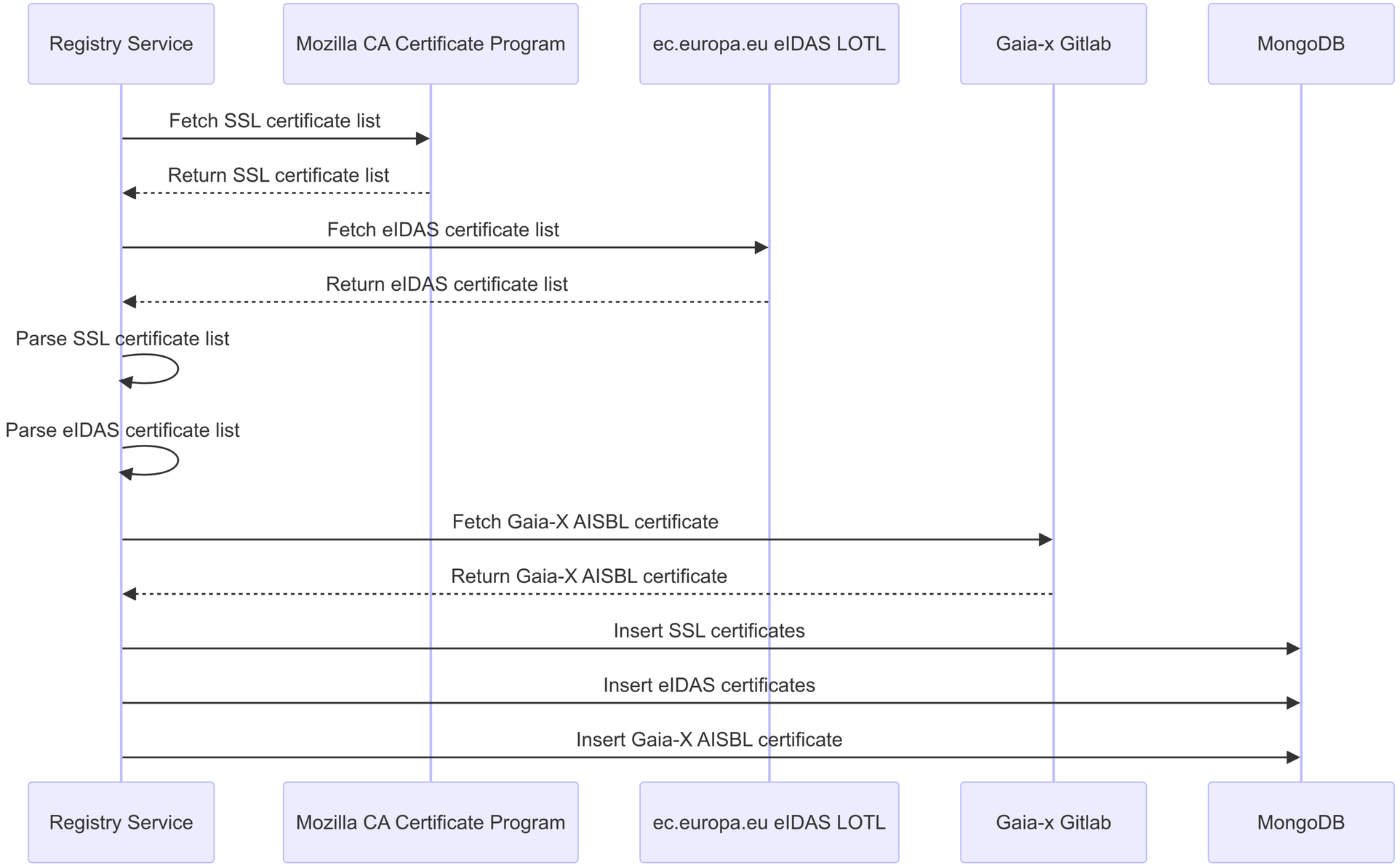
Management of Trust Anchors using Trusted Lists, XAdES and IPFS

How Gaia-X leverages decentralized technologies for trust anchor management

Current Trust Anchor Management

- Registry Service fetches the SSL and eIDAS certificates lists from the Mozilla CA Certificate Program and European Commission / countries APIs.
- Registry Service retrieves the Gaia-X AISBL certificate on gitlab.
- Registry Service need to parse and manage those lists.
- Uses a MongoDB to store the extracted Trust Anchors certificates along with the Gaia-X AISBL certificate.

