Tigress Working Group

Transfer dIGital cREdentialS Securely

July 27th, 2022

Topic	Speaker
Problem Statement	Casey
Goals	Casey
Vocabulary	Casey
Use Cases	Alex
Requirements	Alex
Out of Scope	Alex
Q & A	All
Proposed Solution	Dmitry
Stateless Workflow	Dmitry
Stateful Workflow	Dmitry
Q & A	All

Authors and Contributors

- Dmitry Vinokurov
- Alex Pelletier
- Nick Sha
- Casey Astiz
- Matt Byington
- Matthias Lerch

- Ben Chester
- Jean-Luc Giraud
- Yogesh Karandikar
- Alexey Bulgakov
- Tommy Pauly
- Crystal Qin
- Adam Bar-Niv
- Manuel Gerster
- Igor Gariev

Problem

Problem Statement

Problem Statement

Today, no standardized method exists in a cross-platform, cross-vertical capacity that would enable users to share secure credentials.

Goals

Goals

Created by Flatart
from the Noun Project

Minimize Friction for Sharing

Goals

Created by Flatart
from the Noun Project

Minimize Friction for Sharing

Maintain Access Control

Goals

Created by Flatart
from the Noun Project

Minimize Friction for Sharing

Maintain Access Control

Security and Privacy

Problem Vocabulary

Problem Vocabulary

Credential Authority

Problem Vocabulary

Credential Authority

Credential Information

Problem Vocabulary

Credential Authority

Provisioning Information

Credential Information

Problem Vocabulary

Credential Authority

Provisioning Information

Credential Information

Sender Device

Problem Vocabulary

Credential Authority

Provisioning Information

Receiver Device

Credential Information

Sender Device

Problem Vocabulary

Credential Authority

Provisioning Information

Receiver Device

Credential Information

Sender Device

Relay Server

Use Cases

Use Cases

Vehicle

Friend

Valet

Use Cases

Residential

Visitor

Housekeeper

Use Cases

Hotel

Partner

Friends

Requirements

Solution Expectations

Solution Expectations

- Allow share initiation over any channel

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview
- Allow multiple round trip communications

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview
- Allow multiple round trip communications
- Allow sender and recipient online at different times

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview
- Allow multiple round trip communications
- Allow sender and recipient online at different times
- Allow opaque message content

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview
- Allow multiple round trip communications
- Allow sender and recipient online at different times
- Allow opaque message content
- Allow a variety of types of credentials to be transferred

Solution Expectations

- Allow share initiation over any channel
- Allow share invitation preview
- Allow multiple round trip communications
- Allow sender and recipient online at different times
- Allow opaque message content
- Allow a variety of types of credentials to be transferred
- Allow management of share by Sender or Receiver

Security Goals

Security Goals

- Ensure only the intended recipient is able to provision

Security Goals

- Ensure only the intended recipient is able to provision
- Ensure credential can only be provisioned once (anti-replay)

Security Goals

- Ensure only the intended recipient is able to provision
- Ensure credential can only be provisioned once (anti-replay)
- Ensure sender has the intent to transfer

Privacy Values

Privacy Values

- Server should not be able to associate sender and receiver

Privacy Values

- Server should not be able to associate sender and receiver
- Server should not see shared content

Privacy Values

- Server should not be able to associate sender and receiver
- Server should not see shared content
- Server should not be able to intercept or redeem

Out of Scope

Out of Scope

- Mechanism for receiver to accept share with credential authority

Out of Scope

- Mechanism for receiver to accept share with credential authority
- Mechanism for sender to get provisioning information from credential authority

Out of Scope

- Mechanism for receiver to accept share with credential authority
- Mechanism for sender to get provisioning information from credential authority
- User Interface (UI) for sender or receiver

