
**...And Now,
Something Totally Different**

**Internet's Here To Stay
And It Wont Go Away!
Directories And Security
I NEED GSO!!**

**Lil' Stickys Everywhere!!
Passwords Being Shared!!
Data Everywhere, Everytime I Pray...
I NEED GSO!!**

**One Fine Morning
When I Had One Mainframe
I Had One Password Too!**

Then Came Oracle
Then Came Netscape
There Was Always NetWare
Then This Guy Called Gates
Said To "Just Have Faith"
'97? '98? How Long Must I Wait?

~~Didn't Know What To Do~~
So I Called BIG BLUE
Wanna Talk To Lou
Can You Help Me Please
System's At Its Knees
Single Sign-On Is Key
He Said "I Know, Got The Answer
...GSO"

**Internet's Here To Stay
And It Wont Go Away!
Directories And Security
I NEED GSO!!**

Lil' Stickys Everywhere!!
Passwords Being Shared!!
Data Everywhere, Everytime I Pray...
I NEED GSO!!

IBM Global Sign-On

Secure Single-Entry Access to Your
Computing Resources

ARCHITECH
IT EXECUTIVE CONFERENCE

Agenda

- The Value of Single Sign-On
- What to Look for When Choosing a Single Sign-On Solution
- Overview of IBM's Global Sign-On (GSO)
- IBM Global Sign-On Features and Benefits
- IBM Global Sign-On Directions
- Summary

