
# Microsoft Open Specification Promise

Published: September 12, 2006 | Updated: October 23, 2006

Microsoft irrevocably promises not to assert any Microsoft Necessary Claims against you for making, using, selling, offering for sale, importing or distributing any implementation to the extent it conforms to a Covered Specification ("Covered Implementation"), subject to the following. This is a personal promise directly from Microsoft to you, and you acknowledge as a condition of benefiting from it that no Microsoft rights are received from suppliers, distributors, or otherwise in connection with this promise. If you file, maintain or voluntarily participate in a patent infringement lawsuit against a Microsoft implementation of such Covered Specification, then this personal promise does not apply with respect to any Covered Implementation of the same Covered Specification made or used by you. To clarify, "Microsoft Necessary Claims" are those claims of Microsoft-owned or Microsoft-controlled patents that are necessary to implement only the required portions of the Covered Specification that are described in detail and not merely referenced in such Specification. "Covered Specifications" are listed below.

This promise is not an assurance either (i) that any of Microsoft's issued patent claims covers a Covered Implementation or are enforceable or (ii) that a Covered Implementation would not infringe patents or other intellectual property rights of any third party. No other rights except those expressly stated in this promise shall be deemed granted, waived or received by implication, exhaustion, estoppel, or otherwise.

# Covered Specifications (the promise applies individually to each of these specifications)

**Web Services**

This promise applies to all existing versions of the following specifications. Many of these specifications are currently undergoing further standardization in certain standards organizations. To the extent that Microsoft is participating in those efforts, this promise will apply to the specifications that result from those activities (as well as the existing versions).

Remote Shell Web Services Protocol
SOAP
SOAP 1.1 Binding for MTOM 1.0
SOAP MTOM / XOP
SOAP-over-UDP
Web Single Sign-On Interoperability Profile
Web Single Sign-On Metadata Exchange Protocol
WS-Addressing
WS-AtomicTransaction
WS-BusinessActivity
WS-Coordination
WS-Discovery
WSDL
WSDL 1.1 Binding Extension for SOAP 1.2
WS-Enumeration
WS-Eventing
WS-Federation
WS-Federation Active Requestor Profile
WS-Federation Passive Requestor Profile
WS-I Basic Profile
WS-Management
WS-Management Catalog
WS-MetadataExchange
WS-Policy
WS-PolicyAttachment
WS-ReliableMessaging
WS-RM Policy
WS-SecureConversation
WS-Security: Kerberos Binding
WS-Security: Kerberos Token Profile
WS-Security: Rights Expression Language (REL) Token Profile
WS-Security: SAML Token profile
WS-Security: SOAP Message Security
WS-Security: UsernameToken Profile
WS-Security: X.509 Certificate Token Profile
WS-SecurityPolicy
WS-Transfer
WS-Trust

**Virtualization Specifications**

Virtual Hard Disk (VHD) Image Format Specification

**Security**

RFC 4406 - Sender ID: Authenticating E-Mail
RFC 4408 - Sender Policy Framework: Authorizing Use of Domains in “Mail From”
RFC 4407 - Purported Responsible Address in E-Mail Messages
RFC 4405 - SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail

Message

**Office XML File Formats**

Office 2003 XML Reference Schemas
Office Open XML 1.0 proposed Ecma standard

# Frequently Asked Questions

The Open Specification Promise is a simple and clear way to assure that the broadest audience of developers and customers working with commercial or open source software can implement specifications through a simplified method of sharing of technical assets, while recognizing the legitimacy of intellectual property.

We listened to feedback from community representatives who made positive comments regarding the acceptability of this approach.

**OSP GENERAL**

**Q: Why did Microsoft take this approach?**

A: It was a simple, clear way, after looking at many different licensing approaches, to reassure a broad audience of developers and customers that the specification(s) could be used for free, easily, now and forever.

**Q: How does the Open Specification Promise work? Do I have to do anything in order to get the benefit of this OSP?**

A: No one needs to sign anything or even reference anything. Anyone is free to implement the specification(s), as they wish and do not need to make any mention of or reference to Microsoft. Anyone can use or implement these specification(s) with their technology, code, solution, etc. You must agree to the terms in order to benefit from the promise; however, you do not need to sign a license agreement, or otherwise communicate your agreement to Microsoft.

**Q: What is covered and what is not covered by the Open Specification Promise?**

A: The OSP covers each individual specification designated on the public list posted at http://www.microsoft.com/interop/osp/. The OSP applies to anyone who is building software and or hardware to implement one or more of those specification(s). You can choose to implement all or part of the specification(s). The OSP does not apply to any work that you do beyond the scope of the covered specification(s).

