

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Klimaschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages

Gaia-X  
FEDERATION SERVICES  
GXFS



# Vertrauenswürdiges Gaia-X Ökosystem mit souveränen Identitäten und Notardiensten

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Klimaschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages

Gaia-X  
FEDERATION SERVICES  
GXFS



# Speakers



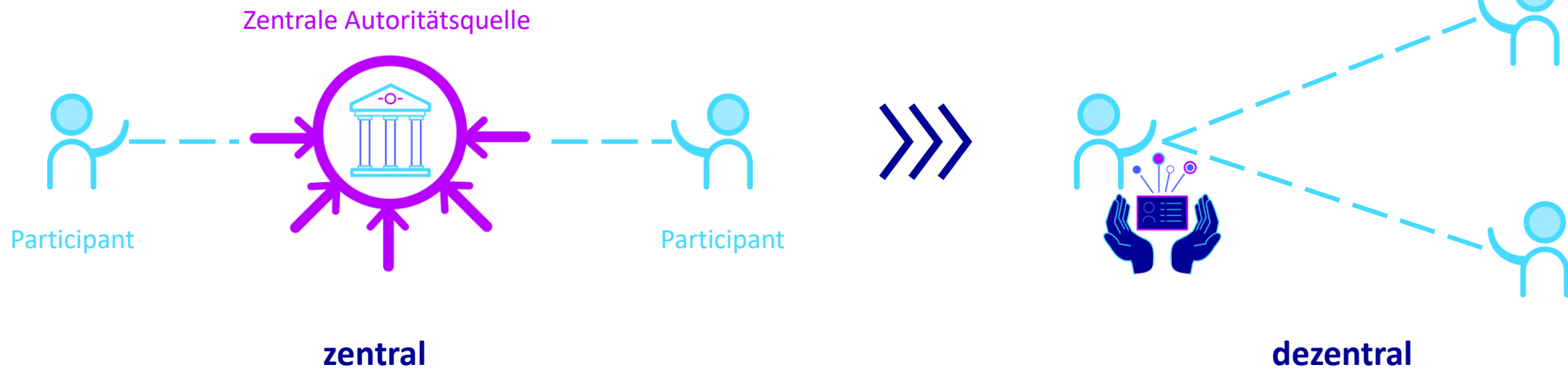
**Berthold Maier,**  
GXFS Experte „Identität & Vertrauen“



**Steffen Schulze,**  
GXFS Experte „Identität & Vertrauen“

# Gaia-X verfolgt ein Dezentrales Identitätsmanagement

- GXFS ermöglicht, Benutzer und Systeme auf vertrauenswürdige und dezentralisierte, selbstsouveräne Weise zu authentifizieren, ohne dass eine zentrale Autoritätsquelle benötigt wird
- Datenschutz nach DSGVO ist gewährleistet
- Verfolgung einer gemeinsamen EU-Strategie mit EBSI/ESSIF



# Wie funktioniert SSI?

- Triangle of Trust

- Issuer

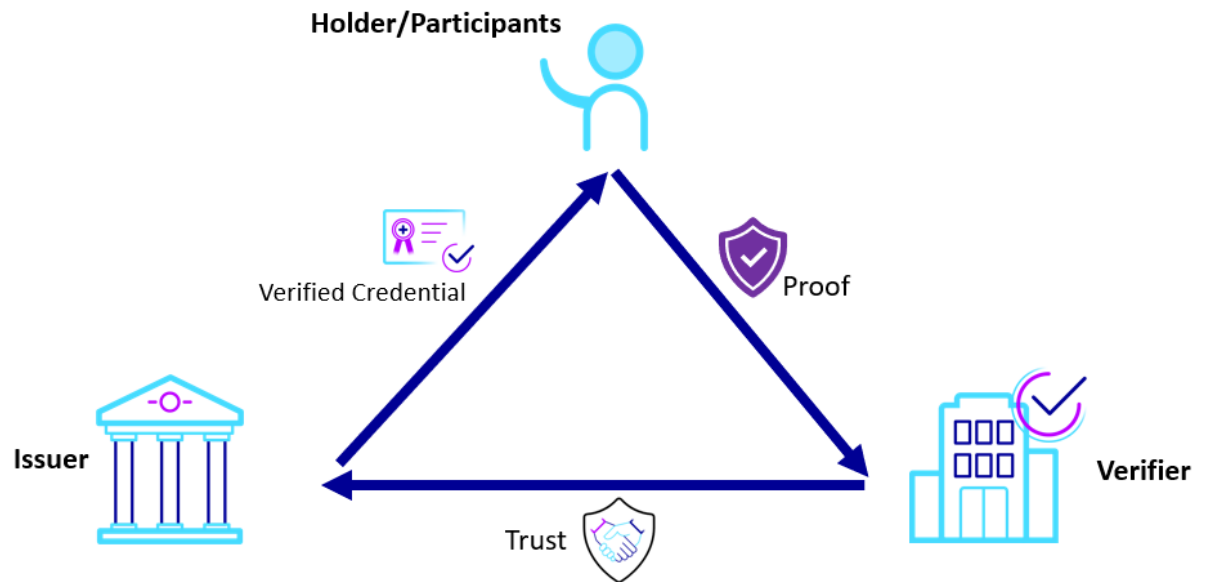
- Ausgabe von Beglaubigungen & überprüfbare digitale Anmeldeinformationen

- Holder

- Benutzer, Organisationen oder technische Geräte, die über legitimierte Anmeldeinformationen verfügen

- Verifier

- z.B. Verbraucher in Form einer Anwendung oder Person, die die Anmeldeinformationen benötigt



# GXFS Komponenten, wenn kein zentrales Identitätsmanagement mehr vorhanden ist

## Authentifizierungs- & Autorisierungsdienst



- ✓ Anfordern von verifizierbaren, dezentralen und kryptografischen Beglaubigungen sowie Identitätsattributen von anderen Teilnehmenden in einer Föderation

## Beglaubigungsmanager für Personen



- ✓ Selbstsouveränes Verwalten der eigenen Beglaubigungen z.B. Ausweisdokumente, Zertifikate oder Berechtigungen
- ✓ Authentifizieren mithilfe einer mobilen App oder einer Browseranwendung

## Registry

- ✓ Das Konzept der dezentralen Identität (DID) ermöglicht es Gaia-X, verschiedene dezentrale Registries - sogar Standard-Webdomänen - als weitere Vertrauensschicht zwischen den Akteuren zu nutzen



## Beglaubigungsmanager für Organisationen



- ✓ Konfigurieren eines selbstbestimmten und leichten Einstiegs in eine Föderation für Firmen durch z.B. eigenständiges Ausstellen und Verwalten von digitalen Teilnahme-Ausweisen an Angestellte



## Vertrauensdienste

- ✓ Durchsetzen von Nutzungsrichtlinien & Etablieren von regelbasiertem Vertrauen
- ✓ Sicherstellen von Vertrauensketten zwischen mehreren Teilnehmenden, Organisationen und Behörden



