

## Executive Summary

Over the years, IT environments have become more complex and more heterogeneous due to diverse customer needs and rapid innovation in the IT industry. Business and government customers frequently manage multiple security and directory services, which involve a wide array of software and hardware requirements.

**To address this issue, Microsoft delivers interoperability by design.**

Microsoft's approach to interoperability increases the value of IT solutions by providing security and identity solutions that integrate easily and reliably with other technology platforms.

## What is Security and Identity Integration?

It's all about providing more secure, reliable, and private computing experiences. Security and identity integration is:

- **Providing identity authentication technologies** that include support for Kerberos authentication, public key infrastructure, X.509 certificates, SAML 1.1 Tokens, and Web services standards.
- **Helping safeguard users from malicious software** such as computer viruses, phishing, and other malicious software through enhanced security features, industry collaboration, and support for industry standards.
- **Enabling enterprise single sign-on scenarios** that are cross-platform and language independent through protocol-based technologies and standardized Web services implementations.
- **Building more secure and reliable systems** with products like Microsoft® Forefront™, Identity Integration Server, Windows Vista™, and Microsoft Windows Server®.

## Microsoft Supports Security and Identity Integration

For customers who manage heterogeneous IT systems, Microsoft delivers security and identity integration four ways:

- **Products:** Providing innovative tools and technologies for developers that enable interoperable solutions based on industry standards for security, encryption, and identity meta-systems.
- **Community:** Working together with customers, partners, and competitors to share security information and to develop integrated solutions for enterprise single sign-on and identity authentication and federation.
- **Access:** Licensing technology assets to and from other companies and offering key Microsoft technologies including Sender ID Framework, Virtual Hard Disk (VHD) Image Format Specification, and 38 Web services standards under the Open Specification Promise.
- **Standards:** Supporting industry and technical standards for security and encryption protocols and actively participating with leading standards-setting organizations to promote technology adoption.

## Microsoft Supports Standards

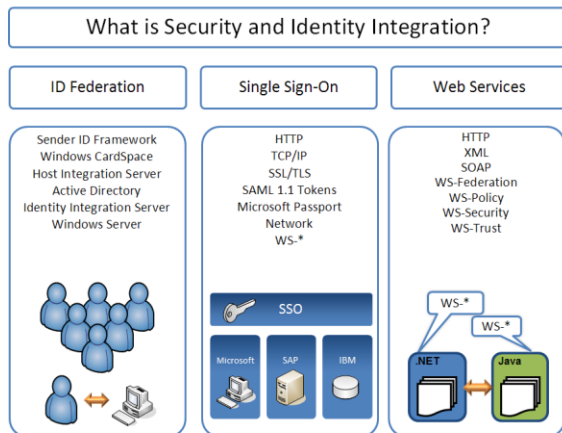
- **Microsoft products and technologies support hundreds of technical standards** such as AES, DHCP, Kerberos protocol, HTTP, IP, IPSec, PKI, SAML 1.1 Token Profile, SSL, TCP, TLS, WPA Security, WS-\*, and X.509.
- **Microsoft is actively engaged with more than 100 national and international standards-setting organizations** including ECMA, ETSI, OASIS, IEEE, IETF, ISO/IEC JTC1, ITU, and W3C.
- **Microsoft engineers have authored or co-authored dozens of industry specifications and standards** such as WS-Addressing, WS-I Basic Profile, WS-Policy, WS-ReliableMessaging, WS-SecureConversation, WS-Security, WS-SecurityPolicy, and WS-Trust.
- **Microsoft is working with industry** to define a new generation of software and Web services based on eXtensible Markup Language (XML).

## Meeting the Challenge of Security and Identity Integration

- Trustworthy Computing (TwC) is a core corporate value at Microsoft and guides almost everything we do. TwC includes four pillars: Security, Privacy, Reliability, and Business Practices.
- Microsoft provides guidance for secure coding practices in the IT industry through the TwC Secure Development Lifecycle (SDL).
- Microsoft products enable a wide range of single sign-on scenarios for online transactions, host systems, and heterogeneous enterprise environments.
- Windows® CardSpace provides a consistent way to work with multiple digital identities, regardless of the kinds of security tokens they use.
- To foster the exchange of security information in the IT industry, Microsoft participates in the Global Infrastructure Alliance for Internet Safety (GIAIS), the Microsoft Virus Initiative (MVI), the Microsoft Security Response and Safety Summit (MSRSS), the Virus Information Alliance (VIA), the Microsoft Security Cooperation Program (MSCP), and the Microsoft Security Support Alliance (MSSA).

