Emerging PKI technologies on OS/390

Paul de Graaff ITSO Poughkeepsie S/390 Security
e-mail: graaff@us.ibm.com

Agenda

□ Components of PKI

□ Authentication on OS/390 using PKI

□ PKI Enabled applications on OS/390

□ Directions

Agenda

☛ Components of PKI

□ Authentication on OS/390 using PKI

□ PKI Enabled applications on OS/390

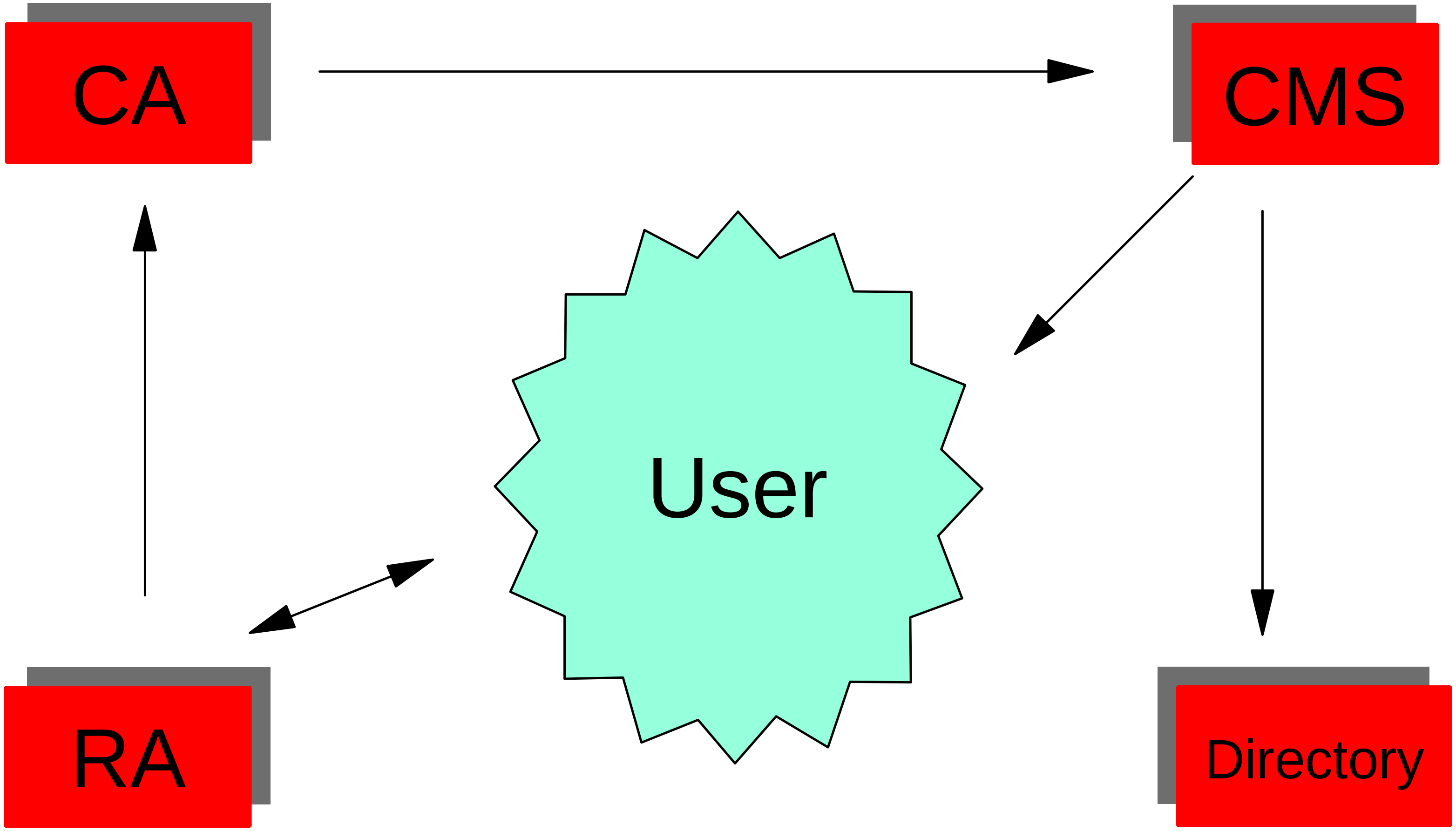
□ Directions

PKI Terminology

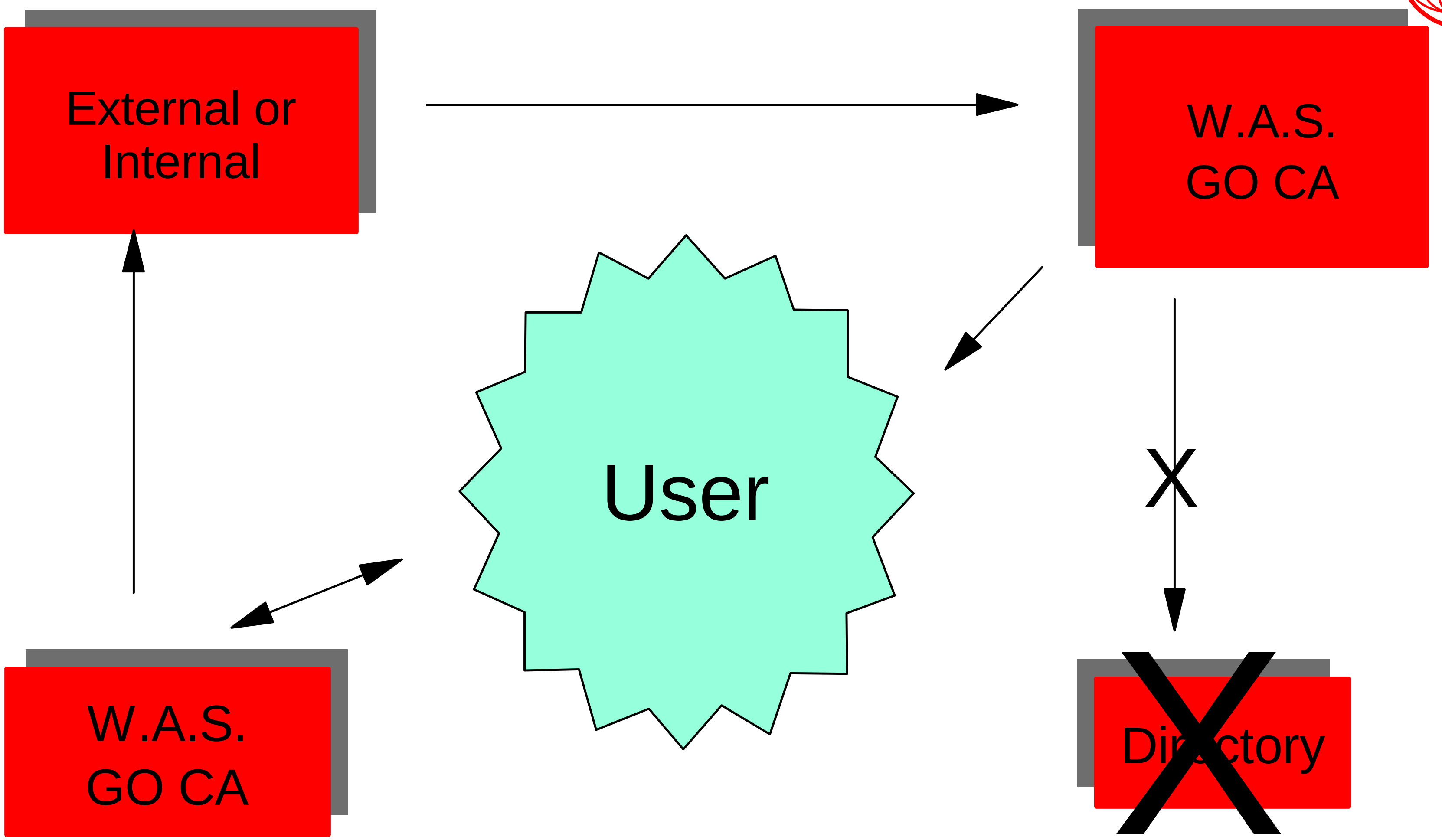
- **Digital Certificate**
  - Document issued by a trusted party to a person or entity
  - Evidence attesting to person's or entity's rights (or privileges)
- **Certificate Authority (CA)**
  - Entity that defines & administers processes for issuance, renewal and revocation
  - Authorizes signing of certificates and registration authorities (RA) to approve requests to sign and issue certificates
- **Registration Authority (RA)**
  - Organization or person that authorizes certificate issuance, renewal & revocation

