M. Scurtescu
Google
A. Backman
Amazon
P. Hunt
Oracle
J. Bradley
Yubico
January 29, 2018

RISC Event Types
risc-event-types-00

Abstract

This document defines the RTISC Event Types. Event Types are introduced and defined in Security Event Token (SET) [SET].

Table of Contents

1. Introduction

This specification is based on RISC Profile [RISC-PROFILE] and uses the subject identifiers defined there.

1.1. Notational Conventions

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].

2. Event Types

The base URI for RISC event types is:
http://schemas.openid.net/secevent/risc/event-type/

2.1. Account Credential Change Required

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/account-credential-change-required

Account Credential Change Required signals that the account identified by the subject was required to change a credential. For example the user was required to go through a password change.

Attributes: none

```
{
  "iss": "https://idp.example.com/",
  "jti": "756E69717565206964656E746966696572",
  "iat": 1508184845,
  "aud": "636C69656E745F6964",
  "events": {
    "http://schemas.openid.net/secevent/risc/event-type/\
    account-credential-change-required": {
      "subject": {
        "subject_type": "iss-sub",
        "iss": "https://idp.example.com/",
        "sub": "7375626A656374",
      }
    }
  }
}
```

(the event type URI is wrapped, the backslash is the continuation character)

Figure 1: Example: Account Credential Change Required

2.2. Account Deleted

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/account-deleted

Account Deleted signals that the account identified by the subject has been permanently deleted.

Attributes: none

2.3. Account Disabled

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/account-disabled

Account Disabled signals that the account identified by the subject has been disabled. The actual reason why the account was disabled might be specified with the nested ’reason’ attribute described below. The account may be enabled (Section 2.4) in the future.

Attributes:

- reason - optional, describes why was the account disabled. Possible values:
  - hijacking
  - bulk-account
- cause-time - the initial cause that lead to the account to be disabled. In most cases this is an estimated time. For example, the actual hijacking time. This is before the event time.

```
{
  "iss": "https://idp.example.com/",
  "jti": "756E69717565206964656E746966696572",
  "iat": 1508184845,
  "aud": "636C69656E745F6964",
  "events": {
    "http://schemas.openid.net/secevent/risc/event-type/\
    account-disabled": {
      "subject": {
        "subject_type": "iss-sub",
        "iss": "https://idp.example.com/",
        "sub": "7375626A656374",
      },
      "reason": "hijacking",
      "cause-time": 1508012752,
    }
  }
}
```

(the event type URI is wrapped, the backslash is the continuation character)

Figure 2: Example: Account Disabled

2.4. Account Enabled

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/account-enabled

Account Enabled signals that the account identified by the subject has been enabled.

Attributes: none

2.5. Identifier Changed

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/identifier-changed

Identifier Changed signals that the identifier specified in the subject has changed. The subject's type MUST be either 'email' or 'phone' and it MUST specify the old value.

Attributes:

- new-value - required, the new value of the identifier.

```
{
  "iss": "https://idp.example.com/",
  "jti": "756E69717565206964656E746966696572",
  "iat": 1508184845,
  "aud": "636C69656E745F6964",
  "events": {
    "http://schemas.openid.net/secevent/risc/event-type/\
    identifier-changed": {
      "subject": {
        "subject_type": "email",
        "email": "foo@example.com",
      },
      "new-value": "bar@example.com",
    }
  }
}
```

The ’foo@example.com’ email changed to ’bar@example.com’. _(the event type URI is wrapped, the backslash is the continuation character)_

Figure 3: Example: Identifier Changed

2.6. Identifier Recycled

Event Type URI: http://schemas.openid.net/secevent/risc/event-type/identifier-recycled

Identifier Recycled signals that the identifier specified in the subject was recycled and now it belongs to a new user. The subject MUST be either ’email’ or ’phone-number’.

Attributes: none

```
{
  "iss": "https://idp.example.com/",
  "jti": "756E69717565206964656E746966696572",
  "iat": 1508184845,
  "aud": "636C69656E745F6964",
  "events": {
    "http://schemas.openid.net/secevent/risc/event-type/\
    identifier-recycled": {
      "subject": {
        "subject_type": "email",
        "email": "foo@example.com",
      }
    }
  }
}
```

The ’foo@example.com’ email address was recycled. _(the event type URI is wrapped, the backslash is the continuation character)_

Figure 4: Example: Identifier Recycled

2.7. Opt Out

Users SHOULD be allowed to opt-in and out of RISC events being sent for their accounts. With regards to opt-out an account can be in one of these three states:

1. opt-in - the account is participating in RISC event exchange.