**Q: If a listed specification has been approved by a standards organization, what patent rights is Microsoft providing?**

A: We are providing access to necessary claims consistent with the scope of our commitments in that organization.

**Q: What if I don't implement the entire specification? Will I still get the protections under the OSP?**

A: The OSP applies whether you have a full or partial implementation. You get the same irrevocable promise from us either way. In all cases, the OSP covers only your implementation of the parts of the specification(s) that you decide to use.

**Q: Does this OSP apply to all versions of the standard, including future revisions?**

A: The Open Specification Promise applies to all existing versions of the specification(s) designated on the public list posted at http://www.microsoft.com/interop/osp/, unless otherwise noted with respect to a particular specification (see, for example, specific notes related to web services specifications).

**Q: Why doesn't the OSP apply to things that are merely referenced in the specification?**

A: It is a common practice that technology licenses focus on the specifics of what is detailed in the specification(s) and exclude what are frequently called "enabling technologies." If we included patent claims to the enabling technology, then as an extreme example, it could be argued that one needs computer and operating system patents to implement almost any information technology specification. No such broad patent licenses to referenced technologies are ever given for specific industry standards.

**Q: Is this OSP sub-licensable?**

A: There is no need for sublicensing. This promise is directly applicable to you and everyone else who wants to use it. Accordingly, your distributees, customers and vendors can directly take advantage of this same promise, and have the exact same protection that you have.

**Q: Is this Promise consistent with open source licensing, namely the GPL? And can anyone implement the specification(s) without any concerns about Microsoft patents?**

A: The Open Specification Promise is a simple and clear way to assure that the broadest audience of developers and customers working with commercial or open source software can implement the covered specification(s). We leave it to those implementing these technologies to understand the legal environments in which they operate. This includes people operating in a GPL environment. Because the General Public License (GPL) is not universally interpreted the same way by everyone, we can't give anyone a legal opinion about how our language relates to the GPL or other OSS licenses, but based on feedback from the open source community we believe that a broad audience of developers can implement the specification(s).

**SECURITY**

**Q: Why are putting Sender ID under the OSP now?**

A: In September of this year, Microsoft announced a new approach to the availability of open specifications. At the time we announced the application of the Open Specification Promise to 38 Web services specifications and earlier this month we expanded it to include the Virtual Hard Disk Image Format specification. At this point, we think we can promote further industry interoperability among all commercial software solutions that utilize email authentication, including open source solutions by making Sender ID more clearly available to the entire internet ecosystem including customers, partners, ISPs, registrars and the developer community. This approach complements Microsoft's

broader commitment to combat the spread of spam, phishing, malware and other exploits in email, as well as interoperability, which we achieve in part through enabling access to our technology.

**Q: Are you making Sender ID available under the OSP because you received so much criticism for your original licensing approach to the spec?**

A: We recognize that there are lingering questions from some members of the development community about Microsoft's licensing terms and how those terms may affect developers' ability to implement Sender ID. It is important to note that great progress has already been made on email authentication worldwide with more than 5 million domain holders adopting Sender ID as a best practice today. Sender ID helps protect brands, reduce spam, and counter email exploits. The OSP is a simple, clear way to reassure a broad audience of developers and customers that any Microsoft patents ever needed to implement all or part of the specification could be used for free, easily, now and forever.

**Q: What's the significance of the OSP for Sender ID?**

A: By extending the OSP to the Sender ID format, Microsoft will help the industry combat e-mail spoofing and phishing by fostering greater interoperability among all commercial software solutions for email authentication, including open source-based solutions. Implementers of the Sender ID Framework will not need to be concerned about signing a license in order to implement the anti-spoofing and anti-phishing technology. This approach also complements Microsoft's broader commitment to interoperability, which we achieve in part through enabling access to our technology.

- Microsoft is committed to working with the IT industry and businesses to help protect consumers and businesses from the blight of online threats. The Sender ID Framework is an e-mail authentication specification that helps address domain spoofing – a common tactic used for the spread of spam, phishing, malware and other exploits in email – by verifying the domain name from which an e-mail is sent.
- After nearly two years of worldwide deployment to over 600 million users, Sender ID already enjoys broad industry support, with approximately 36% of all legitimate email sent worldwide Sender ID compliant and an estimated 5.5 million domains worldwide protected by Sender ID. Adoption of the Fortune 500 has increased from 7% a year ago to over 23% today
- Email authentication and the ability of validating the identity has become critical in the face of the increase sophistication and online threats being propagated. With Sender ID senders and receiving networks are afforded an additional layer of safety and security from these exploits.
- Sender ID provides significant business value at no cost and impact to performance. Today business throughout the world are realizing enhanced brand and user protection while realizing improved deliverability of legitimate email. With the addition of Sender ID and the sender's reputation, false positive are able to be reduced to nearly zero while false negatives being reduced by over 80%.

