



Common Belgium

News tips and techniques with V5R3 and Power5

IBM

Bart De Sitter

*Advisory IT Specialist
IBM Certified*

*IBM Belgium s.a.
Avenue du Bourget, 42
B-1130 Bruxelles
Tel. +32 2 225 33 63
Fax +32 2 225 23 68
E-mail: bart_desitter@be.ibm.com*

IBM

Fabian Michel

*Senior IT Specialist
IBM Certified*

*IBM Belgium s.a.
Avenue du Bourget, 42
B-1130 Bruxelles
Tel. +32 2 225 38 22
Fax +32 2 225 23 68
E-mail: fabian_michel@be.ibm.com*

Agenda

■ Part 1: Security

Single sign-on

SSL: Secure Socket Layer

OpenSSH

Firewall and other security enhancements

Time synchronization



■ Part 2 : Infrastructure management update

Virtualization

LPAR management facilities

TSM: Tivoli Storage Manager





Common Belgium

Single Sign-on



September 20, 2005

© 2005 IBM Corporation

Single Sign-on

Why ?

Benefit for end users and administrators

- No more “cached” passwords
- Less password resets
- User registry



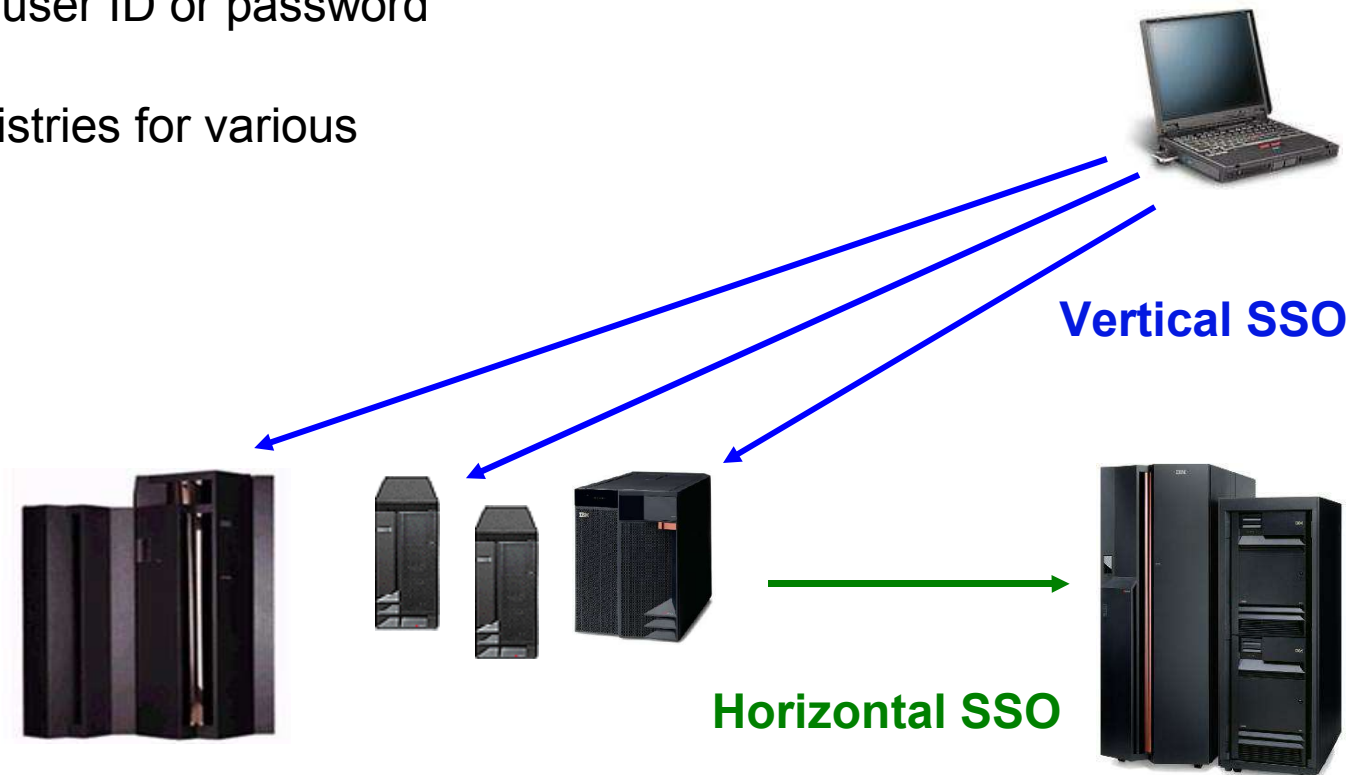
A dream or reality ?

Notes: Single Sign-on

- Simplifies the process for the user; access is controlled under the covers
- Simplifies administration
 - Rely on existing security semantics already in place for existing data
 - Reduces load** on administrators for "lost" passwords **and** therefore **cost**
 - Reduces client side risks (cached passwords, post-it notes, etc..)
- Makes it easy for customers to associate a user's multiple identities in the enterprise and to manage those associations

Vertical or Horizontal?

- Sign on once to the network using a user ID and password
- Connection requests to application services are authenticated without prompting for the user ID or password
- Different user registries for various applications

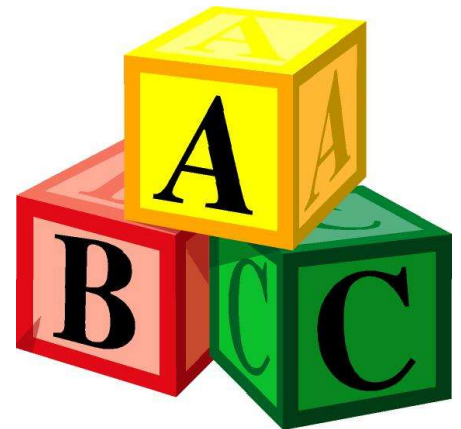


Building blocks

How ?

Several components to build a SSO enabled environment

- Authentication source (e.g. Kerberos or LDAP)
- EIM: Enterprise Identity Mapping
- LTPA keys
- Credential vault
- TAM: Tivoli Access Manager



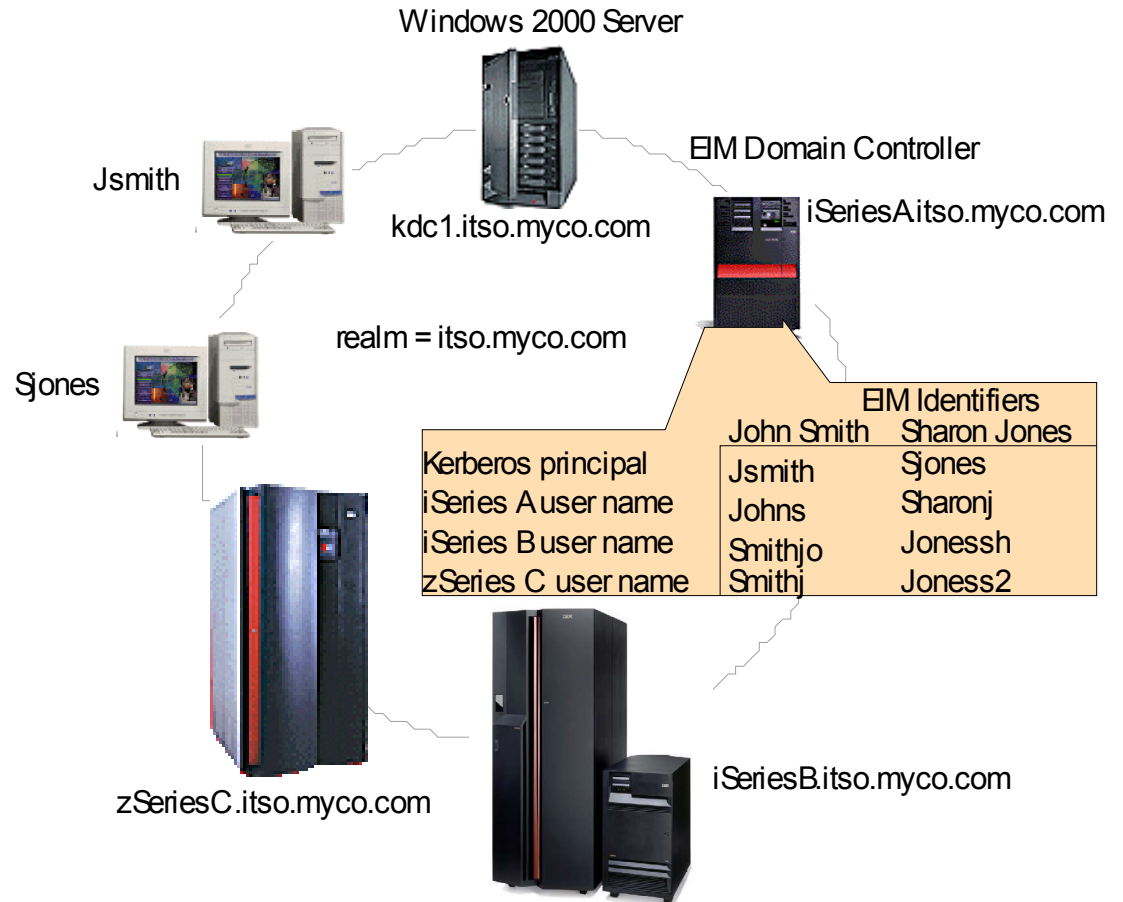
Notes: Building blocks

- The term single signon is often misinterpreted or confused with having a single user ID and password to sign on to a system. However, in most cases, users still have to sign on to each application or service individually. With a true SSO solution, a user signs on only once to the network (a central authentication service) and then accesses all participating services without re-entering a user ID or password. Many available SSO solutions, however, only offer a SSO in a Web environment. It is desirable to have a SSO solution that works for both browser-accessible applications and local applications, such as Telnet or DB access.
- With SSO, we distinguish between horizontal and vertical SSO approaches:
 - Vertical SSO** describes an approach where a client signs on from the client to each individual server using SSO.
 - Horizontal SSO** involves a client signing on, for example, to a server application, which in turn connects to another server to access a database, signing on on behalf of the user (also with SSO).

