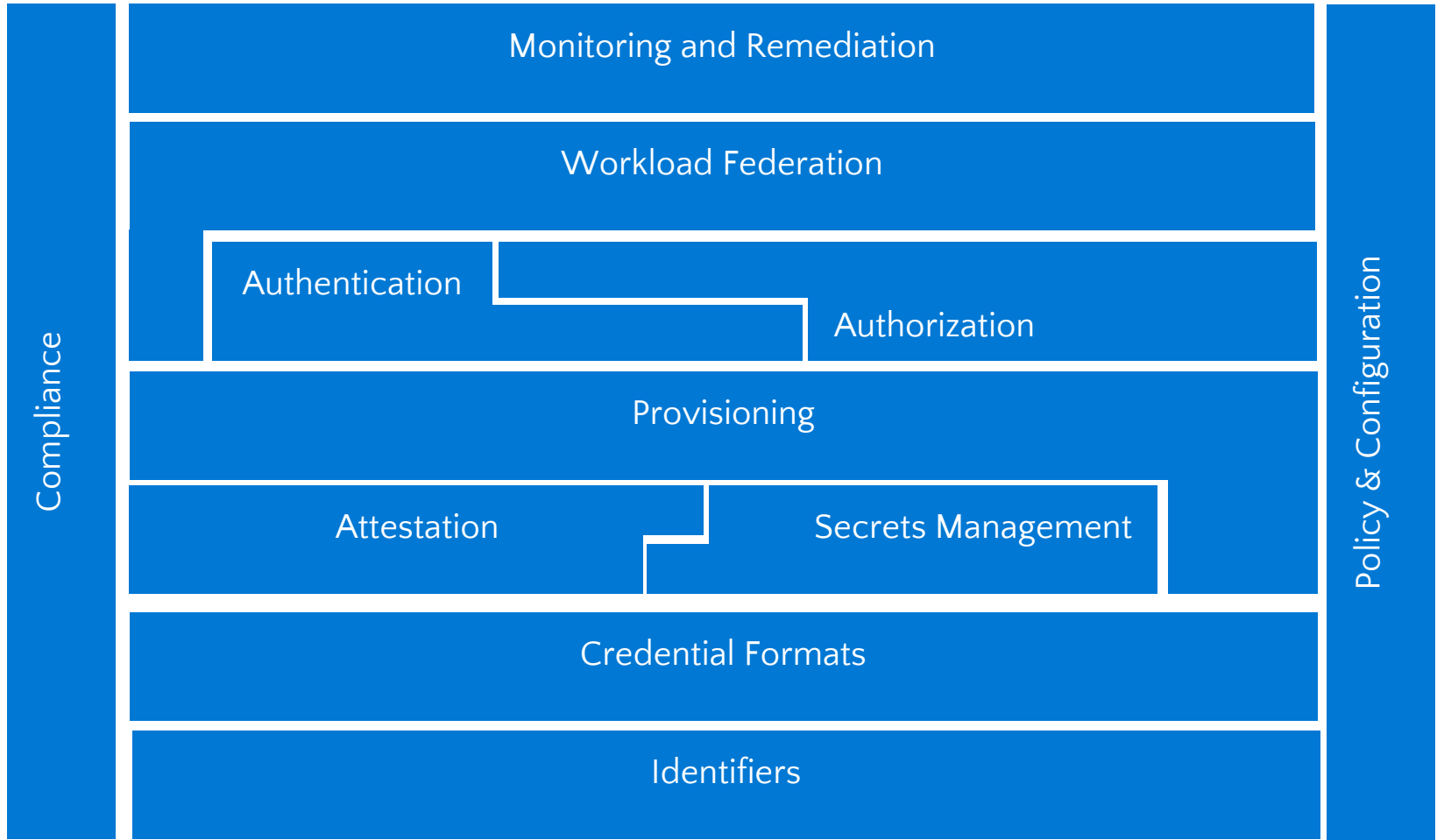# Connecting Identity Ecosystems

IETF 118