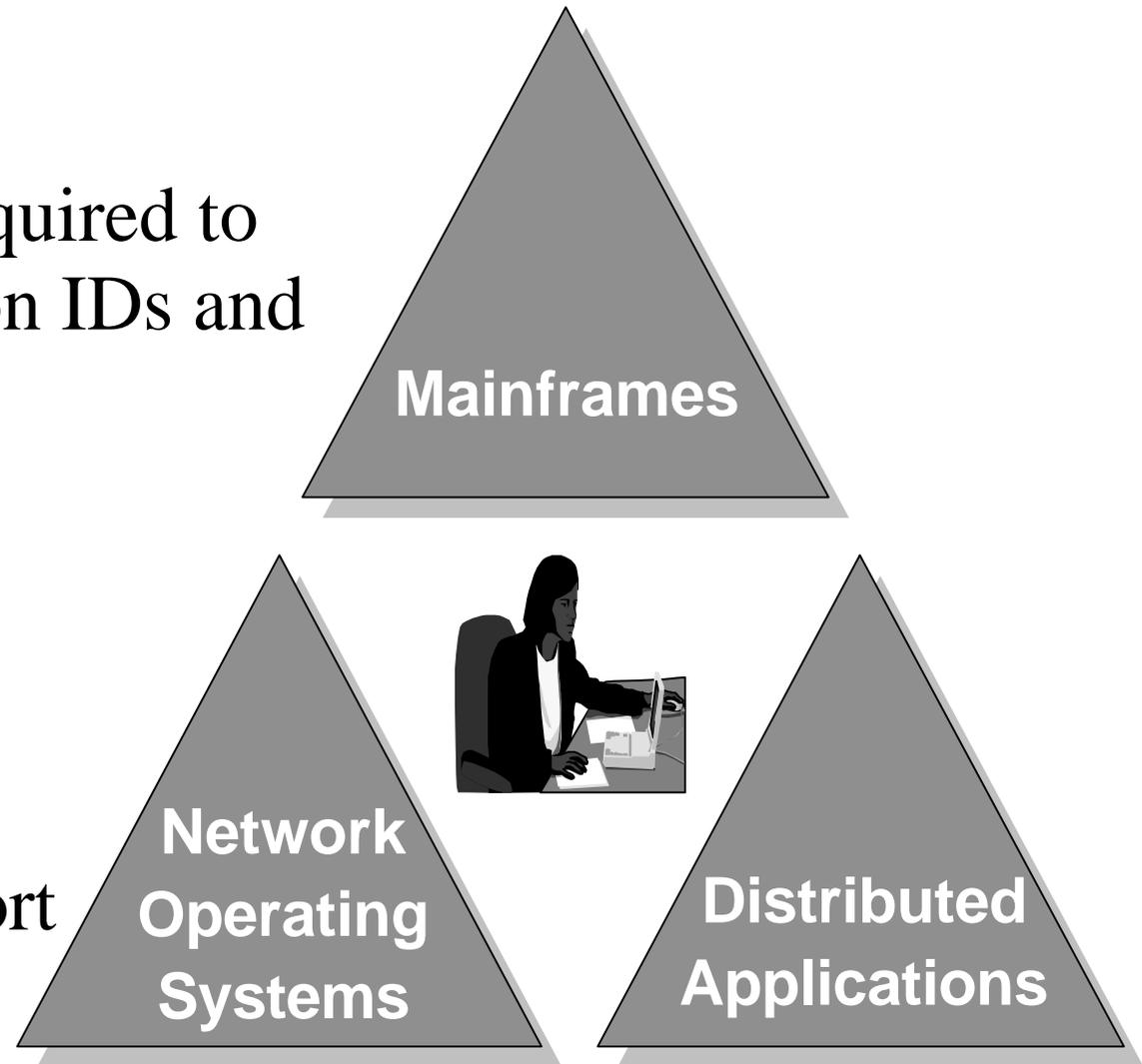
The Value of Single Sign-On

Problem:

End users are now required to manage multiple logon IDs and passwords

Problem causes:

- Loss of productivity
- Security exposures
- Increases admin effort



Who Benefits and How Much?

Which Businesses Benefit The Most?

Those that have large enterprises where employees need to access applications distributed over many types of networked systems

What Do They Gain?

Simplified logon process => Increased user productivity => Cost Savings*

Annual cost, hours	Annual cost, per user	Annual cost, per 10,000 users	Figures based on annual salary ranges: \$25K - \$125K
3	\$100 - 250	\$500K - 2M	
15	\$250 - 1,000	\$2M - 9M	
44	\$500 - 2,600	\$5M - 26M	

Reduced administration effort => Cost Savings

One help desk reports 70% of daily calls are requests to reset passwords*

*Network Application Consortium (NAC), 1996

What To Look For In A SSO Solution

- ✓ **Ease of Use and Administration**
- ✓ **Strengthen, Not Weaken Security**
- ✓ **Integrated With the Operating System**
- ✓ **Consistent Across Operating Systems**
- ✓ **Easily Extendable**
- ✓ **Leverages Existing Security Infrastructure**
- ✓ **Based on Open, Industry Standards**

What To Look For In A SSO Solution

- ✓ **Supports Secret Key Passwords, One Time Passwords, and Public/Private Key Pair Passwords**
- ✓ **Login Location Independence**
- ✓ **Secure Storage of User Information**
- ✓ **Extendable Logon Methods**

IBM's Global Sign-On (GSO)

