

Inhalt

Vorwort	13
Einleitung	15

TEIL I Grundlagen

1 Grundlegende Begriffe und Konzepte 21

1.1	SSO und verwandte Konzepte	21
1.2	Chancen und Risiken	22
1.3	Terminologie	23
1.3.1	Security Assertion	23
1.3.2	Identity Provider	23
1.3.3	Security Token Service	24
1.3.4	Service Provider	24
1.4	Technische und organisatorische Anforderungen	25
1.4.1	SSO im Unternehmen	26
1.4.2	SSO zwischen Unternehmen	27
1.5	Identitätsverwaltung	30

2 Single-Sign-on-Technologien und -Standards 35

2.1	Konzepte im SAP-Umfeld	36
2.1.1	Digitale Signatur und Zertifikate	36
2.1.2	SAP Logon Ticket	41
2.1.3	SAML für Web-Single-Sign-on	44
2.1.4	SAML für Webservices	60
2.1.5	Kerberos	70
2.1.6	OpenID	76
2.1.7	Vergleich der SSO-Technologien	81
2.2	Single-Sign-on-Szenarien mit SAP NetWeaver	83

TEIL II Single-Sign-on für Benutzerschnittstellen

3 Workshop: Single Sign-on mit Kerberos für SAP GUI 89

3.1	Einführung in das Szenario	90
3.2	Systemvoraussetzungen	91
3.3	Konfiguration und Test des Szenarios	91

3.4	Wichtige SAP-Hinweise	92
3.5	Zusammenfassung	92

4 Workshops: Browser-Single-Sign-on mit Zertifikaten 93

4.1	Workshop: Active Directory Certificate Services	94
4.1.1	Einführung in das Szenario	95
4.1.2	Systemvoraussetzungen	96
4.1.3	Konfigurationsschritte	97
4.1.4	Szenario testen	114
4.1.5	Fehleranalyse und -behebung	115
4.1.6	Wichtige SAP-Hinweise	117
4.1.7	Zusammenfassung	117
4.2	Workshop: SAP Trust Center Service	118
4.2.1	Einführung in das Szenario	118
4.2.2	Systemvoraussetzungen	120
4.2.3	Konfigurationsschritte	120
4.2.4	Zusammenfassung	137

5 Workshop: Single Sign-on mit SPNEGO 139

5.1	Einführung in das Szenario	139
5.2	Systemvoraussetzungen	142
5.3	Konfigurationsschritte	142
5.3.1	Servicebenutzer in der Domäne erstellen	143
5.3.2	SPN zuordnen	144
5.3.3	Benutzerspezifisches UME-Attribut für den Kerberos Principal Name hinzufügen	144
5.3.4	Kerberos-Konfiguration für neuen Realm im Portal anlegen	145
5.3.5	Authentication Stack im Portal für SPNEGO konfigurieren	148
5.3.6	Domänen- und Portalbenutzer anlegen	149
5.4	Szenario testen	150
5.5	Fehleranalyse und -behebung	152
5.6	Wichtige SAP-Hinweise	156
5.7	Zusammenfassung	157

**6 Workshops: Single Sign-on für Webanwendungen
mit SAML 2.0 159**

6.1	Workshop: Web-SSO zwischen Unternehmen	159
6.1.1	Einführung in das Szenario	160

6.1.2	Systemvoraussetzungen	162
6.1.3	Konfigurationsschritte	163
6.1.4	Szenario testen	183
6.1.5	Fehleranalyse und -behebung	184
6.1.6	Wichtige SAP-Hinweise	186
6.1.7	Zusammenfassung	186
6.2	Workshop: Web-SSO in einer heterogenen Systemlandschaft	187
6.2.1	Einführung in das Szenario	187
6.2.2	Systemvoraussetzungen	190
6.2.3	Konfigurationsschritte	190
6.2.4	Szenario testen	205
6.2.5	Fehleranalyse und -behebung	211
6.2.6	Wichtige SAP-Hinweise	213
6.2.7	Zusammenfassung	213

7 Workshop: OpenID mit einem externen Portal 215

7.1	Einführung in das Szenario	215
7.2	Systemvoraussetzungen	219
7.3	Konfigurationsschritte	220
7.3.1	OpenID-URL registrieren	220
7.3.2	OpenID-Komponenten im Portal installieren	220
7.3.3	Neue OpenID-Anmeldeanwendung aktivieren	223
7.3.4	UME-Attribut für OpenID-URL anlegen	225
7.3.5	Authentication Stack für OpenID konfigurieren	225
7.4	Szenario testen	227
7.5	Fehleranalyse und -behebung	230
7.6	Wichtige SAP-Hinweise	232
7.7	Zusammenfassung	233

TEIL III Single-Sign-on mit Webservices

8 Workshops: Single Sign-on zum AS/ABAP als WS-Provider 237

8.1	Einführung	238
8.2	Single Sign-on zwischen einer Serveranwendung und AS ABAP mit SAML-Sender-Vouches	241
8.2.1	Konfiguration des WS-Providers für SAML-Sender- Vouches	242
8.2.2	Konfiguration des WS-Providers	244