Out of Scope

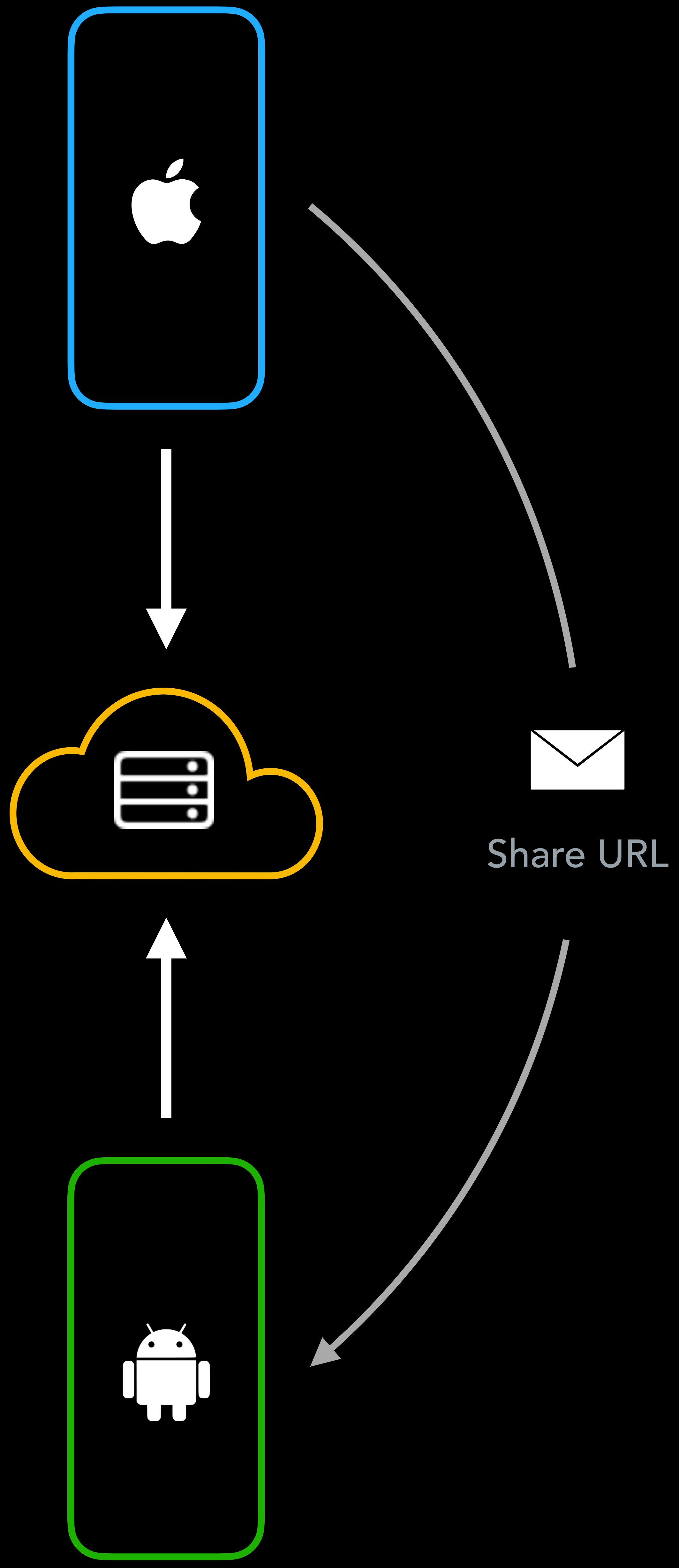
- Mechanism for receiver to accept share with credential authority
- Mechanism for sender to get provisioning information from credential authority
- User Interface (UI) for sender or receiver
- Format or content of encrypted data

Q&A

Technical Solution

Relay Server

- Establishes “connectivity” between sender and recipient
- Simple mailbox, decoupled from provisioning logic
- Only sees encrypted data and metadata