EIM

- EIM is a mechanism to map (associate) a person or entity to the appropriate user identities in various registries throughout the enterprise

EIM defined: Identity associations across user registries associated with operating system platforms, applications, and middleware.



Kerberos and EIM enabled applications

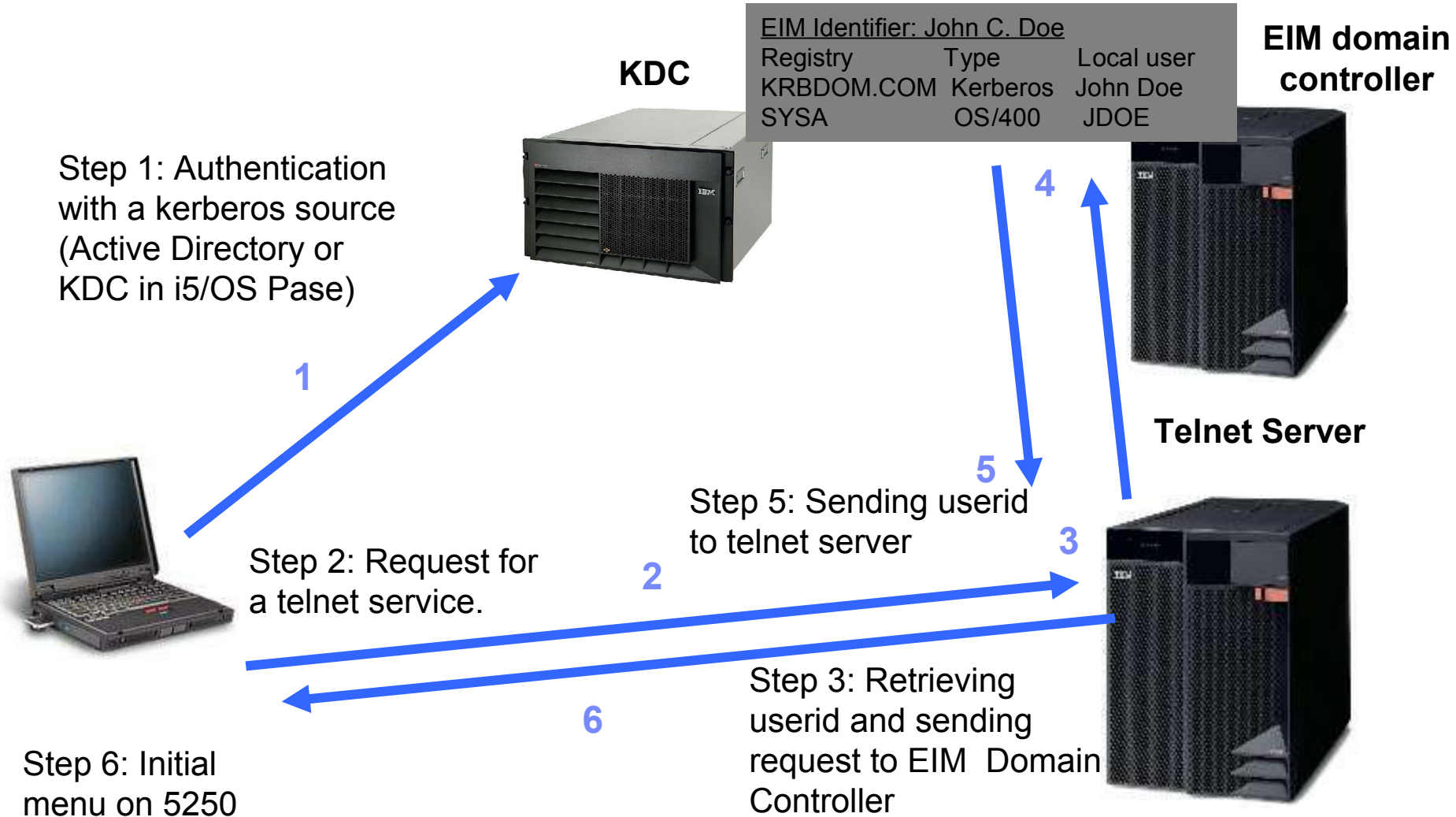
- Host servers (used by iSeries Access for Windows or PComm)
 - Telnet
 - QFileSrv.400
 - Database Connectivity (DRDA, ODBC, JDBC)
- NetServer
- HTTP Server for iSeries (powered by Apache)
- LDAP
- Windows Integration
- Management Central
- FTP (via Exit program on QIBM_QTMF_SVR_LOGON)

Notes: Kerberos and i5/OS enabled applications

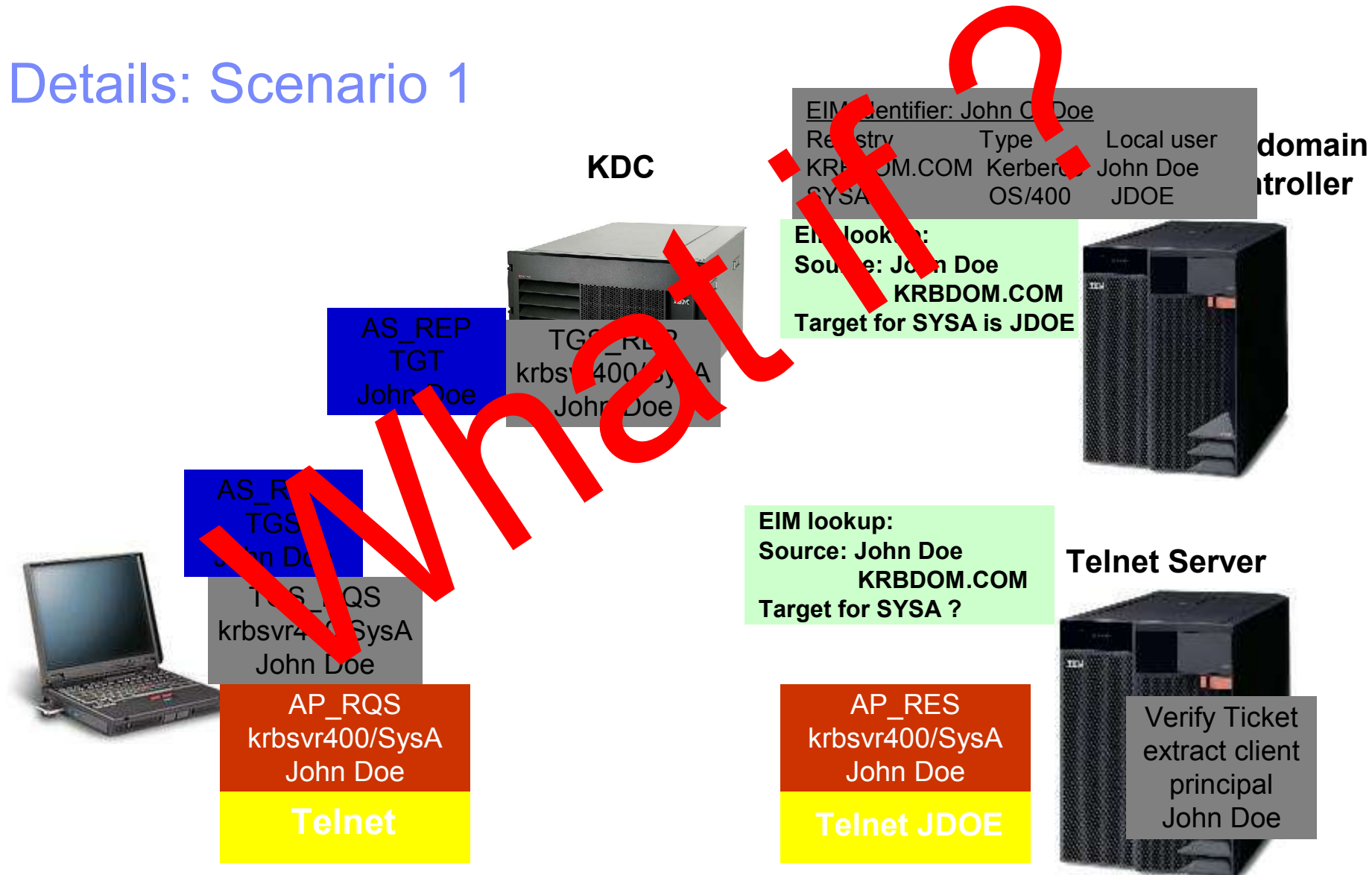
- **OS/400 client and server applications that are currently enabled for SSO are:**
 - OS/400 Host Servers (5722-SS1 Option 12): Currently used by iSeries Access for Windows and iSeries Navigator.
 - Telnet server: Currently used by PC5250 and IBM WebSphere Host On-Demand Version 8: Web Express Logon feature.
 - Open Database Connectivity (ODBC): Allows SSO access to OS/400 databases through ODBC.
 - Java Database Connectivity (JDBC): Allows SSO access to OS/400 databases through ODBC.
 - Distributed Relational Database Architecture (DRDA): Allows SSO access to OS/400 databases through ODBC.
 - QFileSrv.400
 - LDAP Server: Supports Kerberos authentication only. EIM is not used during the authentication process.
- **The following applications were enabled for EIM, Kerberos, or both in V5R3:**
 - Management Central for authentication between endpoint systems and the central system.
 - Windows Integration for user enrollment and for submitting network server commands.
 - HTTP Server for iSeries (powered by Apache) when using Microsoft's Internet Explorer 5.0 or later. This support was also added to V5R2 via the HTTP group PTF.
 - The V5R3 enhancement of storing user certificates in LDAP servers also provides the ability for OS/400 applications, such as the FTP server, to use EIM for lookup operation of a target association. This function only pertains to OS/400 applications using digital certificates for client authentication. It is not related to Kerberos at all.

