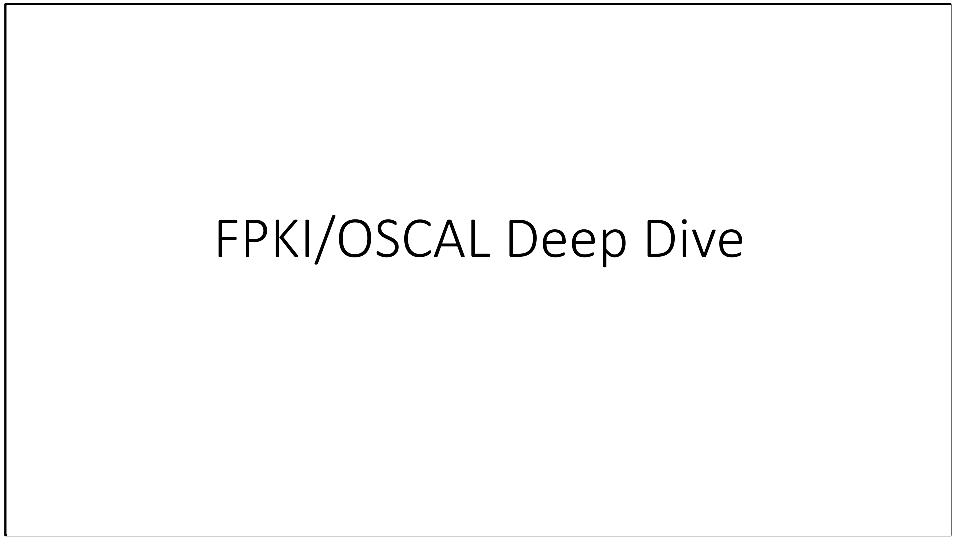
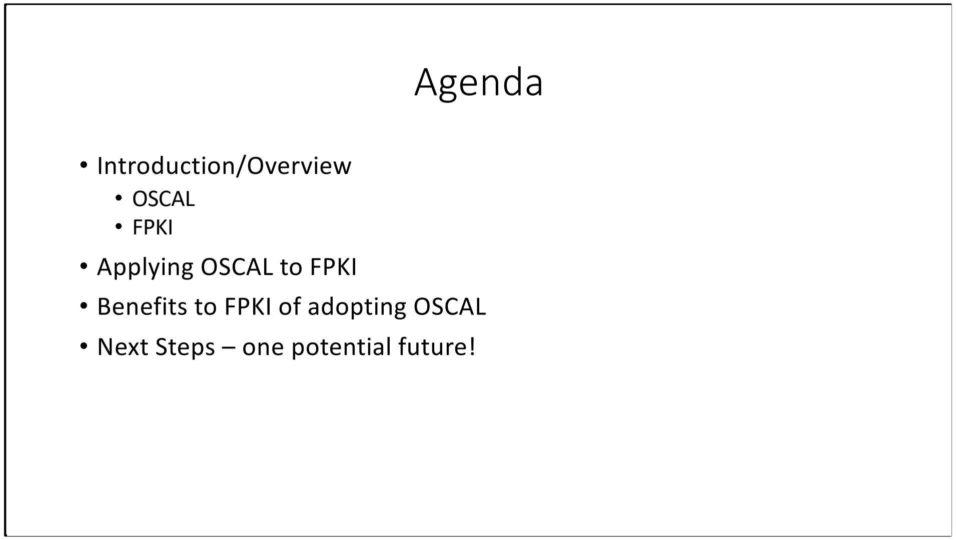


FPKI/OSCAL Deep Dive



Agenda

- Introduction/Overview
  - OSCAL
  - FPKI
- Applying OSCAL to FPKI
- Benefits to FPKI of adopting OSCAL
- Next Steps – one potential future!

First on our agenda we want to introduce the communities to each other.

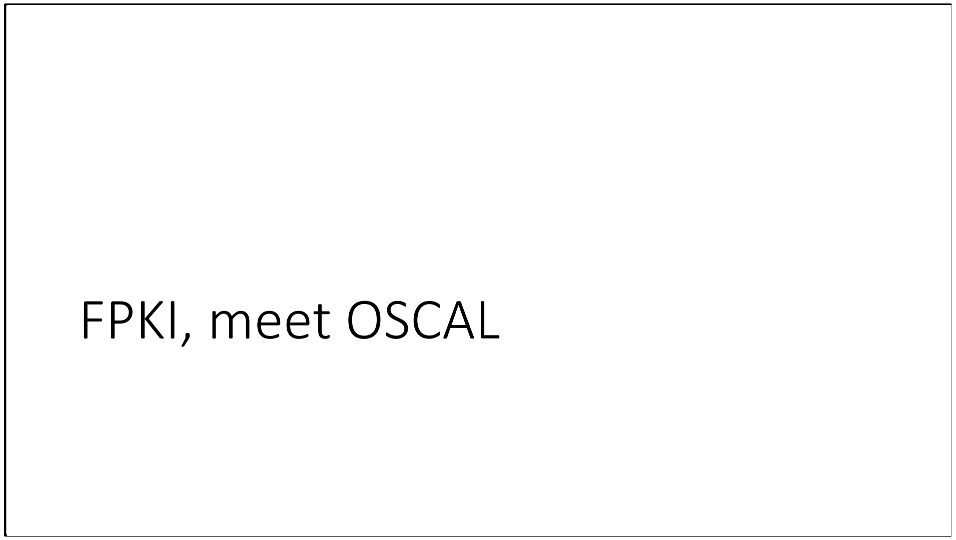
- I would like my friends from the Federal PKI community, or other PKIs to learn about OSCAL
- and I would like my OSCAL friends to understand what the Federal PKI is and how it operates.

With the introduction out of the way, we can talk about how OSCAL can be applied in the context of FPKI,

and then discuss the benefits – why we would want to apply OSCAL to FPKI

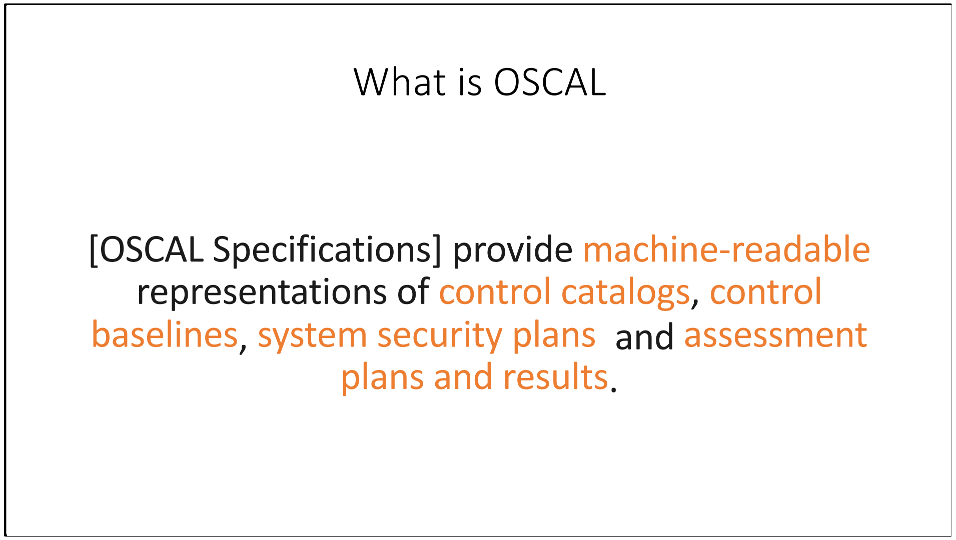
Finally, the CALL TO ACTION! I will identify what I think are the next crucial steps we can take to capture those benefits.

Of course, I am not here as an official representative of FPKI, just a friend who wants to solve some problems – nothing I say should be seen as an official pronouncement by Fed PKI, or the community, or GSA.



FPKI, meet OSCAL

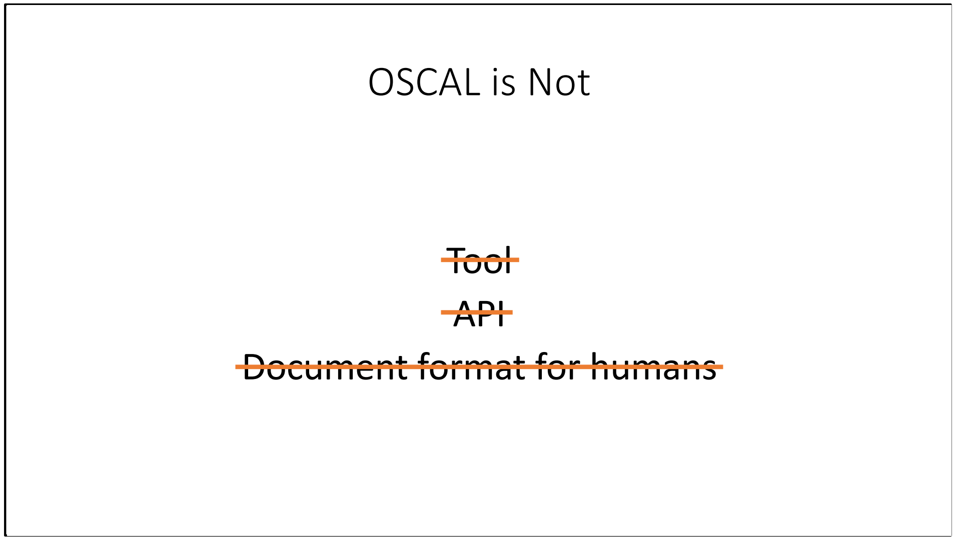
Without further ado, let’s introduce OSCAL to the federal PKI community



What is OSCAL

[OSCAL Specifications] provide machine-readable representations of control catalogs, control baselines, system security plans and assessment plans and results.