Sender

Upload
Provisioning Information

Relay Server

Share URL

Fetch
Provisioning Information

Recipient

Stateless and Stateful flows

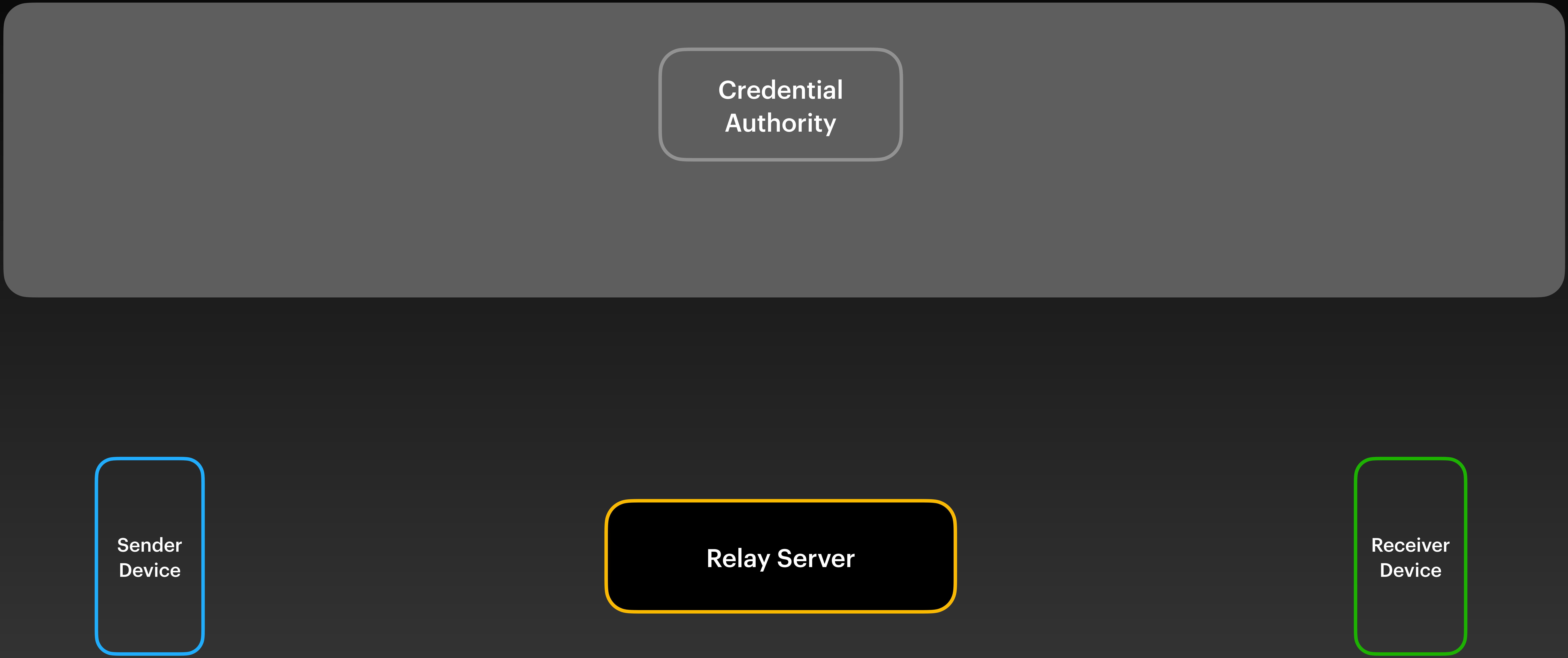
- In Stateless flow there is a single credential data transfer:
  - Sender -> Relay -> Receiver

- In Stateful flow there are multiple data transfers between Sender, Relay and Receiver to prepare credential data for registering or provisioning by Receiver
  - Sender -> Relay -> Receiver
  - Additional round trip between Receiver and Sender for new credential authorization

APIs

- **C**reate Mailbox: POST /{version}/m
- Read Display Information from Mailbox: GET /{version}/m/{mailboxIdentifier}
- **R**ead Secure Content from Mailbox: POST /{version}/m/{mailboxIdentifier}
- **U**pdate Mailbox: PUT /{version}/m/{mailboxIdentifier}
- **D**elete Mailbox: DELETE /{version}/m/{mailboxIdentifier}

