

101 Things to Know About Single Sign On

IDENTITY:

1. Single sign on requires authoritative sources for identity.
2. Identity authoritative sources needs to contain all the enterprise identity data required.
3. Authoritative identity sources need up to date provisioning processes.
4. Provisioning processes need to be integrated with good business processes.
5. When a user is hired, the provisioning process should aim to provide system and application access in the same day.
6. When a user's role is modified, the provisioning process's goal should be to make the change during the same day.
7. When a user is terminated, the provisioning process's goal should be to effect terminate the user from all networks, systems and applications on the same day.
8. Each identity authoritative source should be linked to the enterprise LDAP directory.
9. Synchronizing the changes in the identity authoritative source and the enterprise directory should be within minutes and at worst case, at the end of the day.
10. Authoritative identity sources, which are databases, may be quickly linked to the enterprise LDAP by using a virtual LDAP directory.
11. Virtual directories can also be used to synchronize different enterprise LDAP directories.
12. A global unique enterprise identifier is required for each user.
13. The global enterprise uid needs to be mapped to each application.
14. Don't be fooled by SSO vendors who claim that you can have single sign on in a matter of hours by installing their network hardware SSO appliances. While you can be operational, the quality of the underlying identity data is the bedrock of your enterprise. If it's poor, then your SSO system, while performing wonderfully, will also be poor from a security perspective.
15. Create a enterprise identity data governing body. This is important to regulate changes made by the authoritative sources to the identity data which single sign on and other enterprise applications will use.

RISK:

16. You need to do an enterprise risk analysis for each application.
17. You also need to do an enterprise risk analysis for each network.
18. You also need to do an enterprise risk analysis for each device being used to access the enterprise i.e. workstation, PDA, cell phone, laptop, etc.
19. You then need to construct an enterprise risk chart identifying areas where stronger identity authentication is required.

101 THINGS TO KNOW ABOUT SINGLE SIGN ON

IDENTIFICATION REGISTRATION:

20. Determine how the different identity types are currently registered.
21. Examine the systems of record used to vouch for an identity e.g. driver's license, SSN, passport, etc.
22. Determine if any identity background checks are required and if so, for what type of identity e.g. employee, contractor, consultant, temp, customer, etc.
23. Take your existing identity registration, now compare it to the enterprise risk analysis.
24. What areas are weak in terms of validating the identity before they are accepted and entered into your systems?

AUTHENTICATION STRENGTH:

25. Determine the number of applications and networks that currently require uid and password.
26. Determine the number of help desk calls, per day, pertaining to passwords and password resets.
27. Determine the average cost per help desk call.
28. Determine the number of help desk employees currently managing passwords and their total costs.
29. Read the paper, "Why your use of id's and passwords are likely a joke".
30. Understand why inputting uid and passwords via a keyboard is extremely high risk.
31. Research the use of keyboardless authentication from companies like Bharosa and RSA.
32. Determine if you can begin applying keyboardless authentication to your enterprise as the low level authentication mechanism for enterprise risk.
33. Read the paper "Battling Botnets and Rootkits – A Layered Identity Strategy".
34. Understand the different layers of security you need to have in place in the enterprise to effectively safeguard it based on enterprise risk.
35. Determine the types of authentication mechanisms your enterprise will support to provide different levels of multi-factor authentication.
36. Target system administrators and application super-users with stronger forms of authentication.
37. Create a table showing your enterprise's authentication strength (see this for reference).
38. Don't deploy digital certificates, secureID tokens or biometrics on their own for authentication. These authentication mechanisms, when used remotely, are not as secure as you think.
39. Always try and use multi-factor authentication wherever possible.
40. Create an authentication strength implementation plan.
41. Always remember "A BIOMETRIC IS NOT A SECRET".
42. What plans are in place to protect an identity's biometric data stored on your enterprise systems?
43. Is the biometric removed off your records when the user leaves the enterprise?

101 THINGS TO KNOW ABOUT SINGLE SIGN ON

44. Is there any agreement in place with the user to retain the biometric after the user has left the enterprise?
45. Make sure you are not using SSN numbers as an authentication id.

NETWORK SINGLE SIGN ON

46. What different access are you going to give a user who is coming in remotely versus the user logging on within the enterprise?
47. What kind of device security is in place at the firewall to prevent insecure devices making its way into the enterprise?
48. What kind of network access are you going to give for basic (id and password) authentication?
49. What kind of network operating system design are you going to use for Windows authentication and integrate it with your enterprise SSO lost password system?
50. Does any of your NOS's require LDAP upgrades in order to authenticate to the enterprise directory?

