Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: October 26, 2015

V. Breitmoser

April 24, 2015

Linked Identities for OpenPGP
draft-vb-openpgp-linked-ids-01

Abstract

This document introduces a URI scheme for Linked Identitites to be used in URI Attributes in OpenPGP keys compatible to [RFC4880] and [URIATTR]. A Linked Identity then links the key to a resource on the internet in a mutual and verifiable way. The assumed authorization required to publish the resource forms a limited basis of trust for the key.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 26, 2015.

Copyright Notice

Table of Contents

1. Introduction

The OpenPGP specification [RFC4880] allows primary keys to associate themselves with identities in the form of User ID and User Attribute packets. User IDs consist of a readable string in UTF-8 format, which contains the name and email address of the key holder. However, the content of those identity types is only convention, leaving the user with only the raw content as a basis for trust decisions.

This document introduces a Linked Identity URI scheme to be used in URI Attributes as defined in URI Attributes for OpenPGP [URIATTR]. The purpose of such identity is to mutually connect the key to a resource on the internet, which has some type of established credibility, thereby providing an ad-hoc method of authentication.

1.1. Conventions Used in This Document

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]. Any

implementation that adheres to the format and methods specified in this document is called a compliant application. Compliant applications are a subset of the broader set of OpenPGP applications described in [RFC4880]. Any [RFC2119] keyword within this document applies to compliant applications only.

This specification uses the Augmented Backus-Naur Form (ABNF) notation of [RFC2234], including the following core ABNF syntax rules defined by that specification: ALPHA (letters), CR (carriage return), DIGIT (decimal digits), DQUOTE (double quote), HEXDIG (hexadecimal digits), LF (line feed), and SP (space).

2. Linked Identities

A Linked Identity is a type of identity in an OpenPGP key akin to User IDs and JPEG Attributes, and shares all fundamental properties of those identity types including self-certification lifecycle, foreign certifications and distribution mechanisms. Unlike those types though, a Linked Identity consists not only of the Linked Attribute distributed with the key (see Section 3), but is also linked to an external resource known as the Linked Resource. The only required property of a Linked Resource is that it must be uniquely identifiable by a URI, it is otherwise an abstract concept. As a more concretely specified type of Linked Identities, this document introduces the Cookie-Type Linked Identity (Section 4).

As part of a key, a Linked Identity constitutes a verifiable claim of control by the key owner over the Linked Resource. The verification of this link is intended to require little or no user interaction. Differently from User IDs, the meaning of a Linked Identity Attribute is not based on itself, but instead on the connection between the Linked Attribute and Linked Resource, providing evidence that the owner of the key also controls the referenced resource. This information can then be presented to the user as supporting information.

3. Linked Attibutes

A Linked Attribute is a URI Attribute as specified in URI Attributes for OpenPGP [URIATTR] where the scheme of the contained URI has a defined meaning in terms of a Linked Identity. The general semantics of a Linked Attribute are defined by the scheme of its URI, which should have a well-defined VERIFY operation.

The VERIFY operation on a Linked Identity URI verifies the link between the Linked Attribute (or its key) and its Linked Resource. The semantics of this operation are defined by its scheme but may, for the sake of flexibility, not have a generic mechanism even for a

defined scheme. Because of this, the URI format was chosen as a human readable representation to allow for a generic way of displaying unsupported Linked Identity types, and to aid developer dialogue.

3.1. Certification

Certifications on Linked Attributes are slightly more defined than on other packets: A compliant implementation MUST NOT issue a certificate over a Linked Attribute without a positive result from a VERIFY operation performed on its URI, but it MAY issue one based on the result of a VERIFY operation exclusively. Conversely, an implementation SHOULD NOT assume that certificates make any statement about the genuineness of the Linked Resource or the key itself other than the success of the VERIFY operation on the certified User Attribute from the perspective of the issuer.

This definition has implications on trust models based on Linked Identities, see Section 5.