OSCAL is a set of technical specifications defined by NIST to represent information about security controls, components that implement security controls, and security assessments that validate the security controls



OSCAL is Not

~~Tool~~

~~API~~

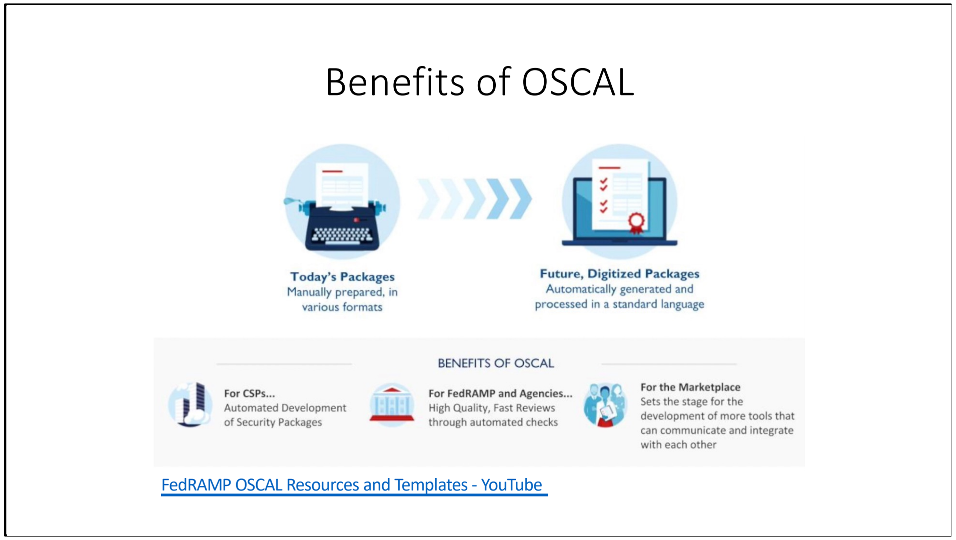
~~Document format for humans~~

Oscal is not a tool, though there are many tools that implement the OSCAL standard

OSCAL is not a service offering an API, though a standard REST API has been proposed by the community

Finally, OSCAL is not a document format for humans – it doesn’t replace any document specification (like RFC 3647)

OSCAL allows us to translate our existing documents into a consistent, standardized, machine-readable format.



Benefits of OSCAL

Today's Packages
Manually prepared, in various formats

Future, Digitized Packages
Automatically generated and processed in a standard language

BENEFITS OF OSCAL

For CSPs...
Automated Development of Security Packages

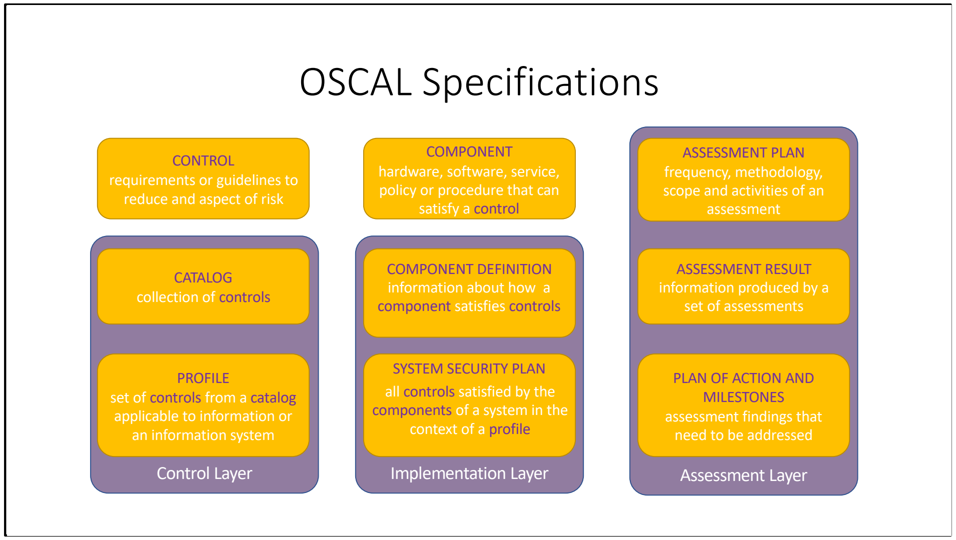
For FedRAMP and Agencies...
High Quality, Fast Reviews through automated checks

For the Marketplace
Sets the stage for the development of more tools that can communicate and integrate with each other

FedRAMP OSCAL Resources and Templates - YouTube

OSCAL has been adopted by FedRamp, because of the benefits of automating and digitizing compliance packages

FedRAMP manages compliance verification for hundreds of services and more services are onboarding all the time. They chose OSCAL because they can reduce the time taken for reviews while improving the quality, and they don't have to implement a proprietary standard.



OSCAL Specifications

CONTROL
requirements or guidelines to reduce and aspect of risk

CATALOG
collection of controls

PROFILE
set of controls from a catalog applicable to information or an information system

Control Layer

COMPONENT
hardware, software, service, policy or procedure that can satisfy a control

COMPONENT DEFINITION
information about how a component satisfies controls

SYSTEM SECURITY PLAN
all controls satisfied by the components of a system in the context of a profile

Implementation Layer

ASSESSMENT PLAN
frequency, methodology, scope and activities of an assessment

ASSESSMENT RESULT
information produced by a set of assessments

PLAN OF ACTION AND MILESTONES
assessment findings that need to be addressed

Assessment Layer

So, what is OSCAL?

There are three major parts to the OSCAL standard.

First, we have Controls – a control is just a security requirement

Sets of related controls can be collected in a catalog. 800-53 is the most famous example
Profiles were defined as subsets of controls. In the case of 800-53, the baselines (Low, moderate, high) are represented as profiles

The Catalog and profile, together represent the “Control Layer” of the OSCAL standard

When it comes to implementation, we start with components – anything that can implement a control

A component can be a system, but it can be a person, or a process, it could be a building or a document

A component definition is a description of how a component or set of related components can satisfy some controls. System owners can document the components of their systems, or vendors can provide Component definitions for their products or services to help their customers with documentation

A system security plan documents all the controls implemented by all the components in a particular information system, in the context of a profile.

The Component Definition and System Security Plan are the two parts of the Implementation Layer

Of course, we need someone to make sure that the controls are operating the way they are intended to

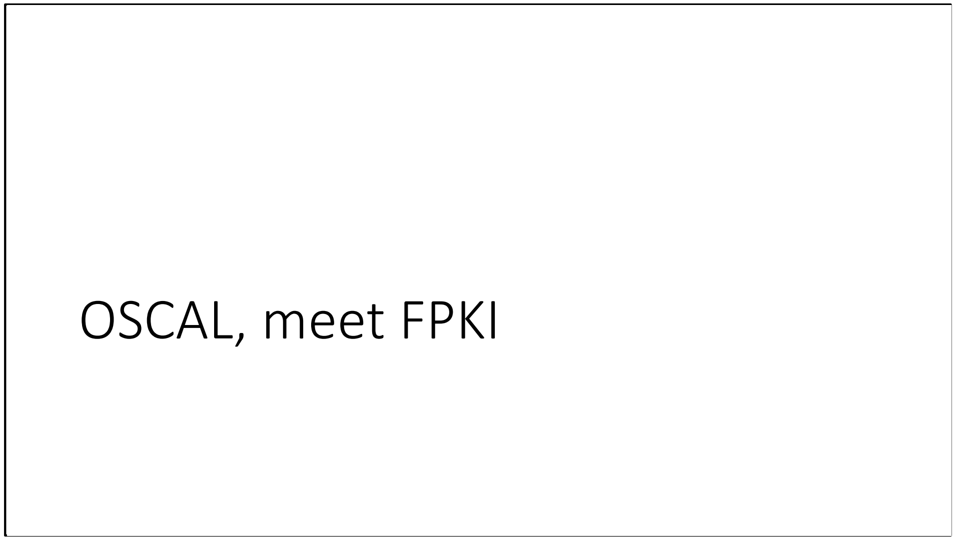
That begins with an assessment plan, which talks about the scope of an assessment, how often it will be performed, and the exact processes that the assessor will follow

When the assessment has been completed, an Assessment Result is produced – this just document the outcome

When the assessor has complemented their process, the system owner will document how they will address any issues or failures identified during the assessment in a Plan of Action and Milestones

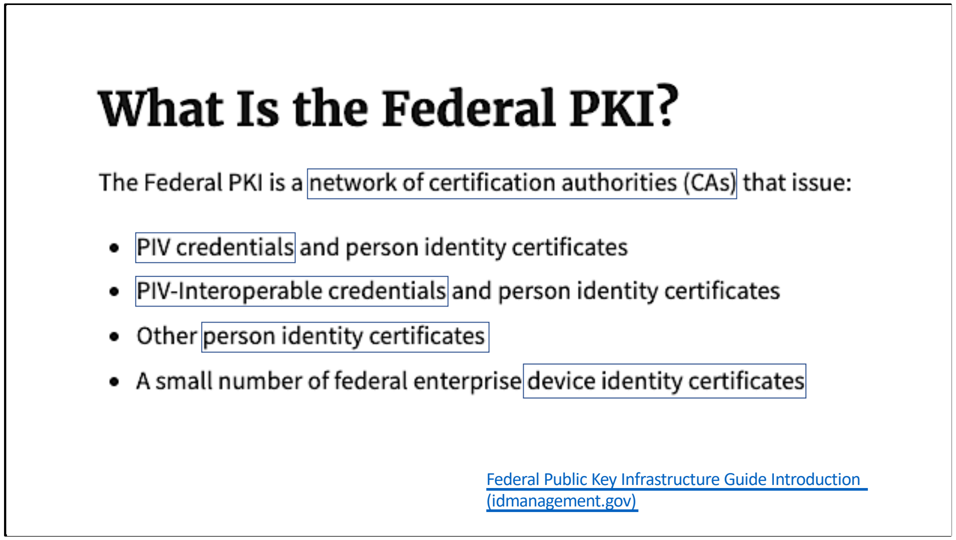
The Assessment Layer includes Assessment Plan, Assessment Result and the Plan Of Action and Milestones.

The text is here in case you all need to print out these slides later.



OSCAL, meet FPKI

We’ve introduced OSCAL to FPKI, now I would like my pals from the OSCAL team to meet the FPKI



What Is the Federal PKI?