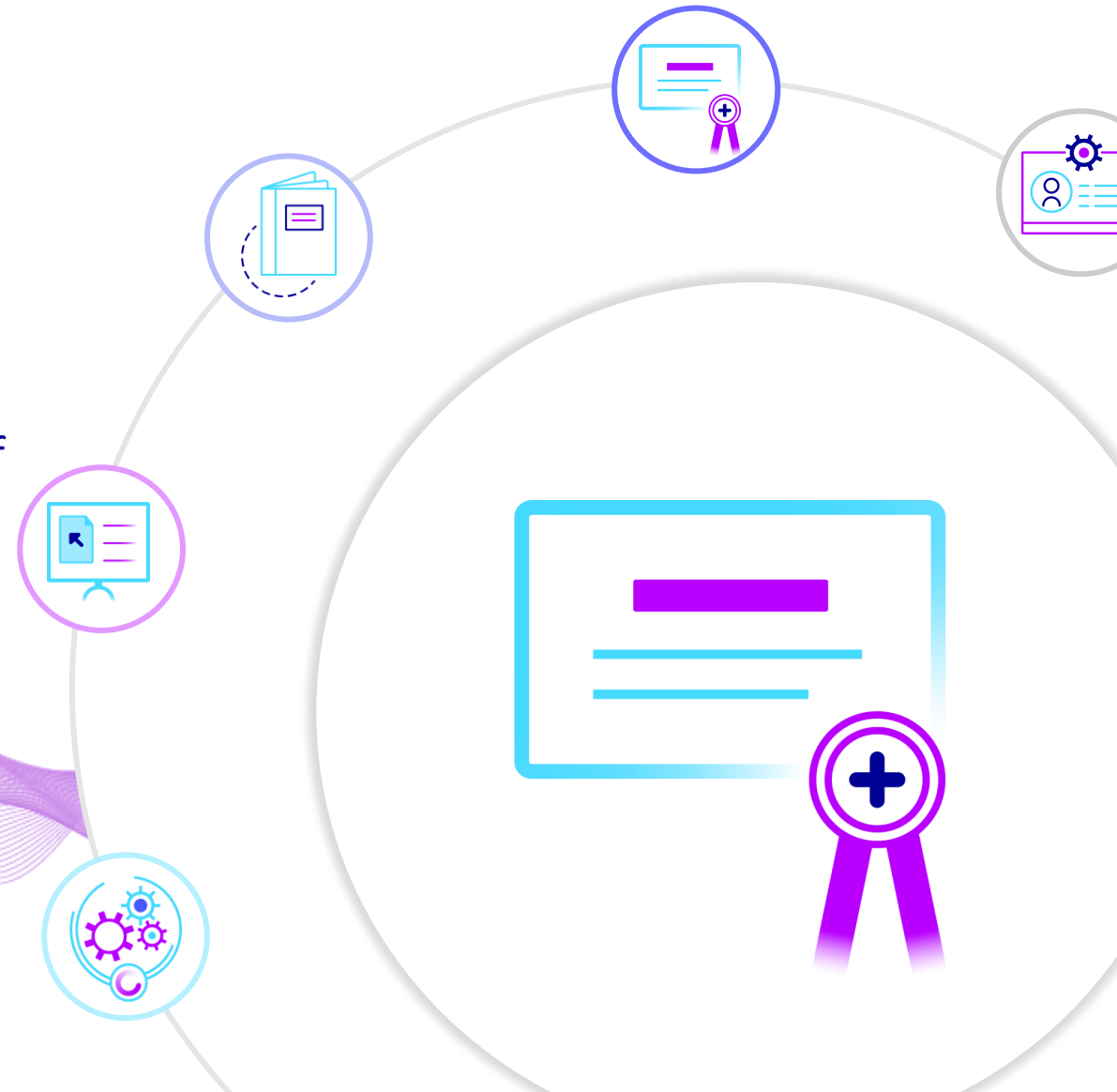
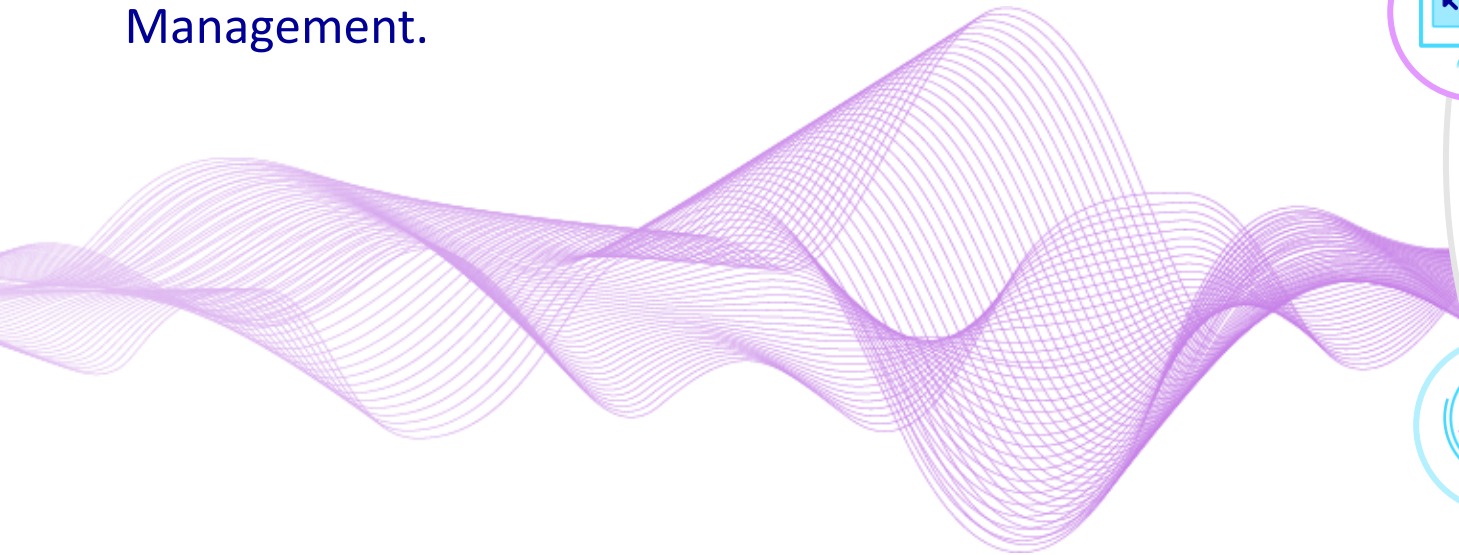
## Notarisierungsdienst

- ✓ Ausstellen einer verifizierbaren Beglaubigung nach erfolgreicher Validierung eines Teilnehmenden, um den Status als registrierter Teilnehmender in einer Föderation zu bestätigen
- ✓ Bearbeiten notarieller Anfragen und Ausstellen von digitalen, rechtsverbindlichen und vertrauenswürdigen Beglaubigungen



# Authentifizierungs- & Autorisierungsdienste

Attributbasierte Authentifizierung und Autorisierung auf Basis von Verifiable Credentials ohne zentrales Identity Management.



# Authentifizierungs- & Authorisierungsdienste

## OIDC IDP Broker

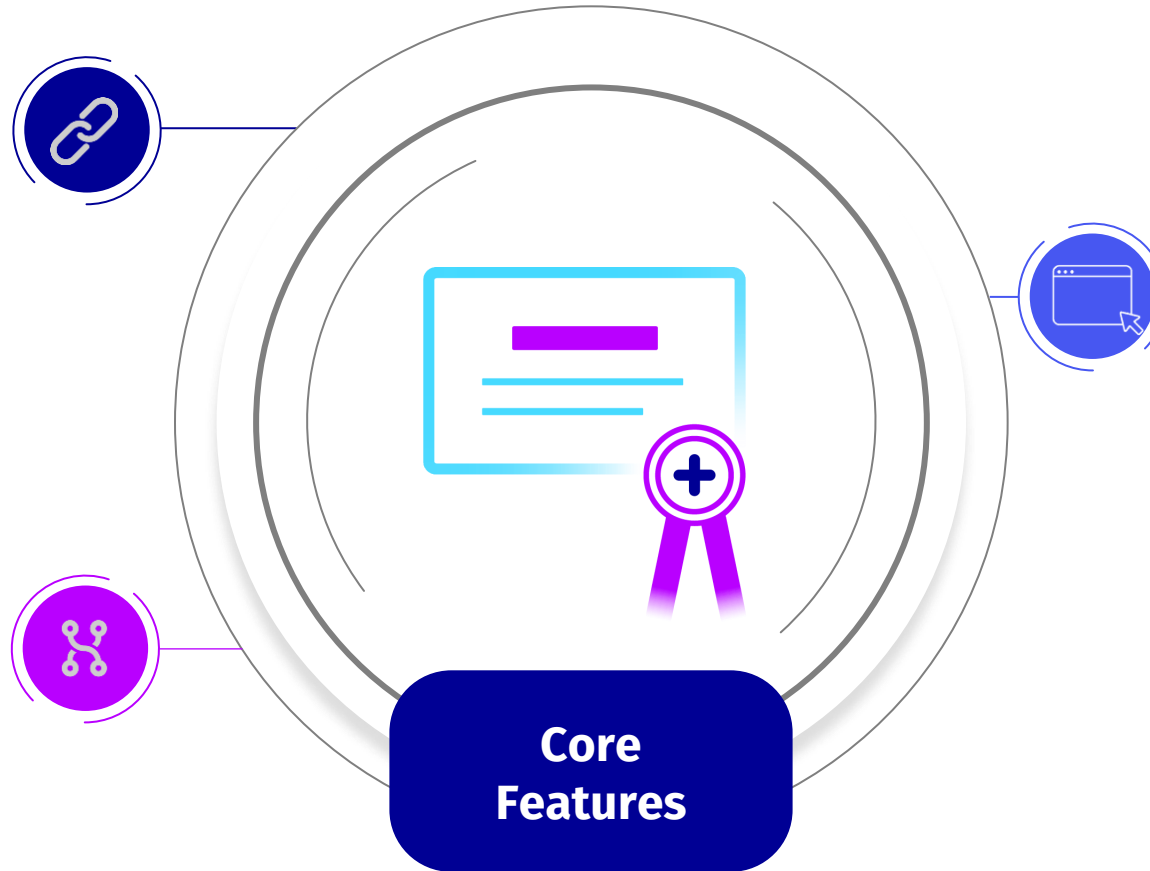
- ✓ Integrated with GXFS TSA (Vertrauensdienst)
- ✓ OIDC Compliant

