Contacts in Metadata

Contact Information in Metadata

The principal use of contact information in metadata is to enable effective communication between Federation participants, especially when systems fail, when users encounter problems, or when a security incident occurs.

> **Meeting Baseline Expectations**
> InCommon will phase in the Baseline Expectations program through much of calendar year 2018. Over time, this program will make some user interface elements mandatory (these are noted below). InCommon recommends adding all of these user elements to your metadata; in particular those that will become mandatory. For more information, see the Baseline Expectations wiki page.

A secondary function is to support user interfaces (UIs) but much of the contact information displayed by an identity provider or service provider (for example on error, discovery, login, or consent pages) is self-owned and therefore known by the presenting site. A notable exception is an identity provider contact suitable for brokering attribute release changes when users encounter failures accessing services because the Requested Attributes are not released to SPs.

There are four types of contacts in Federation metadata:

- **technical contact**: for direct communication between InCommon participants regarding *technical issues* such as troubleshooting software, systems, or networking issues
- **administrative contact**: for direct communication between InCommon participants and by institutional users regarding *non-technical issues* such as attribute release policy, on-boarding issues, privacy, assurance certification and assurance qualifiers, etc.
- **security contact**: for direct communication between InCommon participants regarding security matters, especially for the purposes of Federated Security Incident Response
- **support contact**: for *end-user technical support* but may also handle questions from users regarding attribute release policy, user privacy, access issues relating to assurance, etc.

All are important in different scenarios, and participants are encouraged to provide at least one of each type.

- At least **one technical contact is REQUIRED** in metadata.
- At least **one administrative contact is REQUIRED** in metadata.
- As part of the roll out of InCommon's Baseline Expectations program, at least one security contact **will be REQUIRED**. You are advised to **add a security contact to your metadata NOW**.

> Contact information should be role-based such as help_desk@example.org rather than individual such as janedoe@example.org.

User Scenarios

Here are a number of hypothetical user scenarios that rely on contact information:

- A user authenticates successfully at the IdP and is subsequently redirected to the SP. The SP software, seeing that the SAML assertion does not contain the desired attributes, links to the IdP's `errorURL` location, if available. In addition to displaying a message to the user, the SP software sends a back-channel message to an institutional administrative contact at the IdP, describing in detail the event that just occurred. The message includes a pointer to the SP's Requested Attributes in metadata.
- A user encounters and reports a technical failure while accessing a service. The SP's support staff determine that the user's IdP is misconfigured (e.g., its clock is off), and informs the technical contact at the IdP.
- A user encounters and reports a technical failure while accessing a service. The SP's support staff determine that the user's environment is at fault, and assists the user in informing the support contact at the IdP.
- A user's assurance status is downgraded due to password compromise. They reset their password, but can't get to their grant submission site. The SP's support staff determine that the users assurance level is too low and assists the person in informing the support contact of the IdP.

Reliable contact information in metadata will enable workflows and scenarios such as those described above.

Technical Details

Here is an example of an appropriate set of `<md:ContactPerson>` elements in metadata:

```
<md:ContactPerson contactType="technical"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:GivenName>Technical Support Team</md:GivenName>
  <md:EmailAddress>mailto:tech_support@example.org</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="administrative"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:GivenName>Office of Administrative Support</md:GivenName>
  <md:EmailAddress>mailto:admin_support@example.org</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="support"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:GivenName>Help Desk</md:GivenName>
  <md:EmailAddress>mailto:help_desk@example.org</md:EmailAddress>
</md:ContactPerson>

<!-- there are two types of security contacts in metadata but both serve
the same purpose -->

<!-- security contact with (legacy) InCommon syntax -->
<md:ContactPerson contactType="other"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     xmlns:icmd="http://id.incommon.org/metadata"

icmd:contactType="http://id.incommon.org/metadata/contactType/security">
  <md:GivenName>IT Security Office</md:GivenName>
  <md:EmailAddress>mailto:security@example.org</md:EmailAddress>
</md:ContactPerson>

<!-- security contact with REFEDS syntax -->
<md:ContactPerson contactType="other"
     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     xmlns:remd="http://refeds.org/metadata"
     remd:contactType="http://refeds.org/metadata/contactType/security">
  <md:GivenName>IT Security Office</md:GivenName>
  <md:EmailAddress>mailto:security@example.org</md:EmailAddress>
</md:ContactPerson>
```

XML Technical Requirements

- Each `<md:EntityDescriptor>` element SHOULD contain at least four contacts, that is, three `<md:ContactPerson>` elements with XML attributes `contactType="support"`, `contactType="technical"`, and `contactType="administrative"`, plus a fourth `<md:ContactPerson>` element with XML attribute `contactType="other"` and an extended XML attribute that indicates the contact is a security contact (see above for example).
  - All entities MUST declare a technical contact (`contactType="technical"`).
  - All entities MUST declare an administrative contact (`contactType="administrative"`).
- Each `<md:ContactPerson>` element MUST contain at least one `<md:EmailAddress>` element.
- If a contact is a non-person (such as a mailing list), the `<md:GivenName>` element MAY contain a title or label, and the `<md:SurName>` element SHOULD be omitted.
- If a contact is a real person (which is NOT RECOMMENDED), the `<md:GivenName>` and `<md:SurName>` elements SHOULD reflect the person's real name.