[MS-N2HT-Diff]:

Negotiate and Nego2 HTTP Authentication Protocol

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.
- **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.
- **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.

Revision Summary

Date	Revision History	Revision Class	Comments
12/5/2008	0.1	Major	Initial Availability
1/16/2009	0.1.1	Editorial	Changed language and formatting in the technical content.
2/27/2009	0.1.2	Editorial	Changed language and formatting in the technical content.
4/10/2009	0.1.3	Editorial	Changed language and formatting in the technical content.
5/22/2009	0.1.4	Editorial	Changed language and formatting in the technical content.
7/2/2009	1.0	Major	Updated and revised the technical content.
8/14/2009	2.0	Major	Updated and revised the technical content.
9/25/2009	3.0	Major	Updated and revised the technical content.
11/6/2009	3.0.1	Editorial	Changed language and formatting in the technical content.
12/18/2009	3.0.2	Editorial	Changed language and formatting in the technical content.
1/29/2010	4.0	Major	Updated and revised the technical content.
3/12/2010	4.0.1	Editorial	Changed language and formatting in the technical content.
4/23/2010	5.0	Major	Updated and revised the technical content.
6/4/2010	6.0	Major	Updated and revised the technical content.
7/16/2010	6.0	None	No changes to the meaning, language, or formatting of 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	6.0	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	6.1	Minor	Clarified the meaning of the technical content.
9/23/2011	6.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	7.0	Major	Updated and revised the technical content.

Copyright © 2017 Microsoft Corporation

Date	Revision History	Revision Class	Comments
3/30/2012	7.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	7.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	7.0	None	No changes to the meaning, language, or formatting of the technical content.
1/31/2013	7.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	8.0	Major	Updated and revised the technical content.
11/14/2013	8.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	9.0	Major	Significantly changed the technical content.
10/16/2015	9.0	None	No changes to the meaning, language, or formatting of the technical content.
7/14/2016	9.0	None	No changes to the meaning, language, or formatting of the technical content.
6/1/2017	9.0	None	No changes to the meaning, language, or formatting of the technical content.
9/15/2017	10.0	Major	Significantly changed the technical content.

Copyright © 2017 Microsoft Corporation

Table of Contents

Copyright © 2017 Microsoft Corporation

Copyright © 2017 Microsoft Corporation

1 Introduction

Support for SPNEGO authentication is as specified in [RFC4559]. The tokens are transmitted using base64-encoding. This document will call out the differences in the Microsoft implementation from what is specified in [RFC4559], where applicable.

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:

Backus-Naur Form (BNF): A syntax used to describe context-free grammars, which is a prescribed way to describe languages ([RFC2616] section 2.1). See also "Augmented Backus-Naur Form (ABNF)".

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. We will assist you in finding the relevant information.

[MS-SPNG] Microsoft Corporation, "Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension".

[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

[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

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999, http://www.rfc-editor.org/rfc/rfc2617.txt

[RFC4559] Jaganathan, K., Zhu, L., and Brezak, J., "SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows", RFC 4559, June 2006, http://www.rfc-editor.org/rfc/rfc4559.txt

1.2.2 Informative References

None.

Copyright © 2017 Microsoft Corporation

1.3 Overview

The SPNEGO HTTP (as specified in [RFC4559]) authentication mechanism is used to authenticate a web client to a web server. Any security protocol negotiated under SPNEGO can work under this authentication scheme.

1.4 Relationship to Other Protocols

This document is a companion to the SPNEGO HTTP authentication document, as specified in [RFC4559]. It uses the augmented Backus-Naur Form (BNF), as described in [RFC4559], section 4, and relies on both the non-terminals defined in that document and other aspects of the specification HTTP/1.1, as specified in [RFC2617]. For more information, see [RFC2616].

1.5 Prerequisites/Preconditions

SPNEGO HTTP authentication assumes the following in addition to any assumptions specified in [MS-SPNG].

It is assumed that the web server is capable of authenticating users as specified by [MS-SPNG].

The web client has implemented specification [MS-SPNG] so that it can participate in user authentication to the web server.

1.6 Applicability Statement

SPNEGO HTTP authentication is used in environments where the client and server support specification [MS-SPNG].