Current Trust Anchor Management overview



Challenges in current implementation

- Scaling the system to accommodate to more Trust Anchors implies Registry service updates.
- Lack of standardisation in Trust Anchors list.
- Performance burden of the MongoDB while we already have the IPFS infrastructure.
- Centralised management: registry and MongoDB as a single point of failure in fetching and storing certificates.
- Leads to an increased risk of downtime and data unavailability.
- Increased maintenance burden on the Registry service.

ETSI 119 612 Trusted Lists

Defines a standard format for creating and managing trusted lists of trust service providers (TSPs), it contains:

- Metadata about the list (version, issuer, etc.)
- Detailed information about each TSP (our Trust Anchors)
- Current status of each TSP service (e.g., granted, withdrawn)
- Typically signed using XAdES (XML Advanced Electronic Signatures)

Benefits:

- Ensures consistent format and usage across different systems and jurisdictions
- Provides a clear and verifiable list of trust services
- Protected against tampering and unauthorised modifications

XAdES Signature

Provides a framework for creating advanced electronic signatures on XML documents, it contains:

- Canonicalisation method
- Signature method (algorithm)
- The digital signature created using the signer’s private key
- Information about the signing key (public key, certificates, etc.)

Benefits:

- Classic signature benefits (Integrity, Authenticity, Non-repudiation)
- Required signature method for ETSI 119 612 trusted lists


```
−<ds:Signature Id="id-82589b878d79">
  −<ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    −<ds:Reference>
      −<ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>Sxwsq09iJS7NkXd3I6e2UvD9WgsVdSU/r6//AkQPwLg=</ds:DigestValue>
      </ds:Reference>
    −<ds:Reference URI="#xades-id-82589b878d79" Type="http://uri.etsi.org/01903#SignedProperties">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>Q4WDp56xDOCwG0IJKmL1QsO15QzaSQiorOrH1LwJREE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
  −<ds:SignatureValue>
      LIn0Ue9sd9oZl3qu/2fQHld0FJY2Cup3c2EqYWSzGnVarCNJZzsAzleEhgf6UNhr2bAEAORNIyCDSu6f6wWR68SeLUyVqbmn
      I8uDwKoUyagzrdbf6qR2YgkDY5iUIhcHF2n97AqQdI0BSMwYWLZkJ0fPiO6au9lFLqLYYfEAqhEtLXeMYFZ6lBcMvoeHo97
    </ds:SignatureValue>
  −<ds:KeyInfo>
    −<ds:KeyValue>
      −<ds:RSAKeyValue>
        −<ds:Modulus>
            lljF9fHWnNFB6Wbhab8sZFD2C91up4cYKRbJNe7Tyfh8I5CYHe2qhZ5kOwcTfa1IuDisRvJzKEiArvPLGWKT2icgmeu
            Uqq3FR9Hpt1H7ltbgZVdSI3Dz4eCl7VRN8Ny+N7LNXd2U1Nt0y8NUX3xMHWhKb9BrY8NojzA8lbc5q1SQSX1YYji
          </ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  −<ds:Object>
    −<xades:QualifyingProperties Target="#id-82589b878d79">
      −<xades:SignedProperties Id="xades-id-82589b878d79">
        −<xades:SignedSignatureProperties>
            <xades:SigningTime>2024-07-03T08:31:05.765Z</xades:SigningTime>
          −<xades:SigningCertificate>
            −<xades:Cert>
              −<xades:CertDigest>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>MVA4jWkOBETVIV2D7A/C6i8qUuCWNWB47FxK55JjDWg=</ds:DigestValue>
                </xades:CertDigest>
              −<xades:IssuerSerial>
                −<ds:X509IssuerName>
                    C=BE, ST=Some-State, L=Bruxelles, O=Gaia-X AISBL, E=alexis.deprez@gaia-x.eu
                  </ds:X509IssuerName>
                  <ds:X509SerialNumber>110889052916443191807525709287800207912096420783</ds:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
            </xades:SigningCertificate>
          </xades:SignedSignatureProperties>
```

Implementation details

Trust Anchor Service (gx-trust-anchor-service)

- Single responsibility: manage Trust Anchors
- Fetches trust anchor lists from multiple sources (e.g., Mozilla CA, eIDAS LOTL, Gaia-x AISBL, etc.)
- Parses and aggregates the trust anchor data
- Pushes the TA Trusted List to the IPFS Pinning Service
- Built using NestJS with Nest Commander for CLI capabilities

