Consumer Data Standards Information Security Workshop

www.data61.csiro.au

Introduction

Luke Popplewell
Engineer and Architect
Week 4 at Data61 and the Consumer Data Standards Team
Most Recent Project:
- Technical Lead for the GovPass Exchange at Department of Human Services

www.data61.csiro.au

The Journey so far..

InfoSec Security Proposals Decisions

- Decision Proposal 023 – Initial Direction for Security Profile
  - Adopt FAPI R/W Profile with relevant local changes
- Decision Proposal 035 – Customer Authentication Flow
  - Hybrid Flow and Client Initiated Backchannel Authentication (CIBA)
- Decision Proposal 033 – Use of TLS-MTLS
  - TLS >= 1.2, FAPI compliant ciphers, MTLS for B2B comms and token binding, private key and MTLS for Client authentication
- Decision Proposal 036 – OIDC userinfo support
  - Scopes: openid and profile, Claims: name, family_name, given_name

The Journey Ahead (Part 1)…

- Publish CDR InfoSec Profile 0.1.0 Working Draft by Christmas
- Create **ConsumerDataStandards/infosec** GitHub repository
- Publish 0.0.1 version of the CDR InfoSec Profile early next week
  - Aiming for Wed 21 Nov
- Run an Agile-like delivery process
  - Sprint 1 : Monday 19th Nov - Tue 27th Nov
  - Sprint 2: Wed 28th Nov - Fri 7th Dec
  - Sprint 3: Mon 10th Dec - Tue 18th Dec (Feedback closed)
  - Sprint 4: Wed 19th Dec…

The Journey Ahead (Part 2)…

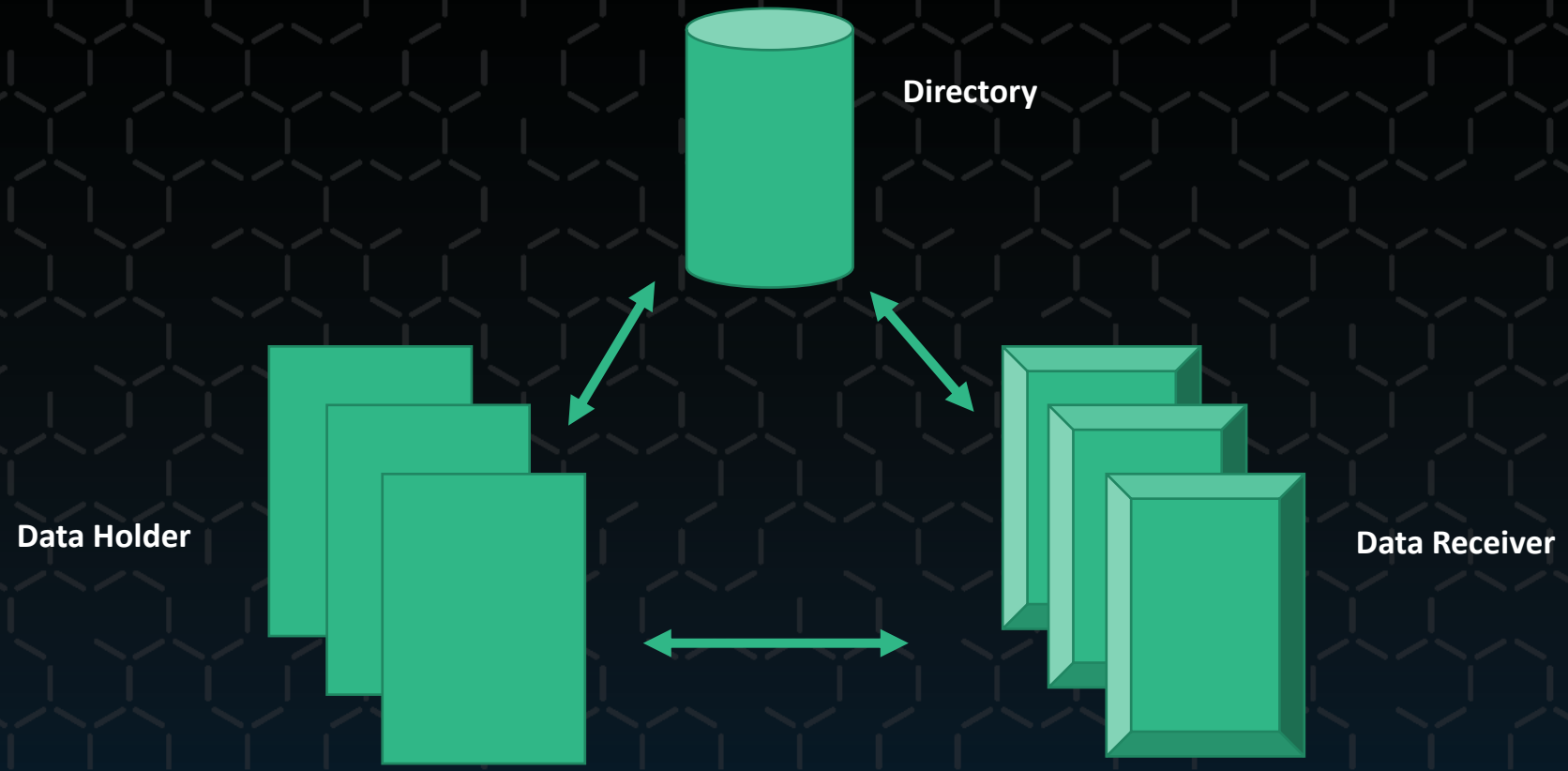
- Sprint 1: Finalise and tag 0.0.1
- Sprint 2: Finalise and tag 0.0.2
- Sprint 3: Finalise and tag 0.0.3
- Sprint 4: Publish 0.1.0
- Iterate over the profile
- Adopt a continuous-delivery type approach – publish often

