ï»¿

      Personal Assertion Token (PASSporT) Extension for Diverted Calls

Abstract

   The Personal Assertion Token (PASSporT) is specified in RFC 8225 to
   convey cryptographically signed information about the people involved
   in personal communications. This document extends PASSporT to
   include an indication that a call has been diverted from its original
   destination to a new one. This information can greatly improve the
   decisions made by verification services in call forwarding scenarios.
   Also specified here is an encapsulation mechanism for nesting a
   PASSporT within another PASSporT that assists relying parties in some
   diversion scenarios.

   This document updates RFC 8224.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8946.

Table of Contents

1. Introduction

    A Personal Assertion Token (PASSporT) [RFC8225] is a token format
    based on the JSON Web Token (JWT) [RFC7519] for conveying
    cryptographically signed information about the people involved in
    personal communications; it is used by the Secure Telephone Identity
    Revisited (STIR) protocol [RFC8224] to convey a signed assertion of
    the identity of the participants in real-time communications
    established via a protocol like SIP. This specification extends
    PASSporT to include an indication that a call has been diverted from
    its original destination to a new one.

    Although the STIR problem statement [RFC7340] is focused on
    preventing the impersonation of the caller's identity, which is a
    common enabler for threats such as robocalling and voicemail hacking
    on the telephone network today, it also provides a signature over the
    called number at the time that the authentication service sees it.
    As [RFC8224], Section 12.1 describes, this protection over the
    contents of the To header field is intended to prevent a class of
    cut-and-paste attacks. If Alice calls Bob, for example, Bob might
    attempt to cut and paste the Identity header field in Alice's INVITE
    into a new INVITE that Bob sends to Carol, and thus be able to fool
    Carol into thinking the call came from Alice and not Bob. With the
    signature over the To header field value, the INVITE Carol sees will
    clearly have been destined originally for Bob, and thus Carol can
    view the INVITE as suspect.

    However, as [RFC8224], Section 12.1.1 points out, it is difficult for
    Carol to confirm or reject these suspicions based on the information
    she receives from the baseline PASSporT object. The common "call
    forwarding" service serves as a good example of the reality that the
    original called party number is not always the number to which a call
    is delivered. There are a number of potential ways for
    intermediaries to indicate that such a forwarding operating has taken
    place. The address in the To header field value of SIP requests is
    not supposed to change, according to baseline SIP behavior [RFC3261];
    instead, it is the Request-URI that is supposed to be updated when a
    call is retargeted. Practically speaking, however, many operational
    environments do alter the To header field. The History-Info header
    field [RFC7044] was created to store the Request-URIs that are
    discarded by a call in transit. The SIP Diversion header field
    [RFC5806], though historic, is still used for this purpose by some
    operators today. Neither of these header fields provide any
    cryptographic assurance of secure redirection, and they both record
    entries for minor syntactical changes in URIs that do not reflect a
    change to the actual target of a call.

    Therefore, this specification extends PASSporT with an explicit
    indication that the original called number in PASSporT no longer
    reflects the destination to which a call is intended to be delivered.
    For this purpose, it specifies a Divert PASSporT type ("div") for use
    in common SIP retargeting cases; it is expected that in this case,
    SIP INVITE requests will carry multiple Identity header fields, each
    containing its own PASSporT. Throughout this document, PASSporTs
    that contain a "div" element will be referred to as "div" PASSporTs.
    Verification services and the relying parties who make authorization
    decisions about communications may use this diversion indication to
    confirm that a legitimate retargeting of the call has taken place,
    rather than a cut-and-paste attack. For out-of-band use cases

[RFC8816] and other non-SIP applications of PASSporT, a separate
"div-o" PASSporT type is also specified, which defines an "opt"
PASSporT element for carrying nested PASSporTs within a PASSporT.
These shall in turn be referred to in this document as "div-o"
PASSporTs.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

3. The "div" PASSporT Type and Claim

This specification defines a PASSporT [RFC8225] type called "div",
which may be employed by authentication services located at
retargeting entities. All "div" PASSporTs MUST contain a new JSON
Web Token "div" claim, also specified in this document, which
indicates a previous destination for a call during its routing
process. When a retargeting entity receives a call signed with a
PASSporT, it may act as an authentication service and create a new
PASSporT containing the "div" claim to attach to the call.

Note that a new PASSporT is only necessary when the canonical form of
the "dest" identifier (per the canonicalization procedures in
[RFC8224], Section 8.3) changes due to this retargeting. If the
canonical form of the "dest" identifier is not changed during
retargeting, then a new PASSporT with a "div" claim MUST NOT be
produced.

