

---

2 **OpenID Authentication Service**  
3 **V1.0**

4 **Working Draft 02, 7 September 2006**

5 **Document I-Name:**

6 xri://@xdi.org/(+specification)/(+authn)\*(+openid)\*(\$v\*1.0)\*(+draft)\*(\$v\*2)

7 **Document I-Number:**

8 *[To be assigned]*

9 **Location:**

10 <http://iss.xdi.org/>

11 **Editors:**

12 Drummond Reed, Cordance, <http://xri.net/=drummond.reed>

13 **Contributors:**

14 Victor Grey, 2idi, <http://xri.net/=victor.grey>  
15 Fen Labalme, 2idi, <http://xri.net/=fen.labalme>  
16 Owen Davis, LinkSafe, <http://xri.net/=ovdavis>  
17 Mike Mell, LinkSafe, <http://xri.net/=mmell>  
18 Les Chasen, NeuStar, <http://xri.net/=les.chasen>  
19 Andy Dale, ooTao, <http://xri.net/=andy.dale>  
20 Steve Churchill, ooTao, <http://xri.net/=steven.churchill>  
21

22 **Abstract:**

23 This document contains the normative specifications for XRI OpenID authentication  
24 service – a means for an XRI authority to authenticate control of an XRI using the  
25 OpenID authentication protocol V1.1 [\[OpenID-Authn\]](#).

26 **Status:**

27 This document is a Working Draft and may be subject to further revision at any time.  
28 Subsequent versions will be identified by a new version identifier and date (reflected in a  
29 new document i-name and i-number).

30 Comments should be posted to the appropriate page of the XDI.org I-Services  
31 Specifications (ISS) wiki at <http://iss.xdi.org>, or submitted to the ISS Comment mailing list  
32 at <http://lists.xdi.org/listinfo.cgi/iss-comment-xdi.org>.

33 This and all contributions to XDI.org are open, public, royalty-free specifications licensed  
34 under the XDI.org license available at <http://www.xdi.org/docref/legal/xdi-org-license.html>.

## Table of Contents

36	1	Introduction.....	3
37	1.1	Related Specifications .....	3
38	1.2	Terminology and Notation .....	3
39	1.2.1	Definitions.....	3
40	1.2.2	Keywords.....	3
41	1.2.3	ABNF Notation.....	3
42	1.2.4	Examples.....	3
43	1.2.5	Variables.....	4
44	1.2.6	XRIs and HXRIs.....	4
45	2	OpenID Authentication Service Endpoints.....	5
46	2.1	OpenID Authentication Service Endpoint Metadata .....	5
47	2.2	Use of the URI Append Attribute .....	5
48	2.3	Examples .....	6
49	3	OpenID Authentication Conformance Requirements .....	7
50	4	User Authentication .....	8
51	5	Server Authentication (Anti-Phishing Protection).....	9
52	5.1	Browser Plug-Ins.....	9
53	5.2	Personalized Login Pages .....	9
54	5.3	Manual Navigation and Pre-Login .....	9
55	6	Configuration.....	10
56	7	Activation and Confirmation.....	11
57	8	Security and Privacy Considerations .....	12
58	9	Future Work.....	13
59	9.1	OpenID Authentication 2.0.....	13
60	9.2	Strong Authentication.....	13
61	10	References .....	14
62	10.1	Normative .....	14
63	10.2	Informative .....	14
64	11	Links.....	15
65		Appendix A. Glossary .....	16
66			

---

## 67 **1 Introduction**

68 The purpose of this specification is to define the conformance requirements for XDI.org-  
69 Accredited I-Brokers and authorized resellers providing XRI authentication service using the  
70 OpenID Authentication 1.1 protocol [\[OpenID-Authn\]](#).

71 As discussed on the [\[OpenID\]](#) website, OpenID Authentication is a lightweight, decentralized,  
72 HTTP-based protocol for proving control of a identifier. OpenID 1.0 was intended for use with  
73 URLs. OpenID Authentication 1.1, when used in conjunction with the Yadis discover protocol  
74 [\[Yadis\]](#) and appropriate client libraries, can support both URLs and XRIs. OpenID Authentication  
75 2.0 (currently in progress) will support both URLs and XRIs natively.