The Journey Ahead (Part 3)…

- Please contribute early
  - There should be no surprises by Sprint 2
- Discussions in private GitHub repositories for sensitive topics?
  - Group level and individual
- Issues created and assigned to Sprints
- Workshop in Melbourne in early December
- Galexia to facilitate, provide technical review capability, incorporate feedback
  - Peter van Dijk - Consultant
  - Chris Connolloy - Consultant
  - Richard Weatherley - Technical Advisor

Technical Deep Dive

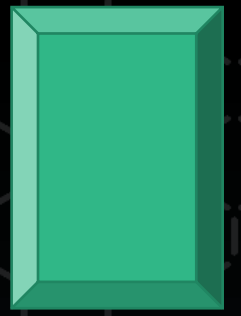
The Consumer Data Right Federation



Data Holders

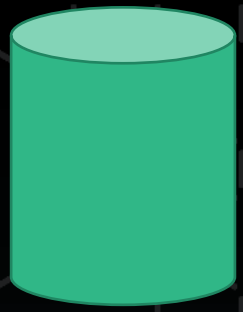
- Are OpenID Providers or Issuers
  - Issues ID Tokens, Access Tokens, Refresh Tokens
- Authenticate End Users (Resource Owners) with High Confidence (LoA 3)
- Establish User Authorisation
- Authorise access to Resource Servers
- Will host Resource Servers that implement the CDR Application Programming Interfaces (APIs) for their industry segment
- Example: Banks

Data Receivers



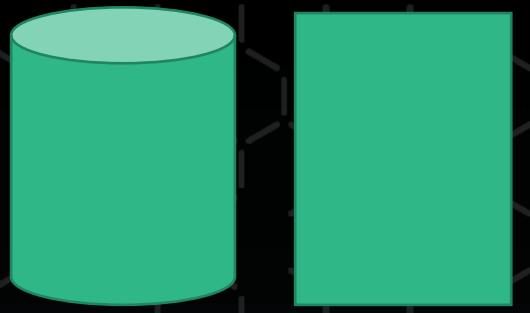
- Are OpenID Clients or Relying Parties (RPs)
  - Consume ID Tokens, Access Tokens, Refresh Tokens
- Invoke the CDR APIs hosted by Data Holder Resource Servers in order to receive Consumer Data
- Offer value-adding services to Consumers
- Example: Fintechs

The Directory



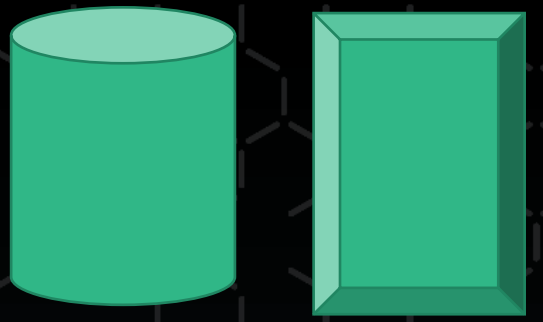
- Managed by the ACCC
  - Updated as part of an Accreditation process
- Also being referred to as the Registry and Address Book
- Will Support Public Key Infrastructure (PKI)
  - CA Root Certificate, Revocation lists, etc
- Point of Discovery
  - Data Receiver Metadata
  - Data Holder Metadata (references OIDC Discovery Endpoints)