The headers of the new PASSporTs generated by retargeting entities
MUST include the "div" PASSporT type and an "x5u" field pointing to a
credential that the retargeting entity controls. "div" PASSporTs MUST
use full form instead of compact form. The new PASSporT header will
look as follows:

```
{ "typ":"passport",
  "ppt":"div",
  "alg":"ES256",
  "x5u":"https://www.example.com/cert.cer" }
```

A "div" PASSporT claims set is populated with elements drawn from the
PASSporT(s) received for a call by the retargeting entity; at a high
level, the original identifier for the called party in the "dest"
object will become the "div" claim in the new PASSporT. If the
"dest" object of the original PASSporT contains multiple identifiers,
because it contains one or more name/value pairs with an array as its
value, the retargeting entity MUST select only one identifier from
the value(s) of the "dest" object to occupy the value of the "div"
field in the new PASSporT. Moreover, it MUST select an identifier
that is within the scope of the credential that the retargeting
entity will specify in the "x5u" of the PASSporT header (as described
below).

The new target for the call selected by the retargeting entity
becomes the value of the "dest" object of the new PASSporT. The
"orig" object MUST be copied into the new PASSporT from the original
PASSporT received by the retargeting entity. The retargeting entity
SHOULD retain the "iat" object from the original PASSporT, though if
in the underlying signaling protocol (e.g., SIP) the retargeting
entity changes the date and time information in the retargeted
request, the new PASSporT should instead reflect that date and time.
No other claims or extensions are to be copied from the original
PASSporT to the "div" PASSporT.

So, for an original PASSporT claims set of the form:

```
{ "dest":{"tn":["12155551213"]},
  "iat":1443208345,
```

```
        "orig":{"tn":"12155551212"} }
```

If the retargeting entity is changing the target from 12155551213 to
12155551214, the claims set of a "div" PASSporT generated by the
retargeting entity would look as follows:

```
    { "dest":{"tn":["12155551214"]},
      "div":{"tn":"121555551213"},
      "iat":1443208345,
      "orig":{"tn":"12155551212"} }
```

The combined full form PASSporT (with a signature covered by the
ES256 keys given in Appendix A) would look as follows:

```
eyJhbGciOiJFUzI1NiIsInBwdCI6ImRpdiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ij \
oiaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5jZXIifQ.eyJkZXN0Ijp7InRuI \
jpbIjEyMTU1NTUxMjE0Il19LCJkaXYiOnsidG4iOiIxMjE1NTU1NTEyMTMifSwiaWF \
0IjoxNDQzMjA4MzQ1LCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.xBHWipDEE \
J8a6TsdX6xUXAnblsFiGUiAxwLiv0HLC9IICj6eG9jQd6WzeSSjHRBwxmChHhVIiMT \
SqIlk3yCNkg
```

The same "div" PASSporT would result if the "dest" object of the
original PASSporT contained an array value, such as
{"tn":["12155551213","19995551234"]}, and the retargeting entity
chose to retarget from the first telephone number in the array.
Every "div" PASSporT is diverting from only one identifier.

Note that the "div" element may contain other name/value pairs than
just a destination, including a History-Info indicator (see
Section 8). After the PASSporT header and claims have been
constructed, their signature is generated per the guidance in
[RFC8225] -- except for the credential required to sign it. While in
the ordinary construction of a PASSporT, the credential used to sign
will have authority over the identity in the "orig" claim (for
example, a certificate with authority over the telephone number in
"orig" per [RFC8226]), for all PASSporTs using the "div" type the
signature MUST be created with a credential with authority over the
identity present in the "div" claim. So for the example above, where
the original "dest" is "12155551213", the signer of the new PASSporT
object MUST have authority over that telephone number and need not
have any authority over the telephone number present in the "orig"
claim.

Note that Identity header fields are not ordered in a SIP request,
and in a case where there is a multiplicity of Identity header fields
in a request, some sorting may be required to match "div" PASSporTs
to their originals.

PASSporTs of type "div" MUST NOT contain an "opt" (see Section 6)
element in their payload.

4. Using "div" in SIP

   This section specifies SIP-specific usage for the "div" PASSporT type
   and its handling in the SIP Identity header field "ppt" parameter
   value. Other protocols using PASSporT may define behavior specific
   to their use of the "div" claim.

