Interoperabilität: Sicherheits- und Identitätsintegration

Weitere Informationen unter www.microsoft.com/interop

Kurzfassung

Im Laufe der Jahre sind IT-Umgebungen aufgrund steigender Kundenanforderungen und rasanter Innovationen im IT-Bereich immer komplexer und heterogener geworden. Geschäfts- und Behördenkunden müssen häufig mehrere Sicherheits- und Verzeichnisdienste verwalten, die ihrerseits hohe Anforderungen an Soft- und Hardware mit sich bringen.

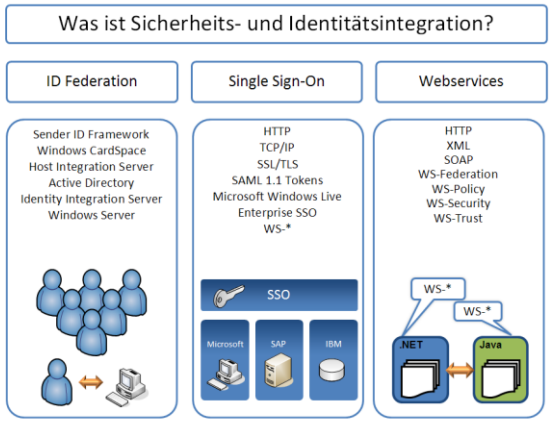
Genau deshalb bietet Microsoft „Interoperabilität by Design".

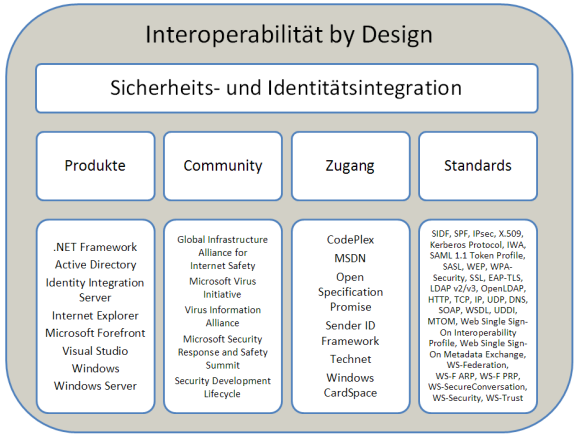
Microsofts Ansatz für eine durchgängige Interoperabilität erhöht den Wert von IT-Lösungen. Möglich wird dies durch Sicherheits- und Identitätslösungen, die sich leicht und verlässlich in andere Technologieplattformen integrieren lassen.

Was ist Sicherheits- und Identitätsintegration?

Hierbei geht es um mehr Sicherheit, höhere Zuverlässigkeit und eine besser geschützte Privatsphäre bei der Computernutzung. Sicherheits- und Identitätsintegration bedeutet:

- **Bereitstellung von Technologien zur Identitätsauthentifizierung,** die die Kerberos-Authentifizierung, eine Public-Key-Infrastruktur, .509-Zertifikate, SAML 1.1 Tokens und Webservice-Standards unterstützen.
- **Anwender dabei unterstützen, sich vor bösartiger Software** wie Computerviren und Phishing zu schützen. Dies erfolgt durch verbesserte Sicherheitseigenschaften, eine enge Zusammenarbeit mit Mitbewerbern und die Unterstützung von Industriestandards.
- **Ermöglichung von Single-Sign-On-Szenarien im Unternehmen**, plattformübergreifend und sprachenunabhängig; durch protokollbasierte Technologien und standardisierte Webservice-Implementierungen.
- **Erstellen sichererer und verlässlicherer Systeme** mit Produkten wie Microsoft® Forefront™, Identity Integration Server, Windows Vista™ und Windows Server®.





Microsoft unterstützt die Sicherheits- und Identitätsintegration

Für Kunden mit heterogenen IT-Systemen bietet Microsoft vier Arten der Sicherheits- und Identitätsintegration:

- **Produkte:** Microsoft bietet innovative Tools und Technologien für Entwickler, um interoperable Lösungen zu ermöglichen, die auf Industriestandards für Sicherheit, Verschlüsselung und Identitäts-Metasystemen basieren.
- **Community:** Microsoft arbeitet zusammen mit Kunden, Partnern und anderen Anbietern daran, Sicherheitsinformationen gemeinsam zu verwenden und integrierte Lösungen zu entwickeln, die ein unternehmensweites Single-Sign-On, eine Identitäts-Authentifizierung sowie eine Identity Federation ermöglichen.
- **Zugang:** Die Lizenzierung von Technologie-Assets an und von anderen Unternehmen und das Bereitstellen von Technologien wie das Sender ID Framework, die Virtual Hard Disk (VHD)-Image-Format-Spezifikation und 38 Webservice-Standards unter dem „Open Specification Promise".
- **Standards:** Microsoft unterstützt Industrie- und technische Standards für Sicherheit und Verschlüsselungsprotokolle. Die aktive Mitarbeit bei Standardisierungsorganisationen fördert die Einführung neuer Technologien.