## New OIDC Flows

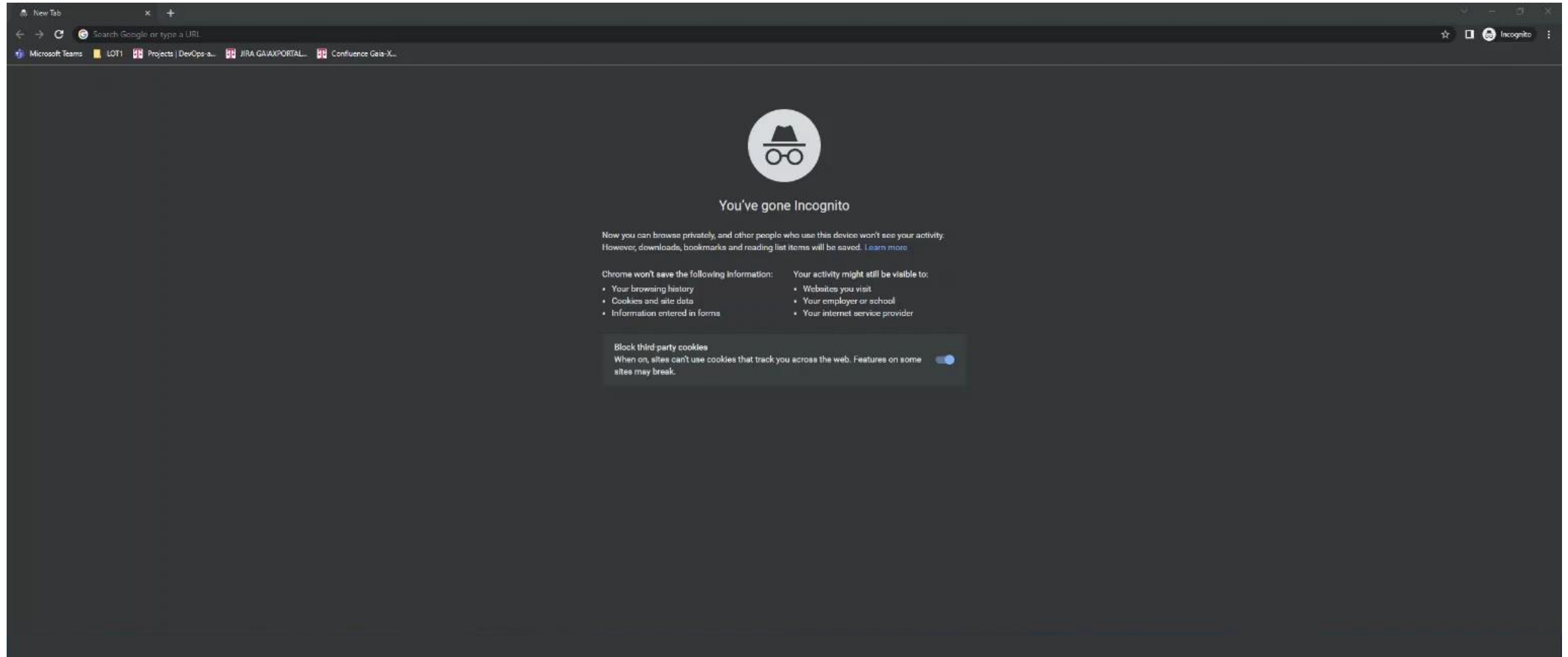
- ✓ DID SIOP

## Dynamic Client Registration

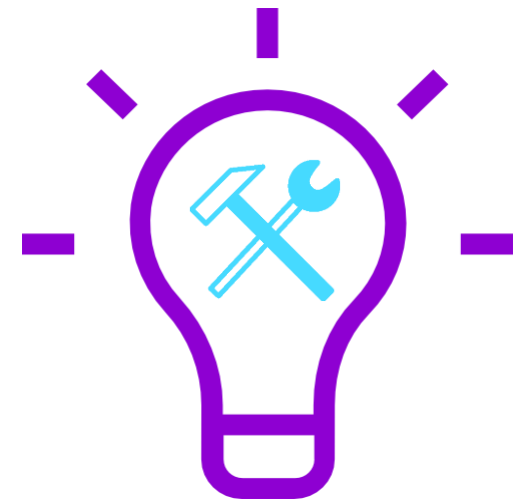
- ✓ Supports Issuing of IAT Tokens based on SSI



# DEMO: Authentifizierungs- & Authorisierungsdienste



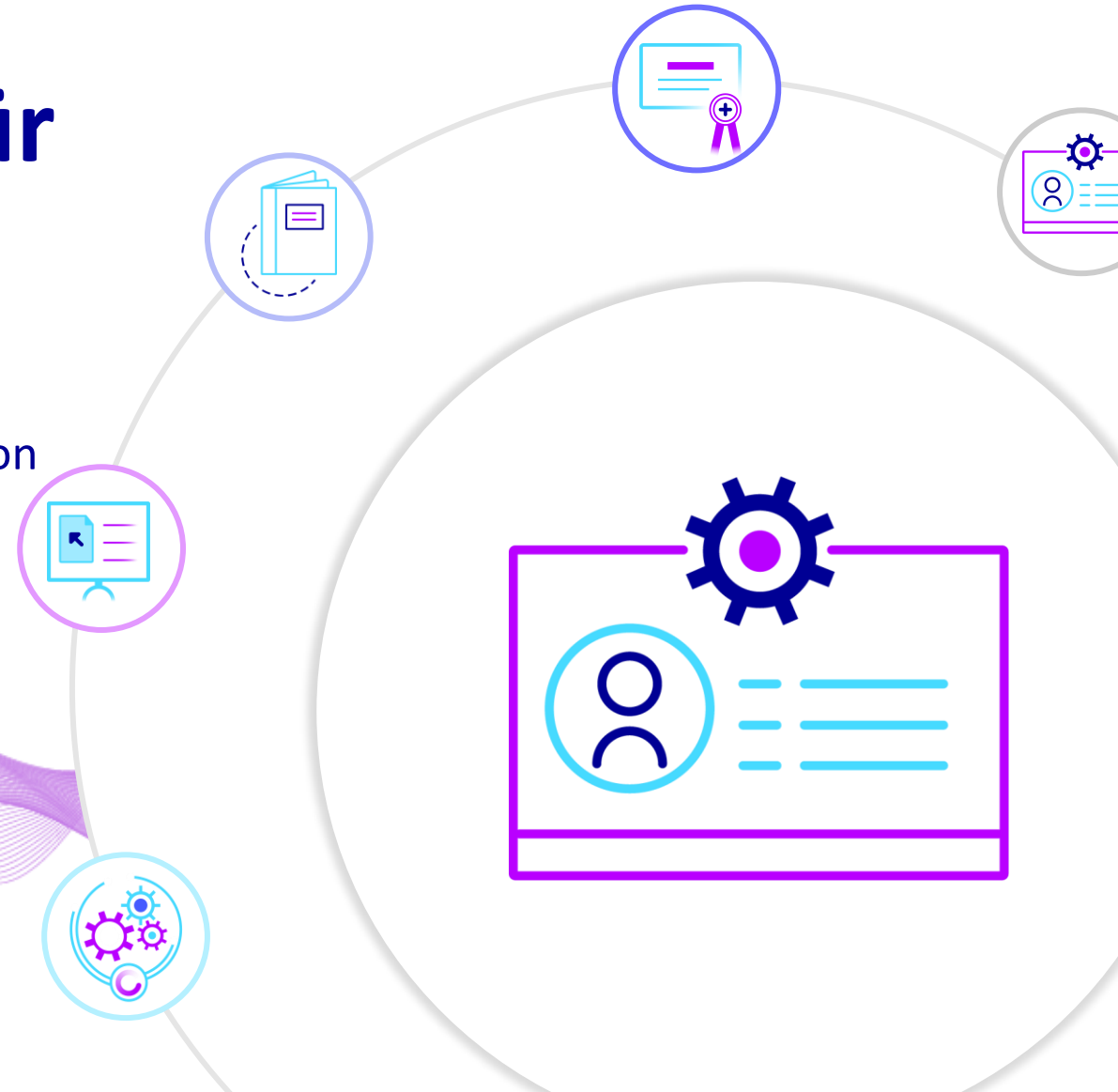
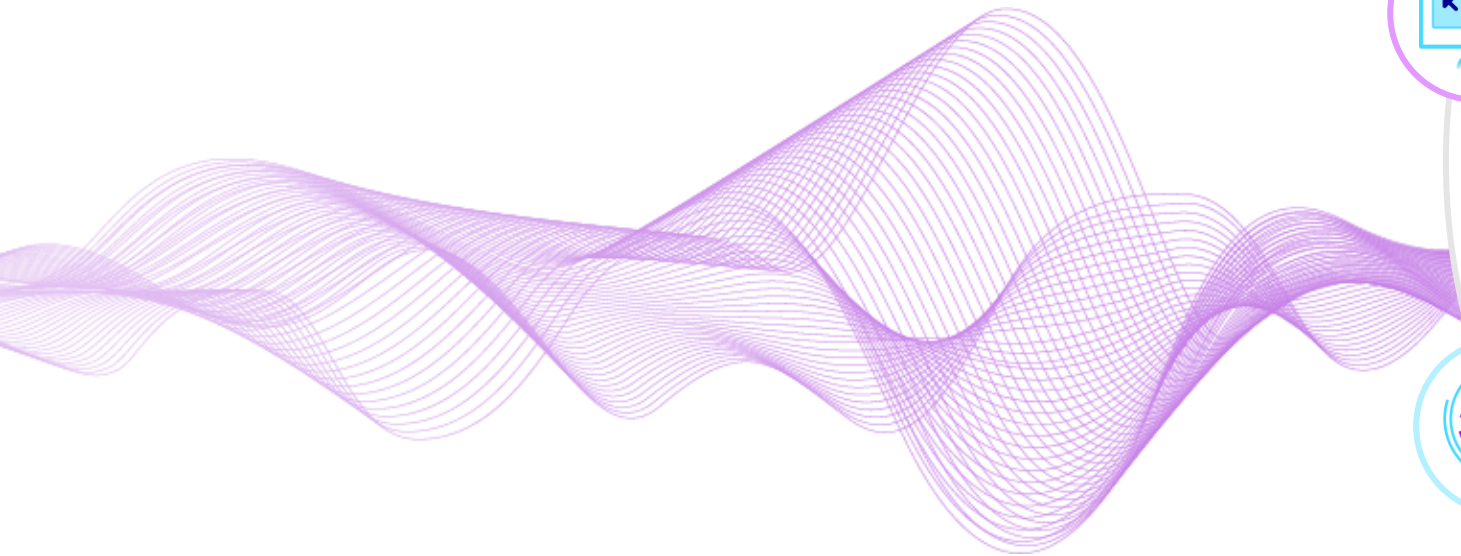
- Die Komponente kann als IDP Broker in andere OIDC Systeme integriert werden
- In Kombination mit dem Policy System können beliebige Scope Mappings aufgebaut werden
- Die Komponente könnte mit dem Einsatz von IPFS oder ähnlichem für weitere dezentrale Szenarien erweitert werden (z.B. Sharing von Rollenmodellen, Konfigurationen etc.)