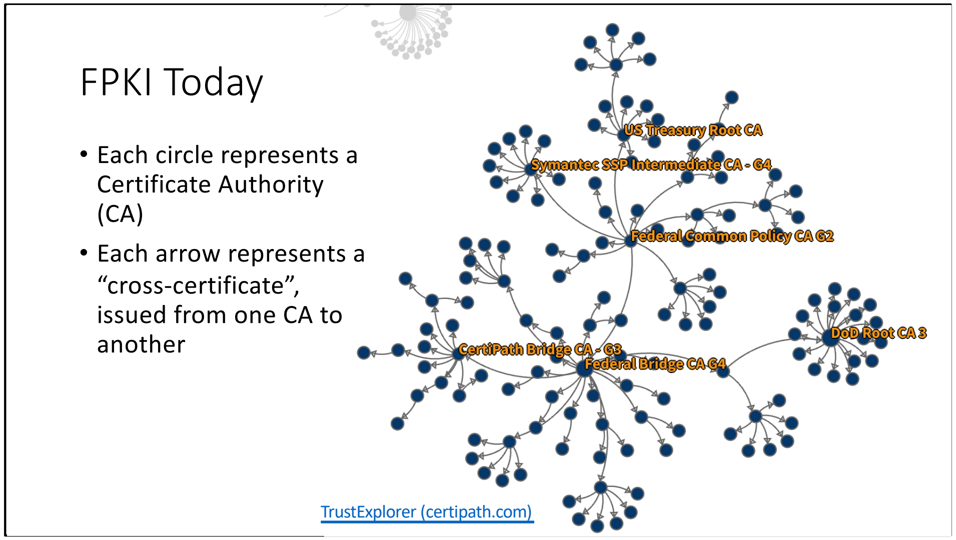
The Federal PKI is a network of certification authorities (CAs) that issue:

- PIV credentials and person identity certificates
- PIV-Interoperable credentials and person identity certificates
- Other person identity certificates
- A small number of federal enterprise device identity certificates

Federal Public Key Infrastructure Guide Introduction (idmanagement.gov)

The Federal PKI is a network of Certification Authorities (CAs)

They mostly issue certificates to people (most famously, the certificates on the PIV card), but they also issue device certificates



FPKI Today

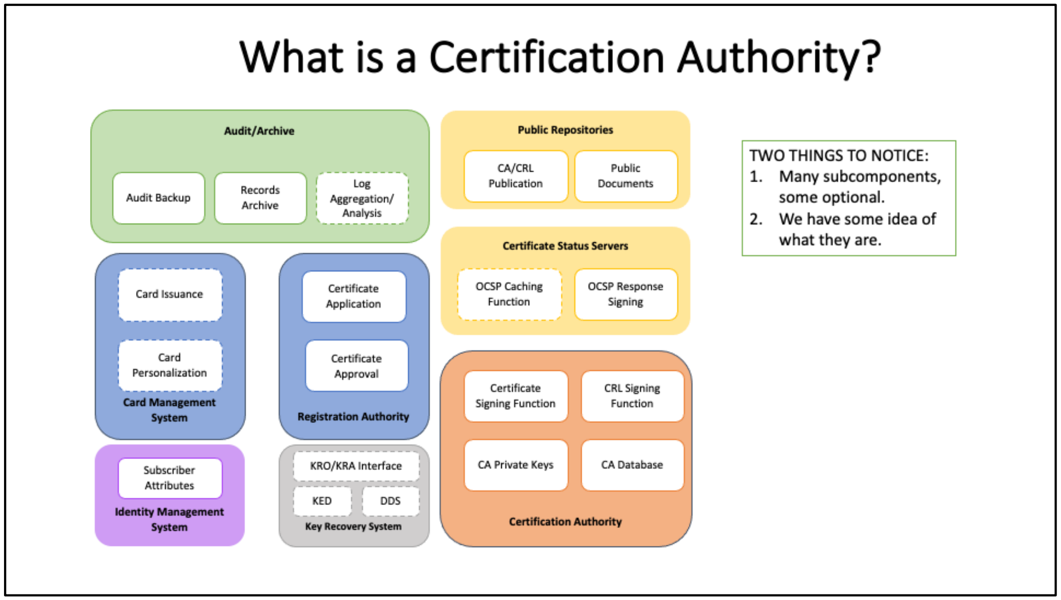
- Each circle represents a Certificate Authority (CA)
- Each arrow represents a "cross-certificate", issued from one CA to another

TrustExplorer (certipath.com)

This is the FPKI today.

Each circle on this diagram represents a Certification Authority, and each arrow represents a cross-certificate, which is a certificate issue by one Certification Authority to another.

There's a lot to look at, but the main thing I want everyone to notice is that there are bunch of Certification Authoritiess in the FPKI, and the relationships are pretty complicated!



What is a Certification Authority?

Audit/Archive

Audit Backup

Records Archive

Log Aggregation/ Analysis

Public Repositories

CA/CRL Publication

Public Documents

Certificate Status Servers

OCSP Caching Function

OCSP Response Signing

Card Issuance

Card Personalization

Card Management System

Certificate Application

Certificate Approval

Registration Authority

Certificate Signing Function

CRL Signing Function

CA Private Keys

CA Database

Certification Authority

Subscriber Attributes

Identity Management System

KRO/KRA Interface

KED

DDS

Key Recovery System

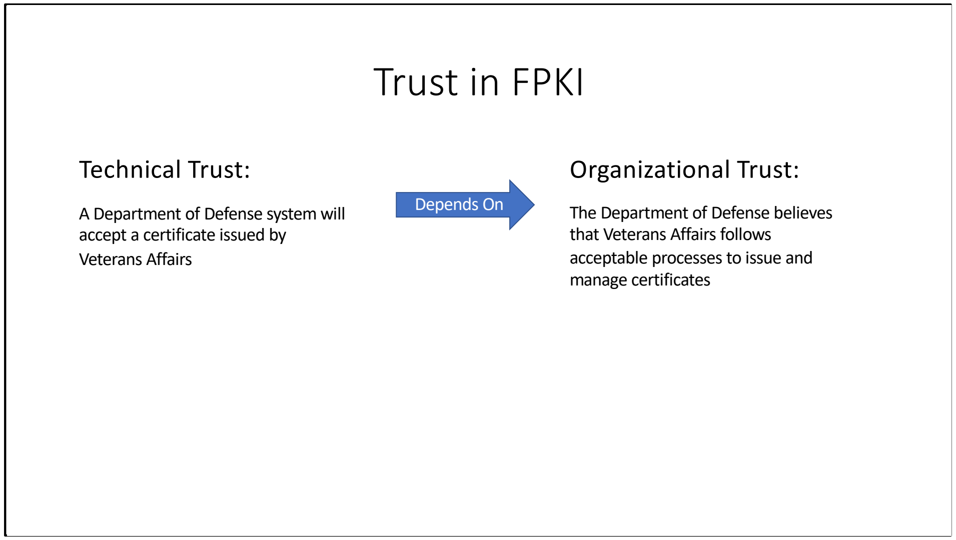
TWO THINGS TO NOTICE:

1. Many subcomponents, some optional.
2. We have some idea of what they are.

Inside each of the bubbles, is a PKI (Public Key Infrastructure).

A couple of things to notice:

- First, there are many components in a PKI, though some of them are optional
- Secondly, we have a pretty clear idea of what a PKI is made of. This is different than a generic system like you would see under 800-53. For a generic system you really don't have any idea what the components might be. This is not the case for a CA and PKI. This will become important later!



Trust in FPKI

Technical Trust:

A Department of Defense system will accept a certificate issued by Veterans Affairs

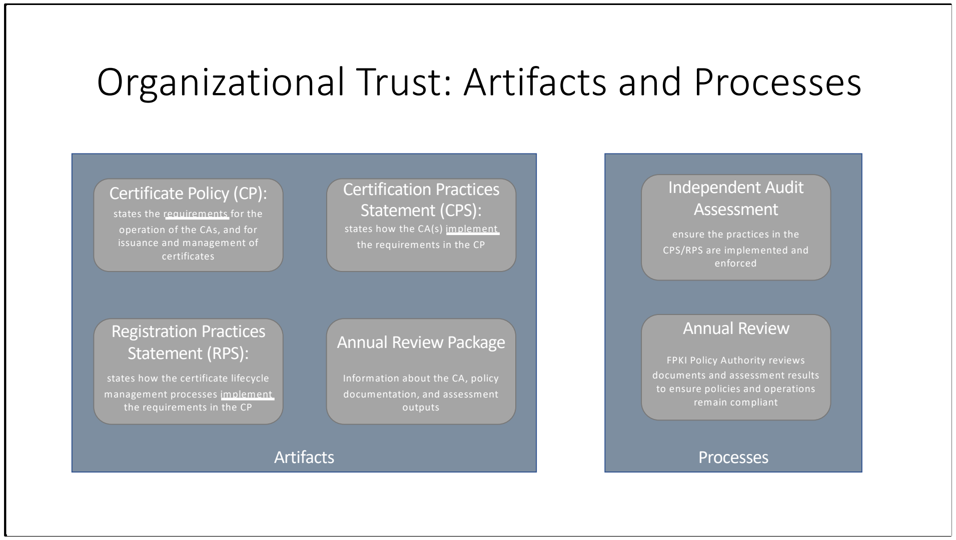
Organizational Trust:

The Department of Defense believes that Veterans Affairs follows acceptable processes to issue and manage certificates

We discussed the bubbles from the FPKI on the last slide, now we're talking about the arrows. The arrows represent "trust relationships", and this is the power of the FPKI. The cross-certificates provide technical trust – enabling, for example, a DOD system to accept a certificate issued by Veterans Affairs.

The technical trust depends on what we might call "Organizational Trust"

Organizational trust means that the Department of Defense believes that Veterans Affairs follows acceptable baseline processes for issuing certificates, performing all of the lifecycle management activities related to Certificate Lifecycle Management, and that their CA implements all of the necessary security controls



Organizational Trust: Artifacts and Processes

Certificate Policy (CP): states the requirements for the operation of the CAs, and for issuance and management of certificates

Certification Practices Statement (CPS): states how the CA(s) implement the requirements in the CP

Registration Practices Statement (RPS): states how the certificate lifecycle management processes implement the requirements in the CP

Annual Review Package

Information about the CA, policy documentation, and assessment outputs

Artifacts

Independent Audit Assessment

ensure the practices in the CPS/RPS are implemented and enforced

Annual Review

FPKI Policy Authority reviews documents and assessment results to ensure policies and operations remain compliant

Processes

How is organizational Trust provided? Through artifacts and processes.

Trust is anchored in a Certificate Policy, which identifies the basic requirements for managing a CA and certificates.

Every CA will produce a Certification Practices Statement, which document how they implement the requirements in the CP.