Solution

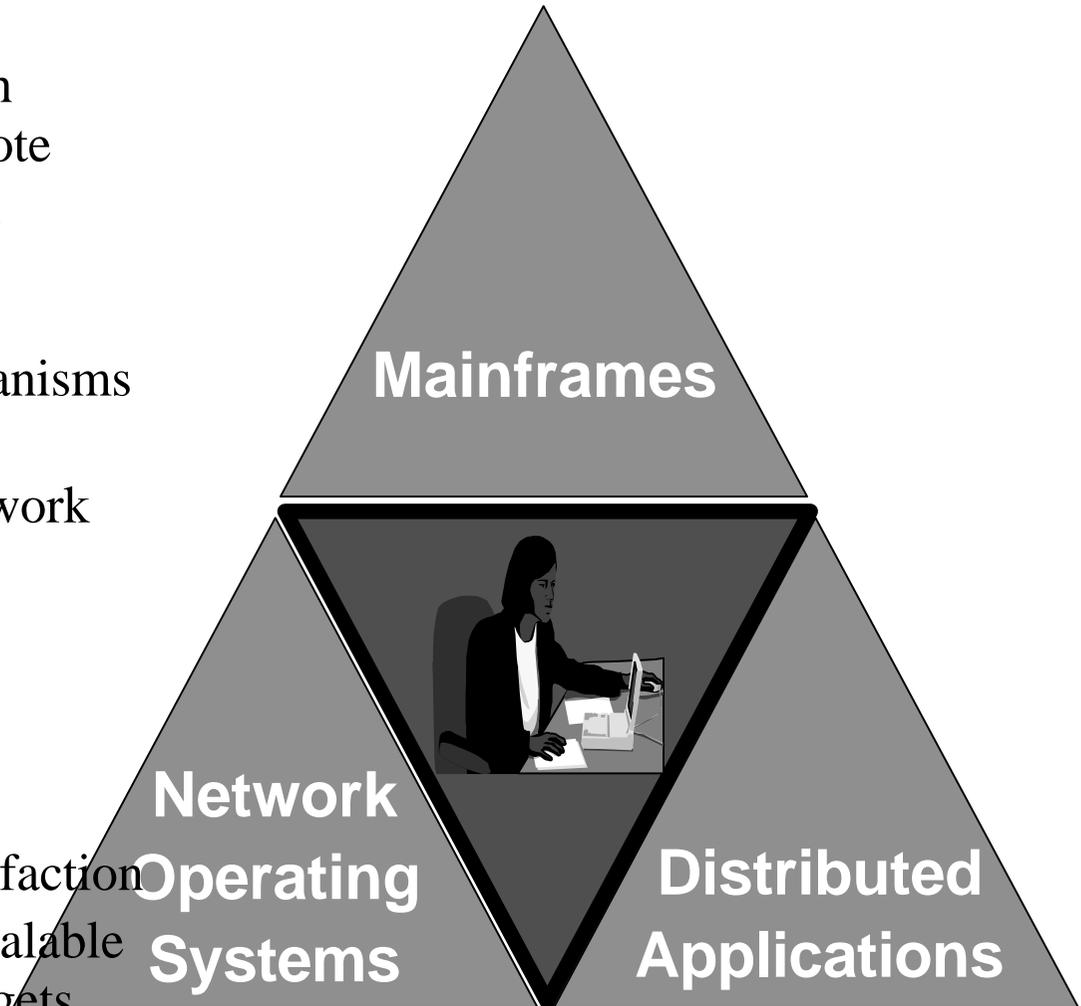
- GUI-based single sign-on tool which coordinates logons to local and remote resources with one ID and password

Implementation

- "*Federates*" existing security mechanisms under the GSO umbrella
- Contains an open, extendible framework – "Can't be all things to all people"
- First release uses Kerberos-based authentication server

Benefits

- Increases user productivity and satisfaction
- Provides an open, extendible and scalable framework for adding additional targets
- ~~Reduces security exposures~~



