

Weak Keys in Metadata

[this is the **final report of 2012**, created on December 27, 2012]

[this document has been ported to the wiki: <https://spaces.internet2.edu/x/bgEVAg>]

Each of the organizations listed below has one or more entities in metadata that contain a certificate with a weak key (1024 bits). These entities, whose entity IDs are shown below, will be **removed from metadata on February 28, 2013** unless the weak key is migrated out of metadata beforehand. If you need to apply for an extension beyond February 28, see the [Upgrading Weak Keys in Metadata](#) wiki page for further instructions.

1. Apple Computer, Inc.

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:apple.com	IDPSSODescriptor	signing	4B:62:D4:03:52:77:9E:64:4C:10:2E:DC:07:05:45:3F:A2:0D:43:16
urn:mace:incommon:apple.com	AADescriptor	signing	4B:62:D4:03:52:77:9E:64:4C:10:2E:DC:07:05:45:3F:A2:0D:43:16

2. Arizona State University

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:asu.edu	IDPSSODescriptor	signing	FA:28:A2:14:0A:61:62:A0:32:37:3A:A4:70:24:24:BA:CD:C8:52:90
urn:mace:incommon:asu.edu	AADescriptor	signing	FA:28:A2:14:0A:61:62:A0:32:37:3A:A4:70:24:24:BA:CD:C8:52:90

3. Carleton College

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:carleton.edu	IDPSSODescriptor	signing	A8:C5:AF:86:14:1A:DB:AB:88:A4:84:BA:0E:0B:2B:A3:56:9A:03:D5
urn:mace:incommon:carleton.edu	AADescriptor	signing	A8:C5:AF:86:14:1A:DB:AB:88:A4:84:BA:0E:0B:2B:A3:56:9A:03:D5

4. Clemson University

Entity ID	Role	Use	SHA1 Fingerprint
https://www.intelligentriver.org/shibboleth	SPSSODescriptor	multi-use	10:33:F9:3F:D9:CC:DA:C3:CC:B5:09:DE:DF:7D:B7:71:7B:5D:E9:46

5. Elsevier

Entity ID	Role	Use	SHA1 Fingerprint
https://scauth.scopus.com/	SPSSODescriptor	multi-use	9D:E0:15:A1:8A:79:90:7E:6F:FE:98:5C:BB:59:32:D6:E0:44:77:28
https://scauth.scopus.com/	SPSSODescriptor	multi-use	B9:BC:39:D7:C3:40:23:E7:6D:18:88:E3:21:5C:DF:0D:34:FE:E2:63
https://sdauth.sciencedirect.com/	SPSSODescriptor	multi-use	9D:E0:15:A1:8A:79:90:7E:6F:FE:98:5C:BB:59:32:D6:E0:44:77:28
https://sdauth.sciencedirect.com/	SPSSODescriptor	multi-use	B9:BC:39:D7:C3:40:23:E7:6D:18:88:E3:21:5C:DF:0D:34:FE:E2:63

6. Lawrence Berkeley National Laboratory

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:lbl.gov	IDPSSODescriptor	signing	4C:55:AD:2B:C3:B2:38:AD:D4:7D:AD:DB:A2:16:F8:42:49:C5:FC:EF
urn:mace:incommon:lbl.gov	AADescriptor	signing	4C:55:AD:2B:C3:B2:38:AD:D4:7D:AD:DB:A2:16:F8:42:49:C5:FC:EF

7. NG Web Solutions

Entity ID	Role	Use	SHA1 Fingerprint
https://federation.nelnet.net	SPSSODescriptor	multi-use	D7:6B:76:B6:4A:41:CA:AD:B6:0C:DB:93:11:D6:B1:A8:8D:81:4C:8A
https://federation.ngwebsolutions.com	SPSSODescriptor	multi-use	41:02:80:72:89:2E:F2:E6:15:E3:77:34:36:7F:21:3C:94:00:0E:B7

8. New York University

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:nyu.edu	IDPSSODescriptor	signing	45:03:0D:D8:4A:AE:E6:05:66:E3:50:34:E6:5D:ED:EB:89:B6:44:1C

9. Northern Arizona University

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:nau.edu	IDPSSODescriptor	signing	63:A8:E5:72:CC:5C:E5:5A:7B:04:8E:BA:BA:8C:95:98:98:B7:36:90
urn:mace:incommon:nau.edu	AADescriptor	signing	63:A8:E5:72:CC:5C:E5:5A:7B:04:8E:BA:BA:8C:95:98:98:B7:36:90
https://alfresco.nau.edu/shibboleth	SPSSODescriptor	multi-use	90:B6:52:52:F4:C1:CF:97:F1:93:55:CE:C3:48:B7:06:53:D0:28:8A

https://confluence.nau.edu/shibboleth	SPSSODescriptor	multi-use	A7:6C:A3:9B:3E:8A:3E:C8:75:02:45:C9:B2:2D:1C:A7:B0:D2:14:91
https://dev-alfresco.nau.edu/shibboleth	SPSSODescriptor	multi-use	84:D3:81:D9:93:44:DA:42:58:63:29:E0:AC:85:1D:29:30:14:3B:AF

