Consumer Data Standards Information Security Workshop 2

06/12/2018 Melbourne

www.data61.csiro.au

Introduction

Luke Popplewell

(Acting) Information Security Lead at Consumer Data Standards Data61

The Journey so far … (Part 1)

InfoSec Proposal up till 16/11/2018

- 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 so far … (Part 2)

- InfoSec Security Workshop held on 16/11/2018 in Sydney
- InfoSec repository created at https://github.com/ConsumerDataStandardsAustralia/infosec
- Publish 0.0.1 of Profile on 23/11/2018
  - Tagged as 0.0.1 on 30/1/2018
- First news letter published on Fri 30/11/2018
- Now in Sprint 2 working on version 0.0.2 of the InfoSec profile

Sprints

- 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: Mon 19th Dec …

Debrief

- InfoSec Security Workshop debrief to be held remotely at 3pm on Mon 10th on WebEx

GitHub Issue Types

- **feature:** This is a piece of work that is to be carried out. It represents a change that is being made or is going to be made to the profile. It will be moved into a *sprint* when it is being actioned.
- **question**: This is a question that the CDS team is posing back to the community and thus open for discussion.
- **bug**: This relates to a bug in the profile that needs to be fixed. For example, a spelling mistake.
- **proposal**: This represents an intent to change the profile based on feedback or requirements and is open for discussion.

Current Issues

- **features**
  - #4 Add Level of Assurance (LoA) 2
  - #10 Add Vectors of Trust (VoT)
  - #11 Refine Introspection Endpoint
  - #12 Consent and Multi-dimensional Scopes
  - #13 Clarify Request Content
  - #14 Change JWKS KeyID to x5t – Matches OBIE
- **questions**
  - #1 Does the FAPI cipher list require restriction?
  - #8 Is SMS a valid LoA 3?
- **proposals**
  - #7 Client Authentication: Private Key Support Only

Technical Discussion

Levels Of Assurance (LoAs)
AND
Vectors of Trust (VoTs)

Levels of Assurance

- Describes the **degree** of *confidence* in the processes leading up to and including an authentication.

FAPI and LoAs

- FAPI References **[X.1254]**
  - **Entity authentication assurance framework**
  - **https://www.itu.int/rec/T-REC-X.1254**
- For **READ**: *At Least an LoA of 2 must be achieved*
  - At LoA2, there is some confidence in the claimed or asserted identity of the entity. This LoA is used when moderate risk is associated with erroneous authentication. Single-factor authentication is acceptable.
- For **WRITE**: *At Least an LoA of 3 must be achieved*
  - At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor authentication.

Authentication refresher

- Plain language description
  - Making sure that a person or thing is the same person or thing that you saw last time (which is different from them being who they say they are!)
- 3 Traditional factors
  - Something you know
  - Something you have
  - Something you are

Scenario…..

- Imagine a whistle blower
- Requires Very High Confidence
  - We need to ensure that the re-authentication is from the same entity and not a malicious actor
- We need LoA 4 which gives us
  - Strong cryptographic authentication
  - Strong man in the middle attack resistance
  - No bearer tokens
  - In-Person Identity
    - This is a problem for our whistleblower!

Vectors of Trusts (VoTs)

- Internet Engineering Task Force (IETF) https://tools.ietf.org/html/draft-richer-vectors-of-trust-14
- A Vector is an item composed of multiple independent values
- A VoT is composable and extensible
- A VoT contains orthogonal component categories that overlap as little as possible
  - **P - Identity Proofing**: Knowing the identity of the person you are interacting with.
  - **C - Method of authentication**: Authenticators like 2FA.
  - **A - Assertion Presentation:** How is the assertion provided.
  - **M - Primary Credential Management**: How strictly credential rotation and issuance revocation happens at the identity provider.