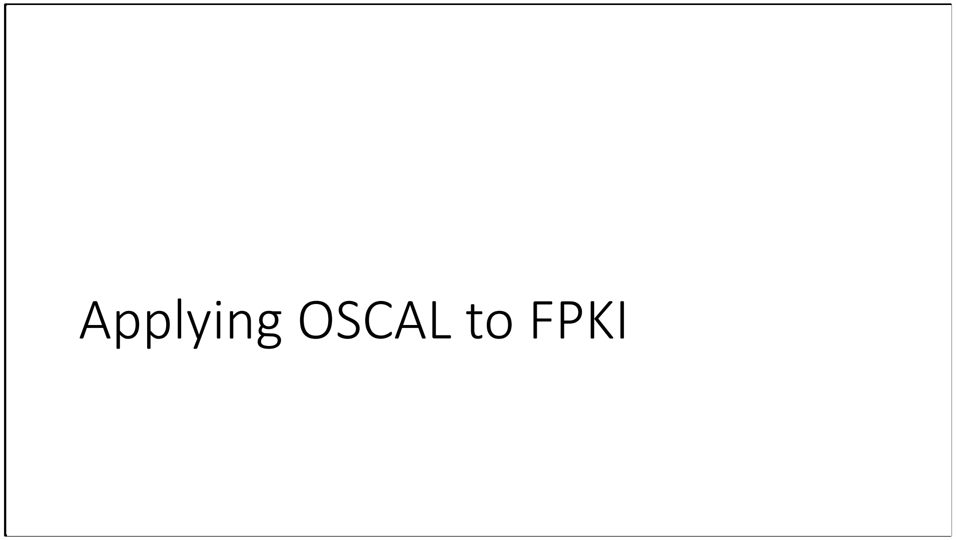
Some entities may use the services of a CA, but perform their own registration – they create a Registration Practices statement, which only documents the registration related practices.

There are two important processes from the perspective of the federal PKI.

First is the independent Audit Assessment – every CA in the federal PKI has to have an annual independent audit. The auditor makes sure that the CA is actually performing the processes that they documented in their CPS.

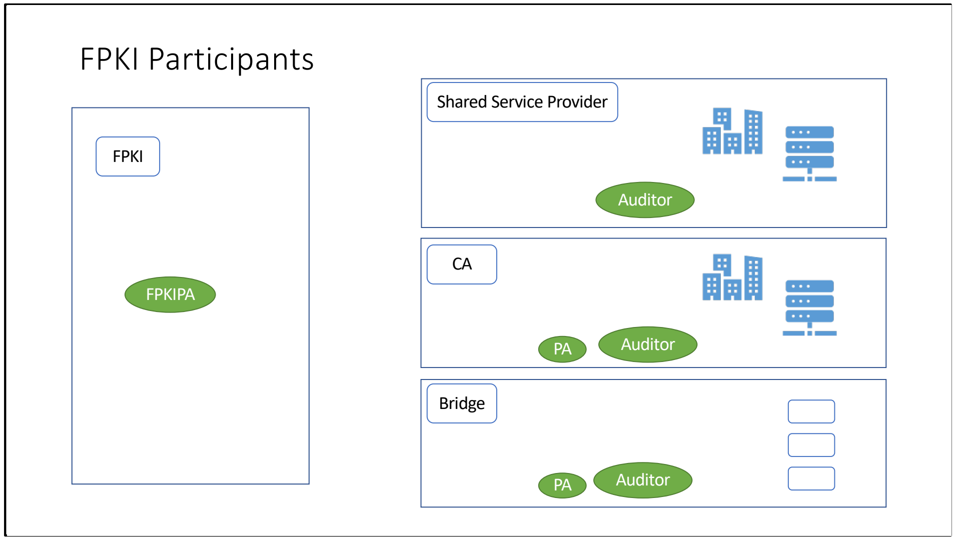
Secondly, there is an annual review. The Federal PKI itself validates the documentation that a CA has produced, and looks at their Annual Review results.

The final artifact is the annual review package, submitted by every CA in the community.



Applying OSCAL to FPKI

We have introduced FPKI and OSCAL, let’s talk about how they work together.



FPKI Participants

FPKI

FPKIPA

Shared Service Provider

Auditor

CA

PA

Auditor

Bridge

PA

Auditor

First, we'll reintroduce the participants.

SQUARES

Starting with the FPKI itself.

The CAs connected to the FPKI come in a few different types:

Shared Service Providers, Independent CAs and Bridges. A bridge is a group of CAs that need to interoperate with each other and want to interoperate with the Federal PKI as one group.

Shared Servicer Providers and CAs have infrastructure – buildings, people processes and systems.

Bridges take care of the trust relationships among themselves without too much interference from the Fed PKI, but they do have members, and the FPKI needs to ensure that they are managing their members properly

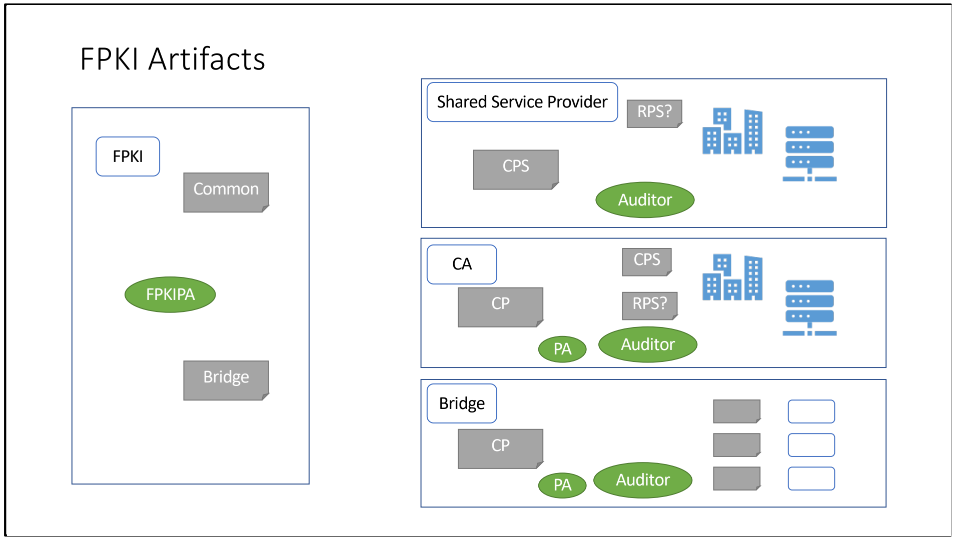
OVALS

The FPKI has a governance body called the FPKI Policy Authority

For Shared Service Providers, we primarily interact with them in the context of their auditors.

Other kinds of CAs will have their own Policy Authorities, but will also engage an auditor.

The same is true for bridges.

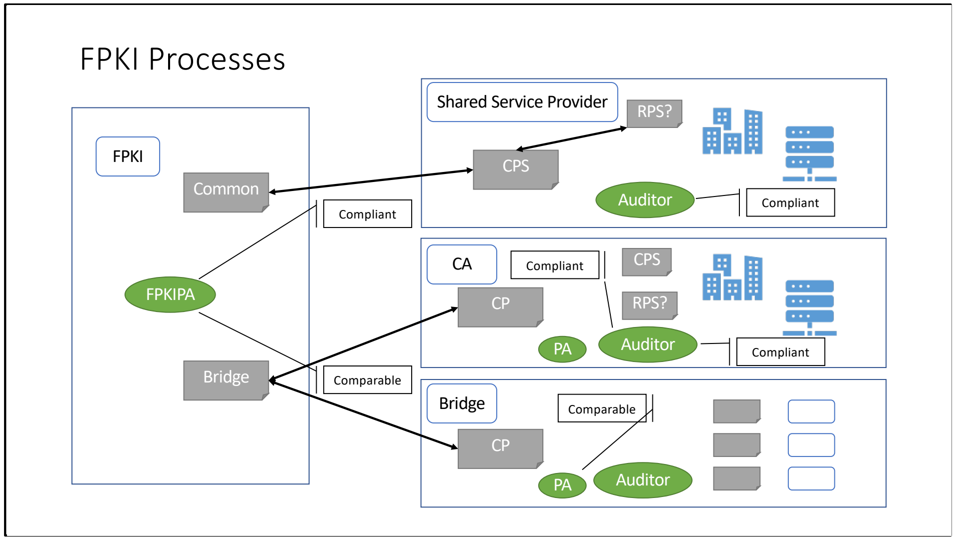


For Federal PKI, the anchor documents are the Federal Common Policy and the Federal Bridge Certificate Policy. These documents are owned and managed by the FPKI Policy Authority.

Shared Service Providers will have at least one CPS, and their customers my publish their own RPS documents.

An independent CA will publish an independent Certificate Policy, which will be owned and managed by their Policy Authority. Like the shared service provider, they will publish at least one CPS and may have RPS documents.

A bridge's Policy Authority will maintain a CP, and their governance documentation will define what documents their members have to produce.



FPKI Processes

We've covered Artifacts, let's talk about processes.

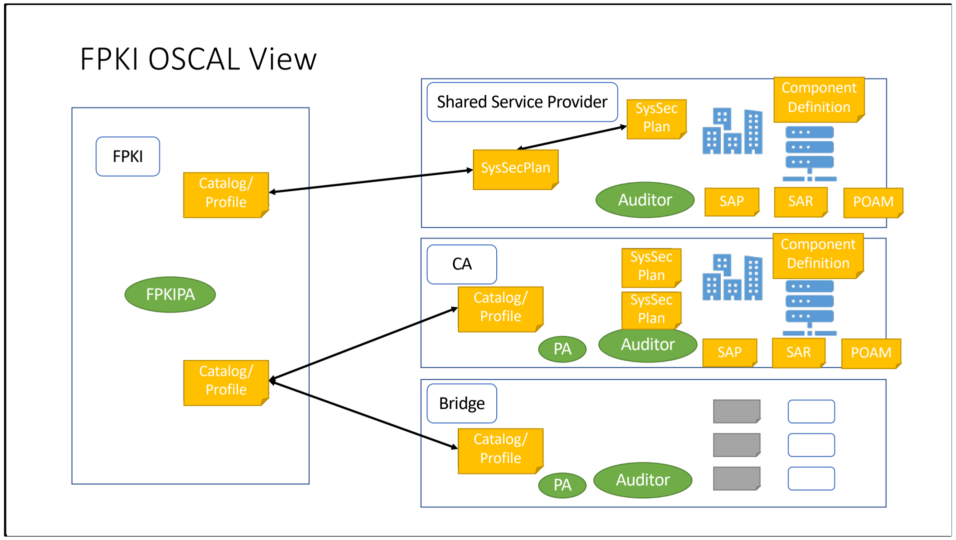
While the Audits are critical, there's one other important process that I need to mention.

We've said that a CPS documents how a CA implements the requirements of a Certificate Policy. As part of the annual review, the Federal PKI Policy Authority will verify that each Shared Service Provider's CPS describes practices that meet the requirements of whatever version of Common Policy is in effect at that time. This is called a compliance analysis, and a CPS that passes the test is called compliant.