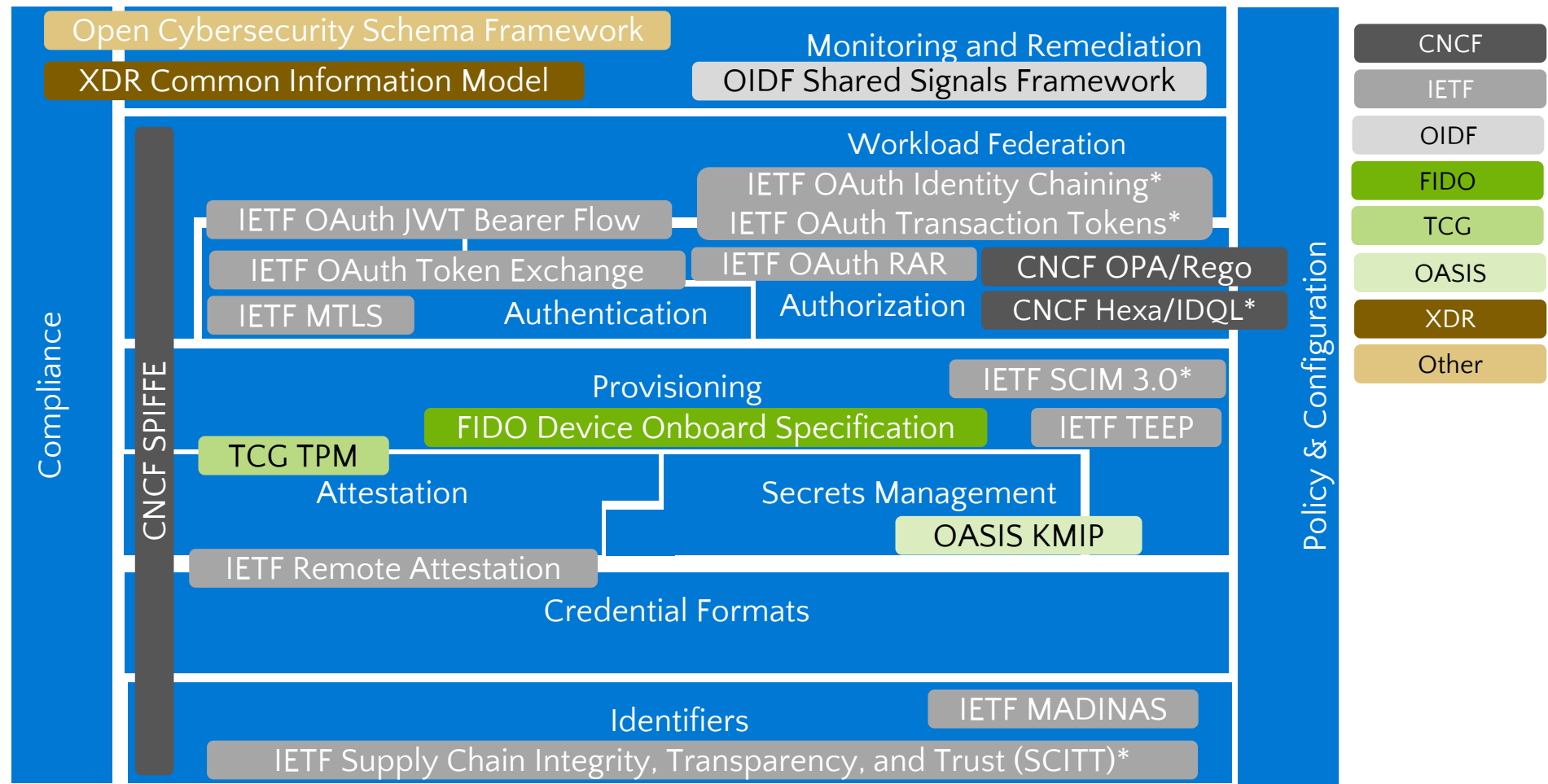
Pieter Kasselman
Workload Identity Enthusiast