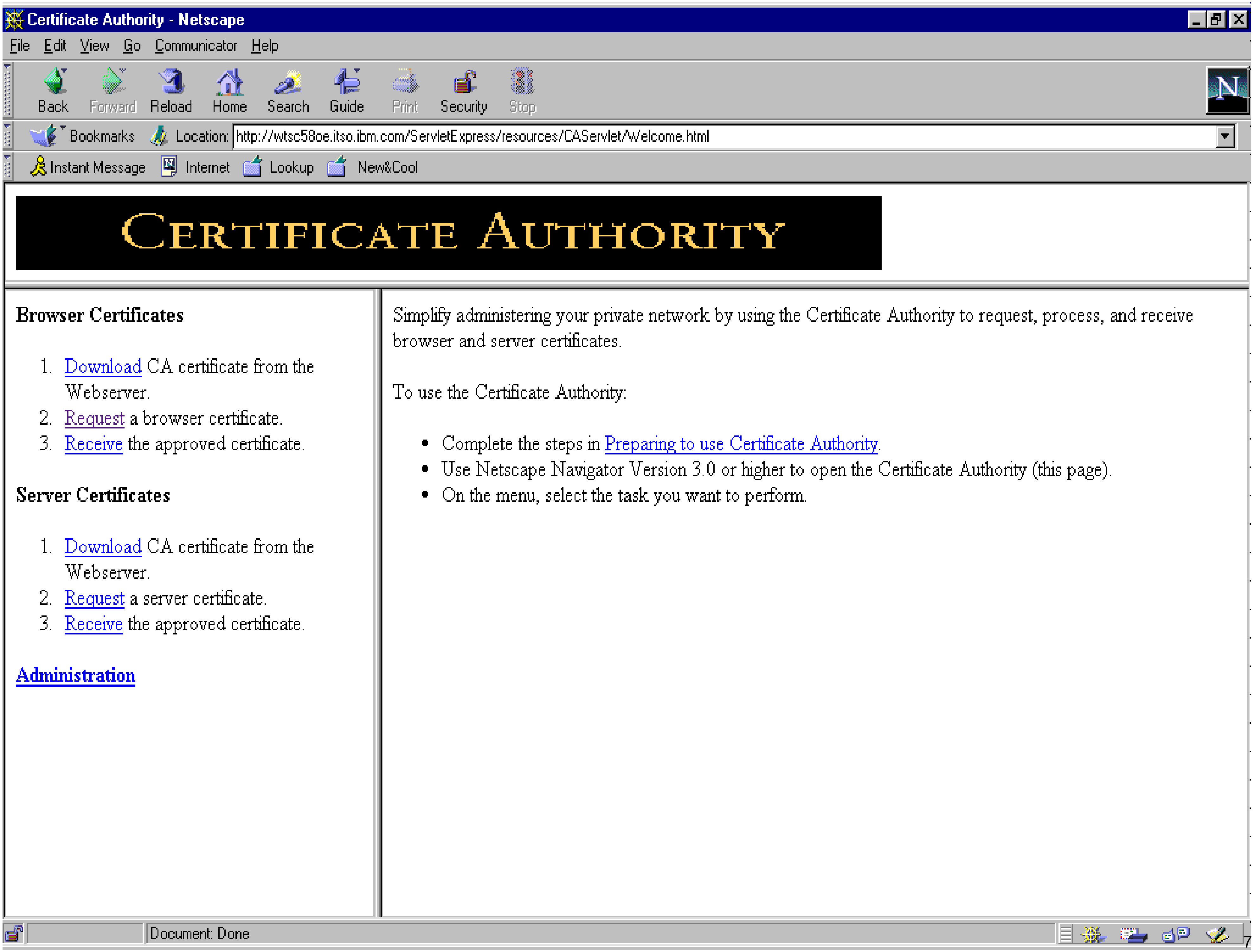
- **Certificate Management System (CMS)**
  - System that signs certificates & revocation lists
- **Repository/Directory**
  - An on-line database containing: public key certificates and Certificate Revocation Lists (CRLs)
- **Public Key Infrastructure (PKI)**
  - System of CA's, RA's and repositories which manage certificate issuance, renewal, revocation, registration, key management and associated security services
  - Structures for authentication, privacy, information integrity, and non-repudiation

Components of PKI



Components of OS/390 PKI




Certificate Authority - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://wtsc58oe.itso.ibm.com/ServletExpress/resources/CAServlet/Welcome.html
Instant Message Internet Lookup New&Cool
Document: Done

CERTIFICATE AUTHORITY

Browser Certificates

1. Download CA certificate from the Webserver.
2. Request a browser certificate.
3. Receive the approved certificate.

Server Certificates

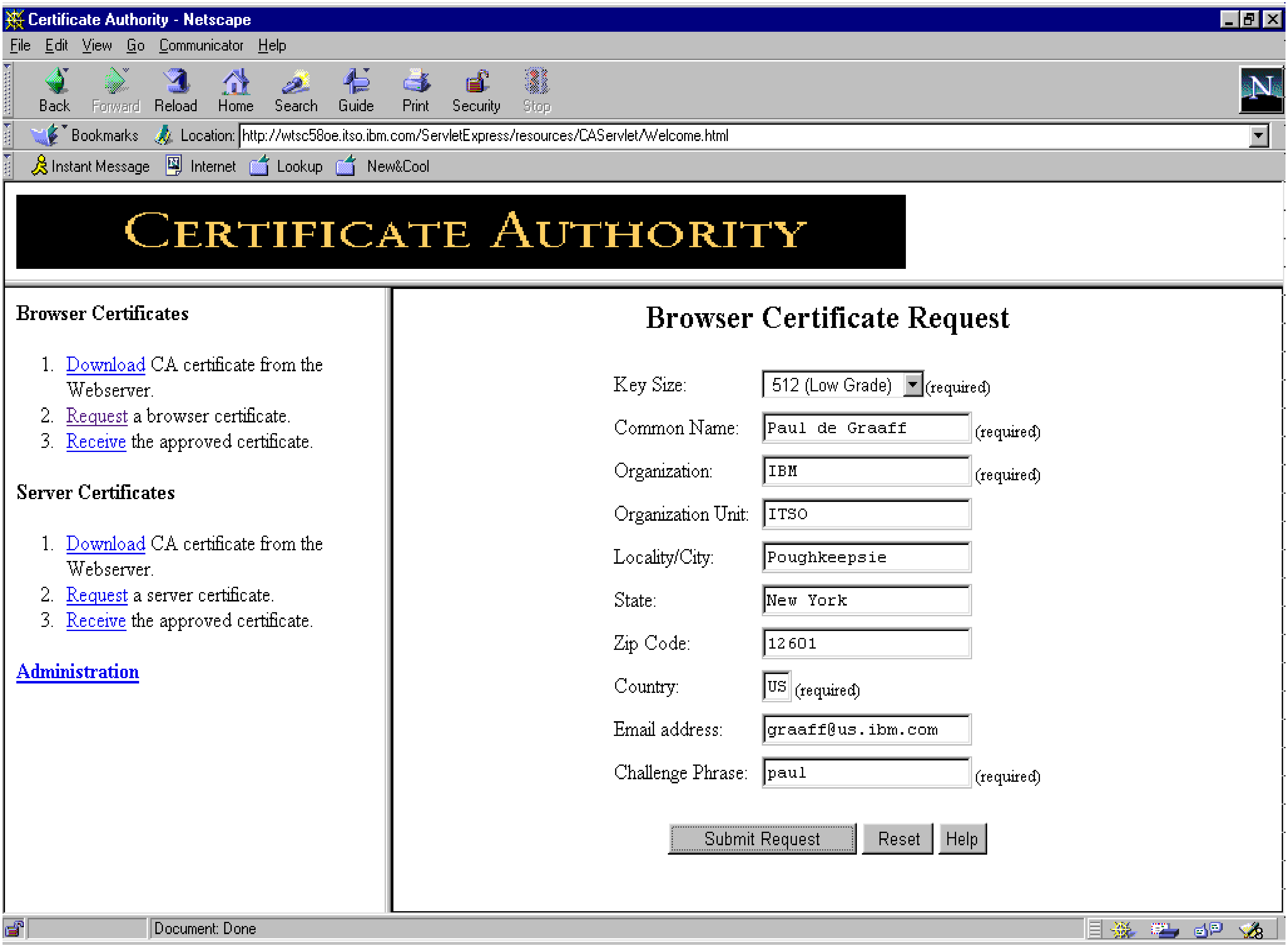
1. Download CA certificate from the Webserver.
2. Request a server certificate.
3. Receive the approved certificate.

Administration

Simplify administering your private network by using the Certificate Authority to request, process, and receive browser and server certificates.

To use the Certificate Authority:

- Complete the steps in Preparing to use Certificate Authority.
- Use Netscape Navigator Version 3.0 or higher to open the Certificate Authority (this page).
- On the menu, select the task you want to perform.