Scenario 1: Traditional configuration

Step 4: Lookup

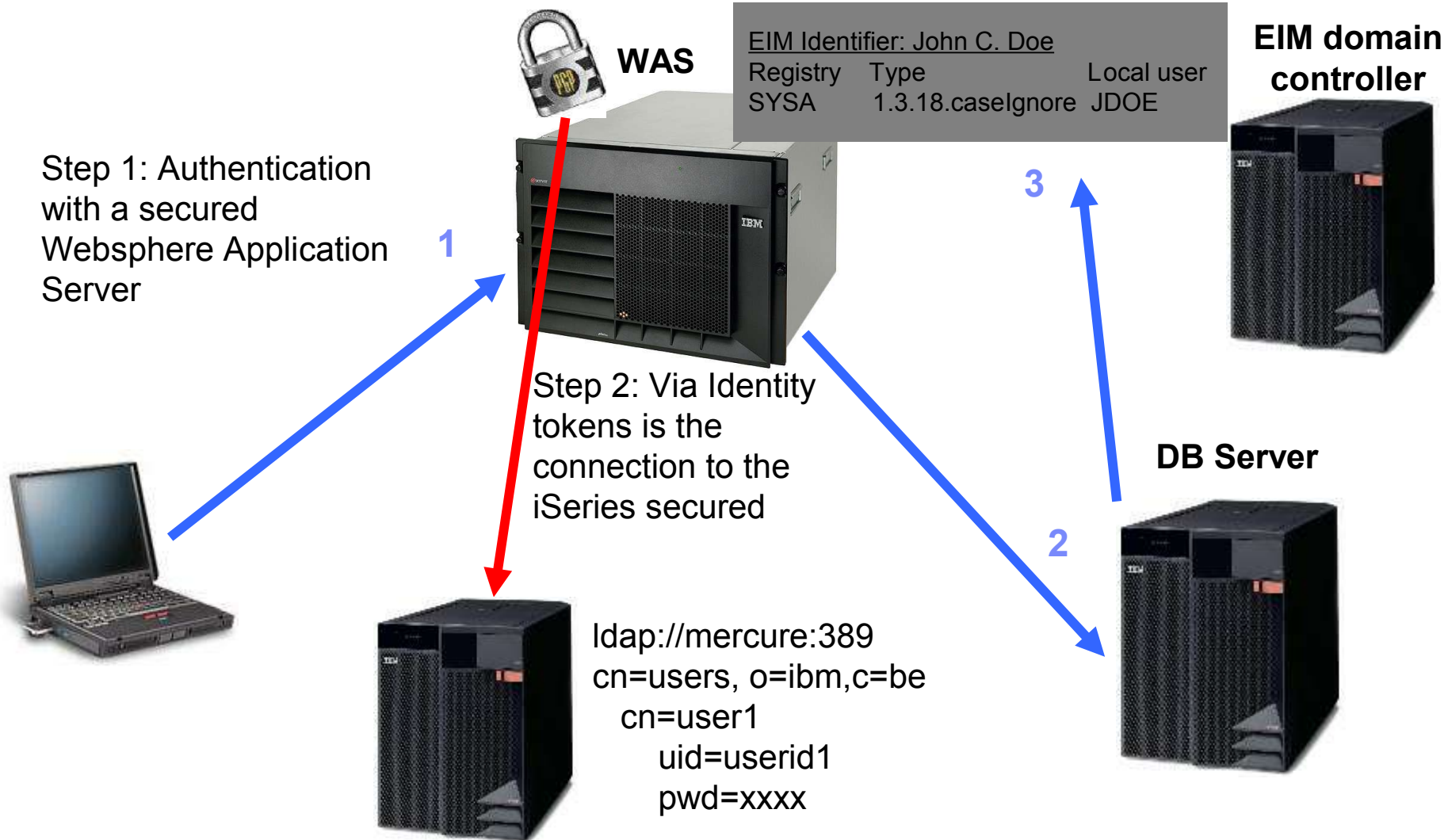


Details: Scenario 1

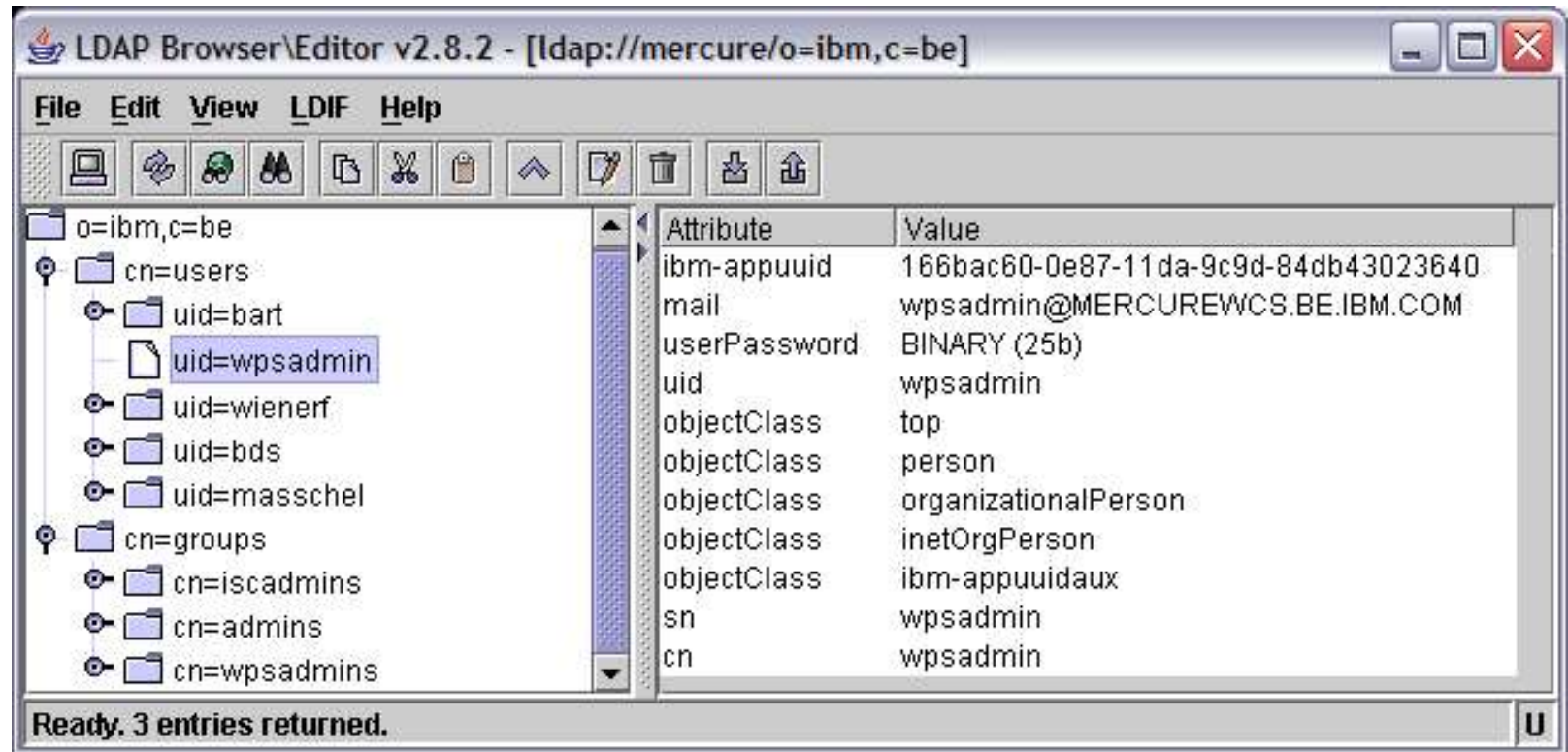


Scenario 2: e-business configuration

Step 3: Lookup



Scenario 2: Authentication source: LDAP



ldap://mercure:389

DN: uid=wpsadmin,cn=users,o=ibm,c=be

Notes: LDAP

- The Lightweight Directory Access Protocol (LDAP) is an open industry standard that has evolved to meet these needs. LDAP defines a standard method for accessing and updating information in a directory. LDAP has gained wide acceptance as the directory access method of the Internet and is therefore also becoming strategic within corporate intranets. It is being supported by a growing number of software vendors and is being incorporated into a growing number of applications. For example, the two most popular Web browsers, Netscape Navigator/Communicator and Microsoft Internet Explorer, as well as application middleware, such as the IBM WebSphere Application Server or the IBM HTTP server, support LDAP functionality as a base feature.