4.1. Authentication Service Behavior

   An authentication service only adds an Identity header field value
   containing the "div" PASSporT type to a SIP request that already
   contains at least one Identity header field value; it MUST NOT add a
   "div" PASSporT to an INVITE that contains no Identity header field.
   The retargeting entity SHOULD act as a verification service and
   validate the existing Identity header field value(s) in the request
   before proceeding; in some high-volume environments, it may instead
   put that burden of validating the chain entirely on the terminating
   verification service. As the authentication service will be adding a
   new PASSporT that refers to an original, it MUST NOT remove the
   original request's Identity header field value before forwarding.

As was stated in Section 3, the authentication service MUST sign any
"div" PASSporT with a credential that has a scope of authority
covering the identity it populates in the "div" element value. Note
that this is a significant departure from baseline STIR
authentication service behavior, in which the PASSporT is signed by a
credential with authority over the "orig" field. The "div" value
reflects the URI that caused the call to be routed to the retargeting
entity, so in ordinary operations, it would already be the STIR
entity holding the appropriate private keying material for calls
originating from that identity.

A SIP authentication service typically will derive the "dest" element
value of a "div" PASSporT from a new Request-URI that is set for the
SIP request before it is forwarded. Older values of the Request-URI
may appear in header fields like Diversion or History-Info; this
document specifies an optional interaction with History-Info below in
Section 8. Note as well that because PASSporT operates on
canonicalized telephone numbers and normalized URIs, many smaller
changes to the syntax of identifiers that might be captured by other
mechanisms that record retargeting (like History-Info) will likely
not require a "div" PASSporT.

When adding an Identity header field with a PASSporT claims set
containing a "div" claim, SIP authentication services MUST also add a
"ppt" parameter to that Identity header with a value of "div". For
the example PASSporT given in Section 3, the new Identity header
added after retargeting might look as follows:

Identity:eyJhbGciOiJFUzI1NiIsInBwdCI6ImRpdiIsInR5cCI6InBhc3Nwb3J0I \
iwieDV1IjoiaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5jZXIifQ.eyJkZXN0 \
Ijp7InRuIjpbIjEyMTU1NTUxMjE0Il19LCJkaXYiOnsidG4iOiIxMjE1NTU1NTEyMT \
MifSwiaWF0IjoxNDQzMjA4MzQ1LCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0. \
xBHWipDEEJ8a6TsdX6xUXAnblsFiGUiAxwLiv0HLC9IICj6eG9jQd6WzeSSjHRBwxm \
ChHhVIiMTSqIlk3yCNkg; \
info=<https://www.example.com/cert.cer>;ppt="div"

Note that in some deployments, an authentication service will need to
generate "div" PASSporTs for a request that contains multiple
non-"div" Identity header field values. For example, a request
arriving at a retargeting entity might contain, in different Identity
header fields, a baseline [RFC8224] PASSporT and a PASSporT of type
"rph" [RFC8443] signed by a separate authority. Provided that these
PASSporTs share the same "orig" and "dest" values, the retargeting
entity's authentication service SHOULD generate only one "div"
PASSporT. If the "orig" or "dest" of these PASSporTs differ,
however, one "div" PASSporT SHOULD be generated for each non-"div"
PASSporT. Note that this effectively creates multiple chains of
"div" PASSporTs in a single request, which complicates the procedures
that need to be performed at verification services.

Furthermore, a request may also be retargeted a second time, at which
point the subsequent retargeting entity SHOULD generate one "div"
PASSporT for each previous "div" PASSporT in the request that
contains a "dest" object with the value of the current target -- but
not for "div" PASSporTs with earlier targets. Ordinarily, the
current target will be readily identifiable, as it will be in the
last "div" PASSporT in each chain, and in SIP cases, it will
correspond to the Request-URI received by the retargeting entity.
Moreover, the current target will be an identifier that the
retargeting entity possesses a credential to sign for, which may not
be true for earlier targets. Ultimately, on each retargeting, the
number of PASSporTs added to a request will be equal to the number of
non-"div" PASSporTs that do not share the same "orig" and "dest"
object values.

4.2. Verification Service Behavior

   [RFC8224], Section 6.2, Step 5 requires that specifications defining
   "ppt" values describe any additional or alternative verifier
   behavior. The job of a SIP verification service handling one or more

"div" PASSporTs is very different from that of a traditional
verification service. At a high level, the immediate responsibility
of the verification service is to extract all PASSporTs from the two
or more Identity header fields in a request, identify which are "div"
PASSporTs and which are not, and then order and link the "div"
PASSporTs to the original PASSporT(s) in order to build one or more
chains of retargeting.