1.7 Versioning and Capability Negotiation

Versioning and capability negotiation is handled by the HTTP protocols specified in [RFC2617] (for more information, see [RFC2616]). This protocol has no additional versioning or capability negotiation.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

Parameter	Value	Reference
HTTP auth-scheme	"Negotiate" "Nego2"	[RFC2617], section 1.2

Copyright © 2017 Microsoft Corporation

2 Messages

2.1 Transport

SPNEGO messages are carried in the HTTP authentication exchanges as auth-data (as specified in [RFC4559] sections 4.1 and 4.2) and auth-data2. This document extends RFC 4559 such that the initial challenge contains GSS-API data.

2.2 Message Syntax

The usage of SPNEGO authentication is indicated by the WWW-Authenticate Response Header (as specified in section 2.2.1) with HTTP auth-scheme (as specified in [RFC2617], section 1.2) "Negotiate" or "Nego2". The auth-params (as specified in [RFC2617], section 1.2) exchanged are base64-encoded messages.

2.2.1 The WWW-Authenticate Response Header

If the server receives a request for an access-protected object, and if an acceptable Authorization header has not been sent, the server responds with a "401 Unauthorized" status code (for more information, see [RFC2616], section 10.4.2) and a "WWW-Authenticate" header, per the framework specified in [RFC2616]. The initial WWW-Authenticate header does not carry any auth-data when the header is "WWW-Authenticate:negotiate"; it does carry data when the header is "WWW-Authenticate:Nego2". WWW-Authenticate response values MAY be spread across multiple WWW-Authenticate headers, as specified in [RFC2616] section 14.47.

The SPNEGO scheme operates as follows.

```
challenge = "Negotiate" "Nego2" auth-data
auth-data = 1#(gssapi-data)
```

2.2.2 The Persistent-Auth Response Header

If the server successfully authenticates the request, it MAY indicate whether the Authorization header will be required for the next request on the connection. This is part of performance optimization and does not guarantee that an Authorization header will or will not be required.

The Persistent-Auth header has the following grammar:

```
Persistent-Auth = "Persistent-Auth" ":" 1#(persistent-auth-token)
persistent-auth-token = token
```

The Persistent-Auth-token has two possible values: "true" and "false". The client behavior in response to this header is specified in section 3.2.5.

2.2.3 The WWW-Authorization Request Header

Upon receipt of the response containing a "WWW-Authenticate" header from the server, the client is expected to retry the HTTP request.

```
credentials= ("Negotiate" | "Nego2") auth-data2
auth-data2= 1encoded-GSSAPI-token
```


Copyright © 2017 Microsoft Corporation

This auth-data2 directive contains the base64-encoding of an SPNEGO token returned by GSS_Init_sec_context() with the input token as the token from the WWW-Authenticate header if present.

The "Nego2" authentication scheme is used when and only when the server's WWW-Authenticate header contains "Nego2"; otherwise the "Negotiate" authentication scheme is used.

Only "401" represents an authentication error. For the meaning of any return code other than a success HTTP 2xx code, refer to [RFC2616], section 10.2.

Copyright © 2017 Microsoft Corporation

3 Protocol Details

3.1 Common Details

3.1.1 Abstract Data Model

The abstract data model for common elements is specified in [RFC2616] and [RFC2617].

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

No local events, other than those specified in [RFC4559].

3.2 Client Details

3.2.1 Abstract Data Model

The client-side abstract data model has one abstract data element in addition to those specified in [RFC2616] and [RFC2617]:

persistent-auth-value: A flag for each connection indicating whether authentication will be persisted for a given connection. A value of 1 for this flag signifies that authentication to this server was persisted, and a value of 0 signifies that the authentication to this server was not persisted.

3.2.2 Timers

None

3.2.3 Initialization

The **persistent-auth-value** flag MUST (section 3.2.1) be initialized to 0.

Copyright © 2017 Microsoft Corporation

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

The Authorization header is only sent by the client. For more information, see [RFC2616] section 14.8.

The Persistent-Auth header is a hint from the HTTP server to the HTTP client. The Persistent-Auth header is only valid when sent with the final response from the server after authentication has completed, and in all other cases it MUST be ignored. After the client has completed authentication with the server it SHOULD process the Persistent-Auth header.

If the persistent-auth-token is set to "true", then the client SHOULD set persistent-auth-value to 1 for the current connection.

If the persistent-auth-token is set to "false", then the client SHOULD set persistent-auth-value to 0 for the current connection.

If the persistent-auth-token is set to any value other than "true" or "false", then the Persistent-Auth header MUST be ignored.

When the Persistent-Auth header is not present and the authentication has completed, then the client SHOULD set persistent-auth-value to 1 if the underlying authentication protocol is NTLM.

