

## [MS-MWBE]:

# Microsoft Web Browser Federated Sign-On Protocol Extensions

---

### Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](#) or the [Microsoft Community Promise](#). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the [Patent Map](#).
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights.** All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

**Tools.** The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

**Support.** For questions and support, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

## Revision Summary

Date	Revision History	Revision Class	Comments
10/22/2006	0.01	New	Version 0.01 release
1/19/2007	1.0	Major	Version 1.0 release
3/2/2007	1.1	Minor	Version 1.1 release
4/3/2007	1.2	Minor	Version 1.2 release
5/11/2007	1.3	Minor	Version 1.3 release
6/1/2007	1.3.1	Editorial	Changed language and formatting in the technical content.
7/3/2007	1.3.2	Editorial	Changed language and formatting in the technical content.
7/20/2007	1.3.3	Editorial	Changed language and formatting in the technical content.
8/10/2007	1.4	Minor	Clarified the meaning of the technical content.
9/28/2007	1.4.1	Editorial	Changed language and formatting in the technical content.
10/23/2007	1.5	Minor	Clarified the meaning of the technical content.
11/30/2007	1.6	Minor	Clarified the meaning of the technical content.
1/25/2008	1.6.1	Editorial	Changed language and formatting in the technical content.
3/14/2008	1.6.2	Editorial	Changed language and formatting in the technical content.
5/16/2008	1.6.3	Editorial	Changed language and formatting in the technical content.
6/20/2008	1.6.4	Editorial	Changed language and formatting in the technical content.
7/25/2008	1.6.5	Editorial	Changed language and formatting in the technical content.
8/29/2008	1.6.6	Editorial	Changed language and formatting in the technical content.
10/24/2008	2.0	Major	Updated and revised the technical content.
12/5/2008	3.0	Major	Updated and revised the technical content.
1/16/2009	3.0.1	Editorial	Changed language and formatting in the technical content.
2/27/2009	3.0.2	Editorial	Changed language and formatting in the technical content.
4/10/2009	3.0.3	Editorial	Changed language and formatting in the technical content.
5/22/2009	3.1	Minor	Clarified the meaning of the technical content.
7/2/2009	4.0	Major	Updated and revised the technical content.
8/14/2009	5.0	Major	Updated and revised the technical content.
9/25/2009	5.1	Minor	Clarified the meaning of the technical content.
11/6/2009	5.1.1	Editorial	Changed language and formatting in the technical content.
12/18/2009	5.1.2	Editorial	Changed language and formatting in the technical content.
1/29/2010	5.2	Minor	Clarified the meaning of the technical content.

<b>Date</b>	<b>Revision History</b>	<b>Revision Class</b>	<b>Comments</b>
3/12/2010	5.2.1	Editorial	Changed language and formatting in the technical content.
4/23/2010	5.2.2	Editorial	Changed language and formatting in the technical content.
6/4/2010	5.2.3	Editorial	Changed language and formatting in the technical content.
7/16/2010	6.0	Major	Updated and revised the technical content.
8/27/2010	6.0	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2010	6.0	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	6.0	None	No changes to the meaning, language, or formatting of the technical content.
1/7/2011	7.0	Major	Updated and revised the technical content.
2/11/2011	7.0	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	7.0	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	7.0	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	7.1	Minor	Clarified the meaning of the technical content.
9/23/2011	7.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	8.0	Major	Updated and revised the technical content.
3/30/2012	8.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	8.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	8.0	None	No changes to the meaning, language, or formatting of the technical content.
1/31/2013	8.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	9.0	Major	Updated and revised the technical content.
11/14/2013	9.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	9.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	9.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	10.0	Major	Significantly changed the technical content.
7/14/2016	10.0	None	No changes to the meaning, language, or formatting of the technical content.

<b>Date</b>	<b>Revision History</b>	<b>Revision Class</b>	<b>Comments</b>
6/1/2017	11.0	Major	Significantly changed the technical content.

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Glossary .....	7
1.2	References .....	10
1.2.1	Normative References .....	10
1.2.2	Informative References .....	11
1.3	Overview .....	11
1.3.1	Query String Response Transfer Protocol .....	11
1.3.2	SAML 1.1 Assertion Extension .....	12
1.4	Relationship to Other Protocols .....	12
1.5	Prerequisites/Preconditions .....	12
1.6	Applicability Statement .....	12
1.7	Versioning and Capability Negotiation .....	12
1.8	Vendor-Extensible Fields .....	13
1.9	Standards Assignments.....	13
<b>2</b>	<b>Messages.....</b>	<b>14</b>
2.1	Transport.....	14
2.1.1	Query String Response Transfer Protocol .....	14
2.2	Message Syntax.....	14
2.2.1	XML Namespace References.....	14
2.2.2	Query String Response Transfer Protocol .....	14
2.2.2.1	wsignin1.0 Message .....	14
2.2.2.1.1	Common Parameters .....	14
2.2.2.1.2	wsignin1.0 Response .....	14
2.2.3	SAML 1.1 Assertion Extension .....	15
2.2.3.1	SAML Advice Elements.....	15
2.2.3.2	WindowsIdentifiers Structure.....	15
2.2.3.2.1	WindowsIdentifierFlags Structure .....	16
2.2.3.2.2	PACKED_SIDs Structure .....	16
2.3	Directory Service Schema Elements .....	17
<b>3</b>	<b>Protocol Details.....</b>	<b>18</b>
3.1	IP/STS Details .....	18
3.1.1	Abstract Data Model.....	18
3.1.1.1	Query String Response Transfer Protocol .....	18
3.1.1.1.1	Pending Result .....	18
3.1.1.1.2	Maximum Query String Response Message Length.....	18
3.1.2	Timers .....	19
3.1.3	Initialization.....	19
3.1.4	Higher-Layer Triggered Events .....	19
3.1.5	Processing Events and Sequencing Rules .....	19
3.1.5.1	Query String Response Transfer Protocol .....	19
3.1.5.1.1	Receiving a wsignin1.0 Request That Does Not Specify a ttpindex .....	19
3.1.5.1.2	Receiving a wsignin1.0 Request That Specifies a ttpindex of 0 .....	19
3.1.5.1.3	Receiving a wsignin1.0 Request That Specifies a ttpindex Other Than 0 .....	19
3.1.5.1.4	Responding to a wsignin1.0 Request That Specifies a ttpindex .....	20
3.1.5.2	SAML 1.1 Assertion Extension.....	20
3.1.5.2.1	Responding to a wsignin1.0 Request .....	20
3.1.5.2.1.1	ClaimSource Element .....	20
3.1.5.2.1.2	CookieInfoHash Element .....	20
3.1.5.2.1.3	WindowsUserIdentifier Element .....	21
3.1.5.2.1.4	WindowsUserName Element .....	21
3.1.5.2.1.5	WindowsIdentifiers Element .....	21
3.1.6	Timer Events.....	21
3.1.7	Other Local Events.....	21

3.2	Relying Party Details .....	21
3.2.1	Abstract Data Model.....	21
3.2.1.1	Query String Response Transfer Protocol .....	21
3.2.1.1.1	Aggregated Result .....	21
3.2.2	Timers .....	21
3.2.3	Initialization.....	22
3.2.4	Higher-Layer Triggered Events .....	22
3.2.5	Processing Events and Sequencing Rules .....	22
3.2.5.1	Query String Response Transfer Protocol .....	22
3.2.5.1.1	Sending a wsignin1.0 Request.....	22
3.2.5.1.2	Receiving a wsignin1.0 Response That Does Not Specify a ttpindex .....	22
3.2.5.1.3	Receiving a wsignin1.0 Response That Specifies a ttpindex .....	22
3.2.5.1.4	Processing the Complete Aggregated Result.....	23
3.2.5.2	SAML 1.1 Assertion Extension.....	23
3.2.6	Timer Events.....	23
3.2.7	Other Local Events.....	23
3.3	Web Browser Requestor Details .....	23
3.3.1	Abstract Data Model.....	23
3.3.2	Timers .....	24
3.3.3	Initialization.....	24
3.3.4	Higher Layer Triggered Events .....	24
3.3.5	Processing Events and Sequencing Rules .....	24
3.3.6	Timer Events.....	24
3.3.7	Other Local Events.....	24
<b>4</b>	<b>Protocol Examples .....</b>	<b>25</b>
4.1	Query String Response Transfer Protocol.....	25
4.1.1	Annotated Example.....	25
4.1.2	Full Network Trace .....	28
4.2	SAML 1.1 Assertion Extension.....	42
<b>5</b>	<b>Security .....</b>	<b>44</b>
5.1	Security Considerations for Implementers .....	44
5.1.1	Data Integrity .....	44
5.1.2	Privacy .....	44
5.1.3	Authorization Validation and Filtering .....	44
5.2	Index of Security Parameters .....	44
<b>6</b>	<b>Appendix A: Product Behavior .....</b>	<b>45</b>
<b>7</b>	<b>Change Tracking.....</b>	<b>49</b>
<b>8</b>	<b>Index.....</b>	<b>50</b>

# 1 Introduction

This specification extends the Microsoft Web Browser Federated Sign-On Protocol described in [\[MS-MWBF\]](#). It is assumed that the reader is familiar with its terms, concepts, and protocols.

The extensions defined in this specification enable **web browser requestors** that do not support scripting (to create POST messages) and enable passing **security identifiers (SIDs)** in Security Assertion Markup Language (SAML) 1.1 assertions. These extensions are referred to, respectively, as the Query String Response Transfer Protocol and the SAML 1.1 Assertion Extension.

The Microsoft Web Browser Federated Sign-On Protocol specifies the use of HTTP POST to transmit the **wsignin1.0** result. The use of HTTP POST requires web browser requestors to support scripting for automated form submittal, but web browser requestors do not always have scripting support. The Query String Response Transfer Protocol provides a method for using a series of HTTP GET messages instead of a single HTTP POST to transmit the result of a wsignin1.0 action. This eliminates the scripting requirement for the web browser requestor. That is, the extension increases the number of messages needed to perform a wsignin1.0 action to avoid the POST message.

The SAML 1.1 Assertion Extension is an extension of the Microsoft Web Browser Federated Sign-On Protocol that specifies a method for transmitting SIDs as elements in **SAML advice**.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

## 1.1 Glossary

This document uses the following terms:

**account:** A **user** (including machine account), group, or alias object. Also a synonym for security principal or principal.

**Active Directory:** A general-purpose network directory service. **Active Directory** also refers to the Windows implementation of a directory service. **Active Directory** stores information about a variety of objects in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in **Active Directory**. **Active Directory** is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [\[MS-ADTS\]](#) describes both forms. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5.2, **Lightweight Directory Access Protocol (LDAP)** versions 2 and 3, Kerberos, and DNS.

**aggregated result:** The assembly of received parts transferred using the Query String Response Transfer Protocol. The **aggregated result** is assembled at a **relying party** and might not represent the complete result if all parts have not been received. Once complete, the **relying party** extracts a **RequestSecurityTokenResponse (RSTR)** from the **aggregated result**. For more information, see section 3.2.1.1.1.

**base64 encoding:** A binary-to-text encoding scheme whereby an arbitrary sequence of bytes is converted to a sequence of printable ASCII characters, as described in [\[RFC4648\]](#).

**claim:** A declaration made by an entity (for example, name, identity, key, group, privilege, and capability). For more information, see [\[WSFederation1.2\]](#).

**domain:** A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a domain controller (DC) and host a member list that identifies all members of the domain, as well as optionally hosting the **Active Directory** service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5 and [\[MS-ADTS\]](#).

**forest:** One or more **domains** that share a common schema and trust each other transitively. An organization can have multiple **forests**. A **forest** establishes the security and administrative boundary for all the objects that reside within the **domains** that belong to the **forest**. In contrast, a **domain** establishes the administrative boundary for managing objects, such as users, groups, and computers. In addition, each **domain** has individual security policies and trust relationships with other **domains**.

**global group:** An **Active Directory** group that allows user objects from its own **domain** and **global groups** from its own **domain** as members. Also called domain global group. **Universal groups** can contain **global groups**. A group object *g* is a **global group** if and only if `GROUP_TYPE_ACCOUNT_GROUP` is present in `g!` `groupType`; see [MS-ADTS] section 2.2.12, "Group Type Flags". A **global group** that is also a security-enabled group is valid for inclusion within ACLs anywhere in the **forest**. If a **domain** is in mixed mode, then a **global group** in that **domain** that is also a security-enabled group allows only user object as members. See also domain local group, security-enabled group.

**identity provider/security token service (IP/STS):** An STS that might also be an identity provider (IP). This term is used as shorthand to see both identity that verifies token services and general token services that do not verify identity. Note that the "/" symbol implies an "or" relationship.

**Lightweight Directory Access Protocol (LDAP):** The primary access protocol for **Active Directory**. Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a directory service (DS), as described in [MS-ADTS]. The Lightweight Directory Access Protocol can be either version 2 [[RFC1777](#)] or version 3 [[RFC3377](#)].

**little-endian:** Multiple-byte values that are byte-ordered with the least significant byte stored in the memory location with the lowest address.

**NetBIOS:** A particular network transport that is part of the LAN Manager protocol suite. **NetBIOS** uses a broadcast communication style that was applicable to early segmented local area networks. A protocol family including name resolution, datagram, and connection services. For more information, see [[RFC1001](#)] and [[RFC1002](#)].

**pending result:** The transformed **RequestSecurityTokenResponse (RSTR)** that an **identity provider/security token service (IP/STS)** maintains for the duration of a Query String Response Transfer Protocol message series. Each message in the Query String Response Transfer Protocol transfers a portion of the **pending result** to the **relying party**, where the portions are assembled into the **aggregated result**. For more information, see section 3.1.1.1.1.1.

**relative identifier (RID):** The last item in the series of SubAuthority values in a **security identifier (SID)** [[SIDD](#)]. It distinguishes one account or group from all other accounts and groups in the domain. No two accounts or groups in any domain share the same RID.

**relying party (RP):** A web application or service that consumes **security tokens** issued by a security token service (STS).

**requestor IP/STS:** An **IP/STS** in the same **security realms** as the **web browser requestor**. The **requestor IP/STS** has an existing relationship with the **user** that enables it to issue **security tokens** containing **user** information.

**RequestSecurityTokenResponse (RSTR):** An XML element used to return an issued **security token** and associated metadata. An **RSTR** element is the result of the **wsignin1.0** action in the Web Browser Federated Sign-On Protocol. For more information, see [[MS-MWBE](#)] section 2.2.4.1.



**resource IP/STS:** An **IP/STS** in the same **security realm** as the **web service (WS) resource**. The **resource IP/STS** has an existing relationship with the **WS resource** that enables it to issue **security tokens** that are trusted by the **WS resource**.

**SAML advice:** The advice element of a **SAML assertion**. The data in the advice element is advisory and can be ignored without affecting the validity of the assertion. See [\[SAMLCore\]](#) section 2.3.2.2. The SAML 1.1 Assertion Extension includes **security identifiers (SIDs)** and related data in the **SAML advice** element.

**SAML assertion:** The Security Assertion Markup Language (SAML) 1.1 assertion is a standard XML format for representing a **security token**. For more information, see [\[SAMLCore\]](#) section 2.

**security identifier (SID):** An identifier for security principals that is used to identify an account or a group. Conceptually, the **SID** is composed of an account authority portion (typically a **domain**) and a smaller integer representing an identity relative to the account authority, termed the **relative identifier (RID)**. The **SID** format is specified in [\[MS-DTYP\]](#) section 2.4.2; a string representation of **SIDs** is specified in [\[MS-DTYP\]](#) section 2.4.2 and [\[MS-AZOD\]](#) section 1.1.1.2.

**security realm or security domain:** Represents a single unit of security administration or trust, for example, a Kerberos realm (for more information, see [\[RFC4120\]](#)) or a Windows Domain (for more information, see [\[MSFT-ADC\]](#)).

**security token:** A collection of one or more **claims**. Specifically in the case of mobile devices, a **security token** represents a previously authenticated user as defined in the Mobile Device Enrollment Protocol [\[MS-MDE\]](#).

**subject:** The entity to which the **claims** and other data in a **SAML assertion** apply. For more information, see [\[SAMLCore\]](#) section 1.3.1.

**trusted forest:** A forest that is trusted to make authentication statements for security principals in that forest. Assuming forest A trusts forest B, all domains belonging to forest A will trust all domains in forest B, subject to policy configuration.

**universal group:** An **Active Directory** group that allows user objects, **global groups**, and **universal groups** from anywhere in the **forest** as members. A group object g is a **universal group** if and only if GROUP\_TYPE\_UNIVERSAL\_GROUP is present in g! groupType. A security-enabled universal group is valid for inclusion within ACLs anywhere in the **forest**. If a **domain** is in mixed mode, then a **universal group** cannot be created in that **domain**. See also domain local group, security-enabled group.

**user:** A person who employs a **web browser requestor** to access a **WS resource**.

**user agent:** An HTTP user agent, as specified in [\[RFC2616\]](#).

**web browser requestor:** An HTTP 1.1 web browser client that transmits protocol messages between an **IP/STS** and a **relying party**.

**web service (WS) resource:** A destination HTTP 1.1 web application or an HTTP 1.1 resource serviced by the application. In the context of this protocol, it refers to the application or manager of the resource that receives identity information and assertions issued by an **IP/STS** using this protocol. The **WS resource** is a **relying party** in the context of this protocol. For more information, see [\[WSFederation1.2\]](#).

**wsignin1.0:** A protocol message exchange defined in [\[WSFederation1.2\]](#) sections 2.1 and 3.1. The **wsignin1.0** request and response are the HTTP binding for the WS-Trust Issue action and response; as such, the WS-Trust **RSTR** element is used to return the issued **security token** in the **wsignin1.0** response ([\[WSTrust\]](#) section 3.2). For more information, see [\[MS-MWBF\]](#) section 2.2.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## 1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](#).

### 1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[MS-ADA1] Microsoft Corporation, "[Active Directory Schema Attributes A-L](#)".

[MS-ADA3] Microsoft Corporation, "[Active Directory Schema Attributes N-Z](#)".

[MS-DTYP] Microsoft Corporation, "[Windows Data Types](#)".

[MS-MWBF] Microsoft Corporation, "[Microsoft Web Browser Federated Sign-On Protocol](#)".

[RFC1950] Deutsch, P., and Gailly, J-L., "ZLIB Compressed Data Format Specification version 3.3", RFC 1950, May 1996, <http://www.ietf.org/rfc/rfc1950.txt>

[RFC1951] Deutsch, P., "DEFLATE Compressed Data Format Specification version 1.3", RFC 1951, May 1996, <http://www.ietf.org/rfc/rfc1951.txt>

[RFC2045] Freed, N., and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996, <http://www.rfc-editor.org/rfc/rfc2045.txt>

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>

[RFC2279] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998, <http://www.rfc-editor.org/rfc/rfc2279.txt>

[RFC2396] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998, <http://www.rfc-editor.org/rfc/rfc2396.txt>

[RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, <http://www.rfc-editor.org/rfc/rfc2616.txt>

[RFC2965] Kristol, D. and Montulli, L., "HTTP State Management Mechanism", RFC 2965, October 2000, <http://www.ietf.org/rfc/rfc2965.txt>

[RFC4395] Hansen, T., et al., "Guidelines and Registration Procedures for New URI Schemes", BCP 115, RFC 4395, February 2006, <http://www.ietf.org/rfc/rfc4395.txt>

[SAMLCore] Maler, E., Mishra, P., Philpott, R., et al., "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", September 2003, <http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>

[WSFederation1.2] Kaler, C., McIntosh, M., "Web Services Federation Language (WS-Federation)", Version 1.2, May 2009, <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>

[WSFederation] Kaler, C., Nadalin, A., Bajaj, S., et al., "Web Services Federation Language (WS-Federation)", Version 1.1, December 2006, <http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf>

[XMLSCHEMA2] Biron, P.V., Ed. and Malhotra, A., Ed., "XML Schema Part 2: Datatypes", W3C Recommendation, May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>

[XML] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0 (Fourth Edition)", W3C Recommendation 16 August 2006, edited in place 29 September 2006, <http://www.w3.org/TR/2006/REC-xml-20060816/>

## 1.2.2 Informative References

[FIPS180] FIPS PUBS, "Secure Hash Standard", FIPS PUB 180-1, April 1995, <http://niatec.info/GetFile.aspx?pid=63>

[IANAScheme] IANA, "Uniform Resource Identifier (URI) Schemes per RFC4395", November 2006, <http://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml>

[MAXURL] Microsoft Corporation, "Maximum URL Length Is 2,083 Characters in Internet Explorer", September 2009, <https://support.microsoft.com/en-us/help/208427/maximum-url-length-is-2,083-characters-in-internet-explorer>

[MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](#)".

[MS-PAC] Microsoft Corporation, "[Privilege Attribute Certificate Data Structure](#)".

[MS-WPO] Microsoft Corporation, "[Windows Protocols Overview](#)".

[SIDD] Microsoft Corporation, "How Security Identifiers Work", March 2003, <http://technet.microsoft.com/en-us/library/cc778824.aspx>

## 1.3 Overview

This document specifies the Query String Response Transfer Protocol and the SAML 1.1 Assertion Extension. These extensions are based on the federated sign-on protocol described in [\[MS-MWBF\]](#). The extensions specified in this document broaden the applicability of the protocol to simpler **web browser requestors** and a wider range of protected applications. The extensions in this specification do not change the services of authentication, identity federation, or single sign-on provided by [\[MS-MWBF\]](#).

### 1.3.1 Query String Response Transfer Protocol

The scripting capability for forms submittal is not specified as part of HTTP [\[RFC2616\]](#); consequently, not all **web browser requestor** implementations support forms submittal as recommended for **wsignin1.0** responses in [\[MS-MWBF\]](#) section 2.1. In addition, the **RequestSecurityTokenResponse (RSTR)** can be too large to be transferred in a single HTTP GET message. The Query String Response Transfer Protocol addresses these issues by eliminating the web browser requestor requirement for scripting support.

When using the Query String Response Transfer Protocol, the wsignin1.0 message exchange in [\[MS-MWBF\]](#) is replaced by a series of wsignin1.0 message exchanges. In [\[MS-MWBF\]](#), the RSTR is transmitted using a single HTTP POST message. The Query String Response Transfer Protocol transmits the RSTR in pieces in query string parameters using multiple HTTP GET messages. The

**relying party** accumulates the pieces from the responses in the series to produce an **aggregated result**. When the relying party has accumulated all the pieces, it extracts the RSTR from the aggregated result.

### 1.3.2 SAML 1.1 Assertion Extension

The Microsoft Web Browser Federated Sign-On Protocol described in [\[MS-MWBF\]](#) does not specify a method for including **SIDs** in a **security token**. For applications requiring SIDs, **claims** are not sufficient for authorization.

The SAML 1.1 Assertion Extension provides a method for including SIDs in a **SAML assertion**. How an **identity provider/security token service (IP/STS)** obtains the security identifiers and how a **relying party** interprets them is implementation-specific.

## 1.4 Relationship to Other Protocols

The Web Browser Federated Sign-On Protocol and the extensions specified in this document use standard web protocols, XML (as specified in [\[XML\]](#)), WS-Federation Passive Requestor Profile (as specified in [\[WSFederation1.2\]](#) section 13), and SAML 1.1 (as specified in [\[SAMLCore\]](#)). The reader has to be familiar with the specifications listed in [\[MS-MWBF\]](#) section 1.4.

A **relying party** uses the Query String Response Transfer Protocol instead of the **wsignin1.0** messages from Web Browser Federated Sign-On Protocol to avoid the use of HTTP POST messages.

The SAML 1.1 Assertion Extension provides a facility for including **security identifiers** in **SAML assertions**. In order to understand the Windows behavior relating to this extension, the reader has to be familiar with the Active Directory Technical Specification [\[MS-ADTS\]](#), security concepts in [\[MS-WPO\]](#) section 9, and security identifiers [\[SID\]](#).

The Web Browser Federated Sign-On Protocol and the extensions specified in this document can be applicable where other web-based authentication protocols are used. For more information, see [\[MS-MWBF\]](#) section 1.4.

## 1.5 Prerequisites/Preconditions

The SAML 1.1 Assertion Extension requires that an **IP/STS** have a source of **security identifiers** and that the **relying party** have an authorization framework in which to interpret them. The exact methods by which the IP/STS obtains the SIDs, and the methods by which the relying party interprets them, are implementation-specific. [<1><2>](#)

## 1.6 Applicability Statement

The Query String Response Transfer Protocol is applicable where the Web Browser Federated Sign-On Protocol described in [\[MS-MWBF\]](#) is applicable. [<3>](#) The Query String Response Transfer Protocol widens the applicability of the Microsoft Web Browser Federated Sign-On Protocol to include **web browser requestors** that do not implement scripting or form submittal via scripting.

The SAML 1.1 Assertion Extension is applicable when the protected HTTP web application requires **SIDs** to perform authorization. [<4>](#)

## 1.7 Versioning and Capability Negotiation

The Web Browser Federated Sign-On Protocol as described in [\[MS-MWBF\]](#) section 1.7 defers all versioning and capability negotiation to [\[WSFederation\]](#), [\[WSFederation1.2\]](#), and [\[RFC2616\]](#).

When using the Query String Response Transfer Protocol, an **IP/STS** uses the presence of the *ttpindex* parameter (as specified in section [2.2.2.1.1](#)) in the request to determine whether the Query String Response Transfer Protocol is used for the response.