76 For more information on OpenID, please see the [\[OpenID\]](#) website and Wikipedia entry at  
77 <http://en.wikipedia.org/wiki/Openid>.

### 78 **1.1 Related Specifications**

79 This specification has a dependency on the following specifications.

- 80 • *The OASIS XRI Specifications* specified by the OASIS XRI Technical Committee,  
81 including XRI Syntax 2.0 [\[XRISyntax\]](#), XRI Resolution 2.0 [\[XRIResolution\]](#), and XRI  
82 Metadata 2.0 [\[XRIMetadata\]](#). These specifications govern the technical interoperability of  
83 XRI identifiers and resolution protocols.

### 84 **1.2 Terminology and Notation**

#### 85 **1.2.1 Definitions**

86 All terms used in this specification as First Letter Uppercase or as an all-uppercase abbreviation  
87 are defined in Appendix A. This specification also includes by reference the XRI glossary as  
88 specified in Appendix C of [\[XRISyntax\]](#) and the XDI.org Global Services Specifications  
89 Definitions as specified in Appendix A of [\[XDI.orgGSS\]](#).

#### 90 **1.2.2 Keywords**

91 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD  
92 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as  
93 described in [\[RFC2119\]](#). When these words are not capitalized in this document, they are meant  
94 in their natural language sense.

#### 95 **1.2.3 ABNF Notation**

96 All ABNF (Augmented Backus-Naur Form) in the GSS uses the notation defined in [\[RFC2234\]](#).  
97 Note that a number of standard ABNF productions, including the HEXDIG production, are also  
98 defined in RFC 2234.

99 ABNF productions are in indented green text as shown below.

```
100 | example = this is an example production
```

#### 101 **1.2.4 Examples**

102 Example XRIs or XML documents in this specification are in indented grey text as shown below.

```
103 | xri://example.xri.authority/(+example.path)
```

## 104 **1.2.5 Variables**

105 All items that appear inside squiggly brackets "{}" are variables that do *not* include the squiggly  
106 brackets.

## 107 **1.2.6 XRIs and HXRIs**

108 | All XRIs used in this specification are shown in XRI-normal form as defined in [\[XRISyntax\]](#). All  
109 | such XRIs can be converted to the equivalent IRI-normal form or URI-normal form as defined in  
110 | [\[XRISyntax\]](#). In addition, all such XRIs may be expressed in an HTTP URI format (called an  
111 | *HXRI*) by prefixing the the URI-normal form of the XRI string (called the query XRI or *QXR*) with  
112 | the address of the XDI.org XRI proxy resolver `http://xri.net` or any other valid XRI proxy  
113 | resolver address. Note that QXRIs SHOULD NOT use the prefix `xri://`. Following are two  
114 | example HXRIs.

```
115 | http://xri.net/=example.person  
116 | http://xri.net/@example*xri*authority/(+example.path)
```

## 117 2 OpenID Authentication Service Endpoints

### 118 2.1 OpenID Authentication Service Endpoint Metadata

119 | [Table 1](#) defines the requirements for an OpenID Authentication Service Endpoint conforming to  
120 this specification. This information is also published on  
121 <http://iss.xdi.org/moin.cgi/ServiceEndpointDefinitions>, however [Table 1](#) is authoritative.

Element	Required/Optional	Element Value	Attribute Value
ProviderID	See note 1	I-Number of OpenID Authentication Service Provider	N/A
Type	Required	<a href="http://openid.net/signon/1.0">http://openid.net/signon/1.0</a>	<code>select="true"</code>
Media Type	See note 2	N/A	N/A
Path	See note 3	N/A	N/A
URI	Required – see sec 2.2	URI to OpenID Authentication service (see notes 4 and 5)	<code>append="none"</code>

