# SAML V2.0 Metadata Deployment Profile for errorURL Version 1.0 DRAFT

## 1. Introduction

[SAML2Meta] defines an `errorURL` XML attribute within the `<md:EntityDescriptor>` element for use in documenting a URL suitable for referral of an end-user in the event an error. It does not provide sufficient detail on the appropriate use of this value for effective use of the feature, nor does it provide for communication of any details about the error that occurred.

This profile provides a set of conventions around the use of the attribute that extends the usefulness of the feature such that Service Providers can make more effective use of the feature when encountering conditions that can plausibly be remedied by the user's Identity Provider. The profile is compatible with existing uses of the attribute such that Service Providers can easily determine if the profile is supported by the Identity Provider.

It is designed to be as simple as possible, does not expose personal information, and does not constrain either party to any specific error-handling procedures. Service Providers are not required to implement these conventions and can continue to rely on the `errorURL` attribute unmodified.

## 1.1. Notation and 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.

This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`, **Datatype**, `OtherCode`.

The abbreviations IdP and SP are used below to refer to Identity Providers and Service Providers in the sense of their usage within the SAML Browser SSO profile, and similar profiles that may make use of the same metadata constructs.

### 1.1.1. References to SAML 2.0 specification

When referring to elements from the SAML 2.0 core specification [SAML2Core], the following syntax is used:

- `<samlp:ProtocolElement>` - for elements from the SAML 2.0 Protocol namespace.
- `<saml:AssertionElement>` - for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specification [SAML2Meta], the following syntax is used:

- `<md:MetadataElement>`

# 2. Profile Description

## 2.1. Overview

This profile defines a convention for the syntax of the `errorURL` XML attribute when appearing in the `<md:EntityDescriptor>` element of an entity acting in the role of an Identity Provider (IdP). It does not address the use of this attribute in other contexts.

The profile defines a set of reserved “placeholder” values that may be placed into the `errorURL` attribute within an IdP’s metadata instance. These values include one REQUIRED placeholder, and several OPTIONAL placeholders. The presence of the REQUIRED placeholder is to be interpreted as a signal to the Service Provider (SP) that the IdP in fact supports this profile.

Upon this determination, the SP MAY at its discretion produce a link to the IdP’s errorURL by replacing all occurrences of the defined placeholder strings in the URL with information specific to the error event.

The required placeholder may appear anywhere in the URL and its content is URL-safe. The optional placeholders MUST appear (if they appear) in the URL’s query string, and MUST be URL-encoded [STD66].

## 2.2. The required ERRORURL_CODE placeholder

This placeholder is replaced by a string code that uniquely identifies the type of error that occurred. The IdP indicates support for this profile when the literal string “ERRORURL_CODE” is present in the IdP's `errorURL` value.

Only the following values are presently defined as replacements:

- MISSING_ATTRIBUTES
- AUTHENTICATION_FAILURE
- AUTHORIZATION_FAILURE
- OTHER_ERROR

Other values may be defined in future revisions of this profile, but no allowance is made for independent definition of these values.

SPs that do not support this profile obviously would not perform replacement of the placeholders. Therefore, IdPs MUST support use of the `errorURL` with no replacement performed.

IdPs SHOULD support all of the possible codes defined.

## 2.2.1. Code Definitions

### 2.2.1.1. MISSING_ATTRIBUTES

The SP did not receive one or more attributes or values it requires. The SP is obviously unaware of the reason for this.

The user may have to request that the IdP releases more attributes (e.g. using attribute filters, entity categories) or ensure the values are released via consent.

### 2.2.1.2. AUTHENTICATION_FAILURE

The user’s authentication “quality”, or some other provided characteristic (time, location), was insufficient for access. “Quality” maps to varying constructs in different protocols (e.g., to SAML’s `<saml:AuthnContext>` element, and to OIDC’s “acr” claim).

This error most commonly applies to SPs that request specific authentication context(s) from an IdP and this code may be used to refer the user back to the IdP when the request could not be satisfied but the SP has no other recourse.

### 2.2.1.3. AUTHORIZATION_FAILURE

The user is not authorized to access the SP. This may be caused by an inadequate assurance level (when expressed independently of authentication), entitlements, affiliation or missing attribute or value but this code SHOULD NOT be used by SPs that manage authorization locally, over which the IdP would have no control.

