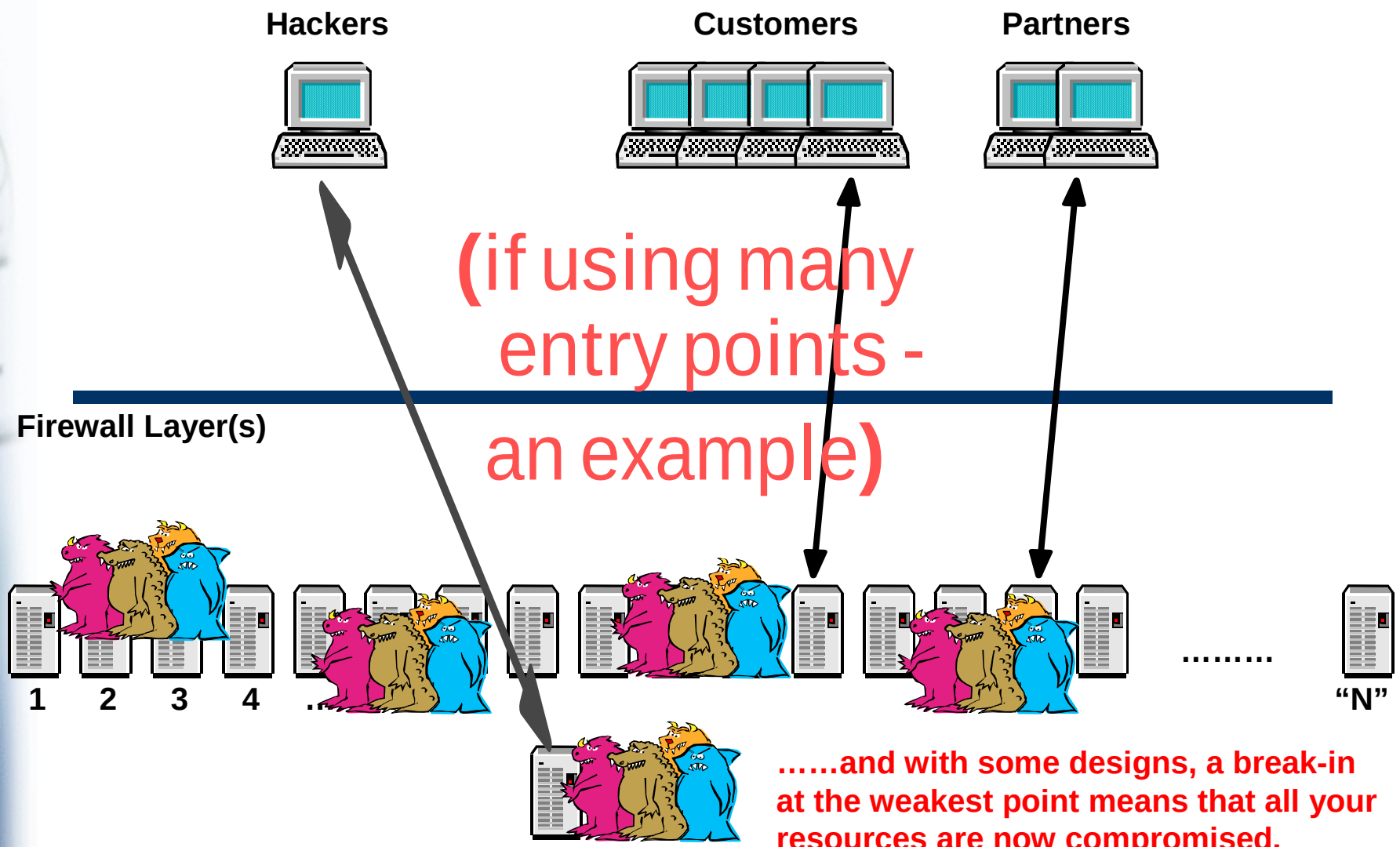


……While other security designs let you open only a few entry points into your secured network, regardless of the number of web servers you are protecting.

