August 2021

Transferring Credentials Between Devices

David Mercer

Steve Paik

Ross Hewit

Transferring Credentials Between Devices

ABSTRACT

A badge user may want to use a different device, e.g., a smartphone, a smartwatch, etc., as their credential in lieu of the badge. This disclosure describes techniques to securely transfer credentials from a first device (e.g., badge) to a second device (e.g., phone) such that only one device with valid credentials exists at any time. Per the techniques, the two devices perform a cryptographic transfer to move credentials, and the credentials on the first device are destroyed. In this manner, only one credential at a time can be authenticated for the user. The techniques can operate offline, e.g., with neither device having internet access; it is just the two devices that need communicate with each other.

KEYWORDS

- Personal identity verification (PIV)
- Identification card
- Smart card
- Credential transfer
- Credential reader
- Near-field communication (NFC)

BACKGROUND

Badges or other forms of identification cards (IDs) are typically issued to employees and/or contractors of organizations to enable entry to access-controlled regions such as an office, warehouse, or other space. A badge user may want to use a device, e.g., a smartphone, a smartwatch, etc., as their credential in lieu of the badge. The transfer of credentials from one

device (e.g., card or badge) to another (e.g., mobile device) must be secure and unique, e.g., only one device with valid credentials should exist at any time.

When a badge is created, a secure chip in the badge generates a public-private key pair. The public key is exported to a trusted root certificate authority. A signed certificate is returned to the badge. The certificate and the private key enable the badge to prove to another device that it is authentic and has been enrolled in the security framework of the organization.

DESCRIPTION

This disclosure describes techniques to securely transfer credentials from a first device (e.g., badge) to a second device (e.g., phone) such that only one device with valid credentials exists at any time. Per the techniques, the two devices perform a cryptographic transfer to move credentials, and the credentials on the first device are destroyed. In this manner, only one credential at a time can be authenticated for the user. The techniques can operate offline, e.g., with neither device having internet access; it is just the two devices that need to communicate with each other, which they can achieve, for example, using near-field communications.

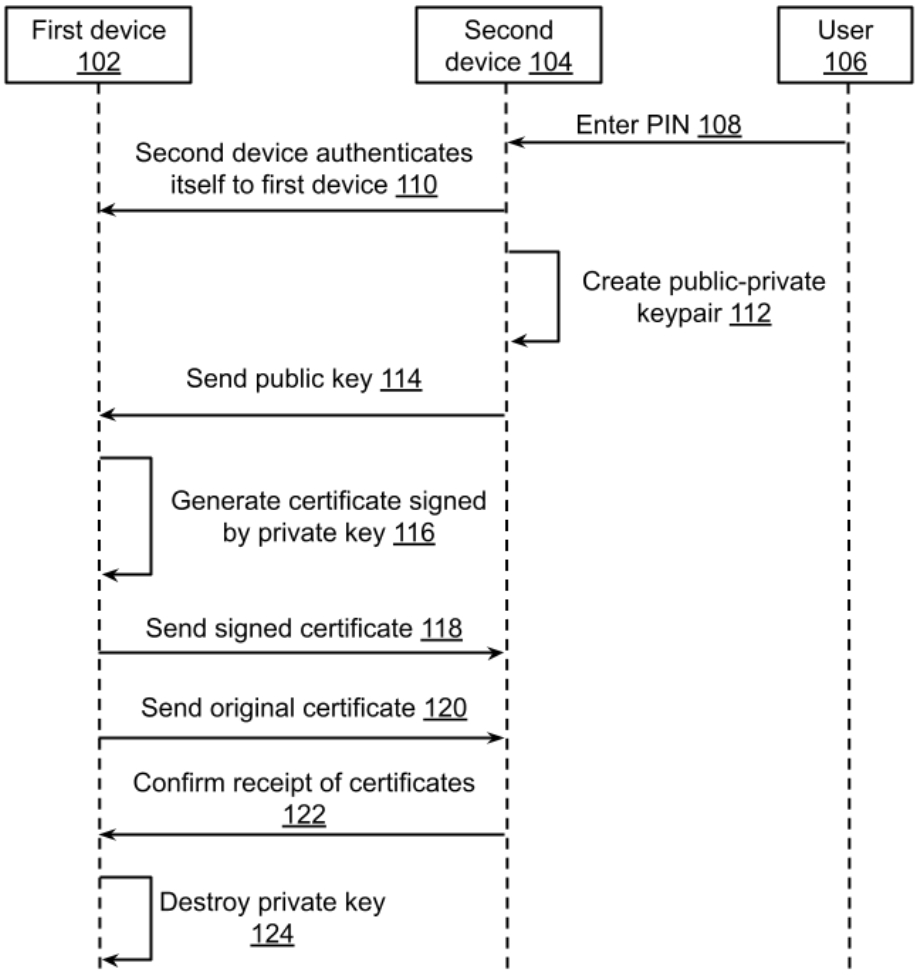

Fig. 1: Transfer of credentials between devices

Fig. 1 illustrates the transfer of credentials from a first device (102), e.g., a badge, to a second device (104), e.g., a phone, where both devices are owned by one user (106). The second device authenticates itself to the first as follows. The user enters their pre-programmed personal identification number (PIN) into the second device (108). The second device sends its trusted root certificate to the first, which the first device authenticates using public-key cryptography (110).

Once the second device is authenticated, it creates a public-private key pair (112), similar to how the first device did originally. The second device sends the public key to the first device

(114), which generates a certificate signed by the private key of the first device (116). The first device sends the signed certificate back to the second device (118). The first device also sends its original certificate (120), which it obtained from the root certificate authority, thus creating a chain of trust from the certificate authority to the second (new) device.

Once the second device has confirmed receipt of the signed certificates (122), the first device destroys its private key (124), ensuring that there is only a single leaf certificate created by the first device. Once the first device has destroyed its private key, it no longer responds to commands from any access-control reader. This procedure for credential transfer can be repeated whenever the user wishes to transfer their credential to other devices. The described techniques are applicable across identity and access control frameworks. Additionally, temporary keys can be created that expire after a certain number of uses (or a certain amount of time) to enable convenient access management that is controlled directly by the original key and/or original certificate.

When the second device is first used to enter an access-controlled area, the reader authorizing entry to the area collects the certificate chain from the second device and verifies that it was the first device that transferred the certificate to the second device. At this point, the reader can, as an optimization, issue a new certificate directly to the second device. If, at any point, the security system sees an old credential reappear after a new one has been enrolled, e.g., someone reuses the first (old) device) then *all* of the user's credentials are revoked.

The described techniques of credential transfer enable a user, e.g., an employee of a company or other organization, to self-manage their credentials without requiring a stable network interface to the security framework of the organization. The techniques make credential

management simpler and more reliable for both organization and employee, and reduce the infrastructure necessary for managing personal devices that can provide a credential.

CONCLUSION

This disclosure describes techniques to securely transfer credentials from a first device (e.g., badge) to a second device (e.g., phone) such that only one device with valid credentials exists at any time. Per the techniques, the two devices perform a cryptographic transfer to move credentials, and the credentials on the first device are destroyed. In this manner, only one credential at a time can be authenticated for the user. The techniques can operate offline, e.g., with neither device having internet access; it is just the two devices that need communicate with each other.

REFERENCES

[1] https://github.com/makinako/OpenFIPS201 accessed Jul. 27, 2021.

[2] https://csrc.nist.gov/publications/detail/fips/201/2/final accessed Jul. 27, 2021.