Example

- *ScoMo* authenticates with:
  - A Password (Cc)
  - A known device (Cb)
  - Hardware cryptographic key (Cf)
  - He is known to the Identity Provider (P3)
    - A biometric Facilitates non-repudiation
  - Token delivered to browser (Ab)
    - Won’t be allowed to access Top Secret material now!
  - Represented as: `CbCcCfP3Ab`

Aligning VoTs and LoAs … (Part 1)

- The CDR Profile (at this stage) has not covering Identity Proofing, Assertion Presentation or Credential Management
- National Institute of Standards and Technology (NIST)
  - https://pages.nist.gov/800-63-3/
  - SP 800-63B - Authentication & Lifecycle Management
  - Authenticator Assurance Level (AAL)
- Digital Transformation Agency (DTA) :
  - https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework
  - Credential Rating (CR) aligns with NIST 800 463 and AALs

Aligning VoTs and LoAs … (Part 2)

- Under this profile…
  - LoA 2 = `urn:csd.au:cdr:2` = CL1 (DTA TDIF) = AAL1 (NIST 800 463)
  - LoA 3 = `urn:csd.au:cdr:3` = CL2 (DTA TDIF) = AAL2 (NIST 800 463)
- *vot* claim: Shipped in ID Token
- CL1 or CL2
- In future may look like `CL1IP2A1` etc
  - IP = Identity Proofing

Consent Framework

What is Consent?

- Express or implied approval, or voluntary agreement, compliance, or permission for some act, decision, or purpose. Consent obtained through coercion, fraud, or undue influence is invalid.
- http://www.businessdictionary.com/definition/consent.html

Requirements For Consent?

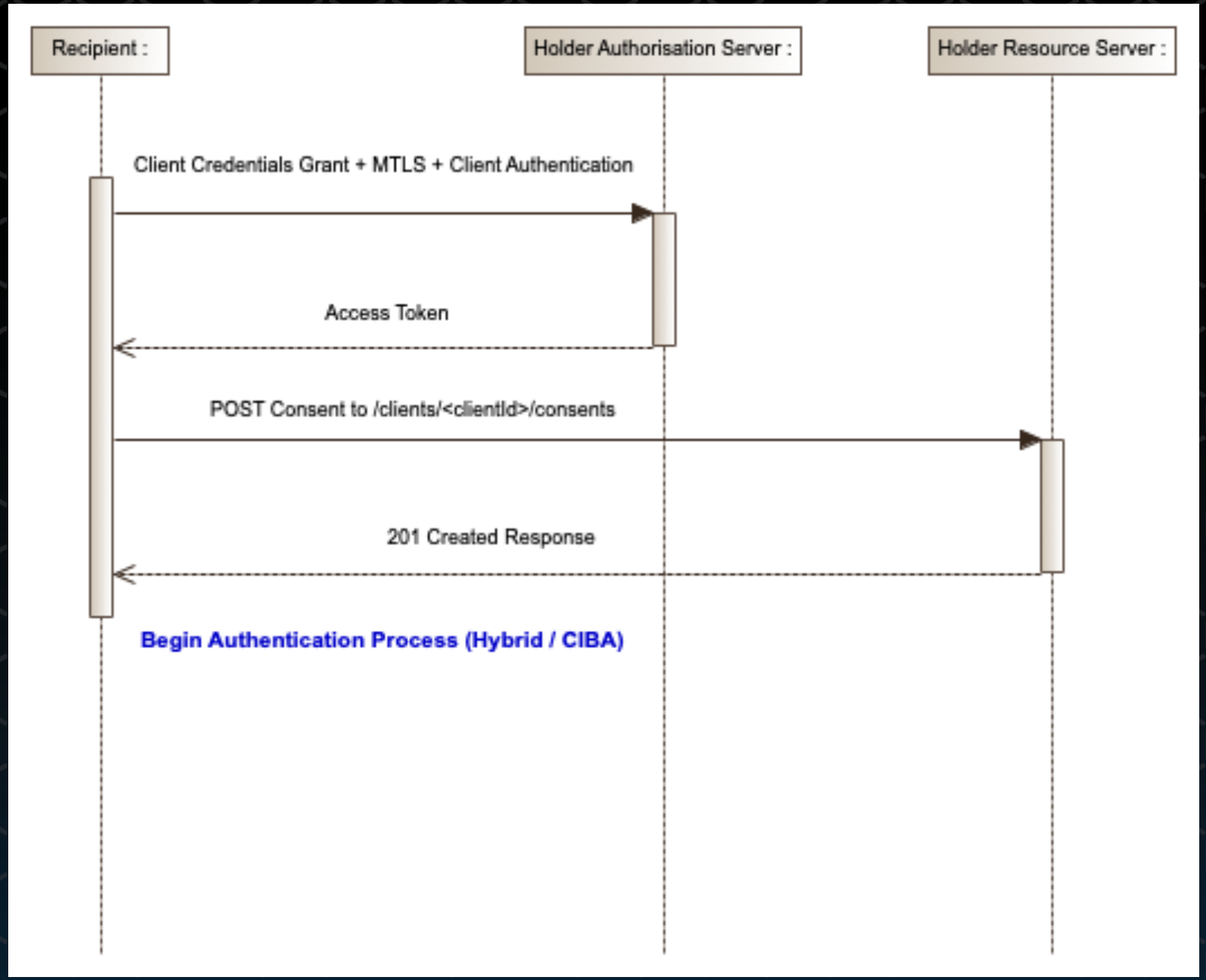
- Consent is enduring
- Consent needs to be fine-grained
- Consent may incorporate multiple dimensions
  - Time Dimensions
    - How long does it last for?
    - Does it last indefinitely?
  - Data Dimensions
    - What data ranges does it apply to?
- Consent can be revoked / updated / deleted
- Consent must carry a status
- Consent can be applied to one or more authorisations