# Beglaubigungsmanager für Personen

Mobile SSI Wallet App zum Speichern und Präsentieren von Verifiable Credentials.



# Beglaubigungsmanager für Personen

## Presenting Credentials

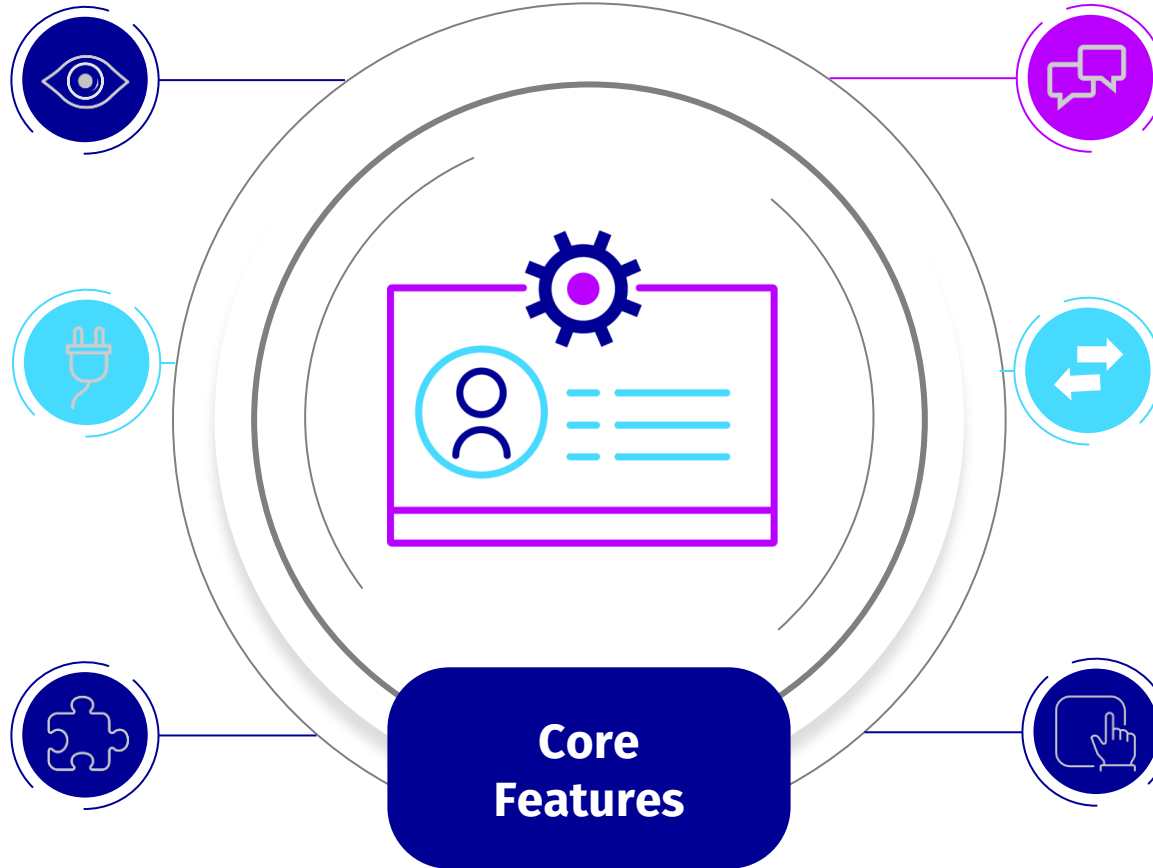
- ✓ QR Code based proofs (Out of band)
- ✓ OCM to OCM proof (API to API)
- ✓ Verifiable Presentations/ Verifiable Credential Presentation

## Indy Network Support

- ✓ Supports IDUnion, Sovrin and other Indy Networks
- ✓ Basic Aries RFCs for proof and request credentials are implemented

## ID Union Compatibility

- ✓ QR Code proofs from Lissi accepted
- ✓ Interaction with IDUnion Network



## DIDComm Messaging

- ✓ Core messaging features between agents like PCM, OCM and others (e.g AcaPy) according to Aries RFCs

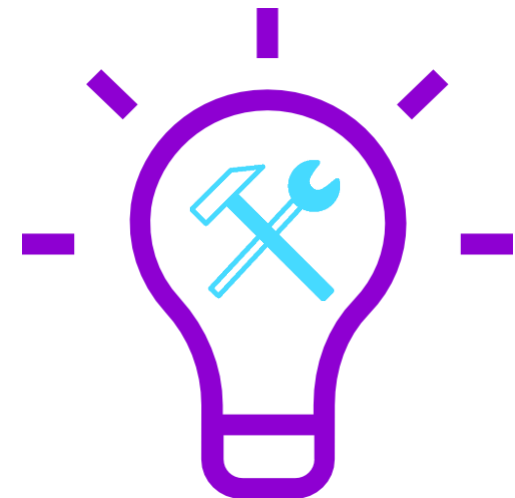
## Aries Mediator

- ✓ Notification Proxy for PCM
- ✓ Decentralizes proxy traffic to anonymize didcomm traffic for PCM
- ✓ Encrypted PCM channel for receiving credentials

## Multi Platform App

- ✓ PCM can be used for IOS/Android (Tablets, Smartphone)
- ✓ Theoretically possible to provide it as Mac/Linux/Windows App (not yet tested)

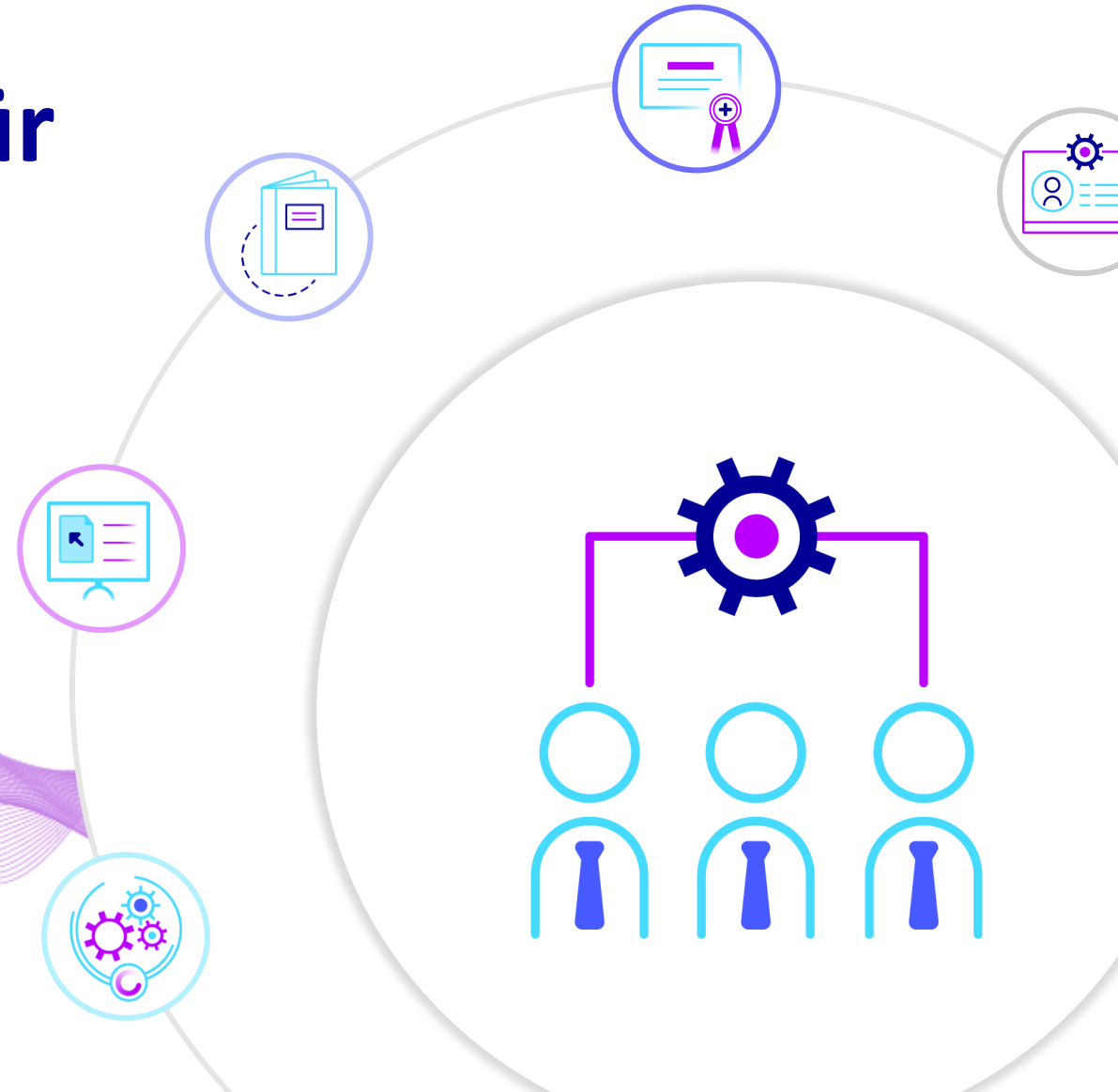
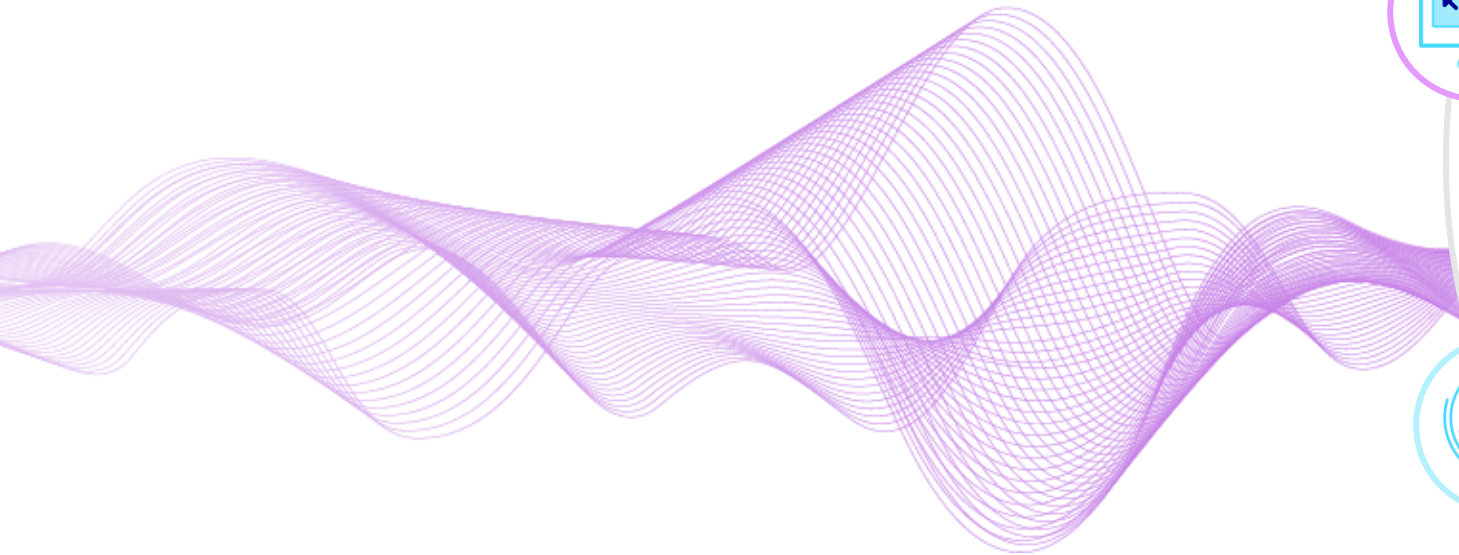
- Der Beglaubigungsmanager für Personen
  - Könnte von Federations modifiziert werden, um Portalaufgaben zu übernehmen (Freelancer/Mobile Use Case)
  - Unterstützt im Moment als Wallet, stellt aber eine gute Plattform dar, um weitere GXFS Services mit Funktionalität zu bedienen (z.B. mobile Suche, Einkäufe etc.)
  - PCM kann auch als Grundlage in andere Apps eingebaut werden (z.B. in Company Apps)





