Mission Critical
Enterprise Systems
Symposium 2006

LOCKHEED MARTIN

Integrated Approach to User Account Management

Kesselman, Glenn and Smith, William

Lockheed Martin Mission Services
Quest Software Public Sector

October 17, 2007

Agenda

- Background
- Analysis of Options
- Requirements
- Considered Architectures
- Architecture Evaluation
- Architecture Conclusions
- Benefits
- Then What?
- Proof-of-Concept (POC)
- POC Conclusions
  - Implementation Strategy
  - Results to Date
  - Conclusion

Background

- Multiple Operating Systems
- Systems configurations which will remain unchanged until the Orbiter retirement
- Users with the same or different user accounts in different domains
- Migration from Network Information System (NIS) style domains to the Active Directory (AD) styled domains
- How to deal with groups privileges
  - Using a Lockheed Martin provided tool known as ‘become’
  - Using organizational units and personalities
  - How to roll out
    - » Roll out with new equipment
    - » Phase in on existing equipment
    - » Dealing with unchanged equipment

Analysis of Options

- **Was it feasible to provide one user ID management system ?**
  - **Yes, but…**
- **What options were considered ?**
  - **Reviewed Light Weight Directory Access Protocol (LDAP) vendor offerings and white papers**
  - **Reviewed LDAP newsgroups and blogs**
  - **Identified 5 candidate architectures**
  - **Industry current "best practices" said 2 architectures are consistent with industry approaches**
  - **Leverage our agreements with our vendors**
    - » Questions were posted to Microsoft, Red Hat, Sun, and Quest with respect to LDAP

Security Requirements

- **User Passwords:**
  - shall **be protected / secured when sent over a network**
  - shall **be protected / secured as stored on the LDAP server**
  - shall **be defined by the user (within guidelines and constraints)**
  - shall **have a minimum and a maximum age**
  - shall **be checked against a password history record to prevent password reuse**
  - shall **generate warnings when the password nears expiration**
  - shall **be checked for triviality and ensure minimum standards (defined) are met (minimum number of characters, types, etc.)**

- **Accounts** shall **be locked out with warning messages upon successive login failures.**

- **Other** *System Entry Applications* **(FTP, Telnet, rsh) will continue to use the existing applications password policies. A follow-on study should be conducted to mitigate application password policy risk acceptance**

What Were the Considered Architectures?

- Parallel Authentication Servers
  - **Both MS Windows and UNIX/Linux**
- Common Authentication Server
  - **Supports both MS Windows and UNIX/Linux from a common 'platform'**

Parallel Authentication Servers

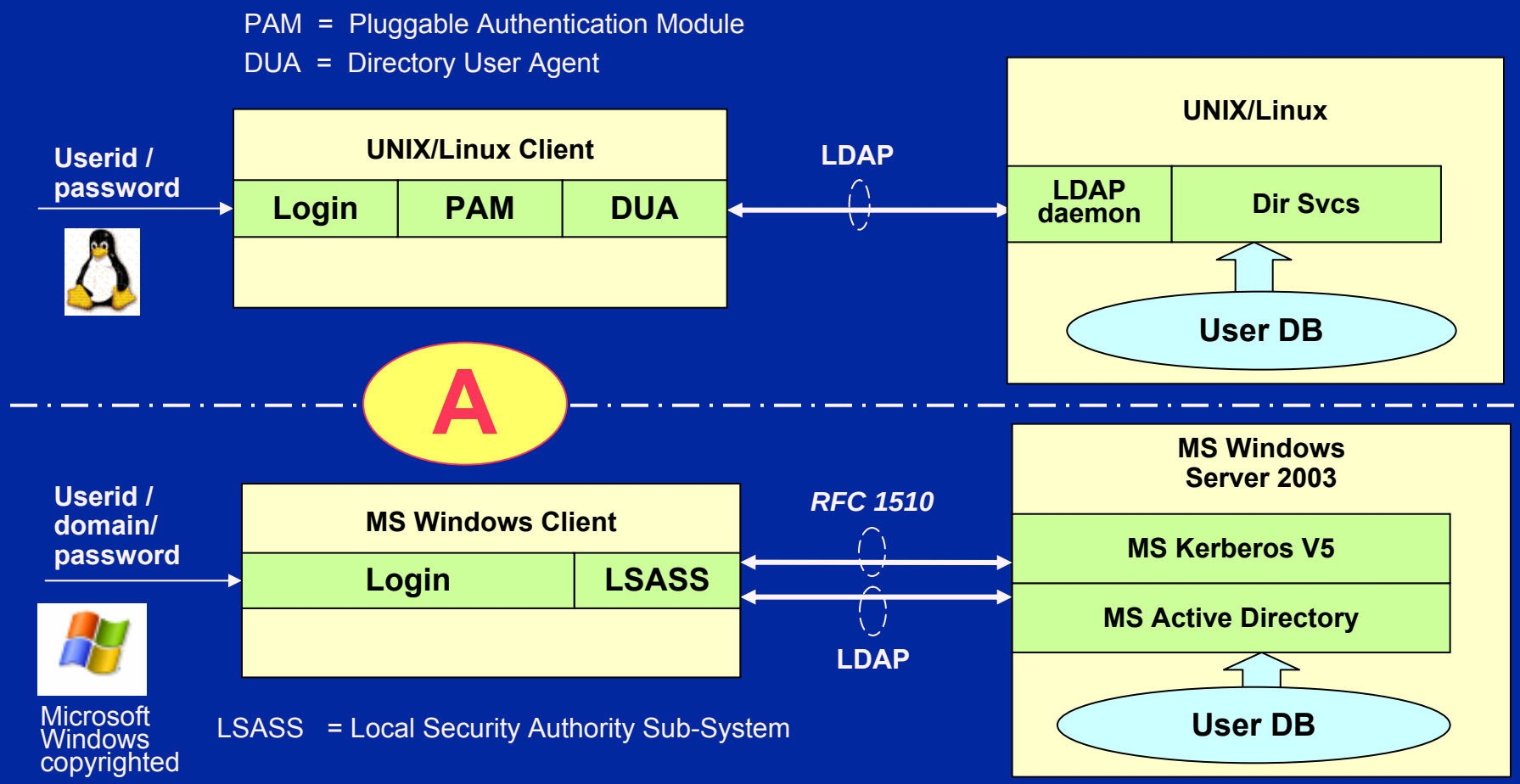
- Architecture A ▪ Separate Management
  - **UNIX/Linux clients authenticate with a UNIX/Linux LDAP server**
  - **Windows clients authenticate with a Windows 2003 server**
  - **Use the same user ID and password on the Windows and UNIX/Linux systems**