The SAML 1.1 Assertion Extension uses **SIDs**. SIDs have a revision mechanism. For more information, see [\[MS-DTYP\]](#), as specified in section 2.1.

## 1.8 Vendor-Extensible Fields

The extensions specified in this document make use of vendor-extensible fields that are specified as part of [\[MS-MWBF\]](#) section 1.8. Specifically, the Query String Response Transfer Protocol specifies new message parameters as allowed by [\[WSFederation1.2\]](#) section 13.2.1, and the SAML 1.1 Assertion Extension specifies new elements in the **SAML advice** as allowed by [\[SAMLCore\]](#) section 2.3.2.2.

The Query String Response Transfer Protocol does not introduce any vendor-extensible fields that are not present in [\[MS-MWBF\]](#) section 1.8.

The SAML 1.1 Assertion Extension introduces the [ClaimSource \(section 3.1.5.2.1.1\)](#) element whose value is a URI that can be extended by vendors. Uniqueness of URIs is scheme-dependent. For more information, see [\[IANASCHEME\]](#) and [\[RFC4395\]](#).

## 1.9 Standards Assignments

There are no standards assignments beyond those for XML namespaces and standard ports specified in [\[MS-MWBF\]](#) section 1.9. [<5>](#)

## 2 Messages

The Query String Response Transfer Protocol and SAML 1.1 Assertion Extension extend the messages specified in [\[MS-MWBF\]](#) section 2 as described in this section.

### 2.1 Transport

No additional transport is required other than that provided for in [\[MS-MWBF\]](#) section 2.1.

#### 2.1.1 Query String Response Transfer Protocol

In the Query String Response Transfer Protocol, all **wsignin1.0** messages MUST use HTTP GET.

### 2.2 Message Syntax

The Query String Response Transfer Protocol extends the **wsignin1.0** message specified in [\[MS-MWBF\]](#) section 2.2. The SAML 1.1 Assertion Extension extends the **SAML assertion** specified in [\[MS-MWBF\]](#) section 2.2.4.2.

#### 2.2.1 XML Namespace References

Prefixes and XML namespaces used in this specification include the following:

Prefix	Namespace URI	Reference
saml	"urn:oasis:names:tc:SAML:1.0:assertion"	<a href="#">[SAMLCore]</a>
adfs	"urn:Microsoft:federation"	This document

#### 2.2.2 Query String Response Transfer Protocol

The Query String Response Transfer Protocol extends the **wsignin1.0** message from [\[MS-MWBF\]](#) section 2.2 to enable passing results in pieces rather than using POST. The protocol does not extend any other message types.

##### 2.2.2.1 wsignin1.0 Message

[\[MS-MWBF\]](#) section 2.2 specifies how parameters are encoded in messages, including new parameters added by extensions. Specifically, it describes that in HTTP GET messages, the parameters are encoded as query string parameters for transmission in the URL. It also specifies how invalid values are handled.

Section [2.2.2.1.1](#) specifies parameters included in both **wsignin1.0** requests and wsignin1.0 responses that use this protocol.

Section [2.2.2.1.2](#) specifies parameters included only in wsignin1.0 responses that use this protocol.

##### 2.2.2.1.1 Common Parameters

*ttpindex*: The length, in characters, of the **aggregated result** as a 32-bit unsigned integer in decimal notation.

##### 2.2.2.1.2 wsignin1.0 Response

*ttpsize*: The length in characters of the **pending result** as a 32-bit unsigned integer in decimal notation.

**wresult**: The current part of the result being transferred, as a string.

### 2.2.3 SAML 1.1 Assertion Extension

The SAML 1.1 Assertion Extension extends the **SAML assertion** subset as specified in [\[MS-MWBF\]](#) section 2.2.4.2. This extension uses the **SAML advice** element specified in [\[SAMLCore\]](#) section 2.3.2.2 as an extensibility point.

The sections that follow define new elements to convey the source of **claims**, hash data, **user** name, and **SIDs**. These new elements are included as child elements of the advice element in a SAML assertion. These elements use the XML namespace "urn:microsoft:federation". The element content is described using XML schema data types, as specified in [\[XMLSCHEMA2\]](#) section 3.

#### 2.2.3.1 SAML Advice Elements

[ClaimSource](#) (optional): A Uniform Resource Identifier (URI) identifying a **requestor IP/STS** or other authentication service (such as a local **account** store) that is the source of the **claims** in the **security token**. The content is of type any URI (as specified in [\[XMLSCHEMA2\]](#) section 3.2.17).

[CookieInfoHash](#) (optional): A **base64-encoded** implementation-specific hash value. The content is of type base64Binary (as specified in [\[XMLSCHEMA2\]](#) section 3.2.16).[<6>](#)

[WindowsUserIdentifier](#) (optional): A **SID** identifying the **subject** of the **SAML assertion**. The content is of type string (as specified in [\[XMLSCHEMA2\]](#) section 3.2.1) and MUST follow the restrictions for the string representation of a SID, as specified in [\[MS-DTYP\]](#) section 2.4.2).

[WindowsUserName](#) (optional): A **user** name associated with the subject of the SAML assertion. The content is of type string (as specified in [\[XMLSCHEMA2\]](#) section 3.2.1) and MUST be of the form "DOMAIN\user name".[<7>](#)

[WindowsIdentifiers](#) (optional): A base64-encoded binary structure that defines a set of SIDs that identify the subject of the SAML assertion and a set of flags that specify the use of the SIDs. The content is of type base64Binary (as specified in [\[XMLSCHEMA2\]](#) section 3.2.16), and the binary data MUST be structured as specified in [WindowsIdentifiers Binary Structure \(section 2.2.3.2\)](#).

#### 2.2.3.2 WindowsIdentifiers Structure

The WindowsIdentifiers structure has variable length. It defines a set of **SIDs** and flags. To reduce the overall data size, the SIDs are not included in full binary expansion. Rather, [PACKED SIDS](#) structures are created for each group of SIDs that are identical except for the last subauthority.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
WindowsIdentifierFlags																															
PackedSidsCount																															
PackedSids (variable)																															
...																															

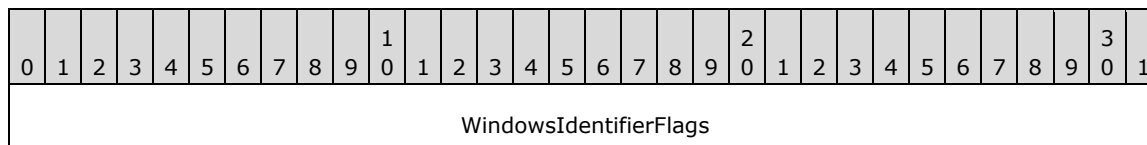
**WindowsIdentifierFlags (4 bytes)**: A 32-bit **WindowsIdentifierFlags** structure (see [2.2.3.2.1](#)).

**PackedSidsCount (4 bytes):** A 4-byte, **little-endian**, unsigned integer that defines the number of **PackedSids** fields in this structure. This field **MUST NOT** be 0.

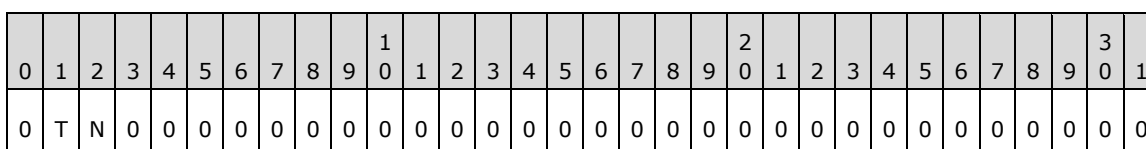
**PackedSids (variable):** A sequence of PACKED\_SIDS structures of variable size, each of which defines a set of SIDs. The sequence defines a set of SIDs, which is the union of the sets of SIDs defined by all the elements.

### 2.2.3.2.1 WindowsIdentifierFlags Structure

The WindowsIdentifierFlags structure is a field of 32 bits.



**WindowsIdentifierFlags (4 bytes):** Bits marked 0 **MUST** be 0. The T and N bits operate independently.

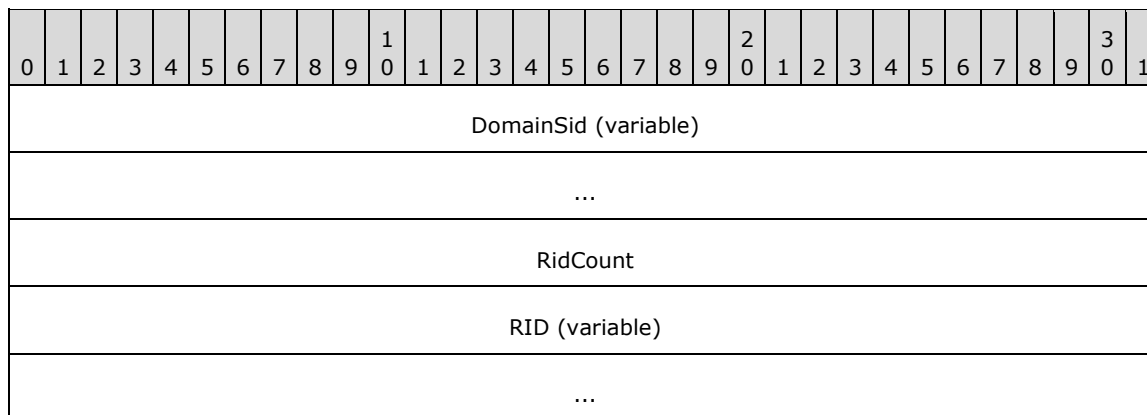


**T - TryLocalAccount (1 bit):** A value of 1 indicates that the SAML NameIdentifier (as specified in [\[SAMLCore\]](#) section 2.4.2.2) takes precedence over the [WindowsIdentifiers structure \(section 2.2.3.2\)](#) element. A value of 0 indicates that the WindowsIdentifiers structure (section 2.2.3.2) element takes precedence over the SAML NameIdentifier (as specified in [\[SAMLCore\]](#) section 2.4.2.2).

**N - NoUserSid (1 bit):** A value of 1 indicates that a **user SID** is not encoded in the WindowsIdentifiers structure. A value of 0 indicates that a user SID is encoded in the WindowsIdentifiers structure.

### 2.2.3.2.2 PACKED\_SIDs Structure

The PACKED\_SIDs structure encapsulates a set of **SIDs** that are identical except for the value of the final subauthority, which is called the **relative identifier (RID)**. The identical portion of the SIDs is included in the **DomainSid** field, and each RID is included separately. The PACKED\_SIDs structure has a variable length.





**DomainSid (variable):** A SID structure of variable size that defines the identical portion of the SIDs encoded in this structure. For details on the SIDs structure, see [\[MS-DTYP\]](#) section 2.4.2.

**RidCount (4 bytes):** A 4-byte, **little-endian**, unsigned integer that defines the number of RID fields in this structure. This field MUST NOT be zero.

**RID (variable):** A sequence of 4-byte, little-endian, unsigned integers that define the RIDs for the SIDs encoded in this structure.

### 2.3 Directory Service Schema Elements

This protocol accesses the following Directory Service schema classes and attributes listed in the following table.

For the syntactic specifications of the following **<Class>** or **<Class><Attribute>** pairs, refer [\[MS-ADTS\]](#), [\[MS-ADA1\]](#), [\[MS-ADA3\]](#).

Class	Attribute
User	All

## 3 Protocol Details

The following sections specify the **IP/STS** and **relying party** protocol details. Each section details role-specific behavior for the extensions specified in this document. There is not a section for the **web browser requestor** role because additional protocol details for the web browser requestor other than those specified in [\[MS-MWBF\]](#) section 3.4 do not exist.

The IP/STS details (see section [3.1](#)) apply to both the **requestor IP/STS** and **resource IP/STS** roles. The relying party details (see section [3.2](#)) apply to both the resource IP/STS and **Web service (WS) resource** roles.

Because the behavior for issuance and consumption of the **SIDs** is implementation-specific, an abstract data model is not introduced for the SAML 1.1 Assertion Extension. Hence, sections [3.1.1](#) and [3.2.1](#) do not have subsections for that extension.

### 3.1 IP/STS Details

The following sections specify the protocol details of the **IP/STS**, including details for the Query String Response Transfer Protocol and SAML 1.1 Assertion Extension. These details apply to both the **resource IP/STS** and the **requestor IP/STS** roles.

#### 3.1.1 Abstract Data Model

This section describes a conceptual organization of data that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

##### 3.1.1.1 Query String Response Transfer Protocol

The following sections specify the abstract data model for transmitting the **pending result** as a series of parts in separate messages that are assembled by a **relying party**.

###### 3.1.1.1.1 Pending Result

When the Query String Response Transfer Protocol is used, the result of a **wsignin1.0** action is transmitted by a series of HTTP 302 responses.

The first message in the exchange establishes the **pending result**. Each message exchange in the series transmits a portion of the pending result to the **relying party** until all parts have been delivered. Consequently, the pending result must be available to the **IP/STS** when processing each message exchange until the series is complete.

The message exchange also includes parameters for the current position and the total length of the result (see section [2.2.2.1](#)) to ensure proper construction and error/completion detection. The method used to maintain the availability of the pending result during the series of exchanges is implementation-specific. The IP/STS MUST discard the pending result when cleaning up local state. See [\[MS-MWBF\]](#) section 3.2.5.3.3 for **requestor IP/STS**. See [\[MS-MWBF\]](#) section 3.3.5.4.2 for **resource IP/STS**.[<8>](#)

###### 3.1.1.1.2 Maximum Query String Response Message Length

Although the HTTP protocol (as specified in [\[RFC2616\]](#)) does not place a limit on the length of a URL, some **web browser requestor** implementations have such a limit. **IP/STS** implementations SHOULD use a maximum query string response message length that will allow a broad range of web browser implementations to act as the web browser requestor. This is a limit on the length of the URL after

escaping, including the scheme, authority, path, and query components (as specified in [\[RFC2396\]](#) section 3). The recommended value is 2,083 octets for all messages. For more information, see [\[MAXURL\].<9>](#)

### 3.1.2 Timers

There are no timers required other than any specified in [\[MS-MWBF\]](#) section 3.1.2; however, a timer MAY [<10>](#) be used to manage state associated with the **pending result**.

### 3.1.3 Initialization

There are no new initializations beyond any described in [\[MS-MWBF\]](#) section 3.1.3; however, the **pending result** is initialized after the protocol has been initiated (see section [3.1.5.1.2](#)).

### 3.1.4 Higher-Layer Triggered Events

There are no higher-layer triggered events other than any described in [\[MS-MWBF\]](#) section 3.1.4.

### 3.1.5 Processing Events and Sequencing Rules

#### 3.1.5.1 Query String Response Transfer Protocol

The following sections specify protocol details for the Query String Response Transfer Protocol when receiving **wsignin1.0** requests.

Sections [3.1.5.1.1](#), [3.1.5.1.2](#), and [3.1.5.1.3](#) specify how **wsignin1.0** requests are processed given the value of the *ttpindex* parameter. Section [3.1.5.1.4](#) specifies common behavior for responding to such requests when the Query String Response Protocol is used.

##### 3.1.5.1.1 Receiving a **wsignin1.0** Request That Does Not Specify a *ttpindex*

When the **IP/STS** receives a **wsignin1.0** request that does not specify the *ttpindex* parameter, the response MUST NOT use the Query String Response Transfer Protocol. The IP/STS MUST discard any **pending result**, and the IP/STS MUST process the message as specified in [\[MS-MWBF\]](#) section 3.1.5.4.

##### 3.1.5.1.2 Receiving a **wsignin1.0** Request That Specifies a *ttpindex* of 0

When the **IP/STS** receives a **wsignin1.0** request that specifies a *ttpindex* parameter value of 0, the IP/STS MUST process the **wsignin1.0** request (as specified in [\[MS-MWBF\]](#) section 3.1.5.4) up to the point where the IP/STS has constructed the **RSTR** element (as specified in [\[MS-MWBF\]](#) section 3.1.5.4.6). The IP/STS MUST apply the following transforms to the RSTR element to produce the **pending result**:

1. Convert the XML string to binary data by applying UTF-8 encoding, as specified in [\[RFC2279\]](#).
2. Compress the result from step 1 to the zlib format (as specified in [\[RFC1950\]](#)) by using the deflate algorithm (as specified in [\[RFC1951\]](#)).
3. Base64-encode the result from step 2, as specified in [\[RFC2045\]](#) section 6.8.

The IP/STS MUST respond as specified in section [3.1.5.1.4](#), by using the result from step 3 as the pending result.

##### 3.1.5.1.3 Receiving a **wsignin1.0** Request That Specifies a *ttpindex* Other Than 0

When the **IP/STS** receives a **wsignin1.0** request that specifies a *ttpindex* parameter value other than 0, the following conditions MUST be evaluated in order:

1. The *ttpindex* value does not conform to message syntax rules (for example, if it is not a number, as specified in section [2.2.2.1.1](#)).
2. The corresponding **pending result** is not available.
3. The value of *ttpindex* is greater than or equal to the length in characters of the pending result.

If the message meets any of the conditions, the IP/STS MUST reject the message and return an HTTP 500 response. Otherwise, the IP/STS MUST respond as specified in section [3.1.5.1.4](#).

#### **3.1.5.1.4 Responding to a wsignin1.0 Request That Specifies a ttpindex**

The **IP/STS** MUST construct a **wsignin1.0** response for the **relying party** by using the following values as properly escaped query string parameters in the returned status URL, as specified in [\[WSFederation1.2\]](#) section 13.2.3.

- *ttpindex* MUST be the same value of *ttpindex* as requested.
- *ttpsize* MUST be the same length in characters as the **pending result**.
- *wctx* MUST be the same value of *wctx* as requested.
- *wresult* MUST contain a portion of the pending result, beginning at the character of index *ttpindex* (zero-based), and including as many characters as possible without exceeding the maximum query string response message length. Note that the maximum query string response message length applies after the escaping rules for URL query string parameters.

The IP/STS MUST transmit the message to the **web browser requestor** using HTTP 302 as specified in [\[WSFederation1.2\]](#) section 13.2.3.

#### **3.1.5.2 SAML 1.1 Assertion Extension**

The **IP/STS** uses the SAML 1.1 Assertion Extension when responding to **wsignin1.0** requests. Although the protocol details are largely similar, it is necessary in this section to distinguish between the **requestor IP/STS** and **resource IP/STS** roles.

The IP/STS is a requestor IP/STS when issuing a token to a **relying party** that is in a different **security realm** than the IP/STS. Conversely, the IP/STS is a resource IP/STS when issuing a token to a relying party that is in the same security realm as the IP/STS.

##### **3.1.5.2.1 Responding to a wsignin1.0 Request**

When responding to a **wsignin1.0** request, the **IP/STS** MAY include any of the [ClaimSource \(section 3.1.5.2.1.1\)](#), [CookieInfoHash \(section 3.1.5.2.1.2\)](#), [WindowsUserIdentifier \(section 3.1.5.2.1.3\)](#), [WindowsUserName \(section 3.1.5.2.1.4\)](#), and [WindowsIdentifiers \(section 3.1.5.2.1.5\)](#) elements in the issued **SAML assertion**. For syntax details, see section [2.2.3](#).

The following sections describe the processing semantics for each of these optional SAML assertion elements.

##### **3.1.5.2.1.1 ClaimSource Element**

The **IP/STS** MAY [<11>](#) include the ClaimSource element in the issued **SAML assertion**.

##### **3.1.5.2.1.2 CookieInfoHash Element**

The **IP/STS** MAY<12> include the CookieInfoHash element in the issued **SAML assertion**.

#### **3.1.5.2.1.3 WindowsUserIdentifier Element**

The **IP/STS** MAY<13> include the WindowsUserIdentifier element in the issued **SAML assertion**.

#### **3.1.5.2.1.4 WindowsUserName Element**

The **IP/STS** MAY<14> include the WindowsUserName element in the issued **SAML assertion**.

#### **3.1.5.2.1.5 WindowsIdentifiers Element**

The **IP/STS** MAY<15> include the WindowsIdentifiers element in the issued **SAML assertion**.

### **3.1.6 Timer Events**

Timer events are not required other than any specified in [MS-MWBF] section 3.1.6; however, a timer event MAY<16> be used to manage the state associated with the **pending result**.

### **3.1.7 Other Local Events**

There are no other local events that impact the operation of this protocol.

## **3.2 Relying Party Details**

These details apply to both the **resource IP/STS** and **WS resource** roles (when acting as a **relying party** for a received **security token**).

### **3.2.1 Abstract Data Model**

This section describes a conceptual model of a possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

#### **3.2.1.1 Query String Response Transfer Protocol**

The following sections specify the abstract data model for receiving and concatenating the **aggregated result** as a series of messages.

##### **3.2.1.1.1 Aggregated Result**

When the Query String Response Transfer Protocol is used, the result of a **wsignin1.0** action is transmitted by a series of message exchanges. When an **aggregated result** is not available, it is considered to be empty (with size 0). The **relying party** concatenates each portion of the result to the aggregated result when it is received, so the aggregated result must be available to the relying party when processing each message exchange. The method used to maintain the availability of the aggregated result is implementation-specific. The relying party **MUST** discard the aggregated result when it receives a **wsignoutcleanup1.0** message (as specified in [MS-MWBF] section 3.3.5.4.2).<17>

### **3.2.2 Timers**

There are no timers required other than any specified in [MS-MWBF] section 3.3.2; however, a timer MAY<18> be used to manage a state associated with the **aggregated result**.

### 3.2.3 Initialization

There are no new initializations other than any described in [\[MS-MWBF\]](#) section 3.3.3; however, the **aggregated result** is initialized after the protocol has been initiated (as specified in section [3.2.5.1.3](#)).

### 3.2.4 Higher-Layer Triggered Events

There are no new higher-layer triggered events other than any described in [\[MS-MWBF\]](#) section 3.3.4.

### 3.2.5 Processing Events and Sequencing Rules

The Query String Response Transfer Protocol and the SAML 1.1 Assertion Extension introduce new message processing rules.

#### 3.2.5.1 Query String Response Transfer Protocol

The following sections specify protocol details for the Query String Response Transfer Protocol when processing **wsignin1.0** messages.

Section [3.2.5.1.1](#) specifies how to send a **wsignin1.0** request by using this protocol. Sections [3.2.5.1.2](#) and [3.2.5.1.3](#) specify how to process a **wsignin1.0** response given the presence or absence of the *ttpindex* parameter. Section [3.2.5.1.4](#) specifies how the completed **aggregated result** is processed.

##### 3.2.5.1.1 Sending a **wsignin1.0** Request

When using the Query String Response Transfer Protocol, the **relying party** sends a **wsignin1.0** request to the **IP/STS** as specified in [\[MS-MWBF\]](#) section 3.3.5.1 and MUST add the *ttpindex* parameter. When included, the value of the *ttpindex* parameter MUST be the length in characters of the **aggregated result**.

**Note** If the aggregated result is not available, it is considered to have length 0 (see section [3.2.1.1.1](#)). Therefore, in the first request, the value of *ttpindex* MUST be 0.<19>

##### 3.2.5.1.2 Receiving a **wsignin1.0** Response That Does Not Specify a *ttpindex*

When the **relying party** receives a **wsignin1.0** response that does not specify the *ttpindex* parameter, the message does not use the Query String Response Transfer Protocol, and the relying party MUST process the message as specified in [\[MS-MWBF\]](#) section 3.3.5.2.

##### 3.2.5.1.3 Receiving a **wsignin1.0** Response That Specifies a *ttpindex*

When the **relying party** receives a **wsignin1.0** response that specifies the *ttpindex* parameter, it MUST evaluate the following conditions in order:

1. The *ttpindex* value does not conform to message syntax rules (for example, it is not a number; as specified in section [2.2.2.1.1](#)).
2. The *ttpindex* parameter is not equal to the length, in characters, of the **aggregated result**. Note that if the aggregated result is not available, it is considered to have length 0 (as specified in section [3.2.1.1.1](#)).

If the message meets one of these conditions, the relying party MUST reject the message and return an HTTP 500 response.

The relying party MUST construct a new aggregated result. If *ttpindex* is 0, the aggregated result MUST be the value of the *wresult* parameter; otherwise, the aggregated result MUST be constructed by appending the *wresult* parameter to the current aggregated result.

The relying party MUST evaluate the *tptsize* parameter as follows:

- If the length in characters of the new aggregated result is greater than the value of the *tptsize* parameter, the relying party MUST reject the message and return an HTTP 500 response.
- If the length, in characters, of the new aggregated result is equal to the value of the *tptsize* parameter, the relying party MUST process the completed result as specified in section [3.2.5.1.4](#).
- If the length, in characters, of the new aggregated result is less than the value of the *tptsize* parameter, the relying party MUST request the next portion of the result as specified in section [3.2.5.1.1](#).

#### 3.2.5.1.4 Processing the Complete Aggregated Result

When the **aggregated result** is complete, the **relying party** MUST apply the following transforms to the aggregated result to produce an XML string:

1. Base64-decode the aggregated result to binary data (as specified in [\[RFC2045\]](#) section 6.8).
2. Decompress the result from step 1 from the zlib format (as specified in [\[RFC1950\]](#)) by using the inflate algorithm (as specified in [\[RFC1951\]](#)).
3. Interpret the binary data from step 2 as a UTF-8-encoded string (as specified in [\[RFC2279\]](#)).

If any error occurs when applying the transforms, the relying party MUST reject the message and return an HTTP 500 response.

The relying party MUST process the **wsignin1.0** response (as specified in [\[MS-MWBF\]](#) section 3.3.5.2), substituting the string output from step 3 for the *wresult* parameter.

