Privacy Consent on FHIR (PCF)

https://profiles.ihe.net/ITI/PCF

John Moehrke (By-Light)
- IHE IT-Infrastructure co-chair
- HL7 Security WG co-chair

Agenda

- Foundation of Privacy Policies and Choices → Appendix P
- Capturing Consent – the output of the Consent Ceremony
- Consent Patterns supported: Basic, Intermediate, Advanced
- Authorization Decisions based on Consents
- Enforcing Authorization Decisions

Use-Cases – Not exhaustive list

- Consent for use within an Organization
- Centralized Consent authorizing disclosure
- Consent authorizing data request
- Basic Consent – Implied Consent vs Explicit Consent
- Intermediate Consent
  - By data date, data Id, data author, episode/encounter, PurposeOfUse
- Advanced Consent
  - Data Segmentation for Privacy (DS4P)– Data Tagging to sensitivity categories

IHE – Integrating the Healthcare Enterprise

- Interoperability Standards Organization that profiles the best standard for a given use-case
- IHE Profiles are Implementation Guides
- Volume 1 – Defines the use-cases and how Actors use
  - Transactions / Content
- Volume 2 – Defines detailed Interop constraints on Transaction
- Volume 3 – Defines detailed Interop on reusable Content modules
- Volume 4 – National Extensions

https://profiles.ihe.net

Appendix P: Privacy Policies

Informative and Foundational

Privacy Policies

- Policies – details of how data will be handled
  - When No Consent is on file
  - When Consent is on file
  - When conflicting consents are on file
- RBAC vs ABAC – The normal business rules are foundation of Privacy Consent
- Break-Glass – Who is authorized, and what will happen if used?
- Audit Logging
  - Policies around reviewing by Privacy office
  - Access by Patient to all uses of their data

Security Labeling Service – Stigmatizing

- E.g. Alcohol abuse, Drug abuse, Mental Health, Sexual assault, HIV
- Single clinical codes match (LOINC, SNOMED, etc) are not enough
  - ValueSets exist
  - All ValueSets would need review and adjustment regularly
- Complexity of combinatorics – set of 3 drugs is a strong indicator of HIV. Set of 2 drugs is a strong indicator of abortion.
- “Normal” confidentiality → statistically most of health data
- “Restricted” confidentiality → more sensitive so should be more restricted
- Architectures: During Publication vs During Use

Volume 1: Use-Case analysis

Use-Case

Part 1: Profiling of Consent

- Capturing the facts of a Privacy Consent Ceremony
- Supporting maintaining Privacy Consent
- Supporting changing Privacy Consent

Part 2: Access Control

- Enforcing the Privacy Consent during activities
- Integrated into typical oAuth flow, that protects business rules (RBAC)
- Adds protection of Privacy according to Privacy Consents on file