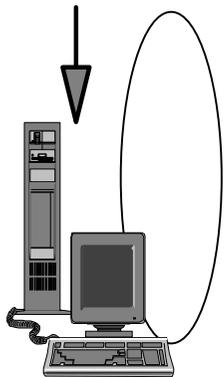
IBM Global Sign-On Architecture



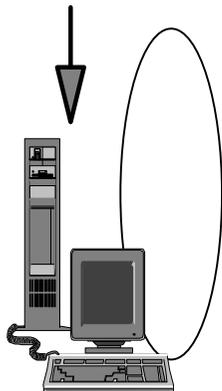
Pluggable Authentication

Primary Authentication Environment

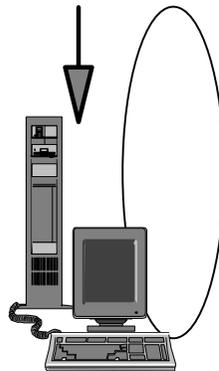
Logon Coordinator



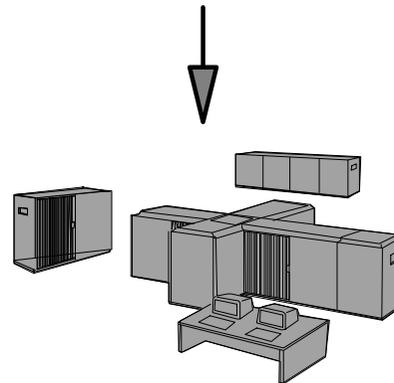
Warp Server



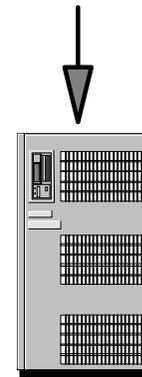
Netware



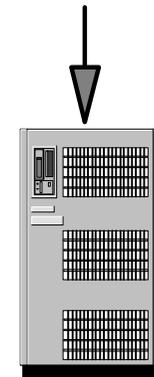
NT



Mainframes

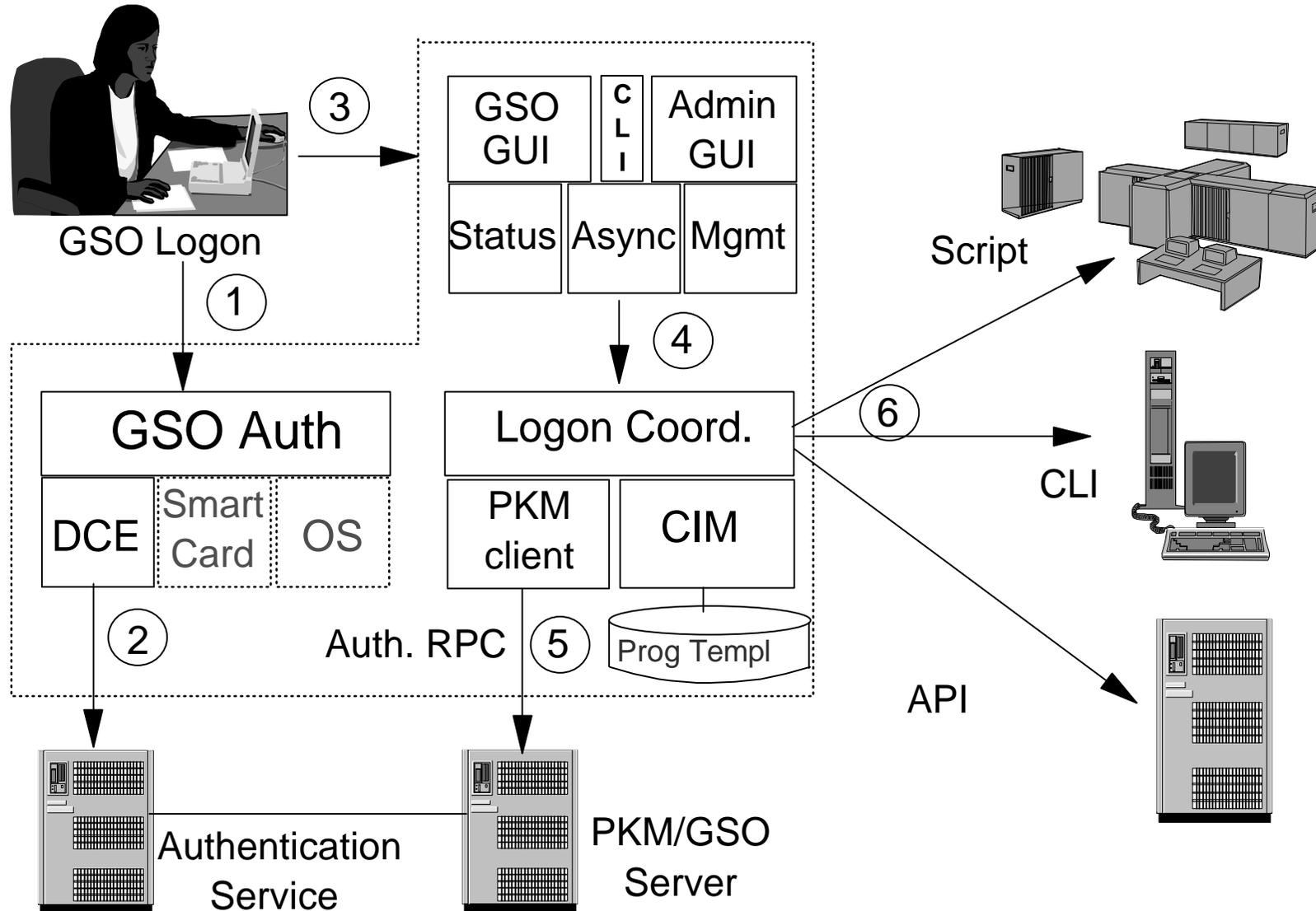


Databases



DCE

IBM Global Sign-On Architecture



IBM GSO System Components

- **Initial Authentication**

- ▶ Used to authenticate user to GSO system
- ▶ Integrated with local operating system security where applicable