For independent CAs and bridges, the Federal PKI Policy authority compares their Certificate Policy to the Federal Bridge Certificate Policy. We're comparing the requirements to see if they are of equal strength. A CP that is of equal or greater strength is called "Comparable"

The auditor performs their assessment of the SSP infrastructure and determines whether the practices being followed are compliant with the practices documented in the CPS.

For an independent CA, an auditor will perform the CP to CPS compliance analysis, and also perform the compliance audit.



FPKI OSCAL View

That may seem complex, and I suppose it is, but it aligns very well with standard compliance frameworks like the ones OSCAL was designed to help automate.

The CP is a collection of requirements, which can be expressed as a Catalog or Profile.

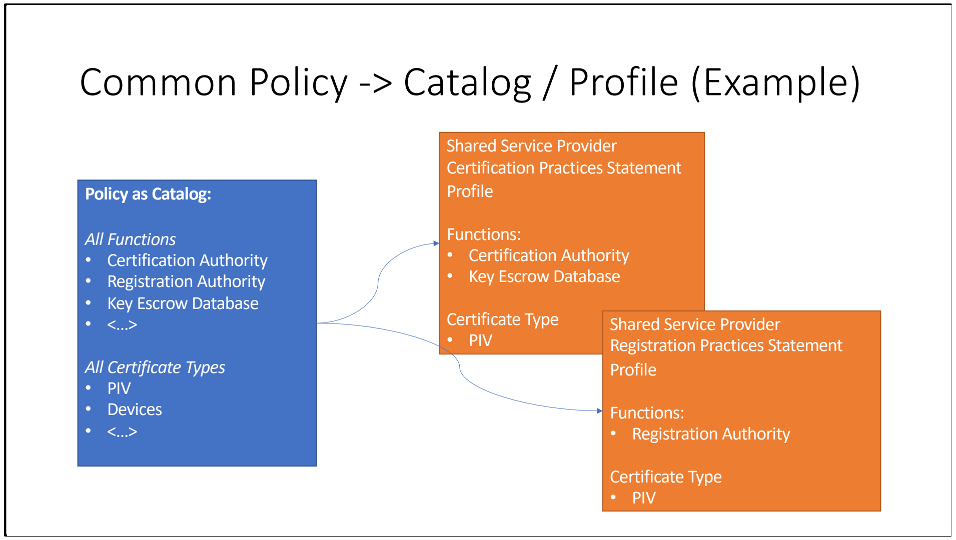
The CPS maps perfectly to the System Security Plan.

OSCAL provides a few extra artifacts that we don’t address in detail in FPKI documentation.

The component definitions specification can document the behavior of the independent elements of the architecture

The auditor can use the OSCAL specifications from the Assessment Layer, Security Assessment Plan, Security Assessment Results and Plan of Action and Milestones to document their activities.

as you can see, The alignment is very clear.



Common Policy -> Catalog / Profile (Example)

Policy as Catalog:

All Functions

- Certification Authority
- Registration Authority
- Key Escrow Database
- <…>

All Certificate Types

- PIV
- Devices
- <…>

Shared Service Provider Certification Practices Statement Profile

Functions:

- Certification Authority
- Key Escrow Database

Certificate Type

- PIV

Shared Service Provider Registration Practices Statement Profile

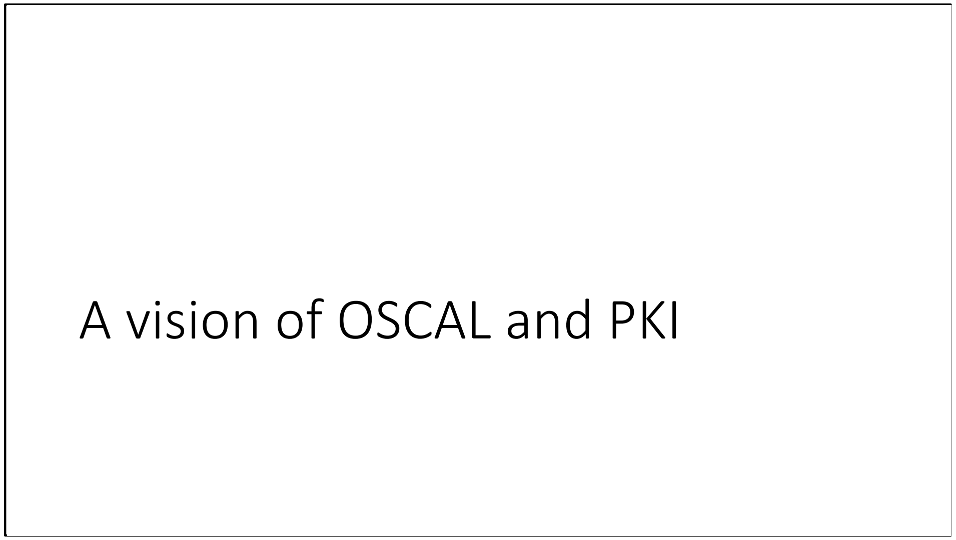
Functions:

- Registration Authority

Certificate Type

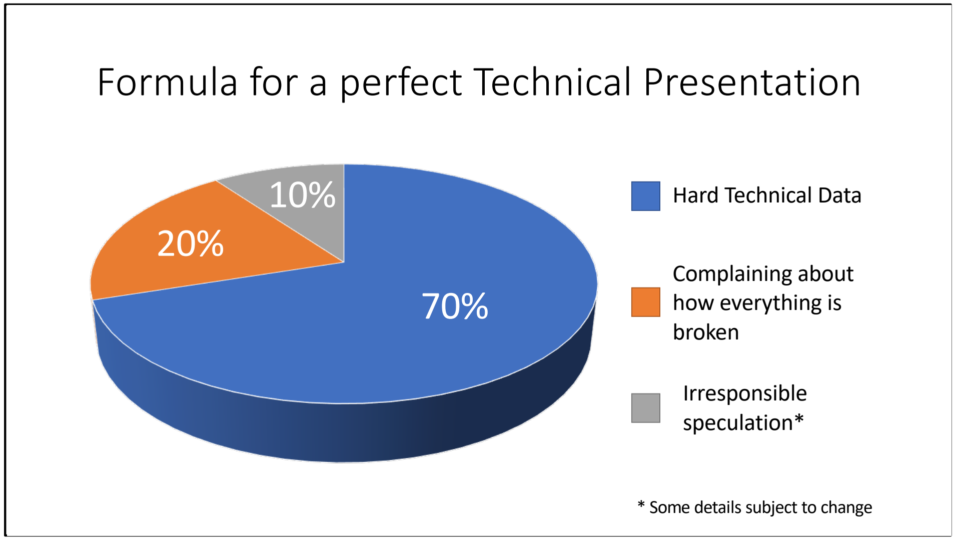
- PIV

A quick word on Catalogs and Profiles – These concepts would be extremely helpful for entities managing CPS or RPS documents. A typical Shared Service Provider will only focus on a subset of the certificate types and functions specified in the Certificate Policy, and an RPS is explicitly limited to a narrow scope. Today, participants are expected to review the entire document and determine for themselves which parts apply. I believe the concept of an FPKI Profile for a subset of functions and certificate types would greatly simplify the management of this documentation at scale.



A vision of OSCAL and PKI

Now that we’ve seen how OSCAL could support FPKI, let’s talk about why FPKI should adopt OSCAL



Formula for a perfect Technical Presentation

* Some details subject to change

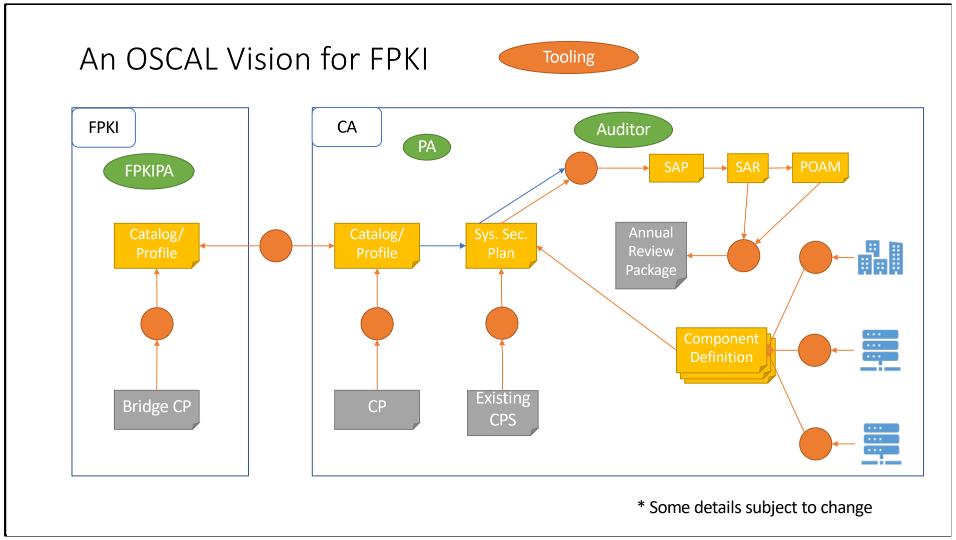
But first, an aside. You may not be aware of the formula for a perfect technical presentation.

It has 70% hard technical detail.

20% of the presentation is basically complaining about how everything is broken,

10% is irresponsible speculation about the future.

I’m not suggesting that any of my speculation is irresponsible, but I do want to emphasize that some of these details will be subject to change.



An OSCAL Vision for FPKI

Tooling

FPKI

FPKIPA

Catalog/ Profile

Bridge CP

CA

PA

Auditor

Catalog/ Profile

Sys. Sec. Plan

CP

Existing CPS

SAP

SAR

POAM

Annual Review Package

Component Definition

* Some details subject to change

We’ve seen the players in the PKI space – let’s pick an independent CA, since it’s the most complicated from a process and artifact perspective.

Here are the present-day artifacts that are produced, and here are the OSCAL equivalents.

The major difference when you replace unstructured artifacts with structured artifacts is the ability to introduce a wider array of tooling.

Tooling can convert existing Policy documentation into an OSCAL structured representation

Tooling can enable vendors or system owners to document component definitions. System owners can enhance their system security plans with the component definitions, and automatically update the System Security Plan when the underlying component configuration changes.

