# Data Standards Body
# Technical Working Group

Decision 325 – Audience claim for Data Holder client authentication of Data Recipients

*Contact: Mark Verstege*
*Publish Date: 3rd December 2020*
Decision Approved By Chairman: *8th December 2020*

## Context

The "audience" claim (aud) is a value provided in the client authentication assertion JWT sent by the data recipient when calling secured end points hosted by the data holder that are not protected resources covered by consumer consent. Typically, these are the oAuth end points for authorisation and token management. The audience claim is intended to be a value that identifies the authorisation server as the intended audience of the client's authentication assertion.

Prior to version 1.4.0 of the Consumer Data Standards, the audience claim was defined as the "URL of the end point being invoked". Within Banking Maintenance Iteration 3, a change request was raised by the community requesting this be updated to support data holder implementations and the community agreed on the audience claim being defined as "The Token Endpoint URL". This change was adopted without any future dated obligations identified.

This change, having been agreed by the community, was approved by the Data Standards Chair and adopted in v1.4.0 of the Consumer Data Standards. Consequently, any participant not supporting the audience claim as per v1.4.0 would be non-compliant with the Consumer Data Standards.

Since consultation and the approval of the decision, two factors have come to light which make the change to this statement required

1. Impacted participants continue to implement the audience claim as per v1.3.1 of the Consumer Data Standards.
2. The upstream standards have been further qualified to ensure there is clear interpretation and implementation consistency.

This decision record reflects consultation on those proposed changes and an agreed transition path.

### Feedback received

Decision Proposal 325 was raised as an urgent change request and consulted over a two-week period. Feedback received by all participants supported the change and the transition period.

## Decision To Be Made

Decide changes required to support the target state audience claim and describe the transition to target state for ADRs and DHs including obligation dates.

# Decision For Approval

The following changes to the standards are proposed:

*Recommendation 1.* Qualify the claims in the JWT relate to the client authentication JWT.
*Recommendation 2.* Change the audience claim description to align to upstream standards.
*Recommendation 3.* Require Data Recipients to continue to set the audience claim value as "the URL of the end point being invoked" until the agreed future dated obligation.
*Recommendation 4.* Set a future dated obligation of 30-March-2021 for DH support of the updated audience validation requirements

## Change 1 – Qualify the claims in the JWT relate to the client authentication JWT

This change is makes it explicit in the Consumer Data Standards that this definition applies only to the client authentication assertion between the ADR and DH. The audience claim is a required claim in other JWTs: its value should continue to be implemented as intended by the relevant upstream standards.

This change was supported by participants.

## Change 2 – Change the audience claim description to align to upstream standards

The audience claim will be updated such that Data Holders must support any single-value string or list (array) of the Issuer Identifier, Token Endpoint URL or the URL of the endpoint being invoked as valid audience values for the client authentication assertion JWT.

The proposed change incorporates clear implementation guidance for ADRs and DHs in the current state as well as the required target state. One reason for this further change is based on recognition within the upstream standards that the interpretation of the related upstream standards created ambiguity.

This change was supported by participants.

## Change 3 – Require Data Recipients to continue to set the audience claim value as "the URL of the end point being invoked" until the agreed future dated obligation

Change 2, in alignment with the upstream standards, provides ADRs with more permissive flexibility as to the audience claim value they set. Until Data Holders can transition to support this flexibility, a transition period is required for Data Holders. Thus, ADRs need to continue to set the audience value as *"the URL of the endpoint being invoked"* up until the future dated obligation.

This ensures that there is no breaking change for ADRs in both current state or future state. It is noted that the updated description, as aligned to the upstream standards, recommends that the client SHOULD set the audience to be the Issuer Identifier. Transition to the use of Issuer Identifier would be within the timeframes of each ADR but would not impact successful interoperability once all DHs support these changes.

This change was supported by participants.

## Change 4 – Set a future dated obligation of 30-March-2021 for DH support of the updated audience validation requirements

To support the transition for Data Holder implementation, a future dated obligation is necessary. So as not to impact, or be impacted by, February obligations, it is proposed that an obligation date at the end of March is set whereby all Data Holders must support the updated requirements.

Further to this, the obligation date has been chosen to be before second tier bank's consumer data sharing obligation date to provide them with implementation certainty without a need to make an immediate change after go-live.

**Up until 31-March-2021, ADRs must set the audience to the URL of the endpoint being invoked for client authentication. From 31-March-2021, ADRs may align to the target state.**

This change will be included in the future dated obligations table within the consumer data standards.

This change was supported by participants.

# Changes to current standards

## Client Authentication

### Data Recipients calling Data Holders

The text regarding the list of claims for the assertion will be updated to be clear that the audience claim and other claims for the JWT pertain to client authentication.

- For the client authentication assertion, the [JWT] represents an assertion that MUST include the following claims:

The audience claim description will be updated as follows:

> *aud: The aud (audience) Claim. Identifies the recipients that the JWT is intended for.*
>
> *The URL of the endpoint being invoked. Until March 31st, 2021, data recipients MUST continue to send as a single value string the URL of the endpoint being invoked.*
>
> *After March 30th, 2021, Data Holders MUST support:*
>
> *The issuer identifier URL of the authorisation server according to [RFC8414] SHOULD be used as the value of the audience. In order to facilitate interoperability, the authorisation server MUST accept its Issuer Identifier, Token Endpoint URL, or the URI of the endpoint being invoked as values that identify it as an intended audience.*

**Note:** Whilst a client *may* be able to send a list of values for the audience claim it is **recommended** that clients only send a single-value string. Per [RFC8414] this SHOULD be the Issuer Identifier URL of the authorisation server.

## Implementation Considerations

These changes give rise to implementation considerations for both ADRs and Data Holders. Primarily, the approach with this change is to:

1. Provide implementation consistency for all participants during the transition stage
2. Avoid impact to ADRs and allow their solutions to continue to work as-is
3. Shift to a target state that allows Data Holders to reduce customisation in their Identity & Access Management (IAM) solution to adopt the upstream standards

As per RFC8414, ADRs are recommended to set the audience claim value to be the Issuer Identifier URL. There is no strict obligation or requirement in the Consumer Data Standards to do so because the target state will support ADRs in their current state. This means any transition plans for ADRs are at their discretion provided they happen *after* the future dated obligation set out in Change 4.

Data Holders will have an implementation impact, but the net result will be a solution that allows compliant IAM vendors to provide a configurable solution rather than customer change. Recognising that Data Holders are currently implementing validation of the audience claim against the "URL of the endpoint being invoked" some effort, although minor, is required to support validation of the Issuer Identifier and Token Endpoint URL as well.

Adopting a future dated obligation that gives sufficient time to Data Holders such that it does not impact near-term obligations (specifically November 2020 builds), provides an acceptable timeframe to comply.

Likewise, the target state means that ADRs are supported with a working solution that is interoperable across all current and future Data Holders.