

ESPreSSO: Establishing Suggested Practices Regarding Single Sign-On

Approved: October 25, 2011

*A Recommended Practice of the
National Information Standards Organization*

Abstract: ESPReSSO explores practical solutions for improving the success of SSO authentication technologies for providing a seamless experience for the user and makes recommendations for promoting the adoption of one or more of these solutions to make the access improvements a reality.



Published by:
NISO, Baltimore, Maryland, U.S.A.

About NISO Recommended Practices

A NISO Recommended Practice is a recommended “best practice” or guideline for methods, materials, or practices in order to give guidance to the user. Such documents usually represent a leading edge, exceptional model, or proven industry practice. All elements of Recommended Practices are discretionary and may be used as stated or modified by the user to meet specific needs.

This recommended practice may be revised or withdrawn at any time. For current information on the status of this publication contact the NISO office or visit the NISO website (www.niso.org).

Published by

National Information Standards Organization (NISO)
One North Charles Street, Suite 1905
Baltimore, MD 21201
www.niso.org

Copyright © 2011 by the National Information Standards Organization

All rights reserved under International and Pan-American Copyright Conventions. For noncommercial purposes only, this publication may be reproduced or transmitted in any form or by any means without prior permission in writing from the publisher, provided it is reproduced accurately, the source of the material is identified, and the NISO copyright status is acknowledged. For permission to photocopy or use material electronically from NISO RP-11-2011, *ESPreSSO: Establishing Suggested Practices Regarding Single Sign-On*, please access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC) at 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. All inquiries regarding translations into other languages or commercial reproduction or distribution should be addressed to: NISO, One North Charles Street, Suite 1905, Baltimore, MD 21201.

ISBN (13): 978-1-880124-98-7

Table of Contents

Foreword	v
Part 1: Introduction	1
1.1 Purpose and Scope	1
1.2 Terms and Definitions.....	1
Part 2: Why Is It Time to Act?	4
2.1 Overview of Issues.....	4
2.2 Library Community.....	4
2.4 End User Community.....	5
Part 3: Traditional Approaches to Controlling Access to Licensed Resources.....	6
3.1 The Evolution of Authentication Requirements.....	6
3.2 The Evolution of Access Control.....	7
3.2.1 Client Machine IP Address and Client Organization VPN Services	7
3.2.2 Proxy Servers	9
3.2.3 Userids/Passwords for a Service Provider Site.....	10
3.2.4 Federated Login (Authentication).....	11
Part 4: ESPReSSO Recommendations	16
4.1 Overview.....	16
4.2 Use Cases	17
4.3 Summary of Recommendations	18
4.4 Recommendations to Service Providers.....	21
4.4.1 Service Provider Open Page.....	21
4.4.2 Service Provider Identity Discovery Page	21
4.4.3 Service Provider Protected Page.....	23
4.4.4 Attribute-Based Authorization	24
4.5 Recommendations to Libraries / Institutions.....	24
4.5.1 Institution Login Page	24
4.5.2 Institution Menu Page.....	25
4.6 Role of a Proxy Server in Supporting a Hybrid Environment.....	27
4.7 Rewriting OpenURLs	27
4.8 Appropriate Use of Branding.....	27
4.9 Additional Functionality	28
4.9.1 Pseudonymous Access.....	28
4.9.2 User Consent to Attribute Release.....	29
Part 5: Content Discovery Services.....	30
5.1 Content Discovery Services	30
5.1.1 Overview of Federated Search	30
5.1.2 Overview of Web-Scale Discovery Services.....	31
5.2 Existing Authentication with Discovery Services.....	32
5.3 Recommendations for Authentication in a Discovery Search Environment	32
Appendix A Description of Functions in Current Authentication Environments	33
Bibliography.....	35

Figures

Figure 1: Use case #1 scenario 17

Figure 2: Use case #2 scenario 17

Figure 3: Use case #3 scenario 17

Figure 4: Use case #4 scenario 18

Figure 5: Mock-up of Identity Discovery page using recommendations..... 23

Figure 6: Mock-up of Institution Login Page using recommendations 25

Figure 7: Example of Institution Menu Page..... 26

Figure 8: Federated search..... 30

Figure 9: Web-scale discovery search 31

Figure 10: Functional components of current authentication environments 33

Foreword

About This Recommended Practice

In 2009, NISO launched a new Chair's Initiative—a project of the chair of NISO's Board of Directors, focusing on a specific issue that would benefit from study and the development of a recommended practice or standard. Oliver Pesch, Chair of NISO's Board of Directors at the time, chose the issue of standardizing seamless, item-level linking through single sign-on (SSO) authentication technologies in a networked information environment.