### 2.2.1.4. OTHER_ERROR

This error code should only be used when the other defined codes are not appropriate but the SP has evidence that the condition could be remedied by the end-user or IdP organization with relatively minimal further involvement by the SP.

## 2.3. Optional Placeholders

The `errorURL` MAY contain any of the following placeholders, but they MUST appear within the query string of the URL. This requirement allows the URL-encoding rules to be less ambiguous.

### 2.3.1. ERRORURL_TS

An integer timestamp reflecting the number of seconds since Jan 1, 1970 00:00:00 UTC indicating when the error occurred. This refers to the standard Unix epoch representation.

### 2.3.2. ERRORURL_RP

The URL-encoded entityID (or non-SAML equivalent identifier) of the SP.

### 2.3.3. ERRORURL_TID

A URL-encoded transaction ID that the IdP can use as a reference if they contact the SP for more information or follow up. The content is at the discretion of the SP but MUST be limited to 128 unencoded characters and MUST NOT disclose personally-identifying information about the end-user.

### 2.3.4. ERRORURL_CTX

A URL-encoded string containing context-specific information for the IdP. This information is intended to supplement the ERRORURL_CODE value with additional details specific to the defined codes and MUST NOT disclose personally-identifying information about the end-user.

The SP SHOULD confine its use of this field to the following guidelines:

> If ERRORURL_CODE is “MISSING_ATTRIBUTES”, this value if present SHOULD be set to a space-delimited list of the names of the missing attributes and, if appropriate, URIs of the applicable entity categories.

> If ERRORURL_CODE is “AUTHENTICATION_FAILURE”, this value if present SHOULD be set to a space-delimited list of the protocol-specific context values that were requested/required, or a compact string indicating some other reason for the failure (e.g. “time”, “location”).

> If ERRORURL_CODE is “AUTHORIZATION_FAILURE” this value if present SHOULD be set to a concise description of the access policy the user failed to satisfy useful to the IdP or useful in the communication with the SP by the IdP. This profile does not seek to define an actual policy language capable of precisely expressing access policy.

If ERRORURL_CODE is “OTHER_ERROR”, this value if present MAY be set to a concise description expected to be useful to the IdP.

# 3. User Interface Guidelines

When an error occurs, the SP SHOULD present its own error page to the user. If the specific error condition falls into one of the categories for which this profile is appropriate, the SP MAY process the IdP's `errorURL` value from its metadata, as described above, and provide a link to the decorated URL.

Errors for which this profile’s criteria do not apply SHOULD NOT be handled via this mechanism.

# 4. Examples

IdP errorURL:

```
https://idp.example.edu/support/ERRORURL_CODE
```

Processed errorURL:

```
https://idp.example.edu/support/MISSING_ATTRIBUTES
```

IdP errorURL:

```
https://idp.example.edu/error/ERRORURL_CODE.html?ts=ERRORURL_TS&rp=ERRORURL_RP&tid=ERRORURL_TID&ctx=ERRORURL_CTX
```

Processed errorURL:

```
https://idp.example.edu/error/AUTHORIZATION_FAILURE.html?ts=1584423772&rp=https%3A%2F%2Fsp.example.edu&tid=1586458594&ctx=eduPersonAffiliation+containing+student+is+required
```

IdP errorURL:

```
https://support.example.edu/faq/idp-error.php?error=ERRORURL_CODE&timestamp=ERRORURL_TS&service_provider=ERRORURL_RP&transaction_id=ERRORURL_TID&info=ERRORURL_CTX
```

Processed errorURL:

```
https://support.example.edu/faq/idp-
error.php?error=AUTHENTICATION_FAILURE&timestamp=1584423772&service_provider=
https%3A%2F%2Fsp.example.edu&transaction_id=12345&info=https%3A%2F%2Frefeds.o
rg%2Fprofile%2Fmfa
```

# 5. References

- [OIDC] “OpenID Connect Core 1.0 incorporating errata set 1”, https://openid.net/specs/openid-connect-core-1_0.html
- [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.
- [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.
- [STD66] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, https://www.rfc-editor.org/info/rfc3986.
- [SAML2Core] OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
- [SAML2Err] OASIS Approved Errata, SAML Version 2.0 Errata 05, May 2012. http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf.
- [SAML2Meta] OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
- [SAML2Int] Ref TBD