- **Configuration Information Manager (CIM)**

- ▶ Contains information on how to logon to the targets configured on a given machine

- **Personal Key Manager (PKM)**

- ▶ Contains information about users and the systems and passwords they use to logon to those systems

- **Logon Coordinator (LC)**

- ▶ Retrieves user information from PKM and uses them in conjunction with the target specific logon code to log user onto target systems

DCE Security Features Used In GSO

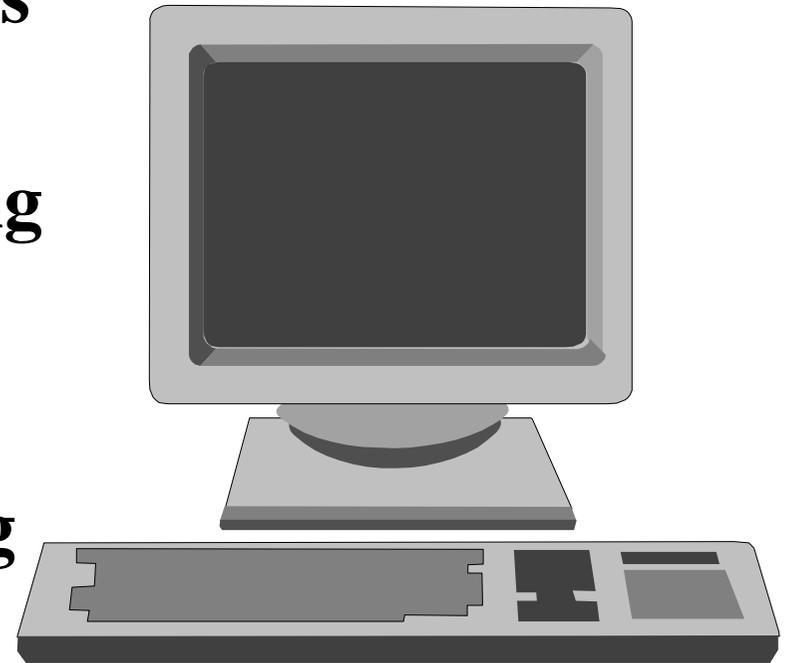
- **User Authentication Based On MIT's Kerberos V5**
 - ▶ Primary and initial authentication method support by GSO
 - ▶ No user password on the wire
- **Security Registry Support And Replication Services For High Level Of Availability**
 - ▶ User configuration and keys are stored in the DCE Security Service's registry
- **Ensures Integrity, User Data Privacy, And Tightly Integrated With Authenticated RPC**
 - ▶ User configuration/preferences via authenticated RPC with data integrity (default)
 - ▶ User keys via authenticated RPC with privacy (highest security level)

Accessing Targets Using GSO

- Target Templates and Script Files
 - ▶ ASCII file containing a target's logon, logoff, and change password characteristics and cmd sequences
 - ▶ File structure and keyword syntax/semantics to be published for solution extendibility
 - ▶ EHLAPI scripts used for 3270 targets
 - ▶ Sample files provided

GSO Client Features

- ✓ **Both graphical and command line interfaces**
- ✓ **Integration with base OS security**
- ✓ **Configurable target logon options**
- ✓ **Displays status of logon/logoff/change pw processing**
- ✓ **Logon/logoff/change pw on selected targets**
- ✓ **GSO password strength checking**
- ✓ **Auditing**
- ✓ **Mobility across workstations within GSO environment**



GSO Administration Features

- ✓ **Add/Delete GSO users and administrators**
- ✓ **Reset GSO passwords**
- ✓ **Add/Delete/Modify user targets**
- ✓ **Enable/disable viewing administrative audit logs**
- ✓ **View GSO server error logs**
- ✓ **Set/modify secret keys used for generation of passtickets**



GSO Supported Systems & Targets

■ Client

- ▶ Microsoft Windows NT 4.0 Workstation
- ▶ OS/2 Warp 3.x (with Fix Pack 21 or higher) or OS/2 Warp 4.x