In order to validate a SIP request using the "div" PASSporT type, a
verification service needs to inspect all of the valid Identity
header field values associated with a request, as an Identity header
field value containing "div" necessarily refers to an earlier
PASSporT already in the message. For each "div" PASSporT, the
verification service MUST find an earlier PASSporT that contains a
"dest" claim with a value equivalent to the "div" claim in each "div"
PASSporT. It is possible that this earlier PASSporT will also
contain a "div" and that it will in turn chain to a still earlier
PASSporT stored in a different Identity header field value. If a
complete chain cannot be constructed, the verification service cannot
complete "div" validation; it MAY still validate any non-"div"
PASSporTs in the request per the normal procedures in [RFC8224]. If
a chain has been successfully constructed, the verification service
extracts from the outermost (that is, the most recent) PASSporT in
the chain a "dest" field; this will be a "div" PASSporT that no other
"div" PASSporT in the SIP request refers to. Its "dest" element
value will be referred to in the procedures that follow as the value
of the "outermost "dest" field".

Ultimately, by looking at this chain of transformations and
validating the associated signatures, the verification service will
be able to ascertain that the appropriate parties were responsible
for the retargeting of the call to its current destination. This can
help the verification service to determine that the original PASSporT
in the call was not simply used in a cut-and-paste attack and inform
any associated authorization decisions in terms of how the call will
be treated -- though, per [RFC8224], Section 6.2.1, that decision is
a matter of local policy and is thus outside the scope of this
specification.

A verification service parses a chain of PASSporTs as follows:

1. The verification service MUST compare the value in the outermost
    "dest" field to the target of the call. As it is anticipated
    that SIP authentication services that create "div" PASSporTs will
    populate the "dest" header from the retargeted Request-URI (see
    Section 4.1), in ordinary SIP operations, the Request-URI is
    where verification services will find the latest call target.
    Note, however, that after a "div" PASSporT has been added to a
    SIP request, the Request-URI may have been updated during normal
    call processing to an identifier that no longer contains the
    logical destination of a call; in this case, the verification
    service MAY compare the "dest" field to a provisioned telephone
    number for the recipient.

2. The verification service MUST validate the signature over the
    outermost "div" PASSporT and establish that the credential that
    signed the "div" PASSporT has the authority to attest for the
    identifier in the "div" element of the PASSporT (per [RFC8224],
    Section 6.2, Step 3).

3. The verification service MUST validate that the "orig" field of
    the innermost PASSporT of the chain (the only PASSporT in the
    chain that will not be of PASSporT type "div") is equivalent to
    the "orig" field of the outermost "div" PASSporT; in other words,
    that the original calling identifier has not been altered by
    retargeting authentication services. If the "orig" value has
    changed, the verification service MUST treat the entire PASSporT
    chain as invalid. The verification service MUST also verify that
    all other "div" PASSporTs in the chain share the same "orig"
    value. Then, the verification service validates the relationship
    of the "orig" field to the SIP-level call signaling per the

guidance in [RFC8224], Section 6.2, Step 2.

4. The verification service MUST check the date freshness in the
    outermost "div" PASSporT, per [RFC8224], Section 6.2, Step 4.
    Furthermore, it is RECOMMENDED that the verification service
    check that the "iat" field of the innermost PASSporT is also
    within the date freshness interval; otherwise, the verification
    service could allow attackers to replay an old, stale PASSporT
    embedded in a fresh "div". However, note that in some use cases,
    including certain ways that call transfers are implemented, it is
    possible that an established call will be retargeted long after
    it has originally been placed, and verification services may want
    to allow a longer window for the freshness of the innermost
    PASSporT if the call is transferred from a trusted party (as an
    upper bound, a freshness window on the order of three hours might
    suffice).

5. The verification service MUST inspect and validate the signatures
    on each and every PASSporT object in the chain between the
    outermost "div" PASSporT and the innermost PASSporT. Note that
    (per Section 4.1) a chain may terminate at more than one
    innermost PASSporT, in cases where a single "div" is used to
    retarget from multiple innermost PASSporTs. Also note that
    [RFC8224], Section 6.2, Step 1 applies to the chain validation
    process; if the innermost PASSporT contains an unsupported "ppt",
    its chain MUST be ignored.

Note that the To header field is not used in the first step above.
Optionally, the verification service MAY verify that the To header
field value of the received SIP signaling is equal to the "dest"
value in the innermost PASSporT; however, as has been observed in
some deployments, the original To header field value may be altered
by intermediaries to reflect changes of target. Deployments that
change the original To header field value to conceal the original
destination of the call from the ultimate recipient should note that
the original destination of a call may be preserved in the innermost
PASSporT. Future work on "div" might explore methods to implement
that sort of policy while retaining a secure chain of redirection.