#### 3.2.5.2 SAML 1.1 Assertion Extension

The method of evaluating **SIDs** transmitted by using the SAML 1.1 Assertion Extension is implementation-specific. For specifications about SIDs and their semantics in Windows, see [\[MS-DTYP\].<20>](#)

#### 3.2.6 Timer Events

There are no timer events required other than any events specified in [\[MS-MWBF\]](#) section 3.3.6; however, a timer event MAY [<21>](#) be used to manage a state associated with the **aggregated result**.

#### 3.2.7 Other Local Events

There are no other local events that impact the operation of this protocol.

### 3.3 Web Browser Requestor Details

This section specifies the **web browser requestor** role in transporting protocol messages.

#### 3.3.1 Abstract Data Model

A **web browser requestor** does not need to understand any protocol-specific data for the correct operation of the protocol. It MUST be able to support HTTP query string and POST body parameterization. To provide the best end-user experience, it SHOULD be able to support HTTP cookies (for more information, see [\[RFC2965\]](#)). [<22>](#)

### 3.3.2 Timers

A **web browser requestor** does not depend on timers beyond those that are used by the underlying transport to transmit and receive messages over HTTP and SSL/TLS, as specified in section [3.1.2](#).

A web browser requestor does not need to be aware of an implementation's use of timers to determine when the validity intervals of **security tokens** and authentication contexts expire.

### 3.3.3 Initialization

There is no protocol-specific initialization for a **web browser requestor**. It only needs to be ready to perform the standard HTTP 1.1 methods required for accessing **WS resources**. Specifically, it **MUST** support HTTP GET and POST methods and properly respond to HTTP 1.1 redirection and error responses.

### 3.3.4 Higher Layer Triggered Events

Protocol messages are exchanged between a **requestor IP/STS** and a **relying party**. The only function of the **web browser requestor** with respect to the protocol is to transport these messages. The web browser requestor can be triggered to begin protocol message exchange by receipt of an HTTP/1.1 302 found that includes a location directive, or an HTTP/1.1 200 OK that includes a form with method set to POST.

### 3.3.5 Processing Events and Sequencing Rules

A **web browser requestor** plays a passive role in the operation of the protocol. Its only function is to transport protocol message requests and responses between a **requestor IP/STS** and one or more relying parties. It is not required to understand the types or content of these protocol messages. The web browser requestor **SHOULD** transport all protocol message requests and responses between a requestor IP/STS and a **relying party** without changing the messages at all. [<23>](#)

### 3.3.6 Timer Events

A **web browser requestor** does not need to interact with any timers, or service any timer events, beyond those that might be used by the underlying transport to transmit and receive messages over HTTP and SSL/TLS, or those specified in section [3.1.6](#).

### 3.3.7 Other Local Events

A **web browser requestor** does not have dependencies on local events beyond those specified in section [3.1.7](#).



## 4 Protocol Examples

### 4.1 Query String Response Transfer Protocol

#### 4.1.1 Annotated Example

The following is a protocol example for the Query String Response Transfer Protocol.

The Query String Response Transfer Protocol is best understood as occurring abstractly between an **IP/STS** and a **relying party**, because the changes to the Web Browser Federated Sign-On Protocol [MS-MWBF] are applied consistently whether between **requestor IP/STS** and **resource IP/STS** or between resource IP/STS and **WS resource**.

This annotated example shows a Query String Response Transfer Protocol exchange between a requestor IP/STS and a resource IP/STS. It is part of a larger network trace (see section 4.2) that also uses the Query String Response Transfer Protocol between the resource IP/STS and the WS resource.

The following table specifies the protocol roles of the hosts.

Protocol role	Host name
IP/STS	adatumsts-7
Relying party	treysts-7

Each HTTP message is prefaced by an annotation that describes its recipient and purpose. This annotated example omits many elements of the HTTP messages. For example, implementation-specific cookies and superfluous HTTP headers are not included. The full messages are specified in section 4.1.2. The following parameters are specified in this document and appear in the HTTP messages that follow:

- *tpindex*
- *ttpsize*
- *wresult*

The following are the processing steps of this annotated example:

1. Just prior to the example, the **web browser requestor** made a GET request to the relying party (treysts-7).
2. The relying party returns an HTTP 302 message that specifies a **wsignin1.0** request for the IP/STS. This wsigin1.0 request includes the *tpindex=0* parameter, which initiates the Query String Response Transfer Protocol (see section 3.2.5.1). At this time, the relying party's **aggregated result** is empty, as specified in section 3.2.5.1.1.

```
HTTP/1.1 302 Found
Location:
https://adatumsts-7/adfs/ls/?wa=wsigin1.0&
wrealm=urn%3afederation%3atreys+research&
wct=2006-07-13T07%3a32%3a21Z&
wctx=https%3a%2f%2ftreys-test%2fclaims%2f%5chttps%3a%2f%
2ftreys-test%2fclaims%2fDefault.aspx&ttpindex=0
```

3. The web browser requestor relays the wsigin1.0 request to the IP/STS (adatumsts-7) in an HTTP GET message.

```
GET /adfs/ls/?wa=wsignin1.0&wtrealm=urn%3afederation
%3atrey+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%
3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%
2fclaims%2fDefault.aspx&ttpindex=0 HTTP/1.1
```

4. The IP/STS engages in a series of messages outside the scope of the protocol whereby it ascertains the **user** identity. These messages are omitted, as they have no bearing on the Query String Response Transfer Protocol. For more details, see [MS-MWBF] section 3.1.5.4.3.
5. Once the user's identity has been determined, the IP/STS creates an **RSTR**, as specified in [MS-MWBF] section 3.1.5.4.6. The RSTR is transformed into the **pending result**, and the first portion is returned in a wsignin1.0 response (as specified in section 3.1.5.1.4). In this message, the *wresult* parameter is the first 1,727 characters of the pending result. The *ttpsize* parameter indicates the length of the full pending result, 2,652.

```
HTTP/1.1 302 Found
Location: https://treysts-7/adfs/ls/?wa=wsignin1.0&
ttpsize=2652&ttpindex=0&wctx=https%3a%2f%
2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%
2fDefault.aspx&wresult=eNrNWFtzqsoS%
2fIUW6zGVBYg3rCRlhquAaAA1yssphOESHVEGRPz1e9BoTNYt59R62D4NPW3311%
2f3dDM8lDgFWHBXQJzb0CuyOK%2bmaA1TC%2bItSjFsHJNjgdE7bEZ5f12QFHYi2Di
4u9kByN3%2bx11IVViqkXTHYpuUXlW4Lz59HBjGfofbD89YDfZDADGMMtj1DauK1V8
bP436NAMGzD%2bvddps%2fftFuzd91ewc79iu5y7Yv1%2b4HeaDRXjAqopzt2UQCPOu
%2fd0755hp3RvwLYGrZ7zppM9NossHQTQh5lbOxm4vpsXSbNhuK8om8MME
%2bFjkyGCOP0oOAdfoz0bQs6O8SB1E4gHuTEwTEAMN
%2fpgXsJoPkWm4BSP64FuDFGOQ8D1MFfoSQKk3SSgSCvsd7q9C86F8YKP4apB0ly8i
z2avtXR59Unj7FnGewamQQQzfzofgqo%2b6n55%2bbpz4FdnHo7
%2bPahOsHmOyidUyyEqChi6M3%2buqdM31J7GUIoyC%2fQdZ8UqK5vj2Kulay0tQy
KoWL1HhnM8%2fS%2bvGB%2bondK94312%2fg8wimeeydrNq5m8OEPDc%2byv9QMB%
2bVDZhHyP%2bxfd4oDco49VGJLzmyi9Ur9PK3pzEpFgWvtYMYZg0ZZYn7
%2b5Pkbdw4wdTsedx8An4SpzFJhpuj7D%2fnsV3uoEQ%2fo%2fGL6xcAVC
%2f4%2bXCWk4yvSpy%2bHnj3xPGR5yN6r%2b22NTStx4A3yflDZuftzEW9eDXwDZ
%2fOxj7m4K%2bOT%2bHvUn7c%2fSP%2bEWUJKgtF7%2fXdQGUUwydKL87yBVm1Rs
%2fy5Iod4kCU7inID9d8ME222G9l9HSf3yXNlxmJiiyt5m6hVXWZb5F5
%2fYEh3QlmgI5iij4OA6%2fNc%2f%2fgn7d%2bp4eBDdFKTnJm
%2fh406AaYBMiM1yj5BcmGYqha5P38ODde0w7%2fdZsUDD4vmjma7IMu
%2fc4cpmTJQsGMKsnR2NmQY%2fnb18b4U8P08xNMRmNCb5Z%2f284YLqHG7SF
%2fj2%2bhHOC9HVZv2CHugUnxiGZif8PTleOzibOVTPhN2GVHqWsG5S6BHgV4f3E
0eycpnEu9V80K7ckvVtLVyzdlYUYTg1c1Gn%2fJ5011Fmx1mmaTOBae%2bMEOjVHb
%2bd96NDIj09jLvrlopNjXwsPNN3kWwtuE2Vj4t90Zram4XtYg1Y2jTyLGrUFmYHmd
V4WW87i6VIm9VO3UNABoiR5XrV0emvSA5kpm9SXZK7rXmHZ
%2fGWXdBd5mpuJX07ZiQ4ru01X%2fmI6gf4De4zmQG
%2fAPOzOUS06Nce6uXteCFVLVVCPLtLYVfVkrEEAWRWCuuVBqOoKGyayCeQfdJiCMR
%2bud9E6Vris5oE5k4EIHMPyStlcinPTFKWYm3OVTeXIfoS1VmeWcHtFBFAu6XL8C
lhjqlbGFJSGOHZPsnNFJplkBr88yCKw%2bXA854ExFVryermwNviTHsVzRqQehiA
VgR7p9jqihVnQcYBQFSZA1HgY1PnQ10017ue4uB4smhLvZzth3SxY7QX1thxeQF0p
%2b9W%2bNmJNkfjzB%2fTga7DDMWjyOeTmeZ07vb8EogLjTrK%2bZRq6weJ1WNn02
k9F6RVHa3%2bWqcZXRkto8gHGZR5oZfYq4g72IsKhFxFvFycmf0Eas4dKvg9xCeC
SI0h1rSDYWDpzG7tcUxxz7Q5WOpisAEPGqrPDoS7p1%2bKYaES4t%2bBuaQISGJIJ
yWhmTexqyJpcka4qzWVXX
```

6. The web browser requestor relays the wsignin1.0 response to the relying party (treysts-7) in an HTTP GET message.

```
GET /adfs/ls/?wa=wsignin1.0&
ttpsize=2652&ttpindex=0&wctx=https%3a%2f%2ft
reyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims
%2fDefault.aspx&wresult=eNrNWFtzqsoS%2fIUW6zGVBYg3rCRlh
quAaAA1yssphOESHVEGRPz1e9BoTNYt59R62D4NPW3311%2f3dDM8lDgFWHBXQJzb0
CuyOK%2bmaA1TC%2bItSjFsHJNjgdE7bEZ5f12QFHYi2Di4u9kByN3%2bx11IVViq
kXTHYpuUXlW4Lz59HBjGfofbD89YDfZDADGMMtj1DauK1V8bP436NAMGzD%2bvddps
%2fftFuzd91ewc79iu5y7Yv1%2b4HeaDRXjAqopzt2UQCPOu%2fd0755hp3RvwLYGr
```

Z7zppM9NossHQTh51bOxm4vpsXSbNhuK8om8MME%2bFjkyGCOP0oOAdfoz0bQS608  
SB1E4gHuTewgTEaMN%2fpgXsJoPkWm4BSP64FuDFGQ8D1MFfoSQKk3SSgSCvsd7q9  
C86F8YKP4apB01y8iz2avtXR59Unj7FnGewamQQzFzozgffqo%2b6n55%2bbpz4FdnH  
o7%2bPahOsHmQyidUyyEqChi6M3%2buqdM31J7GUIOyC%2fQdZ8UqK5vj2Kulay0tQ  
yKoWL1HhnM8%2fS%2bvGB%2bondK94312%2fg8wimeeydrNq5m8OEPDc%2byv9QMB%  
2bVDZhHyP%2bxfD4oDco49VGJLzmyi9Ur9PK3pzEpFdWvtYMYZg0ZZYn7%2b5Pkbdb  
4wdTsedx8An4SpzFJhpj7D%2fnsv3uoEQ%2fo%2fGL6xcAVC%2f4  
%2bXCWk4yvSpy%2bHnj3xPGR5yN66r%2b22NTStx4A3yflDZuftzEW9eDXwDZ  
%2fOxj7m4K%2bOT%2bHvUn7c%2fSP%2bEWUJKgtF7%2fXdQGUwydKL87yBVM1Rs  
%2fy5Iod4kCU7inID9d8ME222G919HSf3yXN1xmJiIyt5m6hVXWZbfs  
%2fYeh3QlmgI5iij4OA6%2fNc%2f%2fgn7d%2bp4eBdDFKtnJm%2fh406AaYBmiM1  
y75BcmGyqha5P38ODde0w7%2fdZsUdd4vmjma7IMu%2fc4cpmTJQsGMksnR2NmQY  
%2fNb18b4U8P08xNMRmNcb5Z%2f284YLqHG7SF%2fj2%2bhHOC9HVzv2CHugUnxi  
GZiF8PT1eOzibOVTPHN2GVHqWsG5S6BHgV4f3E0eycpnEu9V8oK7ckvVtLVyzd1  
YUYTg1c1Gn%2fJ5011Fmx1mmaTOBae%2bMEojVHb%2bd96NDIj09jLvrlonJXws  
PNN3kwwtuE2Vj4t90Zram4XtYglY2jTyLGrUFmYHmdV4WW87i6VIm9V03UNaBPOi  
R5XrV0emvSA5kpm9SXZK7rXmHZ%2fGWXdBd5mpuJX07ZiQa4ru01X%2fmI6gf4De  
4zmQG%2fAPOz0US06Nce6uXteCFVLVVCPLtLYVfVvKREEARWCuuVBqOoKGyayCe  
qfdJiCMR%2bud9E6Vris50E5k4EIHMPyStlcinPTFKWym30VTeXiFOSlVmeWcHtf  
BFAu6XL8ClhjqlbGFJSGOHZPsnNFJplkBr88yCKw%2bXA854ExFVrYermwNViTH  
sVzRqQehiAVgr7p9jqihVNqcYBQFSZA1HgY1PnQ10017uE4uB4smhLvZZth3SxY7  
QXlthxeQF0p%2b9W%2bNmJNkfjZb%2fTGa7DDMwjYoEtmEZO7vb8EogLjTrK%2bZ  
Rq6weJlWNn02k9F6RVHa3%2bWqcZXRkt08gHGZR50zFyq4g72IsKhFxFvVfycmf0E  
as4dKvg9xCeCSIOh1rSDYWDpzG7tcUxxx7Q5WOpisAEPGqrPDoS7p1%2bKYaES4t%  
2bBuaQISGJIJyWhmTexqyJpcka4qzWVXX HTTP/1.1

7. Because the relying party's aggregated result is empty, the *wresult* parameter becomes the aggregated result. Because the length of the *wresult* parameter was 1,727 characters, which is less than the length of the *ttpsize* parameter of 2,652 characters, the relying party needs to request more data from the IP/STS. It does this by sending an HTTP 302 with a *wsignin1.0* request that includes the *ttpindex=1727* parameter. For further specifications, see section [3.2.5.1.3](#).

```
HTTP/1.1 302 Found
Location: https://adatumsts-7/adfs/ls/?wa=wsignin1.0&wtrealm=urn%3afederation%3atrety+research&wct=2006-07-13T07%3a32%3a27Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=1727
```

8. The web browser requestor relays the *wsignin1.0* request to the IP/STS (adatumsts-7) in an HTTP GET message.

```
GET /adfs/ls/?wa=wsignin1.0&wtrealm=urn%3afederation%3atrety+research&wct=2006-07-13T07%3a32%3a27Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=1727 HTTP/1.1
```

9. The IP/STS returns the remaining 925 characters of the pending result, beginning with character 1,727. For further specifications, see section [3.1.5.1.3](#).

```
HTTP/1.1 302 Found
Location: https://treysts-7/adfs/ls/?wa=wsignin1.0&ttpsize=2652&ttpindex=1727&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&wresult=kqNheG50cCSAUgEHIEISLriGRPIJQBEM%2bnGViaAj8ERCSwkseRfLs13wPzbYkh%2bZs6Vn0YZP76zacMJFGrZbrVe%2fYXvUjtZTKE7YND8pSqH2XS543Z0PiuXye9155PxlBGZyO6WHThaJc9Xt2NPJctVwBL2TsZNZOTdPugEvtcupyOtIikMLOZi7tGhPRPtRa7wh9RP5CwuNeqvwqs7ritXKUcJsl6y291pc4gtE1qL3Zmte%2bdK88BIOrwTux%2foje15S1qGDCC9YgeuWLyWeV5UxqSfdkNR3%2bREIOauD%2fKFVtUL%2bflnbVmTGV8LPf16dhUYvF3PalX%2fhMzVLC7xzZABdmSjOdxMuqOK8xbKe4wL6bSWV6m2Xykh791vFMvVaOs1lrrkk
```

```
%2fuCc7LnmQTigP58D%2fnQOyLk1eXYX3x3GU8rrUsn84LO%2bcGRAtt4eNHY1VD
NEDcGh1%2fYOCuJud%2fup3%2bZefDPvB3s91IYB7%2b3VXuK%2bwLyUR23Le07Y
WTLPlDl1p62FeOiHAQuF53jLdrGtc%2b3jPFPkwJFdrk%2b9H1C7ZNDdiyLPcivf
SV2bCmN6ZEmxMRJ0z3KS6G426m1DqL0MYcV1WJ3zzJHR8pWVozlral0wbkuYqT01
eD60fT1hBCVdIcNLmwcRIKRIA9QjsGoiff4T63Xg3zIFiq6rSQ%2fRvr29y6LF
oyBn2NHQ6T1oTaG%2f11Je46h3nqJM8dbElFMpNTRKW7SYduLSjlaHXZKO2m0
%2fTykrVn3ny93nGygPpVKClJt3qFQfFAfe6YZ8m5m1LXDvvee6%2fvKpfLKxH8
7tJe4u2AtJhNDPEUXb8LbL%2fwXaBdT8Qt2sRedfow4A6k1N%2biOM3f3xwu9ty
v2euTi%2bHppT9Owzebb7eAP9x8bzXPTz9gOclvYv3Iy08%2fkzz9A6cx%2fkw
%3d
```

- The web browser requestor relays the `wsignin1.0` response to the relying party (treysts-7) in an HTTP GET message.

```
GET /adfs/ls/?wa=wsignin1.0&
ttpsize=2652&ttpindex=1727
&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a
%2f%2ftreyws-test%2fclaims%2fDefault.aspx&
wresult=kqNHeG50cSAUgEHIEISLriGRPIJQBEM
%2bnGViaAj8ERCsWkseRfLs13wPzbYkh%2bZs6Vn0YZP76zacMJFGrZbrVe
%2fYXvUjtZTKE7YND8pSqH2XS543Z0Piuxye9155PixlBGZyO6WHThaJc9Xt2NP
JctVwBL2TsZnZOTdPugEvtcupyOtIikMLOZI7tGhPRPtRa7wh9RP5CwuNEqvwqs
7ritXKUcJsl6y291pc4gtElqL3Zmte%2bdK88BIOrwTux%2fojel5SlqGDCC9Y
qeuWLyWeV5UxqSfdkNR3%2bREI0auD%2fKFVtuL%2bflnbVmtGV8LPfl6dhUYvF
3PalX%2fHmzVLC7xzZABdmSjOdqXMuqOK8xbKe4wL6bSWV6m2XyKH791vFMVaO
s1lrkk%2fuCc7LnmQTigP58D%2fnQOyLk1eXYX3x3GU8rrUsn84LO%2bcGRAtt4
eNHY1VDNEDcGh1%2fYOCuJud%2fup3%2bZefDPvB3s91IYB7%2b3VXuK%2bwLyU
R23Le07YWTLPlDl1p62FeOiHAQuF53jLdrGtc%2b3jPFPkwJFdrk%2b9H1C7ZND
diyLPcivfSV2bCmN6ZEmxMRJ0z3KS6G426m1DqL0MYcV1WJ3zzJHR8pWVozlral
0wbkuYqT01eD60fT1hBCVdIcNLmwcRIKRIA9QjsGoiff4T63Xg3zIFiq6rSQ
%2fRvr29y6LFoyBn2NHQ6T1oTaG%2f11Je46h3nqJM8dbElFMpNTRKW7SYduLS
jlaHXZKO2m0%2fTykrVn3ny93nGygPpVKClJt3qFQfFAfe6YZ8m5m1LXDvvee6
%2fvKpfLKxH87tJe4u2AtJhNDPEUXb8LbL%2fwXaBdT8Qt2sRedfow4A6k1N
%2biOM3f3xwu9tyv2euTi%2bHppT9Owzebb7eAP9x8bzXPTz9gOclvYv3Iy08
%2fkzz9A6cx%2fkw%3d HTTP/1.1
```

- The relying party appends the `wresult` parameter to the aggregated result. The new aggregated result is 2,652 characters long, which indicates the completion of the Query String Response Transfer Protocol (see section 4.1). The relying party extracts the RSTR from the aggregated result (as specified in section 3.2.5.1.4) and processes it as specified in [MS-MWBF] section 3.3.5.2. The relying party's next action is outside the scope of the protocol, though in this case the relying party, which was a resource IP/STS, issued a new **SAML assertion** and used the Query String Response Transfer Protocol to transmit it to a WS resource.

#### 4.1.2 Full Network Trace

The following is the full network trace for the protocol example in [Annotated Example \(section 4.1.1\)](#).

The following table specifies the protocol roles of the hosts.

