Some Terms

• Digital Credential:
  • Cryptographic Material and Other Data that enables access to Property using Mobile Devices

• Verticals:
  • Standards and bodies that cover different types of properties (Cars, Homes, Hotels etc.)

• Provisioning:
  • Process of getting a Credential on a device

• Provisioning Information:
  • Necessary and sufficient data to complete Provisioning
Sharing Credentials

• Once you have a Credential, sharing it to others is a natural use case.
  • Examples:
    • Sharing your car Credential over Instant Messaging
    • Sharing your Hotel Credential over Email
  • Important to provide convenient and seamless user experience
    • Similar to sharing other digital assets like photos or document
Unique Requirements

• Round trips between Initiator and Recipient without user interaction
  • Users may not be online at the same time

• First Recipient device to claim share is the only device that gets Provisioning Information

• Invitation to share goes over existing communication methods that users prefer
  • No security or privacy properties can be assumed about the communication methods.

• Security and Privacy for Provisioning Information while in transit between Initiator device and Recipient Device.
Simplified Credential Sharing Flow

1. Share Credential
2. CreateMailbox for Provisioning Information
3. mailboxurl
4. Credential Invitation over user-preferred communication method
5. accept the invitation

Loop:
6. get Provisioning Information
7. Provisioning Information
8. Additional Information
9. Additional Information
10. more Information
11. more Information

Get the Credential Provisioned
Solution: Relay Server

- Define a new transport (Relay Server) based on HTTP / REST
- Complexity handled by Relay Server
  - Unique Mailbox creation and lifecycle management
- Guarantee uninterrupted data exchange without relying on Invitation Communication method
  - Bind Initiator Devices to mailbox at time of creation
  - Bind Recipient Device to mailbox at time of first redemption.
  - Thus creating a tunnel between Initiator device and Recipient Device
- Privacy by design - not requiring user identity to transport Provisioning Information
Provisioning Information Structure

- Provisioning Information format differs by Verticals.

- A generic structure defined using JSON to pack Provisioning Information in encrypted form
  - Allows clients to create and consume information easily.
  - Works for all Verticals.

- A single message (shareURL) that can be sent over user-preferred channels (WhatsApp, SMS, email, etc.)

- Preview information recognized by messaging applications - OpenGraph + html
Seamless User Experience

• A single ShareURL used for multiple purposes
  1. Fetch share preview to display to User,
  2. Read encrypted Provisioning Information,
  3. Update encrypted Provisioning Information

• Example ShareUrl: (https://{RelayServerHost}/v{ApiVersion}/m/{MailboxIdentifier}?v={CredentialVertical})

• Push Notifications delivered to user devices during round trips
Deployments

- Entire solution (Relay servers, client applications) is deployed in the market by industry

- At least one Vertical is sharing Credentials over the deployed solutions.
  - Note that Vertical involves various companies that manufacture the type of property.

- More Verticals can start sharing Credentials soon.

- More industry partners are in the process of deploying Relay Servers to unlock more use case.