- Architecture B ▪ Synchronized
  - **Same as Separate Management, but the LDAP database on the Windows and UNIX/Linux servers are synchronized by external tools and processes**

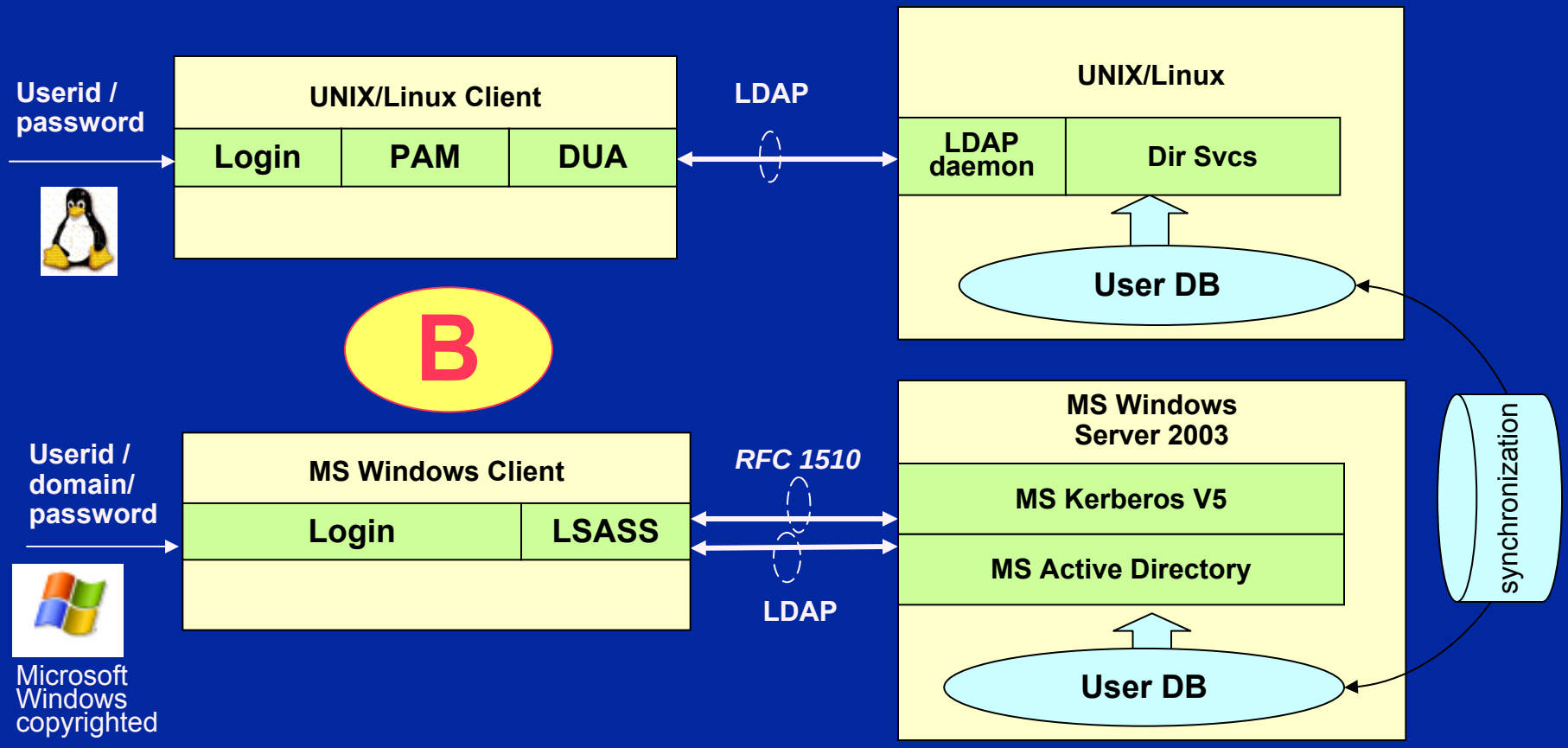
Common Authentication Server

- **Architecture C ▪** Windows AD server
  - **Serves both UNIX/Linux and Windows clients**
- **Architecture D ▪** UNIX/Linux LDAP server
  - **Serves both UNIX/Linux and Windows clients**
- **Architecture E ▪** Vintela + Windows AD server
  - **Serves both UNIX/Linux and Windows clients**
  - **Vintela option facilitates Kerberized authentication, simpler management, and strict password policy adherence**