Scenario 2: e-business configuration

- Identity tokens and LTPA keys
LTPA is the decriptor of the token
- Identity tokens together with EIM
- Credential vault (shared or not)
- TAM: Tivoli Access Manger

Lotus. software

WebSphere. software

IBM **@server**[®]

WebSphere. software

WebSphere. software

Tivoli. software

Where is the standard ?

Notes: Scenario 2

- Identity tokens is one mechanism to authenticate EIM). LTPA keys are also possible (export import), but both the application server must be secured and must refer to the same LDAP server.
- TAM: Tivoli Access Manger. Tivoli has its own product (compared to EIM) to map users.

Demo

References:

- *Implementation and Practical Use of LDAP on the IBM iSeries™ Server, SG24-6193*
- *Using LDAP for Directory Integration, SG24-6163*



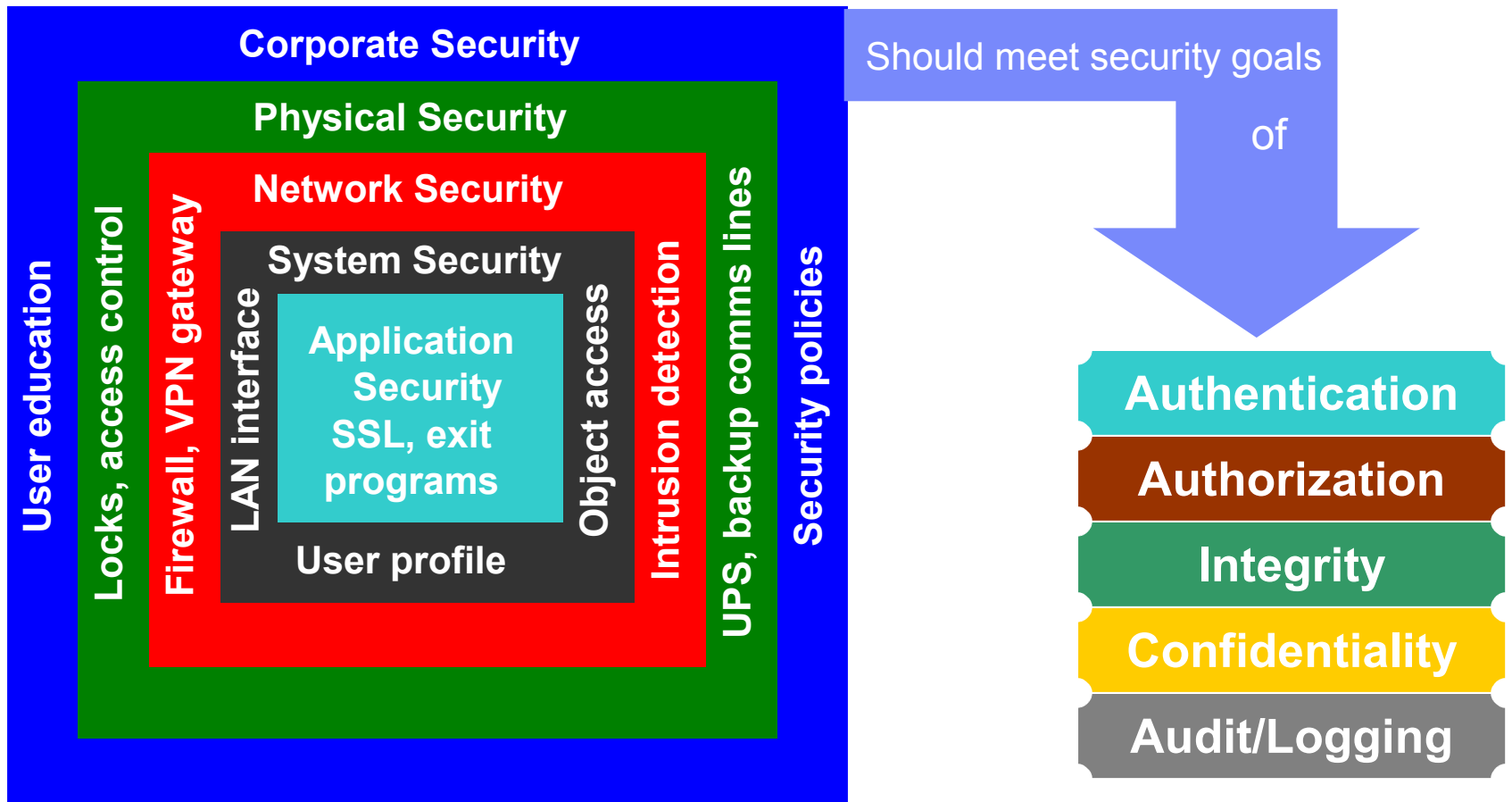
Common Belgium

SSL: Secure Socket Layer

September 20, 2005

© 2005 IBM Corporation

Layered implementation of security



Notes: Layered implementation of security

Simply implementing a firewall is not enough to prevent unwanted access to confidential data on your systems. Implementing security in your e-business environment must begin with your corporate security plan. After you determine what the security plan entails, you must tailor it to secure your environment at all layers identified.

The implementation of security in various layers should always meet one or more of the following common security goals:

Authentication: Determine that the users are who they claim to be. The most common technique to authenticate is by user ID and password.

Authorization: Permit a user to access resources and perform actions on them. An example of authorization is the permissions on OS/400 objects.

Confidentiality: Only authorized users can view the data. For data that is transmitted through a network, there are two ways to achieve this goal:

- Make sure that only authorized persons can access the network

- Encrypt the data

Integrity: Only authorized users can modify the data, and they can only modify it in approved ways. The data is not changed either by accident or maliciously. For data that is transmitted over a network, there are two ways to achieve this goal:

- Make sure that only authorized persons can access the network (not easy to achieve in public networks such as the Internet)

- Digitally sign the data

SSL: Secure Socket Layer

- SSL is at no cost on i5/OS
- A lot of services can be secured:
Telnet, HTTP, Hostservers, Object Signing



Notes: SSL

- Nowadays, security is one of the main topics in the industry. i5/OS is secure because of its outstanding security framework, but it can always be better.
- Sniffer tools are dangerous for password catching ,e.g. Telnet, HTTP and FTP. Netserver uses already encrypted passwords, the http server on i5/OS can be secured via Basic Security ... but this is not secure enough (www.google.be and you find already a decryptor)
- SSL or Secure Socket Layer is the mechanism to encrypt ALL your traffic to and from the i5/OS box and is free of charge.

How ?

SSL and Certificates

- Server authentication:
 - The certificate to do the encryption is downloaded first to the client and then the SSL connection is started.

- Client authentication
 - First: Server authentication
 - Second: Client passes his user certificate to the server and gets validated.
 - Remark: When installing the user certificate a private key is generated.

- CA, Verisign, Geotrust

Notes: How ?

Certificates are used by SSL to implement much of the encryption/decryption and validation work. These certificates used by SSL are stored in *key databases* (sometimes called *key stores*). There can be several different key databases on each platform (PC, iSeries, and so on). These databases are usually protected by a password. It is very important to have SSL certificates under key database password control on iSeries, because data inside each certificate makes it possible for SSL to establish trust and validation for each connection. It is also very important to track and understand when the certificates you are using will expire, so you can renew them ahead of time. Failures can occur if you use an expired certificate. To view and renew your configured certificates, use Digital Certificate Manager interfaces.

SSL gives some performance overhead, therefore Cryptographic Coprocessors are available.

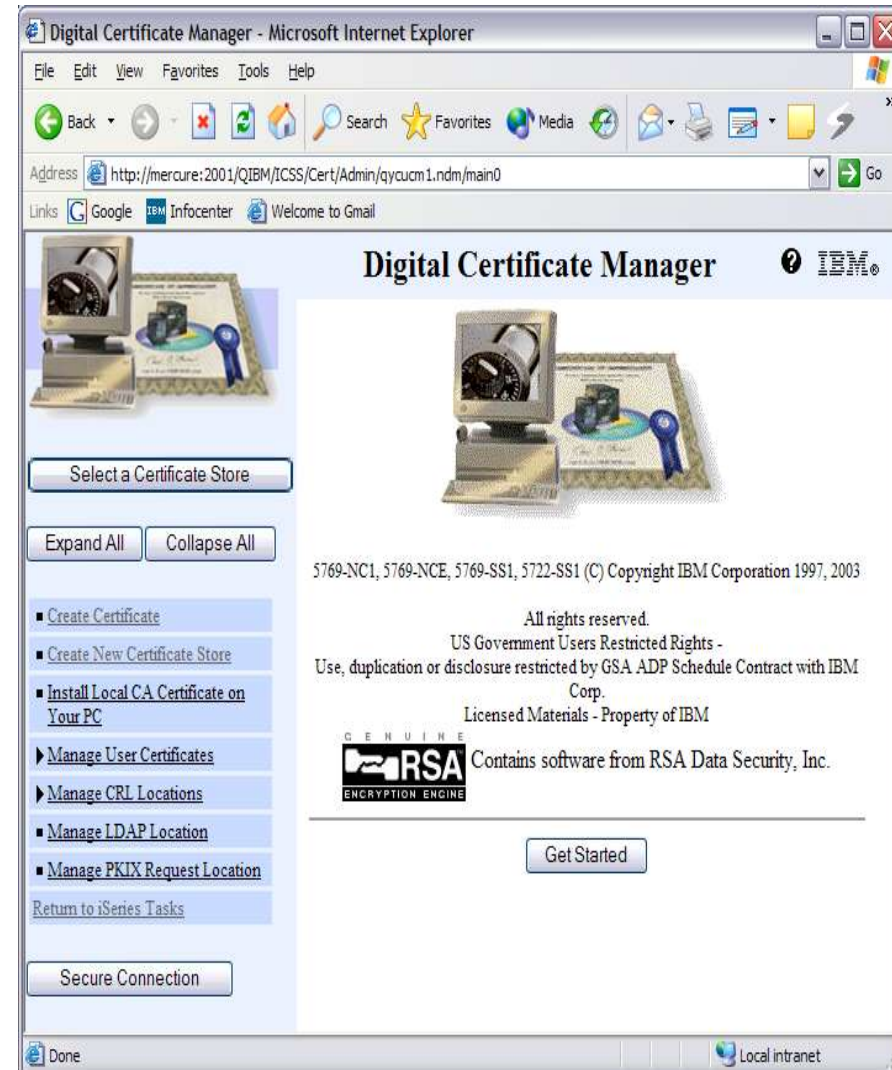
Notes: How ?