Actors / Transactions

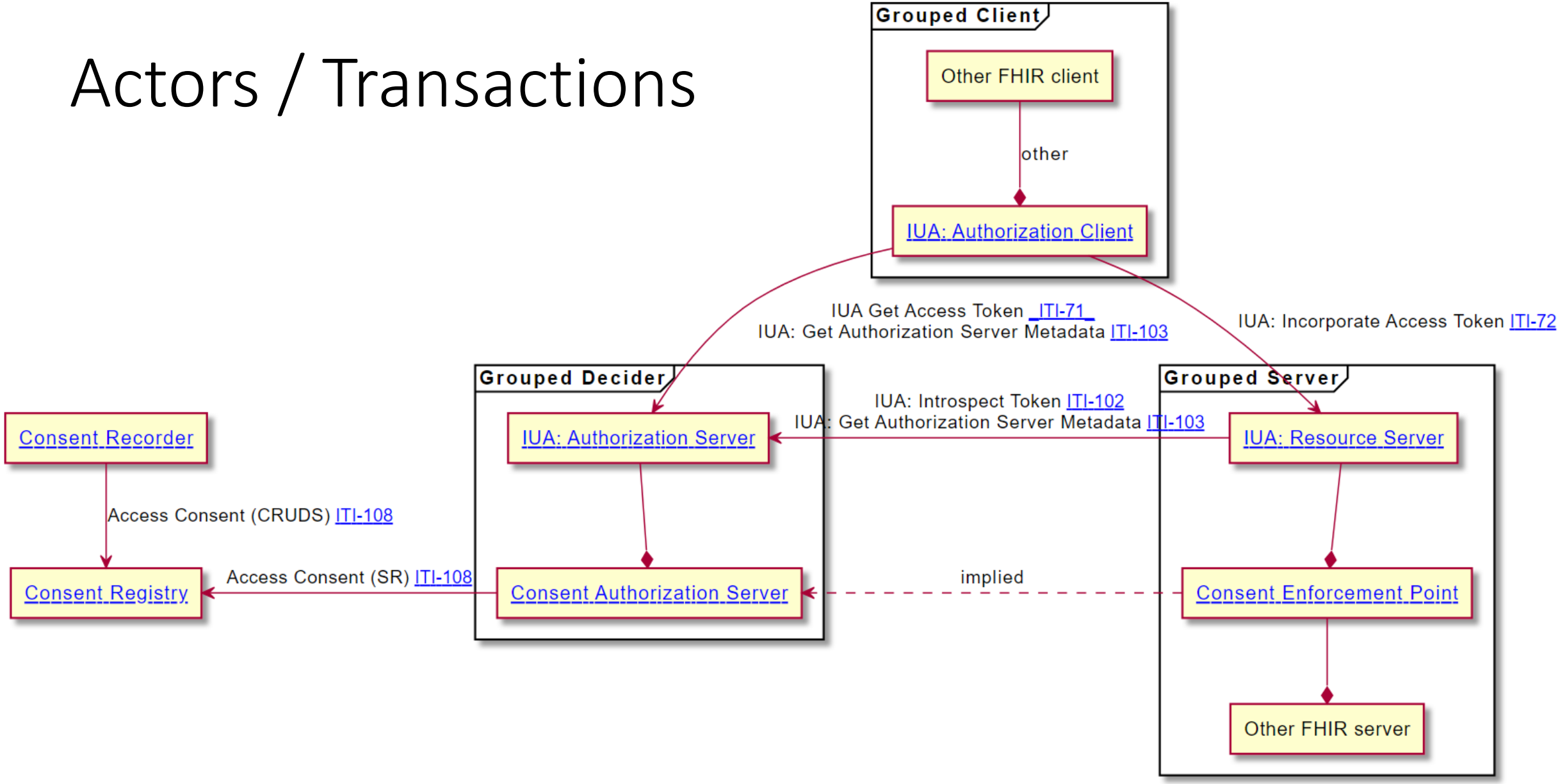
