# Google OpenID Gateway Attributes

## Google OpenID Gateway Attributes

The current version of the Google OpenID Gateway asserts the following attributes:

- `eduPersonTargetedID`
- `eduPersonPrincipalName`
- `mail`
- `givenName`
- `sn` (surName)

The `mail`, `givenName`, and `sn` attributes always pass through the Gateway as-is. The values of the `eduPersonTargetedID` (`ePTID`) and `eduPersonPrincipalName` (`ePPN`) attributes are computed in one of two ways depending on how the Gateway Manager is configured by the administrator.

### Example

Let's take a specific example. Suppose the Google IdP asserts the following email address:

`user@gmail.com`

The Google OpenID IdP also asserts a persistent, non-reassigned identifier called a *Private Personal Identifier* (PPID). Suppose, for example, the asserted PPID is:

Let's also assume that the entityID of the Google IdP is:

`https://www.google.com/accounts/o8/id`

while the entityID of the Gateway is:

`https://google.gateway.incommon.org`

and the entityID of the end SP is:

`https://fm.incommon.org/sp`

Given the above attribute values and entityIDs, the Gateway Manager can be configured to assert `ePTID` and `ePPN` in one of the following ways.

### Gateway Configuration 1

In this configuration, the attributes asserted by Google are passed through the Gateway as-is. The value of the `ePPN` is identical to the email address:

`ePPN`: `user@gmail.com`

The `ePTID` is set to the following triple:

IdP entityID: `https://www.google.com/accounts/o8/id`
SP entityID: `https://google.gateway.incommon.org`
User ID: `26dn84xIqIvilVMqYCPhE`

### Gateway Configuration 2

In this configuration, the `ePTID` and `ePPN` attributes are computed by the Gateway as follows. The `ePPN` computed by the Gateway is:

`ePPN`: `user+gmail.com@gateway.incommon.org`

The `ePTID` is set to the following triple:

IdP entityID: `https://google.gateway.incommon.org`
SP entityID: `https://fm.incommon.org/sp`
User ID: `opaque_value`

where `opaque_value` is computed by the gateway based on the IdP entityID, the SP entityID, and the persistent value `26dn84xIqIvilVMqYCPhE`.

### Discussion

It is important to note that Google email addresses do not always end in "@gmail.com". In fact, a Google email address can be virtually anything since Google Apps accounts are based on arbitrary DNS domains.

Since `ePPN` is identical to email in Configuration 1, it's not possible to know in advance what `<shibmd: Scope>` elements to assert in Gateway metadata. Thus it's left to the SP administrator to configure the SP software for the scoped `ePPN` attribute. In a few isolated cases, the set of allowed scopes will be known in advance, but in the majority of cases, the set of scopes will not be known and so the SP software will have to be configured to accept all scopes from the Google IdP.

To avoid such a configuration (which defeats the purpose of scoped attributes), in Configuration 2 the Gateway can assert an ePPN with a fixed scope (such as “@gateway.incommon.org”). In this case, no configuration at the SP is necessary since the SP performs normal scoped attribute checking based on a fixed set of <shibmd: Scope> elements in Gateway metadata. In the above example, there will be one such <shibmd: Scope> element in Gateway metadata, namely:

```
<shibmd:Scope regexp="false">gateway.incommon.org</shibmd:Scope>
```

Finally, note that the value of ePTID depends on the configuration as well. The actual User ID depends on who is asserting the attributes. In Configuration 1, the Google IdP is the asserting entity and the ePTID reflects that. OTOH, in Configuration 2, the Gateway is the asserting entity and the ePTID reflects that as well.

Bottom line: A 100% passthru gateway is not possible unless the end SP is willing to accept any ePPN, that is, an ePPN with an arbitrary scope.