122 Table 1: Requirements for a OpenID Authentication Service Endpoint conforming to this specification.

123 Notes:

- 124 1. XDI.org-Accredited I-Brokers and their authorized resellers are REQUIRED to have a  
125 ProviderID in the form of a valid global or community i-number as defined in section 4.3.1  
126 of [\[XDI.orgGSSI\]](#). This value SHOULD be used as the ProviderID for a OpenID  
127 Authentication Service Endpoint for which the XDI.org-Accredited I-Broker or authorized  
128 reseller is the OpenID Authentication Service Provider. (It is anticipated that in future  
129 versions of this specification, this ProviderID value will be REQUIRED for trust verification  
130 purposes.) Other trust networks may set their own requirements for this element.
- 131 2. The Media Type element is only required if another Media Type element is also specified  
132 for this endpoint; otherwise it is optional because the implied value of the match attribute  
133 if no Media Type element is present is `match="default"`.
- 134 3. The Path element is optional. If a Path is specified, the path (`+login`) is  
135 RECOMMENDED, and at least one Path element with the attribute value  
136 `match="null"` SHOULD be included so the OpenID Authentication Service Endpoint is  
137 selected even if no path is provided.
- 138 4. Use of at least one HTTPS URI is REQUIRED for compliance with this specification. See  
139 section 3.
- 140 5. For OpenID Authentication Service Providers, the RECOMMENDED third-level DNS  
141 hosting name for Authentication Service is `authn`, e.g. `authn.example.com`.

Deleted: default

### 142 2.2 Use of the URI Append Attribute

143 OpenID Authentication Service V1.1 does not use the URI `append` attribute because: a) most  
144 OpenID Authentication 1.1 client libraries use the raw value of the OpenID Authentication Service  
145 Endpoint URI element, and b) the OpenID Authentication V1.1 protocol passes the identifier  
146 being authenticated in the HTTP(S) authentication request.

147 Future versions of this specification and the OpenID Authentication specification MAY specify  
148 usage of the URI `append` attribute.

## 149 2.3 Examples

150 | [Figure 1](#) is an example of a OpenID Authentication Service Endpoint that offers a single HTTPS  
151 | URI.

```
152 | <Service>  
153 |   <Type select="true">http://openid.net/signon/1.0</Type>  
154 |   <URI append="none">https://authn.example.com/</URI>  
155 | </Service>
```

Deleted: qxri

156 Figure 1: Example OpenID Authentication Service Endpoint #1.

157 | [Figure 2](#) is an example of a OpenID Authentication Service Endpoint that offers both an HTTPS  
158 | and an HTTP URI. Each URI element includes a `priority` attribute.

```
159 | <Service>  
160 |   <Type select="true">http://openid.net/signon/1.0</Type>  
161 |   <URI append="none" priority="1">  
162 |     https://authn.example.com/  
163 |   </URI>  
164 |   <URI append="none" priority="2">  
165 |     http://authn.example.com/  
166 |   </URI>  
167 | </Service>
```

Deleted: qxri

Deleted: qxri

168 Figure 2: Example OpenID Authentication Service Endpoint #2.

169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192

### 3 OpenID Authentication Conformance Requirements

This specification defines an operational profile of [\[OpenID-Authn\]](#). To be conformant with this specification, an OpenID Authentication Service Provider:

1. MUST accept and process authentication requests as defined in [\[OpenID-Authn\]](#).
2. MUST support both “smart” and “dumb” mode as defined in section 3.4 of [\[OpenID-Authn\]](#).
3. MUST provision HTTPS URIs for OpenID Authentication Service Endpoints; MUST make them the highest priority URIs; and SHOULD perform OpenID authentication using HTTPS whenever possible. See section 5 of [\[OpenID-Authn\]](#).
4. MUST accept authentication requests on any valid form of an XRI or HXRI, i.e., [accept unnormalized XRIs \(which should then be normalized to lowercase as defined in \[XRISyntax\]\)](#) and [accept an xri://, http://xri.\\*, or https://xri.\\* prefix, if any \(which should then be removed\)](#).
5. MUST accept authentication requests on any valid CanonicalID synonym for the [original XRI](#).
6. SHOULD NOT support Iframes or popups when accepting a login request. See section 5 of [\[OpenID-Authn\]](#).
7. MUST require user authentication as specified in section 4.
8. SHOULD provide a mechanism for server authentication for anti-phishing protection as specified in section 5.
9. SHOULD provide a configuration interface as specified in section 6.
10. MUST provide a self-description interface for confirming activation as specified in section 7.

