

nexortend

Enabling LDAP Directories in the Federal Bridge

Ed Harrington 14 November 2002



In a word NEXOR

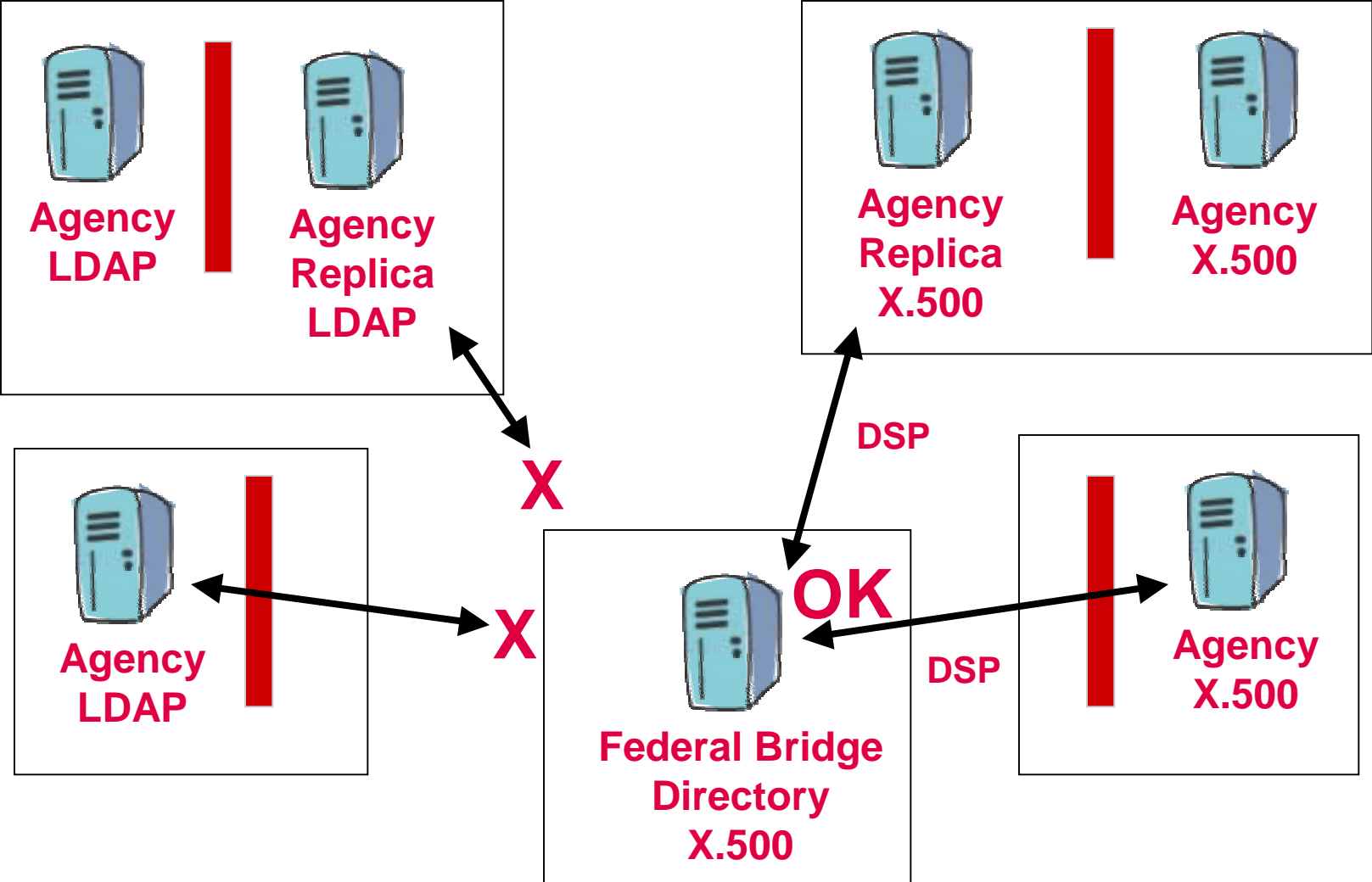
Agenda

- The Problem
- Potential Solution
 - Nexor LDAP \leftrightarrow DSP Gateway
 - » At the Agency/Organization
 - » With MaXware at the Federal Bridge
- Conclusions and Recommendations
- Questions

