Rob’s Yellow Bricks Road to the FPKI OSCAL Catalog

Implementing OSCAL for your use case

- Sketch your process
- Find a problem to solve
- Start with the minimum

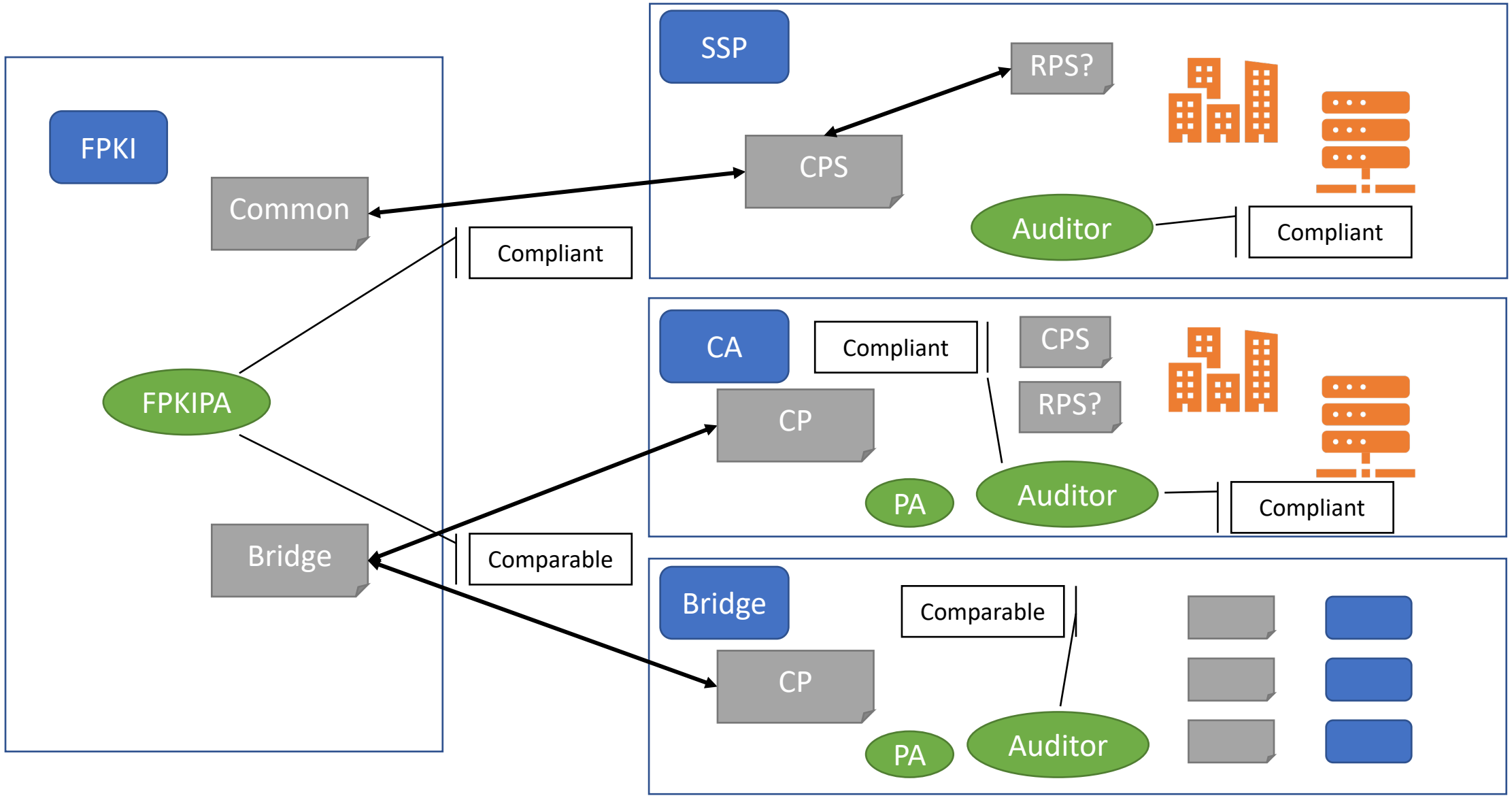
Sketch your process

Sketch your process

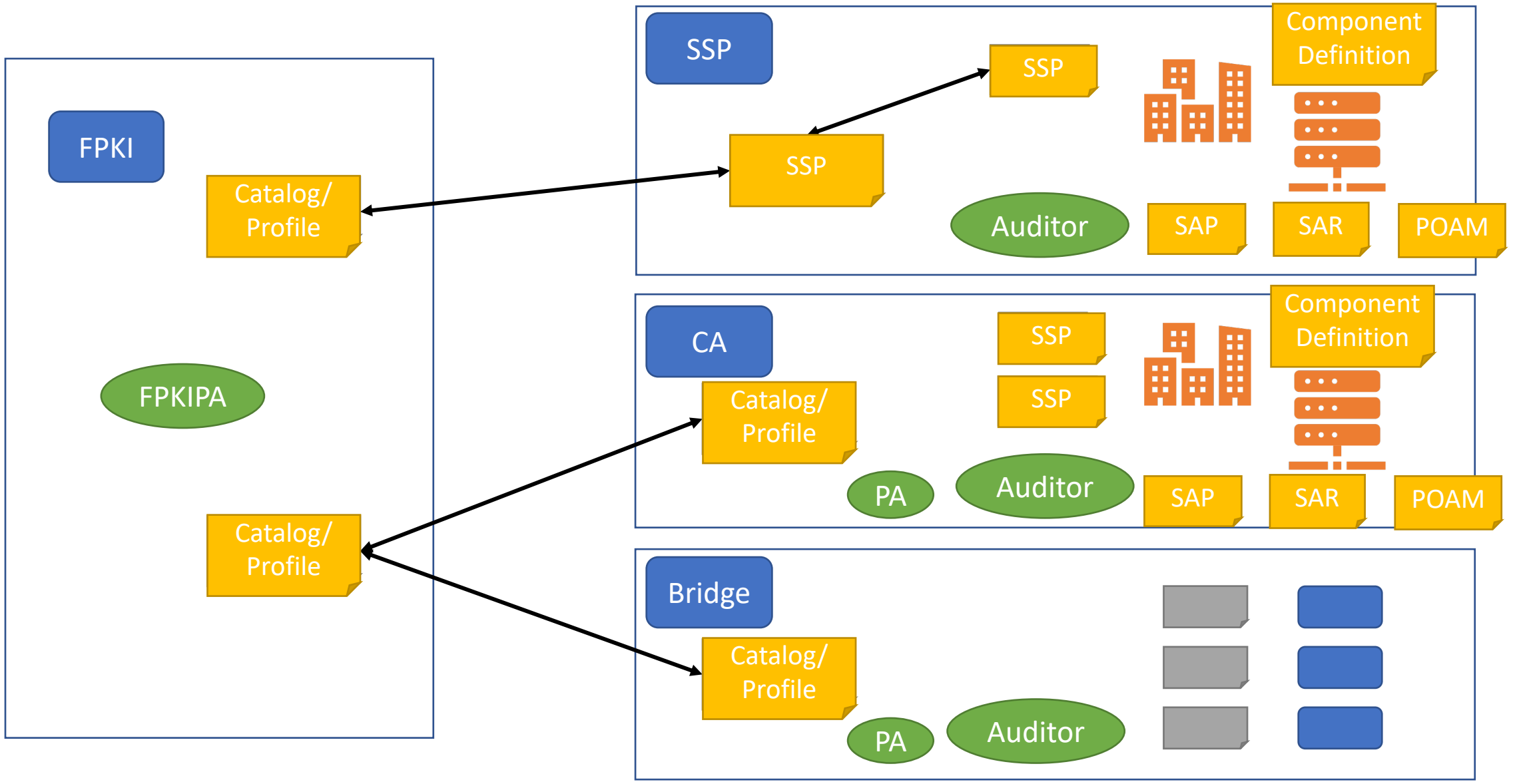
- Identify
  - People
  - Processes
  - Document Artifacts

