The Journey to OpenID Federation 1.0 and the Road Ahead

Michael B. Jones
Giuseppe De Marco
Roland Hedberg

April 21, 2026

Structure of Today's Presentation

- Quick Overview of OpenID Federation Background and Goals
  - Touching on Spec Features Achieving Those Goals
- The Journey to OpenID Federation 1.0
- What's Next for OpenID Federation

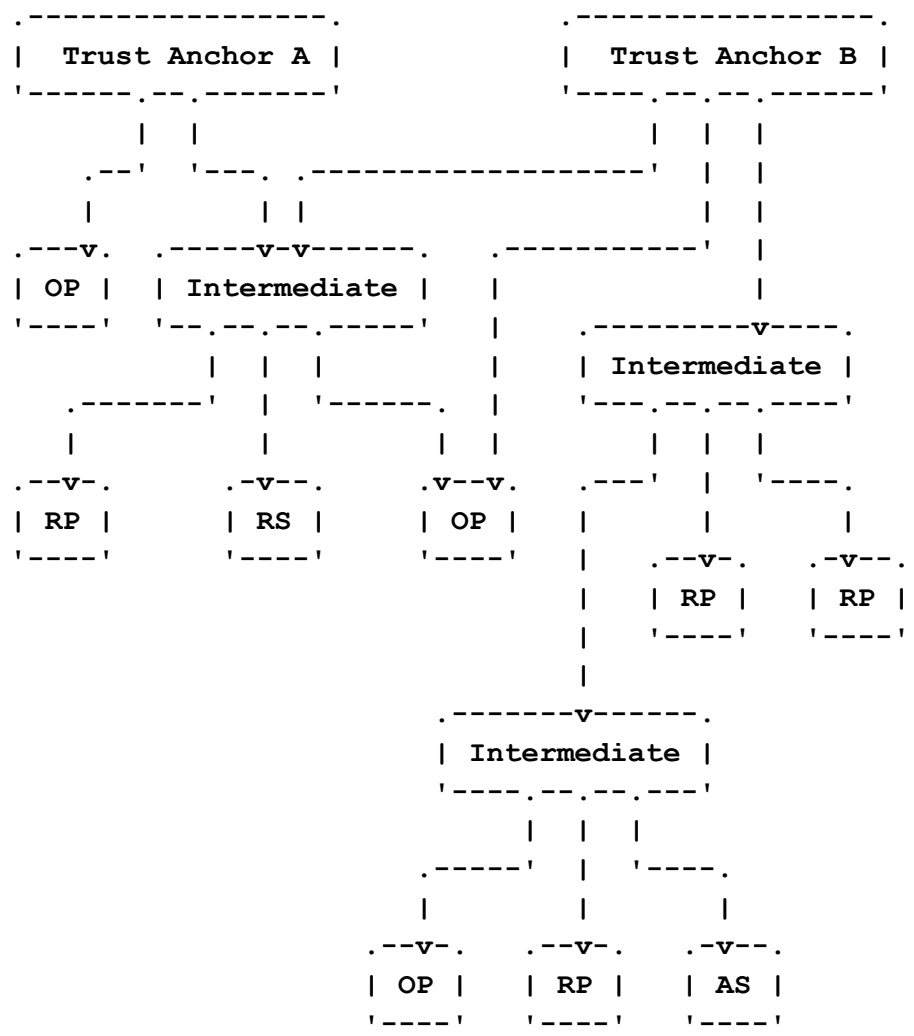
OpenID Federation

- OpenID Federation Specification
  - https://openid.net/specs/openid-federation-1_0.html
  - Enables establishment and maintenance of multi-lateral federations
- Incorporates lessons learned from SAML-based federations
  - Defines hierarchical JSON-based metadata structures for federation participants
  - Entities can be in multiple federations
  - Federations can be in federations

Establishing Trust within a Federation

- How do a Relying Party and an Identity Provider know that they're in the same federation?
  - Important for trust, liability, accountability, and reliability
- Shibboleth/SAML approach
  - Federation Operator polls participants for their metadata, concatenates it into a huge flat file, and distributes it to all nightly *(written in 2020)*
  - In production use, but brittle and not scalable
    - SAML world developing Metadata Query protocol to try to move away from this
- OpenID Federation approach
  - Hierarchical metadata, where organizations publish metadata about themselves and Federation Operators publish statements about subordinate organizations
  - Scalable, maintainable