5. The "div-o" PASSporT Type

This specification defines a "div-o" PASSporT type that uses the
"div" claim element in conjunction with the "opt" (Section 6) claim
element. As is the case with "div" PASSporT type, a "div-o" PASSporT
is created by an authentication service acting for a retargeting
entity, but instead of generating a separate "div" PASSporT to be
conveyed alongside an original PASSporT, the authentication service
in this case embeds the original PASSporT inside the "opt" element of
the "div-o" PASSporT. The "div-o" extension is designed for use in
non-SIP or gatewayed SIP environments where the conveyance of
PASSporTs in separate Identity header fields in impossible, such as
out-of-band STIR scenarios [RFC8816].

The syntax of "div-o" PASSporTs is very similar to "div". A "div-o"
PASSporT header object might look as follows:

{ "typ":"passport",
  "ppt":"div-o",
  "alg":"ES256",
  "x5u":"https://www.example.com/cert.cer" }

Whereas a "div" PASSporT claims set contains only the "orig", "dest",
"iat", and "div" elements, the "div-o" additionally MUST contain an
"opt" element (see Section 6), which encapsulates the full form of
the previous PASSporT from which the call was retargeted, triggering
the generation of this "div-o". The format of the "opt" element is
identical to the encoded PASSporT format given in Appendix A of
[RFC8225].

So, for an original PASSporT claims set of the form:

```
     { "orig":{"tn":"12155551212"},
       "dest":{"tn":["12155551213"]},
       "iat":1443208345 }
```

If the retargeting entity is changing the target from 12155551213 to
12155551214, the new PASSporT claims set for "div-o" would look as
follows:

```
  { "orig":{"tn":"12155551212"},
     "dest":{"tn":["12155551214"]},
     "iat":1443208345,
     "div":{"tn":"121555551213"},
     "opt":"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0c \
     HM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5jZXIifQ.eyJkZXN0Ijp7InRuIjpbIj \
     EyMTU1NTUxMjEzIl19LCJpYXQiOjE0NDMyMDgzNDUsIm9yaWciOnsidG4iOiIxMj \
     E1NTU1MTIxMiJ9fQ.1bEzkzcNbKvgz4QoMx0_DJ2T8qFMDC1sPqHPXl1WvbauzRJ \
     RvYlZqQ0qgGTlS8tJ_wXjVe07Z3wvDrdApHhhYw" }
```

While in ordinary operations, it is not expected that SIP would carry
a "div-o" PASSporT, it might be possible in some gatewaying
scenarios. The resulting full form Identity header field with a
"div-o" PASSporT would look as follows:

```
Identity:eyJhbGciOiJFUzI1NiIsInBwdCI6ImRpdi1vIiwidHlwIjoicGFzc3Bvc \
nQiLCJ4NXUiOiJodHRwczovL3d3dy5leGFtcGxlLmNvbS9jZXJ0LmNlciJ9.eyJkZX \
N0Ijp7InRuIjoiMTIxNTU1NTEyMTQifSwiZGl2Ijp7InRuIjoiMTIxNTU1NTUxMjEz \
In0sImlhdCI6MTQ0MzIwODM0NSwib3B0IjoiZXlKaGJHY2lPaUpGVXpJMU5pSXNJbl \
I1Y0NJNkluQmhjM053YjNKMElpd2llRFYxSWpvaWFIUjBjSE02THk5M2QzY3VaWGho \
YlhCc1pTNWpiMjB2WTJWeWRDNWpaWElpZlEuZXlKa1pYTjBJanA3SW5SdUlqcGJJak \
V5TVRVMU5UVXhNakV6SWwxOUxDSnBZWFFpT2pFME5ETlNRGd6TkRVc0ltOXlhV2Np \
T25zaWRHNGlPaUl4TWpFMU5UVTFNVEl4TWlKOWZRLjFiRXpremNOYkt2Z3o0UW9NeD \
BfREoyVDhxRk1EQzFzUHFIUFhsMVd2YmF1elJKUnZZbFpxUTBxZ0dUbFM4dEpfd1hq \
VmUwN1ozd3ZEcmRBcEhoaFl3Iiwib3JpZyI6eyJ0biI6IjEyMTU1NTUxMjEyIn19.C \
HeA9wRnthl7paMe6rP0TARpmFCXjmi_vF_HRz2O_oulB_R-G9xZNiLVvmvHv4gk6LI \
LaDV2y2VtHTLIEgmHig; \
info=<https://www.example.com/cert.cer>;ppt="div-o"
```

5.1. Processing "div-o" PASSporTs

   The authentication and verification service procedures required for
   "div-o" closely follow the guidance given in Sections 4.1 and 4.2,
   with the major caveats being, first, that they do store or retrieve
   PASSporTs via the Identity header field values of SIP requests and,
   second, that they process nested PASSporTs in the "opt" claim
   element. But transposing the rest of the behaviors described above
   to creating and validating "div-o" PASSporTs is straightforward.