- If the iSeries is used to create client certificates, a browser capable of importing/exporting secure PKCS12 files is required. (Currently Microsoft Internet Explorer 5.x and Netscape 4.x or later have this capability.) After the client certificate is created, you need to export it from the browser and import it into the PC SSL key database using IBM Key Management.
- Next to iSeries certificates you can also use Versign certificates (<http://www.verisign.com>) or Geotrust (<http://www.geotrust.com>).

Prerequisites

- Cryptographic Access Provider
- Client Encryption
- DCM: Digital Certificate Manager

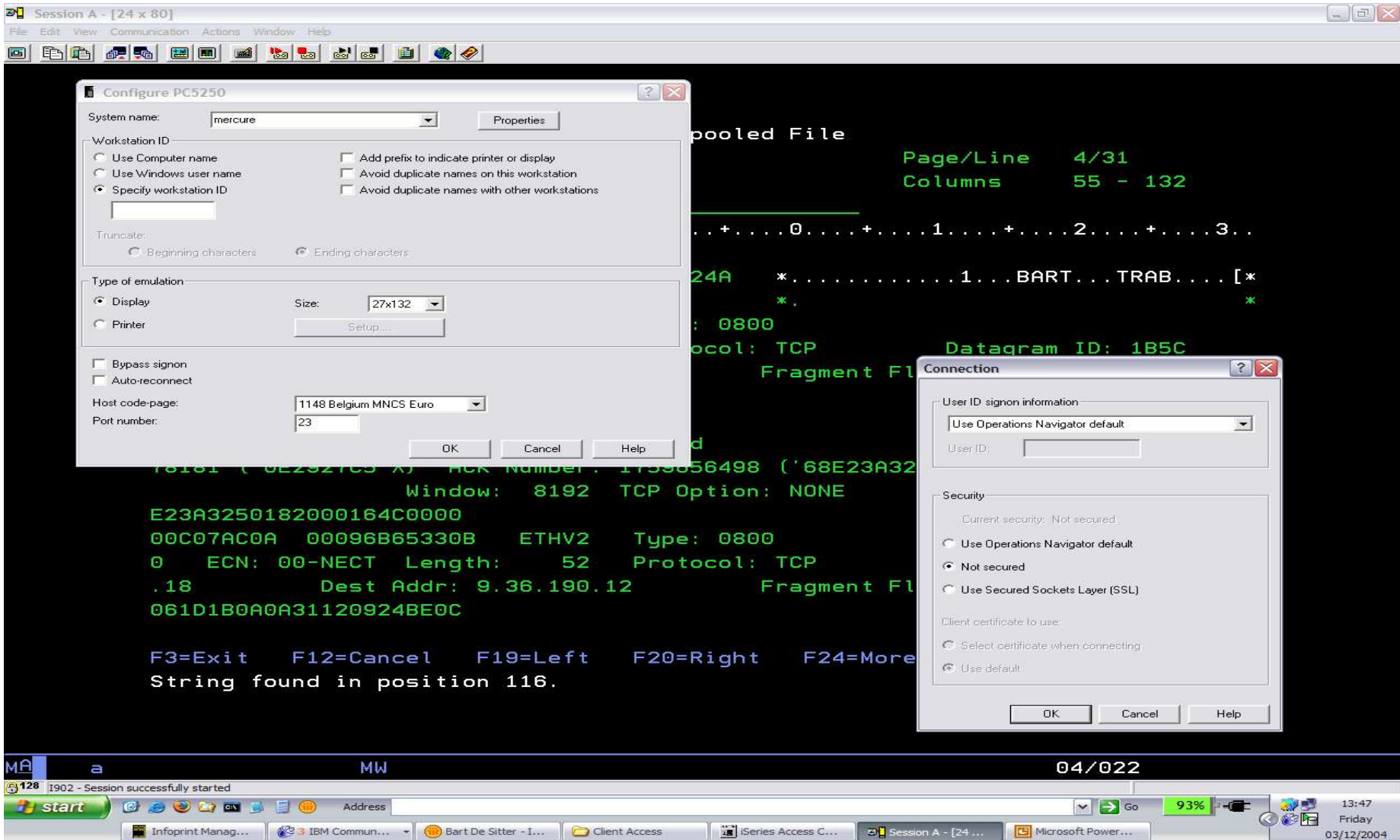
At no charge !



Notes:

- IBM Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1).
- TCP/IP Connectivity Utilities for iSeries (5722-TC1).
- IBM HTTP Server for iSeries (5722-DG1). If you are trying to use the HTTP server to use the DCM, be sure you have the IBM Developer Kit for Java (5722-JV1) installed. By default on the iSeries, this product provides the iSeries HTTP Administration Server, which has a link to the Digital Certificate Manager from the administration server's initial page. If you need to start this administration server, enter the following Start TCP Server command from a 5250 session: `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`
- The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.
- Client Encryption product, 5722-CE3 (128-bit). iSeries Access for Windows needs this product in order to establish the secure connection.

Demo



The screenshot displays a PC5250 emulation environment. The main window, titled "Session A - [24 x 80]", shows a terminal with green text on a black background. The terminal content includes:

```

pooled File
Pa
Co
...2...+...3...
am ID: 1711
'T, LAST
6E4400AA0351D4BC
ED82470B605643C3
93835B74046C615B
3150CE3F35EC0480
6B7E1C87B2E0F5CF
5553CF2CC2D6CDAC
7E2C005C023F337D
B0F1561C10C5867E
*...V...F3...Z'A...+>...M.*
*..6.$G..XYU[...1...DIG..H.B.-..C*
*...L... 'V...G/...LC$.%/$*
*H-I..*N}...%_]3.C...1..&...*
*...L... ,6%.F..K...8,=.G..5.*
*.HC..X.....-..CM.....BO..*
*...EL.....B...I...%=... '*
*L..M,.YP..U.....L.Z0..1...EF=*

```

Below the terminal, a status bar shows: F3=Exit F12=Cancel F19=Left F20=Right F24=More keys

Two configuration windows are open:

- Configure PC5250:** System name: mercure. Workstation ID options: Use Computer name, Use Windows user name, Specify workstation ID. Type of emulation: Display (Size: 27x132). Host code-page: 1148 Belgium MNCS Euro. Port number: 992.
- Connection:** User ID signon information: Use Operations Navigator default. Security: Use Secured Sockets Layer (SSL).

The Windows taskbar at the bottom shows the date 03/12/2004, time 13:45, and 93% battery. The address bar contains "I902 - Session successfully started".



Common Belgium

OpenSSH



September 20, 2005

© 2005 IBM Corporation

Why SSH? (Secure Shell)

Again ... normal communication is not secure.

Sniffer tools are dangerous !



What is SSH? (1/2)

- SSH is a program to log into another computer and run commands
- Entire datastream is encrypted (via public key)
- OpenSSH is the free version of the SSH protocol suite
- Several utilities (ssh – sftp - ...)
- Two protocols are available: SSH1 and SSH2

What is SSH? (2/2)

- `ssh` is the client utility used to connect to and run commands on a server running the SSH daemon (`sshd`)

```
ssh [user@]hostname [command]
```

- The `ssh` client is also needed to connect to the HMC (`cmd`)

- A popular `ssh` client is PuTTY
Available for Windows and Unix clients

And now on iSeries?



