1. Record Nr. UNINA9910964474003321

Autore	Bucker Axel
Titolo	Federated identity management and web services security with IBM tivoli security solutions / / Axel Buecker et al
Pubbl/distr/stampa	San Jose, CA, : IBM, International Technical Support Organization, 2005
Descrizione fisica	xx, 478 p. : ill
Collana	Redbooks
Altri autori (Persone)	FilipWerner HintonHeather HippensteilHeinz Peter HollinMark NeucomRay WeedenShane WestmanJohan
Soggetti	IBM software Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"October 2005." "SG24-6394-01."
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front cover -- Contents -- Notices -- Trademarks -- Preface -- The team that wrote this redbook -- Become a published author -- Comments welcome -- Part 1 Architecture and design -- Chapter 1. Business context for identity federation -- 1.1 Federated identity -- 1.2 Business environment -- 1.2.1 Deconstruction of the enterprise -- 1.2.2 Enterprise re-aggregation -- 1.2.3 High-level example of a re-aggregated business -- 1.2.4 Business models for federated identity -- 1.2.5 The relationship - Trust and assurance -- 1.3 IT environment -- 1.3.1 The role of identity management -- 1.3.2 Dealing with identities -- 1.3.3 User life cycle management -- 1.3.4 Inter-enterprise application to application integration -- 1.3.5 Open standards -- 1.4 Conclusion -- Chapter 2. Architecting an identity federation -- 2.1 Federation example -- 2.2 Federated identity management architecture -- 2.2.1 Background to federation -- 2.2.2 Architecture overview -- 2.2.3 Roles -- 2.2.4 Identity models -- 2.2.5 Identity attributes --

2.2.6 Trust -- 2.2.7 Federation protocol -- 2.3 FIM standards and efforts -- 2.3.1 SSL/TSL -- 2.3.2 Security Assertion Markup Language (SAML) -- 2.3.3 Shibboleth -- 2.3.4 Liberty -- 2.3.5 WS-Federation -- 2.3.6 WS-Trust -- 2.3.7 WS-Security -- 2.3.8 WS-Provisioning -- 2.3.9 Selecting Federation standards -- 2.4 Federated single sign-on -- 2.4.1 Push and Pull SSO -- 2.4.2 Account linking -- 2.4.3 Where are you from (WAYF) -- 2.4.4 Session management and access rights -- 2.4.5 Logout -- 2.4.6 Credentials clean up -- 2.4.7 Global good-bye -- 2.4.8 Account de-linking -- 2.5 Web services security management -- 2.5.1 Web services -- 2.5.2 Web services security -- 2.5.3 Gateways -- 2.6 Federated identity provisioning -- 2.7 On demand security reference architecture -- 2.7.1 Policy management -- 2.7.2 Identity management -- 2.7.3 Key management.
2.7.4 Credential exchange -- 2.7.5 Identity federation -- 2.7.6 Authorization -- 2.8 On demand integration reference architecture -- 2.8.1 Connectivity services -- 2.8.2 User interaction services -- 2.8.3 Application and information assets -- 2.8.4 Business application services -- 2.8.5 Partner services -- 2.8.6 Infrastructure services -- 2.9 Method for architecting secure solution -- 2.9.1 Implementation flow -- 2.9.2 Definition phase of a federated identity management solution -- 2.10 Conclusion -- Chapter 3. Tivoli Federated Identity Manager architecture -- 3.1 Federated Identity Management functionality -- 3.2 Federation services -- 3.2.1 Point of contact (PoC) -- 3.2.2 Single sign-on protocol services (SPS) -- 3.2.3 Trust services -- 3.2.4 Key services (KESS) -- 3.2.5 Identity services -- 3.2.6 Authorization services -- 3.2.7 Provisioning services -- 3.2.8 Management Services -- 3.3 Federated single sign-on -- 3.3.1 Architecture overview -- 3.3.2 Trust in F-SSO -- 3.3.3 F-SSO protocol functionality -- 3.3.4 Integrating SSO with Access Manager for e-business -- 3.3.5 F-SSO approaches -- 3.3.6 InfoService -- 3.3.7 Specified level view of F-SSO architecture -- 3.4 Web services security management -- 3.4.1 Architecture overview -- 3.4.2 WS-Security -- 3.4.3 Web services Gateway or Firewall -- 3.4.4 WS-Trust -- 3.4.5 Authorization services (AS) -- 3.4.6 Web services security management architecture approach -- 3.5 Provisioning services -- 3.5.1 Architecture overview -- 3.5.2 Provisioning architecture approach -- 3.6 Conclusion -- Chapter 4. Deploying Tivoli Federated Identity Manager -- 4.1 Federated SSO architecture patterns -- 4.1.1 Architecture approach -- 4.1.2 Base pattern -- 4.1.3 Plug-in pattern -- 4.1.4 Lightweight Access Manager for e-business pattern -- 4.1.5 Highly available architecture patterns -- 4.1.6 Multiple data center patterns.
4.2 Federated Web services architecture patterns -- 4.2.1 Architecture approach -- 4.2.2 Point-to-point pattern -- 4.2.3 XML gateway pattern -- 4.3 Integrating applications into an F-SSO environment -- 4.3.1 Attribute flow between providers -- 4.3.2 User-controlled federated life cycle management -- 4.3.3 Customized user-managed federation management -- 4.4 Customizing F-SSO -- 4.4.1 Customizing page templates -- 4.4.2 Customizing Access Manager for e-business page templates -- 4.4.3 Storing aliases -- 4.5 Solution design considerations -- 4.5.1 Exchanging metadata with your partners -- 4.5.2 Availability of IBM Access Manager for e-business policy server -- 4.5.3 Key management -- 4.5.4 Session timeout -- 4.5.5 Application logout -- 4.6 Conclusion -- Chapter 5. Integrating with IBM identity management offerings -- 5.1 IBM Tivoli Access Manager for e-business -- 5.1.1 Identity provider integration -- 5.1.2 Service provider integration -- 5.2 IBM Tivoli Identity Manager -- 5.2.1 Identity provider integration -- 5.2.2 Service provider integration -- 5.3 IBM Tivoli Directory Integrator -- 5.3.1 Identity provider integration -- 5.3.2