   For the "div-o" PASSporT type, retargeting authentication services
   that handle calls with one or more existing PASSporTs will create a
   corresponding "div-o" PASSporT for each received PASSporT. Each
   "div-o" PASSporT MUST contain an "opt" claim set element with the
   value of the original PASSporT from which the "div-o" was created; as
   specified in Section 4.1, the authentication service MUST populate
   the "div" claim set element of the "div-o" PASSporT with the "dest"
   field of the original PASSporT. Each received PASSporT may in turn
   contain its own "opt" claim set element if the retargeting
   authentication service is not the first in its chain. Note that if
   the retargeting authentication service is handling a call with
   multiple PASSporTs, which in ordinary SIP operation would result in
   the construction of multiple "div" chains, it will in effect be
   generating one "div-o" PASSporT per chain.

   The job of a verification service is in many ways easier for "div-o"
   than for "div", as the verification service has no need to correlate
   the PASSporTs it receives and assemble them into chains, as any
   chains in "div-o" will be nested through the "opt" element.
   Nonetheless, the verification services MUST perform the same chain
   validation described in Section 4.2 to validate that each nested
   PASSporT shares the same "orig" field as its enclosing PASSporT and
   that the "dest" field of each nested PASSporT corresponds to the
   "div" field of its enclosing PASSporT. The same checks MUST also be

performed for freshness, signature validation, and so on. It is
similarly OPTIONAL for the verification service to determine that the
"dest" claims element of the outermost PASSporT corresponds to the
called party indication of receive telephone signaling, where such
indication would vary depending on the using protocol.

How authentication services or verification services receive or
transport PASSporTs for "div-o" is outside the scope of this document
and dependent on the using protocol.

6. Definition of "opt"

The presence of an "Original PASSporT" ("opt") claims set element
signifies that a PASSporT encapsulates another entire PASSporT within
it, typically a PASSporT that was transformed in some way to create
the current PASSporT. Relying parties may need to consult the
encapsulated PASSporT in order to validate the identity of a caller.
"opt", as defined in this specification, may be used by future
PASSporT extensions as well as in conjunction with "div-o".

"opt" MUST contain a quoted full-form PASSporT, as specified by
[RFC8225], Appendix A; it MUST NOT contain a compact form PASSporT.
For an example of a "div-o" PASSporT containing "opt", see Section 5.

7. "div" and Redirection

The "div" mechanism exists primarily to prevent false negatives at
verification services when an arriving SIP request, due to
intermediary retargeting, does not appear to be intended for its
eventual recipient, because the original PASSporT "dest" value
designates a different destination.

Any intermediary that assigns a new target to a request can, instead
of retargeting and forwarding the request, redirect with a 3xx
response code. In ordinary operations, a redirection poses no
difficulties for the operations of baseline STIR: when the user agent
client (UAC) receives the 3xx response, it will initiate a new
request to the new target (typically the target carried in the
Contact header field value of the 3xx), and the "dest" of the
PASSporT created for the new request will match that new target. As
no impersonation attack can arise from this case, it creates no new
requirements for STIR.

However, some UACs record the original target of a call with
mechanisms like History-Info [RFC7044] or Diversion [RFC5806] and may
want to leverage STIR to demonstrate to the ultimate recipient that
the call has been redirected securely, that is, that the original
destination was the one that sent the redirection message that led to
the recipient receiving the request. The semantics of the PASSporT
necessary for that assertion are the same as those for the "div"
retargeting cases above. The only wrinkle is that the PASSporT needs
to be generated by the redirecting entity and sent back to the
originating user agent client within the 3xx response.

This introduces more complexity than might immediately be apparent.
In the first place, a 3xx response can convey multiple targets
through the Contact header field value; to accommodate this, the
"div" PASSporT MAY include one "dest" object array value per Contact,
but if the retargeting entity wants to keep the Contact list private
from targets, it may need to generate one PASSporT per Contact. Bear
in mind as well that the original SIP request could have carried
multiple Identity header field values that had been added by
different authentication services in the request path, so a
redirecting entity might need to generate one "div" PASSporT for each
PASSporT in the original request. Often, this will mean just one
"div" PASSporT, but for some deployment scenarios, it could require
an impractical number of combinations. But in very complex call
routing scenarios, attestation of source identity would only add
limited value anyway.