Parallel Architecture A

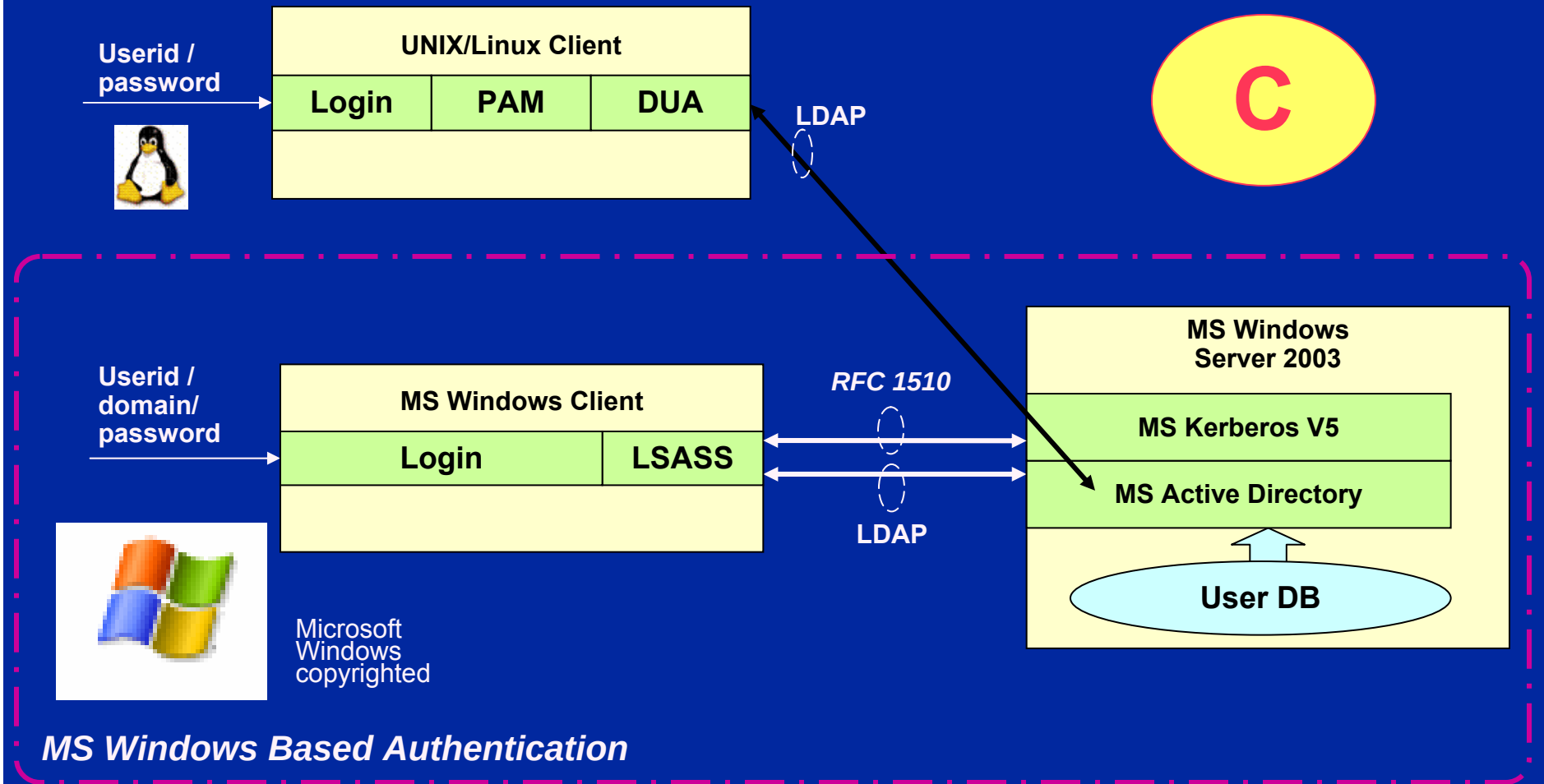


Parallel Architecture B

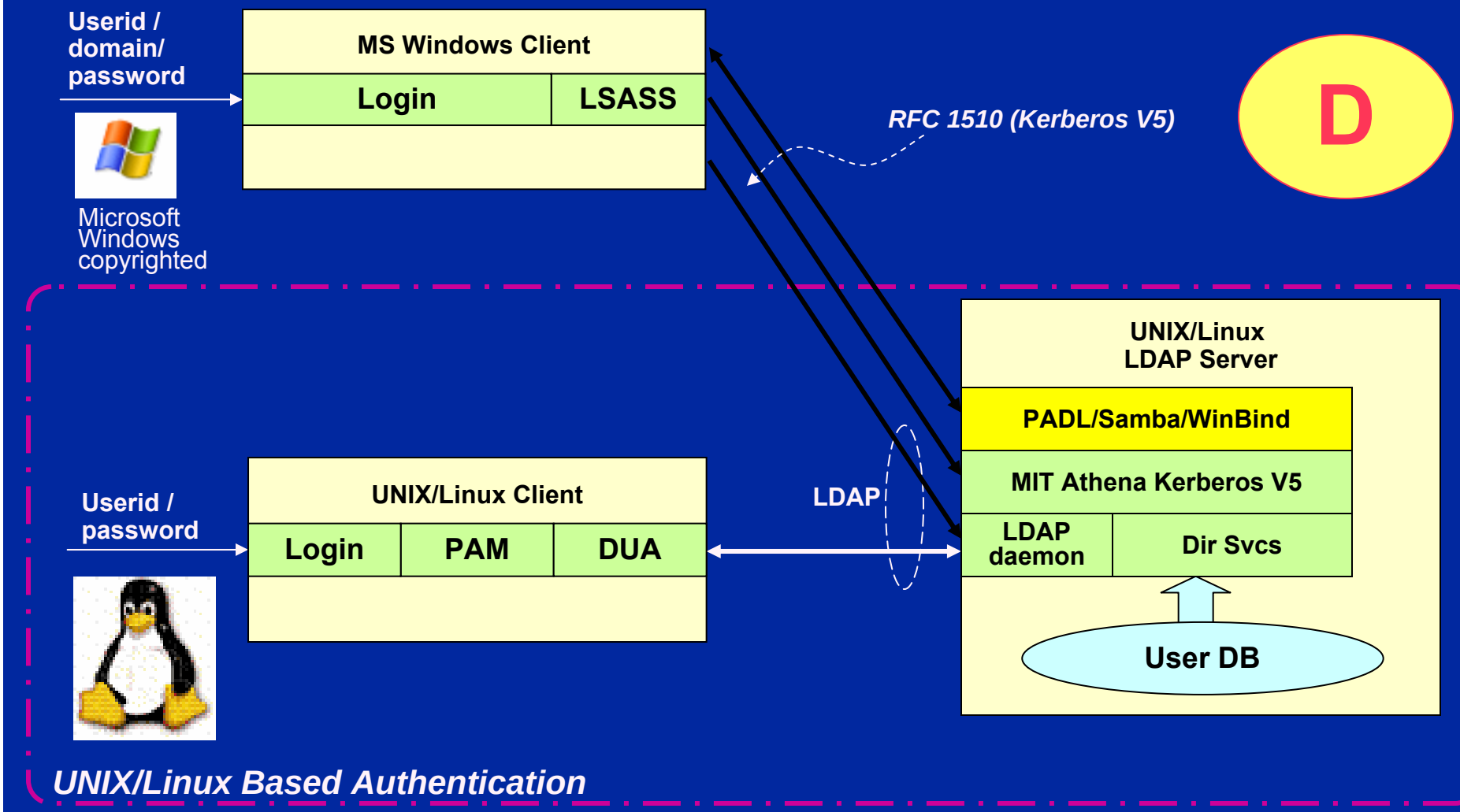


Common Architecture C

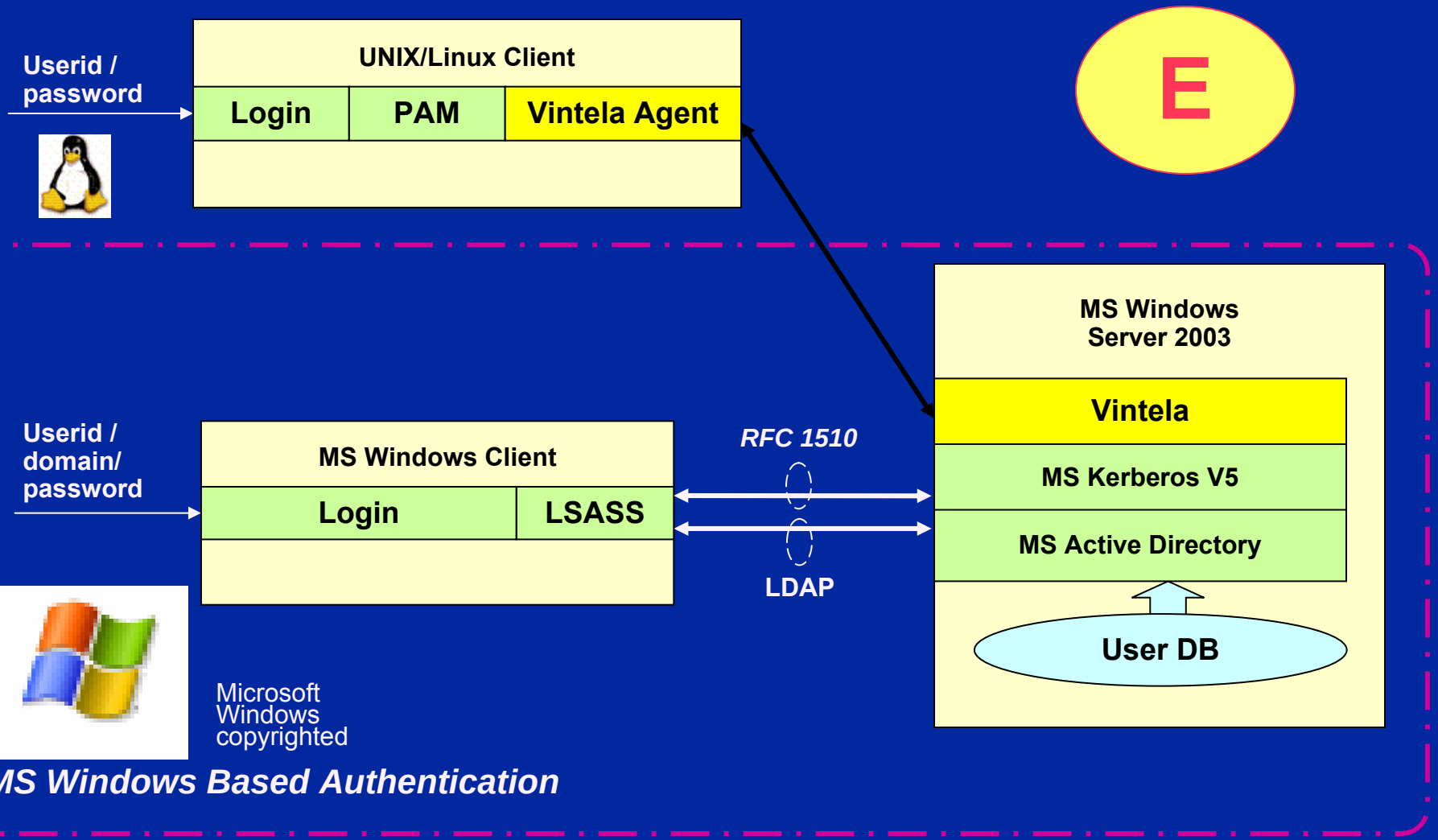
Windows LDAP Deployment Architecture



Common Architecture D
Linux LDAP Deployment Architecture



Common Architecture E
Windows LDAP Deployment Architecture



Candidate Architecture Evaluation Factors

- Highly Available
- Swingable (Ops to Test & back)
- Scalable
- Secure channel to protect authentication
- Supports customized login application
- Cross security level information exchange
- Password History & Aging
- Userid/Password database is secure
- User impacts
- GUI
- Legacy (non-compliant) Systems Support
- Product Support
- Custom Pluggable Authentication Module (PAM) development framework
- Administration tools are adequate
- Customizable
- System administration impacts
- Administration automation
- Interoperable
- Commercial-Off-The-Shelf COTS, COTS, COTS