Objective: Identify places where OSCAL is a natural fit

FPKI Process View



FPKI OSCAL View



Find a problem

Find a problem to solve

- Implementation of OSCAL requires work by the entire community
- The benefits should be clearly identified up front

Possible Benefits

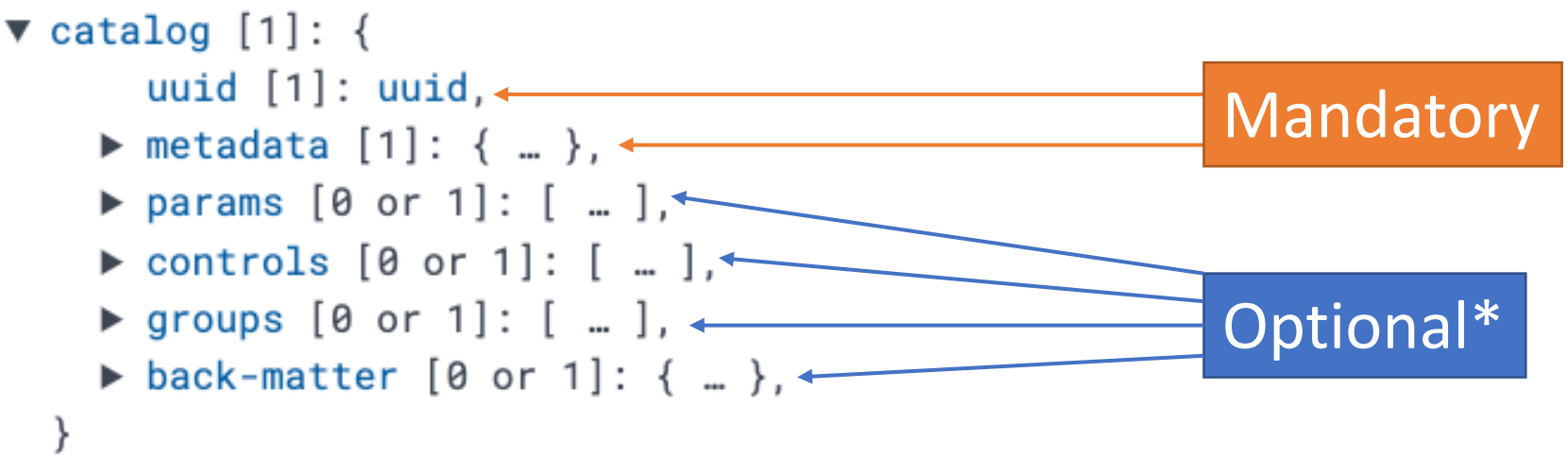
- Reduce cost of compliance over time
- Decrease time to complete compliance reviews
- Improvement in Quality for artifacts

Start with the Minimum

Start with the Minimum

- There are a lot of features and options in the OSCAL Specification
- You don’t have to adopt them all from day 1!

How to identify the minimum?



* Optional from the Data model perspective, but you can’t have a catalog with 0 controls!

Worked Example: Federal PKI Policy

Policy Extract

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

This CP establishes requirements for both subject distinguished names and subject alternative names.

3.1.1.1. Subject Names

The CA must assign X.501 distinguished names to all Subscriber certificates. These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs). Base DNs may be in either of two forms: a geo-political name or an Internet domain component name.

Things to Note

- Deeply nested control grouping
- Descriptive and Normative Text
- Requirements presented as unstructured Narrative

Analyzed Policy Extract

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

This CP establishes requirements for both subject distinguished names and subject alternative names.

3.1.1.1. Subject Names

1 The CA must assign X.501 distinguished names to all Subscriber certificates.[2] These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).[3] Base DNs may be in either of two forms: a geo-political name or an Internet domain component name.