Data Holder OIDP



- Data Holder OIDC Discovery information will include:
  - A Data Holder hosts Issuer / OpenID Provider
  - Issuer ID (URI)
  - Endpoint URLs: Token, Authorisation, JWKS, UserInfo, Revocation, Introspection, CIBA Authorisation
  - Algorithms: Request Object signing algorithms, ID Token signing/encryption algorithms
  - Client Authentication methods: private key JWT, Mutual Authentication TLS
  - Access Token constraining method: MTLS
  - Response Types: **`code id_token`**
  - Grant Types: **`authorisation_code`**
  - Subject Types: **`pairwise`**
  - Supported claims and scopes

Data Receiver OIDC Client



- Data Receiver Registration metadata will include:
  - A Data Receiver hosts Client / Relying Party
  - Client ID
  - Endpoint URLs: JWKS, CIBA Notification
  - Algorithms: Request Object signing algorithms, ID Token signing/encryption algorithms
  - Client Authentication methods: private key JWT or Mutual Authentication TLS
  - Mutual Authentication TLS Distinguished Name (DN)
  - Allowed scopes

JSON Web Key Sets – JWKS

- A JSON Web Key (JWK) is a structure that represents a cryptographic key in JSON format.
- A JWKS is a set of JWK(s)
- Each key in the set has an advertised role function (encryption or signing) and supports predefined JWK algorithms
- Each key has an ID
- A JWT signed with a JWK should include the ID of of key with which it was signed / encrypted
- Published by reference (URI) or by value in the Directory
- Supports rolling of keys and can include a certificate chain (`x5c` parameter)

CSIRO DATA 61

Authentication Flows

- Discussed in Proposal 035
- Hybrid Flow
  - Redirection flow
  - Features aspects of both an implicit flow and authorisation code flow
- Client Initiated Backchannel Authentication (CIBA)
  - Authentication by means of out-band mechanisms

CSIRO DATA 61

Authentication Flows - Hybrid

- The user agent (browser) is redirected from the Data Receiver's web application to Data Holder’s Authorisation Endpoint
  - The Data Receiver includes , as part of the request, a signed Request Object with essential/voluntary claims and details of the request
- Post successful authentication the user agent is redirected to a predefined redirect URI for the Data Receiver with the ID Token and Authorisation Code
  - ID Token is signed and encrypted but must not carry Personally Identifiable Information (PII) claims
  - ID Token is a detached signature - carries hash of state and authorisation code
- Authorisation Code is POSTed to Token Endpoint – Backchannel
  - Protected by Client Authentication – Data Receiver authentication
- Token Endpoint returns Access Token, Refresh Token and ID Token
  - ID Token returned from Token Endpoint may carry PII claims which have been consented to

CSIRO DATA 61

Authentication Flows - CIBA

- Optional for a Data Holder to support
- The Data Receiver sends an authentication request to the backchannel Authorisation endpoint
  - The Data Receiver includes , as part of the request, a signed Request Object with essential/voluntary claims and details of the request.
  - The endpoint is protected and requires Client Authentication
  - Receiver must send a Login Hint.
- The Data Receiver must have registered a Notification endpoint (Polling not supported)
- The Data Holder authenticates end user in the background
- Result of authentication and tokens are sent to the Notification Endpoint

CSIRO DATA 61

ID Token

- The ID Token is signed and encrypted by the Data Holder and contains a number of assertions about the end user and the authentication instance including:
  - `sub`: Subject
  - `acr`: Authentication Context Class Reference
  - amr: Authentication Methods Reference
  - `iss`: The Issuer Identifier for the Data Holder
  - `aud`: Audience. Client ID for the Data Receiver
  - `nbf`, `exp`, `iat`, `nonce`, `auth_time` etc
  - `c_hash` and `s_hash`: Hash of Authorisation Code and Data Receiver State
- The ID Token may also carry PII claims about the authenticated user
  - The Data Holder can request these through the Request object claims field.