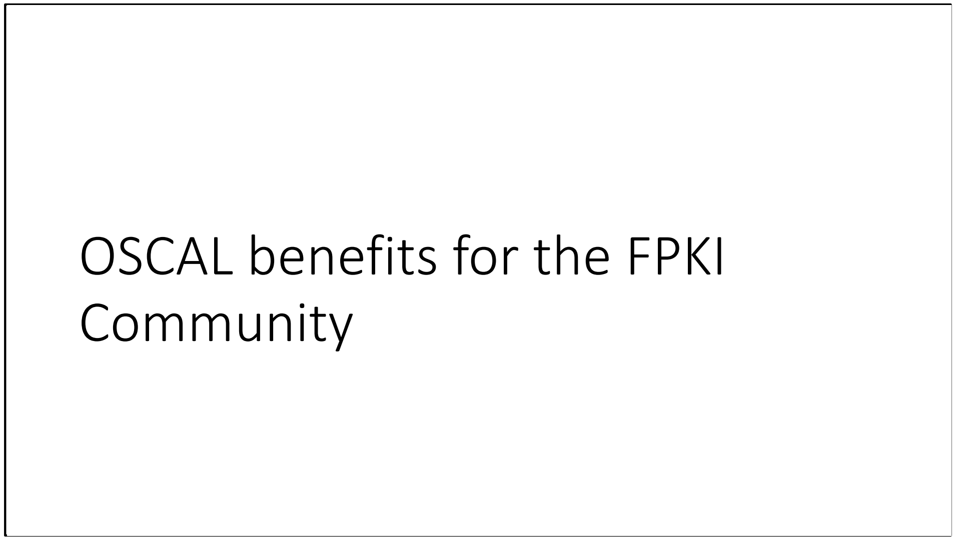
Tooling can facilitate the comparison of independent Policy documents, and this will lead to tool assisted document management.

Tooling can support compliance mapping of a CPS in the OSCAL System Security Plan format to the underlying policy documentation, and this means all of the documentation will benefit from tooling operating on structured representations. Which makes updating and managing the documentation much simpler, reduces the cost and time of the review and comparison process, and should lead to higher quality across the board.

The same tooling used to perform compliance mapping can support creation of audit artifacts.

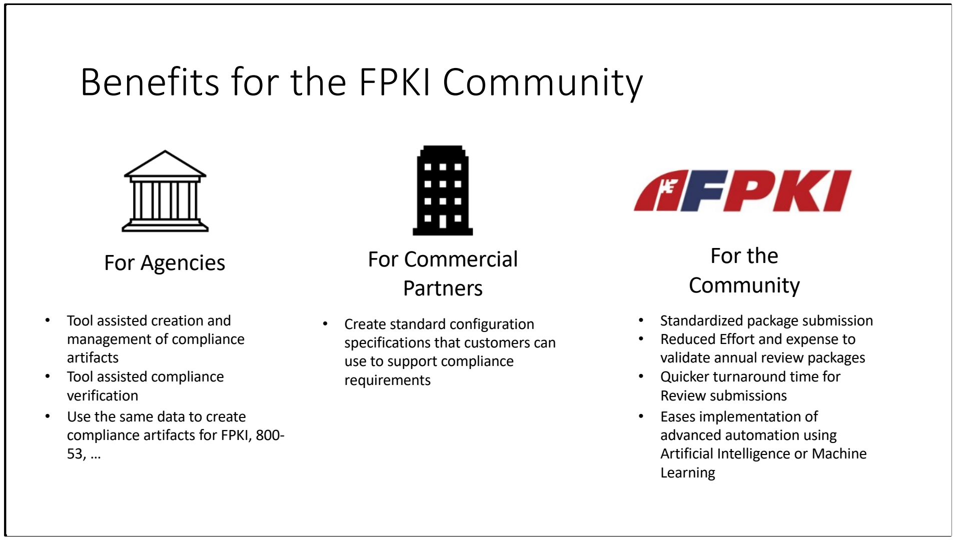
Finally, with everything now documented in a standard, structured representation, production of the annual review package will only require someone to press an "Export" button.

Automation is not new in this space – there are a variety of tools in use by members of the community – the difference is that OSCAL, as a standard that comprehensively addresses the entire compliance management process and all of the artifacts, can allow any tooling that is "OSCAL aware" to interoperate. Because OSCAL is an open, royalty-free standard, any vendor can add OSCAL support to their tool, and any participant can create a tool using several available open-source implementations to suit their own needs.



OSCAL benefits for the FPKI Community

I’ve already started describing the benefits, let’s go over them again.



Benefits for the FPKI Community

For Agencies

- Tool assisted creation and management of compliance artifacts
- Tool assisted compliance verification
- Use the same data to create compliance artifacts for FPKI, 800-53, …

For Commercial Partners

- Create standard configuration specifications that customers can use to support compliance requirements

For the Community

- Standardized package submission
- Reduced Effort and expense to validate annual review packages
- Quicker turnaround time for Review submissions
- Eases implementation of advanced automation using Artificial Intelligence or Machine Learning

Agencies will get the benefit of tooling to manage their Federal PKI compliance artifacts, and the verification processes can use the same data, even if a different tool is used.

THIS ONE IS IMPORTANT! No one is subject to only one set of compliance requirements. Every CA or Registration Authority operated by an agency is subject to multiple sets of requirements. Leveraging the OSCAL standard means that you can reuse your FPKI compliance artifacts for your 800-53 compliance processes, and to support any other compliance regime that has an OSCAL representation

For Commercial partners and vendors, you'll get the same benefits that Amazon, Google and Microsoft have gotten in the FedRAMP space.

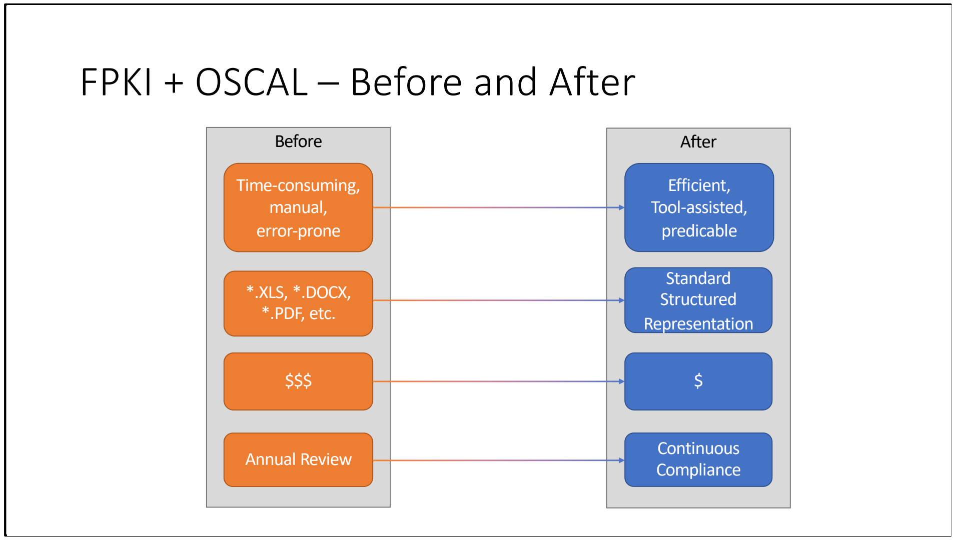
You can provide structured documentation of the controls addressed by your product or service, and this documentation can be directly imported into your customers' compliance documents – there is no more disconnect between the configuration recommendations and the compliance automation tooling.

Vendors and the open source community are working on automatic generation of component definitions from infrastructure as code artifacts like docker files, ansible playbooks and Kubernetes kubeconfig files.

This could produce automatic generation of compliance documentation by the components of your PKI

For the community as a whole, the standardization of package submission formats is already a benefit, but will directly contribute to several secondary benefits:

1. Faster, cheaper validation of annual review packages
2. Quicker turnaround for annual review submissions, with simpler tracking of outstanding issues and findings. This has been the major benefit realized by FedRAMP
3. Implementing structured representations for the whole stack makes automation by AI/ML much simpler when compared to unstructured, inconsistently formatted blobs. Okay, this one is a little futuristic, but we can make the future easier by investing in OSCAL.



FPKI + OSCAL – Before and After

Before

Time-consuming, manual, error-prone

*.XLS, *.DOCX, *.PDF, etc.

$$$

Annual Review

After

Efficient, Tool-assisted, predicable

Standard Structured Representation

$

Continuous Compliance

Today, compliance processes are time-consuming, manual, and error-prone.

After OSCAL, they are efficient, tool-assisted and predictable.

Today artifacts are a mix of spreadsheets, and documents in a wide variety for formats

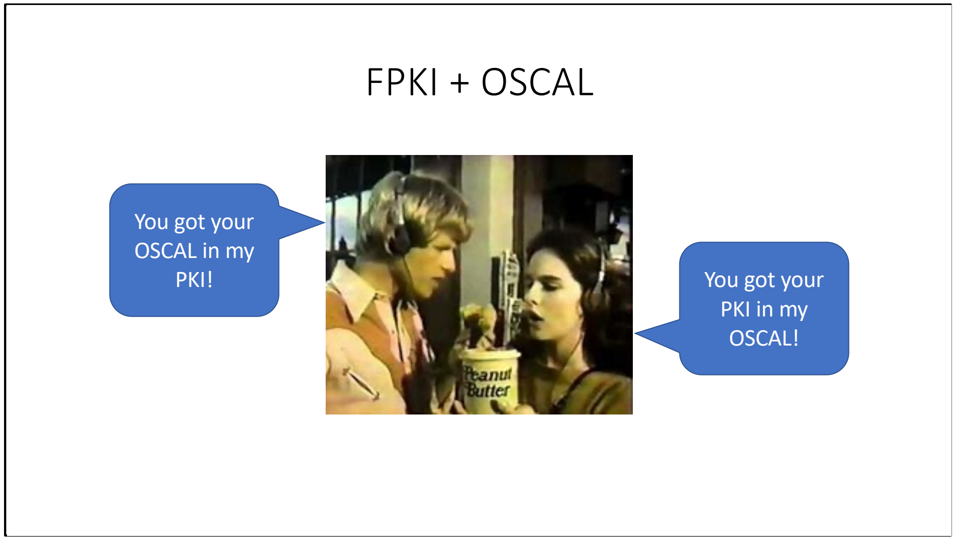
After OSCAL, there is a standard, structured representation of the compliance artifacts

Today, compliance management of FPKI is a big cost across the community.

Tomorrow, automation significantly reduces that cost

Today, we perform annual reviews, because frankly, doing this once a year is about all anyone can take.

In the future, we could replace an annual review with continuous compliance.