Accessing information in a networked environment has been a reality for most library user communities for over a decade. Recent years have seen an explosion in this type of usage. With the advent of hosted, aggregated full-text databases and the proliferation of e-journals and e-books, users' searches for information often take them to a number of different online hosts and platforms as part of a single transaction. When those information resources are commercial products, each platform traditionally required the user to be authenticated and authorized. Service providers (SPs) have used two approaches to this issue: 1) ensuring that the requesting IP address is within a range assigned to the license holder, and 2) issuing userids and passwords to users. In the latter case, the user may have a different identity on each platform.

As usage habits and technology have evolved, these traditional methods no longer work well. With the growing complexity of licensing situations and network design, along with the increased usage from mobile devices, campuses have outgrown the capabilities of these approaches. Using and managing this environment has become confusing and error-prone for browser users, licensee organizations, and service providers. The problems caused by having to manage multiple identities have led to the development of so-called "Single Sign-On" (SSO) authentication technologies, including proprietary technologies such as Athens and formal open standards such as SAML (security assertion markup language). With these technologies, the user authenticates once and can then access all compliant content platforms using the same identity. (The user would typically be authenticated by the organization holding the licenses.) More importantly, these technologies have been designed so the user would encounter only one login event while traversing a multitude of in-sourced and outsourced service providers. In addition, with the SSO technologies' the user does not have to be using a device attached to the license holder's network; they can be anywhere in the world. Simplifying the user experience has become more important as organizations have outsourced more and more of their supporting business functions (not just to licensed content).

A bridge is needed to address today's hybrid environment and move all parties towards a longer-term effective SSO solution. The ESPReSSO Recommended Practice document recommends practical solutions for improving the success of existing SSO authentication technologies to provide a seamless experience for the user. Specifically, ESPReSSO recommends best practices related to selection of authentication method and transparent flow between the service provider (SP) site and the identity provider (IdP) site during authentication.

Recommendations to service providers include the preferred location for login links and input boxes, standard approaches for guiding users to a desired authentication method, where local branding information could be inserted on a webpage, as well as approaches for handling automatic logins.

Recommendations for libraries/institutions include display of the login page, branding of the login page, use of a menu page with all available content listed that transfers with automatic login to the selected service provider, and appropriate passing of parameters to the service provider that authenticate the user.

Additional recommendations are made about methods that provide trade-offs between privacy and advanced functions. Specific recommendations in federated search and web-scale discovery environments are made that will lead all parties from the current environment to a longer-term recommendation to use the Shibboleth authentication model.

ESPreSSO did not invent any new technology or protocols. Instead, ESPReSSO aims to promote the adoption of best practices that make access improvements a reality by using existing technologies while preparing for the future.

Discovery to Delivery Topic Committee

NISO's Discovery to Delivery (D2D) Topic Committee had the following members at the time it approved this Recommended Practice:

Susan Campbell

College Center for Library Automation (CCLA)

Larry Dixon

Library of Congress

David Fiander

University of Western Ontario

Peter Murray

Lyris

John Mark Ockerbloom

University of Pennsylvania Libraries

Jeff Penka

OCLC Online Computer Library Center

Tim Shearer

University of North Carolina Chapel Hill Libraries

Chris Shillum

Reed Elsevier

Robert Walsh

EnvisionWare, Inc.

ESPreSSO Working Group Members

The following individuals served on the NISO ESpReSSO Working Group that developed and approved this Recommended Practice:

Steven Carmody (Co-chair)

Brown University

Frank Cervone

Purdue University Calumet

Pete Ciuffetti

CredoReference

Andy Dale

OCLC, Inc.

Kristine Ferry

University of California, Irvine

Andy Ingham

University of North Carolina, Chapel Hill

Harry Kaplanian (Co-chair)

Serials Solutions, Inc.