# Beglaubigungsmanager für Organisationen

Cloud SSI Wallet zum Speichern, Präsentieren und Ausstellen von Verifiable Credentials.



# Beglaubigungsmanager für Organisationen

## Presenting Credentials

- ✓ OCM to OCM proof (API to API)
- ✓ Verifiable Presentations/ Verifiable Credential Presentation



## Indy Network Support

- ✓ Supports IDUnion, Sovrin and other Indy Networks
- ✓ Basic Aries RFCs for proof and request credentials are implemented



## Modular Structure

- ✓ SSI Abstraction Service
- ✓ Principal Manager Service
- ✓ Proof Manager Service
- ✓ Connection Manager Service
- ✓ Attestation Manager Service



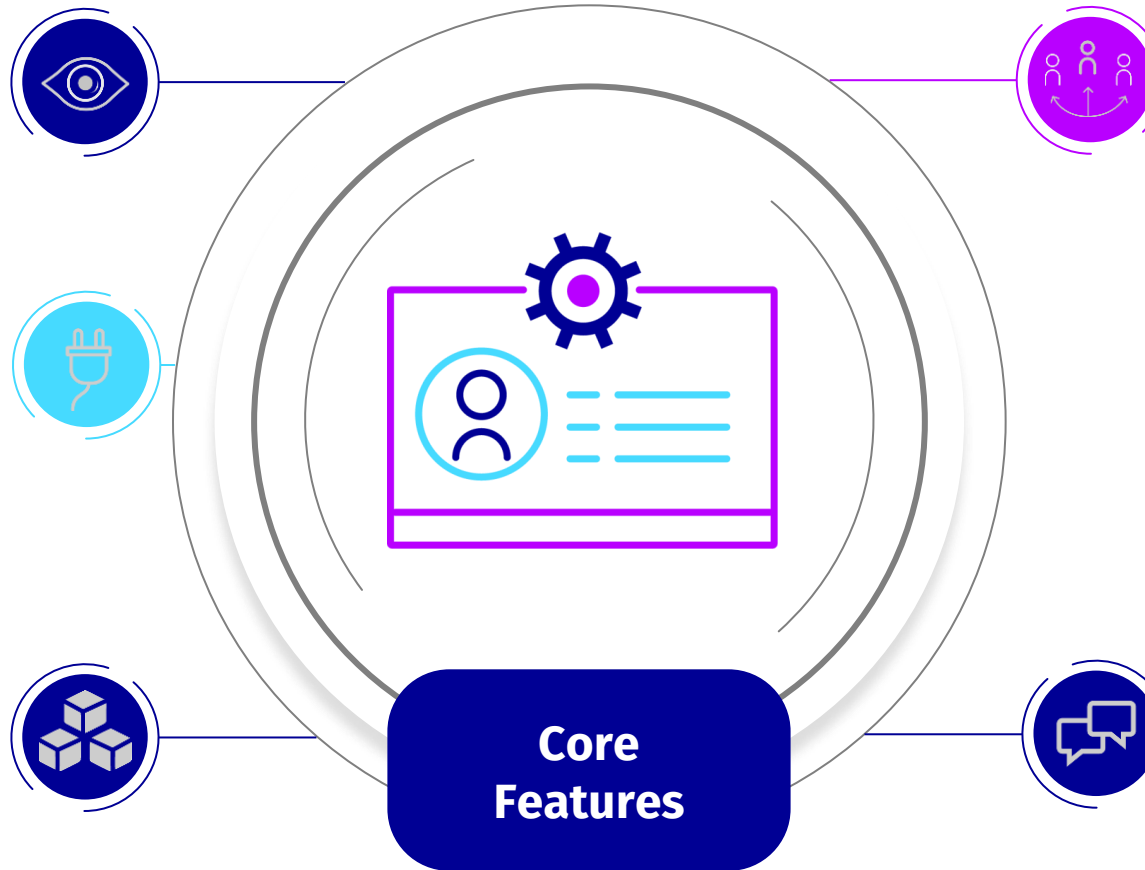
## Issuing of Credentials

- ✓ Participant Credential
- ✓ Principal Credential
- ✓ Other Credentials addable by integrating new Credential Definitions