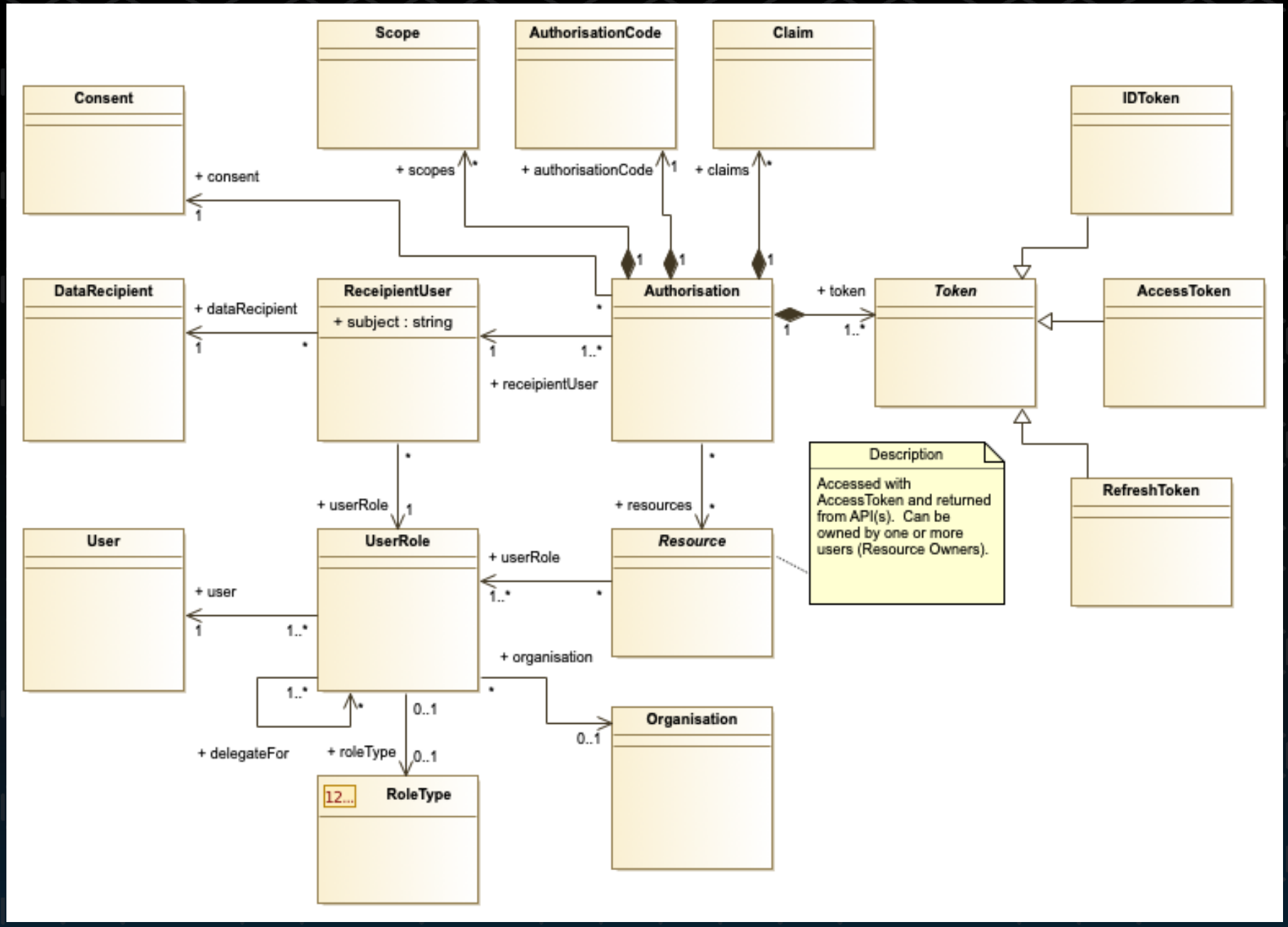
A Consent framework? … (Part 1)

