Using LDAP directory for FIDO 2.0

OSSTech

Open Source Solution Technology Corporation
HAMANO Tsukasa <hamano@osstech.co.jp>

LDAPCon 2019 Sofia

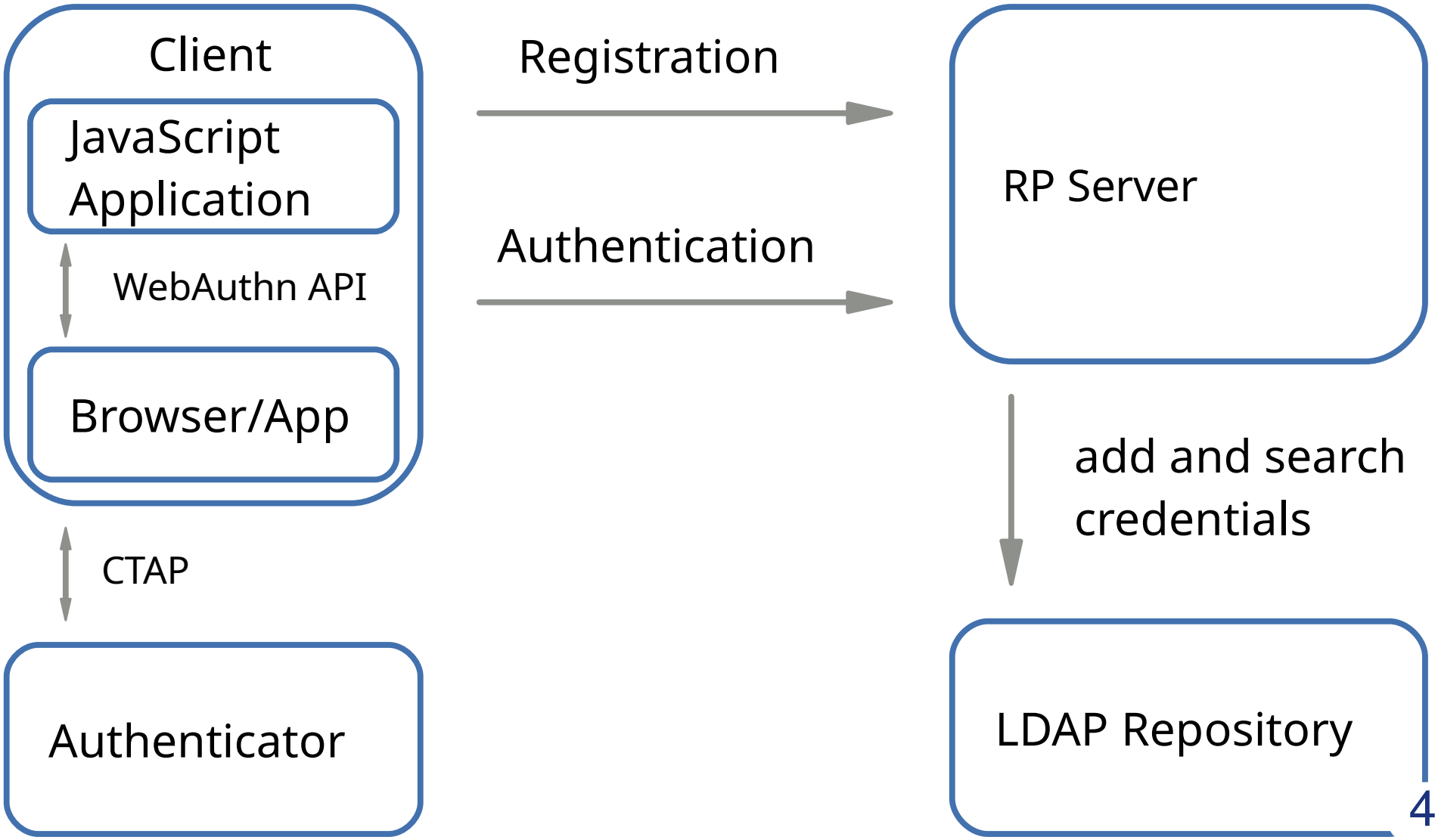
Authenticators

Mt. Витоша

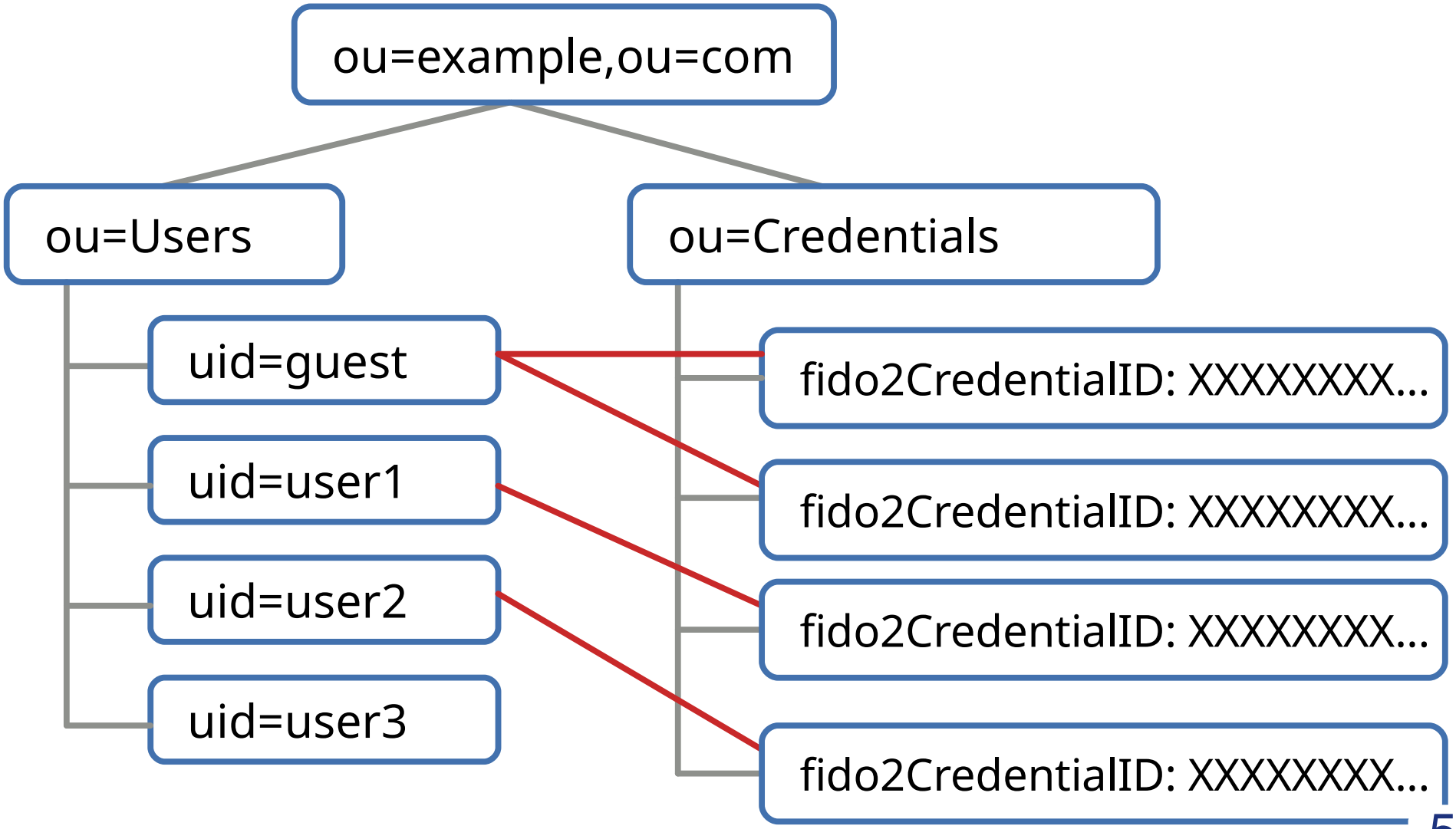
FIDO2 Flow

- 2-factor with Password
  - Password + Authenticator
- Single-factor Password-less
  - Authenticator with UserPresence
- Multi-factor Password-less
  - Autenticator with UserVerify
- Username-less
  - Autenticator with Resident Key

Overview


Client
JavaScript Application
WebAuthn API
Browser/App
CTAP
Authenticator
Registration
Authentication
RP Server
add and search credentials
LDAP Repository

Directory Structure



LDAP Schema

```
objectclass ( 1.3.6.1.4.1.34468.2.56.2.1
  NAME 'fido2Credential'
  DESC 'objectClass for FIDO2 Credential'
  SUP top STRUCTURAL
  MUST ( fido2CredentialID $ fido2PublicKey $
         fido2SignCount $ fido2UserID )
  MAY ( fido2RawID $ fido2AAGUID $
        fido2CredentialName ))
```

