Australian Government
Digital Transformation Agency

dta

Relevant Backlog Item:	n/a
Relevant Backlog Item ID:	n/a
Date decided:	
GPAG Decision Page	

Platform Architecture Group - Architectural Design Decision

Responding to Invalid Claims and Scopes

1 Recommendation

The recommendation is for the Exchange to deal with invalid requests in the following ways:

1. Where the request for a claim or scope includes claims or scopes not supported by the Exchange, this should be dealt with as per s5.5 of the OIDC Core
2. Where the request for a claim or scope includes an attribute from the following attribute sets, this should be dealt with as per s5.5 of the OIDC Core:
    a. Core
    b. Validated Email
    c. Validated Mobile Phone Number
    d. Verified Other Names
    e. Business Authorisations
3. Where the request for a claim or scope includes an attribute from one of the following attribute sets, and the Relying Party is not authorised to request that attribute, the Exchange MUST deny the authentication request as per section 4.1.2.1 of [RFC 6749] using the error code access_denied:
    a. Verified Documents (if they are not a relying party approved to access the attributes requested under section 3.6.1 of the *TDIF: 05 – Role Requirements*)
    b. myGov Link (if the relying party is not a myGov member service)

It is also recommended that Relying Parties do not need prior approval to send a request for Business authorisations, and any of the other attribute sets described above in list item 2.

2 Background

The TDIF did not provide any guidance on what to do if an invalid request for a scope or claim was received by the Exchange. Services Australia requested guidance on this matter in an email dated 29/01/2020.

3 Recommended Option

3.1 Design

The recommendation is for the Exchange to deal with invalid requests in the following ways:

1. Where the request for a claim or scope includes claims or scopes not supported by the Exchange, this should be dealt with as per s5.5 of the OIDC Core

Australian Government
Digital Transformation Agency

dta

2. Where the request for a claim or scope includes an attribute from the following attribute sets, this should be dealt with as per s5.5 of the OIDC Core, regardless of Relying Party:
    a. Core
    b. Validated Email
    c. Validated Mobile Phone Number
    d. Verified Other Names
    e. Business Authorisations
3. Where the request for a claim or scope includes an attribute from one of the following attribute sets, and the Relying Party is not authorised to request that attribute, the Exchange MUST deny the authentication request as per section 4.1.2.1 of [RFC 6749] using the error code access_denied:
    a. Verified Documents (if they are not a relying party approved to access the attributes requested under section 3.6.1 of the *TDIF: 05 – Role Requirements*)
    b. myGov Link (if the relying party is not a myGov member service)

3.1.1 TDIF requirements

3.1.1.1 TDIF: 06B – OpenID Connect 1.0 Profile

Insert the following section in the Exchange to Relying Party Profile:

Responding to invalid claims

TDIF Req: OIDC-02-07-13; **Updated**: Mar-19; **Applicability**: X
If the Applicant receives a request for a scope or claim for which it can not return a value, it MUST ignore the scopes or claims for which a value can not be returned, subject to TDIF Req: OIDC-02-07-14. See s5.5 of the **[OpenID.Core]** for further detail.

TDIF Req: OIDC-02-07-14; **Updated**: Mar-19; **Applicability**: X
The Applicant MUST deny an authentication request as per section 4.1.2.1 of **[RFC 6749]** from a Relying Party using the error code access_denied if the Relying Party requests a claim or scope it is not authorised to request, as defined in section 2.3 of the **[TDIF.Attr].**

3.1.1.2 TDIF: Attribute Profile

The attribute Profile to be updated with the following table, in section 2.3 of the Attribute Profile.

Table 1: Trust Framework attribute sharing policies.

Attribute Set	Relying Parties authorized to request
Core	All
Validated Email	All
Validated Mobile Phone Number	All
Verified Other Names	All
Verified Documents	Relying Parties approved to request Verified documents as restricted attributes under section 3.6.1 of the *TDIF: 05 Role Requirements*.
Common	Not required.
myGov Link	myGov Member Services
Business Authorisations	All

Australian Government
Digital Transformation Agency

dta

3.2 Impacts

Set out the impacts that implementing this decision will have.

3.2.1 Impact to IDPs

No implementation impact.

3.2.2 Impact to Exchange

Requires exchange to be able to send an error response for the above invalid claims.

3.2.3 Impact to Relying Parties

Will receive an error code if they make a request for certain attributes they are not authorised to receive.

3.2.4 Impact on TDIF

Incorporate the Recommended design into both the *TDIF: 06B – OpenID Connect 1.0 Profile* and the *TDIF: Attribute Profile*.

4 Future Work

4.1 DTA

The DTA needs to incorporate this decision into the TDIF.

4.2 Services Australia

Services Australia will need to build out the ability for the Exchange to reject these requests by March 2021, when they are accredited against TDIF release 4. This can also be delivered earlier if desired by Services Australia.

5 Other Documents Relevant

What other documents are relevant to this decision and where can these be found? Include links if possible.

6 Consultation

Members of PAG present at following PAG meetings, as recorded in the minutes:

- 13.02.20
- 20.02.20