ENTERPRISE SINGLE SIGN ON (ESSO)

51. What mainframe and older applications are not going to work with web based single sign on (WSSO)?
52. What are your plans for dealing with this?
53. You might consider purchasing a SSO hardware authentication device from Imprivata.
54. Alternatively, you might also consider purchasing ESSO (Enterprise Single Sign On) from Passlogix.
55. Create an implementation plan for ESSO.

WEB SINGLE SIGN ON (WSSO)

56. Determine the number of potential applications to be integrated into WSSO.
57. Prioritize them based on ease of integration, political importance, etc.
58. Determine the global session time outs.
59. Determine the computer inactivity timeouts.
60. Identify specific applications where due to enterprise risk the timeouts need to be lower than your enterprise values.
61. Design a strategy for handling these timeouts.
62. Determine the authentication strengths to be used in the WSSO system.
63. Determine the failed authentication actions.
64. Determine the post-authentication actions.
65. Determine the authorization actions.
66. Determine the enterprise LDAP values to be sent to each application, after successful authentication to help the application with authorization, personalization and customization.
67. Determine the change management board for managing single sign on.
68. Determine standard audit values to be used in single sign on.

101 THINGS TO KNOW ABOUT SINGLE SIGN ON

69. Determine the SSO performance implications when more audit requirements than standard are turned on.
70. Determine the caching values to be used at the SSO security server, the web and application security agents.
71. Determine when the enterprise LDAP will be called to update cache values.

IMPLEMENTATION

72. Determine the number of environments you will use for SSO (e.g. Development, Test, QA, Pre-production and Production).
73. Determine how applications will be quickly moved between environments?
74. Review with the SSO vendors the work steps required to move an application between environments.
75. Determine what an application owner can and cannot do in each environment.
76. Determine the peak SSO loads.
77. Do load testing in Pre-production to determine that your system will meet much more than your peak load periods.
78. Determine the SSO servers' failover strategy.
79. Determine the SSO Servers' disaster recovery strategy.
80. Test out the failover SSO server strategy.
81. Test out the disaster SSO server recovery strategy.
82. Determine the LDAP directories failover strategy.
83. Determine the LDAP directories disaster recovery strategy.
84. Test out the LDAP directories failover strategy.
85. Test out the LDAP directories disaster recovery strategy.
86. Determine the web, application, security and LDAP directory servers monitoring requirements.
87. Create service level agreements with each portion of the SSO system (network, web servers, app servers, SSO servers, load balancers, directory servers, and authoritative source identity servers).
88. Determine SSO system availability.
89. Determine when you are able to bring down SSO servers for maintenance.
90. Determine what SSO environments you can reduce time and costs by using virtual servers.

FEDERATED AUTHENTICATION

91. Determine what enterprise outsourced services you'd like to apply federated authentication to (e.g. benefits, 401k, training outsources, etc.)
92. Determine what external enterprise requirements are for authenticated federation.
93. Determine any contractual changes required to support this (this may be VERY IMPORTANT AND TIME CONSUMING).
94. Determine what federated authentication standards you are going to support (see this page for reference).
95. Determine what SSO vendor's products you're going to use for federated authentication (e.g. Ping Identity or others).

101 THINGS TO KNOW ABOUT SINGLE SIGN ON

96. Determine any changes required to service level agreements to support federated authentication.
97. Implement federated authentication in a small pilot mode first to get the enterprise over the contractual, infrastructure and ongoing support requirements. Then roll it out to the wider world.

ODDS AND SODS

98. Design help desk routines integrated with your enterprise SSO support team to handle SSO user problems.
99. Have presentations drawn up with lots of supporting documents educating application owners about what they need to know about single sign on.
100. Make sure that senior management is fully behind the SSO implementation and ready to leap in and tell application owners and business units to fall into line in integrating with SSO.
101. Develop a plan to have the majority of applications integrated within two years time.

ABOUT THE AUTHOR:

Guy Huntington, President of Huntington Ventures Ltd, has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website on authentication at www.authenticationworld.com. He also maintains an authentication blog available off his website. He can be reached at guy.huntington@authenticationworld.com or by phone at 604-921-6797.