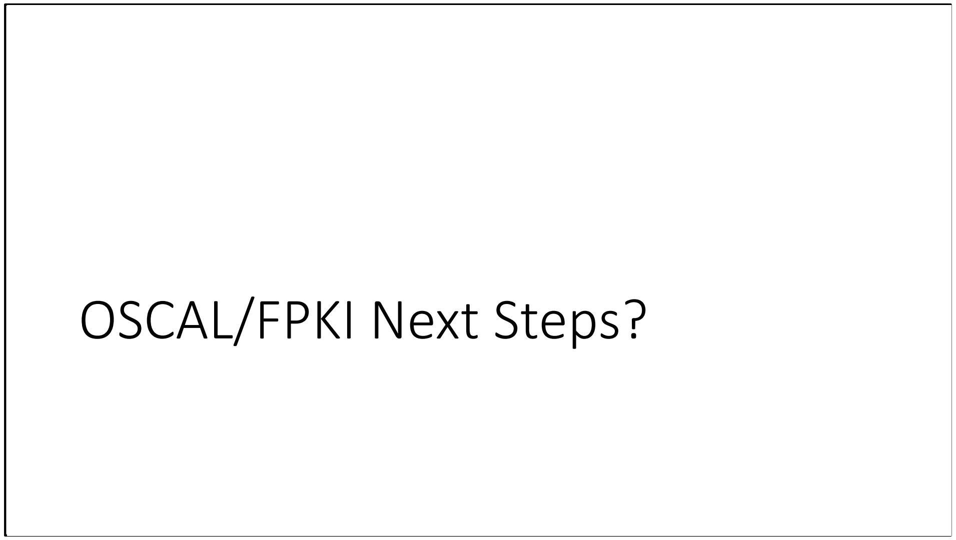
FPKI + OSCAL

You got your OSCAL in my PKI!

You got your PKI in my OSCAL!

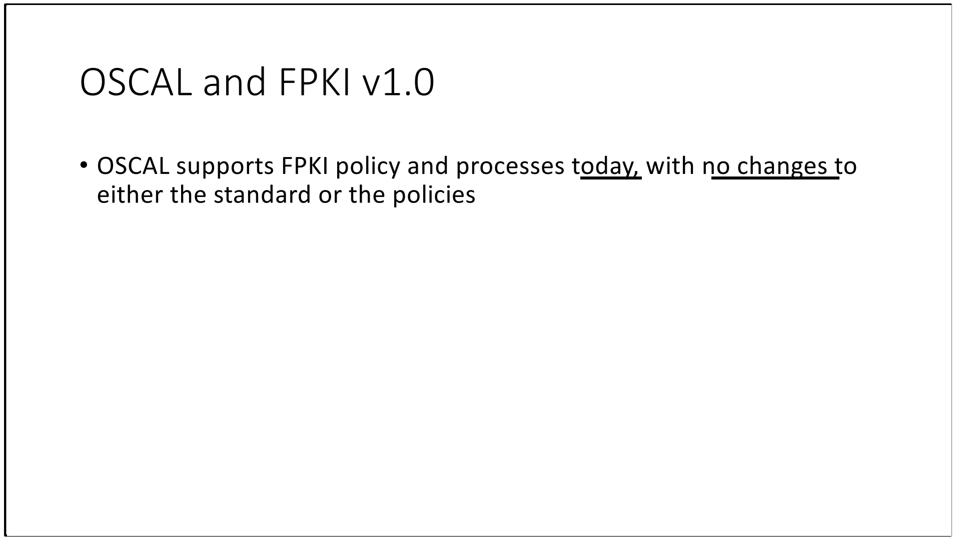
Peanut Butter

Like peanut butter and chocolate!



OSCAL/FPKI Next Steps?

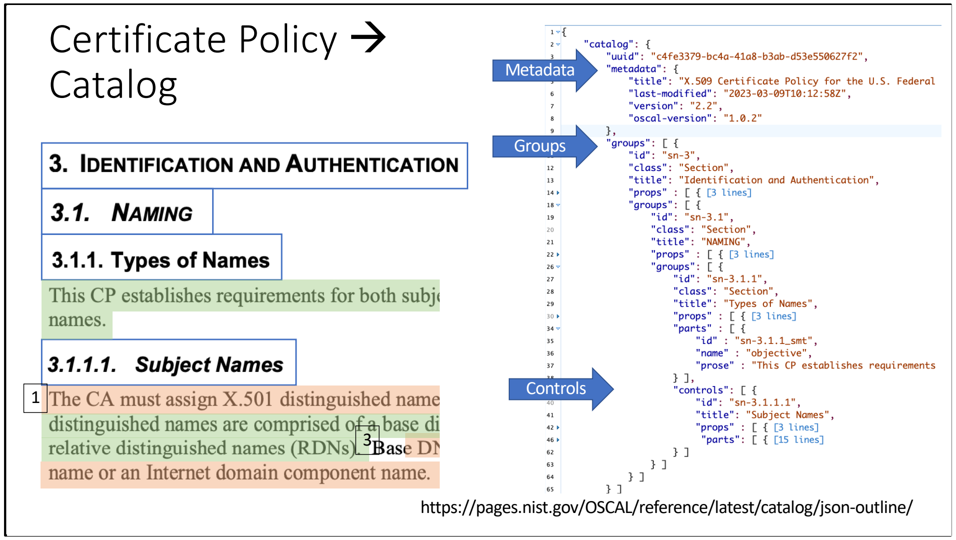
Hopefully you're all sold, so let's talk about how we can get there.



OSCAL and FPKI v1.0

- OSCAL supports FPKI policy and processes today, with no changes to either the standard or the policies

Good news. OSCAL can support PKI today with no changes



Certificate Policy → Catalog

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

This CP establishes requirements for both subj
names.

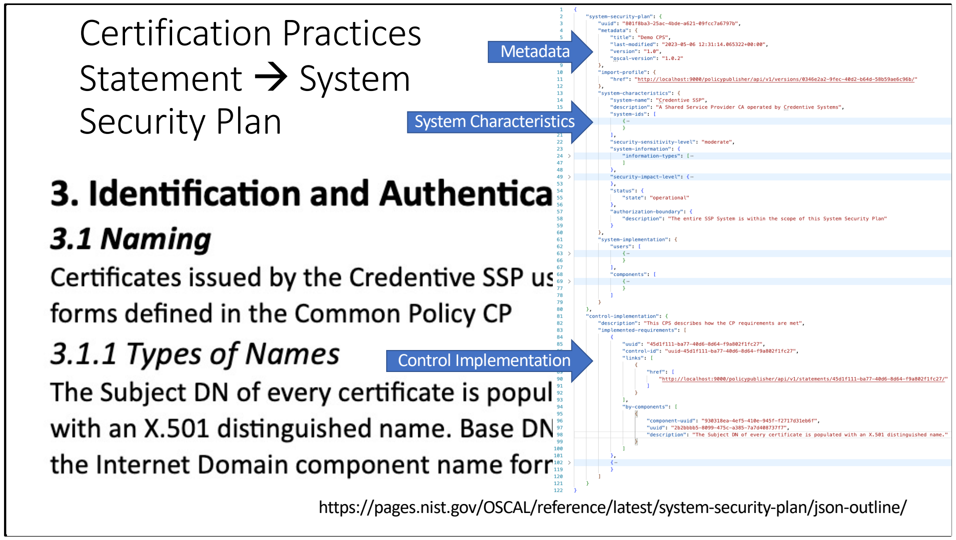
3.1.1.1. Subject Names

The CA must assign X.501 distinguished name
distinguished names are comprised of a base di
relative distinguished names (RDNs). Base DN
name or an Internet domain component name.

```
{
    "catalog": {
        "uuid": "c4fe3379-bc4a-41a8-b3ab-d53e550627f2",
        "metadata": {
            "title": "X.509 Certificate Policy for the U.S. Federal
            "last-modified": "2023-03-09T10:12:58Z",
            "version": "2.2",
            "oscal-version": "1.0.2"
        },
        "groups": [ {
            "id": "sn-3",
            "class": "Section",
            "title": "Identification and Authentication",
            "props" : [ { [3 lines]
            "groups": [ {
                "id": "sn-3.1",
                "class": "Section",
                "title": "NAMING",
                "props" : [ { [3 lines]
                "groups": [ {
                    "id": "sn-3.1.1",
                    "class": "Section",
                    "title": "Types of Names",
                    "props" : [ { [3 lines]
                    "parts" : [ {
                        "id" : "sn-3.1.1_smt",
                        "name" : "objective",
                        "prose" : "This CP establishes requirements
                    } ],
                    "controls": [ {
                        "id": "sn-3.1.1.1",
                        "title": "Subject Names",
                        "props" : [ { [3 lines]
                         "parts": [ { [15 lines]
                    } ]
                } ]
            } ]
        } ]
```

https://pages.nist.gov/OSCAL/reference/latest/catalog/json-outline/

Here, for example, is a section of the Certificate Policy represented as an OSCAL Catalog



Certification Practices Statement → System Security Plan

3. Identification and Authentica

3.1 Naming

Certificates issued by the Credentive SSP us
forms defined in the Common Policy CP

