BT and Federation

Robert Temple
Vice President, Security Technologies
Group CTO’s Office
Agenda

• Why Federation?
• Federation Infrastructure
• Our Experience
• Trust Model
• Next Steps
• Federation Are We Ready
Why Federation – Business Challenge

• Improve Security for existing partnerships
  – 60,000 partner IDs
  – 2,000+ existing partnerships

• Launching new products based on partnerships

• Extension of Web Access Management Security
What We Deployed

- “Common Federation Gateway” based on CA SiteMinder Federation Security Services
- For In Bound
  - Java extensions to call provisioning processes
- For Out Bound
  - Used existing provisioning process
Federation Infrastructure

- CA SiteMinder 5.5 and CA SiteMinder 6.0
- 36,000,000+ transactions per day
- 150,000 employees, partners
- 8,000,000 online customers (20,000,000 potential)
Federated Partners now have access to

- Peoplesoft
- Siebel
- Oracle Applications (Financials)
- Citrix (NFuse / Web Access)
- XML Gateway
- Voice Verification (Persay)
What We Deployed

- Web Proxies
- App Server
- Federation Gateway
- Policy Servers
- Provisioning Service
- Employees & 3rd Parties
- LDAP (AD)
Benefits Achieved

• Managed User Identity as a Common Capability
  – Separation of Authentication and Authorisation from application logic
• Legacy Authentication Services (e.g. RADIUS) retired
• Consolidation of user stores and user accounts
• Reduction in FTE dealing with 3rd party access
Our Experience – Causes of Pain

• Supported SAML Version with Partners
• Legal contracts
  – Trust
  – Liability
  – Point to Point
• Integration of PKI
• Hand-holding!
Trust Model – Existing Standards

- SAML AuthnContext
- RFCs 3280 and 3647
- WS-Trust
- NIST 800-63
- Liberty Alliance Identity Assurance Framework
Progress of Federation Trust Models?

Stage 1 – Scattered clusters
Stage 2 – Single Hub & Spoke

Stage 3 – Multi Hubbed small world

Stage 4 – Meshed multi hubbed

X - we are struggling with issues here
Next Steps

- Federate Guidelines
  - Ultimately publish via UDDI?
- Federate with more partners
- Introduce use of roles
- Federation toolkit
  - Licensed
  - Open source
- “Standard” federation agreement
- Exposing Services Securely to Partners
- More work needed by the community
Questions & Answers

Bringing it all together

© copyright of British Telecommunications plc 2008