- Data Recipients capture indicative consumer consent (an instance of Consent)
- Data Holders expose an API which allows Recipients to
  - Create a Consent (POST)
  - Retrieve a Consent (GET)
  - Remove Consent (DELETE)
- Each Consent instance is assigned a unique consent ID (for the Recipient-Holder relationship)
- A Consent instance carries
  - Access dimensions
    - Time /Data Ranges
  - Fine Grained Permissions
    - Permission allow Read / Write of Data Elements within payloads

A Consent framework? … (Part 2)

- Consent created by Recipient prior to commencement of Authentication (CIBA or Hybrid)
- Consent is carried as a variable scope in the Authentication Request
  - `urn:cds.au:cdr:12334345`
- The Consent instance is authorised and updated at the Holder
- The Consent is bound to an authorisation (one or more)


Recipient :
Holder Authorisation Server :
Holder Resource Server :
Client Credentials Grant + MTLS + Client Authentication
Access Token
POST Consent to /clients/<clientId>/consents
201 Created Response
Begin Authentication Process (Hybrid / CIBA)


Scope
AuthorisationCode
Claim
Consent
IDToken
+ consent
+ scopes
+ authorisationCode
+ claims
1
*
DataRecipient
ReceipientUser
+ subject : string
Authorisation
+ token
Token
AccessToken
+ dataRecipient
+ receipientUser
Description
Accessed with AccessToken and returned from API(s). Can be owned by one or more users (Resource Owners).
RefreshToken
+ userRole
+ resources
User
UserRole
Resource
+ user
+ organisation
+ delegateFor
+ roleType
Organisation
12...
RoleType
0..1
1..*

The End

Thanks for Attending

- What's next?
  - News letter tomorrow Friday 7th Dec
    - Please subscribe
  - Debrief on Monday 10th Dec @ 3 pm
- Questions?

GitHub:
https://github.com/ConsumerDataStandardsAustralia

- Please add yourself as watcher
- Profile will be updated over the next week to incorporate outstanding features
- **data61cds@galexia.com**