Candidate Architecture Scorecard

Scorecard	A	B	C	D	E
Highly available		m			
Swingable	m	m	m	m	m
Scalable		m			
Secure Channel					
POS login support					
Cross Sec Level Info Exchange	m	m	m	m	m
Password History & Aging			m		
Userid/Password DB is secure					
User impact	m				
ACA interface					
Legacy systems support	m	m	m	m	m
Product Support	m	m	m	m	m
Custom PAM framework	m	m	m	m	m
Adequate Tools	m	m	m	m	m
Customizable					
Sysadmin impacts	m			X	
Automated admin					
Interoperable	N/A			X	
Estimated Engineering Effort			m	m	m

No Major Issues	
Issues With Mitigation	M
Issues Have No Mitigation	X

Architecture Conclusions

- Using a single userid/password can be accomplished for a single domain user (i.e. OPS only or Development only)
- LDAP implementation is feasible with at least 2 defined domains (Operations & Development/Verification)
- The existing NASA Mission Control Center Systems (MCCS) and subsystems will be supported as part of a planned equipment replacement / upgrade, remain 'as-is' until an equipment replacement occurs, or be migrated as part of an approved change direction
- Some existing subsystems can be supported with an upgrade
- The recommended architectures will meet the user password management requirements
- The candidate architecture D is not feasible and will not be pursued because the Linux LDAP server with samba and win bind cannot provide all the necessary services required by Windows

Benefits

- Users have 1 User Identity (ID) and fewer passwords for ALL of the MCCS and subsystems
- Password policy will be uniform and consistent across systems and subsystems
- Password change interval will be uniform based upon a NASA Johnson Space Center approved policy
- This is / was *NOT* Single Sign On (SSO)
  - Requesting access to another system or subsystem WILL require the user to provide their User ID and password
  - The candidate LDAP architectures do not preclude moving to SSO in the future

POC Scope

- Then What? DO Proof-Of-Concept (POC)
  - Validate security requirements
    → password syntax, management, expiration, history, etc.
  - Explore mixed architecture to ensure that a consolidated single product type LDAP server implementation is viable, or prove that the parallel candidate architecture deployment is required.
  - Install client and server systems, using existing resources to evaluate the possible architectures and products.

POC Scope

- Then What?
  - Facilitate identifying products for the common approach.
  - Identifying a common PAM configuration to support / authenticate MCCS systems.
  - Determine if a common schema will support all intended targets.
  - Verify that emulated environment swings are supported.
  - Identify administration tools to support LDAP environment.
  - Report results of POC actions.

POC Conclusions

Architecture "B" – Parallel LDAP Servers (A & B collapsed)

- » Uses Windows Active Directory (AD) for Windows/2000 and Windows/XP logon clients.
- » Uses Red Hat Directory Services (RDS) for Linux, Solaris and AIX logon clients.
- » RDS interfaces with AD keep the userid/password database in synchronization over a secure link.

Architecture "E" – Shared LDAP Server (C a variant of E, D infeasible)

- » Uses Windows Active Directory (AD) for Windows/2000 and Windows/XP logon clients.
- » Linux/Unix Clients use the Vintela add-on package to authenticate using Active Directory.
- » No synchronization is required – common Windows LDAP server provides one userid/password database.

POC Conclusions

With Architecture "B", we found RDS + AD, w/sync:

- » Did not support the custom operations satisfactorily;
- » Password strength lies in the individual client PAM's and can *vary* based on host type;
- » Installation of the client PAM was not straightforward, but rather error prone;
- » Some of the user logon messages are missing or very brief in duration.

With Architecture "E", we found Vintela + AD:

- » Was simple to install using Red Hat style RPM's;
- » Provides the messages needed during login processing;
- » Password policy was uniformly implemented by the Windows AD server;
- » Performed well during custom operations.
- » Most COTS oriented solution

POC Conclusions

- **Bottom Line:**

- **Implement Architecture E**

POC Conclusions

- **Implementation strategy**
  - **Infrastructure is installed first, then subsystems are brought in according to outside schedule factors**
  - **Common Userid Phase I: Development Systems and Subsystems**
    - » Install new AD cluster and migrate Windows 2000/XP clients first
    - » Verify custom login on Linux workstations
    - » Migrate Linux/Unix clients next
    - » Support LDAP testing with early adopters
  - **Common Userid Phase II: Operations Systems and Subsystems**
    - » Repeat installation pattern from the Development Systems domain
    - » Support LDAP authentication in equipment replacement devices (Linux workstations and servers)
    - » Implement Windows devices (current and new)
    - » Implement on Unix clients and servers

Results to date

- **All of the Development Domain's workstations and servers are converted to using the LDAP services based upon the Vintela agents**
  - **Caveat:**
    - » Some of the systems in the Development and Operations domain do not support PAM and therefore are still managed separately.
    - » Root is managed locally (at the workstation or server).
- **Some of the Operations Domain's workstations and servers are converted to using the LDAP services**
  - **Caveat:**
    - » Some of the systems in the Operations domain do not support PAM and therefore are still managed separately
    - » Root is managed locally (at the workstation or server)
    - » Roll-out to the Operations Domain systems and subsystems are being achieved incrementally with equipment replacements or retrofits