Attributes

- fido2CredentialID
  - fido2RawID
- fido2PublicKey
- fido2SignCount
- fido2UserID
- fido2AAGUID
- fido2CredentialName

Why COSE Key

format	size
JWK	179 bytes
PKCS#1 PEM	178 bytes
PKCS#1 DER	91 bytes
COSE Key	77 bytes

What's user.id

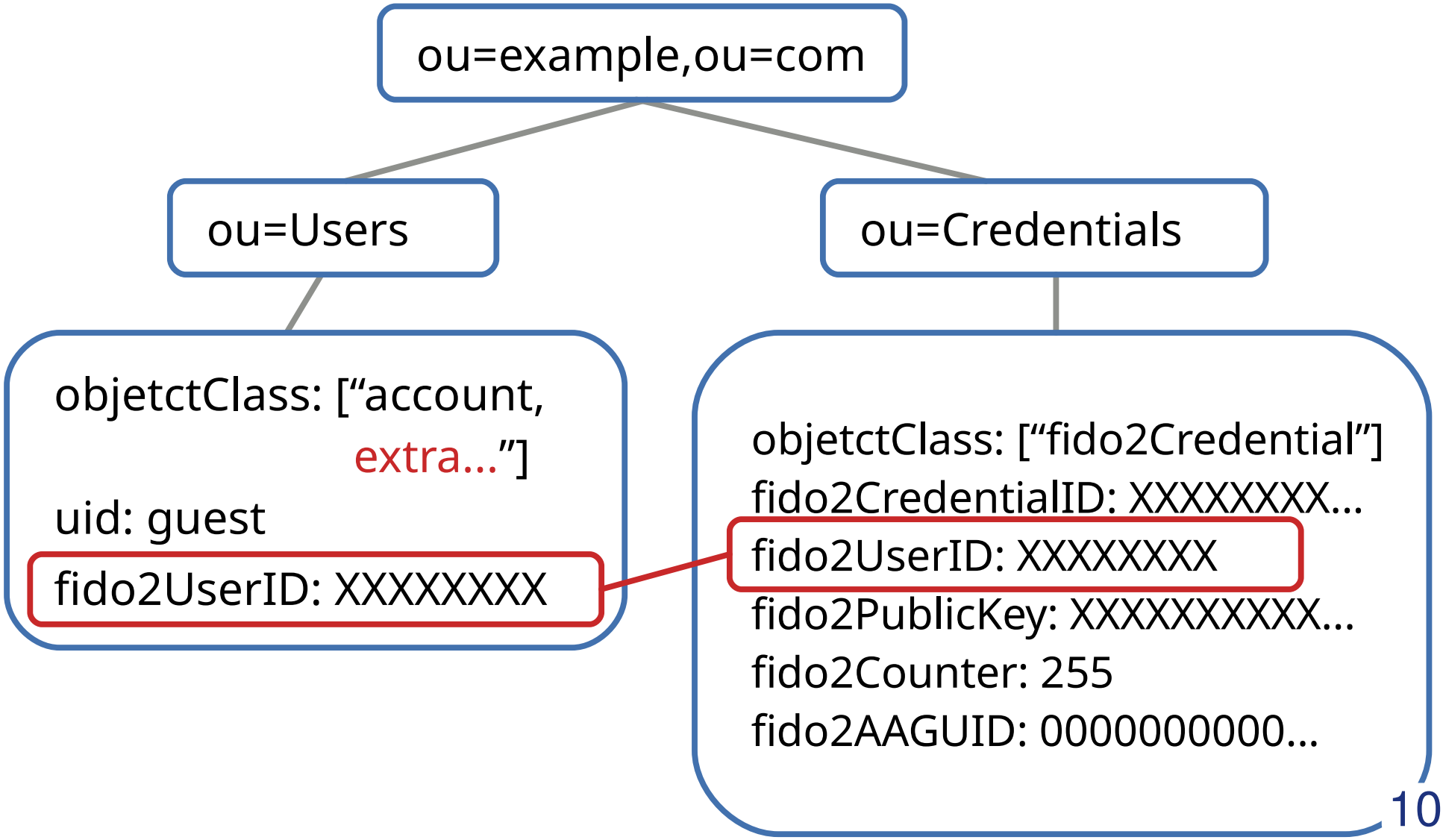
W3C WebAuthn Spec:

> the Relying Party SHOULD NOT include personally identifying information, e.g., e-mail addresses or usernames, in the user handle.