David Kennedy

Johns Hopkins University

Ted Koppel

Auto-Graphics, Inc.

Lyn Norris

Eduserv

Heather Staines

Springer

Pieter van Lierop

Infor Library and Information Solutions

Foster Zhang

Johns Hopkins University

Acknowledgments

The ESpReSSO Working Group would like to offer a special thanks to the following individuals for their assistance:

Adam Chandler (Working Group Observer)

Cornell University

Oliver Pesch (Working Group Observer; Project Proposal Author)

EBSCO Information Services

Rob Walsh (original Working Group member)

EnvisionWare, Inc.

For input regarding publisher, aggregator, and platform experience with implementing single sign-on, we thank the following:

American Institute of Physics: Paul DeCillis
Cambridge University Press: Chris Fell
EBSCO Information Services: Sarah Buck and Heather Klusendorf
Elsevier: Chris Shillum and Ale DeVries
HighWire Press: John Sack
H. W. Wilson: Ronald Miller
IEEE: Gerry Grenier
Institute of Physics: Laura Shaw

Ithaka/JSTOR: Matthew Callow and Brian Larsen
MetaPress: Matthew Wren and Tiffany Rich
Nature Publishing Group: Amanda Ward
Oxford University Press: Claire Dowbekin
Semantico: Colin Caveney and Richard Padley
Taylor and Francis: Margaret Walsh and Rosa Perez
Wiley-Blackwell: Caroline Rothaug

For input regarding accessibility issues, we thank the following:

Kerri Hicks, University of Rhode Island

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2

Part 1: Introduction

1.1 Purpose and Scope

In recent years, many institutions have moved to take advantage of many benefits afforded by Single Sign On, including access to learning management systems (Blackboard, Sakai), research tools (RefWorks, TurnItIn), and, of course, subscription-based library resources (e-journals, e-books, databases). Making the Single Sign-On (SSO) environment work better and smarter will certainly help increase the success of users getting to the content to which they are entitled. Over the last several years many of the larger service providers (SPs) have implemented SSO technologies. However, it is probably fair to say that many content hosts have not implemented these technologies. Library users are required to operate in an environment that includes a mix of authentication technologies with internet protocol (IP) authentication being the most common. An effective solution needs to address this hybrid environment and, at the very least, take into consideration the needs of IP authentication and proxy servers and how they interoperate with SSO authentication technologies.

The ESPReSSO Recommended Practice document recommends practical solutions and a path forward for improving the success of SSO authentication technologies for providing a seamless experience for the user. It further aims to promote the adoption by campuses and service providers of a family of solutions to make the access improvements a reality. This initiative did not invent any new technology or protocols. Rather, it has developed a set of “best practice” recommendations surrounding the use of existing technologies.

The ESPReSSO Working Group was primarily concerned with the situation where an organization (a company, a campus, a public library, etc.) acquires a license to access specific content that is delivered via the web, and where the browser user is a member of the group authorized to access that content. The working group did not address the situation where an individual, either on his or her own or as part of a group, would obtain a license for personal use and then use a personal account from a major internet account provider to authenticate himself or herself to the service provider. Service providers are reporting that users are not currently requesting this functionality. In addition, supporting this approach requires as much work for the publishers in managing userids and passwords within their sites as it does for the licensee organization. The processes publishers use to sell individual articles was considered to be out of scope for this report.

Best practices for user experience on mobile devices are rapidly evolving. Consequently, this report avoids recommendations for screen layout and use on mobile devices. However, the flows described in later sections will work on mobile devices.

Lastly, as with any web-based system, it is important to address accessibility issues. The recommendations contained in this report describe a number of webpages, and include some sample screen images. However, this report does not recommend any specific implementation. All implementations should meet all Web Content Accessibility Guidelines (WCAG) guidelines.

1.2 Terms and Definitions

The following terms, as used in this recommended practice, have the meanings indicated. See also [Appendix A](#), which contains definitions and descriptions of functional components found in an authentication environment.

<u>Term</u>	<u>Definition</u>
service provider (SP)	A website offering services and content to browser users. Often, part of the site is available for open browsing and part of the site is access controlled, requiring proof that the user is authorized for access under an existing contract. Many publishers or content providers are offering licensed content via the Internet.