Certificate Authority - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://wtsc58oe.itso.ibm.com/ServletExpress/resources/CAServlet/Welcome.html
Instant Message Internet Lookup New&Cool
CERTIFICATE AUTHORITY
Document: Done

Browser Certificates

1. Download CA certificate from the Webserver.
2. Request a browser certificate.
3. Receive the approved certificate.

Server Certificates

1. Download CA certificate from the Webserver.
2. Request a server certificate.
3. Receive the approved certificate.

Administration

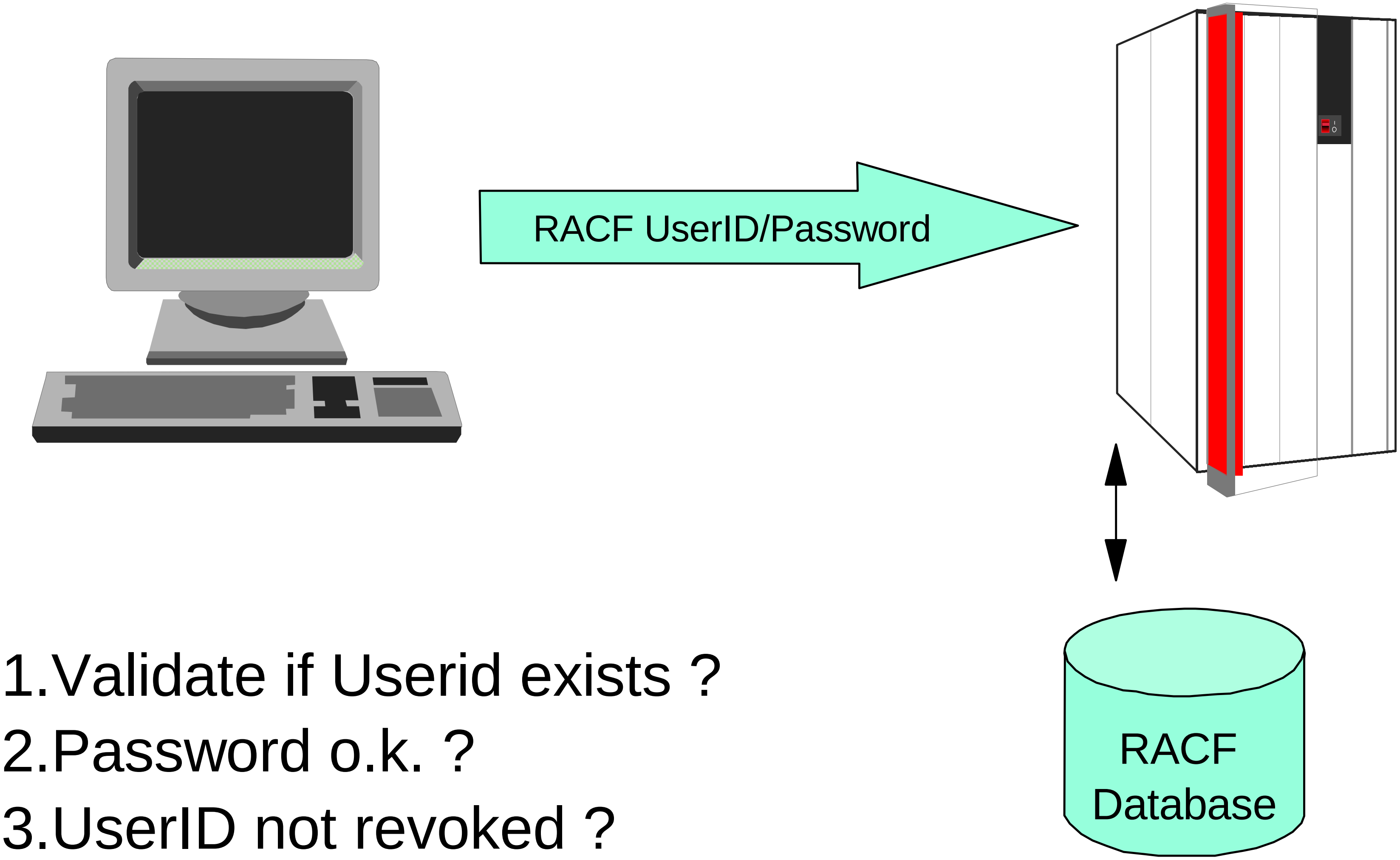
Browser Certificate Request

Key Size:	512 (Low Grade)	(required)
Common Name:	Paul de Graaff	(required)
Organization:	IBM	(required)
Organization Unit:	ITSO	
Locality/City:	Poughkeepsie	
State:	New York	
Zip Code:	12601	
Country:	US	(required)
Email address:	graaff@us.ibm.com	
Challenge Phrase:	paul	(required)

Agenda

- Introduction in to Public Key Infrastructure (PKI)
- Components of PKI
- ☛ Authentication on OS/390 using PKI
- PKI Enabled applications on OS/390
- Concerns
- Directions

Traditional Authentication on OS/390

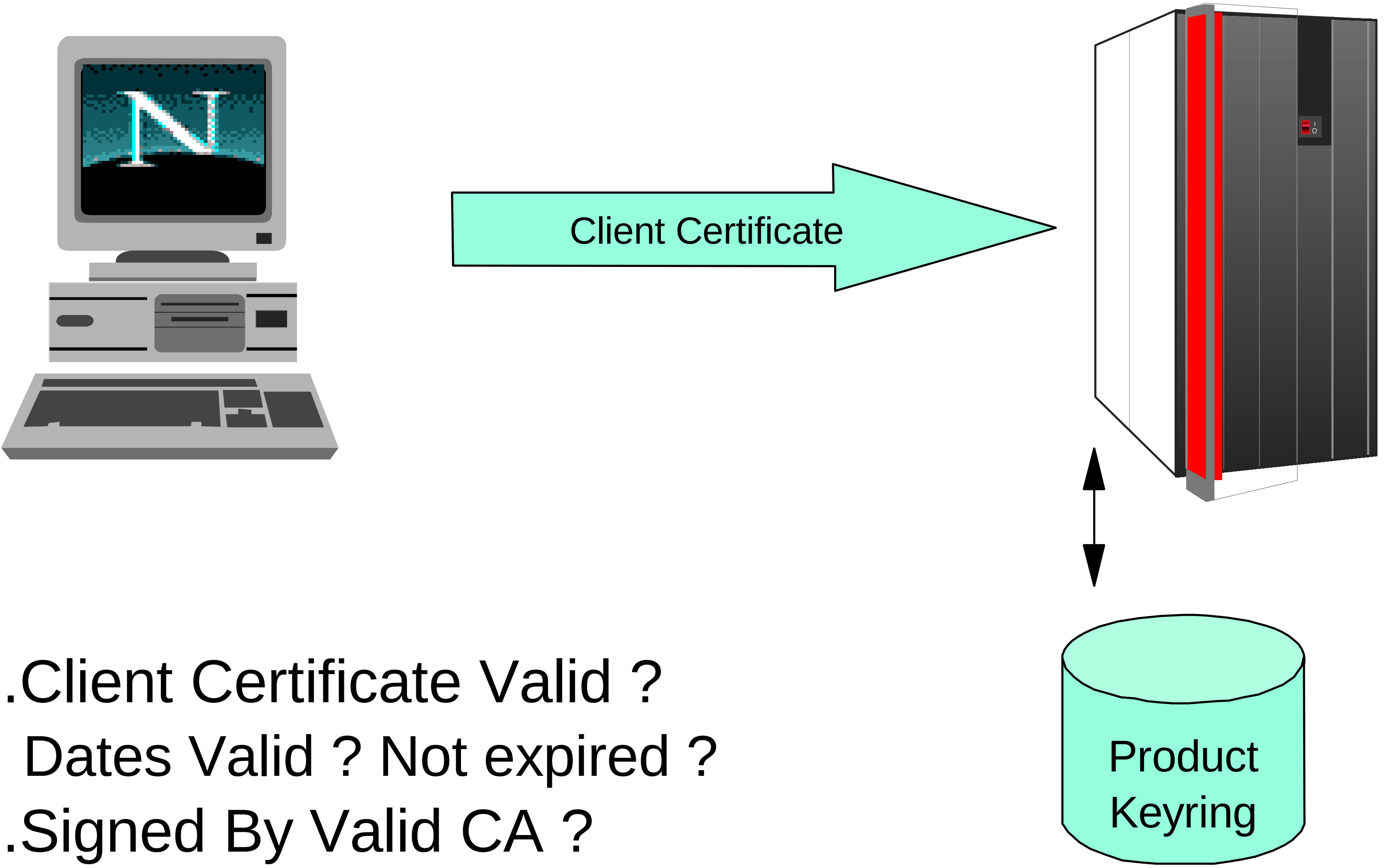


1.Validate if Userid exists ?

