

# BoF: Secure Credential Transfer

IETF Draft: draft-secure-credential-transfer

February 2022

# Notes

- This BoF endeavors to explain the problem statement, assumed constraints, use cases and technical requirements in detail
- Goal: Establish working group
- We want all parties to understand the problem that the new working group would attempt to solve
- We will present a potential solution - this should be discussed in the aforementioned working group, once it's established - not in this BoF
- Clarification questions are welcome in this forum

# Problem Statement

- Many users take advantage of the security and convenience of digital credentials on mobile smartphones in their everyday lives.
- These smartphones are manufactured by different companies and run different operating systems, or “platforms”.
- The digital credentials are available to users for multiple “verticals” - such as gaining physical access to a car, home, hotel, or place of business.
- There are many situations in which it is desirable to share such a digital credential with another person. (Detailed examples will be shared later in the “Use Cases” section.)
- Today, no standardized method exists in a cross-platform, cross-vertical capacity that would enable users to perform such a sharing operation.

# Assumed Constraints

- Whereas the provisioning and usage of digital credentials is highly specific to a myriad of existing specifications and protocols (e.g. ISO18013), the solution the WG comes up with shall only attempt to solve for the transfer of such credentials and not dictate how they are provisioned nor managed on the various platforms.
- In the highly mobile world we live in, we must not require both devices (sender and receiver) to have an active internet connection concurrently for the transfer to be successful.
- Due to the sensitive nature of these credentials, the solution must consider vital security and privacy aspects to the transfer operation.

# Assumed Constraints

## (Continued)

- Due to the security primitives guaranteed by the hardware, it is not possible to transfer the credentials themselves to another entity or person.
- Instead, the sender will authorize the receiver to provision or register a new credential with a subset of the privileges/entitlements that the sender has.
- Certain protocols (such as Digital Car Key defined in the Car Connectivity Consortium) require specific cryptographic data from the sender in order for the vehicle to trust the receiver's credential.

# Assumed Constraints

## (Continued)

- Due to the potential offline nature of mobile devices as mentioned previously, the transfer operation may require multiple steps.
- In order to achieve a standard that works across platforms, it's reasonable to assume that the solution must allow the sender to share the credential in varying communication protocols such as, but not limited to, SMS, email, or proprietary messaging applications.

# Use Cases

## Vehicle

- I own a vehicle. The vehicle supports digital keys which comply with the CCC open standard. I would like to let my friend borrow my car for the weekend.
- I own a vehicle that I share with my partner. I would like to share my car key indefinitely to my partner without restrictions.
- I would like to share my car key with a Valet driver at a hotel or restaurant.

# Use Cases

## Vehicle (continued)

- I own a vehicle and have a CCC-compliant credential on my mobile device. My friend is hiking without cellular service. I want to share my key with them. I initiate the share. Once their device comes back online, they receive & accept the share.
- I own a vehicle and have a CCC-compliant credential on my mobile device. I send the share invitation to my friend. When they later accept the invitation, I myself am hiking in the woods. The share completes when my device gets back online.



# Use Cases

## Home

- I own a single family home. My dog walker comes on Thursdays to walk my dog, Skipper. I would like my dog walker to be able to enter my home on Thursdays, between 8 AM and 12 PM only.
- I own a home, and am having a friend over. They are going to get there before me, and I would like them to have access so they don't have to wait in the cold.
- I have a housekeeper that comes on Fridays. I want to send them a key that will unlock the front door on that day.
- I own a home. I want to share a digital house key with an individual renting my home for a period of time.

# Use Cases

## Hotel

- I am staying at a hotel next week. The hotel supports digital access credentials and I provisioned the credential onto my phone. My significant other is joining me, but they don't arrive until the day after I do. I want to send them the hotel key digitally so they can access the room when they arrive.
- I am staying in a hotel that I'm sharing with several people. I have paid for the hotel room and listed 3 total adults. I will share access to the two other individuals so they have digital access credentials and can enter the room as well.

# Requirements

- Sufficient security measures should be taken to ensure only the intended recipient is able to receive and provision the credential.
- The sharing invitation must be able to be sent thru any communication channel.
- Sender and receiver should not be required to be online at the same time to initiate nor complete a transfer.

# Requirements

## (Continued)

- Sharing mechanism should work for many types of credentials.
- Solution should provide a privacy-friendly method of transport.
- The sender should be able to cancel pending share requests.

# Q&A