<u>Term</u>	<u>Definition</u>
identity provider (IdP)	A user's home organization. The user typically has a strong relationship with this organization, and it can make up-to-date and accurate assertions about the user.
identity discovery service	A webpage presented by service providers to which users are redirected for authentication after selecting their home organization. This page was previously called a WAYF (Where Are You From) Service.
deep link	A URL pointing to a specific resource (e.g., an article) at a service provider site.
federated login (authentication)	An approach to authentication where a service provider site redirects browser users to their home organization for authentication. After a successful authentication, the browser user is returned to the service provider accompanied by attribute assertions describing his/her rights at the service provider. As used in this report, the term includes the authorization process performed at the SP site.
federated search (metasearch; web-scale discovery search)	A portal that allows a user to enter search terms and then uses the terms to search across a wide variety of potential sources. It allows patrons unfamiliar with where content can be found to discover all relevant licensed content available in the library.
IP-based authentication	A method where a service provider and a licensee organization have agreed that every request coming from a range of network/Internet Protocol (IP) addresses associated with the licensee organization should be granted access to the licensed resources.
Just-in-Time (JIT) authentication	A process at a service provider's website that will initiate the login process when an anonymous user attempts to access controlled content. For instance, JIT will often be triggered if an anonymous user attempts to access a deep link.
licensee organization	The institution that signed a contract with a service provider on behalf of the users who are affiliated in some way with the institution. The licensee organization then becomes an identity provider for those users. This report will sometimes use the word campus to refer to a licensee organization.
link resolver	A service run by the licensee organization that will accept an OpenURL syntax (e.g., from a site with abstracts) and map that to a URL at a site where the licensee organization has access to a licensed copy of the full text of the article.
personally identifiable information (PII)	Information which makes it possible to identify a specific individual. A person's name is considered PII (although it may not be sufficient to identify a single individual). This report mentions situations where an identity provider might release attributes which contain PII to a service provider.

Term**Definition**

proxy server

A computer system that acts as an intermediary between a user making a request and the requested service. Licensee organizations operate proxy servers in order to provide their users with access to licensed resources when the users are not directly connected to the licensee organization's network (e.g., they are at home or traveling). Users authenticate to the proxy, which is connected to the licensee organization's network, and the proxy then allows them access to the licensed resources "through" the proxy server.

security assertion markup
language
(SAML)

A standards-based approach to web single sign-on (SSO) authentication. Many interoperable open source and commercial implementations of SAML are available.

virtual private network
(VPN)

A secure method of connecting to an organization's protected network from a remote location through a special server that authenticates the remote user to the network using credentials provided by the organization. To service providers, the user then appears to be coming from an IP address on the licensee organization's network, even though the user is physically remote from that network.

WAYFless URL

A URL created by a licensee organization and pointing to a service provider that includes information about the licensee organization. Clicking a WAYFless URL allows a user to bypass the Identity Discovery process.

web single-sign on (SSO)
authentication

A framework for authenticating users across a family of services. The user authenticates once and all succeeding authentication requests are handled transparently by the service without requesting anything further from the user.

Part 2: Why Is It Time to Act?

2.1 Overview of Issues

The current mélange of approaches to authentication and authorization has resulted in nightmarish operational situations for licensee organizations, for service providers, and for users. Unfortunately, there is no silver bullet that will quickly return us to a set of simple options. We are in a phase of transition to new models for authentication and authorization; it is likely that—for the short term—all parties will have to work in a hybrid environment where a variety of mechanisms need to be supported. However, because of the complexity this adds to the user experience, all organizations are strongly encouraged to transition to the newer models as soon as possible.