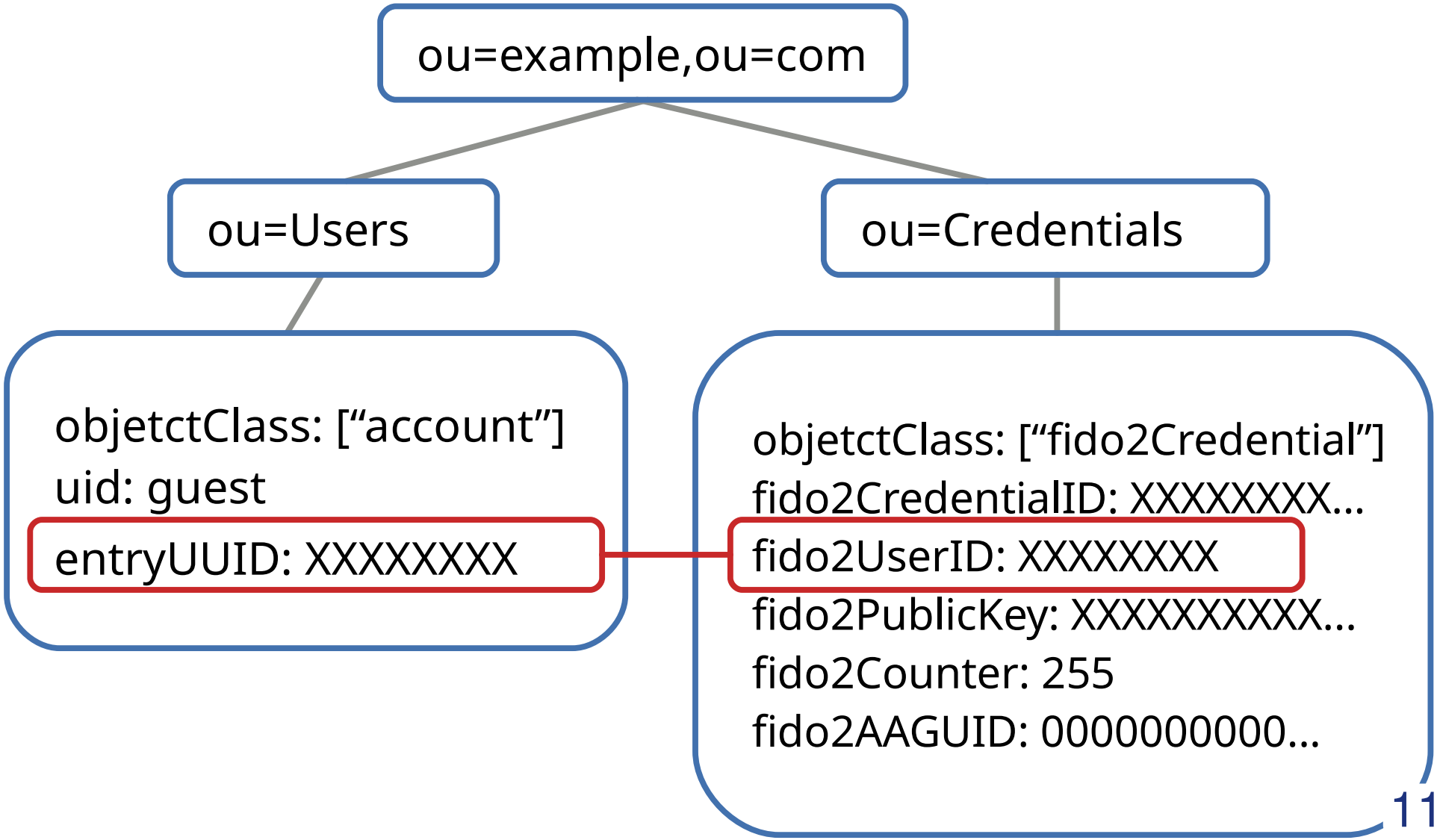
RFC8266 6.1:

> To ensure secure operation of applications that use nicknames, authentication and authorization decisions MUST be made on the basis of the thing's identity, not its nickname.

Entity mapping(1)



Entity Mapping(2)



Demonstration

https://demo.osstech.co.jp

Username: guest

Password: guest

Try your self

```
$ git clone \
  https://github.com/osstech-jp/fido2-ldap-demo.git
$ cd fido2-ldap-demo
$ docker-compose up --build
```

Resource

- Demo server
  - https://demo.osstech.co.jp/
- FIDO2 schema & Demo server source
  - https://github.com/osstech-jp/fido2-ldap-demo/
- Blog
  - https://www.osstech.co.jp/~hamano/posts/fido2-ldap/