Portable Utilities for i5/OS

- Portable Utilities for i5/OS is a license program product (free of charge)
LPP number 5733-SC1 (only in 2924)
- Requires i5/OS Portable Application Solution Environment (PASE)
5722-SS1 Option 33



Common Belgium

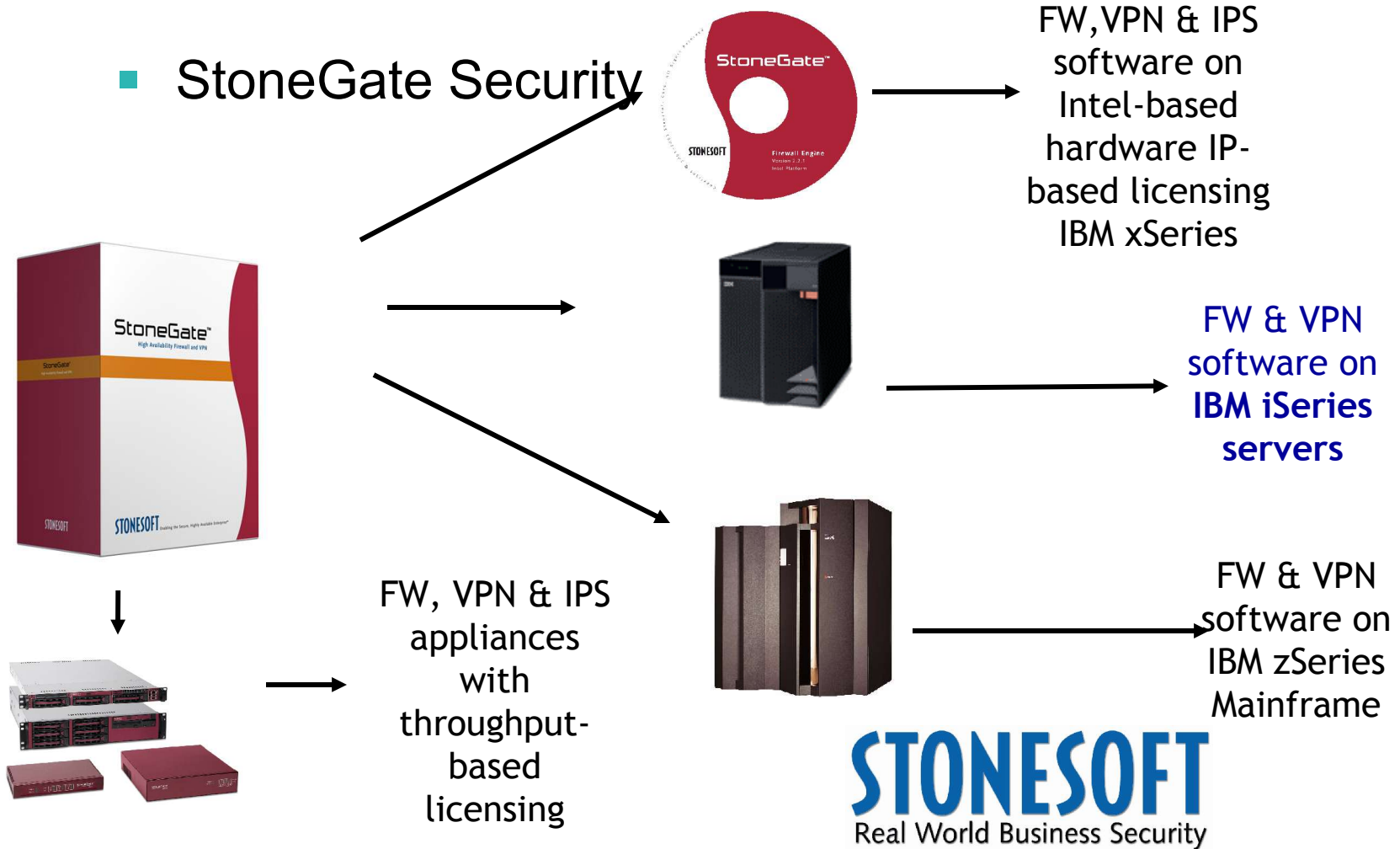
Firewall and other security enhancements

September 20, 2005

© 2005 IBM Corporation

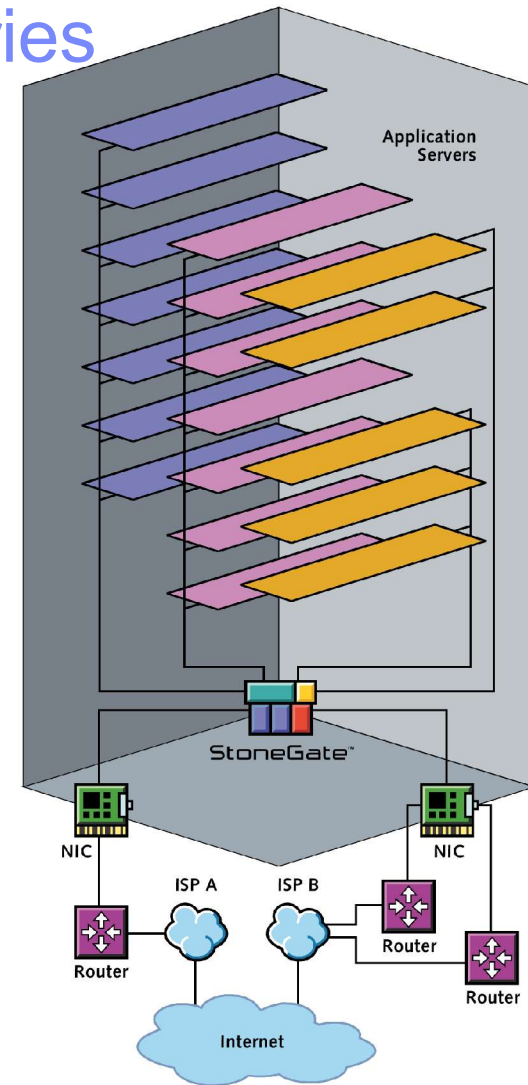
Support of Linux-based firewall

■ StoneGate Security



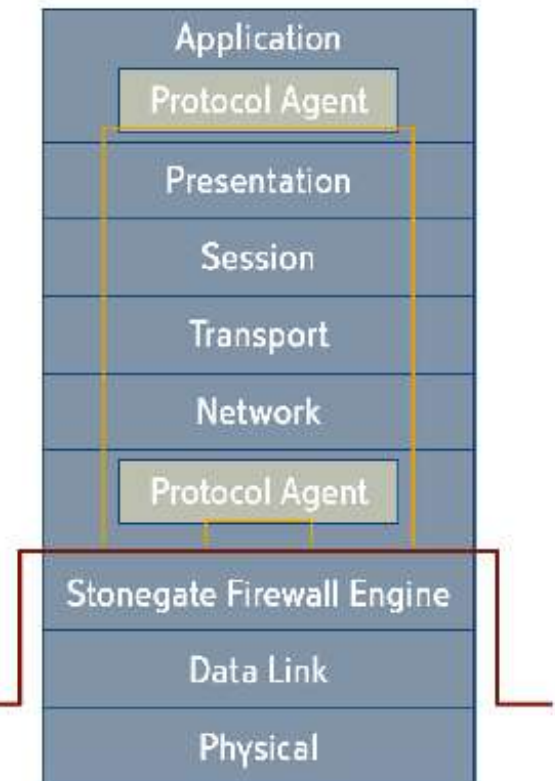
StoneGate Firewall & VPN for iSeries

- **When:**
 - New workloads, new technologies
 - New iSeries installations
 - Legacy firewall replacement
- **What:**
 - Linux powered, advanced security inside iSeries
 - Secure server consolidation
 - Secure network virtualization
- **Benefits:**
 - Best security and availability over the Internet
 - Next-to-application firewall and VPN security
 - Easier to manage and maintain
 - Infrastructure simplification



Linux-based firewall

- Provides
 - Multi-Layer Inspection
 - packet filtering
 - stateful inspection
 - application layer inspection
 - Standards compliant VPN
 - IPSec compliant
 - Multi-Link Technology
 - Manageability
- Application layer security with Protocol Agents
- Remote upgradeable
- Operating system hardened for firewall and VPN use
 - Includes only modules needed by StoneGate
 - e.g. sshd included in the standard installation – no telnet
 - Read only filesystem (romfs)



Firewall on iSeries: Packet filtering

The screenshot displays the iSeries Navigator interface with the following components:

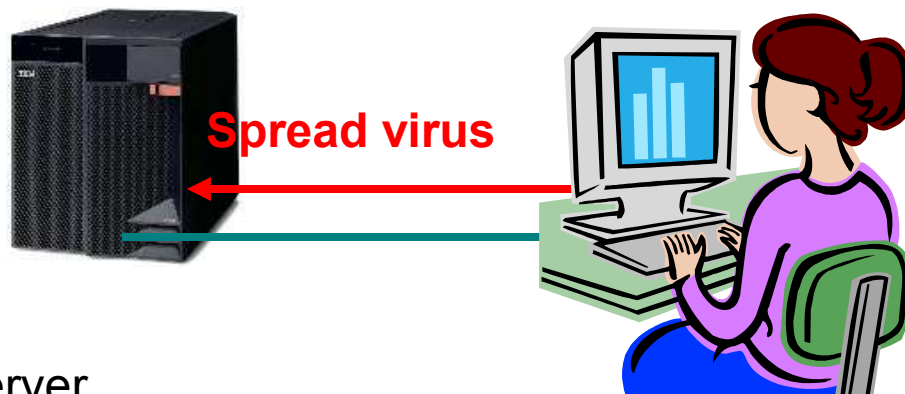
- iSeries Navigator:** The main application window showing a tree view of the environment. The 'My Connections' folder is expanded, showing various connections and services. The 'Packet Rules' folder is selected.
- Service to Permit:** A dialog box titled "Service to Permit" with the question "What service do you want to permit?". It has two radio buttons: "Define a service by protocol and ports" (unselected) and "Permit the service selected in the list below" (selected). A list box contains the following services: CLIENTACCESS, DNS, FINGER, FTP, GOPHER, HTTP, IKE, and L2TP. Navigation buttons "Back", "Next", and "Finish" are at the bottom.
- Service Definition:** A dialog box titled "Service Definition" with the question "What is the protocol and port information for the service?". It has a "Protocol:" dropdown menu set to "TCP". Below it, "Server ports:" are defined as a range from "=" to a text box containing "23", with "Add" and "Remove" buttons. "Client ports:" are defined as a range from ">=" to a text box containing "1024". Navigation buttons "Back", "Next", "Finish", "Cancel", and "Help" are at the bottom.
- My Tasks - Mercure:** A task list at the bottom left showing "Add a connection" and "Install additional components".
- IP Policies tasks:** A task list at the bottom right showing "Edit IP Packet Rules", "Configure Virtual Private N...", and "Order Virtual Private Net...".