Deleted: the identifier  
Deleted: remove the

193

---

## 4 User Authentication

194 OpenID Authentication Service Providers MUST require a reasonably secure means of  
195 authentication for Subscribers. This SHOULD include a password or other credential meeting the  
196 OpenID Authentication Service Provider's own security policy as defined in section 2.4.1.2 of the  
197 XDI.org Global Services Specification V1.0 [GSS]. It MAY include other reasonably secure  
198 means of authentication offered by the OpenID Authentication Service Provider. Two-factor  
199 authentication or other means of strong authentication (see  
200 [http://en.wikipedia.org/wiki/Strong\\_authentication](http://en.wikipedia.org/wiki/Strong_authentication)) is RECOMMENDED.

---

201 **5 Server Authentication (Anti-Phishing**  
202 **Protection)**

203 Due to the extra sensitivity of OpenID Authentication credentials, OpenID Authentication Service  
204 Providers SHOULD offer Subscribers one or more means of server authentication. This enables a  
205 Subscriber to easily and/or automatically verify the identity of the Service Provider in order to  
206 prevent phishing of the Subscriber's password or other credentials.

207 All of the following mechanisms are RECOMMENDED for server authentication.

208 **5.1 Browser Plug-Ins**

209 After proper configuration, a browser plug-in can automatically notify a Subscriber when an  
210 OpenID Authentication Service Provider's login page has been authenticated using its SSL  
211 certificate. Absence of this notification is a highly visible phishing tipoff. See the list of available i-  
212 name security plugins at <http://www.inames.net>.

213 **5.2 Personalized Login Pages**

214 An OpenID Authentication Service Provider may enable Subscribers to specify a personalized  
215 text string or image that will be displayed on the login page when the Service Provider recognizes  
216 a persistent cookie stored on the Subscriber's browser. Although this provides a good server  
217 authentication cue, this mechanism is limited to machines and browsers pre-configured by the  
218 Subscriber.

219 **5.3 Manual Navigation and Pre-Login**

220 A third technique is for Subscribers to navigate directly to their OpenID Authentication Service  
221 Provider's login page (by manually typing the URI or activating a local bookmark) and logging in  
222 before attempting to login to any Relying Parties. This is particularly effective when the login  
223 session will remain active during most or all of a Subscriber's browser session, as the Subscriber  
224 will not need to enter their authentication credentials again. If the login session expires, the  
225 Subscriber can repeat the manual login process before navigating to the next Relying Party.

226

---

## 6 Configuration

227

The OpenID Authentication Service Provider SHOULD provide a configuration interface that enables a Subscriber to easily setup and manage OpenID Authentication Service.

228

229

If a Web configuration interface is offered, the OpenID Authentication Service Provider MUST allow the Subscriber to authenticate using one or more of the Subscriber's Authentication Service Endpoints, including their existing OpenID Authentication Service Endpoint or any other XDI.org ISS Authentication Service Endpoint.

230

231

232

233

The configuration interface SHOULD at a minimum enable a Subscriber to:

234

- Enter and update a password or other authentication credential (see section 4).

235

- Understand how to manually navigate and safely login at the OpenID Authentication Service Provider (see section 5.3).

236

237

The configuration interface MAY enable a Subscriber to:

238

- Configure secret questions/answers or other options for lost passwords.

239

- Control OpenID Relying Party options (see [\[OpenID-Authn\]](#)).

240

- Obtain and configure a browser plug-in for server authentication (see section 5.1).

241

- Personalize a login page for server authentication (see section 5.2).

242

- Control the logging associated with processing OpenID authentication requests.

243

- Control notifications associated with OpenID password changes or login activity.

244

The configuration interface MAY include additional features and functions not specified here.