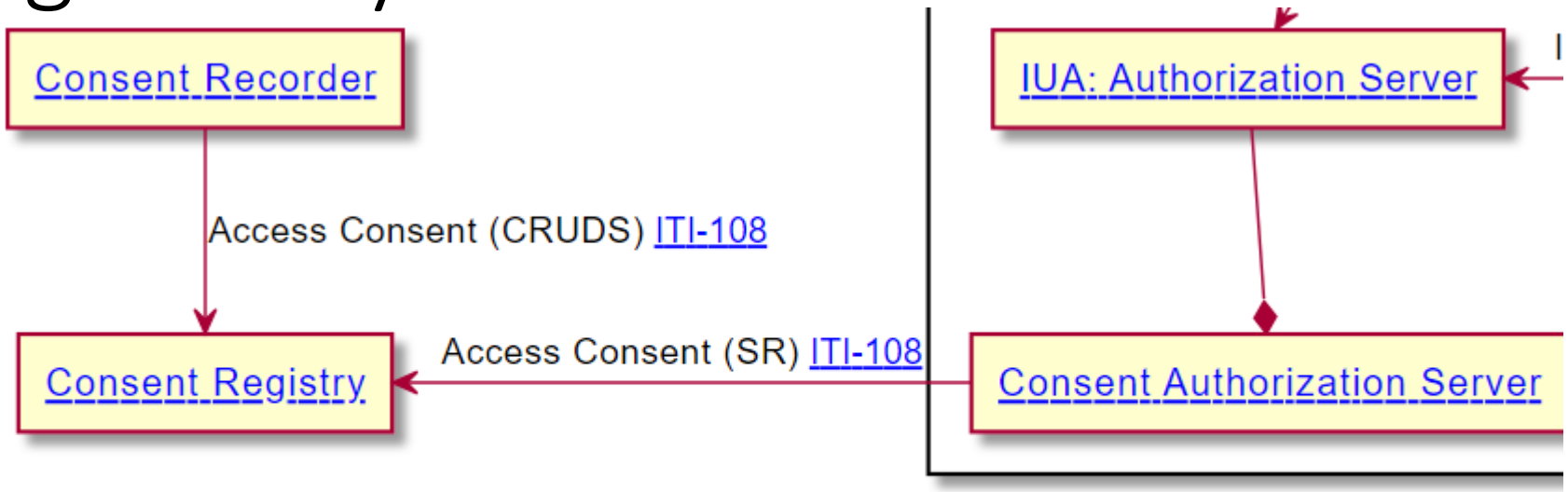