Microsoft unterstützt Standards

- **Microsoft-Produkte und -Technologien unterstützen Hunderte von technischen Standards**. Beispiele hierfür sind AES, DHCP, Kerberos, HTTP, IP, IPsec, PKI, SAML 1.1 Token Profile, SSL, TCP, TLS, WPA Security, WS-* und X.509.
- **Microsoft engagiert sich aktiv in über 100 nationalen und internationalen Standardisierungsorganisationen** wie ECMA, ETSI, OASIS, IEEE, IETF, ISO/IEC JTC1, ITU und W3C.
- **Experten von Microsoft haben Dutzende von Industriespezifikationen und -standards verfasst oder mitverfasst**. Hierzu gehören u. a. WS-Addressing, WS-I Basic Profile, WS-Policy, WS-ReliableMessaging, WS-SecureConversation, WS-Security, WS-SecurityPolicy und WS-Trust.
- **Microsoft arbeitet gemeinsam mit Partnern daran, eine neue Generation von Software und Webservices zu definieren,** die auf XML (eXtensible Markup Language) basiert.

Die Sicherheits- und Identitätsintegration erfolgreich meistern

- Trustworthy Computing (TwC) ist einer der wichtigsten Unternehmenswerte bei Microsoft und bestimmt nahezu alles, was wir tun. TwC ruht auf folgenden vier Eckpfeilern: Sicherheit, Datenschutz, Verlässlichkeit und Geschäftspraktiken.
- Microsoft bietet Leitfäden für sichere Codierungspraktiken in der IT-Branche mit Hilfe von SDL (Secure Development Lifecycle).
- Die Produkte von Microsoft ermöglichen eine Vielzahl von Single-Sign-On-Szenarien für Onlinetransaktionen, Host-Systeme und heterogene Unternehmensumgebungen.
- Windows® CardSpace bietet einen konsistenten Weg, mit mehreren digitalen Identitäten zu arbeiten, unabhängig von der Art der Security-Tokens, die dabei verwendet werden.
- Um den Austausch von Sicherheitsinformationen in der IT-Industrie zu fördern, nimmt Microsoft an der GIAIS (Global Infrastructure Alliance for Internet Safety), der MVI (Microsoft Virus Initiative), dem MSRSS (Microsoft Security Response and Safety Summit), der VIA (Virus Information Alliance), dem MSCP (Microsoft Security Cooperation Program) sowie der MSSA (Microsoft Security Support Alliance) teil.

Weitere Informationen:

- Trustworthy Computing
  http://www.microsoft.com/mscorp/twc/default.mspx
- Microsoft Identity Integration Server
  http://www.microsoft.com/windowsserversystem/miis2003/default.mspx
- Windows CardSpace (früher InfoCard)
  http://msdn.microsoft.com/windowsvista/reference/default.aspx?pull=/library/en-us/dnlong/html/IntroInfoCard.asp

Microsoft

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Interoperabilität: Sicherheits- und Identitätsintegration

