Draft D. Recordon
VeriSign
A. Glasser
VxV Solutions
P. Madsen
NTT
December 5, 2006

OpenID Assertion Quality Extension 1.0 - Draft 3

Abstract

This extention to the OpenID Authentication protocol provides means for a Relying Party to request additional information about the specifics by which a user enrolled and/or authenticated to the OpenID Provider, as well as for an OpenID Provider to add such information into assertions. Such information may be necessary for use cases in which, for an RP to make an assesment of the quality of an assertion from a OP, the OP's identity is not on its alone sufficient (as might be the case were an OP capable of authenticating a user through various authentication mechanisms).

While there are other aspects of lifecycle management that may bear on the resultant quality of an OpenID Authentication assertion - enrollment and authentication are generally the two characteristics that are most useful in distinguishing authentication quality. Consequently, we focus on these aspects here. We expect that other aspects (e.g. security characteristics, credential provisioning, etc) could be dealt with in the future.

As an extension, it requires no changes to either the Yadis protocol or the OpenID Authentication protocol and is viewed as an optional extension though its use is certainly recommended.

We acknowledge that, while none of the information expressed via this extension can be verified by the Relying Party in a technological fashion, this need not be viewed as an issue. The lack of an inherent trust model within OpenID allows for Relying Parties to decide which OPs they trust using whatever criteria they choose - likewise RPs will decide whether or not to trust claims as to authentication quality from such OPs as well.

Table of Contents

1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, B., “Key words for use in RFCs to Indicate Requirement Levels,” ?.).

2. Terminology

The following terms are defined in [OpenIDAuthentication2.0] (Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0 - Draft 10,” 2006.):

- Identifier
- Relying Party (RP)
- OpenID Provider (OP)

3. Extension Overview

1. End Users and OPs advertise both enrollment policy and supported authentication methods via Yadis.
2. Based on Yadis advertisements, the Relying Party includes parameters in the OpenID Authentication request describing its preferences for enrollment and authentication policy for any subsequent assertions.

3. The OpenID Provider responds to the Authentication request with an assertion - supplemented with information about the enrollment and authentication policies under which the assertion was issued. The RP will take this information as input into its assessment of the quality of the assertion.

4. Relation to SAML Authentication Context

The Security Assertion Markup Language (SAML) Authentication Context ([SAMLAC] (Kemp, J., “SAML 2.0 Authentication Context,” 2005.) defines mechanisms by which SAML Service Providers and OpenID Providers can discuss the context of an authentication assertion.

The authors acknowledge the similar motivation between SAML's Authentication Context and this extension. Where possible, we have attempted to stay aligned with the SAML Authentication Context model. Indeed, we see this topic as a likely area of convergence between OpenID and SAML. More work is needed here.

5. Advertising OP Policy

Via the use of [Yadis] (Miller, J., “Yadis Specification 1.0,” 2005.) within OpenID, Relying Parties are able to discover OpenID Provider service information in an automated fashion. This is used within OpenID Authentication for a RP to discover what version of the protocol each OP listed supports as well as any extensions, such as this one, that are supported. To aide in the process of a Relying Party selecting which OP they wish to interact with, it is advised that the following information be added to the End User's XRDS document.

It should be noted that implementors can add additional parameters to describe other attributes that can be verified during the enrollment process or properties of a specific authentication request. The following are meant as examples of what we feel are a reasonable baseline when looking at solving this problem.

The XML namespace SHALL be "http://openid.net/xmlns/aqe".

5.1. Supported Enrollment Properties

The following are properties describing the mechanisms used by the OP policy at the time of enrollment (account creation) and, as such, do not change with each authentication request. In other words, they describe what has already happened, and not a capability for something to happen.

For each property, the following values apply. The value of "yes" means that the End User has successfully passed verification. The value of "no" means that the user has not yet completed or has failed verification. The value of "na" means that the OP has not tried this method of verification. If a particular property is not declared, the property does not need to be declared and will be treated as the "na" or "no" value.

enroll.verified.liveness

Did the OP present the End User with a liveness during the account creation process?