Sharing Process



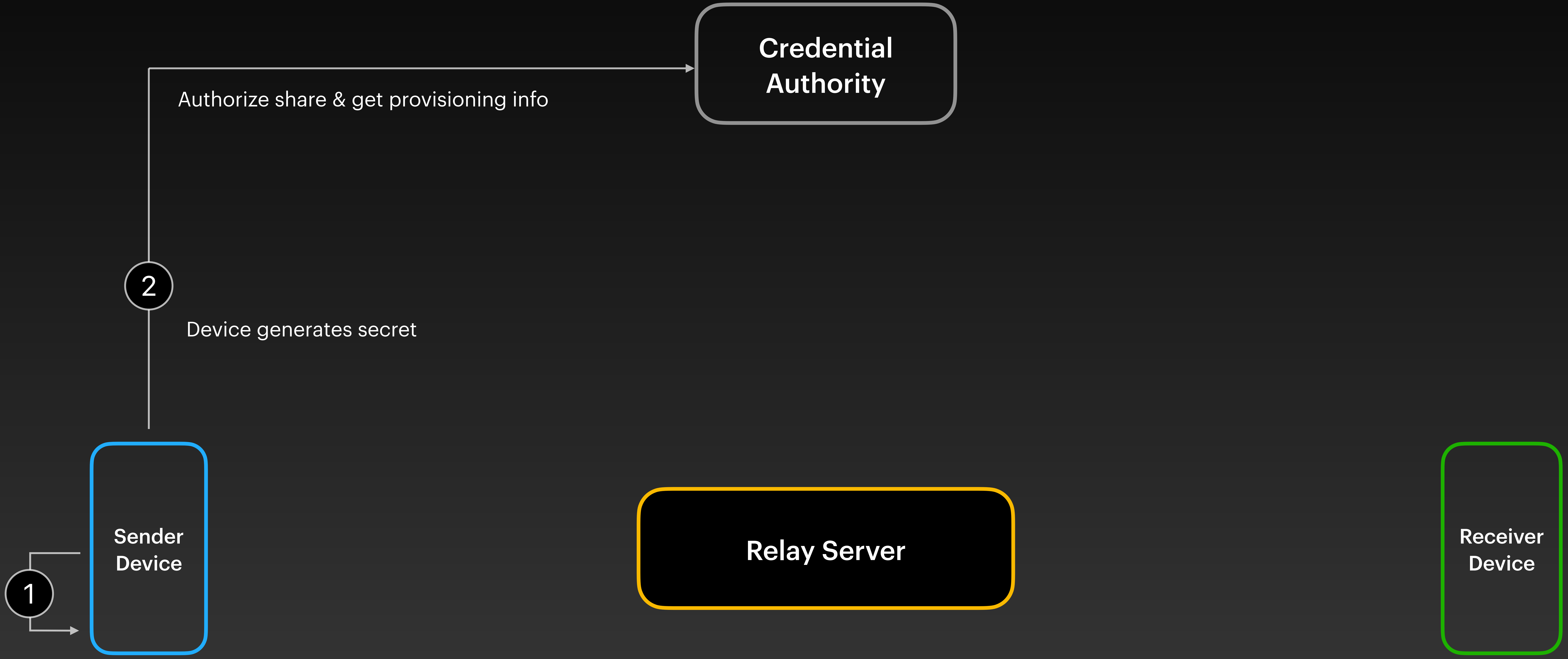
Credential Authority

Sender Device

Relay Server

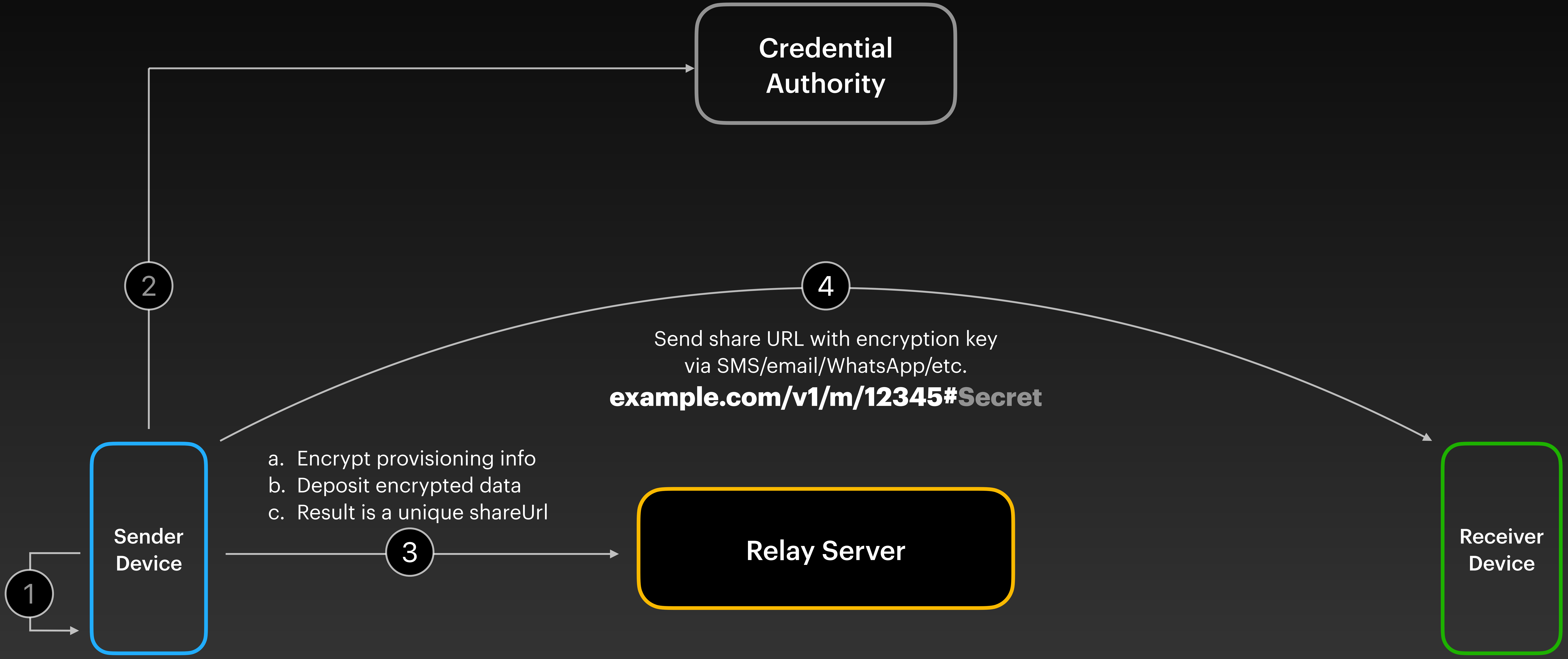
Receiver Device

Stateless Sharing Process