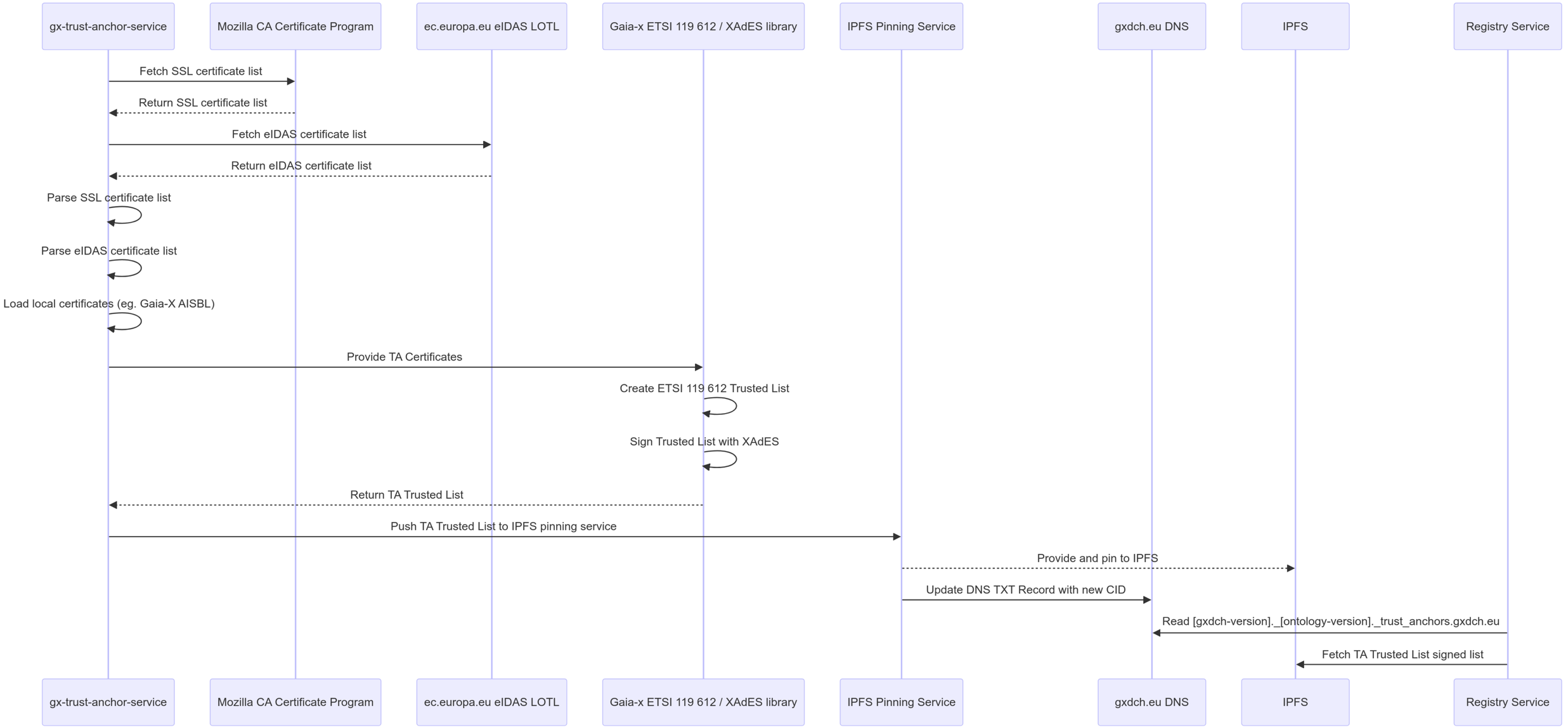
Gaia-x ETSI 119 612 / XAdES library:

- Creates the ETSI 119 612 Trusted list with Gaia-x metadata and Trust Anchors certificates
- Signs the Trusted List with XAdES