Microsoft
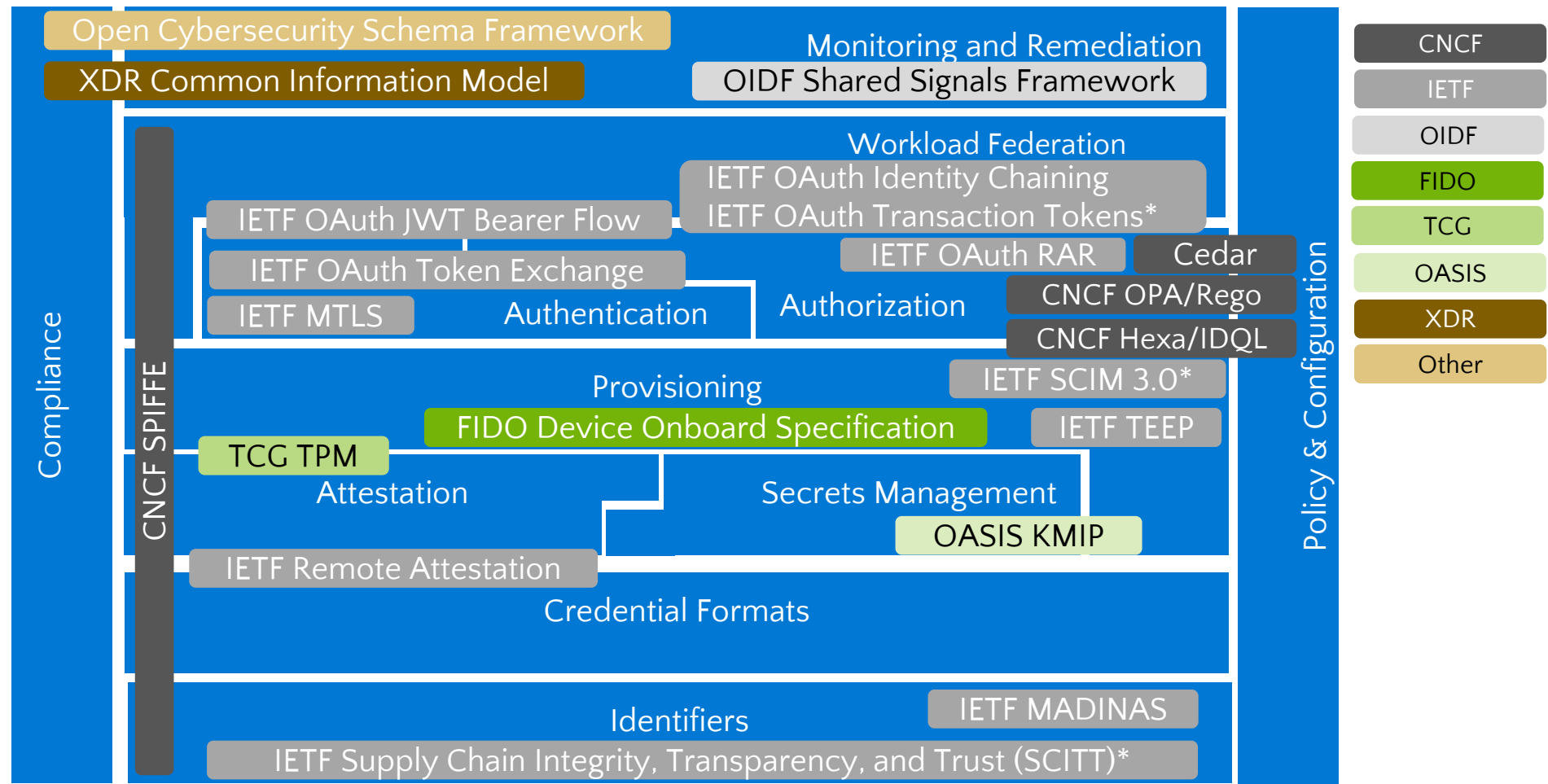
We need standards for….