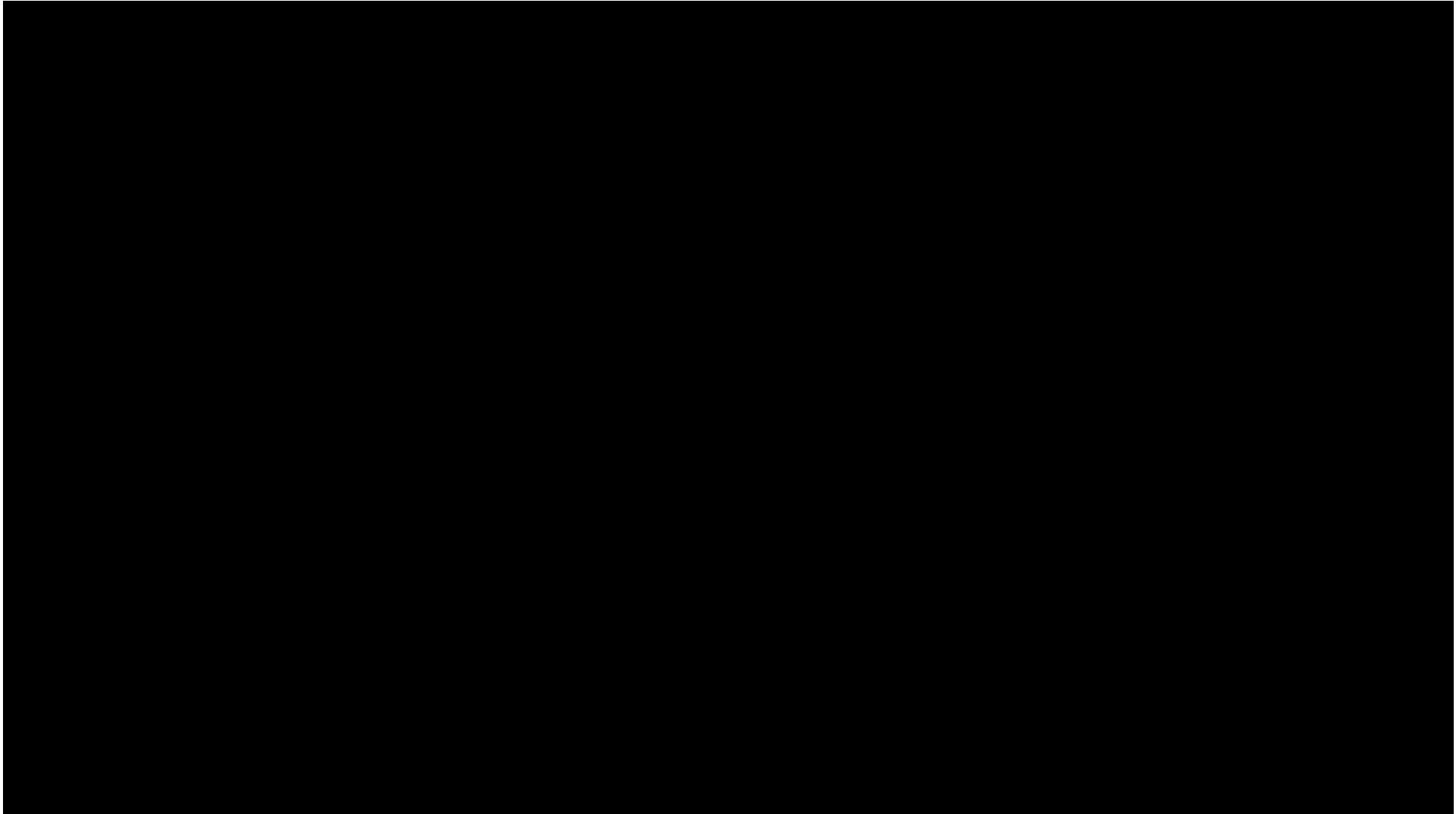
## DIDComm Messaging

- ✓ PCM can be used for IOS/Android (Tablets, Smartphone)
- ✓ Theoretically possible to provide it as Mac/Linux/Windows App (not yet tested)

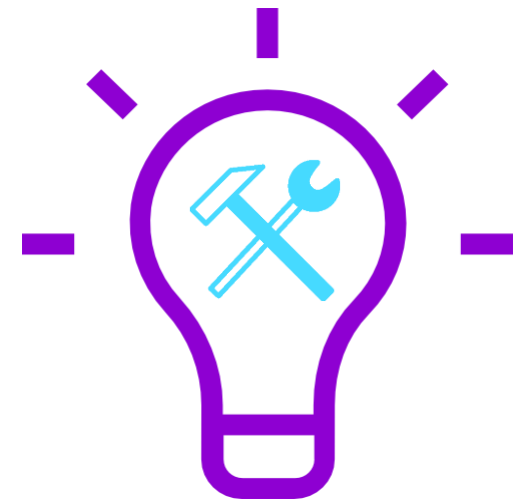


# DEMO: Beglaubigungsmanager für Personen und Organisationen

---



- Der Beglaubigungsmanager für Organisationen
  - lässt sich nicht nur für Organisationen sondern auch für Services einsetzen, wenn er entsprechend deployed wird
  - repräsentiert das Wallet einer Organisation, welches präsentiert werden kann bei Anfrage. Die Notwendigkeit von statischen Statements entfällt.
  - kann durch andere Wallets ersetzt werden, wenn die Federation schon eine andere Implementation besitzt (z.b. Businesspartner Agent)



# Vertrauensdienste

Tools und Services zur Etablierung und Durchsetzung von Vertrauens-Policies und deren Erstellung.



## Policy Execution

- ✓ REGO based policies management
- ✓ Extended policy execution by developed SSI extensions
- ✓ Available for OCM for Trustlist retrieval, signing, etc.

## DID Resolver

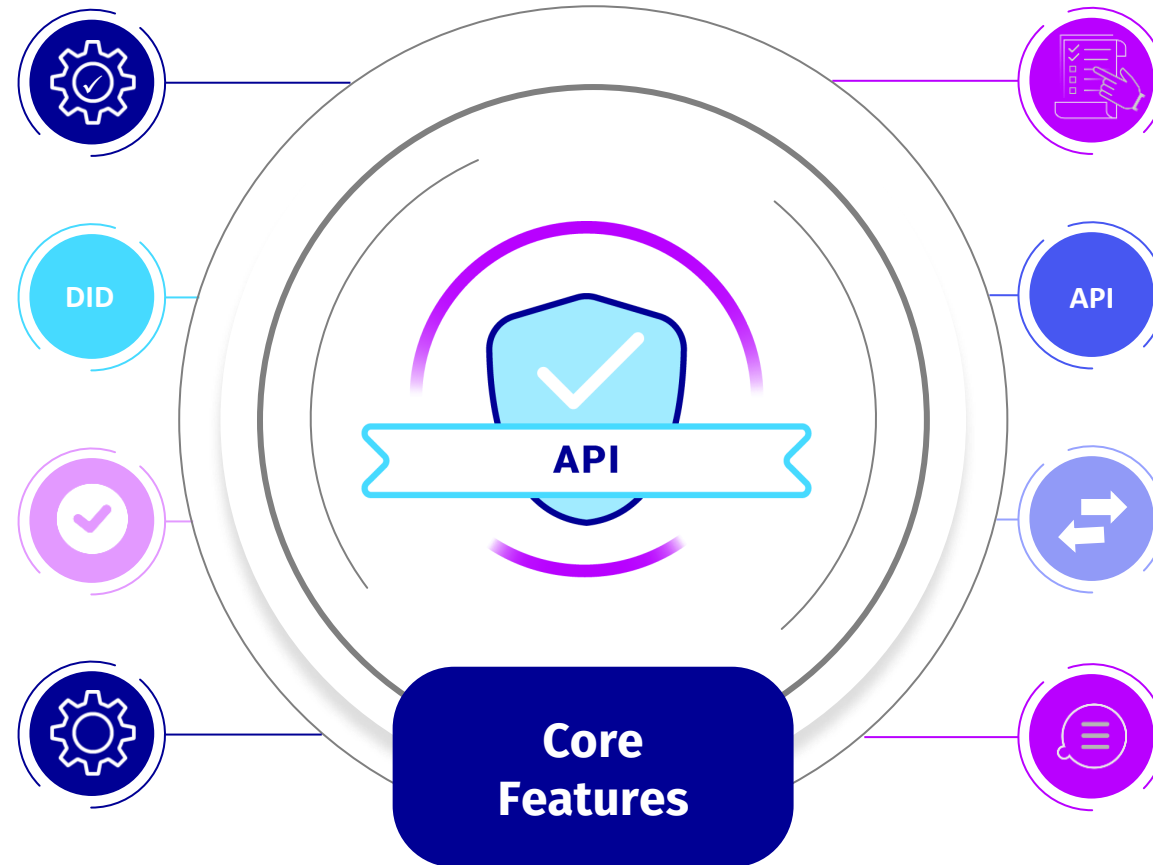
- ✓ Universal Resolver to resolve any DID from trusted sources within a policy definition

## Signing/Verification Service

- ✓ Signing/Verification of VC/VP
- ✓ Supports secure secret management through OCM/Vault integration

## GIT Ops/Flow

- ✓ Policy as Code
- ✓ Git Workflow for Policy approval
- ✓ Automated rollout (Sync) of Git managed Policies – PDP (Policy Decision Point)



## Task Controllers

- ✓ Cron Job Generation for Policies
- ✓ Async/Sync Policy execution
- ✓ Policy Task Groups

## External Input Interface

- ✓ REST API to fill the Data Grid with additional values used in the policy evaluation phase (e.g., Trustlists)