When the client sends a request on a connection, then the client SHOULD use the value of persistent-auth-value to determine when to authenticate.

When persistent-auth-value is 1, then authentication SHOULD NOT be performed.

When persistent-auth-value is 0, then authentication SHOULD be performed whenever permitted under the conditions specified by [RFC2617] and [RFC4559].

When the client receives a "401" status code in the response, it MUST set persistent-auth-value to 0.

All other messages are handled by the client as specified in [RFC2616].

3.2.6 Timer Events

None

3.2.7 Other Local Events

Here are no other local events beyond those specified in [RFC4559].

3.3 Server Details

3.3.1 Abstract Data Model

The server-side abstract data model has no abstract data elements beyond those specified in [RFC2616] and [RFC2617].

3.3.2 Timers

None.

Copyright © 2017 Microsoft Corporation

3.3.3 Initialization

None.

3.3.4 Higher-Layer Triggered Events

None.

3.3.5 Message Processing Events and Sequencing Rules

The WWW-Authenticate header is only sent from the server. For more information, see [RFC2616] sections 14.47.

Upon successful completion of authentication, the server SHOULD emit a Persistent-Auth header in the response. When the server is configured for connection-based authentication and the current connection is authenticated, then persistent-auth-token SHOULD be set to "true"; otherwise it SHOULD be set to "false".

All other messages are handled by the server as specified in [RFC2616].

3.3.6 Timer Events

None.

3.3.7 Other Local Events

Here are no other local events beyond those specified in [RFC4559].

Copyright © 2017 Microsoft Corporation

4 Protocol Examples

An HTTP 1.1 client requests a resource from a server by sending an HTTP GET request as shown in the example below:

```
GET /test.htm HTTP/1.1
User-Agent: WHttpTst Test Harness
Host: webctestlive.ntdev.corp.microsoft.com:543
```

In this message the client is issuing an HTTP GET request to the server for the resource "test.htm".

The resource requested by the client requires client authentication. The server sends an HTTP response indicating this to the client, as shown in the example below:

```
HTTP/1.1 401 Unauthorized
Server: CHATS
Content-Length: 0
WWW-Authenticate: Nego2 YIIBpAYGKwYBBQUCoIIBmDCCAZSgGjAYB ...
```

In this message the server sends an HTTP 401 response to tell the client that it has to authenticate in order to access the requested resource. The server sets the value of the WWW-Authenticate header to "Nego 2" to indicate to the client that this is the scheme that will be used to authenticate.

Subsequently, the HTTP 1.1 client requests a resource from a server by issuing an HTTP GET request. The client also provides authentication information to the server as shown in the example below:

```
GET /test.htm HTTP/1.1
User-Agent: WHttpTst Test Harness
Host: webctestlive.ntdev.corp.microsoft.com:543
Authorization: Nego2 YIIEawYGKwYBBQUCoIIEXzCCBFugDjAMBgorBg ...
```

In this message the client is issuing an HTTP GET request to the server for the resource "test.htm". The client also sets the Authorization header to "Nego 2" and provides the necessary authentication information to authenticate to the server using this scheme.

Copyright © 2017 Microsoft Corporation

5 Security

5.1 Security Considerations for Implementers

The Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions require the client to request mutual authentication services via the mutual authentication flag (as specified in [MS-SPNG] section 3.3.3).

5.2 Index of Security Parameters

None.

Copyright © 2017 Microsoft Corporation

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~~updates to those products.

Windows Releases

- Windows 7 operating system
- Windows Server 2008 R2 operating system
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system
- Windows 10 operating system
- Windows Server 2016 operating system
- Windows Server operating system

Exceptions, if any, are noted ~~below.~~in this section. If ~~a~~ an update version, service pack or ~~Quick Fix Engineering (QFE~~Knowledge Base (KB) number appears with ~~the~~a product ~~version,~~name, the behavior changed in that ~~service pack or QFE.~~update. The new behavior also applies to subsequent ~~service packs of the product~~updates 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.

Copyright © 2017 Microsoft Corporation

7 Change Tracking

~~No table of~~ This section identifies changes ~~is available. The~~ that were made to this document ~~is either new or has had no changes~~ since ~~its~~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.

Section	Description	Revision class
6 Appendix A: Product Behavior	Added Windows Server to the list of applicable products.	Major

Copyright © 2017 Microsoft Corporation

8 Index

Copyright © 2017 Microsoft Corporation

M

N

O

P

R

S

Copyright © 2017 Microsoft Corporation

T

V

Copyright © 2017 Microsoft Corporation