Value: "captcha", "oob", "other" or "no"

Note: "captcha" means any automated CAPTCHA method. "oob" means that a form of out of band liveness verification (phone call, email, physical mail). "other" means another type of liveness challenge and "no" means no liveness testing was performed.

enroll.verified.email

Did the OP verify any email address the End User provided during the account creation process?

Value: "yes", "no" or "na"

enroll.verified.telephone

Did the OP verify any telephone number the End User provided during the account creation process?

Value: "yes" or "no"

5.2. Supported Authentication Properties

The following are properties describing authentication requests.

user.authentication.methods

What authentication methods is the OP capable of authenticating the End User through?

Value: Comma-delimited list of "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

If multiple methods are listed, no significance should be assigned to their order.

none - represents that no authentication operation is required for the OP to make a positive assertion about this Identifier.

password -

pin -

fingerbio -

handbio -

irisbio -

voicebio -

otherbio -

smartcard -

softotp -

OpenID actors are free to extend the above list as necessary. Care MUST be taken to ensure that any identifier for an authentication method will be recognized and interpreted appropriately.

6. Authentication Protocol

6.1. Request Parameters

During an OpenID Authentication 2.0 Request (Section 10), the following parameters can be included by the Relying Party to describe preferences for the particular authentication session.

- openid.ns.aqe

  Value: "http://openid.net/extensions/aqe/1.0"

- openid.aqe.max_auth_age

  If the End User has not actively authenticated to the OP within the number of seconds specified, the OP SHOULD authenticate the End User for this request.

  Value: Numeric value greater than or equal to zero in seconds.

  OP should realize that not adhering to the request for re-authentication means that the user will most likely not be allowed access to the RP.

- openid.aqe.multi_factor_order

  Optional: This will inform an OP that the order of methods used in authentication must follow the order specified by the RP. If not specified, it is treated as a preferred order.

  Value: "mandatory", "preferred"

Mandatory means that the RP must perform the authentications in the order prescribed in the openid.aqe.auth_factor1/2/3

- openid.aqe.auth_factor1

  Optional: The method of authentication the RP would like the OP to perform, or in the case of a multi-factor authentication, the first method that the RP would like the OP to perform. The mode should match one of the advertised values in the XRDS. If this is not specified, it is assumed that only a single factor is required and any authentication method is acceptable.

  Value: Comma-delimited list of "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

  Note: The OP should attempt to authenticate the user with the most secure mode requested. For example, if the OP has determined that their voicebio method is stronger than their password method and the RP requests either "voicebio or password", the OP should strive to authenticate the user by "voicebio" when possible. If the two modes are considered equally strong, then it is the choice of the OP regarding which one to authenticate against. OPs should note that authenticating a user by a non-designated method may result in an RP denying access.

- openid.aqe.auth_factor2

  Optional: In the case of a multi-factor authentication, the second method that the RP would like the OP to perform. The mode should match one of the advertised values in the XRDS. If this is not specified, it is assumed that the RP is requesting only a single factor for authentication. The OP will not use the same method for this factor as was used in any previous factors. For example, if the first factor is a password, the second factor cannot also be a password. For openid.aqe.auth_factor2 to be included, openid.aqe.auth_factor1 must have been previously defined.

  Value: Comma-delimited list of "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

  Note: The OP should attempt to authenticate the user with the most secure mode requested. For example, if the OP has determined that their voicebio method is stronger than their password method and the RP requests either "voicebio or password", the OP should strive to authenticate the user by "voicebio" when possible. If the two modes are considered equally strong, then it is the choice of the OP regarding which one to authenticate against. OPs should note that authenticating a user by a non-designated method may result in an RP denying access.