The Problem

- The Federal Bridge Directory is X.500
- Not all Agencies/Organizations want to/will Stand-up a DSP capable Directory (X.500)
- BUT...most already have LDAP version 3 Directories
- How to perform Certificate Path Validation without DSP and include non-X.500 Agencies and Organizations
- (LDAP referrals can work but the onus is then placed at the agency clients – or proxies – and can open up firewall penetration questions)

The Problem: Including LDAP

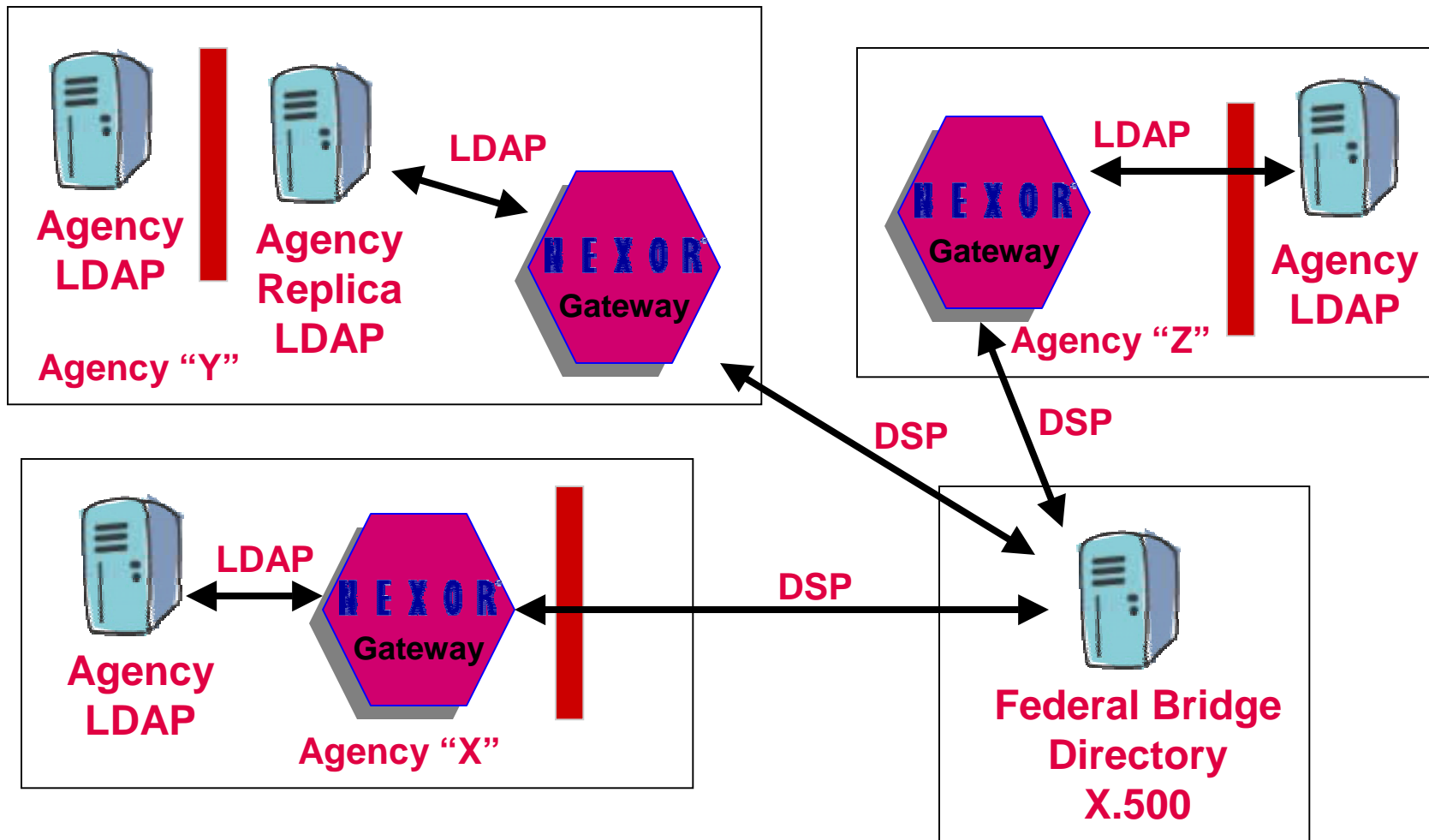


Potential Solution

- Nexor LDAP ↔ DSP Gateway
 - Bi-directional protocol conversion gateway
 - Supports X.500 DSP (1993) (and DAP also)