**Q: Where can I download the Sender ID specifications?**

A:
RFC 4406 - Sender ID: Authenticating E-Mail
RFC 4408 - Sender Policy Framework: Authorizing Use of Domains in “Mail From”
RFC 4407 - Purported Responsible Address in E-Mail Messages
RFC 4405 - SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message

**Office XML File Formats**

**Q: What are you doing by adding Ecma Office Open XML to the OSP?**

A: We are giving potential implementers of Ecma Office Open XML the ability to take advantage of either the CNS or the OSP, at their choice. Microsoft had already stated that it offers an irrevocable covenant not to sue (CNS) to anyone wishing to implement the formats. We understand that some may prefer the new OSP, which we’d like to facilitate.

**Q: Why are you doing this now?**

A: In September, the Ecma Technical Committee created the Final Draft of the Office Open XML v1.0 formats so we want to address any questions people may have with respect to their ability to use our patent rights that are necessary to implement Ecma Office Open XML. We don’t want there to be any open issues with respect to access to necessary Microsoft patent claims.

**Q: Why are you applying both the CNS and the OSP?**

A: Some have asked whether we would apply the OSP to Ecma Office Open XML. We don’t know whether some will choose the OSP over the CNS, but we want to make that an option.

# Feedback From Representatives of the Community

**OSP GENERAL**

**"Red Hat believes that the text of the OSP gives sufficient flexibility to implement the listed specifications in software licensed under free and open source licenses. We commend Microsoft's efforts to reach out to representatives from the open source community and solicit their feedback on this text, and Microsoft's willingness to make modifications in response to our comments."**

Mark Webbink
Deputy General Counsel
Red Hat, Inc.

**"I see Microsoft's introduction of the OSP as a good step by Microsoft to further enable collaboration between software vendors and the open source community. This OSP enables the open source community to implement these standard specifications without having to pay any royalties to Microsoft or sign a license agreement. I'm pleased that this OSP is compatible with free and open source licenses."**

Lawrence Rosen
Rosenlaw & Einschlag, a technology law firm (www.rosenlaw.com)
Stanford University, Lecturer in Law
3001 King Ranch Road, Ukiah, CA 95482
707-485-1242 * fax: 707-485-1243
Author of "Open Source Licensing: Software Freedom and Intellectual Property Law" (Prentice Hall 2004)

**"The Microsoft open specification promise is a very positive development. In the university and open source communities, we need to know that we can implement specifications freely. This promise will make it easier for us to implement Web Services protocols and information cards and for them to be used in our communities."**

RL "Bob" Morgan
Chair, Middleware Architecture Committee for Education (MACE)
Senior Technology Architect, University of Washington

**SECURITY**

**"E-mail security is critical to safeguarding consumer confidence online. It's important that the entire community adopt interoperable, easy-to-implement and low-cost platforms to encourage broad adoption of tools to combat e-mail spoofing and phishing scams. We commend Microsoft in its effort to foster improved industry cooperation."**

Ramesh Lakshmi Ratan
Executive Vice President and Chief Operating Officer
Direct Marketing Association (DMA)

**"The ESPC members have long recognized the need for strong spam solutions that help ensure the delivery of legitimate e-mail, and we welcome Microsoft's announcement today as another positive step for the delivery of safe and authentic e-mails."**

Trevor Hughes
Executive Director
Email Sender & Provider Coalition (ESPC)

**"As a leading Internet gateway security provider, we are interested in seeing the best anti-spam products get to market to improve trust and confidence in e-mail. Moving the Sender ID specification under the OSP is an important move by Microsoft, and we hope it will result in widespread adoption across the industry."**

Patrick Peterson
Vice President, Technology
IronPort Systems Inc.

**"Sender authentication technologies like Sender ID are important tools that help ensure e-mail security, and by making Sender ID available under the OSP, Microsoft is addressing the interoperability needs of heterogeneous e-mail infrastructures. We're pleased to see this development and believe it's a positive step in the fight against spoofing, phishing and other categories of unwanted messaging."**

Eric Allman
Chief Science Officer
Sendmail Inc.