Managing Apache Web Server Environment Variables

Commonly deployed Apache authentication modules exhibit a spectrum of capabilities for setting and managing environment variables with values asserted by an external provider. Some modules allow the deployer to map an asserted value to any environment variable name or label while others offer only limited capabilities such as setting a prefix.

Shibboleth Service Provider

The Shibboleth Service Provider (SP) XML Attribute Extractor, usually configured in the file `attribute-map.xml`, allows the deployer to map a SAML attribute "on the wire" representation such as a URN to any environment variable. For example to map the SAML attribute with on the wire name `urn:oid:2.5.4.42` to the environment variable `ENV_OIS_NAME_GIVEN` one would configure

```
<Attribute name="urn:oid:2.5.4.42" id="ENV_OIS_NAME_GIVEN"/>
```

If it is necessary to map from the on the wire SAML name to a second environment variable one can use a Template Attribute Resolver to add the second mapping:

```
<AttributeResolver type="Template" sources="ENV_OIS_NAME_GIVEN" dest="givenName">
    <Template>$ENV_OIS_NAME_GIVEN</Template>
</AttributeResolver>
```

mod_auth_openidc

The mod_auth_openidc module does not allow the deployer to map claim names to arbitrary environment variables. Only the prefix prepended to the environment variable can be modified (see the explanation for the configuration option OIDCClaimPrefix). For example the standard OIDC `given_name` claim is mapped by default to `OIDC_CLAIM_given_name` and only the prefix `OIDC_CLAIM` can be changed using the OIDCClaimPrefix configuration option, and the change is in effect for all claims.

One may, however, use the mod_rewrite module to write additional environment variables based on those set by mod_auth_openidc. For example to map the given_name claim to OIDC_CLAIM_NAME_GIVEN, and similarly for family_name and middle_name, one may use the configuration

```
RewriteEngine On
RewriteRule .* - [E=REDIRECT_OIDC_CLAIM_NAME_GIVEN:%{HTTP:OIDC_CLAIM_given_name}]
RewriteRule .* - [E=REDIRECT_OIDC_CLAIM_NAME_FAMILY:%{HTTP:OIDC_CLAIM_family_name}]
RewriteRule .* - [E=REDIRECT_OIDC_CLAIM_NAME_MIDDLE:%{HTTP:OIDC_CLAIM_middle_name}]
```

Note, however, that this approach only works in the ".htaccess" context (outside of that context the rewrite rules run before the mod_auth_openidc module has had a chance to populate the CGI environment variables). You may add that configuration to the existing file .../app/webroot/.htaccess, but be aware that it will be overwritten when you next upgrade COmanage.

> ⓘ The REDIRECT_ prefix above is strictly not necessary because the environment variable value is copied from a header, but it is included here for consistency when configuring the Env Source Organizational Identity Source plugin.