Figure 1:53.1-1: PCF Actor Diagram

Volume 2: Transaction

Capturing and Maintaining the Patient’s Privacy Consent

Capturing Privacy Consent



- Consent Registry is a simple FHIR server, it has no logic
- Consent Authorization Server accesses (Searches and Reads)
- Consent Recorder is responsible for the Consent Ceremony, Consistency of Consents on file, Maintenance, workflow, etc.
  - Complexity of Consent no more complex than Access Control can handle
- Transaction is FHIR http RESTful – Create/Read/Update/Delete/Search

Volume 3: Consent profiles

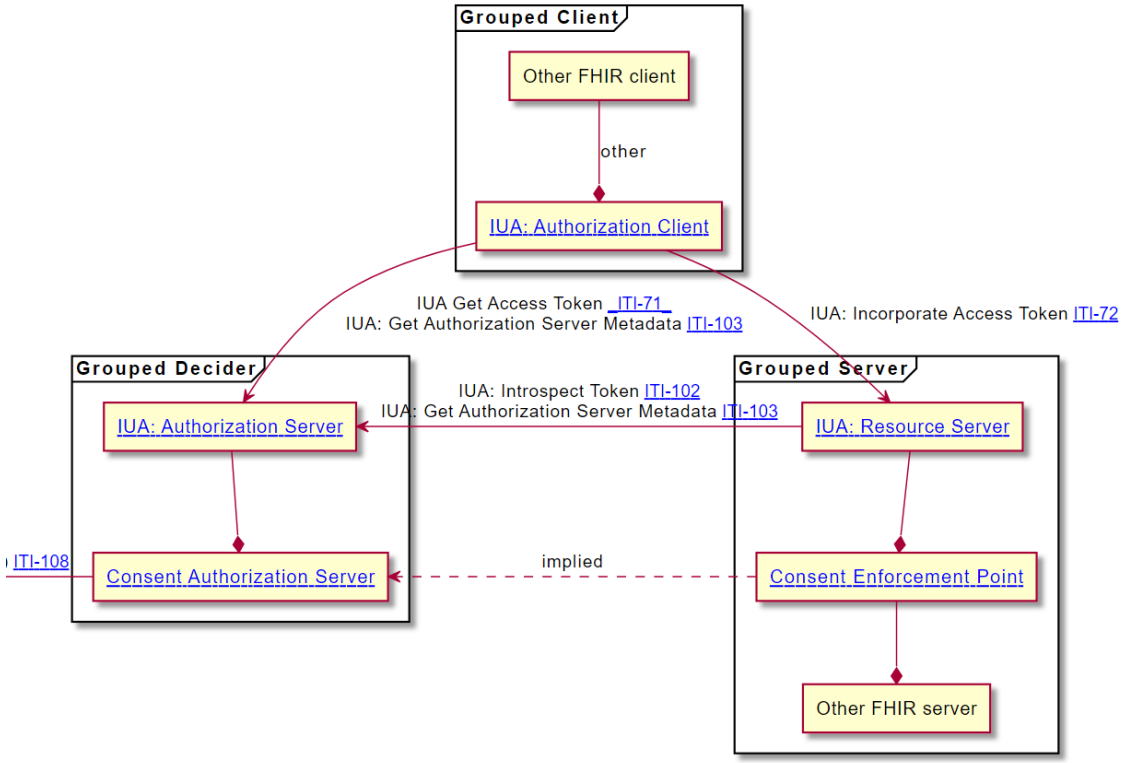
Privacy Consent Profiles

- Implied Consent
  - Basic-normal (TPO), all-normal, only-break-glass, deny-all
- Explicit Basic Consent
  - Identified base policy, timeframe of the consent, who is authorized, who gave consent, what purposeOfUse
- Explicit Intermediate
  - Data Timeframe, Data Id, Data Author, Data Relationship, and PurposeOfUse
- Explicit Advanced
  - Reliant on a Security Labeling Service

- And any combinations

Access Control

Access Control



- Augments a typical oAuth flow
- Where the typical oAuth flow is responsible for business rules such as RBAC
- The Augmentation
  - adds to the oAuth Authorization Server that the Access Token only is issued if the Privacy Consents also agree that the Scope is to be authorized,
  - and any impact on the enforcement is inserted in the Access Token
  - so that the Consent Enforcement Point can further refine the interaction between the FHIR app and the Resource Server.