Protocol role	Host name
<b>Requestor IP/STS</b>	adatumsts-7
<b>Resource IP/STS</b>	treysts-7
<b>WS resource</b>	treyws-test

HTTP requests are prefaced by a line with three right-angle brackets ("**>>>**") and the name of the host to which the request was sent. Requests are followed by the HTTP response, which is prefaced by

a line with three left-angle brackets (" $<<<$ "). The final three HTTP messages (HTTP 302, HTTP GET, and HTTP 200 OK) are an internal implementation detail and shown for completeness only. These messages are not necessary for interoperability.

```
>>> treyws-test (WS Resource)
GET /claims/ HTTP/1.1

<<<
HTTP/1.1 302 Found
Location: https://treysts-7/ads/ls/?wa=wsignin1.0&wreply=https%3a%2f%2ftreyws-test%2fclaims%2f&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0

>>> treysts-7 (Resource IP/STS)
GET /ads/ls/?wa=wsignin1.0&wreply=https%3a%2f%2ftreyws-test%2fclaims%2f&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0 HTTP/1.1

<<<
HTTP/1.1 302 Found
Location: https://adatumsts-7/ads/ls/?wa=wsignin1.0&wrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0
Set-Cookie: _TTPRealm=urn:federation:adatum; path=/ads/ls/; secure; HttpOnly

>>> adatumsts-7 (Requestor IP/STS)
GET /ads/ls/?wa=wsignin1.0&wrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0 HTTP/1.1

<<<
HTTP/1.1 302 Found
Location: /ads/ls/auth/integrated/?wa=wsignin1.0&wrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0

>>> adatumsts-7 (Requestor IP/STS)
GET /ads/ls/auth/integrated/?wa=wsignin1.0&wrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0 HTTP/1.1

<<<
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM

>>> adatumsts-7 (Requestor IP/STS)
GET /ads/ls/auth/integrated/?wa=wsignin1.0&wrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21Z&wctx=https%3a%2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=0 HTTP/1.1
Authorization: Negotiate TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAA
FAs4OAAAADw==

<<<
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Negotiate TlRMTVNTUAACAAAEAAQAdgAAAAFgomi1Z0tC7za4
J0AAAAAAAAAAAAQBBFAFIAAAABQLoDgAAAA9BAEQARgBTAFYATQataEEAAgQAEEARBGAF
MAVgBNAC0AQQABABYAQQBEAEAVABVAE0AUwBUAFMALQA3AAQAQgBhAGQAZgBzAHYAbQA
tAGEALgBuAHQAdAB1AHMAdAAuAG0AaQBjAHIAbwBzAG8AZgB0AC4AYwBvAG0AAwBSAGEA
ZABhAHQAdQBtAHMAdABzAC0ANwAuAGEAZABmAHMAdgBtAC0AYQAUAG4AdAB0AGUAcwB0A
C4AbQBPAGMAcgvBvAHMAbwBmAHQALgBjAG8AbQAFADoAYQBkAGYAcwB2AG0ALQBhAC4Abg
B0AHQAZQBzAHQALgBtAGkAYwByAG8AcwBvAGYAdAAuAGMAbwBtAAAAAA=
```

>>> adatumsts-7 (Requestor IP/STS)  
GET /ads/ls/auth/integrated/?wa=wsignin1.0&wtrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21z&wctx=https%3a%2f%2ftreys-test%2fclaims%2f5chttps%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&ttindex=0 HTTP/1.1  
Authorization: Negotiate TlRMTVNTUAADAAAAGAAAYIAAAAAAYABgAmAAAABAAEABIAAAAGgAaAFgAAAAOAA4AcgAAAAAACAaAAABYKIOgUCzG4AAAAAPYQbKAGYAcwB2AG0ALQBhAGEAZABtAGkAbgBpAHMAdABvAGEAdABvAHIASgBTAEIALQBEAEUAVgBRfVjBrWkBSQAAAAAaAAAAAAAAAAAAAAAAADZmf/wdoShwGwc7CBCpFNGdUHCLsDZPUU=

<<<<  
HTTP/1.1 401 Unauthorized  
WWW-Authenticate: Negotiate  
WWW-Authenticate: NTLM

>>> adatumsts-7 (Requestor IP/STS)  
GET /ads/ls/auth/integrated/?wa=wsignin1.0&wtrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a21z&wctx=https%3a%2f%2ftreys-test%2fclaims%2f5chttps%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&ttindex=0 HTTP/1.1  
Authorization: Negotiate YIIFRWYgKwYBBQUCoIIFOzCCBTegJDAiBgkqhkiC9xIBAgIGCSqGSIB3EgECAGYKkKwYBBAGCNwICCqKCBQ0EggUYJIIIFBQYJKoZIhvcSAQICAQBbagT0MIIE8KADAgEFOQMAQ6iBwMFACAAACjggQDYID/zCCA/ugAwIBBAEfGx1BREZTVk0tQS5OVFRFU1QuTU1DUk9TT0ZULkNPTaIeMBygAwIBAgqEVMBMBEhUVFABc2FkYXRlbXN0cy03o4IDsTCCA62gAwIBF6EDAgECooIDnWSCA5syDvJHfsRntPFOoUy00/THHoAeX2fGt0ND8DenGhkYzdIHU4r98+vIgvn+8iO6qyZR8r8ZPpqIheltafOXWnBCckq8XESARwj4oX1Llnja0i+zoYlvQlv0j8FRVxwiE0Jta5bLnQA+1uMhrRot2F3VAyEzK5kXQFDz7G9PuBSyhrk6nwd9gORXk5AiHlX7H0g03RHe4hYoJ7jTkt9g7lm0wq7RvtsnlvzvW6E1an3UZBjak610lh1kh/zC4YYFKIRtnL2ESLQ2teVerSoMLzyRJu46n4SEY2I5X3J+5Svq+oAwkWUq9B41xqBFEEfI1/4Vc9jwgmmDg8UUvdjiCa4qaAWrsv2JuxiDxHYwYyEiuTCAMz+AniZ4IANQATA/iQV0YEkMcUkWBH6YVz3sz/Sw7KOWmuq8lzhbmgpQdU7GtBkkG7Dj3e3uQffYLUw5AFkxDJlby+q/TBaOtwq/kUfWKTcG1TziWl3wNyyj3CmShctPXlxsJUSUMJj5uVYm9gl7cV0CnaCRM4TJVlQd+eWcuXlwcMrujg2ktZZHAgmk8VxfqjrUyWJbwOgqalZ60uxTId9k3Rxt1kwbICTWqPgeHsDQ3nMOPpHXFLtnqPQvYmKOnCNeJAsqAJ34mOhw4D/Q3qfj9P1dDW1fx0ldBM6AUJ/rpXHGyV3z5EJKLpYqRYpYAm9hrWmmu4/SIALR+5rZHWb5vR4jLiHDGbl2ReqIPhMvP6CUVJGggbIjyvRx5VoYcIm+uRPP3GFej6C4eX9fMrwqN3ktk76bRWZf9HKb9VHuYX/k+tMlktf2VrYAfYqf8oJxMq9XON+Iej3KvqyP3dZgZfaw9389iITrdX4YnzFwKaf/ot/dLYGrgqWxR/xMTYzmMgPjGm8ZVHj6M/CZugh7emvZs2WrZVFWzk2fufFovcgxHc5hzuWav4VtxD0KwplUDnr8DmAK3T65dJ8AsgKpfKaxnbZc+0jDWFZVErgGqgnJCefuOU9QDm/oaFtGgaruQrAUdeAJVUrfNE6rott6jMXECVIOIxtdbAtugbtNhw/9f61Tc0xY+7y/tmY+N5MK1Y/my8a/jJ0+DjFR1UJXUWJMDKun0ITt1xaAmjJAmGsgmkhV6MoAd7JDq3je3oogKcz2rfAavRZt/Gy8ZhvB+QKNFEMWpKq7wXmfUa9w/z6V6q3VHomzipcSGUkr2RQrRpnTcIBopGZcy/kbV1G9RqSB0zCB0KADAgEXooHIB1HFGXJTuH/3yxOagfytHdXt33t4KCBiNzQ/SLH5M/iH4oxfgtJNBj5tNM3rXlRky+36tO0GgLjUTaaBS5P0Fms51HiR9PbK4nY7n335HcdVJQXBFiudOkqGU3U80Kuh6UPrS+ihacMygHCR5E01Dgl1tqveObrarORR0ct1EvnMBOG6saJBRt800sqEjulDL77U7W0Aa9IjDWGreZ+nTzu/rhy+ab0e2tjjgQ8+T+77FUHeYy4B61w7+y5QgnHBBUSP/KAIXaa=

<<<<  
HTTP/1.1 302 Found  
Date: Thu, 13 Jul 2006 07:32:27 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
WWW-Authenticate: Negotiate oYGgMIGdoAMKAQChCwYJKoZIgvcSAQICooGIBIGFYIGCBgkqhkiG9xIBAgICAG9zMHGgAwIBBAEDAgEPomUwY6ADAgEXolwEWjj9oljcrPxx9ipQkjQo69bf5SYXFD7mxzA1pl8q5jKcV4ETZcXVawsYxvnhGV/wTsl/yg8CHMZnZ8D07cNqspIEUkG6joNvB9NQAga4q5441JbEVAblZPZ/9w==  
Location: https://treys-7/ads/ls/?wa=wsignin1.0&ttptsize=2652&ttptindex=0&wctx=https%3a%2f%2ftreys-test%2fclaims%2f5chttps%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&wresult=eNrNWFtzqsos%2fiuW6zGVBYg3rCRlhguAaAA1ysspOESHVEGRPz1e9BoTNYt59R62D4NPW3311%2f3dDM8lDgfwHbXQJzb0CuyOK%2bmaA1TC%2bItSjFsHJJNigde7bEZ5f12QFHYi2Di4u9kByN3%2bx11IVViqkXTHYpuUXlw4Lz59HBjGfobD89YdfZDADGMMtj1DauK1V8bP436NAMGzD%2bvddps%2fftFuzd9lewC79iU5y7Yv1%2b4HeaDRXjAqopzt2UQCPOu%2fd0755hp3RvwLYGzr7zppM9NossHQTQh5lbOxm4vpsXSbNhuK8om8MME%2bFjkyGCOP0oOAdfoz0bQS6O8SB1E4gHuTewgTEAMN%2fpgXsJoPkWm4BSP64FuDFGOQ8DlMfFoSQKk3SSgScvsd7q9C86F8YKP4apB0ly8iz2avtXR59Unj7FnGewamQQzFzozgfo%2b6n55%2bbpz4FdnHo7%2bPahOsHmOyidUyyEqChi6M3%2buqdm31J7GUIoyC%2fQdZ8UqK5vj2Kulay0tQyKoWl1HhnM8%2fs%2bvGB%2bondK94312



Adfoz0bQS608SB1E4gHuTewgTEaMN/pgXsJoPkWm4BSP64FuDFGOQ8D1MFfoSQKk3SSgSC  
vsd7q9C86F8YKf4apB01y8iz2avtXR59Unj7FnGewamQQQzfzogfgo+6n55+bpz4FdnHo  
7+PahOsHmOyidUyyEqChi6M3+uqdm31J7GUIoYc/QdZ8UqK5vj2Kulay0tQyKoWl1HhnM  
8/S+vGB+ondK94312/g8wimeeydrNq5m8OEPDc+yv9QMB+VDZhHyP+xfD4oDco49VGJLzmy  
yi9Ur9PK3pzEpFdWvtYMYZg0ZZYn7+5Pkbw4wdTsedx8An4SpzFJhpj7D/nsv3uoet/  
o/GL6xcAVC/4+XCWk4yvSpy+Hnj3xPGR5yN66r+22NTStx4A3yflDZuftzEW9eDXwDZ/Ox  
j7m4K+OT+HvUn7c/SP+EWUJKgtF7/XdQQGUwydKL87yBVM1Rs/y5Iod4kCU7inID9d8ME2  
22G919HSf3yXNlxmJIiyt5m6hVXWZbfs/YEh3QlmgI5iij40A6/Nc//gn7d+p4eBDDFKTn  
Jm/h406AaYBmiMlyj5BcmGYqha5P380Dde0w7/dZsUdd4vmjma7IMu/c4cpmTJQsGMKsn  
R2NmqY/Nb18b4U8P08xNMRmNCb5Z/284YLqHG7SF/j2+hHOC9HVzv2CHugUnxiGZif8PT  
1eOzibOVTPHN2GVHqWsg5S6BHgV4f3E0eypcpenEu9V8oK7ckvVtLVyZd1YUYTg1c1Gn/J  
5011Fmx1mmaTOBae+MEojVHb+d96NDIj09jLvrlopNJXwsPNN3kWwtuE2Vj4t90Zram4X  
tYg1Y2jTyLGrUFmYHmdV4WW87i6VIm9VO3UNaBPOiR5XrV0emvSA5kpm9SXZK7rXmHZ/G  
WXdBd5mpuJX07ZiQa4ru01X/mI6gf4De4zmQG/APoqzOUS06Nce6uXteCfVLVVCPLtLYV  
FVfKREEARWCUuVBqOoKgyayCeqfdJiCMR+ud9E6Vris5oE5k4EIHMPyStlcinPTFKWYm3  
OVTeXiFOSlVmeWcHtFBFAu6XL8ClhjqLbGFJSGOHZPsnNFJp1kBr88yCKw+XA854ExFVr  
yermwmNviThsVzRqqEhiAVGR7p9jqihVNqcyBQFzSA1HgY1PnQ10017uE4uB4smhLvZZt  
h3SxY7QX1thxeQF0p+9W+NmJNkfjZb/TGa7DDMWjyOeTmeZ07vb8EogLjTrK+ZRq6weJ1  
WNN02k9F6RVHa3+WqzCZRkto8gHGZR5oZfyq4g72IsKhFvVavFycmf0Eas4dKvg9xCeCS  
I0h1rSDYWDpzG7tcUxxz7Q5WOpisAEPGqrPDoS7p1+KYaES4t+BuaQIsGJlJyWhmTexqy  
Jpcka4qzVWXXkqNHeG50cCSAUGEHIEISLriGRPIQBEM+nGviaAj8ERCSwkseRfLs13wP  
zbYkh+Zs6Vn0YZP76zacamJFGrZbrVe/YXvUjtZTKE7YND8pSqH2XS543Z0Piuxye9155P  
ixlBGzy06WHThaJc9Xt2NPJctVWbL2TsZnZOTdPugEvtcupyOtIikMLOZI7tGhPRPtRa7  
wh9RP5CwNNeqvwgs7ritXKUCJs16y291pc4gtElqL3Zmte+dK88BIOrwTux/ojel5SlqG  
DCC9YqeuW; path=/adfs/ls/; secure; HttpOnly  
Set-Cookie: TTPData0=LyWeV5UxqSfdkNR3+REIOaud/KFVTuL+f1nbVmTGV8LPf16  
dhUYf3PalX/hmZVLC7xzZABdmsjOdqXMuqOK8xbKe4wL6bSWV6m2Xykh791vFMyVaOs1  
lrkk+uFC7LnmQTj8zd/nQOyLkLeXYX3x3GU8rrUsn84Lo+cGRAtt4eNHylVDNEDcGhl  
/YOCujud/up3+ZefDPvB3s91IYB7+3VXuK+wLyUR23Le07YWTLP1D1lp62FeOiHAQuF53  
jLdrGTc+3jPFPKwJfdrk+9HLc7ZNDdiylPcivfSV2bCmN6ZEmxMRJ0z3KS6G426mLDqL0  
MYcV1WJ3zJHR8pWozlral0wbkuYqT0leD60fT1hBCVDicNLlmwCRikRIA9QjsGoiff  
4T63Xg3zIFiq6rSQ/RVr29y6LFoyBn2NHQ6T1oTaG/1lJe46h3nqJM8dbELFmpNTRKW7S  
YduLSjlaHXZKO2M/TykrVn3ny93nGygPpVKClJt3qFQfFAfe6Yz8m5m1LXDvvee6/vKp  
fLKxH87tJe4u2AtJhNDPEUXb8LbL/wXaBdT8Qt2sRedfow4A6k1N+iOM3f3xwu9tyv2eu  
Ti+HppT9Owzebb7eAP9x8bzXPTz9gOclvYv3Iy08/kzz9A6cx/kw; path=/adfs/ls/  
; secure; HttpOnly

```
>>> treysts-7 (Resource IP/STS)
GET /adfs/ls/?wa=wsignin1.0&ttpsize=2652&ttindex=0&wctx=https%3a%2f%
2ftreyws-test%2f%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2f
Default.aspx?result=eNRNWftzqsoS%2fuiw6zGVBYg3rCR1hquAaA1ysspHOEShV
EGRPz1e9BoTNYt59R62D4NPW3311%2f3dDM81DgfwHbXQJzboCuyOK%2bmaA1TC%2bItSj
FshJNigde7bEz5f12QFHYi2Di4u9kByN3%2bx11lVivqkXTHYpuUX1W4Lz59HBjGfofbD
89YdfZDADGMmtj1DauK1V8bP436NAMGzD%2bvddps%2fftFuzd91ewc79iu5y7Yv1%2b4
HeaDRXjAqoptz2UQCPOu%2fd0755hp3RvWLYGrZ7zppM9NossHQQTqH51bOxm4vpsXSbNhu
K8om8MME%2bFjkyGCOP0oOAdfoz0bQS608SB1E4gHuTewgTEaMN%2fpgXsJoPkWm4BSP64
FuDFGOQ8D1MFfoSQKk3SSgSCvsd7q9C86F8YKf4apB01y8iz2avtXR59Unj7FnGewamQQQ
zfzogfgo%2b6n55+2bbpz4FdnHo7%2bPahOsHmOyidUyyEqChi6M3%2buqdm31J7GUIoYc
%2fQdZ8UqK5vj2Kulay0tQyKoWl1HhnM8%2fS%2bvGB%2bondK94312%2fg8wimeeydrNq
5m8OEPDc%2byv9QMB%2bVDZhHyP%2bxfD4oDco49VGJLzmyi9Ur9PK3pzEpFdWvtYMYZg0
ZZYn7%2b5Pkbw4wdTsedx8An4SpzFJhpj7D%2fnsv3uoet%2fo%2fGL6xcAVC%2f4%2
bXCWk4yvSpy%2bHnj3xPGR5yN66r%2b22NTStx4A3yflDZuftzEW9eDXwDZ%2foXj7m4K%
2bOT%2bHvUn7c%2fSP%2bEWUJKgtF7%2fXdQQGUwydKL87yBVM1Rs%2fy5Iod4kCU7inID
9d8ME222G919HSf3yXNlxmJIiyt5m6hVXWZbfs%2fYEh3QlmgI5iij40A6%2fNc%2f%2fg
n7d%2b2p4eBDDFKTnJm%2fh406AaYBmiMlyj5BcmGYqha5P380Dde0w7%2fdZsUdd4vmjma
7IMu%2fc4cpmTJQsGMKsnR2NmqY%2fnb18b4U8P08xNMRmNCb5Z%2f284YLqHG7SF%2fj2
%2bhHOC9HVzv2CHugUnxiGZif8PT1eOzibOVTPHN2GVHqWsg5S6BHgV4f3E0eypcpenEu9V
8oK7ckvVtLVyZd1YUYTg1c1Gn%2fJ5011Fmx1mmaTOBae%2bMEojVHb%2bd96NDIj09jLvr
lopNJXwsPNN3kWwtuE2Vj4t90Zram4XtYg1Y2jTyLGrUFmYHmdV4WW87i6VIm9VO3UNaB
POiR5XrV0emvSA5kpm9SXZK7rXmHZ%2fGWXdBd5mpuJX07ZiQa4ru01X%2fmI6gf4De4zm
QG%2fAPoqzOUS06Nce6uXteCfVLVVCPLtLYVfVfKREEARWCUuVBqOoKgyayCeqfdJiCMR%
2bud9E6Vris5oE5k4EIHMPyStlcinPTFKWYm3OVTeXiFOSlVmeWcHtFBFAu6XL8ClhjqLb
GFJSGOHZPsnNFJp1kBr88yCKw%2bXA854ExFVryermwmNviThsVzRqqEhiAVGR7p9jqihV
NqcyBQFzSA1HgY1PnQ10017uE4uB4smhLvZZth3SxY7QX1thxeQF0p%2b9W%2bNmJNkfjZ
b%2fTga7DDMWjyOeTmeZ07vb8EogLjTrK%2b2ZRq6weJ1WNN02k9F6RVHa3%2bWqzCZRkto
8gHGZR5oZfyq4g72IsKhFvVavFycmf0Eas4dKvg9xCeCSIOh1rSDYWDpzG7tcUxxz7Q5WO
pisAEPGqrPDoS7p1%2bKYaES4t%2bBuaQIsGJlJyWhmTexqyJpcka4qzVWXX HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint,
```



application/msword, application/x-shockwave-flash, \*/\*  
Accept-Language: en-us  
UA-CPU: x86  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2;  
SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)  
Host: treysts-7  
Connection: Keep-Alive  
Cookie: \_TTPRealm=urn:federation:adatum

<<<

HTTP/1.1 302 Found  
Date: Thu, 13 Jul 2006 07:32:27 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
X-AspNet-Version: 2.0.50727  
Location: https://adatumsts-7/adfs/ls/?wa=wsignin1.0&wtrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a27&wctx=https%3a%2f%2ftreys-test%2fclaims%2f%5chttps%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&ttpindex=1727  
Set-Cookie: \_TTPData=eNrNWfzqsoS/iuW6zGVBYg3rCR1hquAaAA1ysspHOEShVEGRPz1e9BoTNYt59R62D4NPW3311/3dDM81DgfWHBxQJzb0CuyOK+maA1TC+ItSjFshJUN1gdE7bEz5f12QFHYi2Di4u9kByN3+x11IVViqkXTHYpuUX1W4Lz59HBjGfobD89YDfZDADGMMtj1DauK1V8bP436NAMGzD+vddps/ftFuzd91ewc79iu5y7Yv1+4HeaDRXjAqopzt2UQCPOu/d0755hp3RvwLYGrZ7zppM9NossHQTQh51bOxm4vpsXSbNhuK8om8MME+FjkyGCOP0oAdfoz0bQS608SB1E4gHuTewgTEaMN/pgXsJoPkWm4BSP64FuDFGOQ8D1MfFoSQKk3SSgSCvsd7qC9c6F8YKp4apB0ly8iz2avtXR59Unj7FnGewamQQzFzofgqo+6n55+bpz4FdnHo7+PahOsHmOyidUyyEqChim3+uqdM31J7GUIoYc/QdZ8UqK5vj2Kulay0tQyKoWL1HhnM8/S+vGB+ondK94312/g8wimeeydrNq5m8OEPdc+yv9QMB+VDZhHyP+xfD4oDco49VGJLzmyi9Ur9PK3pzEpFdWvtYMYZg0ZZYn7+5Pkbdw4wdTsedx8An4SpzFJhpuj7D/nsv3uoeQt/o/GL6xcAVC/4+XCWk4yvSpy+Hnj3xPGR5yN66r+22NTStx4A3yflDZuftzEW9eDXwDZ/Oxj7m4K+OT+HvUn7c/SP+EWUJKgtF7/XdQGQUwydKL87yBVM1Rs/y5Iod4kCU7inID9d8ME222G919HSf3yXN1xmJIiYt5m6hVXWZbfs/YEh3QlmqI5iij40A6/Nc//gn7d+p4eBDdFKTnJm/h406AaYBMiM1yJ5BcmGYqha5P380Dde0w7/dZsUd4vmjma7IMu/c4cPmTJQsGMKsnR2NmQy/Nb18b4U8P08xNMRmNCb5Z/284YLqHG7SF/j2+hHOC9HVzV2CHugUnxiGZif8PT1eOzibOVTPHn2GVHqWSG5S6BHgV4f3E0eycpnEu9V8oK7ckvVtLVyzdlYUYTg1c1Gn/J5011FmX1mmaTOBae+MEoJvHb+d96NDIj09jLvrlOpNjXwsPNN3kWwtuE2Vj4t90Zram4XtYg1Y2jTyLGuUFmYHmdV4WW87i6VIm9V03UNaBPOiR5XrV0emvSA5kpm9SXXZK7rXmHz/GWXdBd5mpuJX07ZiQ4aru01X/mi6gf4De4zmQG/AP0qz0US06Nce6uXteCfVLVVCPLtLVYFVkrEEAWRUCUvBqOoKGYayCeafdJiCMR+ud9E6Vris5oE5k4EIHMPySt1cinPTFKWYm30VTEiFOSL1VmeWcHtFBFAu6XL8ClhjqlbGfJSGOHZPsnNFJp1kBr88yCKw+XA854ExFVryermwMNViThsVzRqQehiAVgr7p9jqihVNqcYBQFsZA1HgY1PnQ10017uE4uB4smhLvZzth3SxY7QX1thxeQF0p+9W+NmJNkfjZb/TGa7DDMwjyOeTmeZ07vb8EogLjTRK+ZRq6weJ1WNn02k9F6RVHa3+WqcZXRkto8gHGZR5oZfYq4g72IsKhFxFvFycmf0Eas4dkVg9xCeCSI0h1rSDYWDpzG7tcUxxz7Q5WOpisAEPGqrPDoS7p1+KYAES4t+BuaQISGJIJyWhmTexqyJpcka4qzWVXX; path=/adfs/ls/; secure; HttpOnly

>>> adatumsts-7 (Requestor IP/STS)