Weitere Informationen unter www.microsoft.com/interop

Einsatzszenarien	*Microsoft-Lösungen*	*Von Microsoft-Produkten unterstützte Standards*	*Weitere Informationen:*
ID-Authentifizierungs- und Managementsysteme integrieren	**Microsoft Identity Integration Server (MIIS)** bietet eine einheitliche Sicht für einen Anwender im gesamten Unternehmen. MIIS unterstützt über 20 Account-Repositories wie LDAP-Verzeichnisse, Datenbanken, proprietäre Stores und Dateien mit flachen Strukturen. MIIS Management Agents können zur Verbindung mit verschiedenen Verzeichnisdiensten und Anwendungen wie eDirectory, Lotus Notes, Novell Server, Sun ONE/iPlanet Directory und X.500 Systems verwendet werden.	.txt-Dateien, DSML, Dateien mit flachen Strukturen, HTTP, Kerberos, LDAP, SOAP, WS-I Profiles, WS-Security	• http://www.microsoft.com/windowsserversystem/miis2003/evaluation/overview
Integration von UNIX-Domänen und -Kennwörtern in Windows-Verzeichnisdienste	**Das Windows Server 2003 R2-Betriebssystem** bietet Identitätsmanagementlösungen im Rahmen der Integration in UNIX-basierte Systeme. Auf diese Weise lässt sich ein durchgängiger Anwenderzugriff sowie ein effizientes Management von Netzwerkressourcen über verschiedene Betriebssysteme hinweg sicherstellen. Diese Lösungen beinhalten einen Server für NIS (Network Information Service), was bei der Integration von UNIX-basierten NIS-Servern hilft, sowie die Kennwortsynchronisation, die Unternehmen bei der Einhaltung der Bestimmungen für sichere Kennwörter unterstützt.	IP, HTTP, POSIX-Standards, TCP	• http://www.microsoft.com/windowsserver2003/r2/Identity_Management
Sicherheitsfunktionen in Windows-basierte Systeme integrieren	**Microsoft Forefront** Client Security ist eine umfassende Reihe von Sicherheitsprodukten. Diese unterstützen Unternehmen dabei, Windows-basierte Systeme bei der Integration in eine bestehende IT-Infrastruktur abzusichern, und erleichtern die Bereitstellung, Verwaltung und Analyse. Microsoft Forefront-Sicherheitsprodukte schützen Clientcomputer, Serveranwendungen sowie den Rand („Edge“) des Unternehmensnetzwerks.	802.1X, DCOM, DHCP, IPsec, SMTP	• http://www.microsoft.com/forefront
Enterprise-SSO mit Host-Systemen ermöglichen	**Microsoft Host Integration Server** und **Microsoft BizTalk® Server** ermöglichen es, die Windows-basierte Unternehmenssicherheitsintegration zum Enterprise Single Sign-On (SSO) zu erweitern. Dieses bietet Benutzerkonten- und Kennwortmapping und -caching, ein Single Sign-On für mehrere Windows-Domänen und Host-Sicherheitssysteme sowie eine systemübergreifende Kennwortsynchronisation zur Vereinfachung der Kontenverwaltung. Enterprise SSO gestattet es, Konten in Windows-basierten Active Directory®-Verzeichnissen und Host-Systemen oder Branchenanwendungen (für Eins-zu-eins- oder Mehrfachzuweisungen) abzubilden.	DRDA, HTTP, Kerberos, LU 6.2, SNA, SOAP, WS-*, X.509, XML	• http://download.microsoft.com/download/C/6/5/C65FF9FD-0ED7-47F6-91AB-000E6265EA5B/Enterprise_SSO_Whitepaper.doc
Identity Federation mit WS Federation- und Liberty Alliance ID-FF-Webservice-Architekturen ermöglichen	Das **Web Single Sign-On Interoperability Profile (Web SSO Interop Profile)** definiert ein Interoperabilitätsprofil des Web Single Sign-On Metadata Exchange (Web SSO MEX) -Protokolls. Dieses Profil ermöglicht die Verwendung von Identitätsprovidern, die auf dem Liberty Alliance Identity Federation (Liberty Alliance ID-FF) -Framework oder WS-Federation basieren und die die Interaktion mit einem ID-Authentifizierungsdienst gestatten.	Liberty Alliance ID-FF, WS-Federation, Web SSO Interop Profile, Web SSO MEX	• http://msdn.microsoft.com/library/en-us/dnglobspec/html/websso.pdf
Schutz der Anwender vor Spam und Phishing	Das **Microsoft Sender ID Framework** wurde erstellt, um E-Mail-Domain-Spoofing (Vortäuschung einer falschen Absenderidentität) entgegenzuwirken und einen besseren Schutz gegen Phishing zu bieten. Das Sender-ID-Framework überprüft die Server-IP-Adresse des Absenders, um zu bestätigen, dass jede E-Mail-Nachricht tatsächlich aus der Internetdomäne stammt, aus der sie angeblich stammen soll. Die Eliminierung des Domainspoofing hilft legitimen Absendern, ihre Domänennamen und ihren Ruf zu schützen. Des Weiteren können Empfänger mit diesem Verfahren Junk- und Phishing-E-Mails effizienter identifizieren und herausfiltern.	DNS, HTTP, IP, SIDF, SMTP, SPF, TCP	• http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