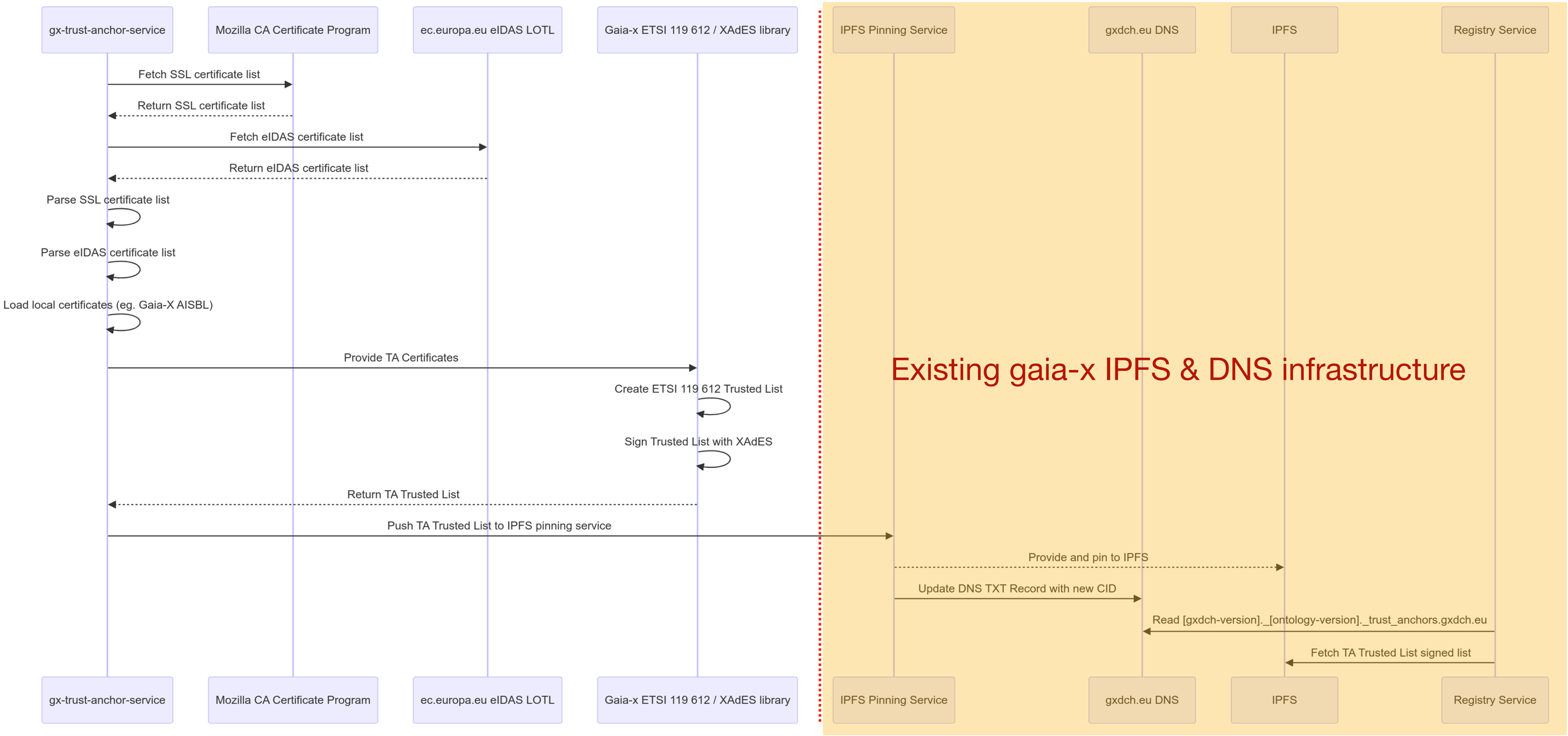
IPFS Pinning Service & DNS Integration

- Manage, update, and seed the artefacts needed by the Gaia-X Lab Registry Service
- Uses our gxdch.eu domain records to advertise CIDs for Gaia-x clearing houses registries

Implementation details



Implementation details



Benefits

- Architecture is designed to easily scale with the addition of new trust anchor sources and growing data needs (adding or removing TAs do not require GXDCH providers to update their registries).
- Decentralised storage using IPFS reduces single points of failure and improves resistance to tampering.
- Adherence to ETSI 119 612 and XAdES standards ensures legal compliance and interoperability with eIDAS regulations.
- Single responsibility service for fetching, parsing, and updating of trust anchors reduces maintenance burden.
- Uses the existing IPFS Kubo node and removes MongoDB deployment which will reduce the GXDCH resources requirements.
- New Trust Anchor service is managed by the Gaia-X AISBL, less operational workload for GXDCH providers.

Get more info or contribute

- Slack : https://join.slack.com/t/gaia-xworkspace/shared_invite/zt-2dr9bj9hx-IM7nwpv3DABR02UVhgQnzw
- Mailing lists: https://list.gaia-x.eu/postorius/lists/oss-community.list.gaia-x.eu/
- OSS Community call, every Thursday, 9am CEST
- Gitlab releases, issues, merge requests: https://gitlab.com/gaia-x/lab

Thank you