10. Online Computer Library Center Inc.

Entity ID	Role	Use	SHA1 Fingerprint
https://shib.oclc.org/shibboleth	SPSSODescriptor	signing	BD:F9:78:AF:4C:8C:C4:EE:55:46:D3:0F:10:C7:C2:62:55:D8:F6:B0

11. ProQuest LLC

Entity ID	Role	Use	SHA1 Fingerprint
https://shibboleth.chadwyck.co.uk/shibboleth-sp	SPSSODescriptor	multi-use	AA:7B:C9:0A:54:49:57:C5:D6:97:E5:D2:DF:BD:70:62:3C:DB:A3:E0

12. Ramapo College of New Jersey

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:ramapo.edu	IDPSSODescriptor	signing	5F:4A:0E:9C:4E:98:BA:5F:9F:5B:5E:00:2B:85:5E:25:84:BC:84:93
urn:mace:incommon:ramapo.edu	AADescriptor	signing	5F:4A:0E:9C:4E:98:BA:5F:9F:5B:5E:00:2B:85:5E:25:84:BC:84:93

13. Sonoma State University

Entity ID	Role	Use	SHA1 Fingerprint
https://login.sonoma.edu/shibboleth	IDPSSODescriptor	signing	F8:36:10:7C:B5:84:05:73:4A:A4:A6:7E:94:09:B9:A4:8D:E4:8F:B6
https://login.sonoma.edu/shibboleth	AADescriptor	signing	F8:36:10:7C:B5:84:05:73:4A:A4:A6:7E:94:09:B9:A4:8D:E4:8F:B6

14. University of Alabama at Birmingham

Entity ID	Role	Use	SHA1 Fingerprint
https://uabgrid.uab.edu/shibboleth	SPSSODescriptor	multi-use	DE:62:E7:6F:B7:C0:76:A4:CB:8D:EC:55:F8:7F:E1:C6:C1:61:57:D9

https://uabgrid.uab.edu/shibboleth	SPSSODescriptor	multi-use	E9:D4:3C:89:93:7E:15:25:8F:58:3F:E5:40:F1:67:AF:96:D3:DE:4C
------------------------------------	-----------------	-----------	-------------------------------------------------------------

15. University of Alaska Statewide System

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:alaska.edu	IDPSSODescriptor	signing	74:60:9F:8B:69:9E:CA:63:F9:A2:0D:FE:57:20:EF:0E:23:A0:EC:E6
urn:mace:incommon:alaska.edu	AADescriptor	signing	74:60:9F:8B:69:9E:CA:63:F9:A2:0D:FE:57:20:EF:0E:23:A0:EC:E6

16. University of Findlay

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:findlay.edu	IDPSSODescriptor	signing	98:25:AC:58:63:A0:DE:8A:EE:93:91:99:6F:A3:A1:23:C5:13:AC:CB
urn:mace:incommon:findlay.edu	AADescriptor	signing	98:25:AC:58:63:A0:DE:8A:EE:93:91:99:6F:A3:A1:23:C5:13:AC:CB

17. University of Washington

Entity ID	Role	Use	SHA1 Fingerprint
urn:mace:incommon:washington.edu	IDPSSODescriptor	signing	0F:73:49:C8:04:C5:F1:9A:6C:D6:36:F7:38:04:8B:66:87:CF:3A:21
urn:mace:incommon:washington.edu	AADescriptor	signing	0F:73:49:C8:04:C5:F1:9A:6C:D6:36:F7:38:04:8B:66:87:CF:3A:21
https://moodle.washington.edu/shibboleth	SPSSODescriptor	multi-use	B1:E4:1D:77:FF:B5:82:8F:31:86:09:66:4E:AA:1D:7A:90:93:07:D5

18. Washington University in St. Louis

Entity ID	Role	Use	SHA1 Fingerprint
https://acadinfo.wustl.edu/shibboleth-sp	SPSSODescriptor	multi-use	5B:00:C8:A5:06:AD:82:6B:3D:88:A7:55:5D:14:14:02:9B:8A:51:EA
https://connect.wustl.edu/shibboleth-sp	SPSSODescriptor	signing	CC:A5:16:FB:1C:13:74:57:54:3B:65:15:46:BD:0C:9A:85:0A:96:D5
https://ehsaweb.wusm.wustl.edu/shibboleth-sp	SPSSODescriptor	multi-use	71:10:9C:66:A2:FD:71:43:79:CA:40:4B:03:CA:42:8B:AD:DB:2A:CA
https://istbilling.wustl.edu/selfservice/shibboleth-sp	SPSSODescriptor	multi-use	F6:FC:83:84:75:02:34:40:7A:D9:D1:4B:56:6C:6E:A5:18:4F:C9:D1

https://istest.wustl.edu/shibboleth-sp	SPSSODescriptor	multi-use	63:CB:5F:B7:D2:8A:C6:41:7A:61:62:1E:0C:FB:4B:DF:F0:5D:51:BB
https://telesis.wustl.edu/shibboleth-sp	SPSSODescriptor	multi-use	5B:00:C8:A5:06:AD:82:6B:3D:88:A7:55:5D:14:14:02:9B:8A:51:EA