Anwendern die Verwaltung ihrer in verschiedenen Providern gespeicherten digitalen Identitäten zum Zugriff auf Onlinedienste ermöglichen	**Windows CardSpace** (früher **InfoCard**) ist ein Bestandteil des Microsoft .NET Framework, Version 3.0, das auf den in WS-Trust, WS-SecurityPolicy und WS-MetadataExchange beschriebenen Mechanismen aufbaut. Mit Windows CardSpace kann eine digitale Identität in ein Framework zur Token-Ausgabe- und -Verwendung integriert werden, das eine Interoperabilität zwischen Identitätsprovidern und „Relying Parties“ (Personen, die auf ein Zertifikat vertrauen) bietet und das den Anwendern eine bessere Kontrolle ihrer digitalen Identität ermöglicht.	DNS, HTTP, Kerberos, SAML 1.1 Token Profile, SOAP, WS-MetadataExchange, WS-Security, WS-SecurityPolicy, WS-Trust, X.509, XML	• http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx • http://msdn2.microsoft.com/en-us/library/aa480189.aspx
Integration von Smartcard-basierten Identitätssystemen in Windows-basierte Systeme	**Windows und Windows Server** unterstützen die Verwendung einer Vielzahl von Smartcards zur Authentifizierung von Konsolenanmeldungen beim Fernzugriff und beim Administratorzugang. Der Active Directory-Verzeichnisdienst in Windows Server 2003 unterstützt serienmäßig die Verifizierung der interaktiven Anmeldung per Smartcard und erlaubt es, Benutzerkonten Zertifikate zuzuweisen. Dadurch wird der privaten Schlüssel auf der Smartcard mit dem im Active Directory gespeicherten Zertifikat verbunden.	EAP-TLS, FTP, HTTP, IP, Kerberos, LDAP, PKI, PPP, SMTP, SSL, TCP, UTF-8, X.509	• http://www.microsoft.com/technet/security/guidance/networksecurity/securesmartcards/default.mspx
Interoperabilität mit anderen Kerberos-Implementierungen	**Produkte und Technologien von Microsoft** sind auf breiter Basis interoperabel mit anderen Standard-Kerberos-Implementierungen für die native Authentifizierung, einseitige Vertrauensstellungen, Dienstkonten, beidseitige Vertrauensstellungen und Szenarien zur Clientkonfiguration. Windows Server unterstützt Kerberos mit verschiedenen Sicherheits- und Identitätsauthentifizierungsanwendungen, die auf verschiedenen UNIX-Betriebssystemen sowie unter Linux, IBM WebSphere und Jboss laufen.	Kerberos, SPNEGO	• http://www.microsoft.com/windows2000/docs/Kerbinterop.doc
Single-Sign-On mit Computern ermöglichen, die UNIX und Linux als Betriebssystemen verwenden	**Active Directory** ermöglicht SSO-Szenarien mit Apache-Webservern, UNIX- und Linux-Anwendungen, IBM WebSphere und BEA WebLogic-Anwendungsservern. Genauso sind SSO-Szenarien mit UNIX-Fileshares und anderen Datenbanken realisierbar, die Drittanbieterlösungen von Quest und Centrify verwenden.	DNS, Kerberos, HTTP, IP, LDAP, SOAP, TCP, WS-*, XML	• http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
Web-Single-Sign-On für verschiedenen Webserver-Anwendungen ermöglichen	**Active Directory Federation Services (ADFS) in Windows Server 2003 R2** können von Drittanbietern erweitert werden, um ein Web-SSO zwischen den Internet Information Services (IIS) und anderen Webserver-Anwendungen zu ermöglichen. Das schließt auch die ADFS-Authentifizierung für Java-Anwendungen in der Ressourcendomäne mit ein, was es Java-Anwendungsservern gestattet, durch die Identity Federation bei Java-Anwendungen innerhalb einer ADFS-basierten „Trust Fabric“ (vertrauenswürdigen Struktur) von einer bestehenden ADFS-Struktur zu profitieren. Des Weiteren werden NTLM und SPNEGO unterstützt. Die WS-Federation-basierte Authentifizierung bietet ebenfalls ein plattformübergreifendes Äquivalent zum ADFS-Agenten für IIS für solche Webserver, die mit Apache-, WebLogic-, Tomcat-, WebSphere- und Jboss-Software arbeiten.	DNS, HTTP, IP, Kerberos, LDAP, NTLM, SAML 1.1 Token Profile, SPNEGO, TCP, WS-Federation, WS-Federation Passive Requestor Profile, WS-Federation Passive Requestor Interoperability Profile, X.509	• http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspx