SECRET BOF

IETF113ish

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Agenda

1. Note Well
2. Chairs intro
3. Presentation on secure credentials transfer
    a. Problem statement
    b. Constraints
    c. Use cases
    d. Requirements
4. Discussion
5. Chartering discussion

Main Event

Charter text…

There are many situations in which it is desirable to share a digital credential with another person. For example, you may want to provide access to your vehicle to a friend or a family member. You may also want to provide access to your home to your cat sitter. Or, you may want to share a hotel key with your spouse. Today, no such standardized method exists in a cross-platform, multidisciplinary capacity.

The WG charter includes the definition and standardization of a protocol that will facilitate such credential transfers from individual to individual. The protocol will leverage a “relay server” to transfer data from sender to recipient. The scope of the transfer is limited to a single origin device and a single destination device.

Charter text…

Privacy goals include:

- The relay server should not see sensitive details of the share
- The relay server should not be able to provision the credential itself, acting as an intermediary for the recipient (MiTM)
- The relay server should not persist the identity of the sender nor receiver
- The relay server should only retain the Provisioning Information for a limited amount of time

Sufficient security measures should be embedded in the protocol in an effort to:

- Ensure only the intended recipient is able to provision the credential
- Ensure the credential can only be provisioned once (Anti-replay)
- Ensure the sender has intent to share (secure user intent)

The solution the WG comes up with must:

- Allow a sender to initiate a share
- Allow a recipient to view the share request, and provision the credential associated with the share upon receipt
- Allow dynamic message formats based on the credential type
- Allow sender device and receiver device to quickly perform multiple round trip communications

Charter text…

Out of scope topics for the proposed WG are:

- Defining the mechanism the receiver will use (which APIs) in order to provision the credential
- The WG will define the full set of different credential types that could be shared. A subset of these credential types adhere to a public standard. For these credential types, the format of the Provisioning Information shall be defined by the appropriate standard. Other credential types may be proprietary. For these credential types, the protocol the WG aims to establish shall not define the actual format nor content of each field within the Provisioning Information.
- The User Interface (UI) that is displayed to the sender or receiver during sending or receiving - this will depend on the device OEM's UI and HI guidelines.

The WG will deliver a set of APIs and workflows to facilitate secure credential transfer. The WG must consider all Privacy and Security considerations in an effort to perform the credential transfer in a secure manner. Privacy-preserving algorithms such as field-level encryption will be used to protect data in transit.

The starting point for Secure Credential Transfer WG discussions shall be draft-secure-credential-transfer.

Questions

1. Do we understand the problem?
2. Is the problem space worth solving in the IETF?
3. Who is willing to edit drafts?
4. Who is willing to review drafts?
5. Is the charter good to go?