2.Password o.k. ?

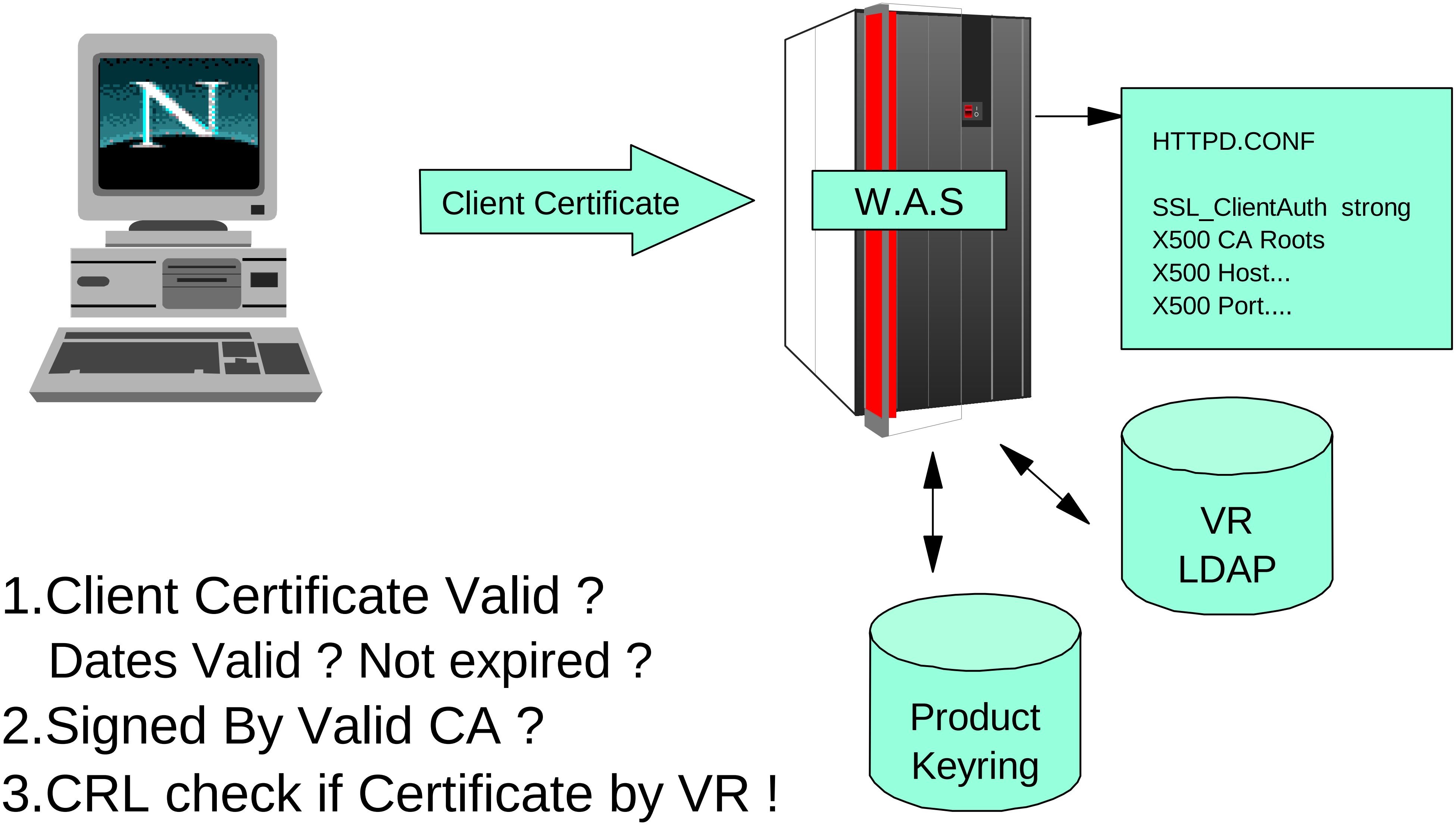
3.UserID not revoked ?

PKI Authentication



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

PKI Strong Authentication using Websphere

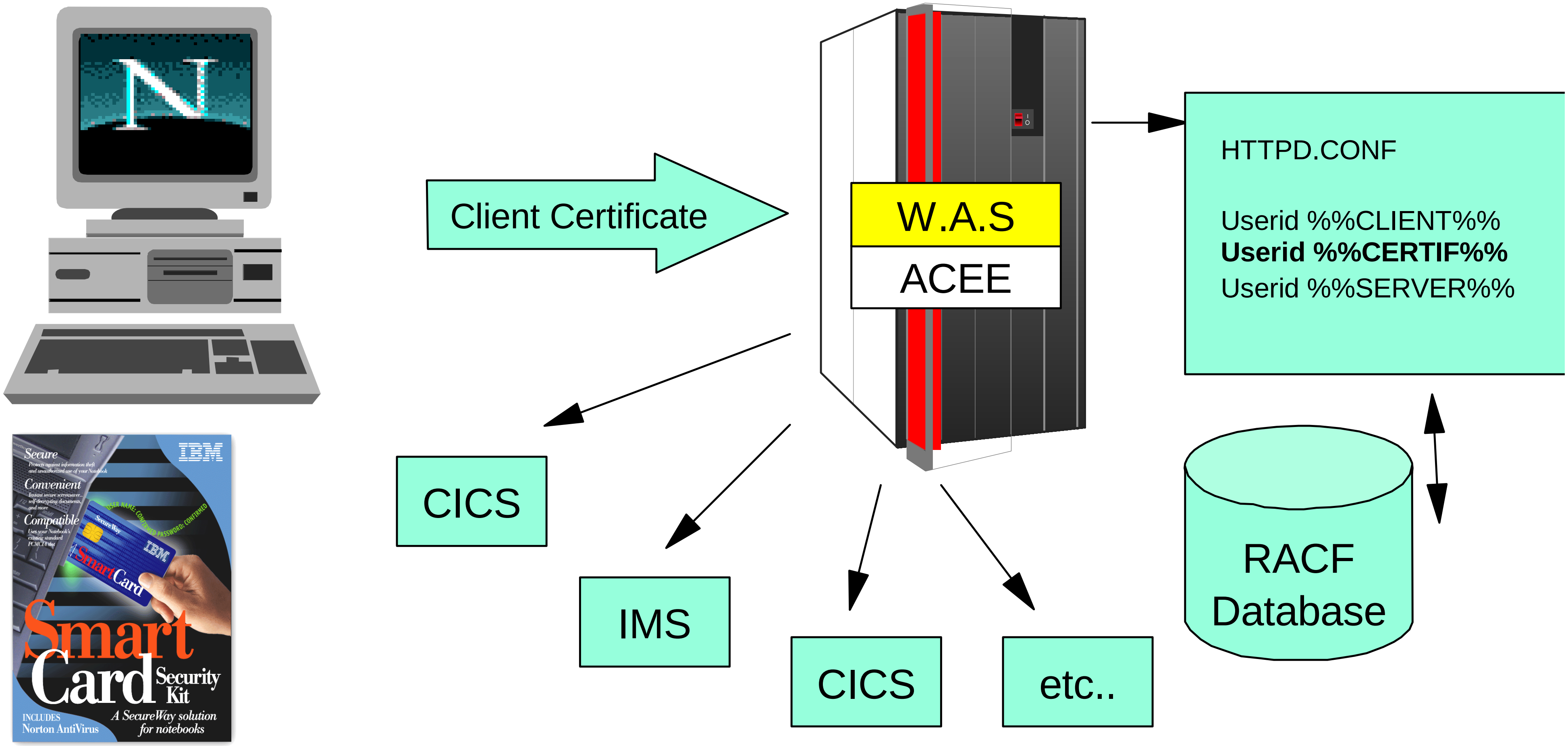


```
HTTPD.CONF

SSL_ClientAuth  strong
X500 CA Roots
X500 Host...
X500 Port....
```

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

PKI Authentication beyond Websphere



Client Certificate

W.A.S

ACEE

HTTPD.CONF

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

CICS

IMS

CICS

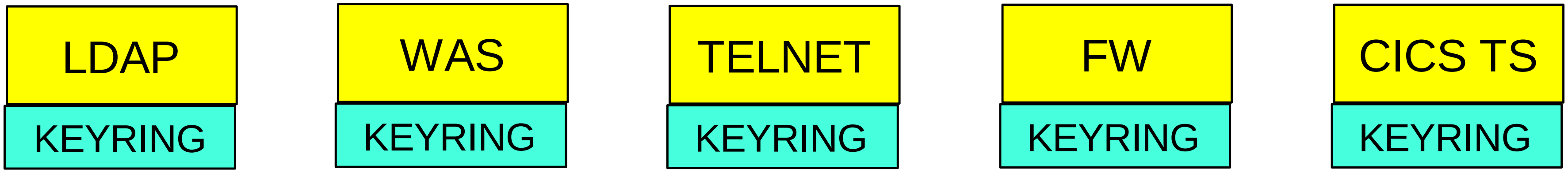
etc..

