X.509 PKD Interop

Introduction

This page describes the approach the ToIP Trust Registry Task Force is taking to interoperability with traditional X.509-based public key directories (PKDs). It is intended for discussion and proposals around this topic, the final results of which will be incorporated into the ToIP Trust Registry Protocol specification.

Problem Description

PKDs based on X.509 digital certificates are widely used by governments and in multiple industries around the world. They use a classic centralized or federated model to issue certificate chains (also called "certification paths" in RFC 5280) that "chain back" to a root certificate. Examples include the ICAO ePassport PKD and the the EU Digital COVID Certificate (DCC) PKD.

Since this model of publishing public key certificates is well-established, it would be ideal if the ToIP Trust Registry Protocol enabled issuers who use X.509 PKDs to have their public key certificates identified, accessed, and verified in a parallel manner as issuers who use DIDs and DID documents.

Proposed Approach

The proposed approach is to use two special DID methods—the `did:web:` method and the `did:key:` method—to adapt DID architecture to X.509 certificates as follows:

1. First, the did:web: method is used to create a DID that encodes the URL of the location of a DID document as a file on a HTTPS server.
2. Second, this DID document contains:
    a. The public key of the issuer (as expressed in the issuer's X.509 certificate).
    b. A Linked Data proof using the x509CertificateChain property from the W3C Security Vocabulary that proves that the X.509 certificate containing the public key in the DID document chains back to an X.509 certificate trusted by the verifier. This Linked Data proof uses the did:key: method to encode the public key in the DID document as the verification key for the X.509 certificate chain.

With this approach, any issuer (or trust registry) that uses X.509 PKDs can "join" the decentralized network that uses the ToIP Trust Registry Protocol specification by publishing a DID document meeting this specification at an HTTPS URL, encoding that HTTPS URL in a `did:web:` DID, and using that DID as the issuer ID in their verifiable credentials. Any verifier that trusts the root X.509 certificate in the certificate chain verified in the x509CertificateChain property will know that the issuer is authorized by that root certificate authority.

Open Issues

1. This approach verifies that the issuer's (or verifier's) X.509 certificate is authorized by the root certificate authority but it does not verify what verifiable credential type URIs the issuer is authorized to issue (or what presentation definition URIs a verifier is authorized to request). Could this be handled by additional attributes in the X.509 certificate?

Remaining Work Items

1. **Verify this end-to-end design** with both X.509 and VC security experts.
2. **Determine if a specific JSON-LD context and/or JSON-LD "@type" property is needed** to identify this specific type of DID document.
3. **Determine if the did:web: DID needs to be included in the X.509 certificate as a SAN (Subject Alternative Name)** as specified in RFC 5280.
4. **Decide if this DID-to-X.509 bridge needs to be a separate specification** or if it can be incorporated directly into the ToIP Trust Registry Protocol spec.
5. **Draft the spec** and hold a public review.