-mls-addl-creds

Richard Barnes

MLS @ IETF 117

Credentials in RFC 9420

Value	Name	R	Ref
0x0000	RESERVED	-	RFC 9420
0x0001	basic	Y	RFC 9420
0x0002	x509	Y	RFC 9420

Additional Credential Types

Value	Name	Recommended	Reference
0x0003	userinfo-vc	Y	RFC XXXX
0x0004	multi	Y	RFC XXXX
0x0005	weak-multi	Y	RFC XXXX

UserInfo Verifiable Credentials

Based on Verifiable Credentials framework

Certificate-like (attrs, pubkey, sig)...

... but managed via OpenID Connect

Main technical challenge is comparing JWKs (`did:jwk`) to MLS public keys

Draft implementation in MLSpp

```
JWT Payload:
{
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1"
    ],
    "type": [
      "VerifiableCredential",
      "UserInfoCredential"
    ],
    "credentialSubject": {
      "id": "did:jwk:eyJrdHki0iJFQyIsInVzZSI6InNpZyIsImNydiI6IlAtMjU2Iiwi
             eCI6InFpR0tMd1hSSm1KU19BT1FwV09IWExYNXVZSWZ6dlB3RHVyV3ZtWkJ3
             dnciLCJ5IjoiaXA4bnl1THBKNU5wcmlaekNWS2lHMFR0ZXFQTWtyemZOT1VR
             OFl6ZUdkayIsImFsZyI6IkVTMjU2In0",
      "sub": "248289761001",
      "name": "Jane Doe",
      "given_name": "Jane",
      "family_name": "Doe",
      "preferred_username": "j.doe",
      "email": "janedoe@example.com",
      "picture": "http://example.com/janedoe/me.jpg",
      "phone_number": "+1 202 555 1212"
    }
  },
  "iat": 1667575982,
  "exp": 1668180782,
  "iss": "https://server.example.com"
}
```

Multi-Credentials

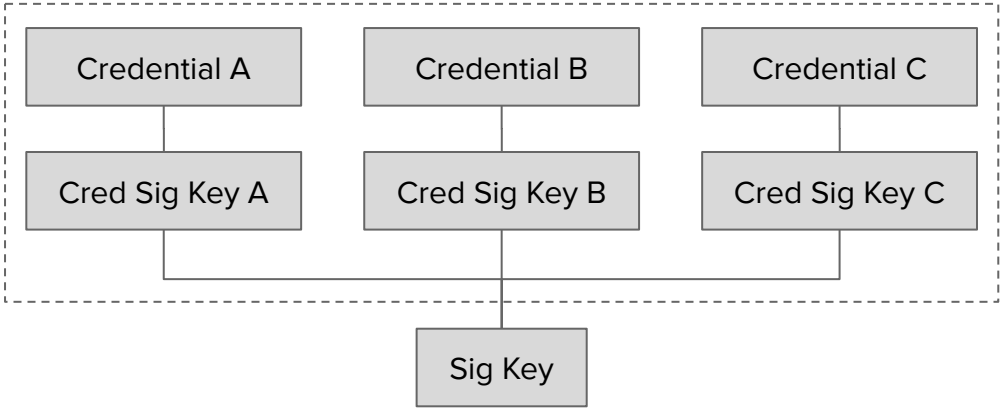
Use cases:

- Multiple sources of attributes (e.g., communications provider + enterprise)
- Heterogeneous credential support

Multiple credentials all “bless” the LeafNode signature key by signing over it

Variants:

- “Multi” - Everyone must support **all credentials** in the multi-cred
- “Weak-multi” - Everyone must support **at least one credential** in the multi-cred




```
struct {
  CipherSuite cipher_suite;
  Credential credential;
  SignaturePublicKey credential_key;

  /* SignWithLabel(., "CredentialBindingTBS", CredentialBindingTBS) */
  opaque signature<V>;
} CredentialBinding

struct {
  CredentialBinding bindings<V>;
} MultiCredential;

struct {
  CredentialBinding bindings<V>;
} WeakMultiCredential;
```

Status & Questions

draft-00, but really draft-01 (we changed the name due to adding multi-cred)

Draft implementation in MLSpp

Interest in adopting in the MLS WG?

Other credential types folks are interested in?