Therefore, STIR-aware SIP intermediaries that redirect requests MAY

convey one or more PASSporTs in the backwards direction within
Identity header fields. These redirecting entities will act as
authentication services for "div" as described in Section 4.1. This
document consequently updates [RFC8224] to permit carrying Identity
header fields in SIP 300-class responses. It is left to the
originating user agent to determine which Identity header fields
should be copied from the 3xx into any new requests resulting from
the redirection, if any; use of these Identity header fields by
entities receiving a 3xx response is OPTIONAL.

Finally, note that if an intermediary in the response path consumes
the 3xx and explores new targets itself while performing sequential
forking, it will effectively retarget the call on behalf of the
redirecting server, and this will create the same need for "div"
PASSporTs as any other retargeted call. These intermediaries MAY
also copy PASSporTs from the 3xx response and insert them into
sequential forking requests, if appropriate.

8. Extending "div" to Work with Service Logic Tracking

It is anticipated that "div" may be used in concert with History-Info
[RFC7044] in some deployments. It may not be clear from the "orig"
and "dest" values which History-Info header a given PASSporT
correlates to, especially because some of the target changes tracked
by History-Info will not be reflected in a "div" PASSporT (see
Section 1). Therefore, an "hi" element as defined here may appear in
"div" corresponding to the History-Info header field index parameter
value. So for a History-Info header field with an index value of
"1.2.1", the claims set of the corresponding PASSporT with "div"
might look like:

        { "orig":{"tn":"12155551212"},
          "dest":{"tn":["12155551214"]},
          "iat":1443208345,
          "div":{"tn":"121555551213",
                 "hi":"1.2.1"} }

Past experience has shown that there may be additional information
about the motivation for retargeting, which relying parties might
consider when making authorization decisions about a call; see, for
example, the "reason" associated with the SIP Diversion header field
[RFC5806]. Future extensions to this specification might incorporate
reasons into "div".

9. IANA Considerations

9.1. JSON Web Token Claims Registrations

Per this specification, IANA has added two new claims to the "JSON
Web Token Claims" registry as defined in [RFC7519].

9.1.1. "div" registration

Claim Name: div

Claim Description: Diverted Target of a Call

Change Controller: IESG

Reference: RFC 8946

9.1.2. "opt" registration

Claim Name: opt

Claim Description: Original PASSporT (in Full Form)

Change Controller: IESG

Reference: RFC 8946

9.2. PASSporT Type Registrations

   This specification defines two new PASSporT types for the "Personal
   Assertion Token (PASSporT) Extensions" registry defined in [RFC8225],
   which resides at <https://www.iana.org/assignments/passport>. They
   are:

   * "div", as defined in Section 3.

   * "div-o", as defined in Section 5.

10. Privacy Considerations

   There is an inherent trade-off in any mechanism that tracks, in SIP
   signaling, how calls are routed through a network, as routing
   decisions may expose policies set by users for how calls are
   forwarded, potentially revealing relationships between different
   identifiers representing the same user. Note, however, that in
   ordinary operations, this information is revealed to the user agent
   service of the called party, not the calling party. It is usually
   the called party who establishes these forwarding relationships, and
   if indeed some other party is responsible for calls being forwarded
   to the called party, many times the called party should likely be
   entitled to information about why they are receiving these calls.
   Similarly, a redirecting entity who sends a 3xx in the backwards
   direction knowingly shares information about service logic with the
   caller's network. However, as there may be unforeseen circumstances
   where the revelation of service logic to the called party poses a
   privacy risk, implementers and users of this or similar diversion-
   tracking techniques should understand the trade-off.

   Furthermore, it is a general privacy risk of identity mechanisms
   overall that they do not interface well with anonymization services;
   the interaction of STIR with anonymization services is detailed in
   [RFC8224], Section 11. Any forwarding service that acts as an
   anonymizing proxy may not be able to provide a secure chain of
   retargeting due to the obfuscation of the originating identity.

   Also see [RFC8224], Section 11 for further considerations on the
   privacy of using PASSporTs in SIP.