4. The openpgpid+cookie Linked Identity Scheme

The openpgpid+cookie scheme in a Linked Attribute describes a claim of control over a Linked Resource which is synchronously accessible for its target audience. To this end, it requires the creator to place a Linked Resource Cookie at the site referenced by a wrapped URI, which may then be accessed and verified independently from the key owner at any point in time after its creation. This synchronous accessibility is the only requirement to make a resource suitable for use as a Linked Resource of this type. Exemplary use cases are connecting a key to its owner's website, profiles on social media, or owned domain names.

4.1. Scheme Definition

The openpgpid+cookie scheme is defined as follows:

```
linked-uri = scheme ":" [options] "@" <absolute-URI>
scheme = "pgpid+cookie"
options = ( option / flag ) [";" options]
option = key "=" value
flag = key
key = *(<unreserved>)
value = *(<unreserved> / <pct-encoded> / ",")
```

Where the grammar for <absolute-URI>, <unreserved> and <pct-encoded> are defined as in [RFC3986]. The scheme includes a wrapped, absolute URI plus any number of flags and/or pairs of key-value options.

Resulting from the definition of the URI Attribute, the encoding of the URI is fixed to UTF-8 (see [URIATTR]). While the flag and option part of the URI use a restricted character set from which no encoding issues should arise, considerations of the wrapped URI must be taken into account. It is generally the job of the issuer of a Linked Attribute to make sure the encoding is compatible, others who process it may safely treat encoding errors in a fail-fast manner.

Examples of openpgpid+cookie URIs:

```
openpgpid+cookie:@https://social.example.net/account/message
openpgpid+cookie:@dns:example.org?TYPE=TXT
openpgpid+cookie:@dns:example.org?TYPE=OPENPGPKEY
openpgpid+cookie:generic@https://example.com/pgpkey.txt
```

4.2. Scheme Semantics

The usual semantics and operations of the wrapped URI explicitly do not apply. Instead, the scheme defines the VERIFY operation (see Section 3), which if successful yields a result on the validity of the Linked Identity. This operation is defined in the context of its key, and parametrized by the flags and options. If any flag or option is unknown to an implementation, the entire Linked Identity URI MUST be treated as not supported. For details on the VERIFY operation, see Section 4.4.

The definition of semantics for specific wrapped URIs is out of scope for this document.

4.3. Linked Resource Cookies

To create a Linked Identity of the openpgpid+cookie scheme, the owner of a key publishes a Linked Identity Cookie at the desired site. The usual format for this cookie is a simple string in plain text format, although others are possible (see Section 4.3.1). The text format begins with an opening bracket, followed by the string "Verifying my OpenPGP key ", followed by a URI and a closing bracket. The contained URI refers back to the key.

```
cookie = "[" "Verifying my OpenPGP key " cookieuri  "]"
cookieuri = "openpgp4fpr" ":" fingerprint
fingerprint = 40<HEXDIG>
```

The cookieuri follows the openpgp4fpr scheme, which unambiguously identifies an OpenPGP key by its fingerprint. Example of a Linked Identity Cookie:

```
 [Verifying my OpenPGP key
openpgp4fpr:d4ab192964f76a7f8f8a9b357bd18320deadfa11]
```

Because publishing a cookie may not be perceived as a security-critical operation, the cookie format is chosen to imply its meaning, reducing the risk of social engineering attacks. It stands to reason that a user could more easily be manipulated into publishing a bare openpgp4fpr URI than a cookie with the text snippet included.

4.3.1. Alternative Cookie Formats

If for some reason a cookie cannot be placed at a site in this format - for example due to a restricted available character set - it may be encoded in a simple encoding scheme. There are no restrictions on this encoding, but it is RECOMMENDED to retain human readability, for example by trivially (but unambiguously) translating restricted characters. It is NOT RECOMMENDED to insert more whitespace or newlines.

For resource sites which are not human readable by nature, an implementation MAY accept Linked Resource Cookies which consist of the encoded fingerprint only. Because of the aforementioned risk of social engineering attacks, this should only be done with careful consideration.