We are not starting from scratch….
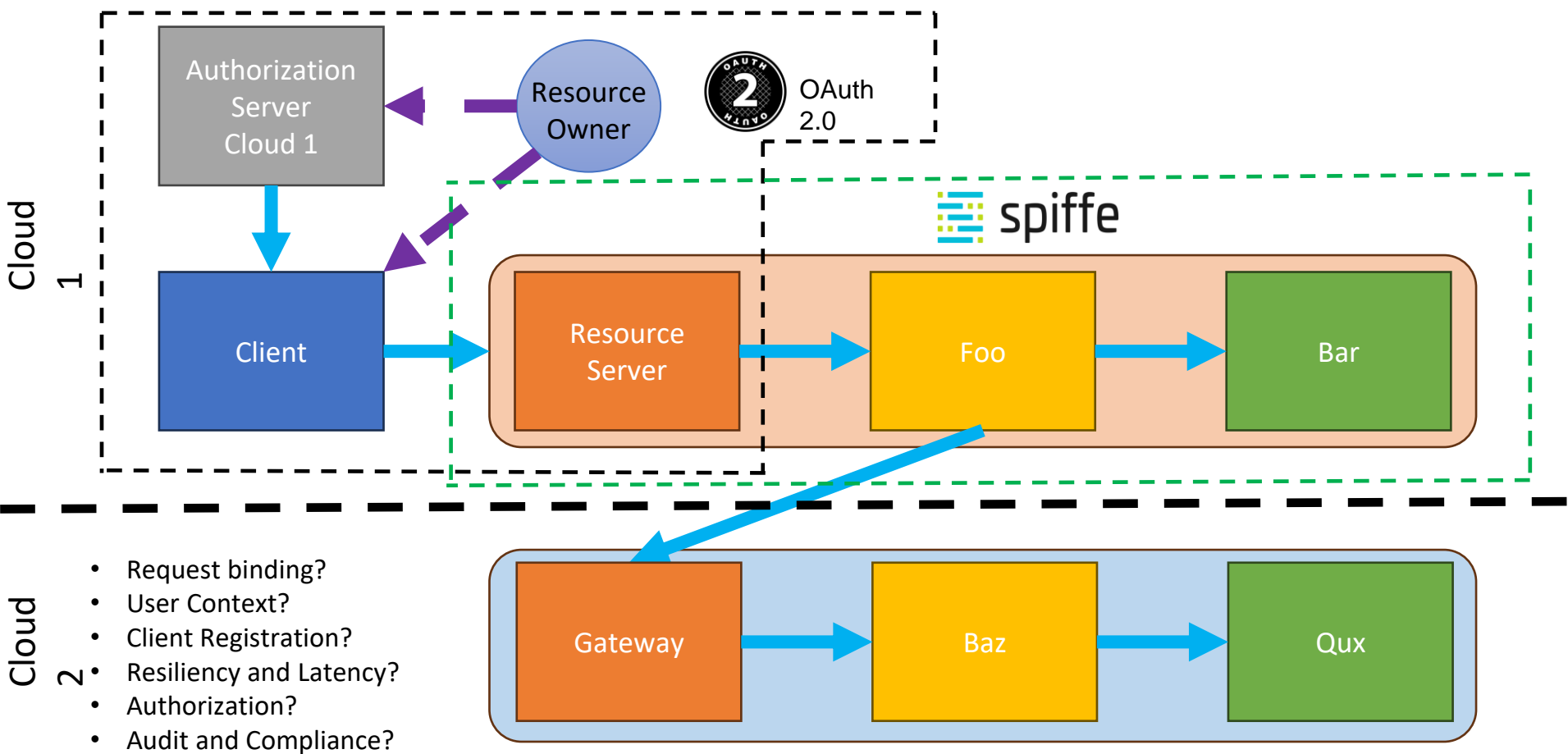
We are not starting from scratch….