Access Control interaction diagram

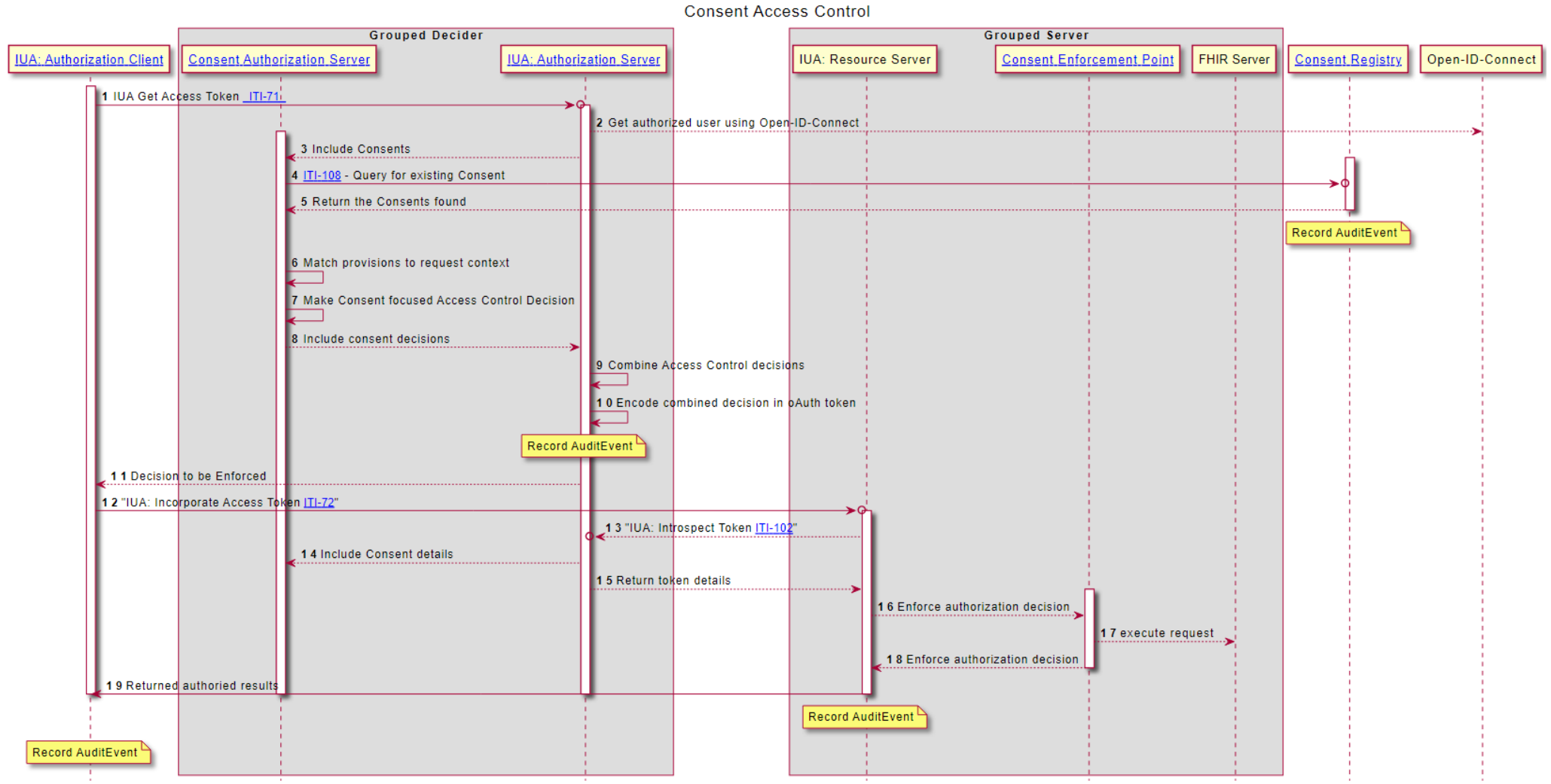


Figure 1:53.4.2.3-1: Consent Access Control Flow

Example: Okay for TPO, but not data authored by Dr Bob

Consent excerpt

```
"policy" : [
  {
    "uri" : "http://example.org/policies/basePrivacyConsentPolicy.txt"
  }
],
"provision" : {
  "type" : "permit",
  "purpose" : [
    {
      "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
      "code" : "TREAT"
    },
    {
      "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
      "code" : "HPAYMT"
    },
    {
      "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
      "code" : "HOPERAT"
    }
  ],
  "provision" : [
    {
      "type" : "deny",
      "data" : [
        {
          "meaning" : "authoredby",
          "reference" : {
            "reference" : "Practitioner/ex-practitioner"
          }
        }
      ]
    }
```

→

oAuth Access Token excerpt

```
"extensions" : {
  "ihe_iua" : {
    ...
    "purpose_of_use" : [{
        "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
        "code" : "TREAT"
      },{
        "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
        "code" : "HPAYMT"
      },{
        "system" : "http://terminology.hl7.org/CodeSystem/v3-ActReason",
        "code" : "HOPERAT"
    }]
  }
  "ihe_pcf" : {
    "patient_id" : "http://example.org/fhir/Patient/ex-patient",
    "doc_id" : ["http://example.org/fhir/Consent/ex-consent-intermediate-not-authoredby"],
    "residual" : [
      {
        "type" : "deny",
        "data" : [{
            "meaning" : "authoredby",
            "reference" : {
            "reference" : "http://example.org/fhir/Practitioner/ex-practitioner"
            }
        }]
      }
    ]
  }
}
```

Hands On

https://profiles.ihe.net/ITI/PCF

JohnMoehrke@gmail.com

Questions?