Two Federations with Some Members in Common

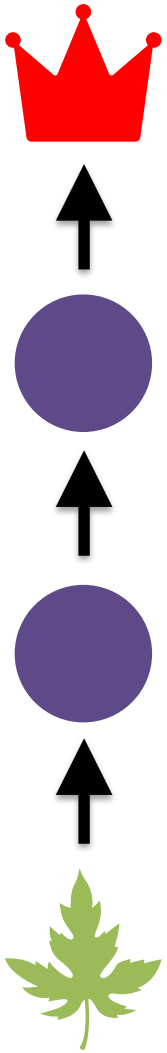


Use of Hierarchical Metadata

- Each leaf member publishes self-signed metadata about itself
  - Relying Parties
  - Identity Providers
  - Other Entity Types, such as those for wallet ecosystems
- Organizations publish signed metadata about the members that belong to them
- Federation operators publish signed metadata about orgs
- Inter-federations publish signed metadata about federations
- Hierarchical metadata is an online graph data structure

Trust Chains

- Participants follow metadata trust chains from leaves up to common roots, verifying signatures
- Both participants are members of a federation if a common Trust Anchor is found
- Participants can be members of multiple federations



Metadata Representation

- Each metadata statement is a signed JSON Web Token (JWT)
  - These are called Entity Statements
- They make statements about
  - The Entity itself
  - Keys used by the Entity
  - Policies of the Entity
  - Superior entities that they are willing to trust
    - This is how trust chains can be followed to federation roots

Example Entity Statement

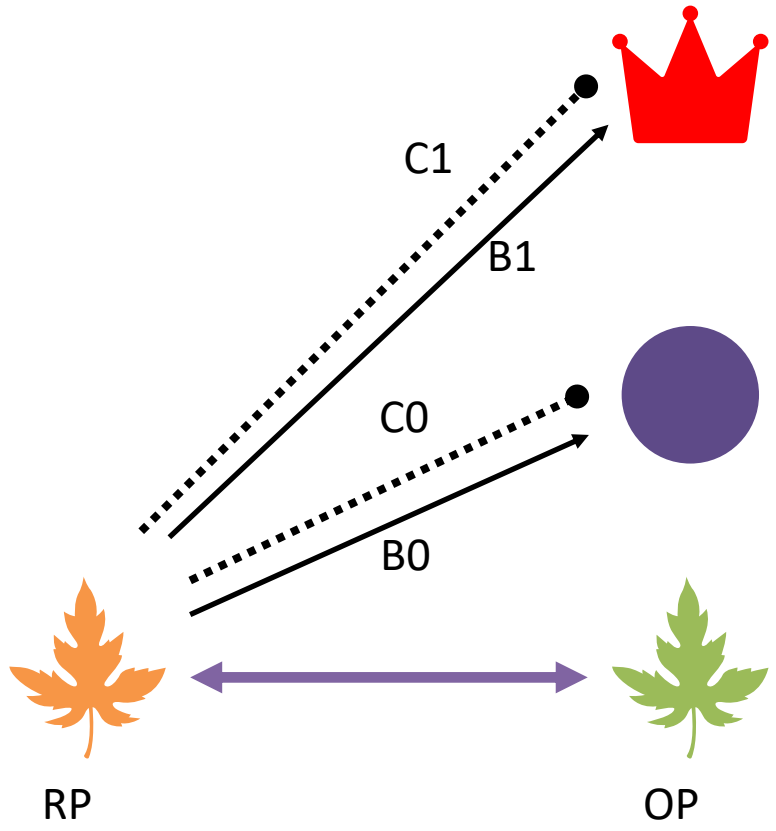

```
{
 "iss": "https://feide.no",
 "sub": "https://ntnu.no",
 "iat": 1516239022,
 "exp": 1516298022,
 "jti": "7l2lncFdY6SlhNia",
 "metadata_policy": {
    "openid_provider": {
      "issuer": {"value": "https://ntnu.no"},
      "organization_name": {"value": "NTNU"},
      "id_token_signing_alg_values_supported":
        {"subset_of": ["RS256", "RS384", "RS512"]},
    }
 },
  "jwks": {
    "keys": [
      {
        "e": "AQAB",
        "kid": "key1",
        "kty": "RSA",
        "n": "pnXBOusEANuug6ewezb9J_...",
        "use": "sig"
      }
    ]
  },
  "authority_hints": [
    "https://edugain.org/federation"
  ]
}
```