Conclusion

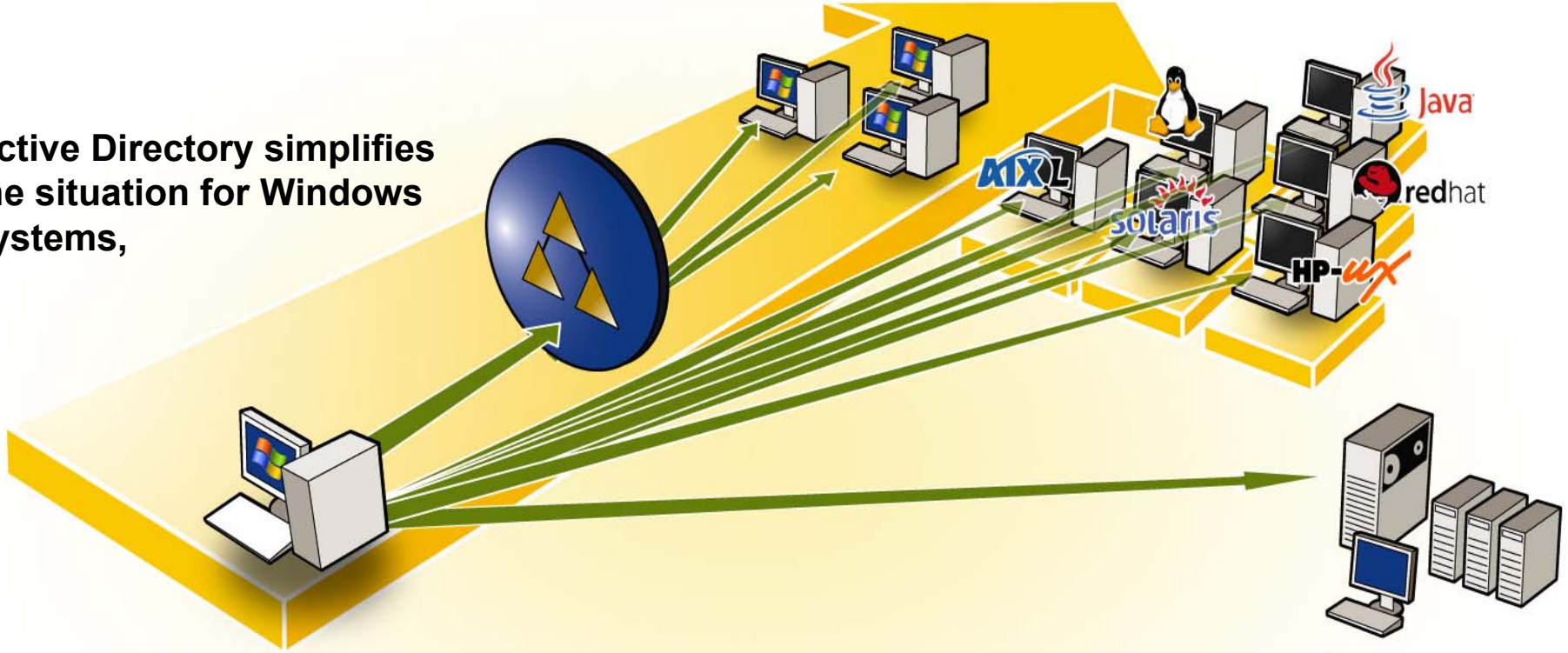
- The implementation proceeds well with little problems.
- Quest has been instrumental in the successful implementation and problem resolution.
  - Problems were resolved at site in some instances with fixes being made in hours or days during the initial testing and roll out to the Development Domain
- For those systems that are being converted from a NIS based service to a PAM based service, develop a password testing system that user's can 'try-it' before the 'use-it'
- Educate the user about this service and why it is important

Conclusion

- **Rolling out a 'one-size-fits-all' solution will be difficult, because the size will change**
  - **For example: If implementation of LDAP services with application authentication is required, then try that first before having the users change to the system.**
  - **Test the systems with many 'high-fidelity' users as possible**
    - » If you have 'vocal' users, get them to be some of those testers and hopefully advocates.
- **We did not advertise this as a 'single sign-on' solution**
- **We did not advertise this as a panacea, just a step forward**