245

---

## 7 Activation and Confirmation

246

Activation of a i-service may be independent of the provisioning of the service endpoint by an i-broker, so existence of a service endpoint in an XRDS document does not necessarily mean that the i-service is active. To enable other service providers and applications to confirm activation of an i-service, a OpenID Authentication Service Provider MUST support the following self-description interface.

247

248

249

250

251

To indicate that a specified i-service is active on a service endpoint URI, an HTTP GET request to the fully-constructed service endpoint URI (see section 8.4 of [XRIResolution](#)) with a Accept header value of `text/uri-list` MUST return:

252

253

254

1. An HTTP status of 200 OK (or a 3xx redirect that ultimately results in a 200 OK).

255

2. A valid, non-empty instance of a URI list [RFC2483](#) containing the URI identifying the service endpoint type as specified in [Table 1](#). (Note that the URI list MAY also contain additional URIs identifying other service types that are also active on this same endpoint.)

256

257

258

Any other response, including a 404 Not Found, a 406 Not Acceptable, an empty URI list, or a URI list that does not include the URI identifying the specified service type, indicates the specified service type is not active on the endpoint.

259

260

261

---

## **8 Security and Privacy Considerations**

262  
263

The primary subject of this specification is security, so there are no addition considerations beyond those already provided.

264  
265

In OpenID Authentication 1.1, a Subscriber shares their identifier directly with a Relying Party; this may be a privacy consideration for some Subscribers relative to some Relying Parties.

266  
267

OpenID Authentication 2.0 will enable Subscribers to login using the identifier of their OpenID Authentication Service Provider—see section 9.1.

---

268

## 9 Future Work

269

### 9.1 OpenID Authentication 2.0

270

OpenID Authentication 2.0 is currently under development at [\[OpenID\]](#). It adds several key features to OpenID authentication, including full support for XRIs and anonymous login (the ability to login using the XRI for a Subscriber's OpenID Authentication Service Provider rather than the Subscriber's own XRI). It is expected that this specification will be updated once OpenID Authentication 2.0 is released.

271

272

273

274

275

### 9.2 Strong Authentication

276

Distributed authentication protocols such as OpenID and SAML [\[ISS-Auth-SAML\]](#) allow many Relying Parties to leverage a service provider's investment in strong authentication (see [http://en.wikipedia.org/wiki/Strong\\_authentication](http://en.wikipedia.org/wiki/Strong_authentication)). It is anticipated that future versions of the OpenID Authentication specification and this specification will address how to request and acknowledge the use of strong authentication.