Collecting a Trust Chain

Start with self-signed Entity Statement – First Entity in Trust Chain

1. From the claim *authority_hints*, pick superior Entity
2. Grab superior's self-signed Entity Statement (using .well-known)
3. Request superior's view of subordinate (federation API). Add to the Trust Chain
4. GOTO 1

Repeat until superior is a trusted Trust Anchor

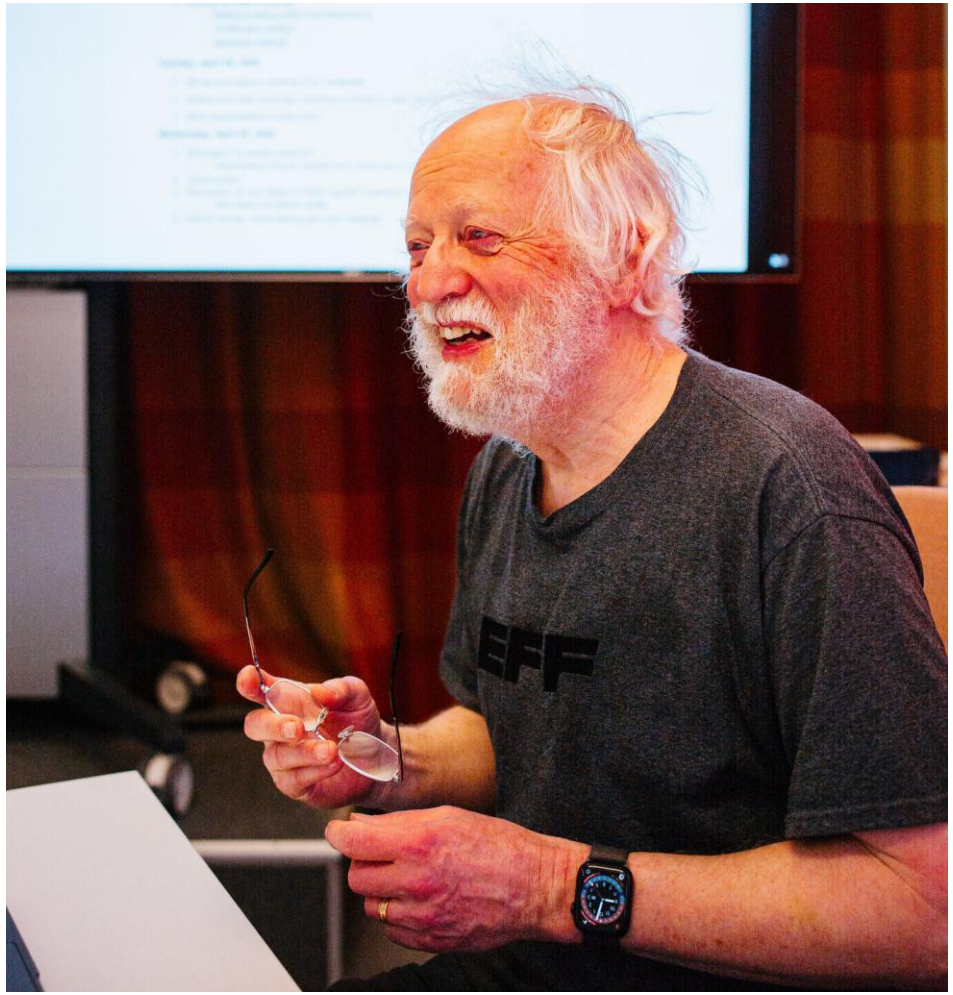


The Journey to OpenID Federation 1.0 and the Road Ahead

The Journey to OpenID Federation 1.0

- In the beginning, there was SAML
  - SAML 2.0 became a standard in March 2005
  - Leaders in R&E built multi-lateral federations using SAML
- Then along came OpenID Connect
  - OpenID Connect became a standard in February 2014
- At TNC 2016 in June, Lucy Lynch challenged Roland Hedberg:
  - “If there is someone who should be able to bring the eduGAIN identity federation into the new world of OpenID Connect, it is you.”
- Roland wrote first draft within months in late 2016