GET /adfs/ls/?wa=wsignin1.0&wtrealm=urn%3afederation%3atreys+research&wct=2006-07-13T07%3a32%3a27&wctx=https%3a%2f%2ftreys-test%2fclaims%2f%5chttps%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&ttpindex=1727  
HTTP/1.1 Cookie: WebSsoAuth=eNrNV1tz4rgS5qekmMcU4zvYVJI68hXbGGIbC1h01ZYr8iVg3zBmF+/AkImYSe7c07Nw/pJarW7v/661ZIEsJfdDEFZwqJK8uzufaSKj90/QgYnqJAiej5DUz2ahIME60Gm51F9zvWogA0DpnunlmUN1ays3Kx67JI43u/hgx5BzfDBkCKH5MB50ykeu3WRDUMYwM190Rm6gVvVaffOcf/zYgLEgkfufwQSN1nwsHdZOXwhPZiJHfLpBxmbgrLYeUPbWCMh8R3fOheA+g+PZxjE/IsSE6C8m6SVzwm8wJ+hRiPtlNpAcLqhPWjDnvVeBmK6iCBmQ8tWfZf4p/svzu6UXm6ibkqYHtXwBK6hR8/YJ91b+Y/N4/dBHZ1G0yTkwk3CEU0mq8T1JUwH711/EbfaeVCX5r4RV7mYfUBWfdJiRf69ijqWkNjM8toFS5Wk51NPEvrwxfSj3bf8b65fgNfxTCrEv9s1a7cCqZoFvdZ/g8F81nZgFWcB38tn09KwybJgrwprzmya+8V+txbbIJKRQ102MECizs5L1IXeY+rajvESNKPyeqW3xFPZe5uv+dFhPkbN01LbP486T6BIE2yBCXDrfLiP5ey/e7n6Vv8n41fWXhGp0dL1fWKpRpr67g7cK/J4zPOO/er6ffHrtS6iYbEASotMvu58Vy6/rwF0B2b30s3E0Nn9y/R32jfSv9J9xCnqZ5dhr/XtQGQowydKb89yBVirze/16QwmkRjThNKgT23w0TbLdFvv911NiX+8pOogwVUQevffEdV9M03xvqDAd1JRzDQWpBGUSfete/oLBqfU9PQhulmdoJ2+S44cGdQc2UV4kVzx+YZLACPxksgcPfs8n6Oxb9w77gOcXzXxCvPrur4xd4mzJgiEStiFH3dxSH7vffu0If3qYFW5WogMxLT+M/zccMNVDTb6FQa+8hn0G9OvmvmAH+whOTCJ0Jv4/PL1zdDFxqZopv4na7CgV/bDRJcCrebmFoppdUTg68T5qPmDv3KLxx1p4z95FUyTRzKxEHQsG0j2jzI/zQtPmAkHvjAaI7T2/XbDxIZWJQCd9xvFxlI+EZ7x+li2ltyMrSblviZn9mZpu6UGLG0W+xy2poX5QaY0XtZpZ7kScbPdqXuIi2BRD7Bm/erIuB+mR3Rmb9KdUvnkgnwsugv8T4x7eSv1lhTYjhfbxlj9kyBgfop14C+QD+QYftJaolg30

iW7mXkXC6VIWnews1N1UVCVEQQNFGoFF5EKm6QkWPbILTJx1mYMJH6128ThSuwXlgzmgUgA  
sew/EY2V+LCNEWpYeausmkdmY/9zGLmKbcPRAD1Bm8mr4AyZmprzEBjiBP3LDteZdJZzVc  
rgywCm48mCx4Y4GU16ulRXjLce63OGWoSmgAXBHsnWKRHiWa0gkHALQyAaLAJ6bOR6Zor  
3YpxsHJdE1LA9K2I7zeEdoLZey4qga6w7pt+ezEm6Pxsst/pBMcQI/Eo8tV0rrnT+z2/AuJ  
Sw45yNcNo/SBReuJsGPK5Rq3qaLFrHSD0ZbyK4wAUUOaFQWp7MXewly2IuLbRktX03mBzS  
nFwsub3EERJKo5GWtqPhIOvEbulxRFHFujysVFFYAI+plU+PyLuHbYRI8S1hT8Dc4Sh4EQ  
QzRpDMj/GrImNSRni/KSr6rmjxnt/gnImgEgAbiJDEK66hoTyCCIRjPhoXoiRiFBHgEiKr  
nkU0T48T0yaUmOzPnKt/DDpgrWNJwSsYZ5q7U3ONIEg6uN1JyxbXjQNMLJd7PieXM+Qr6  
b0WXtleejRs7BXYKzfOQUsbhQXcaeTVcerdg6U1DTebMwz7ohL9HNTOT1XEoiK3ckd2Thv  
pjvx+Rkg+onDpZWPk6t2m+ZV4/SmnFKbFeUtvdlJlg0EJCPxvUku2kBa1H7K1Z7A/bX+kJ6  
fnk3k5iIXujnVld9IPKqE1RPuiGpP+RHIMsvTh6MrGaasPvVybiE4ES3fp5dZyavlou;  
WebSsoAuth0=cFf+wmdmNhb4wZEBdGWqOftPmfFHLecvlR8xLqXzWPYybe8pB/+H3zhc  
KPHWty1zhfzBBVqznBpxgn/ua/68D9C+NX1q19wfJjPM72Pp4hBQgXAkQLHeHjTKG61Fjo  
3AYZANDgro73f7WUBzL4FZseFej6RRyPt7dZC6L7Bq5DFt+c8pNU8XhbrA7rW1kIyCKKsg  
8JxsqX7pVbx9XBSKHDqyy7HY6yGnGyK/f1HkeWVVO61vY1GCjy0pMcaC71tOGt/PxwNtBL  
WEXWw5ht153xwbZK49jyassXVNuKQwVwdK+HygAz01BCXzcsNP11QsXoKR51b+Cu0EiL58  
X7Lc2htVYbhs1VktBx5129y6qUm5BKXGjUYpOcX2BrtqxR1zWGRO+syU11SncznLsWw3ZX  
ByiSlHq0/FWT/b5S8vBT33F+v1jpoFnG0jSun77SsM6wfstmNeJJuduir132B+99/2ucn28  
PhGdPzzSpXASvY04dOPt0dwa73mwz/RcxnVJos+6kPI6ndsXEXor7mGQFOjCnhdtB4iyvT  
B64L+fbv4du0f0mBdfz0bQS608SBL4gHuTewgTEaMN/pgXsJoPkWm4BSP64FuDFGO8D1  
h+mAzudXxxvSh+98dbHvCJ2Pt+eO2JHS7SvIURDw83cCBZ/AgPdteY=; \_LSCleanup=  
2006-07-13:07:32:27Zr0urn:federation:trey research; \_TTPDest=urn:  
federation:trey research; TTPData=eNrNWFtzqsoS/iuW6zGVBYg3rCRlhquAaAA  
1yessphOESHVEGRPzle9BoTNYt59R62D4NPW3311/3dDM81DgEWHBXQJzboCuyOK+maA1TC  
+ItSjFshJJNigde7bEz5f12QFHYi2Di4u9kByN3+x11IVViqkXTHYpuUX1W4Lz59HBjGfo  
fbD89YDFZDADGMMtjLDauK1V8bP436NAMGZd+vdDps/ftFuzd91ewc79iu5y7Yv1+4HeaD  
RXjAqopz2TUQCPOu/d0755hp3RvwLYGrZ7zppM9NosshQTQh51b0xm4vpsXSbNhuK8om8M  
ME+FjkykzG00o0Adfoz0bQS608SBL4gHuTewgTEaMN/pgXsJoPkWm4BSP64FuDFGO8D1  
MFfoSQKk3SSgScvsd7q9C8F6YKp4apB0ly8iz2avtXR59Unj7FnGewamQQzFzozgfoqo+6  
n55+bpz4FdnHo7+PahOsHmOyidUyyEqChi6M3+uqgM31J7GULOYC/QdZ8UqK5vj2Kulay0  
tQyKoWLLHhnM8/S+uVB+ondK94312/g8wimeeydrNq5m8OEPDc+yv9QMB+VDZhhYp+xfD4  
oDco49VGJLzmyi9Ur9PK3pEpFdwvtYMYZg0ZZYn7+5Pkbdw4wdTsedx8An4SpzFJhpuj7  
D/nsv3ueQt/o/GL6xkAVC/4+XCWk4yvSpy+Hnj3xPGR5yN66r+22NTStx4A3yflDZuftz  
EW9eDXwDZ/Oxj7m4K+OT+HvUn7c/SP+EWUJKgtF7/XdQGGUwydKL87yBVMLRs/y5Iod4kC  
U7inID9d8ME222G919HSf3yXN1xmJiIyt5m6hVXWzbfS/Yeh3QlmlqI5iij40A6/Nc/gn7  
d+p4eBDDkFtnJm/h406AaYBmiMlyj5BcmGYgha5P380Dde0w7/dZsUDD4vmjma7IMu/c4c  
pmTJYsGMKsnR2NmQY/Nb18b4U8P08xNMRmNcb5Z/284YLqHG7SF/j2+hHOC9HVzv2CHUgU  
nxiGzif8PTLeOzibOVTPHN2GVHqWsG5S6BHgV4f3E0eypcpcnEu9V8oK7ckvVtLVyzdlYUY  
Tglc1Gn/J5011Fmx1mmaTOBae+MEojVhb+d96NDIj09jLvrLopNJXwsPNN3kWwtuE2Vj4t  
90Zram4XtYglY2jTYLrUFmYHmdV4WW87i6VIm9VO3UNABPOiR5XrV0emvSA5kpm9SXZK7  
rXmHZ/GWXdBd5mpuJX07ZiG4Aru01X/mI6gf4De4zmQG/AP0qzOUS06Nce6uXteCfVLVVC  
PLtLYVfVvkREEAWRWCuuVBqOoKgyayCeqfdJiCMR+ud9E6VriS5oE5k4EIHMPyStlcinPTF  
KWYm30VTeXiFoS1VmeWchtfBFAu6XL8C1hjqlbGFJSGOHZPsnNFJp1kBr88yCKw+XA854E  
xFVryermwmNViThsVzRqqEhiAVgr7p9jqihVNqcYBQFsZA1HgY1PnQ10017uE4uB4smhLv  
ZZth3Sx7QX1thxeQrOp+9w+NmJNkfjZb/TGa7DDMWjyOeTmeZ07vb8EogLjTrK+ZrQ6we  
J1WNn02k9F6RVHa3+WqcZXRkto8gHGZR5oZfYq472IsKhFxFvFycmf0Eas4dKvg9xCeC  
SIOh1rSDYWDpzG7tcUxxz7Q5WOpisAEPGqrPDos7p1+KYAES4t+BuaQISGJIJyWhmTexqy  
Jpcka4qzVvXXkqNHeG5OCCSAUGEHIEISLrigrPIJQBEM+nGvIAaj8ERCSwkseRfLs13wPz  
bYkh+Zs6Vn0YZP7zZABdmsjOdgXMuqOK8xbKe4wL6bSWV6m2YxkH791vFMYVaOs1lrkk/uc  
c7LNmQtigP58D/nQOyLk1eXYX3x3GU8rrUsn84LO+cGRAtt4eNHY1VDNEdcGh1/YOCujud  
/up3+ZeDPvB3s91IYB7+3VXUk+wLyUR23Le07YWTLP1D1lp62FeoIHAQuF53jLdrGTC+3  
jPFPkWFdrk+9H1C7ZNDdiyLpCivfSV2bCmN6ZEmxMRJ0z3KS6G426mlDqL0MYcV1WJ3zz  
JHR8pVozlral0wbkuYt0LeD60fT1hBCVdIcNL1mwcRIKRIA9QjsGoiFF4T63Xg3zIFi  
q6rSQ/RvR29y6LFoyBn2NHQ6T1oTaG/11Je46h3nqJM8dbElFMPNTRKW7SYduLSjlaHXZK  
O2m0/TykrVn3ny93nGyGppVKClJt3qFQfFAfe6Yz8m5m1LXDvvee6/vKpflKxH87tJe4u2  
AtJhNDPEUXb8LbL/wXaBdT8Qt2sRedfow4A6k1N+iOM3f3xwu9tyv2euTi+HppT9Owzebb  
7eAP9x8bzXPTz9gOclvYv3Iy08/kzz9A6cx/kw=

<<<  
HTTP/1.1 302 Found  
Location: https://treysts-7/adfs/ls/?wa=wsignin1.0&ttptime=2652&  
ttptimeindex=1727&wctx=https%3a%2f%2ftreyys-test%2fclaims%2f%5chttps%  
3a%2f%2ftreyys-test%2fclaims%2fDefault.aspx&wresult=kqNHeG5OCCSAUGEH  
IEISLrigrPIJQBEM%2bnGvIAaj8ERCSwkseRfLs13wPzbYkh%2bZs6Vn0YZP7zZacMJF  
GrZbrVe%2fYXvUjtZTKE7YND8pSqH2XS543Z0Piuxye9155PxlBGZyO6WHThaJc9Xt2

NPJctVWbL2TsZnZOTdPugEvtcupyOtIikMLOZI7tGhPRPtRa7wh9RP5CwuNEqvwqs7rit  
XKUcJsl6y291pc4gtElqL3Zmte%2bdK88BIOrwTux%2fojel5SlqGDCC9YqeuWLyWeV5U  
xqSfdkNR3%2bREI0aud%2fkFVTuL%2bflnbVMTGV8LPf16dhUYvF3PalX%2fhMzVLC7xz  
ZABdmSj0dqXMuqOK8xbKe4wL6bSWV6m2XykH791vFMyVaOs1lrkk%2fuC7LnmQTigP58  
D%2fnQOYLk1eXYX3x3GU8rrUsn84LO%2bcGRAtt4eNHY1VDNEdcGh1%2fyOCujud%2fup  
3%2bZefDPvB3s91IYB7%2b3VXuK%2bwLyUR23Le07YWTLP1D1lp62FeOiHAQuF53jLdrG  
Tc%2b3jPFPkWFdrk%2b9HLC7ZNDdiyLPcivfSV2bCmN6ZEmxMRJ0z3KS6G426mLDqL0M  
YcV1WJ3zzJHR8pWVozlral0wbkuYqT0leD60ft1hBCVdIcNL1mwcRIKRIA9QjsGoiff4  
T63Xg3zIFiq6rSQ%2fRvR29y6LFoyBn2NHQ6T1oTaG%2f11Je46h3nqJM8dbElFMpNTRK  
W7SYduLSjlaHXZKO2m0%2fTykrVn3ny93nGygPpVKClJt3qQfFAfe6Yz8m5m1LXDvvee  
6%2fvKpFLKxH87tJe4u2AtJhNDPEUXb8LbL%2fwXaBdT8Qt2sRedfow4A6k1N%2biOM3f  
3xwu9tyv2euTi%2bHppT9Owzebb7eAP9x8bzXPTz9gOclvYv3Iy08%2fkzz9A6cx%2fkw  
%3d

>>> treysts-7 (Resource IP/STS)

GET /ads/ls/?wa=wsignin1.0&ttpsize=2652&ttpindex=1727&wctx=https%3a%  
2f%2ftreyws-test%2fclaims%2f%5chttps%3a%2f%2ftreyws-test%2fclaims%2fd  
efault.aspx&wresult=kqNHeG50cCSAUgEHIEISLrIGRPIJQBEM%2bnGViaAj8ERCSwk  
serFLs13wPzbYkh%2bz56Vn0YZP76zacMJFGRzbrVe%2fYXvUjtZTE7YND8pSQH2XS54  
3Z0PiuXye9155PixlBGZyO6WHTaJc9Xt2NPJctVWbL2TsZnZOTdPugEvtcupyOtIikML  
OZI7tGhPRPtRa7wh9RP5CwuNEqvwqs7ritXKUcJsl6y291pc4gtElqL3Zmte%2bdK88BI  
OrwTux%2fojel5SlqGDCC9YqeuWLyWeV5UxqSfdkNR3%2bREI0aud%2fkFVTuL%2bflnb  
VMTGV8LPf16dhUYvF3PalX%2fhMzVLC7xzZABdmSj0dqXMuqOK8xbKe4wL6bSWV6m2Xyk  
H791vFMyVaOs1lrkk%2fuC7LnmQTigP58D%2fnQOYLk1eXYX3x3GU8rrUsn84LO%2bcG  
RAtt4eNHY1VDNEdcGh1%2fyOCujud%2fup3%2bZefDPvB3s91IYB7%2b3VXuK%2bwLyUR  
23Le07YWTLP1D1lp62FeOiHAQuF53jLdrGTC%2b3jPFPkWFdrk%2b9HLC7ZNDdiyLPci  
vSV2bCmN6ZEmxMRJ0z3KS6G426mLDqL0MYcV1WJ3zzJHR8pWVozlral0wbkuYqT0leD6  
0ft1hBCVdIcNL1mwcRIKRIA9QjsGoiff4T63Xg3zIFiq6rSQ%2fRvR29y6LFoyBn2NHQ  
6T1oTaG%2f11Je46h3nqJM8dbElFMpNTRKW7SYduLSjlaHXZKO2m0%2fTykrVn3ny93nG  
ygPpVKClJt3qQfFAfe6Yz8m5m1LXDvvee6%2fvKpFLKxH87tJe4u2AtJhNDPEUXb8LbL  
%2fwXaBdT8Qt2sRedfow4A6k1N%2biOM3f3xwu9tyv2euTi%2bHppT9Owzebb7eAP9x8b  
zXPTz9gOclvYv3Iy08%2fkzz9A6cx%2fkw%3d HTTP/1.1

Cookie: \_TTPRealm=urn:federation:adatum; \_TTPData=eNrNWFtzqsoS/iuW6zG  
VBYG3rCRlhuAaaAlyssphOEShVEGRPzle9BoTNYt59R62D4NPW3311/3dDM81DgFWHBX  
QJzb0CuyOK+maA1TCtItSjFshJJNigde7bEZ5f12QFHYi2Di4u9kByN3+x11IVviqkXTH  
YpuUx1W4Lz59HBjGfofBd89YdfZDADGMMtjLDauK1V8bP436NAMGzD+vddps/ftFuzd91  
ewc79iu5y7Yv1+4HeadRXjAqopzt2UQCPOu/d0755hp3RvwLYGrZ7zppM9NossHQQTQh51  
bOxm4vpsXSbNhuK8om8MME+FjkyGCOP0oOAdfoz0bQS608SB1E4gHuTewgTEaMN/pgXsJ  
oPkWm4BSp64FuDFGOQ8D1MFfoSQK3SSgScvsd7q9C86F8YKp4apB0ly8iz2avtXR59Unj  
7FnGewamQQQzfzogfgo+6n55+bpz4FdnHo7+PahOsHmOyidUyyEqChi6M3+uqdm31J7GUI  
oyC/QdZ8UkL5y2Kulay0tQyKoWL1Hhnm8/S+vGB+ondK94312/g8wimeeydrNq5m8OEPD  
c+yv9QMB+VDZzhHyP+xfd4oDco49VGJLzmyi9Ur9PK3pzEpFdWvtYMYZg0ZZYn7+5Pkbw4  
wdTsedx8An4SpzFJhpj7D/nsv3uoEQt/o/GL6xcAVC/4+XCWk4yvSpy+Hnj3xPGR5yN66  
r+22NTStx4A3yflDZuftzEW9eDXwDZ/Oxj7m4K+OT+HvUn7c/SP+EWUJKgtF7/XdQQQUwy  
YPL18yBwM1Rs/y5Iod4kCU7inID9d8ME222G919HSf3yXN1xmJiyt5m6hVXWZbfs/Yeh3  
QlmqI5iij40A6/Nc//gn7d+p4eBDDFKTnJm/h406AaYBmiMlyj5BcmGYqha5P38ODde0w7  
/dzSUDD4vmjma7Imu/c4cpmTJQsGMKsnR2NmQY/Nb18b4U8P08xNMRmNcb5Z/284YLqHG7  
SF/j2+hHOC9HVz2CHugUnxiGZif8PT1eOzibOVTPHn2GVHqWGS65BHGv4f3E0eycpnE  
u9V8oK7c1kLVyZdlUYUtg1c1Gn/J5011Fmx1mmaTOBae+MEojVhb+d96NDIj09jLvr1o  
pNjXwsPNN3kWwtuE2Vj4t90Zram4XtYglY2jTyLGrUFmYHmdV4WW87i6VIm9VO3UNaBPOi  
R5XrV0emvSA5kpm9SxZK7rXmHZ/GWXdBd5mpuJX07ZiqA4ru01X/mI6gf4De4zmQG/APOq  
zOUs06Nce6uXteCfVLVVCPLtLYVfVvkREAAWRWCUvBqoKGYayCeQfdJiCMR+ud9E6VriS  
5oE5k4EIHMPyStlclnPtFKWYm3OVTeXIFOSlVmeWcHtfBFAu6XL8ClhjqlbGfJSGOHZPsu  
NFJp1kBr88yCkW+XA854ExFVryermwMNViThsVzRqqEhiAVGR7p9jqihVNqcYBQFSZA1Hg  
Y1PnQ10017ue4uB4smhLvZZth3SxY7QX1thxeQF0p+9W+NmJNkfjZb/TGa7DDMWjyOeTme  
ZO7vb8EogLjTrK+ZRq6weJ1WnN02k9F6RVHa3+WqcZXRkto8gHGZR5oZfYq4g72IsKhFxV  
avFycmf0Eas4dKvg9xwCecSI0h1rSDYWDpzG7tcUxxz7Q5WOpisAEPGqrPDoS7p1+KYaES4  
t+BuaQIsGJIJyWhmTexqyJpcka4qzVWXX

<<<

HTTP/1.1 302 Found  
Date: Thu, 13 Jul 2006 07:32:28 GMT  
Location: https://treyws-test/claims/?wa=wsignin1.0&ttpsize=2708&  
ttpindex=0&wctx=https%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&  
wresult=eNrNWFtqjow%2fiuW59HqDd7aS3V3TUBRUFaQFX2ZihAuKgkSEPHXT9DW  
bfc%2bu6dnaj8cnsLK41lvfumQ15CWjSddAhxTRZIBsNA6S3CQ7hA1EI4IpKp3CPaZd  
pvZa9pMk6nIctX0UQvqDzVACox8k9riMcyjWeb3J8jUv1lCb1t5cHZOR8wH57oTDCdw  
G1KE4Cgkv3kdx7Lf%2b79VxD9eam%2f1Rttfinhms%2fP3U2z9WnTpu3EXSR7Wwa5Z  
JMaYpkTBOIGTVm%2fPmJbz1V6ybf6tZr3Vp7%2fa4Tv5bTGHdd5KAYFka6SYzyUowo

grHt10sq3JJ4gWLK517LVSYI8EFBNQYF6SsWgTsgXQxDRLUj3Z0Bddyt%2fuC78OZH  
%2bd1FkWAkAS0pJFFQC6J0e%2fIMoUJnsTATQrKjzrtm84tcKkTIGwjlqMkDuwC%2  
f27ok8pbkTPKk1b4nNGnhH3C2XsYhJR74T6qfnr%2fe3Tuk183e84xKCCg49KuWODP  
SBrbt%2fIpxNFQhYEDe0rc5CEh5bdPCYIOTNLwhfuMdsMnZBew3LtkCKn%2fTRM13Y  
47sCe5R01PzWSen%2fydKC4c0Uzfb5Y%2b4N7j8e7ae3ASH%2bEksC%2boswQmKGTv  
pY%2fyL8qyxTL9UV1FiU%2bcX4oUf1DqZgF2SEZvJTBln1tkJ%2b9vGqtE2Sm03QDF  
JYnEifx6vb6XwHyqlD%2bAEwY4YmMGCYn%2fdY39D5uE7%2f5%2fBL9F5U6A%2byou  
t6glrJI2aYI%2bT%2fxz3PjIs3QfFZ%2b9lvshDPbAcVjToOWPpzSCNvoGyfJnGwu4  
T9Eb%2fJr1J%2b3P0v%2fGwYRhSHAx%2frosVcaYZegS8j%2fDdBCtNPqzJiv6KYEO  
iskRxf9slqwMwyBjvk%2bT%2b%2b26mgUeZkUUv7fe07Esy35k9Qsf1pV4ju9wTMGh  
gfdX%2bfoVcorW9%2fYiQkwwW8n74PzQoEpg7xG2hfvhbyCrXJUvIJ%2fQyX6yqw38  
V7nEPfD5JswH2jGFT9SH1QuSgVwUfztTaW7Ir%2bW%2fvndQeHsxY4gp231D%2bjD%  
2b33ggfER7EiHnid7cuVD6PtXvosM9kusFHttz%2f5843WN0hbhWjYmb1qkyIaitDM  
fgMM09sVbFyT6d2mzHe9R84e6xZePHWrhn76qIe4MFMbB5xsE6nDdirEdh5gyHJ%2f  
uUq67WbrbgpcK1%2fdpYLMKV2YjsYfU3XYpt%2bnIUoY7SjupI7encWwuk1045HaN  
TFLttsiOecXP233TfWx62LKRu53ou1hut6G2%2fpIMTLenu%2fCkwqja9aUsbPORq  
cnX98odatB%2bePkLEQVK5QtZapMturr1ZEh8i8j1f%2b9spp8pwcTeB2JxZnNLbYu  
1thkucdvRRHEBw9ksqA8eTRoSerdA8XTP52Bjuni7g78LbP2MF4A%2b10APrFXDziR9  
1Vvoeq%2bfNedwsM%2fxkudb2GjOw87R6QEkzXymbUfDNeVcnfuZ21PgrXA%2byeSL  
TBXU38LMDHTFgJQPTA8Ehr1PztdNDhOoB%2f4dCXAJgIWx1k3moneqs%2bSGP5Gc  
9FEHhDX6%2fk00yY7ks0MqU5oBNOqsg5TiZnrjoeB7OipXDQPjaIittxro5Ned0Zzd  
FxrEqLSRue832FHV2DyUi11%2bPFRLGgk4TD2dLeWs2phG1nq001UqkNfTWWN66Rzt  
Ozu%2bHTsamPDkdRrX3reQJAPPKST%2f0nzdN15zshZU%2ba4JyZCSzPgBwIqKoZp  
43cFXQGI1Dq30llfYHL9D7LQ7%2fdE%2fqPPot6u8%2fiVi10Rf  
Set-Cookie: \_TTPData=; expires=Wed, 12-Jul-2006 07:32:28 GMT; path=  
/adfs/ls/Set-Cookie: \_WebSsoAuth=eNrNV1uXqrgS9qe4nEeXG/COq7vXCSAKC  
gre0JdZacJFJSgXEX/9BG3dds/uffqcnQ/DU6hUqr76q1JJXmIY7Hsgj1GU+CEuP0a  
S8F5s90uo0bLhNSYTOeuNR2rXWPNn1Nju7SfoIMs22xWylIcp0jCcQJx8lqp03S7R  
ndqTGN0d3qNeq/e3bzrRK+VNMI9B9kogoWTXhKhvByhGMHI8iplBW7DaImimMy9Vhg  
i8PHwTnY47hXgL7ZCmHsxxOMaxT3Eqs3A8q4x/yge/Aer+Xt5RoIh2LbLwRxxWQ0TD  
jlhhL4CSxQmeBIBJykqP+t07zrvVfQ+whbSEdxEvlWYf/h6JPKm5ckh7hHUUXMwVx  
LyBLK2kM/iKkX6qPqp/9fw6c+xxX3Z5/8wgS0nbjHF/ZnYRpZ6J26QnyjLvCtKIxDJ  
3lKSOXtU4KgDZM0eKE+W7vbD80dT3LvhEMYe990UdesiIWC6JxULZ0ni/zs7Xh+aYd  
d+vXu6YpDbx/vob2Tk3gIJ751tTpLYIIC81/+KP9NWXZIpj8qKyjxQvtvRQc/KPUyH  
9thFt9LYJaaWZq1738qqUTJLRQdHOVLMYwCSLwXUsepjy0PBTD+QxiKQ3j4EUbuVQQ  
WU7XyBuzAxx5JNKzC6D837n9YyfAe/0fjd1YeAKjF8XJnLSGVZKYJ+jzx7wnjI87yY  
1Qse630A+jvgW2TphFXPk7GB2ihb4CsfPaxhPsUvcHfo/6k/Vn633DzYRCEuBj/s6g  
Vgphk6Er5P4N0EIXp4z8FwDRPGRwOUXhC0b8bJSnDwE+S780kvtxXM9/FpIii99b7A  
JZ12Y+scvDuhJN0SxFFOzYd/+o3FYhu2h9by88xCEm03nvX54aVbns3TDyEy/4wiR  
DMXRhsobOVs1imviPsp16wvNNMx+QRTGsxR5krpZ05KCo0JnKC116rfzxvYvC28s8g  
jmuJ28P43/NxwIn9A+PCC7Ft/DuUL6vrkv2KGewQm+S87c/4enB0c3E7eqsXHTOFc  
nIerKwzE4zrAwVhmc7N0pRU68Z80X6sEtGT/XwiN7N0UsDJahjucX7G+CRTPC2iHI7  
OHwbJ1zxVG7rQ5cTbKRU3vjlZbCenW/WiKLBruSuvHIKic7GLdSW+p0o2i+TM7Bit  
o1M1FJNzXpWUvn/XJKkx0L+Fc0nOPPWyP08022DZGsp7R1mIXnBV4mAoNQ5yxphafP  
c2UG0Yzpk+TC3e0GoKfYFN5s1Veb4E8gX8ZofwW1dGiqWEm8DbiiuzubUxxdpLFJkKb  
ver5ERxdkEgdcaTRoinLDBcXXP1+Ayrm7ofzB2xGc0BbiEAG0W3M1FbC0tNE/pza  
wEH+3wjcp6F9dYiYe+2AJCY0Zm6BQ11LuXKvJ8pggyvsstDj111Cqed+1ugca665IA  
y5w093xj7iz1UEvXcc/hvGpoiABNuq4HMxe94d90HaSS18YIHjvjtGo+zbjpkfkr  
bgA8YQSQ1K0k8mFYobgOK+qKRx0T81Qwd0oV8ZzacOOFug0VsTlpAsv+b5Krq7+ZKR  
Yq/FyIhvDSULhbGVtjdZUXJY91PBKrtahnhJjppqOni/TimHQ6nmuj4wkZa9sZy4cRg  
Hn1rB37bbPlhGdraaRt1ZNPBGTWbWBoeACVzHUHjgKaA8AsbCHrc1Sm9Uke+12B6z/  
HzGvdPuGNKXR5/jiYSWZD0BSe5Au4AiHdde+6AgckHkgg47K10MqaAnctjJAKjckN5  
J0sFWRWNixyp9MTjlV3RXwoJ3ZibqpOW7Qm  
jnLIkdZlOknesBRouWKTNU1RQeh8x40iBrhm4RWue52Tmm2tcBCIHJJZrg6bGjMbpI  
vdJRhuUz2fQvayV8TFVXeY6R0ln2WzIyefFtjQbX5tdD0F7nLPbjSHTa2NjQ761M7GS  
rutsbvGtBK7U3Gyopw3WClkyptU9qTPRxPLJHGSn5cA7WIGurcl6tCSyBtFryLEiDS  
DhJeLcvshpFqmbGbed; path=/adfs/ls/; secure; HttpOnly  
Set-Cookie: \_WebSsoAuth=85y/5fgneQbCdR00ddoSwt04frXt2Yyefvazri9ze  
yAy9sBzvvBJK33tJ0cXwHtbL4Cr837id0+GeP4Z03gWirG+auVm/RwbG59+DUYPoSH  
vFgmxt4f7mVln6XGg5mRP/X0vAlJhpGSMZGxhr7Ufyh1j0S7Enc5yKpzmlBFE4V4Jt  
44h64Y9SEORD7DuL6n5eileZiK/pAWW96Z43jRpZxox5DHkAdobY09K/FXSddWmq3H  
M1Btgme3sZT1Yq055TBqMqtSbx6HcMHWns0eSYUHA4TEt8U6nzfeNxZoz3E4w97VLJ  
7Ini5FPCU6GeLQKkWh30moibyProFdN52L7YLZi80A7dLfLqjwFKp/vJvokX515/uQ  
OAm6ky1W4pGT2kiEYhkyX0lm0ZkLqhoZwAr96hxt92cRbzKn2ozmxuG8M7Akr7ACr  
H57Z8WH43oozOXp2mcoWrrH8yiPWWufezvtgtV23e5o0B268x2rZ3BqHraM+0qa6ue  
OeZPcuin16LA/e+/jrnJ/G78xpT+7dNNqs6ZZY2iTnNzNFqpBx2rVgp02w3QcFjWad  
qn0y1dhiXm6VupPdVnl+1VgmUvnoqlLjSV/fxE196vvSWnKHK6+X9/3GR+ww53Ngf  
; path=/adfs/ls/; secure; HttpOnly  
Set-Cookie: \_LSRealm=urn:federation:adatum; expires=Sat, 12-Aug-2006