a. Sender initiates Wallet sharing process
b. Sender configures recipient’s entitlements & capabilities

Stateless Sharing Process

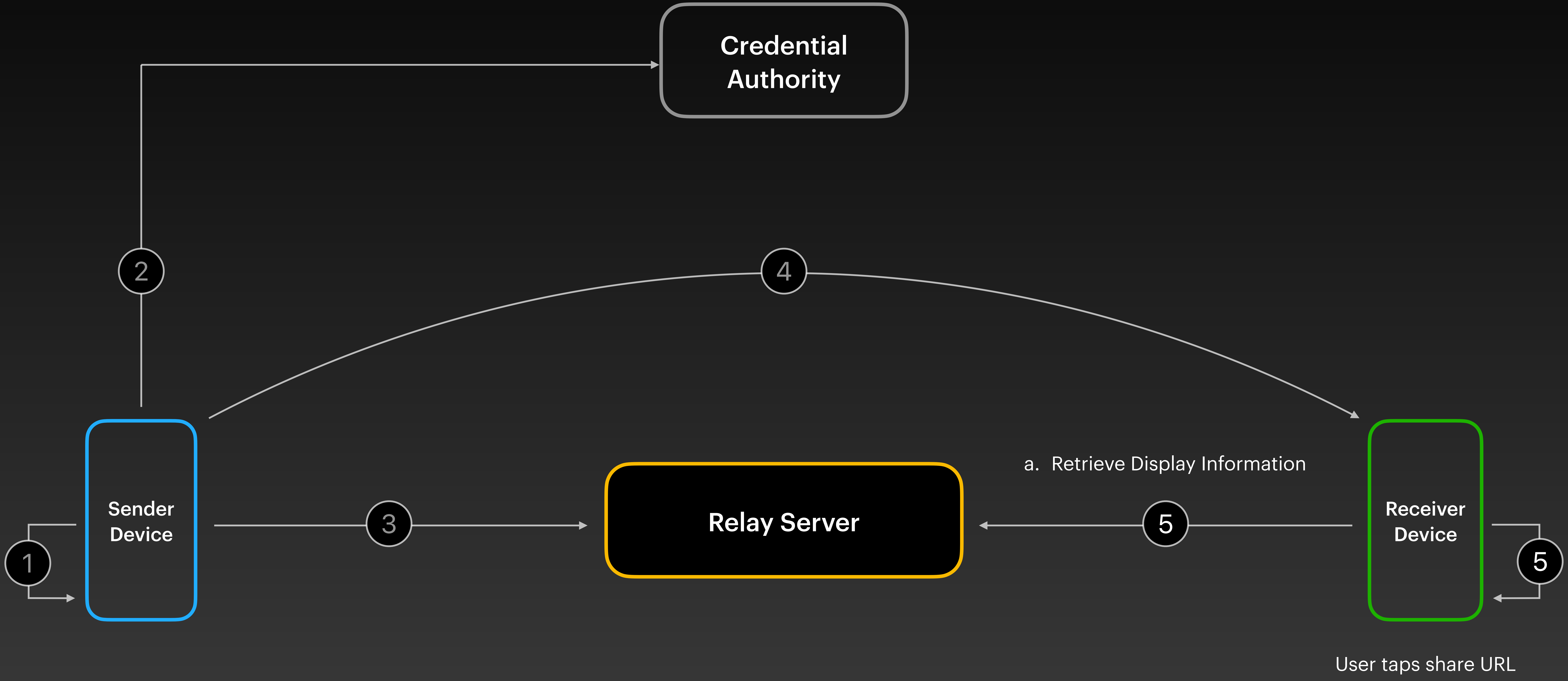


Send share URL with encryption key via SMS/email/WhatsApp/etc.

