draft G. Monroe
JanRain
August 9, 2006

# OpenID DTP Version 1.0 Adjuncts - Draft 02

**Abstract**

OpenID DTP is a protocol for sending, receiving, and relaying an arbitrary signed and encrypted payload between two endpoints. DTP Version 1.0 Part 2: Adjuncts defines a set of adjuncts that may be used with DTP Version 1.0 Part 1: Envelopes. This specification depends on the messages described in Part 1.

---

**Table of Contents**

1. Additional Terminology
2. Discovery
3. Extension Algorithms
4. HTTP(S) Binding
   4.1. HTTP Request
   4.2. HTTP Response
5. Normative References
§ Author's Address

---

## 1. Additional Terminology

Reciever Endpoint URL:
: The HTTP URL that accepts incoming messages for a User.

---

## 2. Discovery

User public keys and Reciever Endpoint URLs are discovered using Yadis or XRI Resolution. If the Identifier is a URL, the Yadis protocol MUST be attempted on that URL. The Yadis protocol and XRI resolution both yield an XRDS document. This is a simple XML document with entries for services that are related to the Identifier. Each <xrd:Service> element in the XRD that provides messaging will contain the following information:

An <xrd:Type> element whose inner text is "http://www.example.com/2006/06/dtp#"
An <xrd:URI> tag whose text content is the Reciever Endpoint URL
A <PublicKey> element whose text content is the URL of the Public Key for that Reciever Endpoint URL.

Once the appropriate Service has been discovered, the Public Key for that Reciever Endpoint URL can be retrieved by performing an HTTP GET using URL contained in the <PublicKey> element.

Currently only one form of public key is defined. The HTTP response should be a PEM formatted RSA Public Key and have a Content-Type of "application/pem".

## 3. Extension Algorithms

If a Reciever Endpoint supports alternative cryptographic algorithms, they can be advertised in the <xrd:Service> element of the XRDS document containing the Reciever Endpoint URL by adding an additional <xrd:Type> element containing the algorithm identifier.

When a sender parses the XRDS document during discovery (Discovery), they can then look for advertised extension algorithms that they know about. It is up to the sender what algorithm is used. Advertising extenstion algorithms is purely advisory, and senders are in no way obligated to use them. It is an error to use an extension algorithm that is not advertised.

## 4. HTTP(S) Binding

This section describes a mechanism for sending and recieving messages using the Hypertext Transport Protocol 1.1 [HTTP] (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1,” .). If a Reciever Endpoint URL has an HTTPS scheme, it may be reasonable to use the NULL encryption type, depending on the application.

### 4.1. HTTP Request

A request to send a message to a Reciever Endpoint URL is an HTTP request with the Method set to POST. The body the request is the Outer Envelope XML document. The Content-Type header of the request should be set to "application/dtp+xml".

The Reciever Endpoint should verify the message according to the rules described in the Message Validation section of [DTP-1] (Monroe, G., “DTP Version 1.0 Part 1: Envelopes,” .) as well as any application-specific verification that is necessary before returning a response.

### 4.2. HTTP Response

The HTTP Response Entity will either be emtpy, denoted by a Content-Length Header of 0, or an Outer Envelope XML Document. If the response entity exists, it should be accompanied by a Content-Type header of "application/dtp+xml".

It is up to the application whether a response entity is appropriate. A response entity is only appropriate with an HTTP Status Code of 200.

HTTP Status Codes should be interpreted as follows:

200
: The message was delivered successfully; no further action is required of the client.

400
: Processing the message resulted in an error code. The HTTP Response Entity will contain the signed error message, including the error code and the digest of the bytes recieved.

500
: Indicates an internal error while the recieving server was processing the request. The Sender MAY retry delivery.

Any response with a Status Code not listed above is considered a permanent failure to deliver.

## 5. Normative References


[DTP-1] Monroe, G., “DTP Version 1.0 Part 1: Envelopes.”

[HTTP] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1.”


## Author's Address


Grant Monroe
JanRain, Inc.
5331 SW Macadam Avenue
Suite #375
Portland, OR 97239
USA
Email: grant@janrain.com