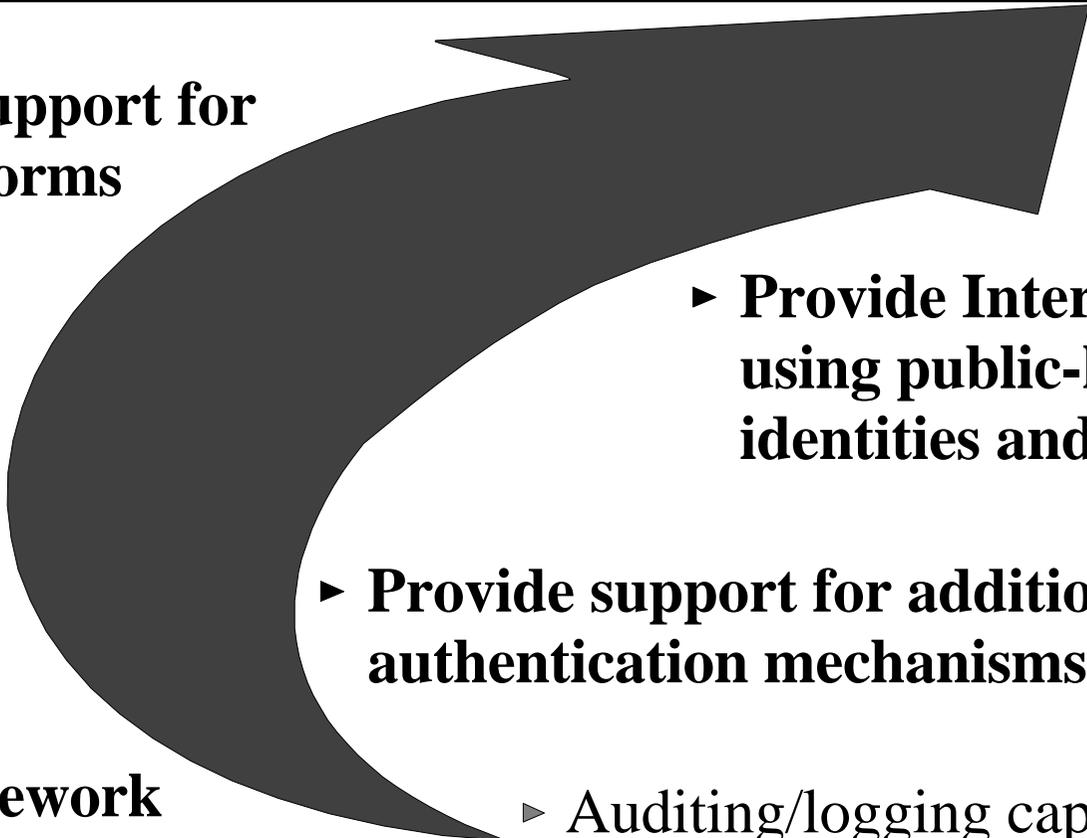
■ GSO Server

- ▶ IBM AIX 4.1.4+ or 4.2
- ▶ IBM Directory and Security Server AIX V4

■ Targets Supported

- ▶ 3270 Mainframe Applications
- ▶ OS/2 Lan Server
- ▶ OS/2 Warp Server
- ▶ Novell Netware 3.x and 4.x
- ▶ Windows NT 4.0 Server
- ▶ Databases (DB2/6000, Oracle, Sybase, Informix, MS SQL Server)
- ▶ DCE-based Applications

IBM Global Sign-On Directions

- 
- ▶ Enhance support for other platforms
 - ▶ Single point of administration for user management
 - ▶ Provide Internet support using public-key based identities and credentials
 - ▶ Provide support for additional authentication mechanisms

Build GSO Framework

- ▶ Based on open standards
- ▶ Use OSF DCE 1.1 security
- ▶ Provide "snap-in" I/F for customer and vendor apps.

- ▶ Auditing/logging capabilities
- ▶ Graphical User Interface
- ▶ Single sign-on based on user authorizations and user roles
- ▶ Single point of administration for password management

Summary

- **IBM's Global Sign-On is a GUI-based logon solution which coordinates user logins to DCE-based applications and non-DCE targets**
- **GSO improves productivity by reducing time required to complete logons, and manage passwords**
- **GSO provides an open, extendable and scalable framework for adding additional logon targets**
- **GSO improves security by eliminating exposures caused by common passwords and "sticky pads" with passwords**

Visit Our Website: www.networking.ibm.com/gso/gsohome.html