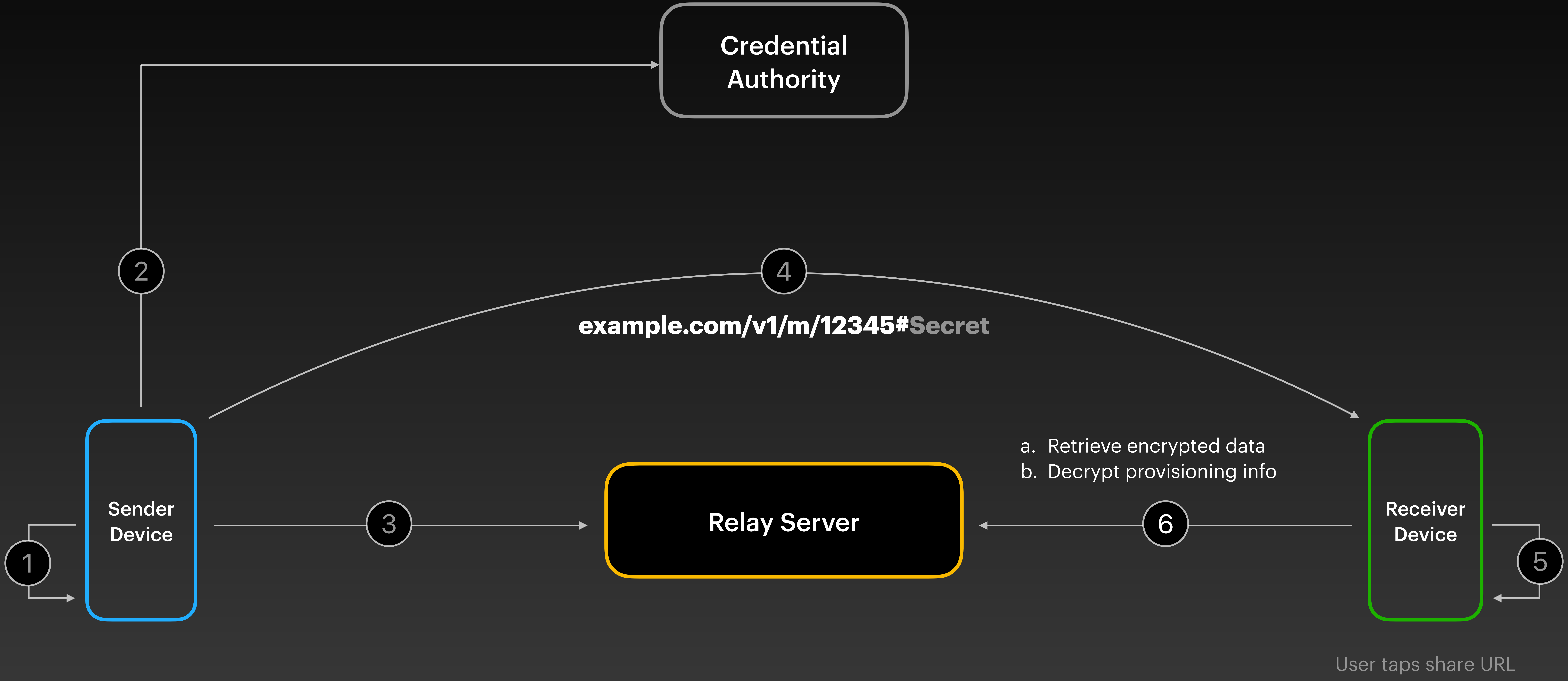
example.com/v1/m/12345#Secret

a. Encrypt provisioning info
b. Deposit encrypted data
c. Result is a unique shareUrl