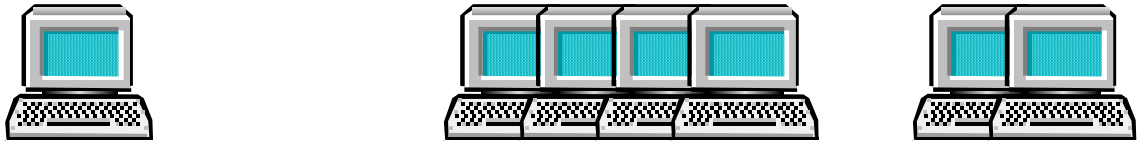
How many entry points to your secured network: many or few? (potential exposure with "many")



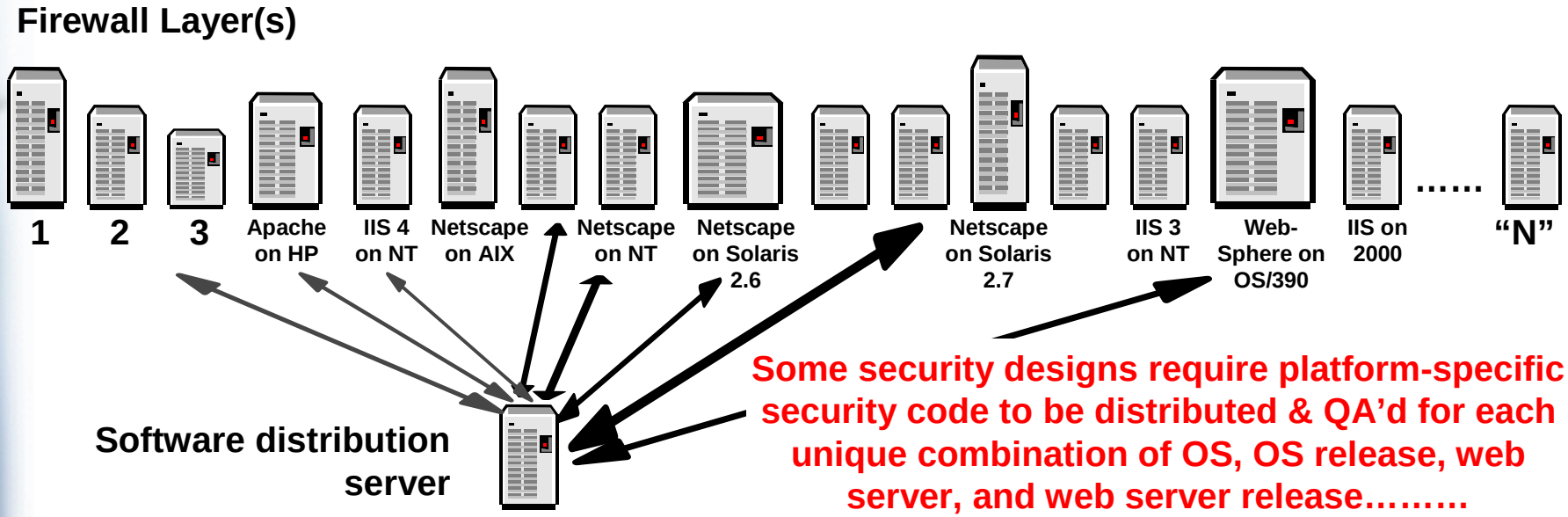
How many entry points to your secured network: many or few? (potential exposure with "many")



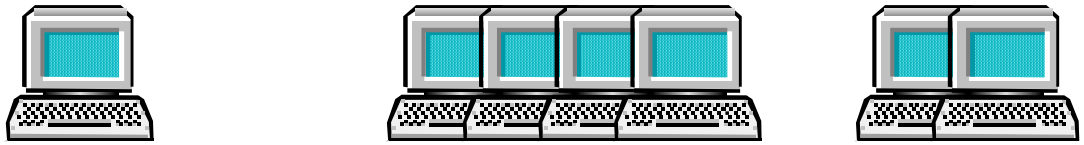
Number of software distribution points: many or few? (scenario 1)



(if security code is distributed to many points)



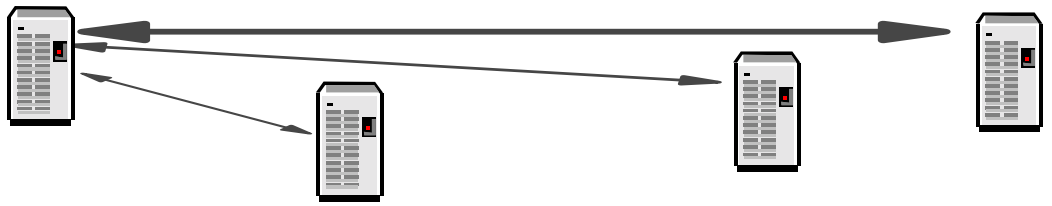
Number of software distribution points: many or few? (scenario 2)