 - Supports LDAP version 3
 - LDAP Initiation Support
 - » LDAP Server → LDAP → Gateway → DSP → X.500 Server
 - » X.500 Server → DSP → Gateway → LDAP → LDAP Server
 - Current Limitation: Only ONE Configurable connection at a time is supported

(Following assumes all is OK with X.500 to X.500 DSP connections)

Potential Solution: At the Agency/Organization



Potential Solution: At the Agency/Organization

■ Pro:

- Agency/Organization Control

■ Con:

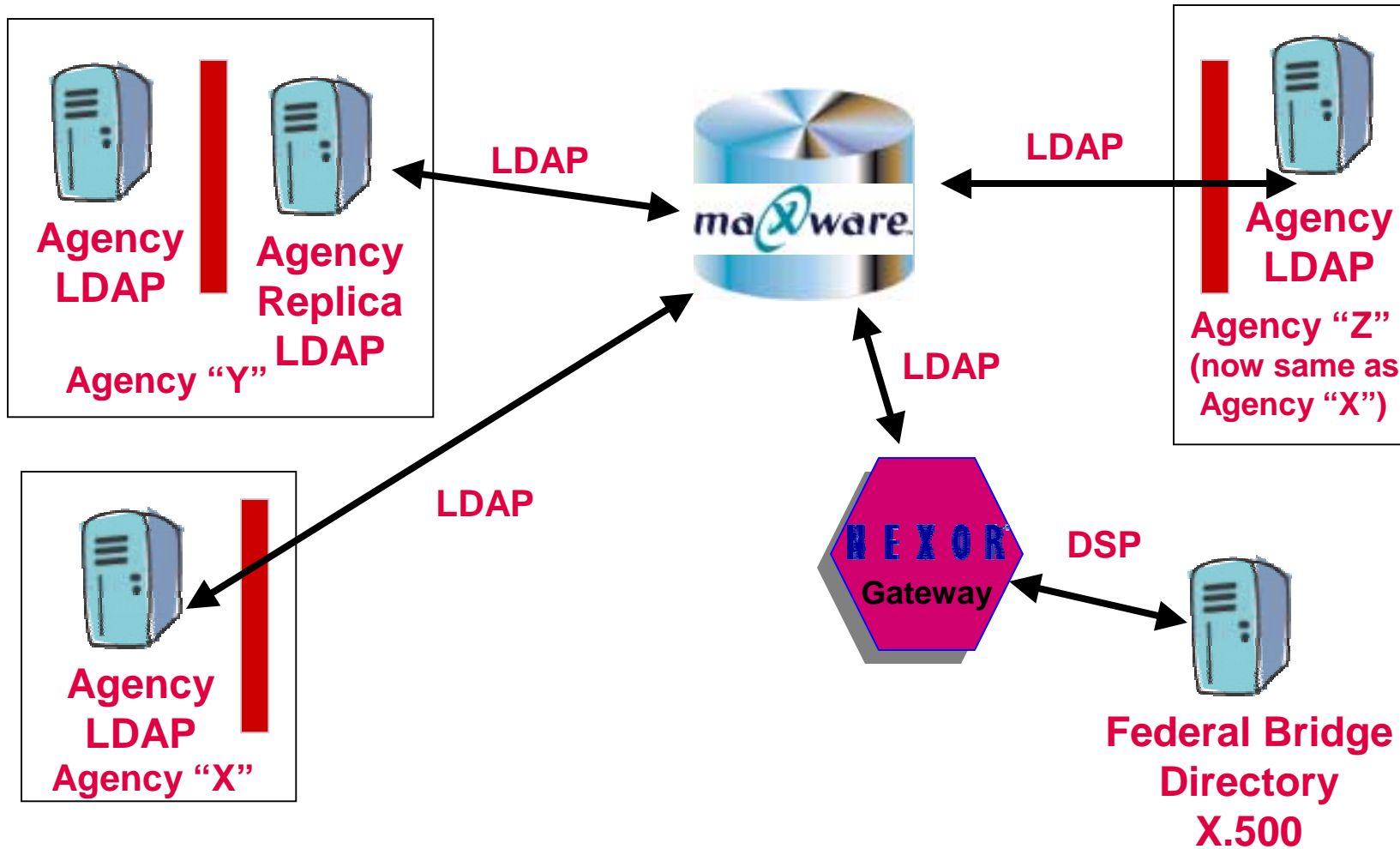
- Onus on the Agency/Organization
- Proliferation of Solutions
- Deterrent to Implementation
 - » Cost
 - » Installation
 - » Testing
 - » Maintenance
 - » Support
 - » Upgrades