## For More Information, Visit:

- Trustworthy Computing <http://www.microsoft.com/mscorp/twc/default.aspx>
- Microsoft Identity Integration Server <http://www.microsoft.com/windowsserversystem/miis2003/default.aspx>
- Windows CardSpace (formerly InfoCard) <http://msdn.microsoft.com/windowsvista/reference/default.aspx?pull=/library/en-us/dnlong/html/IntroInfoCard.asp>
- Find more [www.microsoft.com/interop](http://www.microsoft.com/interop)



Use Case Scenarios	Microsoft Solutions	Standards Supported in Microsoft Products	For More Information, Visit
Integrate ID authentication and management systems	<b>Microsoft Identity Integration Server (MIIS)</b> provides a single view of a user across the enterprise. MIIS supports more than 20 account repositories including LDAP directories, databases, proprietary stores, and flat files. MIIS Management Agents can be used to connect with different directory services and applications such as eDirectory, Lotus Notes, Novell servers, Sun ONE/iPlanet Directory, and X.500 systems.	.txt files, DSML, flat files, HTTP, Kerberos protocol, LDAP, SOAP, WS-I Profiles, WS-Security	1) <a href="http://www.microsoft.com/windowsserver/system/miis2003/evaluation/overview">http://www.microsoft.com/windowsserver/system/miis2003/evaluation/overview</a>
Integrate UNIX domains and passwords with Windows directory services	<b>The Windows Server 2003 R2</b> operating system provides identity management solutions as part of its integration with UNIX-based systems to help establish uninterrupted user access and efficient management of network resources across operating systems. These solutions include Server for NIS, which helps integrate Windows and UNIX-based Network Information Service (NIS) servers; and Password Synchronization, which helps simplify the process of maintaining secure passwords.	IP, HTTP, POSIX standards, TCP	1) <a href="http://www.microsoft.com/windowsserver2003/r2/identitymanagement">http://www.microsoft.com/windowsserver2003/r2/identitymanagement</a>
Integrate security across Windows-based systems	<b>Microsoft Forefront</b> client security is a comprehensive line of business security products that help safeguard Windows-based systems through integration with existing IT infrastructure and through simplified deployment, management, and analysis. The Microsoft Forefront line of business security products helps safeguard client machines, server applications, and the network edge.	802.1X, DCOM, DHCP, IPsec, SMTP	1) <a href="http://www.microsoft.com/forefront">http://www.microsoft.com/forefront</a>
Enable enterprise single sign-on with host systems	<b>Microsoft Host Integration Server and Microsoft BizTalk® Server</b> support an extension of Windows-based enterprise security integration called Enterprise Single Sign-On (SSO). Enterprise SSO provides user account and password mapping and caching, single sign-on to multiple Windows domains and host security systems, and password synchronization to simplify account administration. Enterprise SSO offers a means to efficiently map accounts across Windows-based Active Directory® services and host systems or line-of-business applications, and it supports one-to-one and many-to-one associations.	DRDA, HTTP, Kerberos protocol, LU 6.2 protocol, SNA, SOAP, WS-*, X.509, XML	1) <a href="http://download.microsoft.com/download/C/6/5/C65FF9FD-0ED7-47F6-91AB-000E6265EA5B/Enterprise_SSO_Whitepaper.doc">http://download.microsoft.com/download/C/6/5/C65FF9FD-0ED7-47F6-91AB-000E6265EA5B/Enterprise_SSO_Whitepaper.doc</a>
Enable identity federation across WS-Federation and Liberty Alliance ID-FF Web services-based architectures	<b>The Web Single Sign-On Interoperability Profile (Web SSO Interop Profile)</b> defines an interoperability profile of the Web Single Sign-On Metadata Exchange Protocol (Web SSO MEX) that allows the use of identity providers based on Liberty Alliance Identity Federation Framework (Liberty Alliance ID-FF) or WS-Federation to interact with an ID authentication service.	Liberty Alliance ID-FF, WS-Federation, Web SSO Interop Profile, Web SSO MEX	1) <a href="http://msdn.microsoft.com/library/en-us/dnglobspec/html/webssso.pdf">http://msdn.microsoft.com/library/en-us/dnglobspec/html/webssso.pdf</a>