Configure the packet rules.

Antivirus scanning

Viruses cause significant damage to businesses every year

- Infrastructure support added for enhanced virus scanning for the Integrated File System (IFS)
- Allows third-party vendors to develop antivirus scanning software that plugs into i5/OS (OS/400)
- Scanning support available to scan for any other purpose as an object is opened or closed

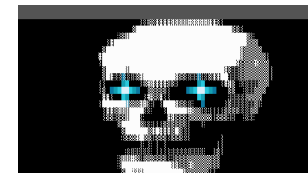


NetServer
FTP, NFS



From the Creators of BugBear

W32/BabyBearA



Phantom 1



W32/Cidu-A

Antivirus scanning

- OS/400 keeps track of all changes and only calls the scanning software when files or virus definition files change.
Scanning behavior can be controlled via IFS object attributes and system values.
- Only objects with IFS *TYPE2 in /root, QOpenSys and UDFS file systems are scanned.

Antivirus scanning

- Virus scanning products can register to the following exit points:
 - QIBM_QP0L_SCAN_OPEN: Integrated File System Scan on Open Exit Program
 - QIBM_QP0L_SCAN_CLOSE: Integrated File System Scan on Close Exit Program

- System-wide behavior

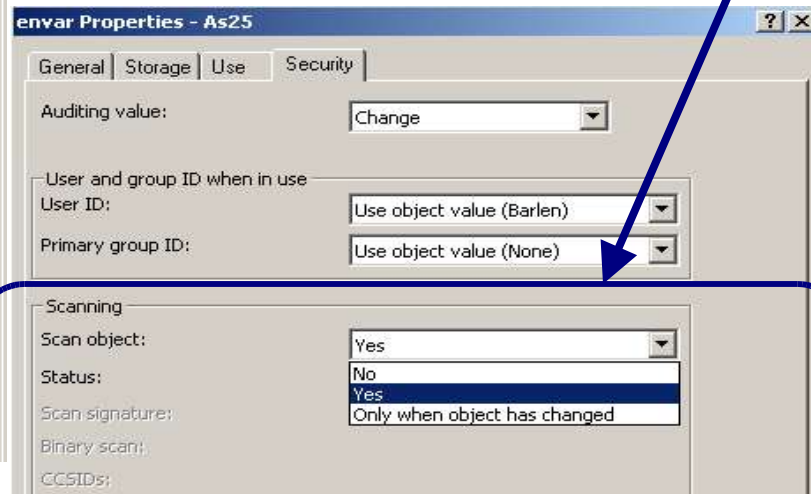
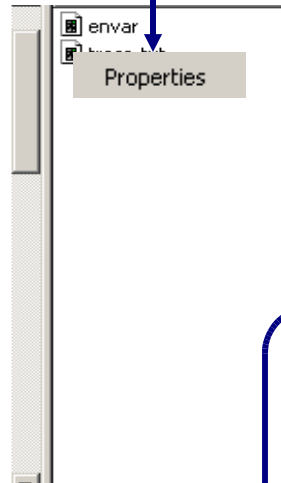
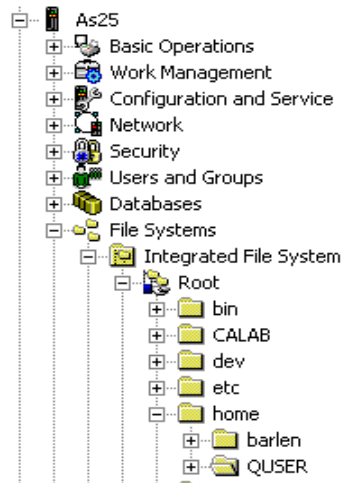
System value
QSCANFS

System value
QSCANFCTL



Antivirus scanning

- Which files are being scanned can be further controlled via IFS object attributes.
- The following two new attributes were added and can be set via the Change Attribute (CHGATR) command:
 - *CRTOBJSCAN: Specifies whether to scan objects created in a directory
 - *SCAN: Specifies whether to scan a specific object



File properties

```
CHGATR OBJ ( ' /home/quser/envar ' ) ATR ( *SCAN ) VALUE ( *NO )
```



Common Belgium

Time Synchronization

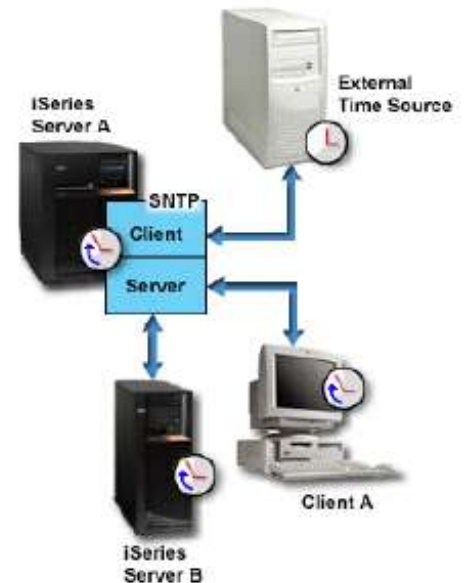


September 20, 2005

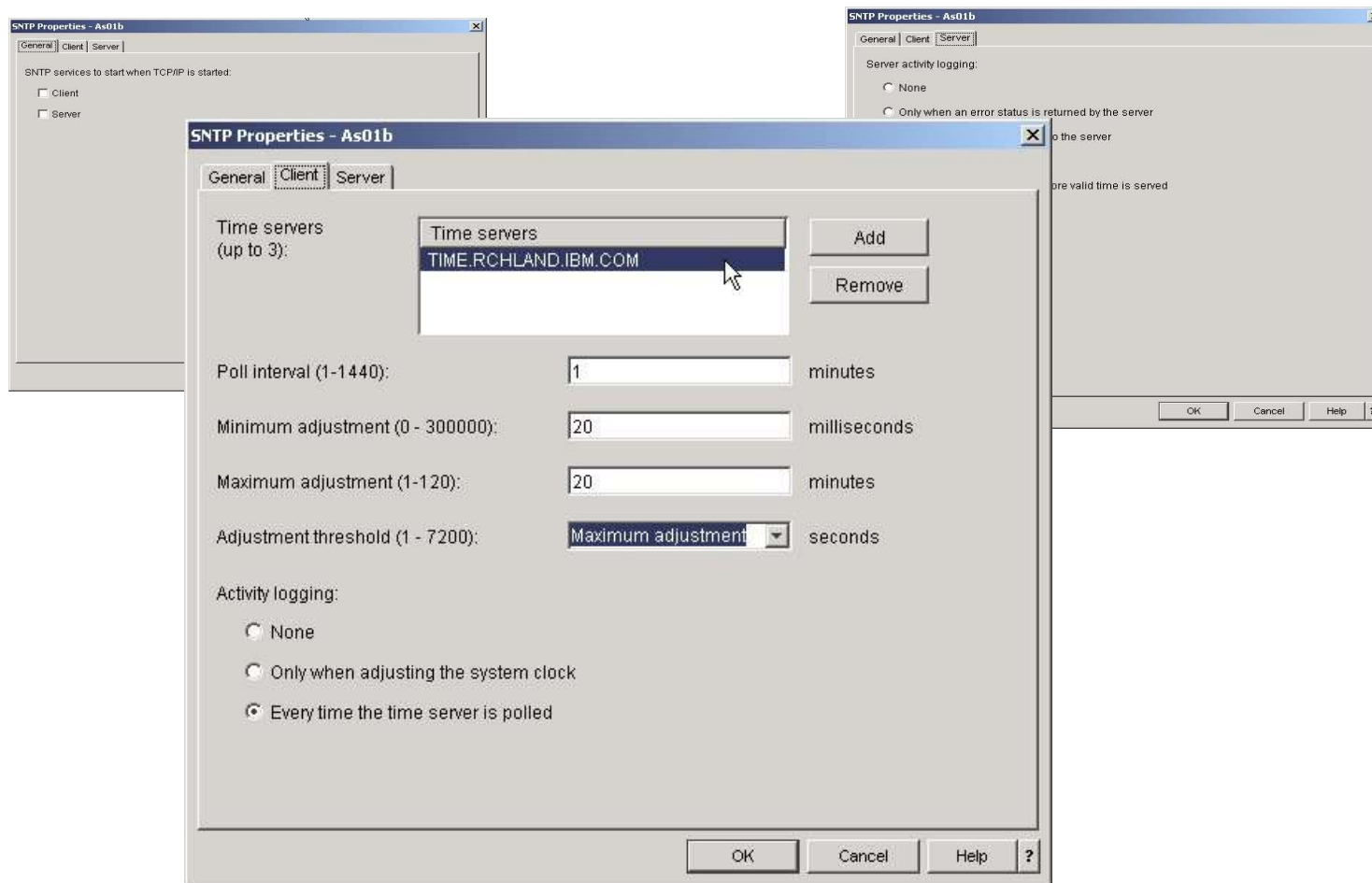
© 2005 IBM Corporation

What time is it?