- Much more to Deter an Agency/Organization from Participating in the Benefits of the Bridge CA

Potential Solution: At the Federal Bridge

- A Centralized Solution appears to be a better approach
- But the Gateway only supports ONE configurable connection...
- Mitre has Recognized the Better Solution is to Add a Virtual Directory to provide for the many LDAP connections that will eventually be required
- MaXware and Nexor Team to provide the complete Bridge-Based Solution

Potential Solution: At the Agency/Organization



Conclusion and Recommendation

■ Current Status:

- In Test with Mitretek
- Problematic DSP between Gateway and Current Bridge X.500 Directory...with workaround:
 - » LDAP ↔ Gateway ↔ DSP ↔ Nexor Directory ↔ DSP ↔ Bridge Directory

■ Conclusion:

- Centralized MaXware/Nexor Solution takes the onus off the Agencies and Organizations

■ Recommendation:

- Implement the Proposed Solution at the Bridge to enlarge the potential participant population immediately!

■ Future-proof the Bridge: Other protocols (i.e., DSML) can be added as needed...

QUESTIONS???

Contact Information:

NEXOR®

Ed Harrington
Business & Technical
ed.harrington@nexor.com
Office: +1.757.259.7438
Mobile: +1.757.342.4552

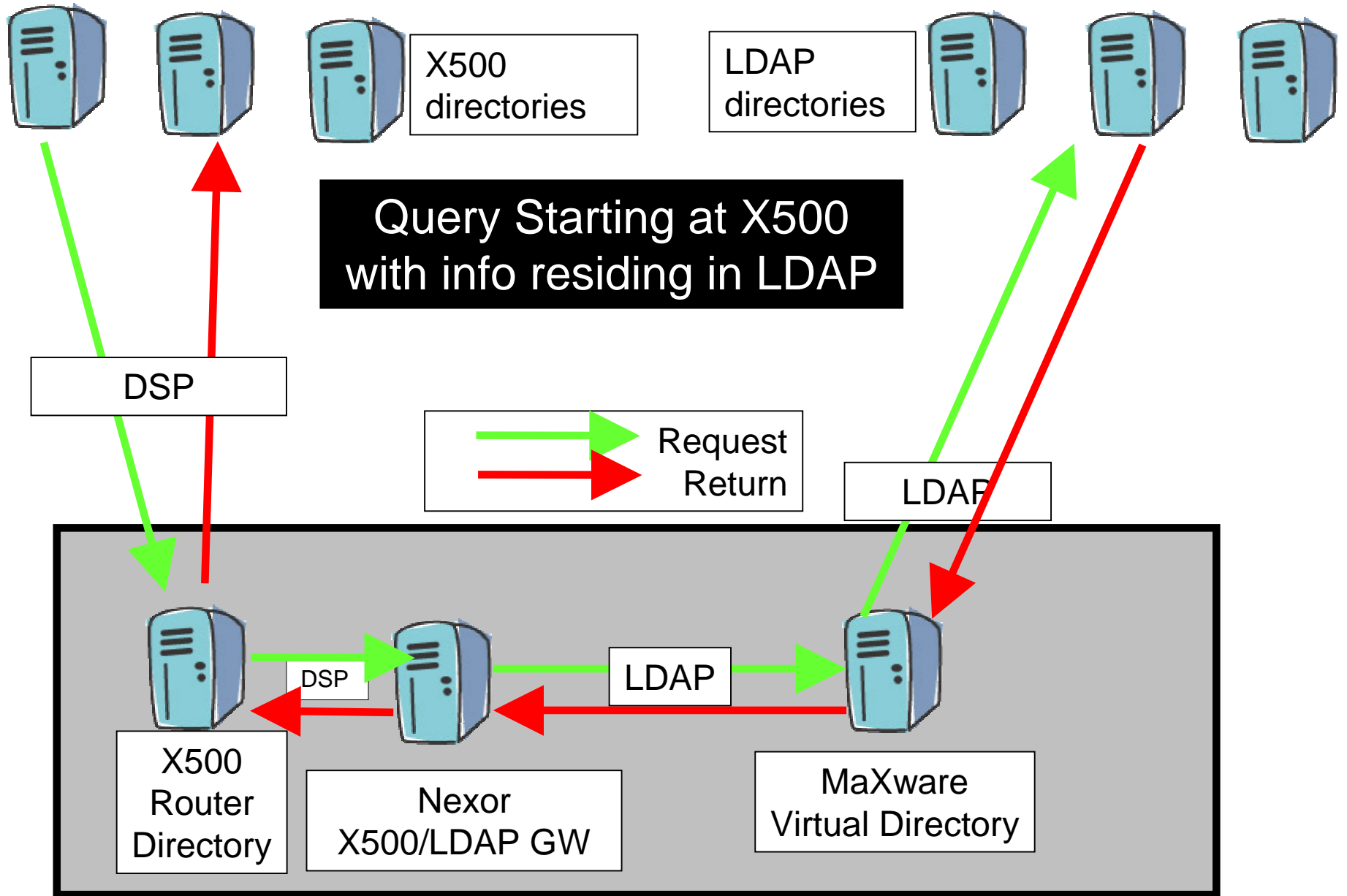
Contact Information:

