Secure Credential Transfer

internet-draft

November 2022

Problem Statement

- More and more credentials are being stored securely in users' digital wallets rather than physical badges or cards
- Some use cases necessitate the sharing of these credentials from one person to another (e.g. your friend borrows your car)
- However, no secure method to share these digital credentials exists in a cross-platform and channel-agnostic capacity today

Design Goals

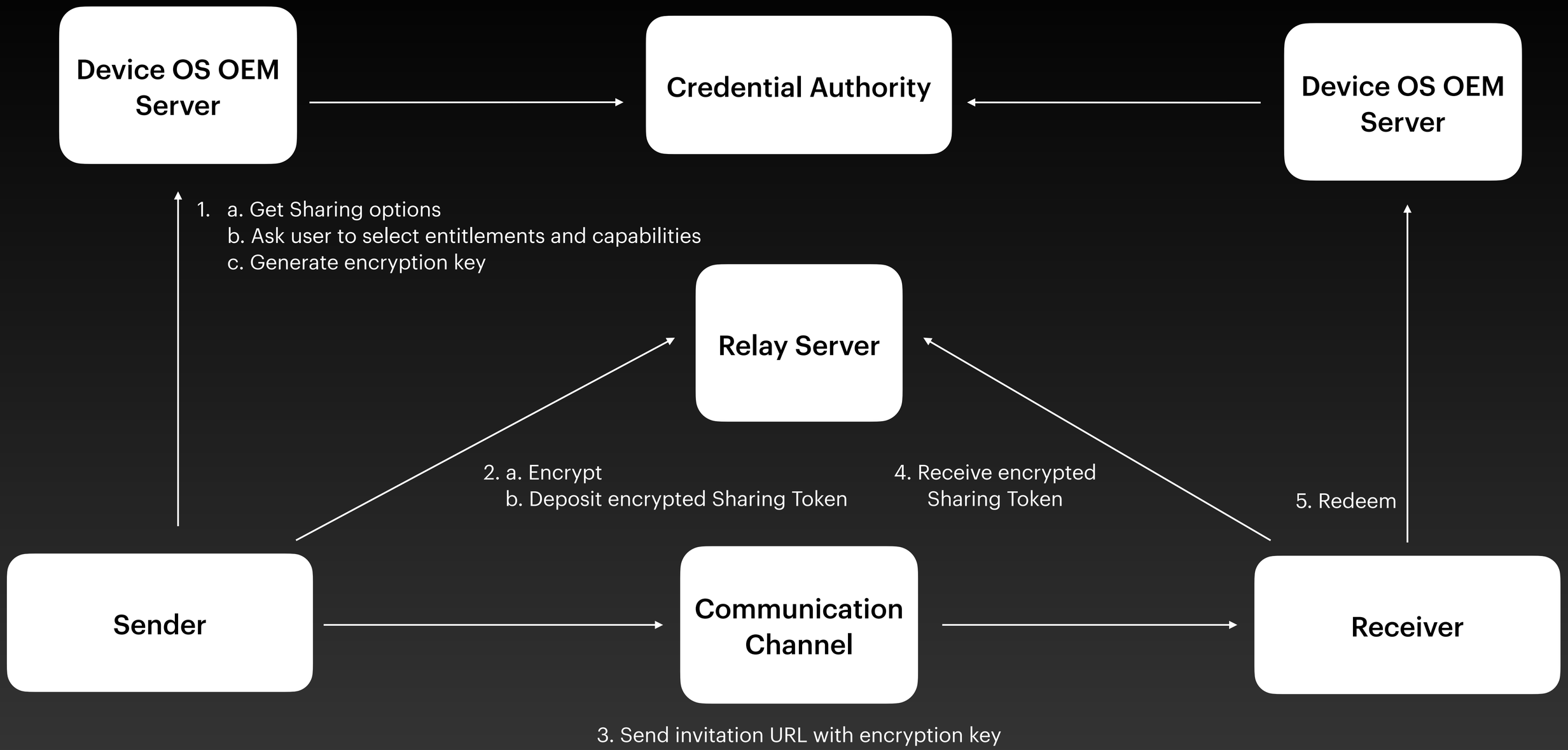
- Sharing mechanism should work regardless of credential type (e.g. a key to unlock and drive a car, a key to access a hotel, et cetera)
- Must work for symmetric and asymmetric credentials
- Sender must retain ability to manage credentials they have shared
- Sharing ecosystem supports any mobile device operating system OEM that adheres to the standard being proposed here

High Level Solution

- New relay server establishes “connectivity” between sender and receiver
- Relay server is a simple mailbox and decoupled from credential provisioning/registration
- Relay server only sees encrypted data and metadata

Design Requirements

- Relay server does not know the identity of the sender nor receiver
- Relay server does not interface with any other server - it is purely used for transport between sender and recipient
- Sensitive data sent over relay server is field-level encrypted, ensuring the relay server cannot see what is being shared
- Sharing must be able to be initiated from any communication channel


Device OS OEM Server
Credential Authority
Device OS OEM Server
1. a. Get Sharing options
b. Ask user to select entitlements and capabilities
c. Generate encryption key
Relay Server
2. a. Encrypt
b. Deposit encrypted Sharing Token
4. Receive encrypted Sharing Token
5. Redeem
Sender
Communication Channel
Receiver
3. Send invitation URL with encryption key