Metadata

Groups

Controls


```
{
  "catalog": {
    "uuid": "c4fe3379-bc4a-41a8-b3ab-d53e550627f2",
    "metadata": {
      "title": "2.2",
      "last-modified": "2023-03-09T10:12:58.703",
      "version": "2.2",
      "oscal-version": "1.0.2"
    },
    "groups": [
      {
        "id": "sn-3.",
        "class": "Section",
        "title": "Identification and Authentication",
        "groups": [
          {
            "id": "sn-3.1.",
            "class": "Section",
            "title": "NAMING",
            "groups": [
              {
                "id": "sn-3.1.1.",
                "class": "Section",
                "title": "Types of Names",
                "groups": [
                  {
                    "id": "sn-3.1.1.1.",
                    "class": "Section",
                    "title": "Subject Names",
                    "controls": [
                      {
                        "id": "uuid-cf82929d-5763-42e4-b265-0e0f8555306d",
                        "class": "Normative",
                        "title": "The CA must assign X.501 distinguished names to all Subscriber certificates.",
                        "parts": [
                          {
                            "name": "requirement",
                            "prose": "The CA must assign X.501 distinguished names to all Subscriber certificates."
                          }
                        ]
                      },
                      {
                        "id": "uuid-56ceb38d-afcb-4bcf-b30f-9a9259051632",
                        "class": "Descriptive",
                        "title": "These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).",
                        "parts": [
                          {
                            "name": "requirement",
                            "prose": "These distinguished names are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs)."
                          }
                        ]
                      },
                      {
                        "id": "uuid-9772c188-7be3-4e29-968f-3b6525cb38d3",
                        "class": "Normative",
                        "title": "Base DNs may be in either of two forms: a geo-political name or an Internet domain component name.",
                        "parts": [
                          {
                            "name": "requirement",
                            "prose": "Base DNs may be in either of two forms: a geo-political name or an Internet domain component name."
                          }
                        ]
                      }
                    ]
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

Metadata

```
2     "catalog": {
3         "uuid": "c4fe3379-bc4a-41a8-b3ab-d53e550627f2",
4         "metadata": {
5             "title": "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework",
6             "last-modified": "2023-03-09T10:12:58.703",
7             "version": "2.2",
8             "oscal-version": "1.0.2"
9         },
```

- “Catalog” – top level organizational object
- ”UUID” – UUIDs are used widely throughout OSCAL as systemic identifiers
- Metadata
  - Title
  - Last Modified
  - Version
  - OSCAL Version - latest is 1.0.4

Groups

```
10      "groups": [
11          {
12              "id": "sn-3.",
13              "class": "Section",
14              "title": "Identification and Authentication",
15              "groups": [
16                  {
17                      "id": "sn-3.1.",
18                      "class": "Section",
19                      "title": "NAMING",
20                      "groups": [
21                          {
22                              "id": "sn-3.1.1.",
23                              "class": "Section",
24                              "title": "Types of Names",
25                              "groups": [
26                                  {
27                                      "id": "sn-3.1.1.1.",
28                                      "class": "Section",
29                                      "title": "Subject Names",
```

- Groups - Structural component
- ID (Optional)
  - Human oriented
  - consistent across revisions
- Class (Optional)
  - Characterization

Controls


```
"controls": [
    {
        "id": "uuid-cf82929d-5763-42e4-b265-0e0f8555306d",
        "class": "Normative",
        "title": "The CA must assign X.501 distinguished names to all Subscriber certificates.",
        "parts": [
            {…
            }
        ]
    },
    {
        "id": "uuid-56ceb38d-afcb-4bcf-b30f-9a9259051632",
        "class": "Descriptive",
        "title": "These distinguished names are comprised of a base distinguished name (Base DN) a
        "parts": [
            {
                "name": "requirement",
                "prose": "These distinguished names are comprised of a base distinguished name (Ba
            }
        ]
    },
    {
        "id": "uuid-9772c188-7be3-4e29-968f-3b6525cb38d3",
        "class": "Normative",
        "title": "Base DNs may be in either of two forms: a geo-political name or an Internet doma
        "parts": [
            {
                "name": "requirement",
                "prose": "Base DNs may be in either of two forms: a geo-political name or an Inter
            }
        ]
    }
]
```


- Controls
- ID (mandatory)
  - Human oriented
  - Token
  - Note that I cheated
- Class (optional)
  - characterization
  - Useful for me to distinguish between Normative or Descriptive
- Parts
  - optional (but not really)
  - Name (mandatory)
  - Prose – the contents (optional)