Service provider integration -- 5.4 IBM Tivoli Directory Server -- 5.4.1 Identity provider integration -- 5.4.2 Service provider integration -- 5.5 IBM WebSphere Application Server -- 5.5.1 Integrated Solutions Console (ISC) -- Part 2 Customer environment -- Chapter 6. Overview -- 6.1 Use case 1 - SAML/JITP -- 6.2 Use case 2 - WS-Federation -- 6.3 Use case 3 - Liberty -- 6.4 Use case 4 - Web services security management -- 6.5 Conclusions -- Chapter 7. Use case 1 - SAML/JITP -- 7.1 Scenario details -- 7.1.1 Contract -- 7.1.2 User experience -- 7.2 Functionality -- 7.2.1 Single sign-on - SPNEGO -- 7.2.2 Single sign-on - SAML/JITP -- 7.3 Partners involved -- 7.3.1 BigCorp -- 7.3.2 RBTravel -- 7.4 Interaction description.
7.4.1 High-level Interaction overview -- 7.4.2 Single sign-on from Windows workstation (SPNEGO) -- 7.4.3 Single sign-on from BigCorp to RBTravel (SAML/JITP) -- 7.5 Configuration data -- 7.5.1 IdP-related configuration data -- 7.5.2 SP-related configuration data at RBTravel -- 7.6 Assumptions/implementation notes -- Chapter 8. Use case 2 - WS-Federation -- 8.1 Scenario details -- 8.2 Contract -- 8.3 User experience -- 8.3.1 Single sign-on user experience -- 8.3.2 Sign-off user experience -- 8.4 Functionality -- 8.4.1 Single sign-on - WS-Federation -- 8.5 Partners involved -- 8.5.1 BigCorp -- 8.5.2 RBTelco -- 8.6 Interaction description -- 8.7 Configuration data -- 8.7.1 Identity provider configuration at BigCorp -- 8.7.2 Service provider configuration at RBTelco -- 8.8 Assumptions/implementation notes -- 8.8.1 Understanding the many-to-one user identity mapping -- Chapter 9. Use case 3 - Liberty -- 9.1 Scenario details -- 9.1.1 Contract -- 9.1.2 User experience -- 9.2 Functionality -- 9.3 Partners involved -- 9.3.1 RBTelco -- 9.3.2 RBTickets -- 9.3.3 RBBanking -- 9.4 Interaction description -- 9.4.1 Liberty account federation -- 9.4.2 Single sign-on to partners (Liberty) -- 9.4.3 Single sign-off -- 9.5 Configuration data -- 9.5.1 Identity provider configuration at RBTelco -- 9.5.2 RBTickets service provider configuration data -- 9.5.3 RBBanking service provider configuration data -- 9.6 Assumptions/implementation notes -- 9.6.1 InfoService integration -- 9.6.2 Page customizations -- Chapter 10. Use case 4 - Web services security management -- 10.1 Scenario details -- 10.1.1 Contract -- 10.1.2 User experience -- 10.2 Functionality -- 10.2.1 Web services security management at RBTelco -- 10.2.2 Web services security management at RBStocks -- 10.3 Partners involved -- 10.3.1 RBTelco -- 10.3.2 RBStocks -- 10.4 Interaction description.
10.4.1 Web services security management Token Generator with Access Manager binary security token callback handler -- 10.4.2 Web services security management Token Consumer with Access Manager Credential login module -- 10.4.3 Web services security management Token Generator with Web services security management Callback handler -- 10.4.4 Web services security management Token Consumer with SAML Assertion login module -- 10.5 Configuration data -- 10.5.1 Overall architecture and prerequisites -- 10.5.2 RBTelco configuration -- 10.5.3 Outbound Web services gateway configuration -- 10.5.4 RBStocks configuration -- 10.6 Troubleshooting -- 10.6.1 Using the logs for Web services security management -- 10.6.2 Using the logs for the Secure Token Service -- 10.6.3 Using the WebSphere logs -- 10.6.4 Using TCPMON -- Part 3 Appendixes -- Appendix A. Configuring Access Manager WebSEAL and Web plug-in -- Introduction -- Identity provider integration -- Configuring WebSEAL as an identity provider -- Updating WebSEAL configuration file -- Configuring a junction to Tivoli Federated Identity Manager -- Configuring extended attributes for credentials in WebSEAL -- Configuring Web plug-ins as an identity provider -- Updating Web plug-in configuration file -- Configuring

extended attributes for credentials in Web plug-ins -- Service provider integration -- External Authentication Interface -- Trigger URIs -- EAI headers -- External Authentication Interface example -- EAI header variables reference -- Configuring WebSEAL as a service provider -- Updating WebSEAL configuration file -- Configuring a junction to Tivoli Federated Identity Manager -- Access Manager policy for trigger URLs for EAI -- Sending extended attributes as HTTP headers with WebSEAL -- Configuring Web plug-ins as a service provider -- Updating Web plug-in configuration file.
Access Manager policy for trigger URLs.