RACF Database

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

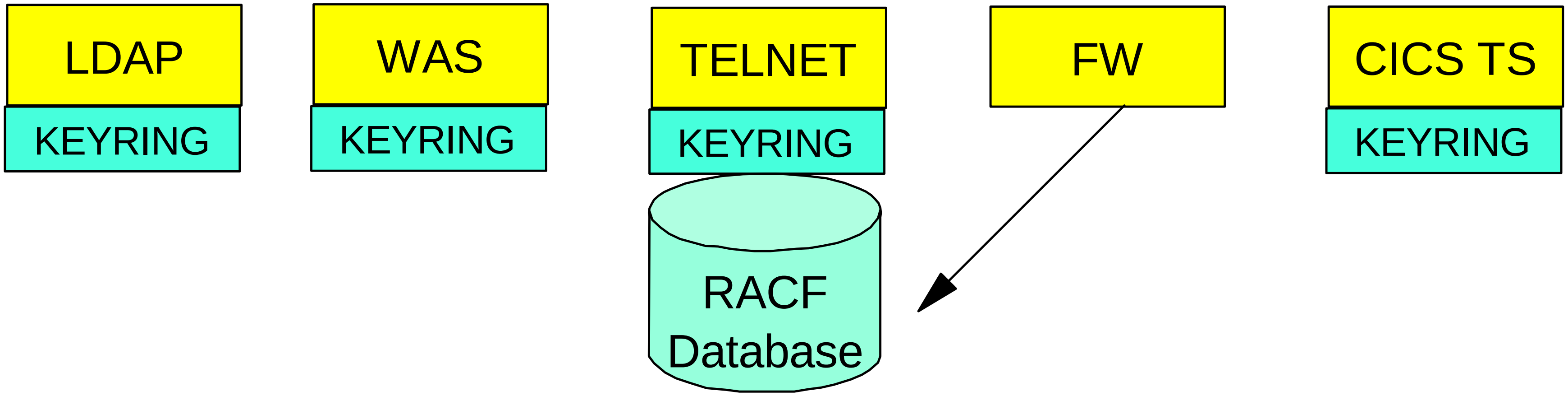
RACF Keyring support V2R8

Currently every product his own keyring !



Managed by MKKF, IKEYMAN or GSKKYMAN !

Release 8 will add keyring support to RACF



RACF Keyring Support V2R8

- RACDCERT GENCERT
  - create public/private key pair and digital certificates
- RACDCERT GENREQ
  - create a certificate request for off-platform certificate authority signing
- RACDCERT EXPORT
  - extract certificate from RACF database and place in a data set
- RACDCERT ADDRING or CONNECT
  - create keyring and add certificates

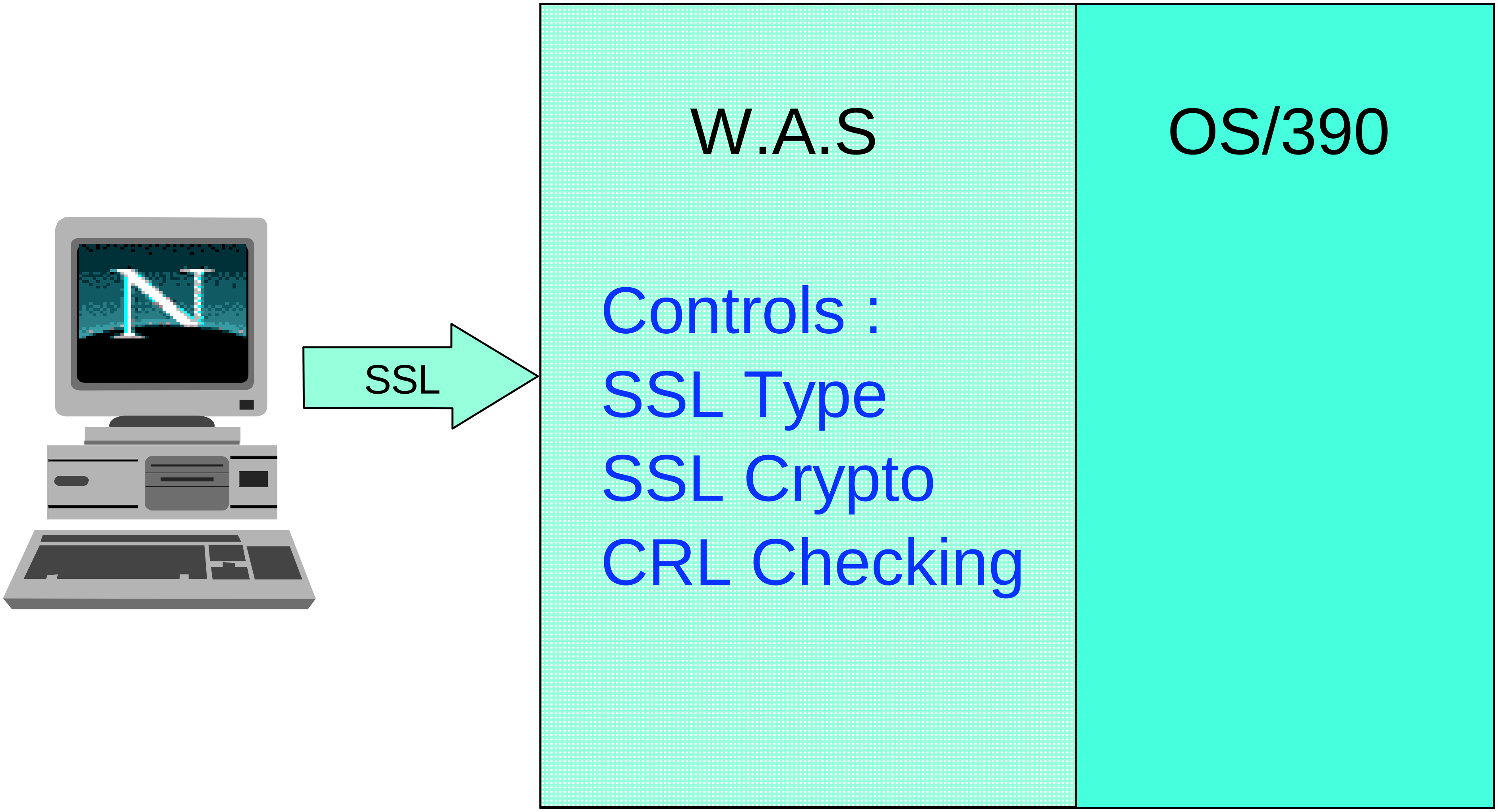
Agenda

- Components of PKI
- Authentication on OS/390 using PKI
- ☞ PKI Enabled applications on OS/390
- Directions

OS/390 PKI Exploiters

- Websphere (SSL)
- LDAP Server (SSL)
- Secure Telnet (SSL)
- OS/390 FW GUI (SSL)
- OS/390 VPN IKE Support
- CICS TS Web Interface (SSL)