07:32:28 GMT; path=/adfs/ls/; secure; HttpOnly  
Set-Cookie: \_LSCleanup=2006-07-13:07:32:28ahttps://treyws-test/  
claims/; path=/adfs/ls/; secure; HttpOnly  
Set-Cookie: \_TTPDest=https://treyws-test/claims/; path=/adfs/ls/;  
secure; HttpOnly  
Set-Cookie: TTPData=eNrNWFuTqjoW/iuW59HqDd7aS3V3TUBRUFQAQFX2ZihAuK  
gkSEPHXT9DWbfc+u6dnaj8cnsLK41vfumQ15CWjSddAhxTRZlbsNA6S3CQ7hA1E14I  
pKp3CPaZdpvZa9pMk6nIctX0UQvqDzVACox8k9riMcyjWeb3J8jUvilCblt5cHZOR8w  
H57oTDcdwG1KE4Cgkv3kdx7Lf+79VxD9eam/1Rttfinhms/P3U2z9WnTpu3EXSR7Ww  
a5ZJMaYpkTBOIGTVm/PmJbz1V6ybf6tZr3Vp7/a4Tv5bTGHdd5KAYFka6SYzyUowog  
rHt10sq3JJ4gWLK517LVSYI8EfBNQYF6SsWgTsgXQxDRLuJ3Z0Bddyt/uc78OZH+d1  
FkWANKASOpJFEQC6J0e/YiMoUJnsTATQrKjzrtm84tcKkTIGwj1qMkDwC/27ok8pbk  
TPKklb4nNgNhH3C2XsYhJR74T6qfnr/e3Tuk183e84xKCCg49KuWODPSBrbt/IpxNf  
QhYEdE0rc5CEh5bdPCYIOTNLwhfMdsMnZBew3LtkCKn/TRM13Y47sCe5R01PzWsen  
/ydKC4c0uzfb5Y+4N7j8e7ae3ASH+EksC+oswQmKGTvpY/yL8qyxTL9UV1FiU+cX4o  
Uf1DqZgF2SEZvJTBLN1tkJ+9vGqtE2Sm03QDFJYnEIfx6vb6XwHyqld+AEwY4YmGc  
Yn/dY39D5uE7/5/BL9F5U6A+yout6glrJI2aYI+T/xz3PjIs3QfFZ+9lvshDPbAcVj  
ToOWPgzSCNvoGyfJnGwu4T9Eb/Jr1J+3P0v/GWyRhSHAx/rOsVcaYZegS8j/DdBCTN  
PqzJiv6KYEoisKRx9slqWmWYBjvk+++26mgUeZkUUv7fe0E7Esy35k9QsflpV4ju9  
u9wTMGhgfdX+2bfvCorW9/YiQkwwW8n74PzQoEpg7xG2hfvhbyCrXJUvIJ/QyX6yqw38V  
7nEPfD5JswH2jGFT9SH1QuSgVwUFztTaW7Ir+W/vndQeHsxY4gp231D+jD+33ggfER  
7E1hnid7cuVD6PtxvosM9kusFhttz/5843WN0hbhwjYmb1qkyIaitDMfGMMO9sVbFy  
T6d2mzHe9R84e6xZepHwrhn76qIe4MFMB5xsE6nDdirEdh5gyHJ/uUq67WbrbgcPK  
l/DpYLMKV2YjsYfU3Ypt+nIUoY7Sjup17encWwuk1045HaNTFLtSi0ecXPZ332F  
Wa6Z2LKRu53oulhut6G2/pIMTLenu/Ckwqjaa9uSbPORqcnX98odatB+ePKLEQVK5Q  
tZapMturrlZEh8i8j1f+9spp8pwcTeB2JxZnNLbYulthkucdvRRHEBw9ksgA8eTRoS  
ErdA8XTP52BJni7c78LBP2MF4A+l0APrFXDziR91Vvoeq+fNedwsM/XkuDb2GjOw87  
R6QEkkZYXmbUFDNeVcNUL21PvGrXa+yeSLTBX0U38LdMHTFgJQtdEY8rW1PztdNDHoo  
oB/4dCXAjgIWx1k3moneqs+SGP5Gc9FEHhDX6/k00yY7ks0MqU5oBNOqsg5TiZnrjo  
EB7OipXDQPjaIittxr05Ned0ZzdFxrEqLSRue832FHV2DyUill+PFRLGGk4TD2dLeW  
s2phG1nq00lUqkNfTWWN66RztOzu+HTsamPdKdRrX3rEQjAPPKST/0nzdn15zshZU  
+a4JyZCSzPgbWgKoZp43cFXQIDq30l1fYHL9D7LQ7/dE/qPPot6u8/iVi10RFEmw  
Mmbek9XRZyV4PVYMDzvptsTgCwCGWRCTpJGwAMHPDtjQZJH2C37R1sDmZ0Ni9wZ/EQ  
QVn1JGxqJk2zWffdzsieuGuVIB1dbSV63VUG9cFN0XVUBYbbpoKgBIVNFVWhf5uRMX  
6kCBJKAlI5Qgw290huk8905HFSEXZDCznmvSvOL7jAzJmo/y2YHQZS9ODAGPu8Mwfm  
472zX1sKvrAUPxeZug9V0Vevkttm4FLLN3XtuM26; path=/adfs/ls/; secure;  
HttpOnly  
Set-Cookie: \_TTPData0=IUvGvLZndSZtsHLcDLLjYbHdmjok/Y9WjBZnenVFark  
A8jiEgteXxJ0m9XNTNiaohBsBfFBngGyqsGhwds9chzXLti+Yxnks51VbZE7A6nqDH  
z3NzZ5ta//jNEziP7WD+HytJ8E7aMlnX76KJ16xdhYnVNN7USTwU+7VtUgOFJ284GU  
08P9bFPz8ONQy9ma+nUtAlZhrGSsZGxjv7kfk1rrs2lndERNdJNuQOIyV41W9dSDM  
sZpEQSQ2wEC85cLaTzTBIXfK8j+1NsNja80j1byhiKAO2tsS8nwtJpelrD04Xq1B9g  
pdPaK0Y417zTmDUYTao1Dk0lvjF0wRnJlG2BgMe8LLqtZ7FvzVeC5bVCM9DPrdiZzE  
cB13MzJK1lQZLTSiuJso01i1823LMTgNmyk4d61N4uKsoUaGk+mxITfhkSxam3CIWR  
oVTgglM65wXqoptwahW5y2zp7m0A2wSVEy03Z8kvM7cSiM2rei0s7CsLLEK7P7zq  
bRYTXsmcp0ZdejpUGLIsppx97n/k4/Y+255rR0nA49c9cxMjjjDRNuq98qa6ueOeZVc  
uy1377A/e+/9rHL7N2aCr64GMhp12aFtHyBqkvvtQ/SN24dGsSNGZB/Y+eX6AXb72I  
lIgjOfJ4cbHvweXpv9GF40/QH23jHf/wK+/rF+vLy+/ULlIn9w9WNY/vYu5u0//Xcu  
dA==; path=/adfs/ls/; secure; HttpOnly

>>> treyws-test (WS Resource)  
GET /claims/?wa=wsignin1.0&httpsize=2708&httpindex=0&wctx=https%3a%2f%  
2ftreyws-test%2fclaims%2fdefault.aspx&wresult=eNrNWFuTqjoW%2fiuW59Hq  
Dd7aS3V3TUBRUFQAQFX2ZihAuKgkSEPHXT9DWbfc%2bu6dnaj8cnsLK41vfumQ15CWjSd  
dAhxTRZlbsNA6S3CQ7hA1E14IppKp3CPaZdpvZa9pMk6nIctX0UQvqDzVACox8k9riMcyj  
Web3J8jUvilCblt5cHZOR8wH57oTDcdwG1KE4Cgkv3kdx7Lf%2b79VxD9eam%2f1Rttf  
inhms%2fP3U2z9WnTpu3EXSR7Wwa5ZJMaYpkTBOIGTVm%2fPmJbz1V6ybf6tZr3Vp7%2  
fa4Tv5bTGHdd5KAYFka6SYzyUowogrHt10sq3JJ4gWLK517LVSYI8EfBNQYF6SsWgTsg  
XQxDRLuJ3Z0Bddyt%2fuC78OZH%2bd1FkWANKASOpJFEQC6J0e%2fIMoUJnsTATQrKjz  
rtm84tcKkTIGwj1qMkDwC%2f27ok8pbkTPKklb4nNgNhH3C2XsYhJR74T6qfnr%2fe3  
Tuk183e84xKCCg49KuWODPSBrbt%2fIpxNfQhYEdE0rc5CEh5bdPCYIOTNLwhfMdsMn  
ZBew3LtkCKn%2fTRM13Y47sCe5R01PzWsen%2fydKC4c0uzfb5Y%2b4N7j8e7ae3ASH%  
2bEksC%2boswQmKGTvpY%2fyL8qyxTL9UV1FiU%2bcX4oUf1DqZgF2SEZvJTBLN1tkJ%  
2b9vGqtE2Sm03QDFJYnEIfx6vb6XwHyqld%2bAEwY4YmGcYn%2fdY39D5uE7%2f5%2f  
BL9F5U6A%2byout6glrJI2aYI%2bT%2fxz3PjIs3QfFZ%2b9lvshDPbAcVjToOWPgzSC  
NvoGyfJnGwu4T9Eb%2fJr1J%2b3P0v%2fGWyRhSHAx%2frOsVcaYZegS8j%2fDdBCTN  
PqzJiv6KYEoisKRx9slqWmWYBjvk%2bT%2b%2b26mgUeZkUUv7fe0E7Esy35k9QsflpV4  
ju9wTMGhgfdX%2bfvCorW9%2fyiQkwwW8n74PzQoEpg7xG2hfvhbyCrXJUvIJ%2fQyX  
6yqw38V7nEPfD5JswH2jGFT9SH1QuSgVwUFztTaW7Ir%2bW%2fvndQeHsxY4gp231D%2

bjd%2b33ggfER7EiHnid7cuVD6PtxvosM9kusFHttz%2f5843WN0hbhWjYMb1qkyIait  
DMfgMMO9sVbFyT6d2mzHe9R84e6xZePHWrhn76qIe4MFMB5xsE6nDdirEdh5gyHJ%2f  
uUq67WbrbgcpK1%2fdpYLMKV2YjsJYfU3XYpt%2bnIUoY7SjupI7encWwuk1045HaNTF  
LTtSi0ecXPZ332Fwa6Z2LKRu53oulhut6G2%2fpIMTLenu%2fCkwqjaa9uSbPORqcnX9  
8odatB%2bePkLEQVK5QtZapMturrlZEh8i8j1f%2b9spp8pwcTeB2JxZnNLbYulthkuc  
dvRRHEBw9ksgA8eTRoSERda8XTP52BjNi7g78LbP2MF4A%2b10APrFXDziR91Vvoeq%2  
bfNedwsm%2fXkuDb2GjOw87R6QEKZXymbUFdNeVcNfuZ21PgRXa%2byeSLTBX0U38LdM  
HTFgJQTdEy8rW1PztDndH0oob%2f4dCXAjgIWx1k3moneqs%2bSGP5Gc9FEHhDX6%2fk  
00yY7kS0MqU5oBNOqsg5TiZnrjoEB7OipXDQPjaIittxro5Ned0ZzdFxrEqLSRue832F  
HV2DyUii11%2bPFRLLGGk4TD2dLeWs2phGlnqOOLUqkNfTWWN66RztOzu%2bHTsamPdkd  
rRx3rEQjAPPKST%2f0nzdN15zshZU%2ba4JyZCSzPgBwIgKoZp43cFXQGIIdq3O11fYHL  
9D7LQ7%2fde%2fqPPot6u8%2fiVi10Rf HTTP/1.1

<<<  
HTTP/1.1 302 Found  
Cache-Control: private  
Content-Length: 316  
Content-Type: text/html; charset=utf-8  
Location: https://treysts-7/adfs/ls/?wa=wsignin1.0&wreply=  
https%3a%2f%2ftreyws-test%2fclaims%2f&wct=2006-07-13T07%3a32%3a28Z&  
wctx=https%3a%2f%2ftreyws-test%2fclaims%2fDefault.aspx&ttpindex=1758  
Set-Cookie: \_TTPData=eNrNWfuTqjoW/iuW59HqDd7aS3V3TUBRUFAQFX2ZihAuKqk  
SEPHXT9DWbfc+u6dnaj8cnsLK41vfumQ15CWjSddAhxTRZIBsNA6S3CQ7hAlEi4Ipkp  
3CPaZdpvZa9pMk6nIctX0UQvqDzVACox8k9riMcjWeb3J8jUvilCblt5cHZOR8wH57o  
TDcdwG1KE4Cgkv3kdx7Lf+79VxD9eam/lRttfinhms/P3U2z9WnTpu3EXSR7Wwa5ZJM  
aYpkTBOIGTvm/PmJbz1V6ybf6tZr3Vp7/a4Tv5bTGHdd5KAYFka6SYzyUowogrHt10sq  
3J4gWLK517LVSYI8EFBNQYF6SsWgTSgXQxDRLuJ3Z0Bddyt/uc780ZH+d1FkWANKAS0  
pJFEQC6J0e/IMoUJnsTATQrKjzrtm84tcKkTIgWjlqMkDuwC/27ok8pbkTPKklb4nNGn  
hH3C2XsYhJR74T6qfnr/e3Tuk183e84xKCCg49KuWODPSBrbt/IpxNfQhYEdE0rc5CEh  
5bdPCYIOTNLwhFuMdsMnZBew3LtkCKn/TRM13Y47sCe5R01PzWSen/ydKC4c0uZeb5Y+  
4N7j8e7ae3ASH+EksC+oswQmKGTvpY/yL8qyxTL9UUVlFiU+cX4oUflDqZgF2SEZvJTBL  
N1tkJ+9vGgtE2Sm03QDFJYnEIfx6vb6XwHyqlid+AEWY4YmMGCYn/dY39D5uE7/5/BL9F  
5U6A+yout6glrJi2aYI+T/xz3PjIs3QfFZ+9lvshDPbAcVjToOWPkzSCNvoGyfJnGwu4  
T9Eb/Jrlj+3P0v/GWyRhSHAx/roSVcaYZegS8j/DdBCtNPqzJiv6KYEOiskRxf9slqWm  
wyBjvk+T++26mgUeZkUUV7fe07E5y35k9Qsfl1pV4ju9wTMghgfdx+foVcorW9/YiQkww  
W8n74PzQoEpg7xG2hfvhbyCrXJUvIJ/QyX6yqw38V7nEPfD5JswH2jGFT9SH1QuSgVwU  
FztTaW7Ir+W/vndQeHsxY4gp231D+dJ+33ggfER7EiHnid7cuVD6PtxvosM9kusFHttz  
/5843WN0hbhWjYMb1qkyIaitDMfgMMO9sVbFyT6d2mzHe9R84e6xZePHWrhn76qIe4MF  
MbB5xsE6nDdirEdh5gyHJ/uUq67WbrbgcpK1/DpYLMKV2YjsJYfU3XYpt+nIUoY7Sjup  
I7encWwuk1045HaNTFLTtSi0ecXPZ332Fwa6Z2LKRu53oulhut6G2/pIMTLenu/Ckwqj  
aa9uSbPORqcnX98odatB+ePkLEQVK5QtZapMturrlZEh8i8j1f+9spp8pwcTeB2JxZnN  
LbYulthkucdvRRHEBw9ksgA8eTRoSERda8XTP52BjNi7g78LbP2MF4A+10APrFXDziR9  
1Vvoeq+fNedwsm/XkuDb2GjOw87R6QEKZXymbUFdNeVcNfuZ21PgRXa+yeSLTBX0U38L  
dMHTFgJQTdEy8rW1PztDndH0oob/4dCXAjgIWx1k3moneqs+SGP5Gc9FEHhDX6/k00yY  
7kS0MqU5oBNOqsg5TiZnrjoEB7OipXDQPjaIittxro5Ned0ZzdFxrEqLSRue832FHV2D  
yUii11+PFRLLGGk4TD2dLeWs2phGlnqOOLUqkNfTWWN66RztOzu+HTsamPdkdkrRx3rEQj  
APPKST/OnzdN15zshZU+a4JyZCSzPgBwIgKoZp43cFXQGIIdq3O11fYHL9D7LQ7/dE/qP  
Pot6u8/iVi10Rf; path=/claims; secure; HttpOnly

>>> treysts-7 (Resource IP/STS)  
GET /adfs/ls/?wa=wsignin1.0&wreply=https%3a%2f%2ftreyws-test%2fclaims  
%2f&wct=2006-07-13T07%3a32%3a28Z&wctx=https%3a%2f%2ftreyws-test%  
2fclaims%2fDefault.aspx&ttpindex=1758 HTTP/1.1  
Cookie: TTPRealm=urn:federation:adatum; WebSsoAuth=eNrNVluXqrgS9qe4  
nEeXG/Coq7vXCSAKCgre0JdZacJfJSgXEX/9BG3dds/uffqcNQ/DU6hUqr76q1JjXmIY7  
HsgjlGU+CEuP0aS8Fr5s9Ouo0bLbNSYToeuNR2rXWPNN1nju7SfOImS22xWylIcp0jCcQ  
Jx81qp03S7RndqTGN0d3qNeq/e3bZrRK+VNMI9B9kogoWTXhKhvByhGMHI8iplBW7DaIm  
imMy9Vhgi8PFHwTnY47hXgL7ZCmHsxz0MAxT3Eqs3A8q4x/yge/AeR+Xt5RoiH2LbLwRxw  
Q0TDj1hhL4CSxQmeBIBJykgP+tt07zrvVkfGq+whbSEdxEv1WYf/h6JPKm5ckh7hHUUXMMVx  
LyBLK2km/ikKx6qPqp/9fW6c+xx3Z5/8wgS0nbjHF/ZnYRpZ6J26QnyjLvCtKIxDJ31KS  
OxtU4KqGD2m0eKE+W7vbD8OdT3LvhEMyE990UdesiIWC6JxULZ0ni/zs7Xh+aYdd+vXu6YP  
dBx/vob2Tk3gIj751tTpLYIIC81/+KP9NWXZIpj8qKyjxQvtvRQo/KPUyH9thFt9LYJaaW  
2Ql738qqUTJLrQdH0VlMYwCSLwXuSepjy0PBTD+QXiKQ3j4EUbuVQQWU7XyBuzAxz5JNkz  
C6D837n9YyfAe/0fjd1YeAKjf8XJnLSGVZKYJ+Jzx7wnjI87yY1Qse630A+jvgW2TphFXP  
k7GB2ihb4CsfAxhP5UvcHfo/6k/Vn633DzYRCeUBj/s6GvGphk6Er5P4N0EIXp4Z8FwDR  
PGRwOUXhC0b8bJsnDwE+S780kvtXm9/FpIii99b7AJZl2Y+scvVDuhJN0SxFFOZyD/+o3  
FYhu2h9by88xCeM03nvX54aVBns3TDyEy/4wiRDMXRhsobOVs1imviPsp16wvNNMx+QRTG  
sxR5krpZ05KCoOJnKC116rfzxxvYvC28s8gJgmJ28QP43/NxwIn9A+PCC7Ft/DuUL6vrkv2  
KGewQm+S87c/4enB0c3E7eqsXHTOfcnIerKwzE4zrAwVhmc7NOpRU68Z80X6sEtGT/XwiN