Roland Hedberg at the 2025 Interop Event at SUNET in Stockholm



Adding to the Early Editorial Team

- Mike Jones, John Bradley joined Roland Hedberg as editors in 2017
- Heather Flanagan (then RFC Editor) detailed review 2017
- First Implementer's Draft (draft 04) approved in January 2018
- Andreas Åkre Solberg of Uninett joined as editor in October 2018
  - Adding Implicit Registration (later renamed Automatic Registration)
  - Enables federated parties to interact without pre-registration
- Second Implementer's Draft (draft 10) approved in November 2019

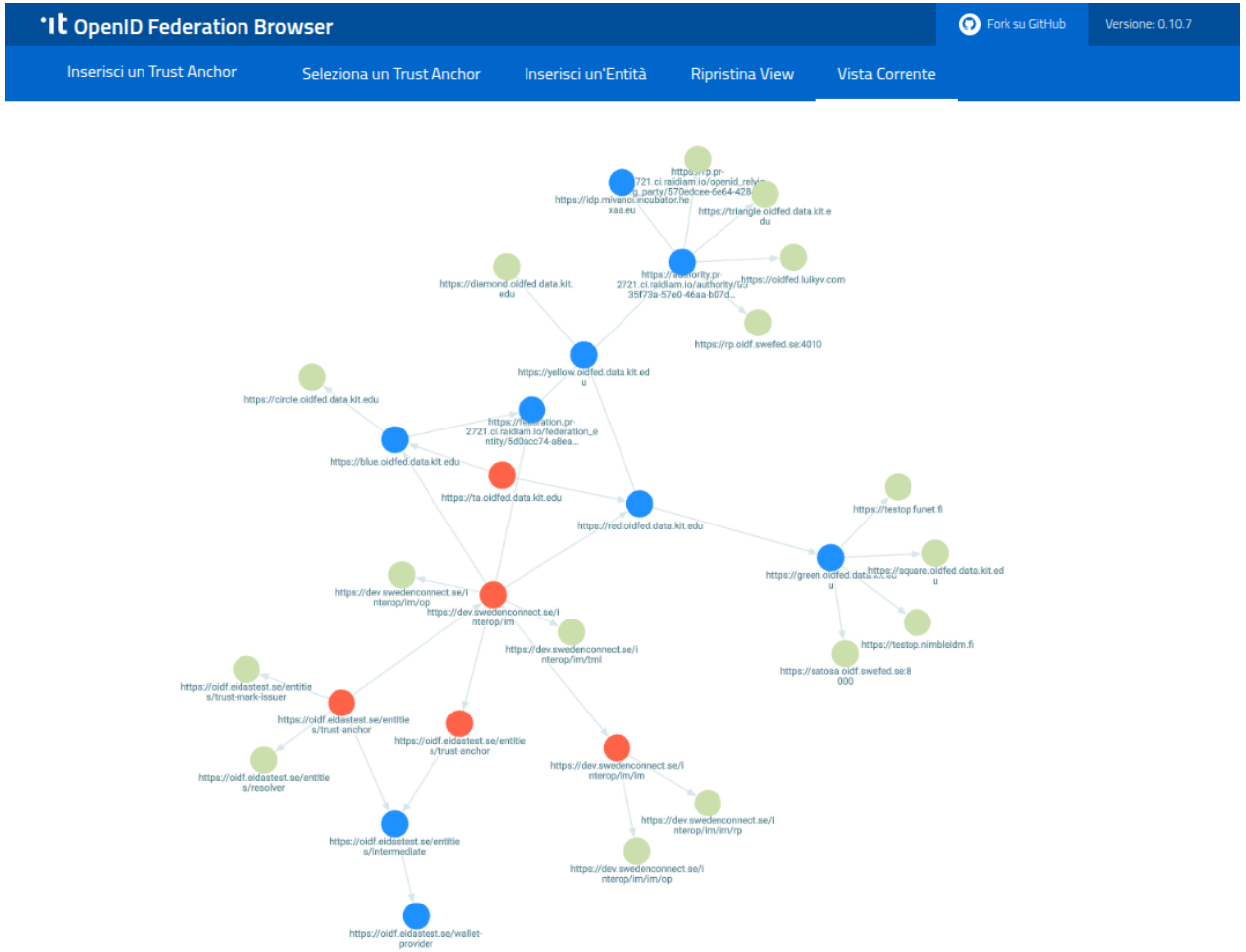
Federation Events Shaping the Spec

- Spec informed by discussions at many federation events
  - NORDUnet 2017, Copenhagen
  - SURFnet 2018, Utrecht
  - Internet2 Technology Exchange/REFEDS 2019, New Orleans
  - OpenID Japan Workshop 2020, Tokyo
  - GÉANT TNC/REFEDS 2022, Trieste
  - Internet2 Technology Exchange/REFEDS 2022, Denver
  - TIIME 2024, Copenhagen
  - Internet2 Technology Exchange/REFEDS 2025, Denver
  - TIIME 2026, Amsterdam

Interop Events Along the Journey

- Repeatedly interoperating among implementations refined spec
  - Much like five interops were held for OpenID Connect
  - Interop results were used to improve the specification
- Hackathon & interop with multiple implementations at Internet2/REFEDS 2019
- OpenID Foundation held three (virtual) interop events in 2020
- Third Implementer's draft (draft 17) approved September 2021
- Interop event in Stockholm at SUNET in April 2025
  - 30 participants, 14 implementations, 15 countries including AU, NZ!
  - Read about it at https://self-issued.info/?p=2697
- Interop event in Amsterdam at TIIME in February 2026
  - 12 people, 9 implementations, 9 countries
    - Croatia, Finland, Greece, Italy, Netherlands, Poland, Serbia, Sweden, US
  - Read about it at https://self-issued.info/?p=2807
  - *This one organized by the community – not the OpenID Foundation!*

OpenID Federation Browser View of KIT Federation during 2025 SUNET Interop



Significant Developments Mid-Journey

- Many open source implementations
  - See https://openid.net/developers/openid-federation-implementations/
- Trust Marks added, April 2020
- Connect2ID Server product implementation, August 2020
- Italy decided to use Third Implementer's Draft (draft 17) for national federations (SPID/CIE), 2022
- Giuseppe De Marco added as an editor, June 2022
- Vladimir Dzhuvinov added as an editor, October 2022
  - Tightened metadata policy processing
- Historical Keys Endpoint added, October 2022