Websphere on OS/390



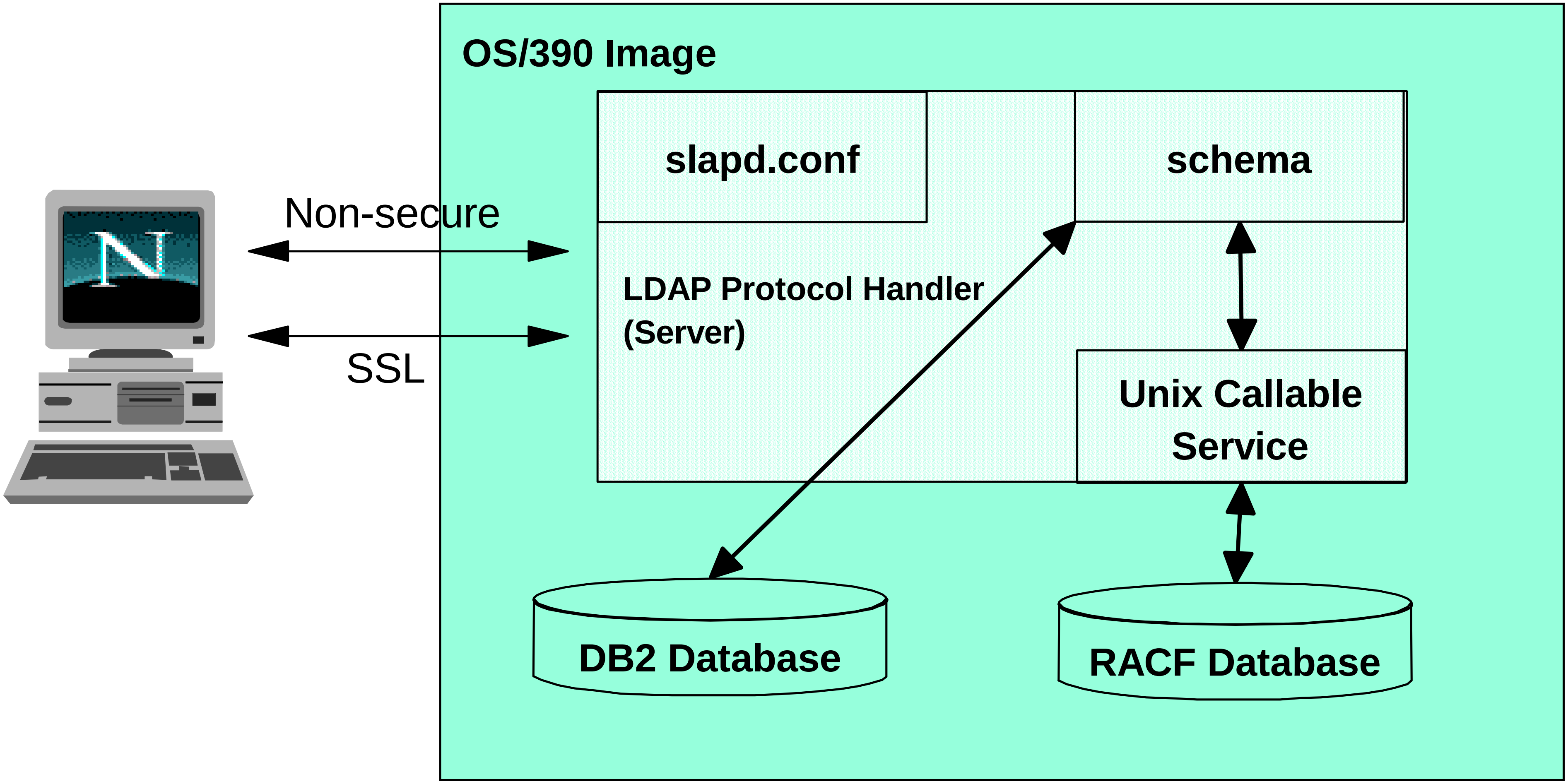
Controls :

