XEP-0383: Burner JIDs

Sam Whited
mailto:sam@samwhited.com
xmpp:sam@samwhited.com
https://blog.samwhited.com/

2017-01-28
Version 0.1.1

Status	Type	Short Name
Deferred	Standards Track	burner

A mechanism by which users may request anonymous, ephemeral ”burner” JIDs.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

In many XMPP applications it is desirable to be able to act anonymously to prevent leaking personally identifiable information (PII) to a third party. Traditionally this is accomplished using SASL authentication and the ANONYMOUS mechanism as detailed in Best Practices for Use of SASL ANONYMOUS (XEP-0175) [1], however, the ANONYMOUS mechanism is in reality an authorization mechanism and does not provide authentication of users.
This specification solves these problems by decoupling anonymous identity management from authentication (auth) and authorization (authz). This allows logged in users (authenticated or anonymous at the server operators disgression) to request a new temporary identifier, a ”burner” JID, which may be used by its owner to construct a new session with the server that is authorized to communicate anonymously with third parties and is (optionally) locally authenticated.

2 Glossary

Burner JID A temporary JID that is not valid for the purpose of authentication but which may be authorized by an existing pre-authenticated session.

Ephemeral identity The identity of a user on the server comprising a burner JID and any other associated data.

Authentication identity The users normal identity and JID which they use to authenticate with the server and create new XMPP sessions.

3 Use Cases

- As a user concerned about spam I want to join a public chat room anonymously to prevent JID harvesting.
- As the author of a social website I want to allow users to create ephemeral identities which can be used to contact them even if they have not granted access to their personal information.
- As a server operator I want to allow users to act anonymously, but also want a way to rate limit the creation of ephemeral identities associated with a given authentication identity.

4 Business Rules

The user requests an ephemeral identity from the server or another XMPP service by sending an IQ containing an ”identity” payload qualified by the urn:xmpp:burner:0 namespace.

[1] XEP-0175: Best Practices for Use of SASL ANONYMOUS <https://xmpp.org/extensions/xep-0175.html>.

Listing 1: User requests ephemeral identity

```
<iq from='caiusmarcius@example.net/corioli'
    id='h7ns81g'
    to='example.net'
    type='get'>
  <identity xmlns='urn:xmpp:burner:0'/>
</iq>
```

If the service wishes to issue an ephemeral identity to the user it replies with a new burner JID:

Listing 2: Server issues burner JID

```
<iq from='example.net'
    id='h7ns81g'
    to='caiusmarcius@example.net/corioli'
    type='result'>
  <identity xmlns='urn:xmpp:burner:0'>
    <jid>
      hfgnINTSA-ciCLz6NhTtCD5Jr0k:1477672278884j@example.net
    </jid>
  </identity>
</iq>
```

The burner JID MUST be a bare JID. Burner JIDs are not valid for the purpose of authentication, but may be authorized to perform actions. To use the burner JID the client then attempts to establish a new session with the server using the account that requested the burner JID as the authentication identity and the burner JID as the authorization identity as defined in RFC 4422 [2] §2. If the server does not support SASL, or does not support any SASL mechanisms that support authorization identities, burner JIDs cannot be used.

5 Determining Support

Services that support issuing burner JIDs MUST advertise the fact in responses to Service Discovery (XEP-0030) [3] "disco#info" requests by returning an identity of "authz/ephemeral":

Listing 3: Service responds to disco#info query

```
<iq type='result'
    from='muc.example.net'
    to='caiusmarcius@example.net/corioli'
```

[2] RFC 4422: Simple Authentication and Security Layer (SASL) <http://tools.ietf.org/html/rfc4422>.
[3] XEP-0030: Service Discovery <https://xmpp.org/extensions/xep-0030.html>.

```
    id='k3hs5174'>
  <query xmlns='http://jabber.org/protocol/disco#info'>
    <identity type='im' name='MyServer' category='server'/>
    <identity type='pep' name='MyServer' category='pubsub'/>
    <identity type='ephemeral' category='authz'/>…

    <feature var='http://jabber.org/protocol/disco#info'/>
    <feature var='http://jabber.org/protocol/disco#items'/>
    <feature var='http://jabber.org/protocol/muc'/>…
```

6 Implementation Notes

It may be impractical to store verification information for every burner JID issued by the system. To this end servers that implement this specification MAY choose to encode information into the localpart of issued burner JIDs which can be verified when a user attempts to authorize a new session to use the burner JID. If an implementation chooses to do this it is RECOMMENDED that an HMAC [4] be used. This HMAC MAY include the JID of the associated authentication identity, an expiration or issued time for the burner JID, session information, TLS channel binding data, or any other information the server wishes to verify. The format of this key or its input values is left as an implementation decision.
As with persistent JIDs, the client MUST NOT assign any meaning to the localpart or resourcepart of a burner JID.

7 Security Considerations

To prevent burner JIDs from being abused for spamming, implementations MAY rate limit all burner JIDs in use by an authn identity as a single unit. However, be advised that this may provide a third party that can monitor traffic patterns with the ability to determine what burner JIDs belong to the same user. To prevent a burner JIDs authn identity from being discovered the same way, burner JIDs SHOULD NOT share a rate limit with their authn identity.
If TLS channel binding information is encoded in the local part of the burner JID it is RECOMMENDED that the tls-unique channel binding value be used as defined by RFC 5929 [5] §3. Note that unless the master-secret fix from RFC 7627 [6] has been implemented channel binding information does not include enough context to successfully verify the binding when resuming a TLS session.
Implementations that choose to encode information in the localpart of burner JIDs should take

[4] The Keyed-Hash Message Authentication Code (HMAC): Federal Information Processing Standards Publication 198-1 <http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf>.
[5] RFC 5929: Channel Bindings for TLS <http://tools.ietf.org/html/rfc5929>.
[6] RFC 7627: Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension <http://tools.ietf.org/html/rfc7627>.

care when choosing a hash function. For current recommendations see Use of Cryptographic Hash Functions in XMPP (XEP-0300) [7].

8 IANA Considerations

This docment requires no interaction with the the Internet Assigned Numbers Authority (IANA) [8].

9 XMPP Registrar Considerations

9.1 Service Discovery Category/Type

Upon advancement of this proposal from experimental to draft status the XMPP Registrar [9] will include a category of "authz" in its registry at <https://xmpp.org/registrar/disco-categories.html>. The registrar will also add a value of "ephemeral" to that category. The registry submission is as follows:

```
<category>
  <name>authz</name>
  <desc>Services and nodes that provide authorization identities.</
     desc>
  <type>
    <name>ephemeral</name>
    <desc>
      An authorization service that provides ephemeral identities.
    </desc>
    <doc>XEP-0383</doc>
  </type>
</category>
```

Future submissions to the XMPP Registrar may register additional types.

9.2 Protocol Namespaces

This specification defines the following XML namespaces:

[7] XEP-0300: Use of Cryptographic Hash Functions in XMPP <https://xmpp.org/extensions/xep-0300.html>.

[8] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

[9] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

- urn:xmpp:burner:0

Upon advancement of this proposal from experimental to draft status the registrar will include the foregoing namespaces in its registry at <https://xmpp.org/registrar/namespaces.html> as governed by XMPP Registrar Function (XEP-0053) [10].

9.3 Namespace Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

10 XML Schema

TODO.

11 Acknowledgements

The author wishes to thank Philipp Hancke for his feedback.

[10] XEP-0053: XMPP Registrar Function <https://xmpp.org/extensions/xep-0053.html>.