- Authlete Server product implementation, January 2023
- "OpenID Connect Federation" became "OpenID Federation", October 2023
  - Recognizing that core functionality is protocol-independent

Gaining Momentum

- Italy decides to use OpenID Federation for EUDI Wallet
  - Giuseppe creates OpenID Federation Wallet Architectures spec
- Sweden decides to use OpenID Federation for multiple national federations, including healthcare
- Australia decides to use OpenID Federation for Open Banking / Open Finance
  - OpenID Federation Extended Subordinate Listing extension created
- Netherlands and Finland collaborate on a Federation profile
- Shibboleth OpenID Federation implementation
- eduGAIN OpenID Federation pilot

Pushing for Completion

- Fourth Implementer's Draft (draft 36) published, May 2024
  - Many cleanups made in preparation for this draft
  - Made what we believed would be the last sets of breaking changes
    - Including changing some parameter names for consistency
  - Read about the changes made at https://self-issued.info/?p=2560
- Draft underwent formal security analysis by University of Stuttgart
  - Something the OpenID Foundation believes is important
  - For instance, FAPI1, FAPI2 also analyzed
  - OpenID4VP specs will also be analyzed

Findings from 2024 Security Analysis

- Actionable vulnerability in audience values of Client Registration JWTs detected
  - https://openid.net/notice-of-a-security-vulnerability/
- Applies to:
  - OpenID Federation
  - OpenID Connect private_key_jwt registration
  - RFC 7523 (JWT Client Authentication)
  - RFC 9126 (Pushed Authorization Requests)
  - Client-Initiated Backchannel Authentication (CIBA)
- All have been or are being updated to address the vulnerability

Federation Integrity & Metadata Integrity

- 2024 Security Analysis also identified that two important federation properties may not hold
  - Federation Integrity and Metadata Integrity
  - Whether two parties interacting in a Federation are using the same Trust Chain and Metadata values
- Read about them at https://connect2id.com/blog/how-to-link-an-app-protocol-to-an-openid-federation-trust-layer
- `trust_chain` and `peer_trust_chain` header parameters were added to be able to ensure these properties

Long Journey from Almost Final to Final

- We thought we were essentially done in mid-2024 with ID4
- The security analysis told us differently
- Feedback from emerging deployments told us differently
- Stockholm interop event in April 2025 told us differently
- We kept getting more feature requests – not fewer!
- What to do…?