Help safeguard users from spam and phishing scams	<b>The Microsoft Sender ID Framework</b> was created to counter e-mail domain spoofing and to provide better protection against phishing schemes. The Sender ID Framework checks the sender's server IP address to verify that each e-mail message originates from the Internet domain from which it claims to originate. Eliminating domain spoofing will help legitimate senders safeguard their domain names and reputations, and it will help recipients more effectively identify and filter junk e-mail and phishing scams.	DNS, HTTP, IP, SIDS, SMTP, SPF, TCP	1) <a href="http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspix">http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspix</a>
Allow users to manage their digital identities from various identity providers to access online services	<b>Windows CardSpace (formerly InfoCard)</b> is a component of the Microsoft .NET Framework version 3.0 that builds on the mechanisms described in WS-Trust, WS-SecurityPolicy, and WS-MetadataExchange. With Windows CardSpace, digital identity can be integrated into a token issuance and consumption framework that promotes interoperability between identity providers and relying parties and that gives the user better control of their digital identity.	DNS, HTTP, Kerberos protocol, SAML 1.1 Token Profile, SOAP, WS-MetadataExchange, WS-Security, WS-SecurityPolicy, WS-Trust, X.509, XML	1) <a href="http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx">http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx</a> 2) <a href="http://msdn2.microsoft.com/en-us/library/aa480189.aspx">http://msdn2.microsoft.com/en-us/library/aa480189.aspx</a>
Integrate smart card identity systems with Windows-based systems	<b>Windows and Windows Server</b> support the use of a variety of smart cards to authenticate console logon for remote access and administrator access. The Active Directory service in Windows Server 2003 offers built-in support for verifying smart card interactive logon capabilities and the ability to map accounts to certificates. Mapping user accounts to certificates ties the private key on the smart card to the certificate held in Active Directory.	EAP-TLS, FTP, HTTP, IP, Kerberos protocol, LDAP, PKI, PPP, SMTP, SSL, TCP, UTF-8, X.509	1) <a href="http://www.microsoft.com/tech/net/security/guidance/networksecurity/securesmartcards/default.mspix">http://www.microsoft.com/tech/net/security/guidance/networksecurity/securesmartcards/default.mspix</a>
Interoperate with other Kerberos implementations	<b>Microsoft products and technologies</b> are broadly interoperable with other standard Kerberos implementations for native authentication, one-way trust, service account, two-way trust, and client configuration scenarios. Windows Server supports Kerberos functionality with different security and identity authentication applications running on different UNIX operating systems, Linux, IBM WebSphere, and JBoss.	Kerberos protocol, SPNEGO	1) <a href="http://www.microsoft.com/windows2000/docs/Kerbinterop.doc">http://www.microsoft.com/windows2000/docs/Kerbinterop.doc</a>
Enable single sign-on with computers running UNIX and Linux operating systems	<b>Active Directory</b> enables SSO scenarios with Apache Web server; UNIX and Linux applications; IBM WebSphere and BEA WebLogic application servers; UNIX file shares; and other databases that use third-party support from Quest and Centrifuy.	DNS, Kerberos protocol, HTTP, IP, LDAP, SOAP, TCP, WS-*, XML	1) <a href="http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspix">http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspix</a>
Enable Web single sign-on across various Web server applications	<b>Active Directory Federation Services (ADFS) in Windows Server 2003 R2</b> can be extended with third-party support to enable Web SSO between Internet Information Services (IIS) and other Web server applications. This includes ADFS authentication for Java applications in the resource domain, allowing Java application servers to capitalize on an existing ADFS infrastructure, enabling the federation of Java applications within an ADFS-based trust fabric, and supporting NTLM and SPNEGO. WS-Federation-based authentication also provides a cross-platform equivalent of the ADFS Agent for IIS for Web servers running Apache, WebLogic, Tomcat, WebSphere, and JBoss software.	DNS, HTTP, IP, Kerberos protocol, LDAP, NTLM, SAML 1.1 Token Profile, SPNEGO, TCP, WS-Federation, WS-Federation Passive Requestor Profile, WS-Federation Passive Requestor Interoperability Profile, X.509	1) <a href="http://www.microsoft.com/WindowsServer2003/R2/IdentityManagement/ADFSwhitepaper.mspix">http://www.microsoft.com/WindowsServer2003/R2/IdentityManagement/ADFSwhitepaper.mspix</a>