4.4. Verification

To perform the VERIFY operation on a typical openpgpid+cookie URI, the resource is requested as referred to by the wrapped URI. From this reply, the cookie is extracted and possibly decoded, and then matched against the cookie expected for the Linked Identity packet. The particular mechanisms for requesting and extracting the cookie may be specific to the entire Linked Identity URI, including flags and options. For the Linked Identity to be considered valid, the extracted cookie text must match the expected value. An implementation MAY allow some flexibility in the cookie matching routine, but such decisions should be made with care. See Section 5.2.

An implementation SHOULD NOT perform verification based on a generic mechanism, unless specifically instructed to do so. While it is possible to retrieve the contents of a wrapped URI with a https scheme in a generic way, a proper VERIFY operation might require additional insight. For example, profiles on social media websites may include comment sections or other parts which are not entirely user-controlled, and thus require extraction of the specific, owner-controlled part. The use case of a website retrieved in a generic way is a special case of Linked Resource and should be indicated with a flag.

For certification, see the general notes on certification of Linked Identities in Section 3.1.

5. Security Considerations

The specification of Linked Identities in this document includes implications on a trust model which is based on Linked Attributes. This is unlike the general practice of [RFC4880], which strictly sticks to a technical description of the data exchange format.

5.1. Trust Model Implications

Linked Identities diverge from established certification practices, since the assumptions which can be drawn from foreign certifications issued for Linked Identities have a defined upper bound; Specifically, an implementation MUST NOT assume a certification to have any more meaning than the success of the VERIFY operation from the issuer's perspective (see Section 3.1). This affects a possible trust model in two ways: Firstly, the certificates issued by foreign keys should only be regarded as evidence for the validity of the Linked Identity, not of the genuineness of the Linked Resource or the key owner. Secondly, it allows automated services to issue certifications for Linked Identities which are verifiable from their perspective.

As a means of authentication, Linked Identities are a vector for Man-in-the-Middle attacks. The difference between the verification of a Linked Identity and the authentication of the owner of a key in particular may be non-obvious to users. While a certificate may be issued and published based on the VERIFY operation alone, the decision of whether the key as a whole is trustworthy must at some point take into account the genuineness of the Linked Resource. An implementation should take care to provide the user with sufficient guidance on this matter.

5.2. Linked Resource Verification

The security properties of a Linked Identity depend on the reliability of the URI-specific mechanism for verification. For this reason, it is very important that this mechanism is robust against false positives. An implementation should be very conservative about what is accepted as a valid Linked Resource. This especially includes acceptance of any sort of alternative cookie format (see Section 4.3.1).

In the case of Linked URIs with a https scheme, scraping the content of the linked site during verification should be avoided if possible. For example, if the service used in the URI provides an API, and the

URI contains information like a message id which can be parsed and used to access the content directly via the API, this method should be preferred.

6. IANA Considerations

The IANA is asked to register the openpgp+cookie URI scheme as a provisional scheme according with [RFC2717]. See the registration template in Appendix A.

7. Acknowledgements

This document was created with substantial feedback from Dominik Schuermann and Daniel Kahn Gillmor. The general concept of Linked Identities for OpenPGP (albeit in a centralized and out-of-band fashion) was first deployed by the founders and contributors of [keybase], whose work this document is heavily inspired by.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC2717] Petke, R. and I. King, "Registration Procedures for URL Scheme Names", BCP 35, RFC 2717, November 1999.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[URIATTR] Breitmoser, V., "URI Attributes for OpenPGP", 2015, <http://www.ietf.org/id/draft-vb-openpgp-uri-attribute-00.txt>.

8.2. Informative References

[keybase] Krohn, and Coyne, "Keybase", <https://keybase.io>.

Appendix A. Registration Template

URI scheme name: openpgpid+cookie

URI scheme syntax: See Section 4.1

URI scheme semantics: See Section 4.2

Intended usage: See Section 4

Encoding considerations: See Section 4.1

Applications/protocols that use this URI scheme name: The openpgpid+cookie scheme appears in URI Packets of OpenPGP compliant keys.

Interoperability considerations: None.

Security considerations: Section 5

Contact: V. Breitmoser, see below

Author/Change controller: IESG

Author's Address

Vincent Breitmoser
Braunschweig
DE

Email: v.breitmoser@my.amazin.horse