Open Cybersecurity Schema Framework

XDR Common Information Model

Monitoring and Remediation

OIDF Shared Signals Framework

Compliance

CNCF SPIFFE

Workload Federation

IETF OAuth Identity Chaining

IETF OAuth Transaction Tokens*

IETF OAuth JWT Bearer Flow

IETF OAuth Token Exchange

IETF OAuth RAR

Cedar

CNCF OPA/Rego

IETF MTLS

Authentication

Authorization

CNCF Hexa/IDQL

IETF SCIM 3.0*

Provisioning

FIDO Device Onboard Specification

IETF TEEP

TCG TPM

Attestation

Secrets Management

OASIS KMIP

IETF Remote Attestation

Credential Formats

IETF MADINAS

Identifiers

IETF Supply Chain Integrity, Transparency, and Trust (SCITT)*

Policy & Configuration

CNCF

IETF

OIDF

FIDO
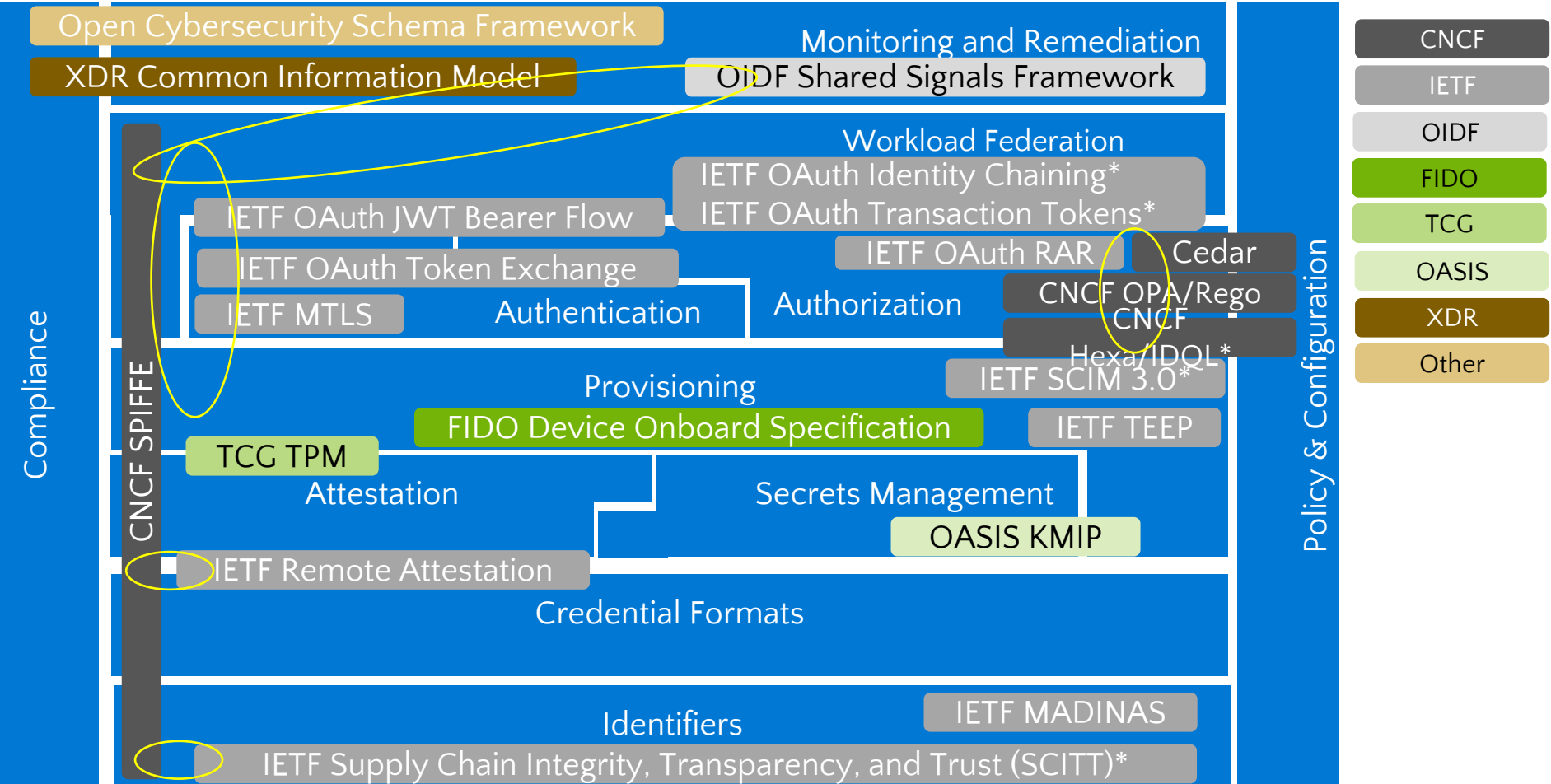
TCG

OASIS

XDR

Other

But…
mind the gap!

Going End-2-End does not quite line-up...

- Request binding?
- User Context?
- Client Registration?
- Resiliency and Latency?
- Authorization?
- Audit and Compliance?

Image Courtesy Justin Richer

Connecting standards…. And eco systems…

Open Cybersecurity Schema Framework

XDR Common Information Model

Monitoring and Remediation

OiDF Shared Signals Framework

Workload Federation

IETF OAuth Identity Chaining*

IETF OAuth JWT Bearer Flow

IETF OAuth Transaction Tokens*

IETF OAuth Token Exchange

IETF OAuth RAR

Cedar

CNCF OPA/Rego

IETF MTLS

Authentication

Authorization

CNCF Hexa/IDOL*

IETF SCIM 3.0*

Provisioning

FIDO Device Onboard Specification

IETF TEEP

TCG TPM

Attestation

