Draft H. Granqvist
VeriSign, Inc.
September 2006

OpenID Authentication Security Profiles - Draft 1

Abstract

This memo defines security profiles for OpenID 2.0 authentication protocol. By agreeing on one or several such security profiles, an OpenID relying party and identity provider can decide the security properties for their mutual OpenID communication before such communication takes place.

Table of Contents

---

1. Introduction

The OpenID Authentication 2.0 (Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0,” .) [OPENID] protocol defines a way to prove ownership of an identifier. The typical use-case of this protocol is to log into one or several web sites without having to deal with multiple usernames and passswords.

In the protocol, claims of ownership to a specific identifier have several security dependencies, for example cryptographic primitives, trust in keying material, and reliance on underlying domain

system. This memo seeks to describe a framework for mechisms to describe such dependencies, as well as defining a few usable profiles.

This memo intentionally does not advise on usage of specific profiles, nor does it implicitly claim to cover all security dependencies of the protocol, nor does it decide how to process a party's willing or unwilling departure from a previously agreed-upon profile.

2. 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 RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

3. Definitions and Terminology

TODO.

4. Goals

This security profile specification has the following goals.

1. Define a framework for describing profiles that security mechanisms with in OpenID Authentication 2.0 (Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0,” .) [OPENID].
2. Define a number of security profiles using this framework.
3. Absence or presence of these profiles MUST have no effect on the referenced OpenID protocol. Compliance (and non-compliance) should only be governed by the protocol's parties and not the protocol itself.
4. The list of identified security variants must be extensible for future additions. This is necessary to handle security risks that were identified after this memo was written.
5. Any new security variants MUST be appended to the list of identified variants, and not override them. This is needed to keep previous defined profiles unchanged over time. A security variant that should no longer be used will be marked as such in the current version of this memo.

5. Non-goals

This security profile specification has the following non-goals.

1. Automatic negotiation of profile. This memo intentionally does not define a profile negotiation phase.
2. Automatic detection of profile violations. Some security properties are enforceable only via cooperation of the protocol parties.

6. Requirements

TODO.

7. Conventions

It is assumed an OpenID Authentication 2.0 (Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0,” .) [OPENID] party will advertise its intended profile compliance via the service discovery phase by using the service types defined in this memo.

8. Security variants

The following section describes the identified security variants in the OpenID Authentication 2.0 (Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0,” .) [OPENID] protocol.

This table defines the security variants and the expected values. References are tp the OpenID specification.

Number	Variant	Values
1.	Wildcards allowed in trust roots. This relates to whether the idp accepts wild carded trust roots as specified in section 8.2	One of Yes/No
2.	Allow unsecure associations? Whether the idp agrees to process authentication messages with no assoc_handle in section 8.	One of Yes/No
3.	Types of claimed identifiers accepted. Types of identifiers as enumerated in section 9.3.	Set of Http/Https/XRI
4.	Self-issued certificates allowed for authentication. This Applies to all https traffic. If 'no' here, then idp *probably* requires all https identifiers to chain up to known trust roots, but that's intentionally not implied.	One of Yes/No
5.	XRDS file must be signed. Signature on the XRDS as per XMLDSIG. Keying material not specified, since RP ultimately needs to make own decision whether to trust keys used for such signature.	One of Yes/No
6.	XRDS must be retrieved over secure channel. This does not imply SSL. See note on 4. about trust roots.	One of Yes/No
7.	Accepted association session types. What types of session types can be used as defined in section 7.4.3	Set of No-encryption/DH-SHA1/DH-SHA256

8.	RP must have XRDS. Should the relying party be required to advertise compliance with specific profiles as per section 11.	One of Yes/No
9.	Accepted association types. What section 7.3. association types the IDP agrees to use for signatures.	Set of HMAC-SHA1/HMAC-SHA256
10.	Association must be over secure channel. Whether the 7.4.1 request must take place on a secure channel.	One of Yes/No

Identified security variants.

Table 1

9. Profiles

The following section specifies two profiles "A" and "B" as examples. The identifier of these profiles are URLs that appends to http://openid.net/authn/2.0/.

This memo uses names like "A" and "B" tather than"low security" and "medium security" as such distinctions carry implications and liabilities. There is also a risk of security creep that forces definitions to change over time -- what is now 'medium security' could be 'low security' in a few years, and possibly 'useless security' in yet another few years. But the definition will be stuck as 'medium security' forever.

9.1. Profile A

The identifier for this profile is http://openid.net/authn/2.0/A

These are the profile settings as they relate to Section 9 (Profiles) .

Number	Values
1.	Yes
2.	Yes
3.	Http/Https/XRI
4.	Yes
5.	No
6.	No
7.	DH-SHA1/DH-SHA256
8.	No
9.	HMAC-SHA1/HMAC-SHA256

10.	No

Table 2

9.2. Profile B

The identifier for this profile is http://openid.net/authn/2.0/B

These are the profile settings as they relate to Section 9 (Profiles).

Number	Values
1.	Yes
2.	No
3.	Http/Https/XRI
4.	Yes
5.	No
6.	No
7.	No-encryption
8.	No
9.	HMAC-SHA1/HMAC-SHA256
10.	Yes

Table 3

10. Usage

Intention to following one or several profiles defined in this memo or in other location can be advertised.

Section 4.2. of the OpenID protocol defines the protocol discovery phase in which parties find out properties about each other. Adherence to one or several profiles should be advertised via this mechanism, including intendet expiry of such adherence.

11. Security considerations

TODO.

12. IANA considerations

This document has no actions for IANA.

13. Normative References

[OPENID] Recordon, D., Hoyt, J., Hardt, D., and B. Fitzpatrick, “OpenID Authentication 2.0.”

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, March 1997.

Author's Address

Hans Granqvist
VeriSign, Inc.
487 East Middlefield Rd.
Mountain View, CA 94043
US