2. opt-out-initiated - the user requested to be excluded from RISC event exchanges, but for practical security reasons for a period of time RISC events are still exchanged. The main reason for this state is to prevent a hijacker from immediately opting out of RISC.

3. opt-out - the account is NOT participating in RISC event exchange.

State changes trigger Opt-Out Events as represented bellow:

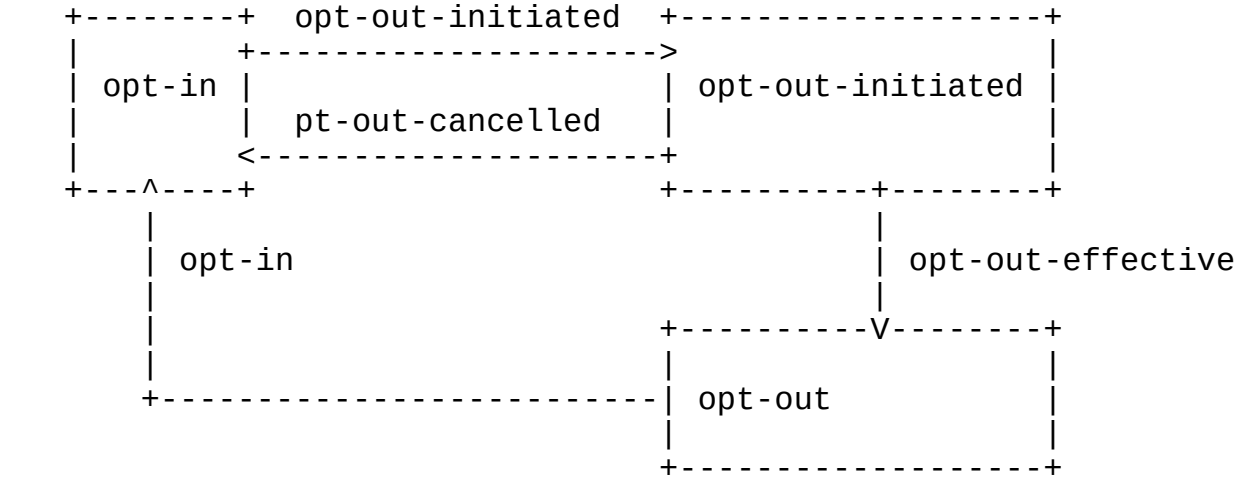

Figure 5: Opt-Out States and Opt-Out Events

Both Transmitters and Receivers SHOULD manage Opt-Out state for users. Transmitters should send the events defined in this section when the Opt-Out state changes.

2.7.1. Opt In

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/opt-in

Opt In signals that the account identified by the subject opted into RISC event exchanges. The account is in the ’opt-in’ state.

Attributes: none

2.7.2. Opt Out Initiated

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/opt-out-initiated

Opt Out Initiated signals that the account identified by the subject initiated to opt out from RISC event exchanges. The account is in the ’opt-out-initiated’ state.

Attributes: none

2.7.3. Opt Out Cancelled

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/opt-out-cancelled

Opt Out Cancelled signals that the account identified by the subject cancelled the opt out from RISC event exchanges. The account is in the 'opt-in' state.

Attributes: none

2.7.4. Opt Out Effective

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/opt-out-effective

Opt Out Effective signals that the account identified by the subject was effectively opted out from RISC event exchanges. The account is in the 'opt-out' state.

Attributes: none

2.8. Recovery Activated

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/recovery-activated

Recovery Activated signals that the account identified by the subject activated a recovery flow.

Attributes: none

2.9. Recovery Information Changed

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/recovery-information-changed

Recovery Information Changed signals that the account identified by the subject has changed some of its recovery information. For example a recovery email address was added or removed.

Attributes: none

2.10. Sessions Revoked

Event Type URI:
http://schemas.openid.net/secevent/risc/event-type/sessions-revoked

Sessions Revoked signals that all the sessions for the account identified by the subject have been revoked.

Attributes: none

3. Normative References

[JSON] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

[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>.

[RISC-PROFILE] OpenID Foundation, "RISC Profile".

[SET] IETF, "Security Event Token (SET)", <https://tools.ietf.org/html/draft-ietf-secevent-token>.

Authors' Addresses

Marius Scurtescu
Google

Email: mscurtescu@google.com

Annabelle Backman
Amazon

Email: richanna@amazon.com

Phil Hunt
Oracle Corporation

Email: phil.hunt@yahoo.com

John Bradley
Yubico

Email: secevemt@ve7jtb.com