SSL Type

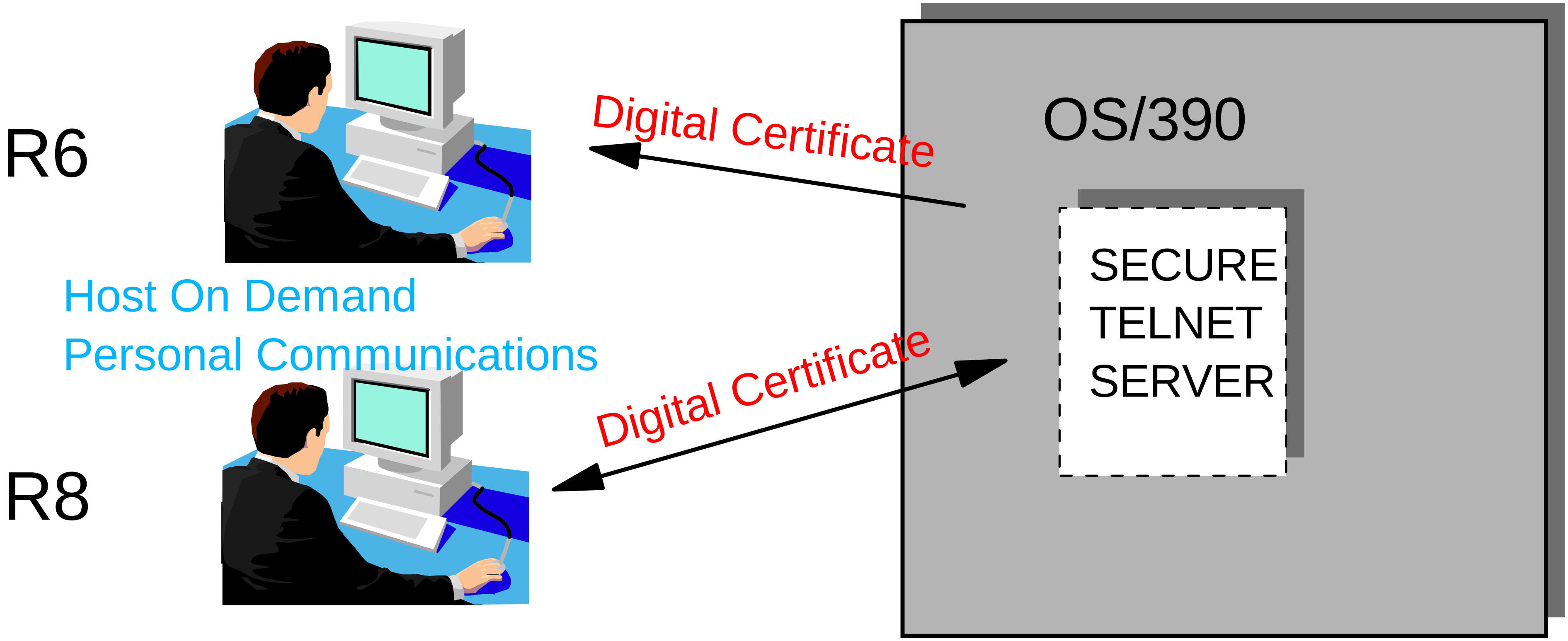
SSL Crypto

CRL Checking

LDAP Server on an OS/390 Image



Secure TELNET



R6

Host On Demand

Personal Communications

R8

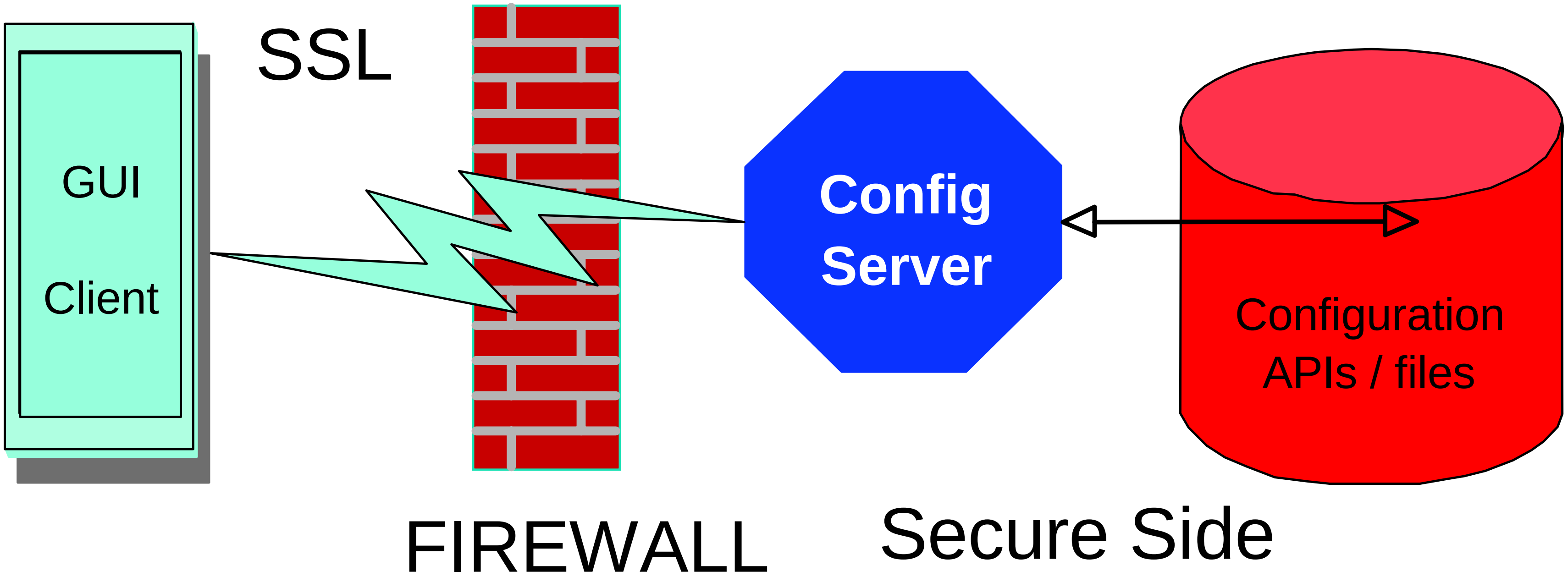
Digital Certificate

Digital Certificate

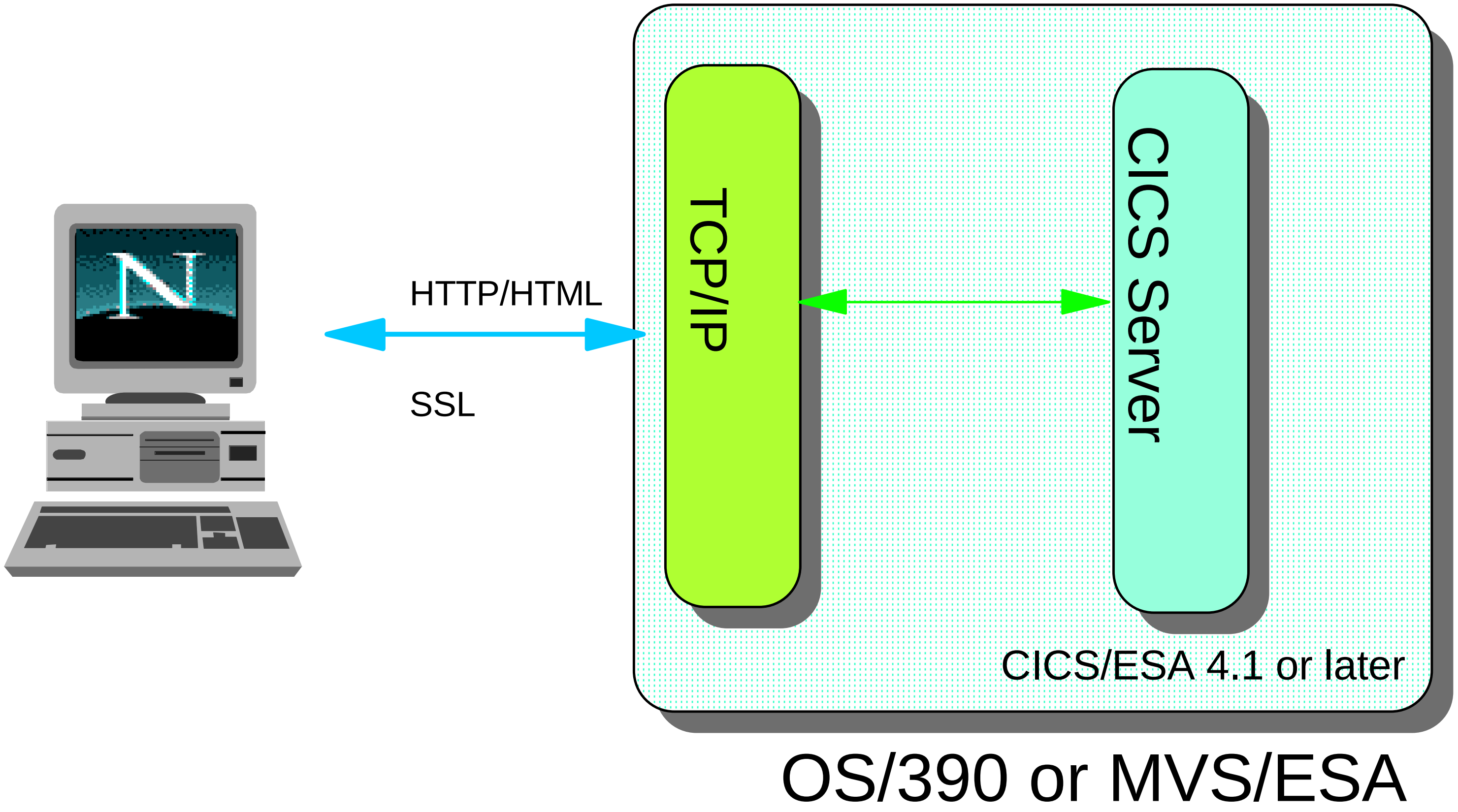
OS/390

SECURE
TELNET
SERVER

FW Management through GUI



CICS Web Interface



HTTP/HTML

SSL

TCP/IP

CICS Server

CICS/ESA 4.1 or later

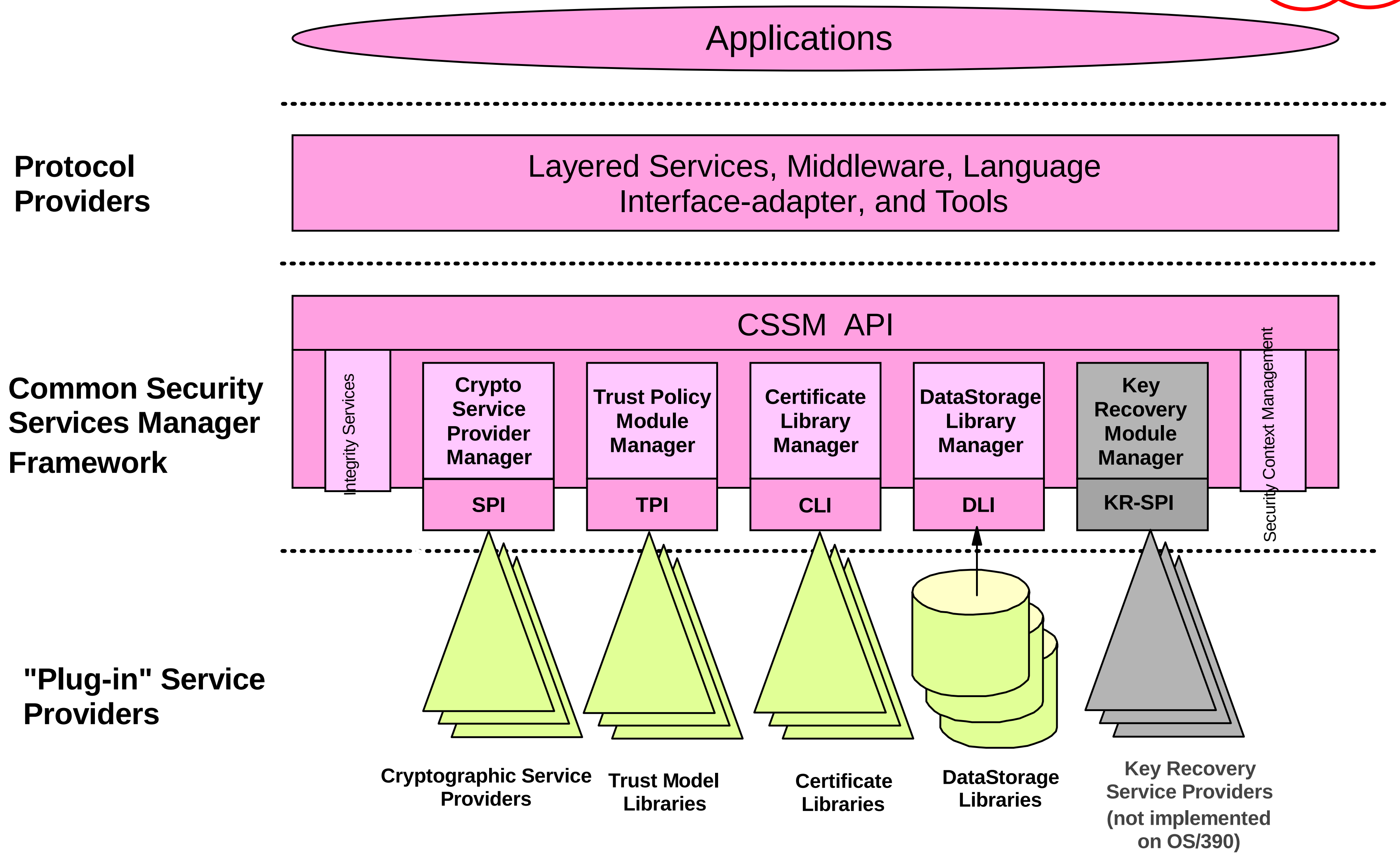
OS/390 or MVS/ESA

Note : SSL support as of CICS TS 1.2

Agenda

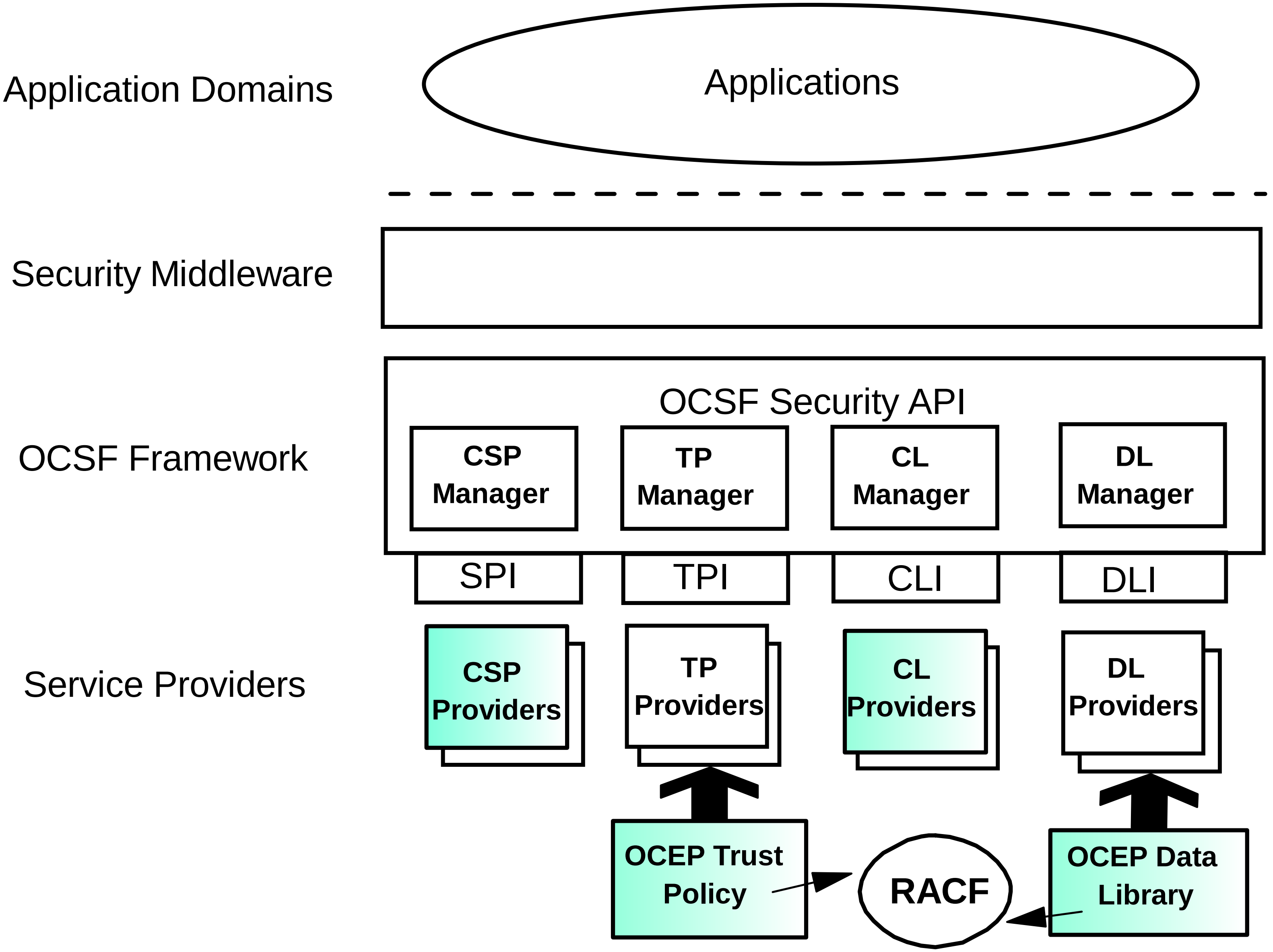
- □ Components of PKI
- □ Authentication on OS/390 using PKI
- □ PKI Enabled applications on OS/390
- ☛ Directions

CDSA Overview

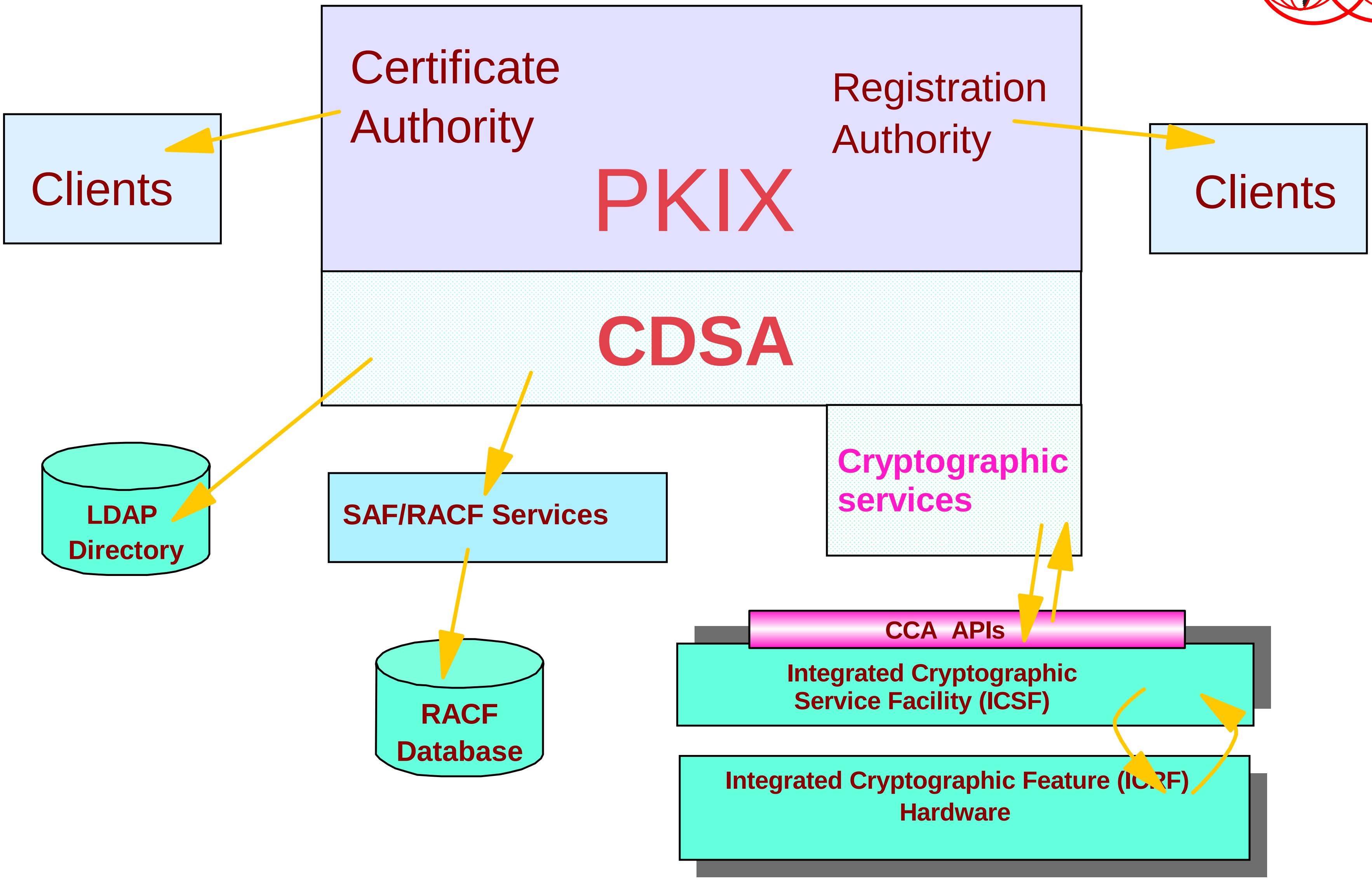

Applications
Protocol Providers
Layered Services, Middleware, Language Interface-adapter, and Tools