3.1.1 Types of Names

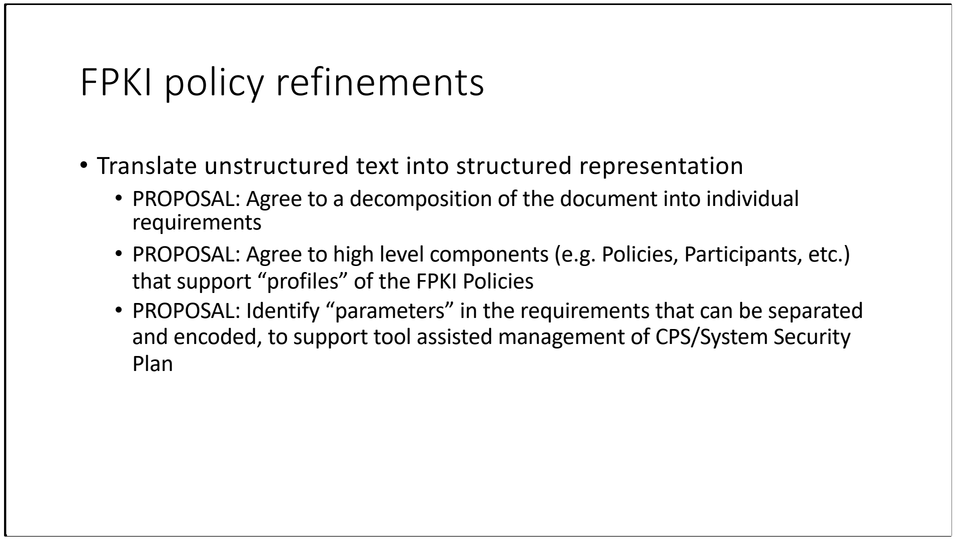
The Subject DN of every certificate is popul
with an X.501 distinguished name. Base DN
the Internet Domain component name forr

```
{
    "system-security-plan": {
        "uuid": "801f8ba3-25ac-4bde-a621-09fcc7a6797b",
        "metadata": {
            "title": "Demo CPS",
            "last-modified": "2023-05-06 12:31:14.065322+00:00",
            "version": "1.0",
            "oscal-version": "1.0.2"
        },
        "import-profile": {
            "href": "http://localhost:9000/policypublisher/api/v1/versions/0346e2a2-9fec-40d2-b64d-58b59ae6c96b/"
        },
        "system-characteristics": {
            "system-name": "Credentive SSP",
            "description": "A Shared Service Provider CA operated by Credentive Systems",
            "system-ids": [
                {⋯
                }
            ],
            "security-sensitivity-level": "moderate",
            "system-information": {
                "information-types": [⋯
                ]
            },
            "security-impact-level": {⋯
            },
            "status": {
                "state": "operational"
            },
            "authorization-boundary": {
                "description": "The entire SSP System is within the scope of this System Security Plan"
            }
        },
        "system-implementation": {
            "users": [
                {⋯
                }
            ],
            "components": [
                {⋯
                }
            ]
        }
    },
    "control-implementation": {
        "description": "This CPS describes how the CP requirements are met",
        "implemented-requirements": [
            {
                "uuid": "45d1f111-ba77-40d6-8d64-f9a802f1fc27",
                "control-id": "uuid-45d1f111-ba77-40d6-8d64-f9a802f1fc27",
                "links": [
                    {
                        "href": [
                            "http://localhost:9000/policypublisher/api/v1/statements/45d1f111-ba77-40d6-8d64-f9a802f1fc27/"
                        ]
                    }
                ],
                "by-components": [
                    {
                        "component-uuid": "930318ea-4ef5-410e-945f-f2717d31eb6f",
                        "uuid": "2b2bbbb5-8099-475c-a385-7a7d408737f7",
                        "description": "The Subject DN of every certificate is populated with an X.501 distinguished name."
                    }
                ]
            },
            {⋯
            }
        ]
    }
}
```

https://pages.nist.gov/OSCAL/reference/latest/system-security-plan/json-outline/

Here, you see a fictional CPS represented as a System Security Plan.

Again, the details may change, but this is not a heavy lift



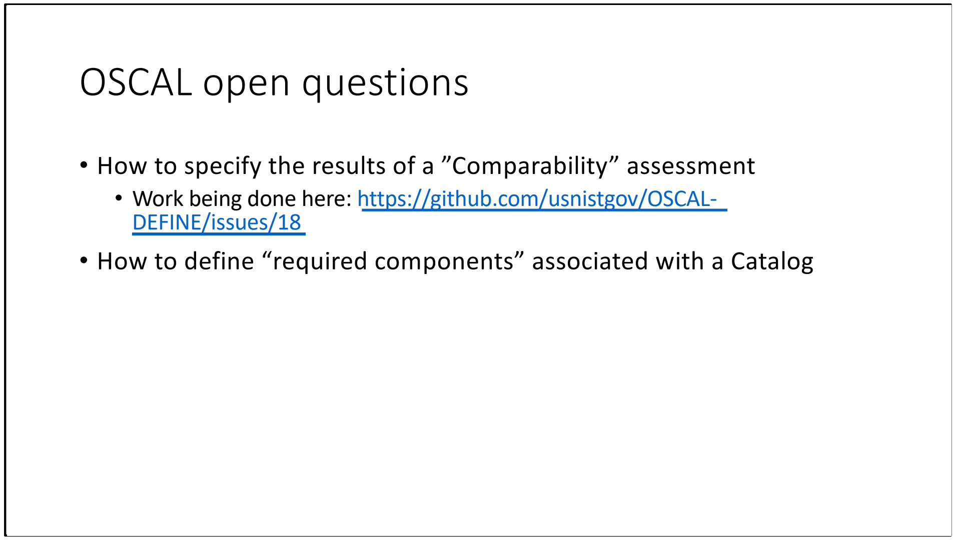
FPKI policy refinements

- Translate unstructured text into structured representation
  - PROPOSAL: Agree to a decomposition of the document into individual requirements
  - PROPOSAL: Agree to high level components (e.g. Policies, Participants, etc.) that support “profiles” of the FPKI Policies
  - PROPOSAL: Identify “parameters” in the requirements that can be separated and encoded, to support tool assisted management of CPS/System Security Plan

However, we can make it better with a little careful thought.

A few extra steps could help us translate our unstructured text into a structured representation.

First, we need to extract the pieces of the structure from the current, narrative oriented document
Second, we can make the entire process simpler by defining the high level components and capabililties that will support creation of profiles
Third, we can adopt a couple of features from 800-53 to help with the documentation – especially parameterization of the requirements.



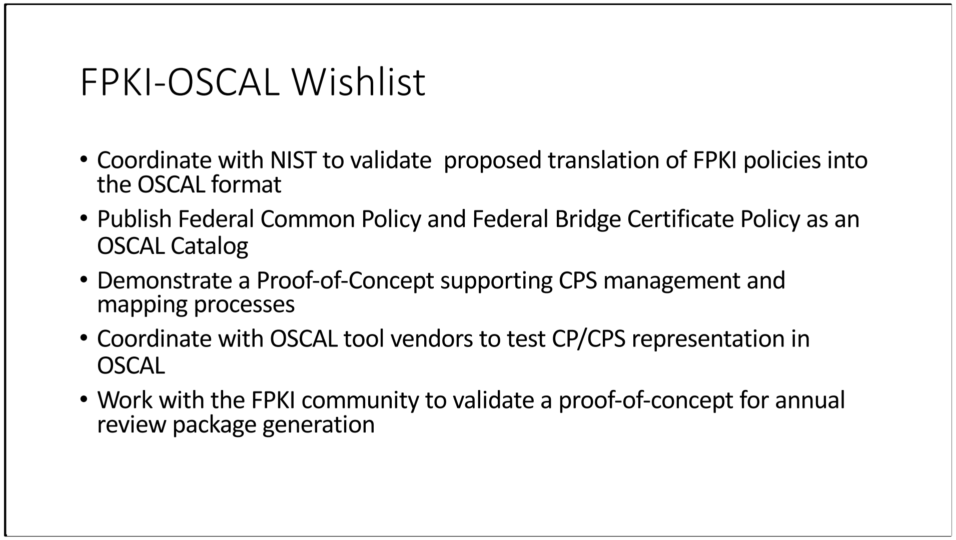
OSCAL open questions

- How to specify the results of a ”Comparability” assessment
  - Work being done here: https://github.com/usnistgov/OSCAL-DEFINE/issues/18
- How to define “required components” associated with a Catalog

There are some open questions that I am working on with the OSCAL team and community.

How do we specify the results of a comparability assessment? We talked about compliance mapping, how would we actually create and publish one? This under active discussion.

Second, how do we define “required components” that are associated with a catalog or profile. Remember component definitions are part of the Implementation layer. This being discussed by the team.



FPKI-OSCAL Wishlist

- Coordinate with NIST to validate proposed translation of FPKI policies into the OSCAL format
- Publish Federal Common Policy and Federal Bridge Certificate Policy as an OSCAL Catalog
- Demonstrate a Proof-of-Concept supporting CPS management and mapping processes
- Coordinate with OSCAL tool vendors to test CP/CPS representation in OSCAL
- Work with the FPKI community to validate a proof-of-concept for annual review package generation

This is the obligatory call to action.

First, coordination with NIST is important to ensure that any fpki specific features are implemented in a way that maximizes interoperability.

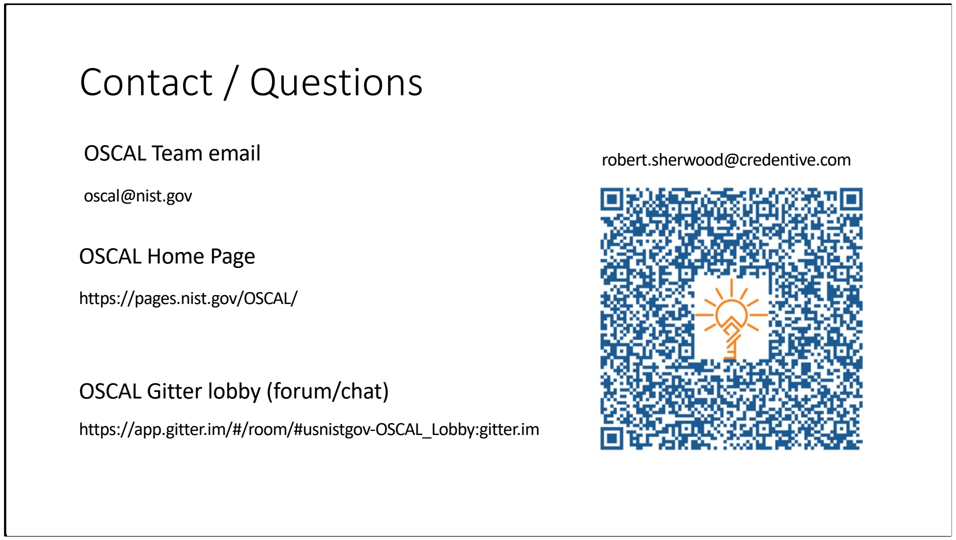
Second, Common Policy and the Federal Bridge Certificate Policy should be published as oscal Catalogs.

Third, the process of comparing CPs to CPs or CPs to CPSs involves a number of, let’s call them “peculiarities”. But, a proof of concept, If done publicly and openly, would help to demonstrate that it’s feasible, and clarify any issues.

Fourth – the benefit of OSCAL vs other standards is the wide array of supporting tools. We should validate that the current generation of tools can consume an FPKI flavored Catalog and System Security Plan

Fifth – A proof of concept for an end-to-end annual review process leveraging OSCAL artifacts would help to uncover issues and quantify the expected benefits.

Anyone interested in participating, or furthering the discussion of FPKI and OSCAL is encouraged to reach out.



Contact / Questions

OSCAL Team email

oscal@nist.gov

OSCAL Home Page

https://pages.nist.gov/OSCAL/

OSCAL Gitter lobby (forum/chat)

https://app.gitter.im/#/room/#usnistgov-OSCAL_Lobby:gitter.im

robert.sherwood@credentive.com