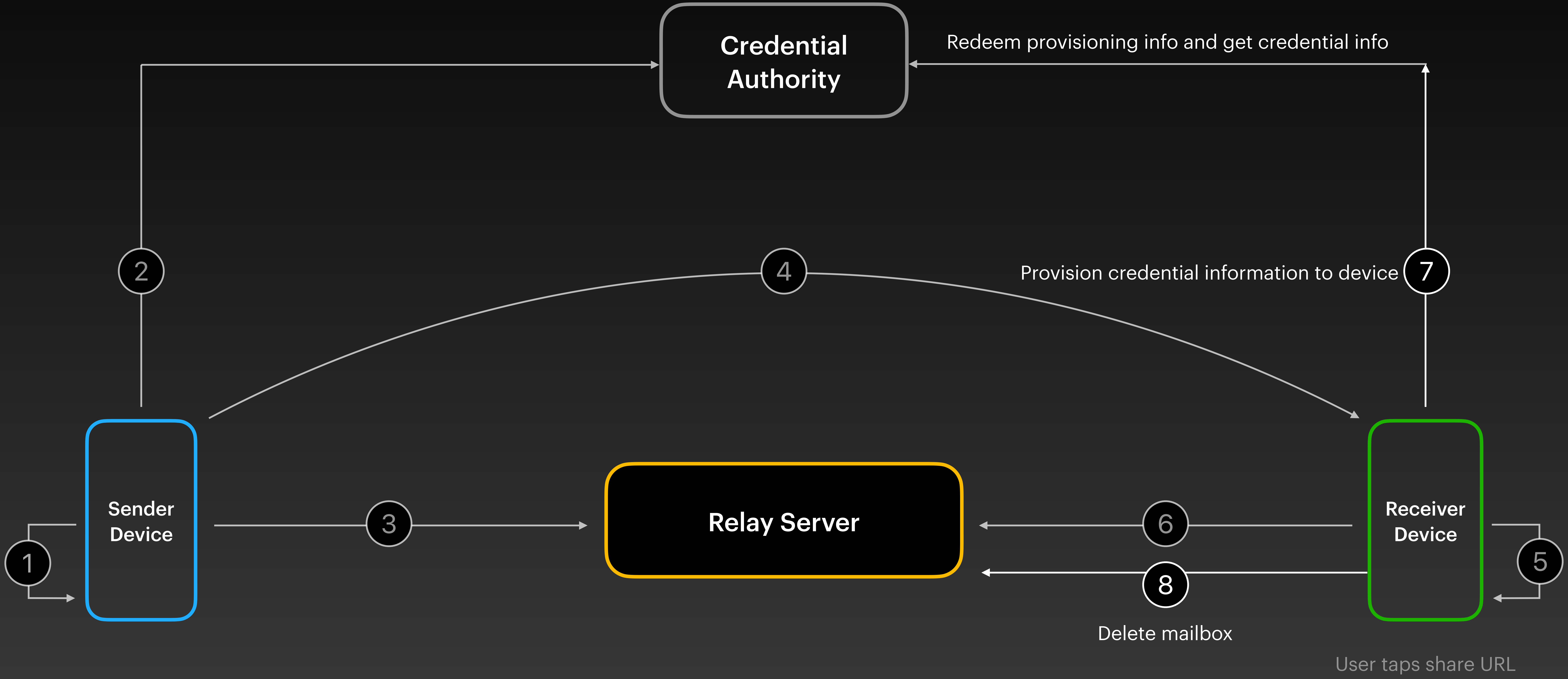
Stateless Sharing Process



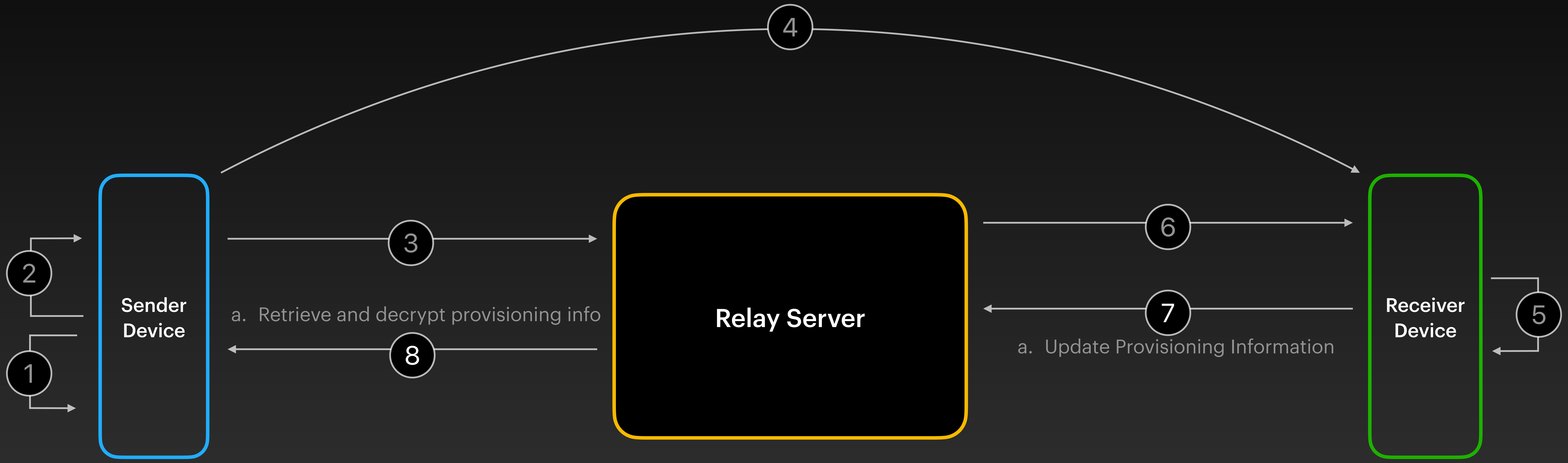
Stateless Sharing Process



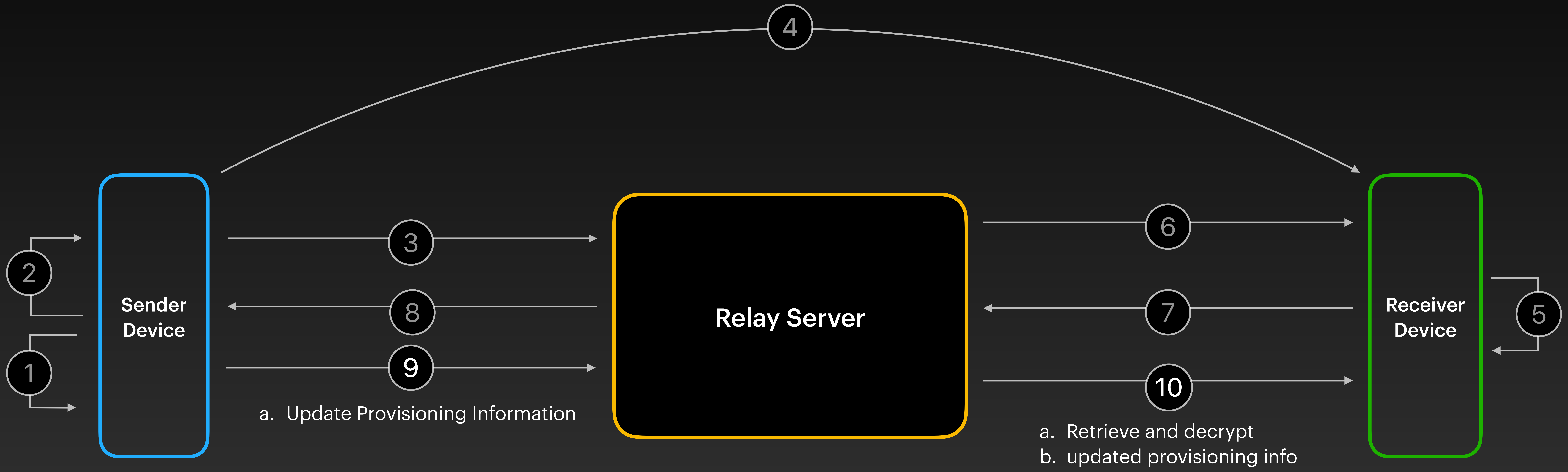
Stateless Sharing Process



Stateful Sharing Process


4
2
1
Sender Device
3
a. Retrieve and decrypt provisioning info
8
Relay Server
6
7
a. Update Provisioning Information
Receiver Device
5

Stateful Sharing Process



a. Update Provisioning Information

a. Retrieve and decrypt
b. updated provisioning info

User taps share URL

Ending Notes

- Tigress Problem and Solution.
- Goals.
- IETF adoption.
- https://datatracker.ietf.org/doc/draft-secure-credential-transfer/

Thank you!

Q&A