7N0UsdJahjucX7G+CRTPC2iHI70HwbJ1zxVG7rQ5cTbKU3vjLZbCeNw/WikLKbrUsvvHIk  
Ic7GLdSW+po02i+TM7Bit0M1FJNzzXpWUvn/XJKkx0L+Fc0nOPPyP08022DZGsp7R1mI  
XnBV4maoNQ5yphafPc2UG0Yzpk+TC3eoGoFkyFN5s1Veb4E8gX8ZofwWldGiWQEm8Dbii  
zubbUxxdPLFJkbVver5ERxdkEgdcATROinLDBcXP1+Ayrm707fzB2xGc0BbiEAAAG0W3M1F  
bc0tNE/pZawEH+3wjc6F9dYiYE+2AJCY0Zm6BQ1lLuXkVj8pggyvstsdJ11lCqed+lugc  
a665IAy5w093xj7iz1UeVXc+/hVGpoiABNuq4HMxe94d90HaSS18YIHvju0Go+zbjpkf  
rubgA8YQsq1KOK8mfYobgOK+qKRx0T81Qwd0oV8ZzacOOvFug0VsTlPAsv+b5Krq7+ZKRYq  
/FyThvDSULhbGvtjdZUxJY91PBKrtAHnhJJpqoni/TimHQ6nmuj4wkZa9sZy4cRgHn1rB3  
7bbPlhGdraaRtLZNPBGTWbWoEAcVzHuhjgKaA8AsbCHrc1Sm9Uke+l2B6z/HzGvdPuGNK  
XR5/jiYSWZD0BSe5Au4AiHDde+6AgckHkgg47K1OMqaAnCtJjAkcjKN5J0sFWRWNixyp9M  
Tjlv3RXWoJ3ZibqpoW7QmjnLI  
kdZlOknesBRouWKTNU1RQEh8x40iBrhM4RWue52Tmm2tcBCIHJJZrg6bGjMbpIvdJRhUu  
Z2fQvayV8TFVXeY6ROIn2WzIyefTjQbx5td0F7nLpBjSHTa2NjQ761m7GsrutsbvGtBK7  
U3Gyopw3WC1kyptU9qTPRXLJHGSn5cA7WIGurcl6tCsYBtFryLEiDSdHJelcvshpFqmbG  
bed;\_WebSsoAuth0=85y/5fgneQbCdR0OdoSwt04frXt2Yefvazri9zeyAy9sBzvvBJ  
K3tJ0cXwHtbL4Cr837ld0+GeP4z03gWirG+uAvm/RwbG59+DUYPosHvFgmXt47f7m1N6G  
Gg5mRP/X0vAlJHpGSMZGxhr7UfyhljOS7Enc5yKpzmlBFE4V4Jt44h64Y9SEORD7DuL6n5  
eileZiK/pAWW96Z43jRpZxox5DHkAdobY09K/FXSddWmq3HMLbtgme3sZT1YqO55TBqMqt  
Sbx6HcMHWNS0eSYUHA4Tet8U6nzfeNxxZoz3E4w97VLJ7Ini5FPCU6GeLQKkWh30moibyPR  
oFdn52LY7Lzi80A7L7Lid0+Gep4z03gWirG+uAvm/RwbG59+DUYPosHvFgmXt47f7m1N6G  
OzWAr96hxt92cRbzKn2ozmxuG8M7Akr7ACrH57Z8WH43oozOXp2mocWrrH8yiPWWufezvt  
gtV23e5oOB268x2rZ3BqHraM+0qa6ueOeZPcuin16LA/e+/jrnJ/G78xpT+7dNNqs6ZYZ2  
iTnNZNFqpbX2rVGP02w3QcFjWadqn0y1dhiXxM6VuPpdIvnl+lvGmUvnoqlljSV/fxEl96  
vVSwNHXh+X9/3GR+vv53Ngf;\_LSRealm=urn:federation:adatum;\_LSCleanup=  
2006-07-13:07:32:28Zahttps://treyws-test/claims/;\_TTPDest=  
https://treyws-test/claims/;\_TTPData=eNrNWfuTqjoW/iuW59HqDd7a5S3V3TUB  
RUFAQFX2ZihAuKkgSEPHXT9DwBfc+u6dnaj8cnsLK4lVfumQ15CwJsddAhXTRZlbsNA6S  
3Cb71AE1AIPk3CPA2dpvZa9pMk6nIctX0UQVqDzVACox8k9riMcjWeb3J8jUvilClbt  
5cHZOR8wH57oTdcdwG1KE4Cgkv3kdx7Lf+79VxD9eam/lRttfihms/P3U2z9WnTpu3EX  
SR7Wwa5ZJmAYpkTBOIGTvm/PmJbz1V6ybf6tZr3Vp7/a4Tv5bTGHdd5KAYFka6SzyUow  
ogrHtl0s3JJ4gWkL517LVSYI8EfbNQYF6SSwGTSGXqXDRLu3Z0Bddy/uc780ZH+dlF  
kWANKASOpJFEQC6J0e/IMoUJnsTATQrKjzrtm84tcKkTIGwjLgMkDuwC/27ok8pbkTPKk  
lb4nNGnhH3C2XsYhJR74T6qfnr/e3Tukl83e84xKCCg49KuWODPSBrbt/IpxNfQhYEdE0  
rc5CEh5bdPCYIOTNLwhfuMdsMnzBew3LtkCKn/TRM13Y47sCe5R01PzWsen/ydK4c0uZ  
fb5Y+4N7j8e7ae3ASh+Eksc+oswQmKGTvpY/yL8qyxTL9UV1FiU+C40Uf1DqzGF2SEZv  
JTBLN1tkJ+9vGqtE2Sm03QDFJYnElfx6vb6XwHyqld+AEwY4YmmGCYn/dY39D5uE7/5/B  
L9F5U6A+you6g1rJ12aYI+T/xz3PjIs3qFFz+9lvshDPbAcVjToOWPkzSCNvoGyfJnGw  
u4T9Eb/Jr1J+3P0v/GWYRhSHax/rOsVcaYZegS8j/dBCTNPqzJIv6KYEoisKRxf9slqW  
MwyBJvk+T+26mgUeZkUUV7fe07Esy35k9QsfpV4ju9wTMGhgfdX+foVcorW9/YiQkww  
W8n74PzQoEpg7xG2hfvhbyCrXJUvIJ/QyX6yqw38V7nEPfD5JswHJZjGFT9SH1QuSgVwUF  
zTnTaW7I+r+w/vndQeHsx47gpp23ld+jD+33ggfER7EiHnid7cuVd6PtXvsoM9kusFHttz/  
5843WN0hbbWjYmb1qkyIaitDMfgMMO9sVbFyT6d2mzHe9R84e6xZepHWrhN76qIE4MFMB  
B5xsE6nDirEdh5gyHJ/uuq67WbrbgcpK1/DpYLMKvY2jsJYfU3XYpt+nIuoY7SjupI7e  
nWwukl045HaNTFLTtSi0ecXPZ332Fwa6Z2LKRu53oulhut6G2/pIMTLenu/Ckwjja9u  
SbPORqcn98odatB+EpkLEQVK5QtZapMturrlZEh8i8jlf+9spp8pwcTeb2JxznNlbYul  
thkucdvRRHEBw9ksgA8eTRoSerdA8xTP52BJni7g78LBp2MF4A+10APrFXDziR91Vvoeq  
+fnedwsM/Xkudb2GjOw87R6QEkZxymbUfdNeVcnfuZ2LPgRXa+yeSLTBXOU38LdMHTfgJ  
QtdEY8rwlPztdNDH0ooB/4dCXAjgIwX1k3moneqsgSGP5Gc9FEHhDX6/k00yY7kS0MqU5  
oBNOqsg5TiZnrj0E7ipXDQPjaIittxro5Ned0ZzdFxrEqLsRue832FHV2DyU11l+PFR  
LGGk4TD2dLeW52phG1nqOOLUgkNfTWNW66RztOzu+HTsamPdkdRrX3reQjAPPKST/Onz  
dN15zshZU+a4JyZCSzPgBwIgKoZp43CFXQGIDq30l1fYHL9D7LQ7/dE/qPPot6u8/ivi1  
0RfEwmMmbek9XRZyV4PYMDZvptsTgCwCGWRCTpJGwAMHPDtjQZJH3C37R1sDmZ0Ni9wZ  
/EQQVn1JGxqJk2zWFfdZsieuGuVib1dbSV63VUG9cFNNOXVUBYbbpKgbIVNFVWhf5uRMX  
6kCBJKALI5QgW290huk8905HFSEXZDCznmvSvOL7jAzJmo/y2YHQSZ90DAGPu8Mwfm472  
zXlsKvraUPxexZug9V0VevktthM4FLN3xtuM26;\_TTPData0=IUvGvLZndSztSHLcdLL  
jYuBhdjmoK/Y9WjBZnenVFArKA8jiEgteXxJ0m9XNTNiAohBsBfFBngGyqsGhwds9chzX  
Lti+Yxns51VbZE7A6nqDH3ZnZ5ta//jNEZiP7WD+HytJ8E7aMlnX76KJ16xdhYnvNn7  
UStwU+7vtUgOFJ284GU08P9bFPr8ONQy9ma+nUtAlZHRGSsZGxjv7kfkilrrs2lndERNd  
jNuQOIYv41W9dSDMSzPEQSQ2wEC85cLaTzTBIXFK8j+lNsNja80j1byhiKAO2tsS8nwTJ  
pelrD04Xq1B9gpdPAK0Y417zTmdUYTa01Dk0lvjF0wRnJlg2BgMe8LQzt7FvzVeC5bVC  
M9DPrdizEcb13MzPK1lQZLTsiuJso0l11823LMTgNmyk4d61N4uKsoUaGk+mxifHkSx  
aM3CIWRvTgg1M65wxBQqptwAhW5y2zp7m0A2wSVEy03Z8kvM7cSiM2rei0  
s7CsLLEK7P7zzqBRYTXsmcp0ZdejpuGLIsp97n/k4/Y+255rR0A49c9cxMjjdRNuq9  
8qa6ueOeZVcuy1377A/e+/9rHL7N2AcR64GMhp12aFtHyBqkvvtQ/SN24dGSNGZB/Y+e  
X6AXb72l1IlgJofJ4cbHvHwXp9GF40/QH23jHf/wK+/rF+VLy+/ULlIn9w9WNY/vYu5u0  
//XcudA==

<<<  
HTTP/1.1 302 Found

Location: https://treys-test/claims/?wa=wsignin1.0&ttpsize=2708&ttpindex=1758&wctx=https%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&wresult=EwmMmbek9XRZYv4PVYMDzvpTsTgCwCGWRCTpJGWAHPDtpjQZJHZC37R1sDmZ0Ni9wz%2fEQQVn1JGxqJk2zWFFdZsieuGuV1b1dbSV63VUG9cFN0XVUBYbbpKqBIVNFVWhf5uRMX6kCBJKAL15Qgw290huk8905HFSEXZDCznmvSvOL7jAzJmo%2fy2YHQSZ90DAGPu8MwFM472zX1sKvrAUPxeZug9V0VevktthM4FLN3XtuM26IUvGvLZndsZtsHLcD LLjYuBhdmjok%2fy9WjBZnenVFarKA8jiEgteXxJ0m9XNTNiaohBsBfFBngGyqsGhwds9chzXLti%2bYxnks51VbZE7A6nqDHz3NzZ5ta%2f%2fjNEZiP7WD%2bHytJ8E7aMlnX76KJ16xdhYnVnN7UstWU%2b7VtUg0FJ284GU08P9bFPr8ONQy9ma%2bnUtAlZHRGSSzGxjv7kfkilrrs2lndERNdJnuQOIyV4lW9dSDMsZpEQSQ2wEC85cLaTzTBIXfk8j%2blNsNja80jlbyhiKA02tsS8nwTJpelrD04Xq1B9gpdPaK0Y417zTmDUYT a01Dk0lvjF0wRnJlg2BgMe8LLqtZ7FvzVeC5bVCM9DPrdizZecB13MzJKI1LQZLTSiuJs o0li1823LMTgNmyk4d61N4uKsoUaGK%2bmxITfHkSxaM3CIWRoVtgg1M65wxBQqptwah W5y2zp7m0A2wSVEy03Z8kvM7cSiM2rei0s7CsLLEK7P7zZqbRYTXsmcp0ZdejpuGLIsp px97n%2fk4%2fy%2b255rR0NA49c9cxMjjdRNUq98qa6ueOeZVcuy1377A%2fe%2b%2f9rHL7N2aCr64GMhp12aFtHyBqkvvtQ%2fSN24dGsSNGZB%2fy%2beX6AXb72I1IlgJofJ4cbHvweXpv9GF40%2fQH23jHf%2fwK%2b%2frF%2bVly%2b%2fULlIn9w9WNY%2fvYu5u0%2f%2fXcudA%3d%3d

>>> treys-test (WS Resource)

GET /claims/?wa=wsignin1.0&ttpsize=2708&ttpindex=1758&wctx=https%3a%2f%2ftreys-test%2fclaims%2fDefault.aspx&wresult=EwmMmbek9XRZYv4PVYMDzvpTsTgCwCGWRCTpJGWAHPDtpjQZJHZC37R1sDmZ0Ni9wz%2fEQQVn1JGxqJk2zWFFdZsieuGuV1b1dbSV63VUG9cFN0XVUBYbbpKqBIVNFVWhf5uRMX6kCBJKAL15Qgw290huk8905HFSEXZDCznmvSvOL7jAzJmo%2fy2YHQSZ90DAGPu8MwFM472zX1sKvrAUPxeZug9V0VevktthM4FLN3XtuM26IUvGvLZndsZtsHLcD LLjYuBhdmjok%2fy9WjBZnenVFarKA8jiEgteXxJ0m9XNTNiaohBsBfFBngGyqsGhwds9chzXLti%2bYxnks51VbZE7A6nqDHz3NzZ5ta%2f%2fjNEZiP7WD%2bHytJ8E7aMlnX76KJ16xdhYnVnN7UstWU%2b7VtUg0FJ284GU08P9bFPr8ONQy9ma%2bnUtAlZHRGSSzGxjv7kfkilrrs2lndERNdJnuQOIyV4lW9dSDMsZpEQSQ2wEC85cLaTzTBIXfk8j%2blNsNja80jlbyhiKA02tsS8nwTJpelrD04Xq1B9gpdPaK0Y417zTmDUYT a01Dk0lvjF0wRnJlg2BgMe8LLqtZ7FvzVeC5bVCM9DPrdizZecB13MzJKI1LQZLTSiuJs o0li1823LMTgNmyk4d61N4uKsoUaGK%2bmxITfHkSxaM3CIWRoVtgg1M65wxBQqptwah W5y2zp7m0A2wSVEy03Z8kvM7cSiM2rei0s7CsLLEK7P7zZqbRYTXsmcp0ZdejpuGLIsp px97n%2fk4%2fy%2b255rR0NA49c9cxMjjdRNUq98qa6ueOeZVcuy1377A%2fe%2b%2f9rHL7N2aCr64GMhp12aFtHyBqkvvtQ%2fSN24dGsSNGZB%2fy%2beX6AXb72I1IlgJofJ4cbHvweXpv9GF40%2fQH23jHf%2fwK%2b%2frF%2bVly%2b%2fULlIn9w9WNY%2fvYu5u0%2f%2fXcudA%3d%3d HTTP/1.1

Cookie: \_TTPData=eNrNWFuTqjow/iuW59HqDd7aS3V3TUBRUFaQFX2ZihAuKgkSEPHXT9DWbfc+u6dnaj8cnsLk4lvfumQ15CWjSddAhxTRZIBsNA6S3CQ7ha1EI4IpKp3CPaZdpvZa9pMk6nIctX0QvqZVACox8k9riMjWeb3J8jUvilCb1t5cHZOR8wH57oTDcdwG1KE4Cgkv3kdx7L+79VxD9eam/lRtftfihms/P3U2z9WnTpu3EXSR7Wwa5ZJMaYpKtBOIGTVm/PmJbz1V6ybf6tZr3Vp7/a4Tv5bTGHdd5KAYFka6SYzyUowogrHt10sq3JJ4gWLK517LVSYI8EfBNQYF6SsWgTSgXQxDRLuJ3Z0Bddyt/uc780ZH+d1FkWANkAS0pJFEQC6J0e/IMoUJnsTATQrKjzrtm84tcKkTiGwj1qMkDuc/27ok8pbkTPKklb4nNGnhH3C2XsYhJR74T6qfnr/e3Tuk183e84xkCC949KuWODPSBrbt/IpxNFqHyeE0rc5CEh5bdPCYIOTNLwhfuMdsMnzBew3LtkCKn/TRM13Y47sCe5R01PzWSen/ydKC4c0uZfb5Y+4N7j8e7ae3ASH+EksC+oswQmKGTvpY/yL8qyxTL9UUV1FiU+cX4oUf1DqZgF2SEZvJTBLN1tkJ+9vGgtE2Sm03QDFJYNEIfx6vb6XwHyqld+AEWY4YmMGCYn/dY39D5ue7/5/BL9F5U6A+yout6glrJI2aYI+T/xz3PjIs3QfFZ+9lvshDPbAcVjTeOWPKzSCNvoGyFJnGwu4T9Eb/Jr1J+3P0v/GWYRhSHAx/rOsVcaYZegS8j/DdBCNTPqzJiv6KYEoisKRx9f9slqWmWYBjvk+T++26mgUeZkUUv7fe07Esy35k9Qsf1pV4ju9wTMghgfdX+foVcorW9/YiQkwwW8n74PzQoEpg7xG2hfVhbyCrXJUvIJ/QyX6yqw38V7nEPfD5JswH2jGFT9SH1QuSgVwUFztTaW7Ir+W/vndQeHsxY4gp231D+jD+33ggfERTeIHnid7cuVD6PtxvosM9kusFHttz/5843WN0hbhwjYmb1qkyIaitDMfgMMO9sVbFyT6d2mzHe9R84e6xZePHWRhn76qIe4MFMbB5xsE6nDdirEdh5gyHJ/uUq67WbrbgcpK1/DpYL MKV2YjsYfU3XYpt+nIUoY7Sjup17encWwuk1045HaNTFLtSi0ecXPZ332Fwa6Z2LKRu53oulhut6G2/pIMTLenu/Ckwqjaa9uSbPORqcnX98odatB+ePkLEQVK5QtZapMtur1ZEh8i8jlF+9sp8pwcTeB2JxZnLbYulthkucdvRRHEBw9ksG8eTRoSErda8XTP52BjNi7g78LBp2MF4A+10AprFXDziR91Vvoeq+fNedwsM/XkuDb2GjOw87R6QEekZXymbUFdNeVcnfuZ21PgRXa+yeSLTBX0U38LdMHTFgJQTdEy8rW1PztDNDHooB/4dCXAjGIWx1k3monegs+SGP5Gc9FEHhDX6/k00yY7kS0MqU5oBNOqsg5TiZnrjoeB7OipXDQPjaIittxro5Ned0ZzdFxrEqLSRue832FHV2Du111+PFRLGgk4TD2dLeW52phG1nq00LqkNfTWWN66RzTOzu+HTsamPDKdkrRx3REqJAPPKST/0nzdn15zshZU+a4JyZCSzPgBwIqGkZp43cFXQGIDq30llfYHL9D7LQ7/dE/qPPot6u8/iVi10Rf

<<<

HTTP/1.1 302 Found

Location: https://treys-test/claims/Default.aspx

Set-Cookie: \_TTPData=; expires=Wed, 12-Jul-2006 07:32:28 GMT;

path=/claims



Set-Cookie: \_WebSsoAuth=eNrNV9uSosoS/RXDeTR6wLsY3R2nAEFQUBAVfdlRQnFRqVIuIn79LrR1unvOzOmzYx62T0WYKnPlyiSrfE5gt0+DJEFxGhJceawU8aX6V7fTQM32pv1U73bZp5bndJ64Taf+xPVYB0EPOe6mVa0oSziHbScpx0LtcGynSe2+1RvWmy332z0G731GyZ+qWYx7nvIRTEsg/TTGBWVGCUiXk5QrWhws+IFihP67qVap4YQfzScoz10+iXpmy8CkzDpYxihpJ86/RnQxv36d7YP731UX5+vKQoEu2FpSCo6SXnkkRj9iivFTPakB15aUn6P6d0xb15B5oYIO8hESRqHTun/EegT5DVI00PSZ5gy5zx5SukWxtndMEqYZ+Yj9NPzf/fOEMrrHs89haUL6HpJXyj9z0gWO+hNutJ8ky4KnZgkxEvfFaT6+q1A0IVpFj0zn73d/RoyC2ntPTKESfDFEA3DiTkoSt5JNzIrnRfnYCCIC5f02Jd7pA9+H3q8pfYmThognIb01esshSmK6HPlo/03bdm1l4I11AaEPenJoUfQP08xC7Jk3sLzLLNFjnp25NOO1Fxs7QXorgikTiCNHpZelr6xAlQBJPvVKeEwMN3Evv3FphP9eorcKMqH7TYMXXf27af3dI9Jb/R+d3VR4EmN/pclctpZ20yVL0+cW/J42PPCuPvbnTPtqIYLgHrkuHRL1L9+DI5QAd9gWT1c4wF3GfoFf6e9Sf0Z+v/4i2QKC4Xp9Z1hplTct01fzPMJVjkh3+LMmyfyrgcIjJcCx/bpa0DaMwTb9Ok/nldzULfUybKH4bV9ieZ5/z5tXpNqqsQzLMRTgJqH/rXrbhdxy9L0+CxATTL/kfXh5N6AqYO+TOEyD6Bcu60ydlV0+obPz5NRb+Fu1wrzj80U3H5jFCXxKAlI/ejKRh+LyZKRMTEw1+ulrF4XXZyuGOKEnb5S8W/9/PBA+oT05IPcpuadzpfr1d79Qh31PTgx9eub+E50eGt1c3LrGxS37XJsQ1FOHY3CcYXGs13G6z6YOPfHeI5+Zh7Z0/b4XhtW7AbEoL4iJrQs019G8FWPjE0XucHh2zoXm6b12Fy4necauw8UiWlmtg7NkkLbbLpVeMrLV4Q4m7cxVetM4thbpOVoyu1YuaDL4HusGhSzaD2FKFZCZLMUAsu6wPU7X22jBHK1mzjrzXXTW4GEqNm1pxm2M5BwYG7VptxL2NLnwh5odKbY6VSDb7eWWyDvyzyNU3LKy2ywnwhTEvkJ5Z/PK04sONkUR2a0ggPjog1zhga+M5JakNn1Q/gbnC9B5f3cMdgHM5SwPjLkERLDWTCeXjJW4MAxxkLfnUN4Xa4kPHGy25x3ckWApJzN9S1oapZSaNYg10QVXm2Xu0252jTeOA+2wOB9fcEDzRjss1jb+4s71FL9IvD4Jw4DCYAjvzVA7q92gr8agCwWongugNAfBkatmOb8dCeg1SXNQTJhpJpS4HRyYepDcLRqegbl3qlFNNyLC21sKWtuNEensSYtJj14KfY1enUNJyPNWY4XE9UeTlIG50tna7enEnbcoYGXaq0xDLRY2XhmNs8u3obNxpYxOp6QvXK9sXoYAVjUzsZx0Nm0PXJ2FnbW0Xn1REnmAwDgRABQy31f9jTQkkf97or5gGdyY0DrMOiJ/OB9zoLRG1Dd6iVWEI7yTNk0RUMtAl2AL1Ixf+OFXmgCEABOZ+vpFHeoHv5FQkZUTWsnBydJA7+bCsnc1Oeh41kPSHmbrpZ13zOpIz8bRDgYxevZsWTUfjtSs31TA0DRaa05HLHuBzTdD43vWdkhsrjYdA4pHK8Q3YMuoz0ZvVpFfc43dhBrnLxpPmV+wwNyfaIM9nR14hAyibcsC6Q9AZF9x2bavsy16wUGjvNljLVG2ucIR2Cpd6sWnqpzU2Sls6ZvU97TNpg9XTRs5PCzk40JFprOh+tKC2JsU11URTZEhliXl/IPGGQ/tmXm8tgQ+3; path=/claims; secure; HttpOnly