Common Security Services Manager Framework
CSSM API
Integrity Services
Crypto Service Provider Manager
SPI
Trust Policy Module Manager
TPI
Certificate Library Manager
CLI
DataStorage Library Manager
DLI
Key Recovery Module Manager
KR-SPI
Security Context Management
"Plug-in" Service Providers
Cryptographic Service Providers
Trust Model Libraries
Certificate Libraries
DataStorage Libraries
Key Recovery Service Providers
(not implemented on OS/390)

IBM Technical Support

Current CDSA Support on OS/390



OS/390 Security Trust Infrastructure

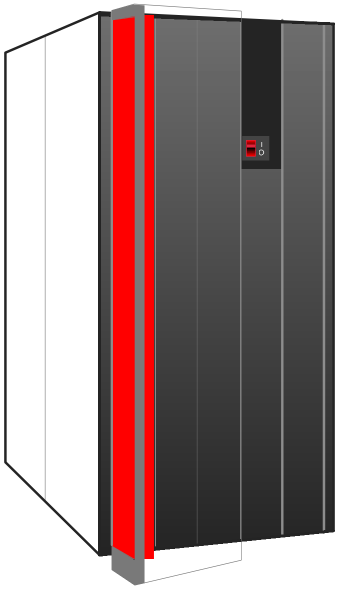


Agenda

- ☑ Components of PKI
- ☑ Authentication on OS/390 using PKI
- ☑ PKI Enabled applications on OS/390
- ☑ Directions

My Message to you !

Security does not have to be e-complicated !



Big Iron is there to make it easy !