Diverse Systems & Directories

Active Directory simplifies the situation for Windows systems,

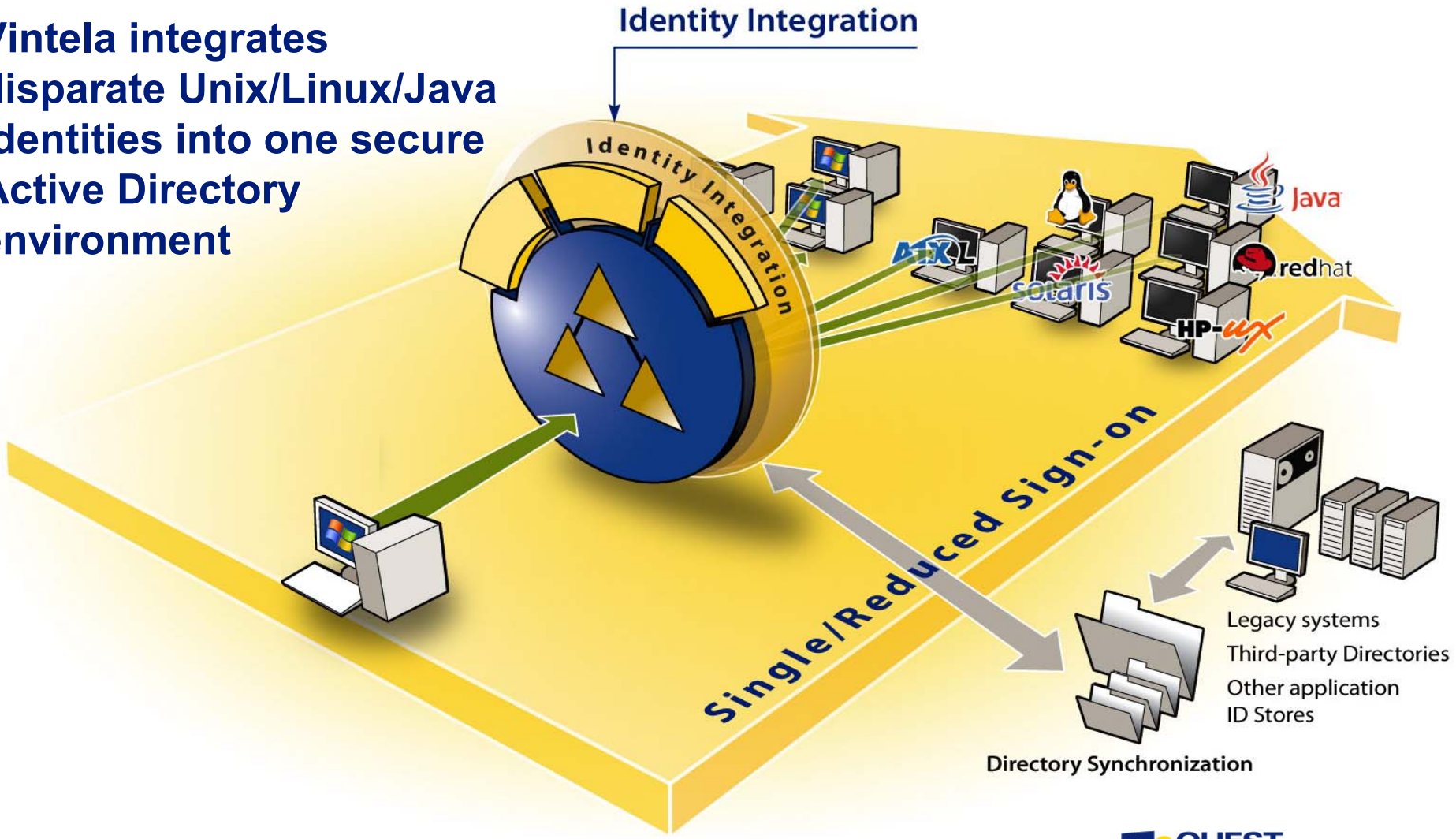


but for non-Windows systems, directories and authentication must all be managed separately

- **Multiple directories**
- **Multiple identities**
  - **Multiple logins**
  - **Not secure**

Vintela Authentication Services

Vintela integrates disparate Unix/Linux/Java identities into one secure Active Directory environment



QUEST SOFTWARE

Presentation MetaData

Metadata Name	Metadata Content
Abstract Number	ABS-1559
Subject	Integrated Approach to User Account Management
Additional Contributors Enter the names of people, besides the listed presenter/author, who contributed to the content	Smith, William
Keywords Enter additional keywords to supplement search	MCES 2007, Identity Management, Account Management
Legend In accordance with CPS-710	Leave blank or use a legend as specified in CPS-710 - http://policy.global.lmco.com/p3/lockmart/cps/legal/cps-710.html
Coverage	Case Studies
Audience	All Attendees
Track	Enabling Infrastructure Agility
Abstract	IT environments consist of both Windows and other platforms. Providing user account management for this model has become increasingly difficult. If Microsoft's Active Directory could be enhanced to extend a Windows identity for authentication services for Unix, Linux, Java and Macintosh systems, then an integrated approach to user account management could be realized.