How We Finished

- We asked the clarifying question “Must this feature be in OpenID Federation 1.0?”
  - If a feature was essential for the core spec, we included it
  - If a feature could be done as a non-breaking extension, we left it for future work
  - If we hadn’t asked that question, we probably still wouldn’t be done

- OpenID Federation 1.0 became a standard February 17, 2026!

The Road Ahead

- Finishing one successful journey is often the start of the next
- Continued adoption is the next frontier
  - Application areas include authentication, digital wallets, open finance, and possibly AI agents
- Trust establishment with OpenID Federation is protocol independent
  - But protocol-specific profiles are needed to apply it in context

Protocol-Specific Federation Profiles

- OpenID Federation for OpenID Connect 1.1
  - Extracted OpenID Connect profile from OpenID Federation 1.0
  - Exactly equivalent to what's in 1.0, but editorially separated
  - Vote to approve as Final starts today!
- OpenID Federation for Wallet Architectures 1.0
  - Based on Italian EUDI Wallet choices
  - Finishing this specification is next priority on our journey

Federation Extensions in Progress

- OpenID Federation Extended Subordinate Listing
  - Extends OpenID Federation to facilitate listings of large numbers of subordinates
- OpenID Federation Subordinate Events Endpoint
  - Specifies a mechanism for Trust Anchors and Intermediates to publish historical events related to their Immediate Subordinates
- OpenID Federation Entity Collection
  - Defines an endpoint to retrieve a filterable list of all resolvable entities in a (sub-)federation. Useful for populating the set of IdPs in a Federation for home realm discovery user interfaces.

Second Security Analysis

- Security analysis of Final OpenID Federation 1.0 approved
  - University of Stuttgart security analysts have begun this work
  - Updates the formal model used in analysis to match final space
  - Will verify that audience security vulnerability fixed
  - Will verify that Federation Identity and Metadata Integrity achievable

OpenID Federation Testing Resources

- OpenID Certification Tests for OpenID Federation
  - https://openid.net/certification/federation_testing/
- Metadata tests created by Connect2ID
  - https://connect2id.com/blog/metadata-policy-test-vectors-openid-federation

OpenID Federation Resources

- OpenID Federation Specification
  - https://openid.net/specs/openid-federation-1_0.html
- My talk at TIIME 2026 describing OpenID Federation in detail
  - https://self-issued.info/?p=2805
- OpenID Connect Working Group Specifications
  - https://openid.net/wg/connect/specifications/
- OpenID Blog
  - https://openid.net/
- Mike Jones' Blog
  - https://self-issued.info/

Backup Slides

SAML vs. OpenID Federation

SAML

- Appearing in a metadata file means you are part of a federation

OpenID Federation

- Entities with Trust Chains up to the same Trust Anchor belong to the same federation

SAML vs. OpenID Federation

SAML

- An entity's complete metadata must be accepted by the federation operator for the entity to be allowed into the federation

OpenID Federation

- The federation operator sets the boundaries of what is acceptable

Policy Language for Entity Statements

- Policy Operators
  - `subset_of`
  - `one_of`
  - `superset_of`
  - `add`
  - `value`
  - `default`
  - `essential`
- Constraints
  - `max_path_length`
  - `naming_constraints`
  - `allowed_entity_types`

Applying Metadata Policies

- Policies applied top-down from root to leaves of trust chain
- Policies higher in the chain override those lower in the chain

- For instance, a Federation Operator might specify that only a particular set of signing algorithms may be used
  - Policies are applied to all subordinate entities in the federation

SAML vs. OpenID Federation

SAML

- It is rare that an entity belongs to more then one federation. I believe that eduGAIN recommends that an entity only belong to one.

OpenID Federation

- There is no drawback to belonging to multiple federations

SAML vs. OpenID Federation

SAML

- The is no metadata negotiation

OpenID Federation

- The RP proposes and the OP decides, subject to applicable policies from the Trust Chain