11. Security Considerations

   This specification describes a security feature and is primarily
   concerned with increasing security when calls are forwarded.
   Including information about how calls were retargeted during the
   routing process can allow downstream entities to infer particulars of
   the policies used to route calls through the network. However,
   including this information about forwarding is at the discretion of
   the retargeting entity, so if there is a requirement to keep an
   intermediate called number confidential, no PASSporT should be
   created for that retargeting -- the only consequence will be that
   downstream entities will be unable to correlate an incoming call with
   the original PASSporT without access to some prior knowledge of the
   policies that could have caused the retargeting.

   Any extension that makes PASSporTs larger creates a potential
   amplification mechanism for SIP-based DDoS attacks. Since diversion
   PASSporTs are created as a part of normal forwarding activity, this
   risk arises at the discretion of the retargeting domain; simply using
   3xx response redirections rather than retargeting (by supplying a
   "div" per Section 7) mitigates the potential impact. Under unusual
   traffic loads, even domains that might ordinarily retarget requests
   can switch to redirection.

   SIP has an inherent capability to redirect requests, including
   forking them to multiple parties -- potentially, a very large number
   of parties. The use of the "div" PASSporT type does not grant any
   additional powers to attackers who hope to place bulk calls; if
   present, the "div" PASSporT instead identifies the party responsible

for the forwarding. As such, senders of bulk unsolicited traffic are
unlikely to find the use of "div" attractive.

12. References

12.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
              A., Peterson, J., Sparks, R., Handley, M., and E.
              Schooler, "SIP: Session Initiation Protocol", RFC 3261,
              DOI 10.17487/RFC3261, June 2002,
              <https://www.rfc-editor.org/info/rfc3261>.

   [RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and
              C. Holmberg, "An Extension to the Session Initiation
              Protocol (SIP) for Request History Information", RFC 7044,
              DOI 10.17487/RFC7044, February 2014,
              <https://www.rfc-editor.org/info/rfc7044>.

   [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token
              (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015,
              <https://www.rfc-editor.org/info/rfc7519>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt,
              "Authenticated Identity Management in the Session
              Initiation Protocol (SIP)", RFC 8224,
              DOI 10.17487/RFC8224, February 2018,
              <https://www.rfc-editor.org/info/rfc8224>.

   [RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion
              Token", RFC 8225, DOI 10.17487/RFC8225, February 2018,
              <https://www.rfc-editor.org/info/rfc8225>.

   [RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity
              Credentials: Certificates", RFC 8226,
              DOI 10.17487/RFC8226, February 2018,
              <https://www.rfc-editor.org/info/rfc8226>.

12.2. Informative References

   [RFC5806] Levy, S. and M. Mohali, Ed., "Diversion Indication in
              SIP", RFC 5806, DOI 10.17487/RFC5806, March 2010,
              <https://www.rfc-editor.org/info/rfc5806>.

   [RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure
              Telephone Identity Problem Statement and Requirements",
              RFC 7340, DOI 10.17487/RFC7340, September 2014,
              <https://www.rfc-editor.org/info/rfc7340>.

   [RFC8443] Singh, R., Dolly, M., Das, S., and A. Nguyen, "Personal
              Assertion Token (PASSporT) Extension for Resource Priority
              Authorization", RFC 8443, DOI 10.17487/RFC8443, August
              2018, <https://www.rfc-editor.org/info/rfc8443>.

   [RFC8816] Rescorla, E. and J. Peterson, "Secure Telephone Identity
              Revisited (STIR) Out-of-Band Architecture and Use Cases",
              RFC 8816, DOI 10.17487/RFC8816, February 2021,
              <https://www.rfc-editor.org/info/rfc8816>.

Appendix A. Keys for Examples

   The following EC256 keys are used in the signing examples given in

this document. WARNING: Do not use this key pair in production
systems.

-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEmzGM1VsO+3IqbMF54rQMaYKQftO4
hUYm9wv5wutLgEd9FsiTy3+4+Wa2O7pffOXPC0QzO+yD8hGEXGP/2mZo6w==
-----END PUBLIC KEY-----

-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIFKCsFZ4Wsw3ZpBxgc4Z0sOjaXDdMk07Ny1fKg6OntAkoAoGCCqGSM49
AwEHoUQDQgAEmzGM1VsO+3IqbMF54rQMaYKQftO4hUYm9wv5wutLgEd9FsiTy3+4
+Wa2O7pffOXPC0QzO+yD8hGEXGP/2mZo6w==
-----END EC PRIVATE KEY-----

Acknowledgments

Author's Address

Jon Peterson
Neustar, Inc.
1800 Sutter St., Suite 570
Concord, CA 94520
United States of America

Email: jon.peterson@team.neustar