277

278

279

280

281

## 10 References

282

### 10.1 Normative

283

- 284 **[ISS-Auth-SAML]** P. Davis, *SAML Authentication Service V1.0*, XDI.org I-Services  
285 Specification, <http://iss.xdi.org>, Work-In-Progress.
- 286 **[ISS-Contact]** D. Reed, *Contact Service V1.0*, XDI.org I-Services Specification,  
287 <http://iss.xdi.org>, Work-In-Progress.
- 288 **[ISS-Forwarding]** D. Reed, *Forwarding Service V1.0*, XDI.org I-Services Specification,  
289 <http://iss.xdi.org>, Work-In-Progress.
- 290 **[GSS]** B. Lewis, D. Reed, L. Chasen, J. Neuman, S. Blackmer, XDI.org Global  
291 Services Specification V1.0, <http://gss.xdi.org>, June 2006.
- 292 **[OpenID-Authn]** D. Recordon, B. Fitzpatrick, *OpenID Authentication 1.1*,  
293 [http://openid.net/specs/openid-authentication-1\\_1.html](http://openid.net/specs/openid-authentication-1_1.html), May 2006.
- 294 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
295 <http://www.ietf.org/rfc/rfc2119.txt>, RFC 2119, March 1997.
- 296 **[RFC2234]** D. H. Crocker and P. Overell, *Augmented BNF for Syntax Specifications:*  
297 *ABNF*, <http://www.ietf.org/rfc/rfc2234.txt>, RFC 2234, November 1997.
- 298 **[RFC2483]** M. Mealling, R. Daniel Jr., *URI Resolution Services Necessary for URN*  
299 *Resolution*, <http://www.ietf.org/rfc/rfc2483.txt>, RFC 2483, January 1999.
- 300 **[XRIEPP]** NeuStar Registry Development Group, *EPP XRI Mapping*, <http://epp-ver-04.sourceforge.net/XRI/>, March 2006.
- 302 **[XRISyntax]** D. Reed, D. McAlpin, *Extensible Resource Identifier (XRI) Syntax V2.0*,  
303 OASIS Committee Specification, [http://www.oasis-](http://www.oasis-open.org/committees/download.php/15377)  
304 [open.org/committees/download.php/15377](http://www.oasis-open.org/committees/download.php/15377), November 2005.
- 305 **[XRIResolution]** G. Wachob et al, *Extensible Resource Identifier (XRI) Resolution V2.0*,  
306 (Work-in-Progress), [http://www.oasis-](http://www.oasis-open.org/committees/download.php/17293)  
307 [open.org/committees/download.php/17293](http://www.oasis-open.org/committees/download.php/17293), March 2006.
- 308 **[XRIMetadata]** D. Reed, *Extensible Resource Identifier (XRI) Metadata V2.0*,  
309 [<http://www.oasis-open.org/committees/xri>], March 2005.
- 310 **[Yadis]** J. Miller, *Yadis Specification V1.0*, <http://yadis.org/papers/yadis-v1.0.pdf>,  
311 March 2006.

312

### 10.2 Informative

- 313 **[XRIFAQ]** OASIS XRI Technical Committee, *XRI 2.0 FAQ*, [http://www.oasis-](http://www.oasis-open.org/committees/xri/faq.php)  
314 [open.org/committees/xri/faq.php](http://www.oasis-open.org/committees/xri/faq.php), November 2005.

---

315 **11 Links**

316	[XDI.org]	<a href="http://www.xdi.org">http://www.xdi.org</a>
317	[XDI.orgContact]	<a href="http://xri.net/@xdi.org/(+contact)">http://xri.net/@xdi.org/(+contact)</a>
318	[XDI.orgGSS]	<a href="http://gss.xdi.org">http://gss.xdi.org</a>
319	[XDI.orgISS]	<a href="http://iss.xdi.org">http://iss.xdi.org</a>
320	[OASISXRITC]	<a href="http://www.oasis-open.org/committees/xri">http://www.oasis-open.org/committees/xri</a>
321	[OASISXDITC]	<a href="http://www.oasis-open.org/committees/xdi">http://www.oasis-open.org/committees/xdi</a>
322	[OpenID]	<a href="http://www.openid.net">http://www.openid.net</a>
323		

324

## Appendix A. Glossary

325

In addition to the definitions provided below, the GSS also incorporates by reference the glossary definitions in the XRI Specifications (Appendix C of [\[XRISyntax\]](#) and the XDI.org Global Services Specifications (Appendix A of [\[XDI.orgGSS\]](#)).

326

327

328

OpenID Authentication Service	The XRI identity service (i-service) defined in this specification—see section 1.
OpenID Authentication Service Endpoint	An XRDS service endpoint containing the metadata defined in <a href="#">Table 1</a> of this specification.
OpenID Authentication Service Provider	Generally, the real-world provider of OpenID Authentication Service to a OpenID Authentication Service Subscriber. Legally, an authorized representative of the legal entity identified by the ProviderID for the OpenID Authentication Service Endpoint. Note that in <a href="#">[OpenID-Authn]</a> this is referred to as the <i>Identity Server</i> , <i>Identity Provider</i> , or <i>IdP</i> .
OpenID Authentication Service Subscriber	The authority for an XRI that subscribes to OpenID Authentication Service for that XRI.
OpenID XRI	The XRI presented for authentication to an OpenID Relying Party.
Relying Party	A website or application that makes OpenID authentication requests and consumes OpenID authentication responses as defined in <a href="#">[OpenID-Authn]</a> .
Subscriber	See OpenID Authentication Service Subscriber.

329