The complexity arises for several reasons:

- The internet world has evolved to provide users with many more options. Users can follow different paths, traversing multiple websites, in order to enter a publisher's site. They can have different starting points (e.g., a link found on the open web, a search on the open web, directly accessing a publisher front page, a redirect from a library navigation page/menu page, a redirect via an OpenURL to a deep-link URL within the publisher site, a bookmark, e-mailed hyperlinks, etc.). The result is that users arrive at many different points on the publisher's site. It has been difficult to create a consistent, coherent user experience amidst all this variety.
- Users may experience multiple authentication mechanisms, depending on how they enter a publisher's site. Sometimes, the user's physical location could affect the browser flows and authentication mechanisms. Within the publisher's site, the user might—innocently—navigate from a public page to a protected page, and thus unwittingly trigger authentication.
- Service providers generally have to present and support multiple authentication mechanisms. They have to construct and present a usable authentication graphical user interface (GUI) that somehow combines multiple methods into an interface that can be used successfully by people with a low familiarity with technical concepts.
- Campuses have deployed various approaches over the years; some of them require users to be able to use, handle, and manipulate proxy-prefixed URLs that are incomprehensible to the average person.

The hybrid environment will likely include both IP and web Single Sign-On (SSO) authentication, and may include other options, as well. Licensee organizations will likely have contracts with some organizations that support SSO and some that still only support IP authentication. Service providers will likely have to work with licensee organizations that want to use web SSO and some that are still relying on IP authentication. However, it is clear that requirements have evolved such that IP authentication is now a poor fit with user requirements, and that, going forward, web SSO implementations will be more secure, easier to user, and more functional for service providers, licensee organizations, and users.

Each of these three communities is impacted in negative ways when confronted with the hybrid environment as described in the following sections.

2.2 Library Community

Patron demand for remote access to content via computer or mobile device has become the norm rather than the exception. Keeping track of numerous usernames and passwords for the multitude of publisher sites and platforms is unmanageable. Ensuring the privacy of user searches, reading history, and behavior has long been a principle of library operations. Librarians are insisting that the traditional levels of privacy remain as an option for the digital user. Many users may be willing to trade some of their privacy for a higher level of service. However, a set of users and situations remain where user privacy is an absolute requirement. Libraries must provide patrons with an efficient, seamless way to access content and to search across this content from multiple sources without continually being challenged for credentials, or having to change the steps they follow as a

function of their physical location. For libraries in countries where national federations have evolved to advocate for SSO, data challenges remain. However, for libraries in locations without government-funded federations, the obstacles are greater, as there is no legal mandate requiring content providers to offer such a service.

2.3 Publisher Community

As licenses increase in their complexity, customers may participate in numerous agreements, allowing varying degrees of access at an institutional, consortial, departmental, or other level. Keeping track of which affiliated users have access to what content becomes more challenging all the time.

At the same time, customer demands for privacy concerning their users' personal details and online search behavior have grown at an even quicker pace. Implementing single sign-on that allows institutions to vouch for their authorized users puts the responsibility and the authority for access back into the hands of the institution, allowing content providers to concentrate on the content rather than the access details. Spurred to action by support for single sign-on amongst European federations, service providers and content providers have labored to meet the varying requirements, including certification, interface adaptation, required attributes, and more. Demands for SSO implementation come now from around the globe and include corporate and government, as well as academia and libraries.

Streamlining the process and the variety of approaches has become essential to service providers who must also ensure that their branding remains visible to end users. The current variability in the end user experience creates a high level of confusion and results in users giving up rather than being able to complete their tasks. A decrease in usage may be used as evidence for cancelation by librarians, so this situation poses a threat to publisher business models.

2.4 End User Community

Researchers and students have access to content through a variety of channels; however, if access is from outside of the university's IP range, a multitude of usernames and passwords might be required. When seeking access to a secured resource, a researcher should be able to identify easily whether the publisher/aggregator supports SSO. He or she should be able to navigate to the institution login page, to identify the appropriate federation and institution, and, once authenticated, to return to the secured resource with minimal disruption. All stages of this process should be identified and branded so that the request for credentials is not misinterpreted as phishing or malware. As an authorized user of a resource licensed by his/her institution, the researcher should be able to gain access in a manner that is as seamless and painless as possible.

Working in the hybrid environment is particularly confusing for users. Various studies of user interface issues have consistently focused on usability and consistency issues. Browser users are visiting multiple sites, but are seeking some consistency in how they identify themselves to service provider (SP) sites. In addition, in the Federated Login model, users can be redirected from the SP site to the identity provider (IdP) site and back to the SP site; throughout this process, users are seeking visual feedback indicating that the sequence of pages they are seeing are related to their goal of obtaining access to a particular SP site.