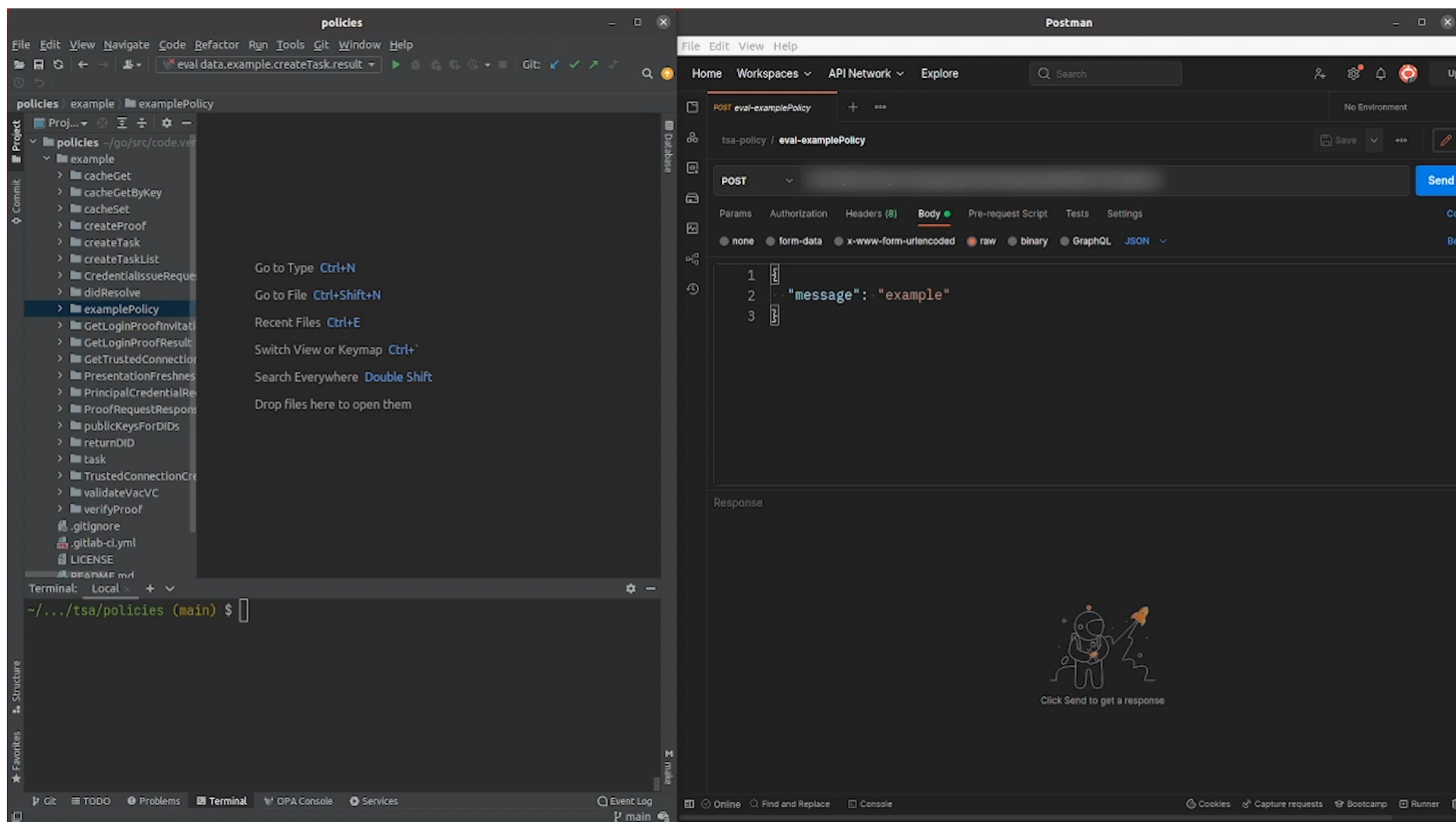
## Trusted Import/Export

- ✓ VC/VP Generation
- ✓ Export Configuration for any combination of policies

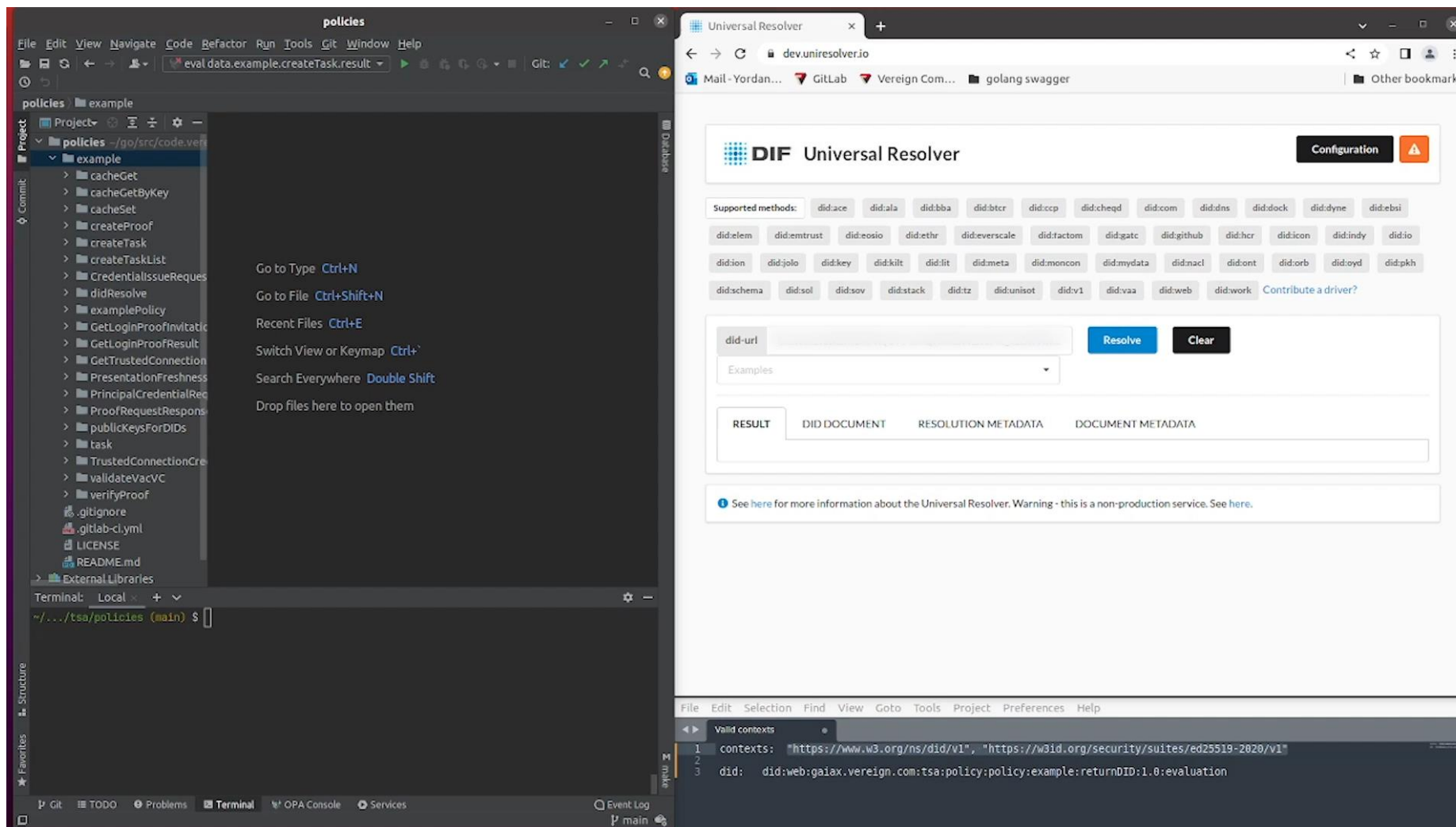
## Self-Description Generation

- ✓ DID Document generation through policy definition and Vault secrets
- ✓ Generation of arbitrary VC/JSON
- ✓ Injectable Values from Data Grid

# DEMO Vertrauensdienste: Policy Creation & Execution



# DEMO Vertrauensdienste: DID:web as a Service



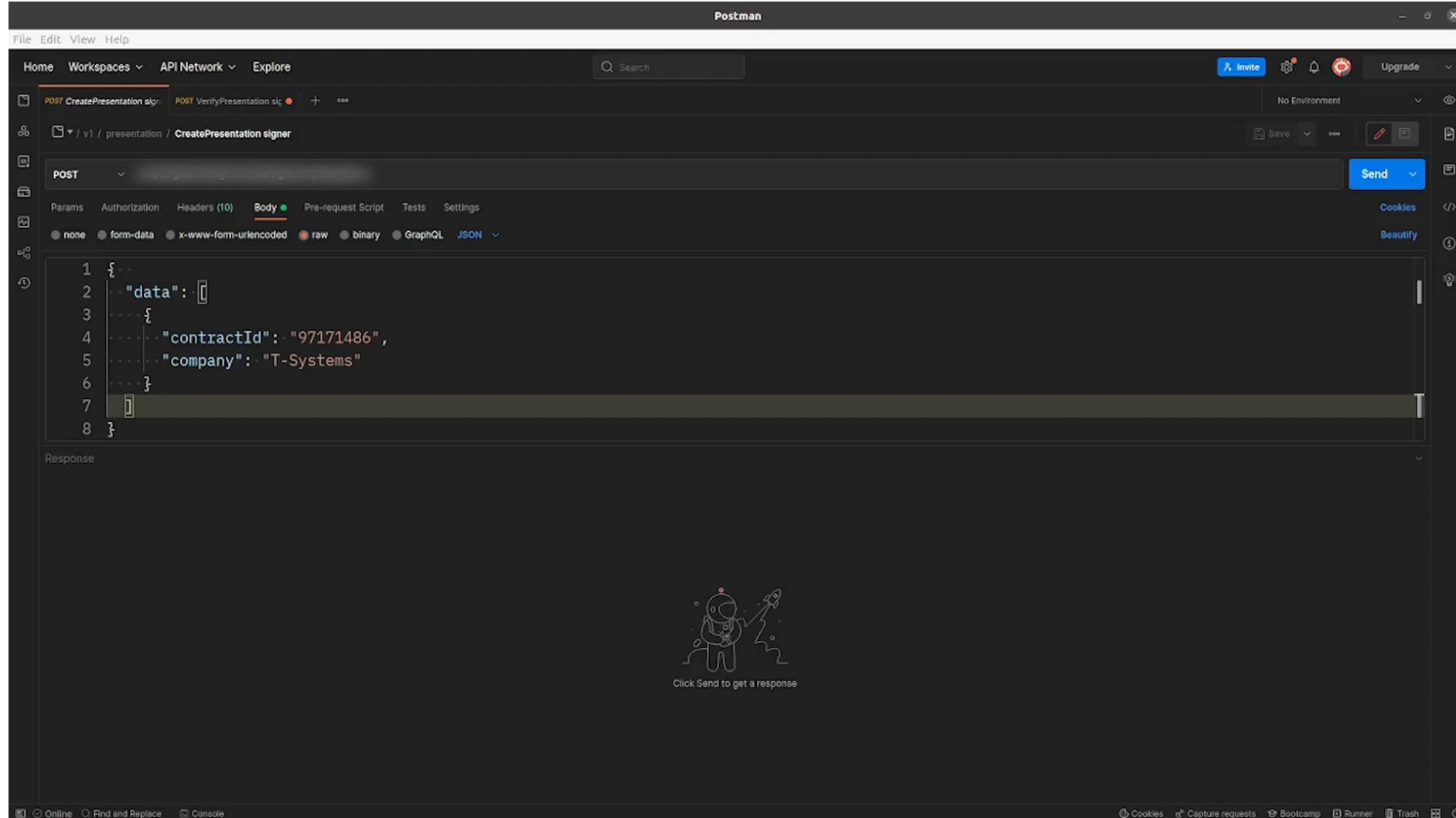
The screenshot displays a development environment with a code editor, terminal, and a web browser.