- openid.aqe.auth_factor3

  Optional: In the case of a multi-factor authentication, the third method that the RP would like the OP to perform. The mode should match one of the advertised values in the XRDS. If this is not specified, it is assumed that the RP is requesting only two factors for authentication. The OP will not use the same method for this factor as was used in any previous factors. For example, if the first factor is a password, the second factor cannot also be a password. For openid.aqe.auth_factor3 to be included, openid.aqe.auth_factor2 must have been previously defined.

Value: Comma-delimited list of "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

Note: The OP should attempt to authenticate the user with the most secure mode requested. For example, if the OP has determined that their voicebio method is stronger than their password method and the RP requests either "voicebio or password", the OP should strive to authenticate the user by "voicebio" when possible. If the two modes are considered equally strong, then it is the choice of the OP regarding which one to authenticate against. OPs should note that authenticating a user by a non-designated method may result in an RP denying access.

6.2. Response Parameters

In response to a Relying Party's request, the following parameters MUST be included in the OpenID Authentication 2.0 Response (Section 11). It is RECOMMENDED that an OP supporting this extension include the following parameters even if not requested by the Relying Party.

- openid.ns.aqe

  Value: "http://openid.net/extensions/aqe/1.0"

- openid.aqe.enrollment_liveness

  Was liveness verified by the OP during the End User's enrollment.

  Value: Comma-delimited list of "captcha", "oob", "other" or "no".

  Note: These values correspond with those in Section 5.1 (Supported Enrollment Properties).

- openid.aqe.enrollment_verified

  Attributes verified by the OP during the End User's enrollment.

  Value: Comma-delimited list of "email", "telephone".

  Note: These values correspond with those in Section 5.1 (Supported Enrollment Properties).

- openid.aqe.auth_factor1

  Description of the mechanism by which the End User authenticated to to the OP for this request.

  Value: "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

- openid.aqe.auth_factor2

  Only provided if the OP uses two or more factors for authentication.

  Value: "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

- openid.aqe.auth_factor3

  Only provided if the OP uses three for authentication.

  Value: "none", "password", "pin", "fingerbio", "handbio", "hardotp", "irisbio", "otherbio", "smartcard", "softotp", "voicebio"

- openid.aqe.auth_age

  The number of seconds prior to this request that the End User authenticated to the OP using the mode specified in "openid.aqe.auth_factor".

  Value: Numeric value greater than or equal to zero in seconds.

If the OP used more than one method to authenticate the End User for this request, it SHOULD be expressed to the RP in the response. To do so, the OP MUST post-fix both "openid.aqe.auth_mode" and "openid.aqe.auth_age" with a numeric value starting at 1 and incrementing by one for each authentication method used. Thus an OP using two authentication methods would include the following parameters in its response: "openid.aqe.auth_factor1", "openid.aqe.auth_age1", "openid.aqe.auth_factor2", openid.aqe.auth_age2".

7. Security Considerations

None known.

8. To-Do List

1. Use an existing schema when referring to attributes such as email, telephone, etc. This will also provide for the extension to be extensible by other parties.
2. Define the XML namespace to be used in the XRDS document.

3. Define the URI to represent this extension.

9. Examples

Non-normative

9.1. XRDS Document

The following examples show how information in Section 5 (Advertising OP Policy) can be expressed.

A 'weak' OP supporting only password based authentication that presented a captcha upon enrollment and verified the End User's email address.

```
<xrds:XRDS xmlns:openidaqe="http://openid.net/xmlns/aqe"
xmlns:openid="http://openid.net/xmlns/1.0" xmlns:xrds="xri://$xrds"
xmlns="xri://$xrd*($v*2.0)">
    <XRD>
        <Service>
            <Type>http://openid.net/signon/2.0</Type>
            <Type>http://openid.net/extensions/aqe/1.0</Type>
            <URI>http://weakidp.example.com/openid/server</URI>
            <openidaqe:enroll.verified.captcha>
                yes
            </openidaqe:enroll.verified.captcha>
            <openidaqe:enroll.verified.telephone>
                no
            </openidaqe:enroll.verified.telephone>
            <openidaqe:enroll.verified.email>
                yes
            </openidqe:enroll.verified.email>
            <openidaqe:user.authentication.methods>
                password
            </openidaqe:user.authentication.methods>
        </Service>
    </XRD>
</xrds:XRDS>
```