Secrets Management

OASIS KMIP

IETF Remote Attestation

Credential Formats

Identifiers

IETF MADINAS

IETF Supply Chain Integrity, Transparency, and Trust (SCITT)*

Compliance

CNCF SPIFFE

Policy & Configuration

CNCF	
IETF	
OIDF	
FIDO	
TCG	
OASIS	
XDR	
Other	

Example: Request Binding

IETF 118

Evan Gilman
SPIFFE/SPIRE Contributor
SPIRL

Typical workload JWT

```
{
  "iss": "https://optional_oidc_compat.example.com"
  "sub": "some_meaningful_workload_identifier",
  "aud": ["some_meaningful_workload_identifier"],
  "iat": $(now)
  "exp": $(now + 5m),
}
```

DPoP proof example from spec

```
{
  "typ":"dpop+jwt",
  "alg":"ES256",
  "jwk": {
    "kty":"EC",
    "x":"l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
    "y":"9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA",
    "crv":"P-256"
  }
}
.
{
  "jti":"e1j3V_bKic8-LAEB",
  "htm":"GET",
  "htu":"https://resource.example.org/protectedresource",
  "iat":1562262618,
  "ath":"fUHyO2r2Z3DZ53EsNrWBb0xWXoaNy59IiKCAqksmQEo"
}
```

DPoP proof example from spec

```
{
  "typ":"dpop+jwt",
  "alg":"ES256",
  "jwk": {
    "kty":"EC",
    "x":"l8tFrhx-34tV3hRICRDY9zCkDlpBhF42UQUfWVAWBFs",
    "y":"9VE4jf_Ok_o64zbTTlcuNJajHmt6v9TDVrU0CdvGRDA",
    "crv":"P-256"
  }
}
.
{
  "jti":"e1j3V_bKic8-LAEB",
  "htm":"GET",
  "htu":"https://resource.example.org/protectedresource",
  "iat":1562262618,
  "ath":"fUHyO2r2Z3DZ53EsNrWBb0xWXoaNy59IiKCAqksmQEo"
}
```

~incompatible w/ workload auth

do we need a new spec?