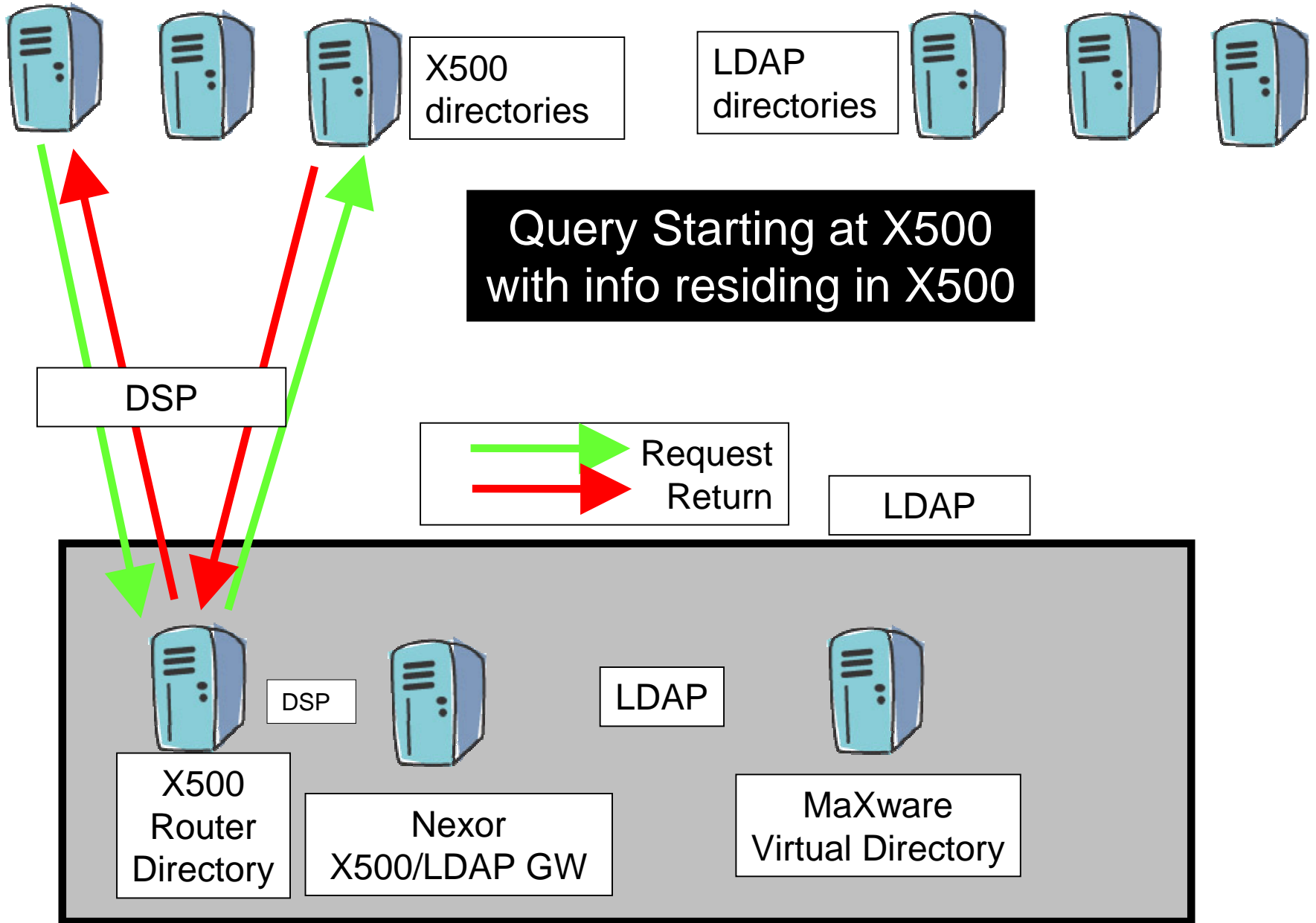
maxware™

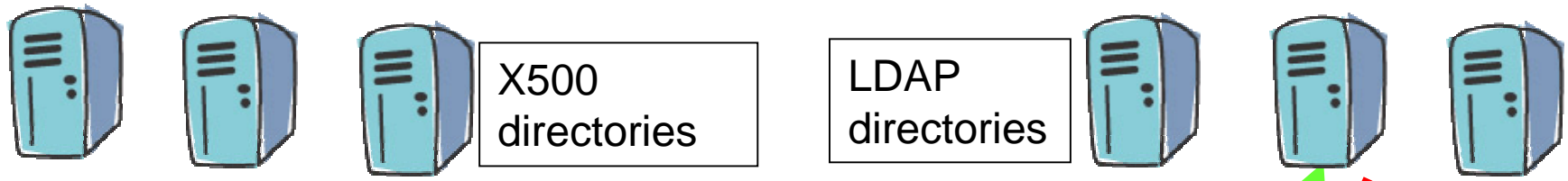
Elliott Friedman –
Sales/Management
elliott.friedman@maxware.com
(732) 409 5000 x108

Chris Krabsetsve – Senior
Technical Contact
perck@maxware.com
(732) 409 5000 x105

In a word NEXOR®

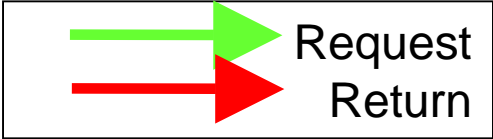






Query Starting in LDAP
with info residing in
LDAP

DSP



LDAP