- V5R3 SNTP client changes system clock instead of software clock
- V5R3 SNTP server support iSeries serves time to other clients
- iSeries SNTP client and server can run concurrently

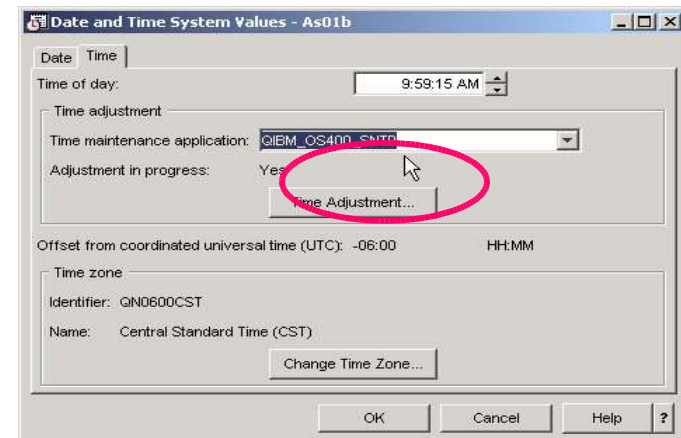


SNTP Configuration in iNav

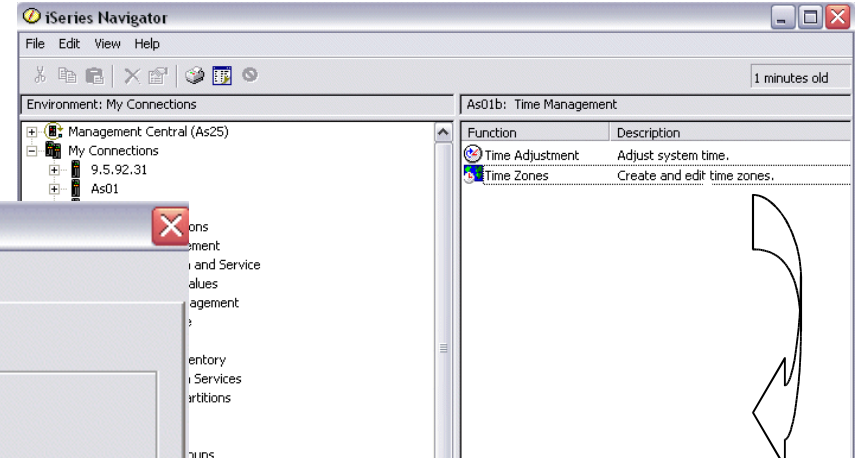


System values

- QDATETIME
Composed of system values QDATE and QTIME
- QTIMADJ
Time adjustment system value
Identify the software to use to adjust system clock
Keep system clock synchronized with external time source
- QTIMZON
Central European Time: QP0100CET2



Daylight savings time



Edit Time Zone QN0600CST - As01b

General | Daylight Saving Time

Enable Daylight Saving Time

Daylight Saving Time name

Use system-generated name

Use name specified in message

Message ID:

Note: Specify message file on General page.

Use specified name

Full name:

Abbreviated name:

Start

Month:

Day:

Occurrence of day in month:

Time:

End

Month:

Day:

Occurrence of day in month:

Time:

Time Zones - As01b

Current time zone system value

Identifier: QN0600CST

Name: Central Standard Time (CST)

Available time zones:

Identifier	Offset	Standard Time Name	Daylight Saving Time Name
Q0000GMT	00:00	Greenwich Mean Time (GMT)	
Q0000GMT2	00:00	Greenwich Mean Time (GMT)	British Summer Time (BST)
Q0000UTC	00:00	Coordinated Universal Time (UTC)	
QN0100UTC5	-01:00	UTC-01:00 Standard Time (UTC-01:00S)	
QN0200UTC5	-02:00	UTC-02:00 Standard Time (UTC-02:00S)	
QN0300UTC5	-03:00	UTC-03:00 Standard Time (UTC-03:00S)	
QN0300UTC2	-03:00	(GMT - 3:00) Brasilia (UTC-03:00S)	(GMT - 3:00) Brasilia Daylight Saving Time (UTC-03:00D)
QN0330NST	-03:30	Newfoundland Standard Time (NTS)	Newfoundland Daylight Time (NDT)
QN0400AST	-04:00	Atlantic Standard Time (AST)	Atlantic Daylight Time (ADT)
QN0400UTC5	-04:00	UTC-04:00 Standard Time (UTC-04:00S)	
QN0400UTC2	-04:00	(GMT - 4:00) Caracas, La Paz (UTC-04:00S)	
QN0500EST	-05:00	Eastern Standard Time (EST)	Eastern Daylight Time (EDT)
QN0500EST2	-05:00	Eastern Standard Time (EST)	
QN0500UTC5	-05:00	UTC-05:00 Standard Time (UTC-05:00S)	
QN0600CST	-06:00	Central Standard Time (CST)	Central Daylight Time (CDT)
QN0600S	-06:00	Central Standard Time (S)	Daylight Saving Time (DST)
QN0600UTC5	-06:00	UTC-06:00 Standard Time (UTC-06:00S)	
QN0700MST	-07:00	Mountain Standard Time (MST)	Mountain Daylight Time (MDT)
QN0700MST2	-07:00	Mountain Standard Time (MST)	
QN0700T	-07:00	Mountain Standard Time (T)	Daylight Saving Time (DST)
QN0700UTC5	-07:00	UTC-07:00 Standard Time (UTC-07:00S)	
QN0800PST	-08:00	Pacific Standard Time (PST)	Pacific Daylight Time (PDT)
QN0800U	-08:00	Pacific Standard Time (U)	Daylight Saving Time (DST)
QN0800UTC5	-08:00	UTC-08:00 Standard Time (UTC-08:00S)	

Change System Value...

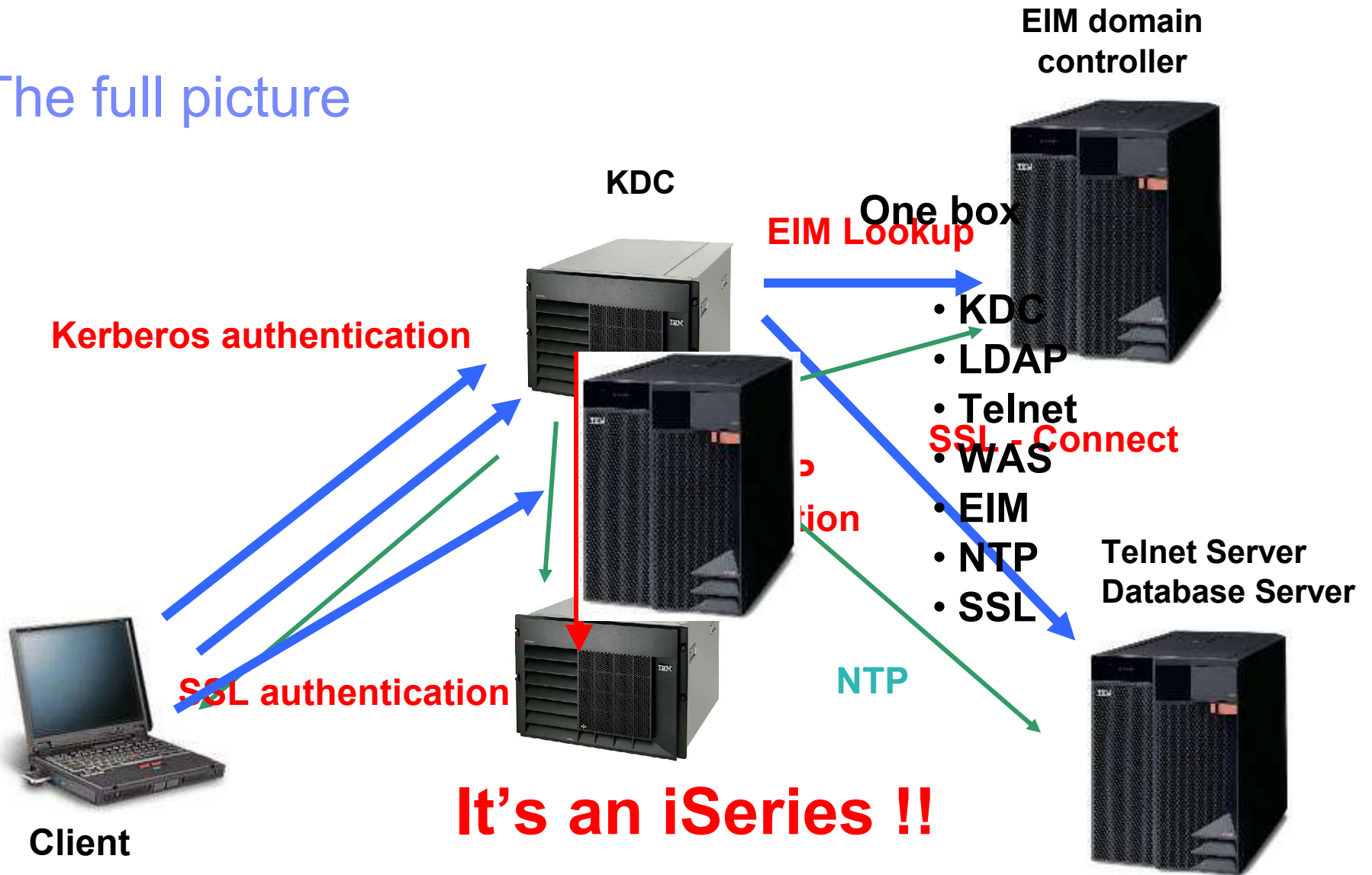
New...

New Based On...

Edit...

Delete...

The full picture





Time for lunch ...