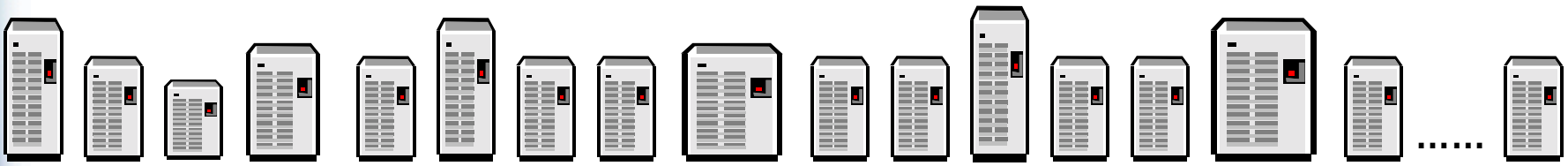
Firewall Layer(s)

(if security code is distributed to few points)

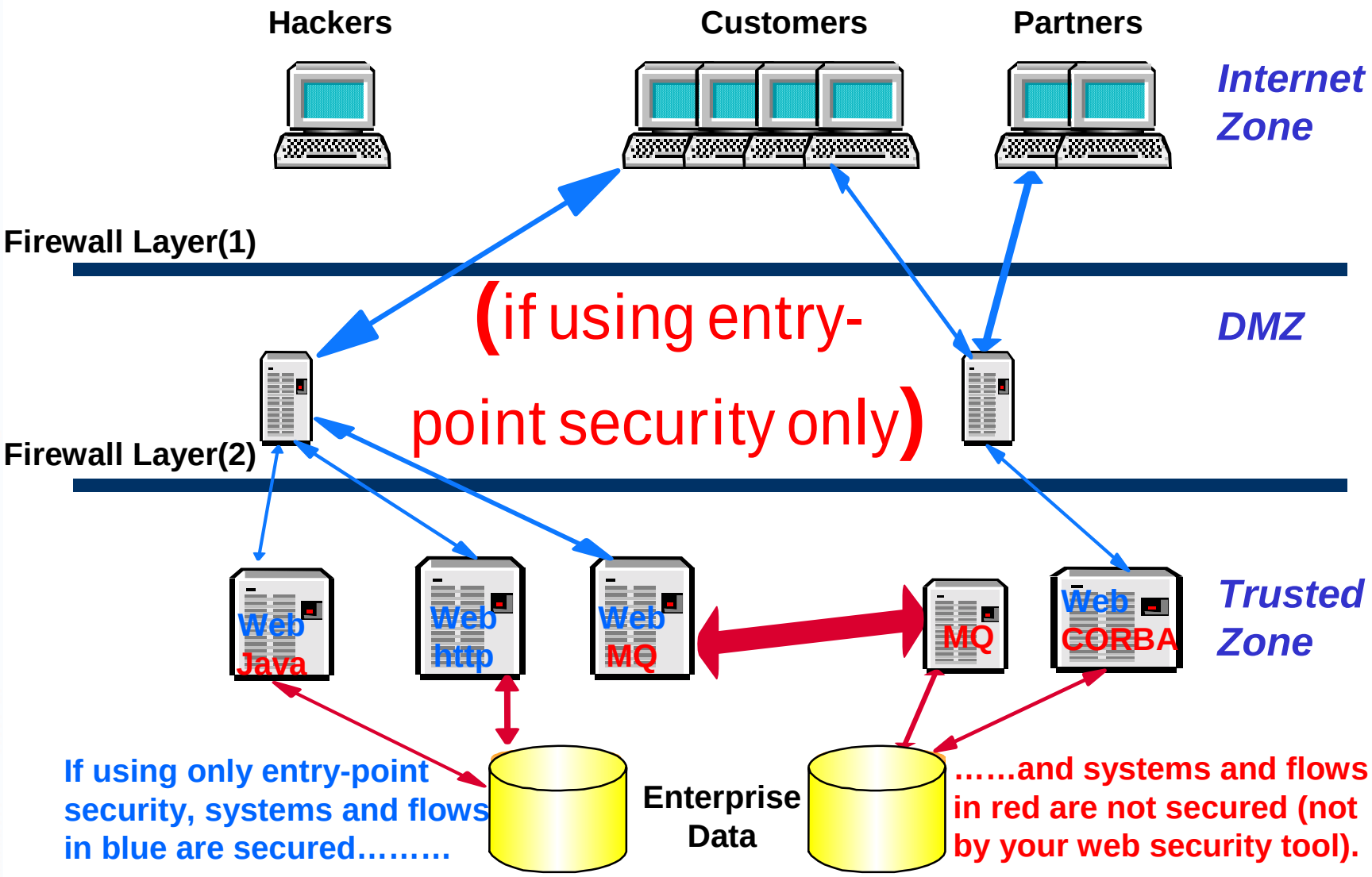
SW dist. server



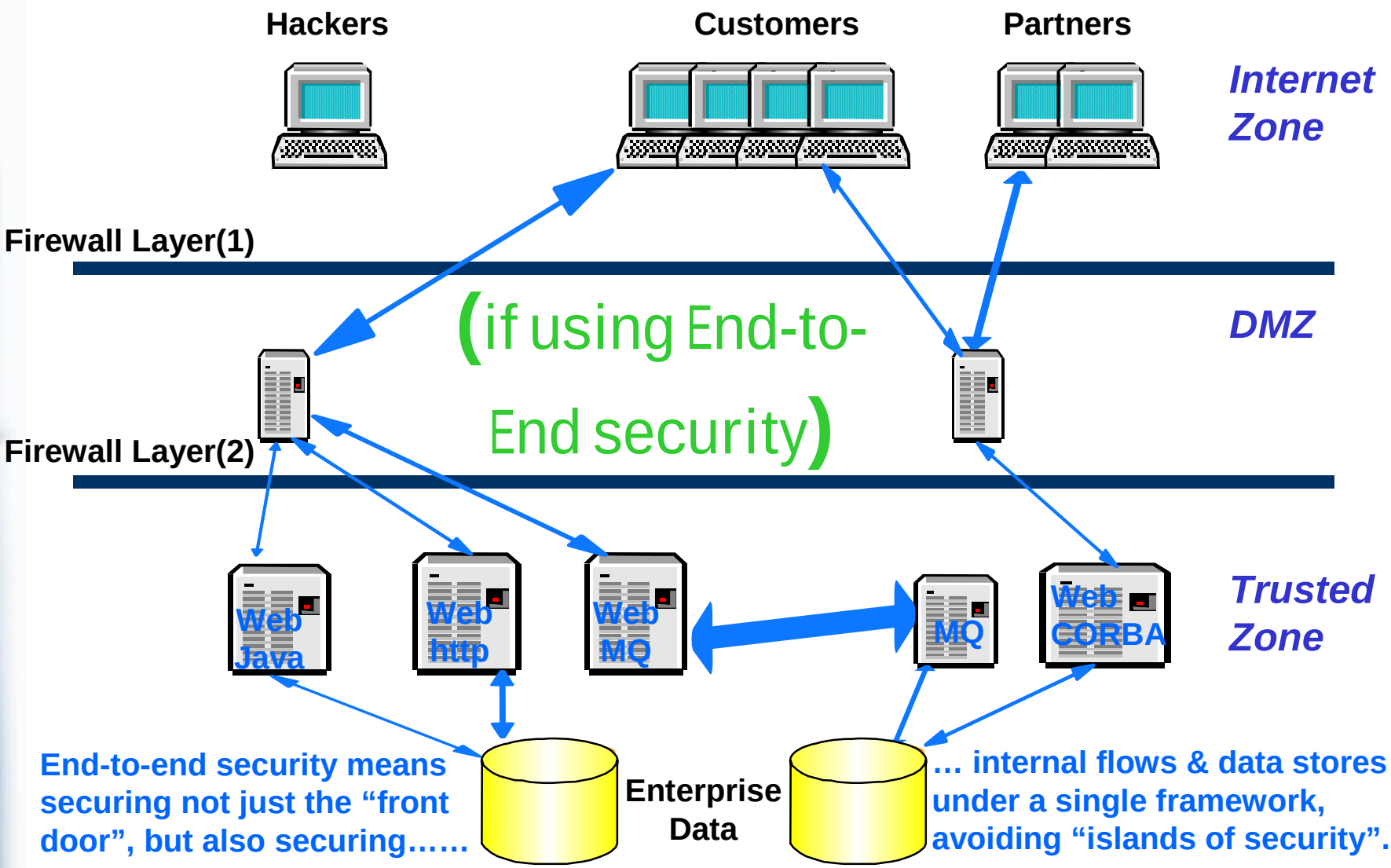
……while other security designs require security code be deployed only to a smaller number of boxes – even if you are securing many servers (as shown below)



Do you want Entry-point security only, or End-to-End security?



Do you want Entry-point security only, or End-to-End security?



References: Redbooks

- Global Server Certificate Usage with OS/390 Webservers
  - SG24-5623-00
- Ready for e-Business: OS/390 Security Server Enhancements
  - SG24-5158-00
- Enterprise Web Serving with the Lotus Domino Go Webserver for OS/390
  - SG24-2074-01
- OS/390 Securiry Server 1999 Updates Technical Presentation Guide
  - SG24-5627
- OS/390 Security Server 1999 Updates Installation Guide
  - SG24-5629
- ITSO Website:
  - http://www.redbooks.ibm.com/