CSIRO DATA 61

Access Token

- An Access Token is included in the authorisation header as a bearer token for access to Data Holder Resource Server APIs
- It is short-lived and will expire in less that 60 mins
- It is bound to the certificate to which it was issued (Holder of Key with MTLS)
- A new Access Token can be can issued through the Token Endpoint through the use of a Refresh Token
- Profile may support by value or by reference tokens - TBD

CSIRO DATA 61

Refresh Token

- A Refresh Token is returned from the Token Endpoint with the Access Token
- It is long-lived and will expire after a number of months
- It it is sent to the Token Endpoint in order for the Data Receiver to be issued a new Access Token

CSIRO DATA 61

Transaction Security

- All Endpoints must be secured with TLS >= 1.2 and the following ciphers are supported (as outlined in the FAPI-RW profile):
  - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  - Authorisation endpoint may use other ciphers
  - Covered in Proposal 033
- Holder of Key (HOK) mechanisms for B2B calls:
  - Access Tokens and Refresh Tokens are bound to the Client Certificate Presented during the TLS handshake
  - Trust Store: Server and Client Certificates must be issued by the CDR Certificate Authority (CA) in order to trust to be established
  - MTLS not required for Authorisation (non CIBA) and JWKS endpoints

Client Authentication

- 2 methods are supported as outlined in proposal 033
- Only Confidential Clients will be supported.
  - Therefore, Public and Dynamically-Registered clients are not supported
- Private Key JWT Authentication
  - A JWT signed by the Data Receiver is POSTed to the Token or CIBA Authorisation Endpoint
  - JWT Contains the claims:
    - `iss` and `sub`: The Data Receiver Client Id
    - `aud`: The Data Holder Token endpoint URL
    - `jti`: JSON Token Identifier which should be unique
    - `iat`, exp
- TLS Client Authentication
  - The Distinguished Name (DN) on the presented Client Certificate is used to identify Data Receiver

CSIRO DATA 61

Scopes and Claims

- The profile won't cover industry-specific scopes like bank_account.
- Outlined in Proposal 036
- `openid` scope is mandatory
- `profile` scope will be supported
- Personally Identifiable Information (PII) Claims:
  - given_name
  - famiy_name
- Will be available in ID Token and/or UserInfo Endpoint

CSIRO DATA 61

Endpoints (Part 1)

- JWKS
  - Data Holders and optionally Data Receivers must implement a JWKS endpoint
- UserInfo
  - For accessing PII claims, Data Holders must implement a UserInfo endpoint
  - Invoked with Access Token and enforces Token Binding/MTLS
  - Must contain requested claims and those related to `profile` scope
  - Response include `sub` claim which must match `sub` in ID Token
  - Response includes `updated_at`
  - The profile won't cover industry-specific scopes like bank_account.
- Token
  - Data Holder must implement a Token Endpoint which is protected with Client Authentication
  - Secured with MTLS

CSIRO DATA 61

Endpoints (Part 2)

- Introspection
  - Data Holders must implements an Introspection Endpoint to allow Resources Servers to gather metadata on Access and Refresh Tokens in order to service a request
  - Token scopes, validity, expiry and Token Binding metadata is returned.
- Revocation
  - Data Holders must implement a Revocation endpoint to allow Data Receivers to invalidate their tokens.
  - Allows Data Holders to clean up their associated metadata

CSIRO DATA 61

Endpoints (Part 2)

- Introspection
  - Data Holders must implements an Introspection Endpoint to allow Resources Servers to gather metadata on Access and Refresh Tokens in order to service a request
  - Token scopes, validity, expiry and Token Binding metadata is returned.
- Revocation
  - Data Holders must implement a Revocation endpoint to allow Data Receivers to invalidate their tokens.
  - Allows Data Holders to clean up their associated metadata

CSIRO DATA 61

Level of Access - LoA

- Data Holder must establish an LoA of 3 which demonstrates there is a high-level of confidence in the claimed or asserted identity of the end user

CSIRO DATA 61

Subject Types and User Identifiers

- The identifier for an authenticated end-user is passed in the sub claim. The Data Holder must create a pairwise anonymous identifier and this value must be unique per Data Receiver (Client).
- Different Data Receivers should not be able to link to the same person.
- A new identifier may also be generated on a per scenario basis. For example, a user authenticating as a business delegate should receiver a different anonymous identifier that when that user is consenting to access their personal account.

CSIRO DATA 61

The End

Thanks for Attending

Questions?

GitHub: https://github.com/ConsumerDataStandardsAustralia