**Code Editor (Left):** Shows a project named "policies" with a file tree on the left. The main editor area displays a file named "eval data.example.createTask.result". The terminal at the bottom shows the command prompt: `~/.../tsa/policies (main) $`.

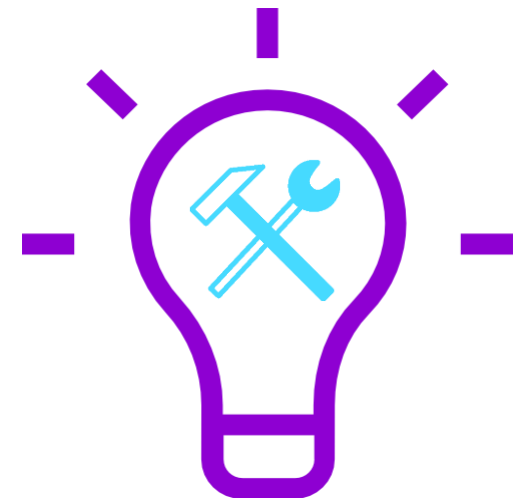
**Web Browser (Right):** Displays the "DIF Universal Resolver" interface. The address bar shows `dev.uniresolver.io`. The interface includes a "Configuration" button, a list of supported methods (e.g., did:ace, did:ala, did:bba, did:btr, did:ccp, did:cheqd, did:com, did:dns, did:dock, did:dne, did:bsi, did:elem, did:emtrust, did:zosio, did:ethr, did:verscale, did:factom, did:gatc, did:github, did:hcr, did:icon, did:indy, did:io, did:ion, did:jolo, did:key, did:kilt, did:lit, did:meta, did:moncon, did:mydata, did:nacl, did:ont, did:orb, did:oyd, did:pkh, did:schema, did:sol, did:sov, did:stack, did:tz, did:unisot, did:v1, did:vaa, did:web, did:work), a "Resolve" button, and a "Clear" button. Below the input field, there are tabs for "RESULT", "DID DOCUMENT", "RESOLUTION METADATA", and "DOCUMENT METADATA". A warning message at the bottom states: "See here for more information about the Universal Resolver. Warning - this is a non-production service. See here."

**Terminal (Bottom):** Shows the output of the command: `contexts: "https://www.w3.org/ns/did/v1", "https://w3id.org/security/suites/ed25519-2020/v1"` and `did: did:web:gaiax.vernigen.com:tsa:policy:policy:example:returnDID:1.0:evaluation`.

# DEMO Vertrauensdienste: Singing & Verification of Verifiable Presentations



- Per GitOps können Policies per Standardmechanismus zwischen verschiedenen Federations geteilt werden (z.B. per Git, Gitlab etc.)
- Per Data Grid Komponenten kann die Policy Execution dynamisch beeinflusst werden (um z.B. Preislisten oder Trustlisten direkt aus Bestandssystemen zu aktualisieren)
- Per Policy und dem entsprechenden Key Management, kann DID Web as a Service angeboten werden (ähnliches kann man hineinintegrieren)
- DID Web as a Service kann benutzt werden, um beliebige DID Web IDs anzubieten und so z.B. Services und Sub-Entitäten abseits des Beglaubigungsmanager für Organisationen (OCM) flexible Möglichkeiten zu geben (z.B. für Data Connectoren)



# Notarisierungsdienst

Workflow API zum Anfordern von Verifiable Credentials und digitalisieren vorhandener analoger Credentials.



## Evidence Based Issuing Flow

- ✓ API to start Issuance Sessions
- ✓ Upload of Evidence Documents



## Indy Network Support

- ✓ Supports IDUnion, Sovrin and other Indy Networks
- ✓ Basic Aries RFCs for proof and request credentials are implemented



## Digital Signer Service Support

- ✓ Document Signatures can be checked



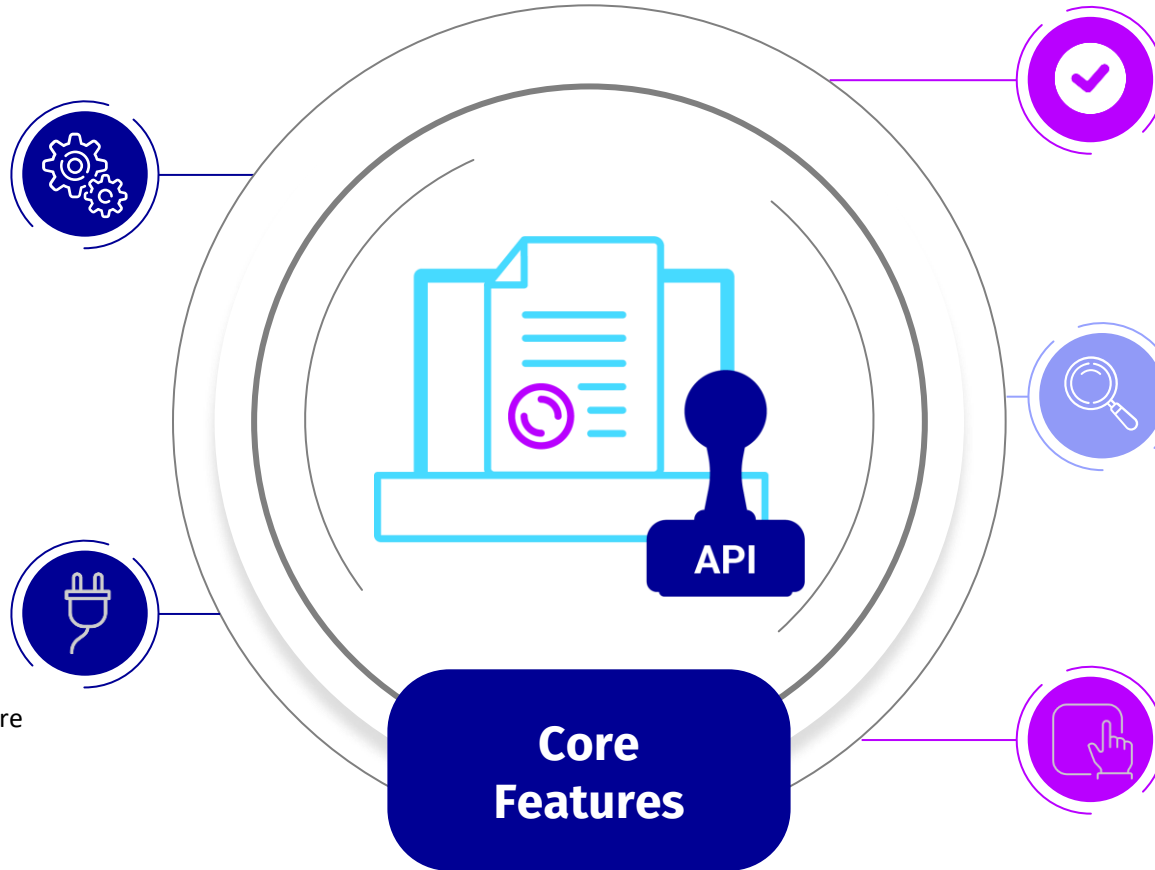
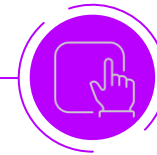
## OIDC Based Identification

- ✓ Requestor identified on OIDC basis

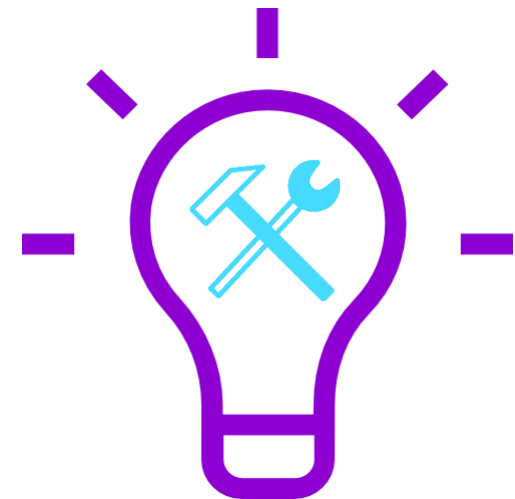


## Operator Interface API

- ✓ Management Interface for Requests



- Der Notarisierungsdienst sollte als Trust Etablierung in vorhandene Registrierungsprozesse der Federation eingebunden werden, sofern notwendig
- Jede Form der Verankerung von Fakten, sollte innerhalb der Federation durch den Notarisierungsdienst durchgeführt werden (z.B. die Überprüfung von Zertifizierungen)
- Der Notarisierungsdienst kann Kontext-spezifisch deployed werden, um z.B. innerhalb von GXFS für bestimmte Szenarien zu unterstützen



# Zeit für Ihre Fragen



## Hackathons

26 + 27. September



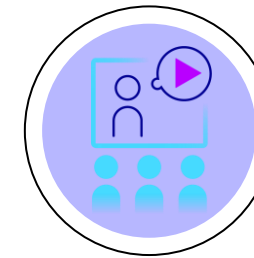
## Whitepaper

SSI Whitepaper



## GitLab

GXFS Toolbox



## Videos

GXFS Erklärvideos



Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Klimaschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages

Gaia-X  
FEDERATION SERVICES  
GXFS



# Vielen Dank

# Wir sehen uns in der Community :)