Set-Cookie: \_WebSsoAuth0=vPDongOyasChyToiOY0bV9+Ba5vkc5xVY1G4s1R35cD7RUxWGxg/NLoAIdgVEy95Owd7Kl848cpbNYrs1lu9g0zokt/4hr100CbXU316XChE5nmwbHjio9n/Uz98ioH1EW8ZOxw402vuh2rXn+lzamRyvw2nBHEFM9hrZerZq2q6cEUMIsBkuGGu1kC4zSV1wIicEU2y1NqW2vdjgGAoA7elxokThMu35ess3+Po0kLHKdfegc11/zyMa0bXGq3jZUgluTIN3R4rtQMDjMasIXrcjD0z5irf9bmsFfxqUbu5P5KRGEL0cCWhIkud2slqrbWLLZzCu7uCGYlBkiMg697aKmTouEuFLuJOSmWZ0E4+XLEj0y1BheMy1lyBAmp93izXp93LVH3Eg44JKzZaLs/S3ide7VWbNmH887GirreGnAGnZ2THI6rowip05XTPLTNQBQkXDOvgh2xgXrnYbbNXA29K0dZ+Zwujls6/4LHaqfJ+bNcpumzGPC/pi9j7vK/b/x69+bsI8T; path=/claims; secure; HttpOnly

```
>>> treyws-test (WS Resource)
GET /claims/Default.aspx HTTP/1.1
Cookie: _WebSsoAuth=eNrNV9uSosoS/RXDeTR6wLsY3R2nAEFQUBAVfdlRQnFRqVIuIn79LrR1unvOzOmzYx62T0WYKnPlyiSrfE5gt0+DJEFxGhJceawU8aX6V7fTQM32pv1U73bZp5bndJ64Taf+xPVYB0EPOe6mVa0oSziHbScpx0LtcGynSe2+1RvWmy332z0G731GyZ+qWYx7nvIRTEsg/TTGBWVGCUiXk5QrWhws+IFihP67qVap4YQfzScoz10+iXpmy8CkzDpYxihpJ86/RnQxv36d7YP731UX5+vKQoEu2FpSCo6SXnkkRj9iivFTPakB15aUn6P6d0xb15B5oYIO8hESRqHTun/EegT5DVI00PSZ5gy5zx5SukWxtndMEqYZ+Yj9NPzf/fOEMrrHs89haUL6HpJXyj9z0gWO+hNutJ8ky4KnZgkxEvfFaT6+q1A0IVpFj0zn73d/RoyC2ntPTKESfDFEA3DiTkoSt5JNzIrnRfnYCCIC5f02Jd7pA9+H3q8pfYmThognIb01esshSmK6HPlo/03bdm1l4I11AaEPenJoUfQP08xC7Jk3sLzLLNFjnp25NOO1Fxs7QXorgikTiCNHpZelr6xAlQBJPvVKeEwMN3Evv3FphP9eorcKMqH7TYMXXf27af3dI9Jb/R+d3VR4EmN/pclctpZ20yVL0+cW/J42PPCuPvbnTPtqIYLgHrkuHRL1L9+DI5QAd9gWT1c4wF3GfoFf6e9Sf0Z+v/4i2QKC4Xp9Z1hplTct01fzPMJVjkh3+LMmyfyrgcIjJcCx/bpa0DaMwTb9Ok/nldzULfUybKH4bV9ieZ5/z5tXpNqqsQzLMRTgJqH/rXrbhdxy9L0+CxATTL/kfXh5N6AqYO+TOEyD6Bcu60ydlV0+obPz5NRb+Fu1wrzj80U3H5jFCXxKAlI/ejKRh+LyZKRMTEw1+ulrF4XXZyuGOKEnb5S8W/9/PBA+oT05IPcpuadzpfr1d79Qh31PTgx9eub+E50eGt1c3LrGxS37XJsQ1FOHY3CcYXGs13G6z6YOPfHeI5+Zh7Z0/b4XhtW7AbEoL4iJrQs019G8FWPjE0XucHh2zoXm6b12Fy4necauw8UiWlmtg7NkkLbbLpVeMrLV4Q4m7cxVetM4thbpOVoyu1YuaDL4HusGhSzaD2FKFZCZLMUAsu6wPU7X22jBHK1mzjrzXXTW4GEqNm1pxm2M5BwYG7VptxL2NLnwh5odKbY6VSDb7eWWyDvyzyNU3LKy2ywnwhTEvkJ5Z/PK04sONkUR2a0ggPjog1zhga+M5JakNn1Q/gbnC9B5f3cMdgHM5SwPjLkERLDWTCeXjJW4MAxxkLfnUN4Xa4kPHGy25x3ckWApJzN9S1oapZSaNYg10QVXm2Xu0252jTeOA+2wOB9fcEDzRjss1jb+4s71FL9IvD4Jw4DCYAjvzVA7q92gr8agCwWongugNAfBkatmOb8dCeg1SXNQTJhpJpS4HRyYepDcLRqegbl3qlFNNyLC21sKWtuNEensSYtJj14KfY1enUNJyPNWY4XE9UeTlIG50tna7enEnbcoYGXaq0xDLRY2XhmNs8u3obNxpYxOp6QvXK9sXoYAVjUzsZx0Nm0PXJ2FnbW0Xn1REnmAwDgRABQy31f9jTQkkf97or5gGdyY0DrMOiJ/OB9zoLRG1Dd6iVWEI7yTNk0RUMtAl2AL1Ixf+OFXmgCEABOZ+vpFHeoHv5FQkZUTWsnBydJA7+bCsnc1Oeh41kPSHmbrpZ13zOpIz8bRDgYxevZsWTUfjtSs3
```

```
1TA0DRAaO5HLHuBzTdD43vWdkhsrjYdA4pHK8Q3YMuozOZvvLpFc43dhBrnLXpPmV+wwNy
faIM9nR14hAyibcsC6Q9AZF9x2bavsy16wUGjvN1jLVg2ucIR2Cpd6sWngpzU2S1s6ZvU9
7TNpg9XTRs5PCzk4OJFprOh+tKC2JsU11URTZEh1iXl/IPGGQ/tmxm8tgQ+3;_WebSsoA
uth0=vPDongOyasChyToiOY0bv9+Ba5vkc5xVY1G4s1R35cd7RUxWGxg/NLoAIdgGEVye9
5Owd7K1848cpbNYrsl1u9g0zokt/4hr100CbXU316XChE5nmwbHjiO9oN/Uz98ioH1EW8Z
Oxw402vuh2rXn+lzamRyv2nBHEFM9hrZerZq2q6cEUmIsBkuGGulkc4zSViwiCEU2y1N
qw2vdjqGAoA7e1xoKThMu35ess3+Po0kLHKdfeqGc11/zymA0bXGq3jUGluTIN3R4rtQMD
jMasIXrcjD0z5irf9bmsFxfqUbu5P5KGREL0cWhIkud2slqrbWLLZzc7uCGYlBkiMg697
aKmToEuFLuJOSmWZ0E4+XLEj0y1BheMyllYbAmp93izXp93LVH3Eg44JKxZaLs/S3ide7V
WbNmH887GirrEGnAGnZ2THI6roWip05XTPLTNQBBQkXDovgh2xgXrnYbbNXA29K0dZ+Zwu
jls6/4LHaqfJ+bNcpumzGPC/pi9j7vK/b/x69+bsI8T
```

<<<

HTTP/1.1 200 OK

[Application specific content]

## 4.2 SAML 1.1 Assertion Extension

Following is a **SAML assertion** fragment that illustrates the message syntax of the SAML 1.1 Assertion Extension elements in the advice element, as specified in section [2.2.3](#).

```
<saml:Advice xmlns:adfs="urn:microsoft:federation">
  <adfs:WindowsIdentifiers>
    AAAAAAEBAAAAABAAAAABRUAAAAVU+0xvWJxlC9CDm4GAAAA9AEAAAYCAAHAAGAACAIAA
    AECAAAAAGAA
  </adfs:WindowsIdentifiers>
  <adfs:CookieInfoHash>
    K6GNTL15/jljype53+PFRAiOfek=
  </adfs:CookieInfoHash>
  <adfs:WindowsUserIdentifier>
    S-1-5-21-837636885-2507236029-1846428367-500
  </adfs:WindowsUserIdentifier>
  <adfs:WindowsUserName>
    ADFSVM-A\Administrator
  </adfs:WindowsUserName>
</saml:Advice>
```

The raw octets of the [WindowsIdentifiers \(section 3.1.5.2.1.5\)](#) binary structure, after **base64** decoding are as follows.

```
00 00 00 00 01 00 00 00 01 04 00 00 00 00 05 15 00 00 00 15 53 ED
31 BD 62 71 95 CF 42 0E 6E 06 00 00 00 F4 01 00 00 06 02 00 00 07 02
00 00 08 02 00 00 01 02 00 00 00 02 00 00
```

The octet stream is structured as follows (see section [2.2.3.2](#)).

```
00 00 00 00  WindowsIdentifierFlags = 0
                TryLocalAccount = 0
                NoUserSid = 0
01 00 00 00  PackedSidsCount = 1 (0x00000001)
                PackedSids1
                    DomainSid
01                Revision = 1 (0x01)
                04                SubAuthorityCount = 4 (0x04)
                    00 00                IdentifierAuthority[0..1] = {0, 0, ...
00 00 00 05                IdentifierAuthority[2..5] = 0, 0, 0, 5
                    (0x05)}
15 00 00 00                SubAuthority1 = 21 (0x00000015)
15 53 ED 31                SubAuthority2 = 837636885 (0x31ED5315)
BD 62 71 95                SubAuthority3 = 2507236029 (0x957162BD)
```

```
CF 42 0E 6E      SubAuthority4 = 1846428367 (0x6E0E42CF)
06 00 00 00      RidCount = 6 (0x00000006)
F4 01 00 00      Rid1 = 500 (0x000001F4)
06 02 00 00      Rid2 = 518 (0x00000206)
07 02 00 00      Rid3 = 519 (0x00000207)
08 02 00 00      Rid4 = 520 (0x00000208)
01 02 00 00      Rid5 = 513 (0x00000201)
00 02 00 00      Rid6 = 512 (0x00000200)
```

The **SIDs** encoded in the structure are as follows:

- S-1-5-21-837636885-2507236029-1846428367-500
- S-1-5-21-837636885-2507236029-1846428367-518
- S-1-5-21-837636885-2507236029-1846428367-519
- S-1-5-21-837636885-2507236029-1846428367-520
- S-1-5-21-837636885-2507236029-1846428367-513
- S-1-5-21-837636885-2507236029-1846428367-512

## 5 Security

### 5.1 Security Considerations for Implementers

Security considerations for the Microsoft Web Browser Federated Sign-On Protocol Extensions are specified in the following subsections. Additionally, the security considerations outlined in [\[MS-MWBF\]](#) section 5 apply to the Microsoft Web Browser Federated Sign-On Protocol Extensions.

#### 5.1.1 Data Integrity

Data integrity concerns, as described in [\[MS-MWBF\]](#) section 5.1.1, apply to the extensions specified in this document. Of particular concern are the **SAML advice** elements specified by the SAML 1.1 Assertion Extension. These elements are included in the **SAML assertion**, which is signed to prevent tampering (see [\[MS-MWBF\]](#) section 2.2.4.2.2).

#### 5.1.2 Privacy

The privacy considerations in [\[MS-MWBF\]](#) section 5.1.5 apply to the extensions in this document. The extensions also introduce new privacy concerns.

The Query String Response Transfer Protocol is used to communicate **security tokens** from one party to another by using the query string of the HTTP request URL. The use of Secure Sockets Layer/Transport Layer Security (SSL/TLS) prevents the exposure of **user** information outside the services participating in the protocol (see [\[MS-MWBF\]](#) section 5.1.3); however, a GET message might provide a lesser degree of confidentiality than a POST message due to URL tracking concerns. For example, **web browser requestor** implementations might track URL history, or web proxy servers might log URLs.

The SAML 1.1 Assertion Extension provides a method for including **SIDs** in a **SAML assertion**. These SIDs might identify user identity, capabilities, or affiliations. For this reason, SIDs should not be included indiscriminately; rather, their distribution should be limited to specific **relying parties**.<24>

#### 5.1.3 Authorization Validation and Filtering

When processing **SIDs** from an **IP/STS**, **relying parties** must ensure that the IP/STS is authorized to issue SIDs that fall under a particular set of subauthorities. This is similar to namespace collision concerns with UPN and EmailAddress **claims** (as specified in [\[MS-MWBF\]](#) section 5.1.6).<25>

### 5.2 Index of Security Parameters

Because the Microsoft Web Browser Federated Sign-On Protocol Extensions is an authentication protocol, the security details are in the message processing rules section.

Security parameter	Section
WindowsUserIdentifier	<a href="#">2.2.3.1</a>
WindowsUserName	2.2.3.1
WindowsIdentifiers	2.2.3.1

## 6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

- Windows Server 2003 R2 operating system
- Windows Server 2008 operating system
- Windows Server 2008 R2 operating system
- Windows Server 2012 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

[<1> Section 1.5](#): The Windows implementation of the SAML 1.1 Assertion Extension is integrated with Windows **Active Directory**. All **SIDs** that are transmitted in the **SAML assertion** correspond to Active Directory **accounts**. In order to transmit SIDs between a **requestor IP/STS** and a **resource IP/STS** that reside in different **forests**, the requestor IP/STS forest must be a **trusted forest** of the resource IP/STS forest.

[<2> Section 1.5](#): Local configuration is used to modify several of the Windows behaviors described in this document. In all cases, the local configuration must exist before the protocol is initiated. Specific instances where local configuration is used are listed below.

By default, an **IP/STS** does not issue **security tokens** with SIDs (see section [3.1.5.2](#)). The issuance of SIDs (that is, including the WindowsUserIdentifier (section [3.1.5.2.1.3](#)), WindowsUserName (section [3.1.5.2.1.4](#)), and WindowsIdentifiers (section [3.1.5.2.1.5](#)) elements in issued SAML assertions) can be enabled for specific **relying parties** by using local configuration.

By default, when a **user** authenticates to a resource IP/STS by using a security token from a requestor IP/STS (see section [3.1.5.2](#)), any SIDs in the SAML assertion are ignored (that is, the WindowsUserIdentifier (section [3.1.5.2.1.3](#)), WindowsUserName (section [3.1.5.2.1.4](#)), and WindowsIdentifiers (section [3.1.5.2.1.5](#)) elements). Processing these SIDs (as described in section [3.1.5.2](#)) can be enabled for specified requestor IP/STSs using local configuration. In this case, the local configuration also specifies a Windows **domain** associated with the IP/STS, so that SID filtering can be performed (as specified in section [5.1.3](#)).

When a user authenticates to a resource IP/STS by using a security token from a requestor IP/STS (as specified in section [3.1.5.2](#)), **claims** can be mapped to SIDs based on local configuration. In this case, the local configuration also specifies the desired value of the **TryLocalAccount** flag (as specified in WindowsIdentifierFlags Structure (section [2.2.3.2.1](#))).

A special algorithm is used to determine when the Query String Response Protocol is used (as specified in section [3.2.5.1.1](#)). This algorithm uses local configuration to force the use of the protocol and for the **FileExtensionBypassList** flag.

[<3> Section 1.6](#): The Query String Response Transfer Protocol is supported only in Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.

<4> [Section 1.6](#): SAML1.1 Assertion Extension is supported only in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2.

<5> [Section 1.9](#): The following URIs are used as local assignments in fields specified by the SAML 1.1 Assertion Extension: "urn:federation:activedirectory" and "urn:microsoft:federation".

<6> [Section 2.2.3.1](#): Support for this field is conditional, as specified in [CookieInfoHash Element \(section 3.1.5.2.1.2\)](#).

<7> [Section 2.2.3.1](#): WindowsUserName Element (section 3.1.5.2.1.4) specifies how Windows constructs the WindowsUserName value.

<8> [Section 3.1.1.1.1](#): The **pending result** is maintained in secure session cookies written using Set-Cookie headers (as specified in [RFC2965](#)), which are added to the HTTP 302 response to the **web browser requestor**.

<9> [Section 3.1.1.1.2](#): The recommended value is used.

<10> [Section 3.1.2](#): There are no new timers. The pending result is stored by using secure session cookies (see section [3.1.1.1.1](#)).

<11> [Section 3.1.5.2.1.1](#): The IP/STS only includes this element when it is a resource IP/STS. The value identifies Active Directory, a **Lightweight Directory Access Protocol (LDAP)** service, or a **security realm**. If the user authenticated by using Active Directory, the [ClaimSource \(section 3.1.5.2.1.1\)](#) value is "urn:federation:activedirectory". If the user authenticated by using an LDAP service, the ClaimSource (section 3.1.5.2.1.1) value is a URI associated with the LDAP service, for example "LDAP://ldap.example.com". If the user authenticated by using a SAML assertion from a Requestor IP/STS, the ClaimSource (section 3.1.5.2.1.1) value is the value of the Security Assertion Markup Language (SAML) issuer. For more information about user authentication, see [MS-MWBF](#) section 3.1.5.4.3.

<12> [Section 3.1.5.2.1.2](#): The IP/STS includes the CookieInfoHash (section 3.1.5.2.1.2) element when an authentication cookie is issued at the same time as a SAML assertion. The authentication cookie is a **base64-encoded** binary structure. Windows includes the base64-encoded SHA-1 hash value (as described in [FIPS180](#)) of the raw octets.

<13> [Section 3.1.5.2.1.3](#): By default, the IP/STS does not include the WindowsUserIdentifier (section 3.1.5.2.1.3) element. It can be enabled for specific relying parties (see section [1.5](#)). A requestor IP/STS populates this field only if the user authenticated by using Active Directory. A resource IP/STS populates this field only if the user authenticated by using a security token from a requestor IP/STS, in which case the value, if present, is copied from that security token.

<14> [Section 3.1.5.2.1.4](#): By default, the IP/STS does not include the WindowsUserName (section 3.1.5.2.1.4) element. It can be enabled for specific relying parties (see section [1.5](#)). Windows constructs the user name by including the **NetBIOS** domain name (as it is always available in this context) and Active Directory account name, separated by a backslash (for example, "DOMAIN\user name"). A requestor IP/STS populates this field only if the user authenticated by using Active Directory. A resource IP/STS populates this field only if the user authenticated by using a security token from a requestor IP/STS, in which case the value, if present, is copied from that security token.

<15> [Section 3.1.5.2.1.5](#): By default, the IP/STS does not include the WindowsIdentifiers (section 3.1.5.2.1.5) element. It can be enabled for specific relying parties (see section [1.5](#)).

A requestor IP/STS populates this field only if the user authenticated by using Active Directory. In this case, a WindowsIdentifiers (section 3.1.5.2.1.5) binary structure is constructed that contains a subset of the security identifiers (SIDs) associated with the Active Directory account. The subset consists of the user SIDs, the **global group** SIDs, and the **universal group** SIDs. That structure is base64-encoded and included in this field.

A resource IP/STS populates this field only if the user authenticated by using a security token from a requestor IP/STS. If the SAML assertion issued by the requestor IP/STS contains a **WindowsIdentifiers** field, its value is copied to this field. Otherwise, the resource IP/STS maps claims from the SAML assertion of the requestor IP/STS to SIDs based on local configuration (see section 1.5). If any claims are mapped to SIDs, those SIDs are encoded in a WindowsIdentifiers (section 3.1.5.2.1.5) binary structure with the **NoUserSid** flag set to 1 and the **TryLocalAccount** flag set based on local configuration (see section 1.5). The structure is base64-encoded and included in the **WindowsIdentifiers** field.

<16> [Section 3.1.6](#): There are not any new timer events. The pending result is stored by using secure session cookies (see section 3.1.1.1.1).

<17> [Section 3.2.1.1.1](#): The **aggregated result** is maintained in secure session cookies written using Set-Cookie headers (as specified in [RFC2965]), which are added to the HTTP 302 response to the web browser requestor.

<18> [Section 3.2.2](#): There are no new timers. The aggregated result is stored using secure session cookies (see section [3.2.1.1.1](#)).

<19> [Section 3.2.5.1.1](#): A special algorithm (described later) determines whether to use the Query String Response Transfer Protocol or not.

The algorithm is presented in pseudocode.

Let KnownClients be a constant set composed of the following strings, which specify **user agent** string fragments that are known to identify user agents that do not support scripting:

- "Microsoft FrontPage"
- "Microsoft Office"
- "Test for Web Form Existence"
- "Microsoft Data Access Internet Publishing Provider"
- "Microsoft-WebDAV"

Let FileExtensionBypassList be a set of strings retrieved from local configuration (see section 1.5) that identify file name extensions.

The algorithm is as follows.

```
IF local configuration forces Query String Response Transfer
Protocol
OR User-Agent is empty
OR User-Agent is in KnownClients
OR NOT User-Agent contains "Mozilla"
OR NOT Http-Verb is in (GET,POST) THEN
    Use Query String Response Transfer Protocol
ELSE
    IF local machine state indicates Windows Sharepoint Services
    AND NOT Request-URL's file extension is in
FileExtensionBypassList THEN
        Use Query String Response Transfer Protocol
    ELSE
        Use the base protocol specified in [MS-MWBF]
    END IF
END IF
```

<20> [Section 3.2.5.2](#): By default, the resource IP/STS ignores these fields and processes the security token as though the extension elements are absent. Their processing can be enabled for specific requestor IP/STSs (as specified in section 1.5). Section [3.1.5.2.1](#) specifies how the resource IP/STS

includes the fields. The **web service resource** uses the fields to provide authorization services to a web-based application on the same machine by using methods that are outside the scope of this protocol.

<21> [Section 3.2.6](#): There are no new timer events. The aggregated result is stored by using secure session cookies (as specified in section 3.1.1.1.1).

<22> [Section 3.3.1](#): Windows Internet Explorer supports the use of session and persistent HTTP cookies (for more information, see [RFC2965]). The Windows implementation of this protocol requires that web browser requestor support at least session cookies. It uses persistent cookies to preserve security realm identifiers if they are supported by the web browser requestor.

<23> [Section 3.3.5](#): The RMS 2.0 client in Windows Vista operating system with Service Pack 1 (SP1), Windows Server 2008, Windows 7 operating system, Windows Server 2008 R2, Windows 8 operating system, and Windows Server 2012 adds a *whr* parameter to the wsignin 1.0 Request Message (section [2.2.2](#)) if the wsignin 1.0 Request Message does not already contain a *whr* parameter.

<24> [Section 5.1.2](#): The inclusion of SIDs can be enabled for specific relying parties (as specified in section 1.5).

<25> [Section 5.1.3](#): A relying party that accepts security identifiers from an IP/STS in another security realm performs SID filtering based on local configuration that associates the IP/STS with a Windows domain (as specified in section 1.5). For more information about SID filtering, see [\[MS-PAC\]](#) section 4.1.2.2.



## 7 Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements.
- A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

Section	Description	Revision class
<a href="#">1.4</a> Relationship to Other Protocols	Specified the section number in the [WSFederation1.2] reference.	Major
<a href="#">1.8</a> Vendor-Extensible Fields	Updated the section number in the [WSFederation1.2] reference.	Major
<a href="#">3.1.5.1.4</a> Responding to a wsignin1.0 Request That Specifies a ttpindex	Updated the section number in the [WSFederation1.2] references.	Major

## 8 Index

### A

Abstract data model  
[IP/STS](#) 18  
[relying party](#) 21  
[Aggregated result](#) 21  
[Applicability](#) 12  
[Assertion extension example](#) 42  
[Assertion Extension syntax](#) 15  
[Authorization validation security](#) 44

### C

[Capability negotiation](#) 12  
[Change tracking](#) 49  
[ClaimSource element](#) 20  
[CookieInfoHash element](#) 20

### D

[Data - security integrity](#) 44  
Data model - abstract  
[IP/STS](#) 18  
[relying party](#) 21  
[Directory service schema elements](#) 17

### E

[Elements - directory service schema](#) 17  
Examples  
[full network trace](#) 28  
[Query String Response Transfer Protocol](#) 25  
[Query String Response Transfer protocol example](#) 25  
[Security Assertion Markup Language \(SAML\) v1.1 assertion extension example](#) 42

### F

[Fields - vendor-extensible](#) 13  
[Filtering - security](#) 44

### G

[Glossary](#) 7

### H

Higher-layer triggered events  
[IP/STS](#) 19  
[relying party](#) 22

### I

[Implementer - security considerations](#) 44  
[Implementer security considerations](#) 44  
[Index of security parameters](#) 44  
[Index security parameters](#) 44  
[Informative references](#) 11  
Initialization  
[IP/STS](#) 19

[relying party](#) 22  
[Integrity - data](#) 44  
[Introduction](#) 7  
IP/STS  
[abstract data model](#) 18  
[higher-layer triggered events](#) 19  
[initialization](#) 19  
[local events](#) 21  
[message processing](#) 19  
[overview](#) 18  
[sequencing rules](#) 19  
[timer events](#) 21  
[timers](#) 19

### L

Local events  
[IP/STS](#) 21  
[relying party](#) 23

### M

[Maximum query string response message length](#) 18  
Message processing  
[IP/STS](#) 19  
[relying party](#) 22  
Messages  
[overview](#) 14  
Query String Response Transfer protocol ([section 2.1.1](#) 14, [section 2.2.2](#) 14)  
[SAML 1.1 Assertion Extension](#) 15  
[syntax](#) 14  
[transport](#) 14  
[XML namespace](#) 14  
[XML Namespace References](#) 14

### N

[Normative references](#) 10

### O

[Overview \(synopsis\)](#) 11

### P

[PACKED\\_SIDS packet](#) 16  
[Parameters - security](#) 44  
[Parameters - security index](#) 44  
[Pending result](#) 18  
[Preconditions](#) 12  
[Prerequisites](#) 12  
[Privacy - security considerations](#) 44  
[Processing - complete aggregated result](#) 23  
[Product behavior](#) 45  
Protocol Details  
[overview](#) 18

### Q

Query String Response Transfer Protocol ([section 1.3.1](#) 11, [section 3.1.1.1](#) 18, [section 3.1.5.1](#) 19, [section 3.2.1.1](#) 21, [section 3.2.5.1](#) 22)  
[syntax](#) 14  
[transport](#) 14  
[Query String Response Transfer protocol example](#) 25  
[Query String Response Transfer Protocol message](#) 14

## R

[References](#) 10  
[informative](#) 11  
[normative](#) 10  
[Relationship to other protocols](#) 12  
Relying Party  
[abstract data model](#) 21  
[higher-layer triggered events](#) 22  
[initialization](#) 22  
[local events](#) 23  
[message processing](#) 22  
[overview](#) 21  
[sequencing rules](#) 22  
[timer events](#) 23  
[timers](#) 21

## S

[SAML 1.1 Assertion Extension message](#) 15  
[SAML advice elements](#) 15  
[SAML v1.1](#) 12  
[assertion extension example](#) 42  
[Assertion Extension syntax](#) 15  
[Schema elements - directory service](#) 17  
Security  
[authorization validation and filtering](#) 44  
[data integrity](#) 44  
[implementer considerations](#) 44  
[parameter index](#) 44  
[privacy](#) 44  
[Security Assertion Markup Language \(SAML\) V1.1 - assertion extension](#) 23  
Security Assertion Markup Language (SAML) v1.1  
Assertion Extension ([section 1.3.2](#) 12, [section 3.1.5.2](#) 20)  
[syntax](#) 15  
[Security Assertion Markup Language \(SAML\) v1.1 assertion extension example](#) 42  
Sequencing rules  
[IP/STS](#) 19  
[relying party](#) 22  
[Standards assignments](#) 13  
Syntax  
[messages](#) 14  
[Query String Response Transfer protocol](#) 14  
[Security Assertion Markup Language \(SAML\) V1.1 Assertion Extension](#) 15

## T

Timer events  
[IP/STS](#) 21  
[relying party](#) 23  
Timers  
[IP/STS](#) 19  
[relying party](#) 21

[Tracking changes](#) 49  
[Transport](#) 14  
Triggered events - higher-layer  
[IP/STS](#) 19  
[relying party](#) 22

## V

[Vendor-extensible fields](#) 13  
[Versioning](#) 12

## W

[WindowsIdentifierFlags packet](#) 16  
[WindowsIdentifiers element](#) 21  
[WindowsIdentifiers packet](#) 15  
[WindowsUserIdentifier element](#) 21  
[WindowsUserName element](#) 21  
[wsignin1.0 message](#) 14  
[common parameters](#) 14  
[response](#) 14  
wsignin1.0 request  
receiving - ttpindex not specified ([section 3.1.5.1.1](#) 19, [section 3.2.5.1.2](#) 22)  
[receiving - ttpindex of 0 specified](#) 19  
[receiving - ttpindex other than 0 specified](#) 19  
[receiving - ttpindex specified](#) 22  
[responding - ttpindex specified](#) 20  
[wsignin1.0 request - sending](#) 22  
[wsignin1.0 request response](#) 20

## X

[XML namespace message](#) 14  
[XML Namespace References message](#) 14