8.2.3	Selbst signierten Signaturschlüssel für den WS-Consumer erzeugen	246
8.2.4	Vertrauensbeziehung einrichten	248
8.3	Workshop: Single Sign-on mit Apache Axis2 und Apache Rampart	255
8.3.1	Single Sign-on mit SAML 1.1-Sender-Vouches	256
8.3.2	Konfiguration des WS-Providers	256
8.3.3	WS-Consumer erstellen	257
8.3.4	WS-Consumer konfigurieren	262
8.3.5	Webservice aufrufen	266
8.3.6	Vertrauensbeziehung einrichten	267
8.3.7	Szenario testen	268
8.3.8	Fehleranalyse und -behebung	269
8.4	Workshop: Single Sign-on mit Sun Metro 2.0	270
8.4.1	Single Sign-on mit SAML 1.1-Sender-Vouches	271
8.4.2	WS-Provider konfigurieren	271
8.4.3	WS-Consumer erstellen	272
8.4.4	WS-Consumer konfigurieren	275
8.4.5	Webservice aufrufen	277
8.4.6	Vertrauensbeziehung einrichten	278
8.4.7	Szenario testen	279
8.4.8	Fehleranalyse und -behebung	279
8.5	Workshop: Single Sign-on mit anderen EE5-Plattformen	280
8.5.1	Single Sign-on mit SAML 1.1-Sender-Vouches	281
8.5.2	WS-Provider konfigurieren	282
8.5.3	WS-Consumer erstellen	282
8.5.4	WS-Consumer konfigurieren	282
8.5.5	Vertrauensbeziehung einrichten	283
8.5.6	Szenario testen	283
8.5.7	Fehleranalyse und -behebung	283
8.6	Workshop: Single Sign-on mit einer .Net-Serveranwendung	283
8.6.1	Single Sign-on mit SAML 1.1-Sender-Vouches	284
8.6.2	WS-Provider konfigurieren	285
8.6.3	WS-Consumer erstellen	285
8.6.4	WS-Consumer konfigurieren	285
8.6.5	Vertrauensbeziehung einrichten	286
8.6.6	Szenario testen	287
8.6.7	Fehleranalyse und -behebung	287
8.7	Single Sign-on zwischen Desktop-Anwendungen und dem AS ABAP	287
8.7.1	Authentifizierung mit SAML-Holder-of-Key	288

8.7.2	Einführung in das Szenario	289
8.7.3	Authentifizierung mit X.509-Zertifikaten	290
8.8	Workshop: Single Sign-on mit X.509-Zertifikaten zwischen einer Java-Desktop-Anwendung mit Sun Metro und AS ABAP 7.00	290
8.8.1	Provider-Konfiguration anlegen	291
8.8.2	Vertrauensbeziehung einrichten	292
8.8.3	Benutzerabbildung über den Report RSUSREXT	292
8.8.4	WS-Consumer erstellen	293
8.8.5	WS-Consumer konfigurieren	293
8.8.6	Szenario testen	293
8.8.7	Fehleranalyse und -behebung	294
8.9	Workshop: Single Sign-on zwischen Microsoft Office und dem AS ABAP	294
8.9.1	Single Sign-on mit SAML 1.1-Holder-of-Key	295
8.9.2	Systemvoraussetzungen	297
8.9.3	ADFS-Security-Token-Service konfigurieren	298
8.9.4	Relying Partys mit AS ABAP 7.02 und 7.30 konfigurieren	299
8.9.5	Relying Partys mit AS ABAP 7.01 und 7.11 konfigurieren	302
8.9.6	Auszustellende Claims konfigurieren	304
8.9.7	Vertrauensbeziehung im SAP-WS-Provider-System einrichten	305
8.9.8	WS-Provider konfigurieren	311
8.9.9	WS-Consumer erstellen	313
8.9.10	WS-Consumer konfigurieren	313
8.9.11	Szenario testen	316
8.9.12	Fehleranalyse und -behebung	317
8.10	Zusammenfassung	320

9 Workshop: Single Sign-on in SAP NetWeaver BPM 321

9.1	Einführung in das Szenario	321
9.2	Systemvoraussetzungen	326
9.3	Konfigurationsschritte	327
9.3.1	Voraussetzungen für die Konfiguration des Szenarios	327
9.3.2	Benutzer für das Szenario anlegen	328
9.3.3	SAP NetWeaver Developer Studio vorbereiten	330
9.3.4	BPM-Prozess für Single Sign-on konfigurieren	334
9.3.5	Nachrichtenbasierte Authentifizierung einrichten	335

9.3.6	Vertrauensbeziehung zwischen WS-Provider und WS-Consumer einrichten	338
9.3.7	WS-Provider für Single Sign-on konfigurieren	346
9.3.8	WS-Consumer für Single Sign-on konfigurieren	349
9.3.9	Abbildungsinformationen des Benutzernamens auf dem SAP ERP-System pflegen	352
9.4	Szenario testen	354
9.5	Fehleranalyse und -behebung	359
9.5.1	Fehlersuche im AS Java	359
9.5.2	Fehlersuche im AS ABAP	359
9.6	Wichtige SAP-Hinweise	362
9.7	Zusammenfassung	362

Anhang **363**

A	Fehleranalyse für die SAML- und X.509-Authentifizierung	365
B	Literatur und weiterführende Websites	367
C	Die Autoren	369
	Index	371