A 'strong' OP supporting both hardotp and voice print biometric based authentication that presented a captcha but and verified the End User's email address upon enrollment.

```
<xrds:XRDS xmlns:openidaqe="http://openid.net/xmlns/aqe"
xmlns:openid="http://openid.net/xmlns/1.0" xmlns:xrds="xri://$xrds"
xmlns="xri://$xrd*($v*2.0)">
    <XRD>
        <Service>
            <Type>http://openid.net/signon/2.0</Type>
            <Type>http://openid.net/extensions/aqe/1.0</Type>
            <URI>http://strongidp.example.com/openid/server</URI>
            <openidaqe:enroll.verified.captcha>
                yes
            </openidaqe:enroll.verified.captcha>
            <openidaqe:enroll.verified.telephone>
                no
            </openidaqe:enroll.verified.telephone>
            <openidaqe:enroll.verified.email>
                yes
            </openidqe:enroll.verified.email>
            <openidaqe:user.authentication.methods>
                hardotp,voicebio
            </openidaqe:user.authentication.methods>
        </Service>
    </XRD>
</xrds:XRDS>
```

A description of two seperate OPs, both the prior strong and weak examples. This would allow the RP to choose the applicable OP for the particular authentication request.

```
<xrds:XRDS xmlns:openidaqe="http://openid.net/xmlns/aqe"
xmlns:openid="http://openid.net/xmlns/1.0" xmlns:xrds="xri://$xrds"
xmlns="xri://$xrd*($v*2.0)">
    <XRD>
       <Service>
            <Type>http://openid.net/signon/2.0</Type>
            <Type>http://openid.net/extensions/aqe/1.0</Type>
            <URI>http://weakidp.example.com/openid/server</URI>
            <openidaqe:enroll.verified.captcha>
                yes
            </openidaqe:enroll.verified.captcha>
            <openidaqe:enroll.verified.telephone>
                no
            </openidaqe:enroll.verified.telephone>
            <openidaqe:enroll.verified.email>
                yes
            </openidqe:enroll.verified.email>
            <openidaqe:user.authentication.methods>
                password
            </openidaqe:user.authentication.methods>
        </Service>

        <Service>
            <Type>http://openid.net/signon/2.0</Type>
            <Type>http://openid.net/extensions/aqe/1.0</Type>
            <URI>http://strongidp.example.com/openid/server</URI>
            <openidaqe:enroll.verified.captcha>
                yes
            </openidaqe:enroll.verified.captcha>
            <openidaqe:enroll.verified.telephone>
                no
            </openidaqe:enroll.verified.telephone>
            <openidaqe:enroll.verified.email>
                yes
            </openidqe:enroll.verified.email>
            <openidaqe:user.authentication.methods>
                hardotp,voicebio
            </openidaqe:user.authentication.methods>
        </Service>
    </XRD>
</xrds:XRDS>
```

10. Normative References

[OpenIDAuthentication2.0] Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0 - Draft 10,” 2006 (TXT, HTML).

[RFC2119] Bradner, B., “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, ?.

[SAMLAC] Kemp, J., “SAML 2.0 Authentication Context,” 2005.

[Yadis] Miller, J., “Yadis Specification 1.0,” 2005 (PDF, ODT).

Authors' Addresses

David Recordon
VeriSign, Inc.
487 E Middlefield Road
Mountain View, CA 94043
USA
Email: drecordon@verisign.com

Avery Glasser
VxV Solutions, Inc.
329 Bryant Street
Suite #2D
San Francisco, CA 94107
USA
Email: aglasser@vxvsolutions.com

Paul Madsen
NTT
150 Insmill Crescent
Ottawa, ON K2T 1G2
Canada
Email: paulmadsen@ntt-at.com