August 2021

Data Object Extensions for Access Control Credentials

David Mercer

Steve Paik

Ross Hewit

Data Object Extensions for Access Control Credentials

ABSTRACT

Traditional access control credentials require authentication against a backend and have no mechanism to work offline. Also, traditional credentials such as badges typically have a photo to identify the credential holder. The forgery of the outward appearance of a credential to the extent that it will pass a visual inspection is easily possible, even when modern anti-forgery techniques are employed. This disclosure describes techniques that extend security credentials to provide secure, authenticated, offline access. An authorized person can validate a badge or other credential by tapping it against an authenticated credential reader. Data on the credential is containerized such that specific data objects are accessible by specific classes of credential readers. For example, a credential reader operated by a security officer may have access to name, image, and emergency contact information stored on the credential while a credential reader operated by a receptionist can have access to only the name and image.

KEYWORDS

- Personal identity verification (PIV)
- FIPS-201
- ISO-7816
- Identification card
- Smart card
- Employee badge
- Near-field communication (NFC)
- Credential reader

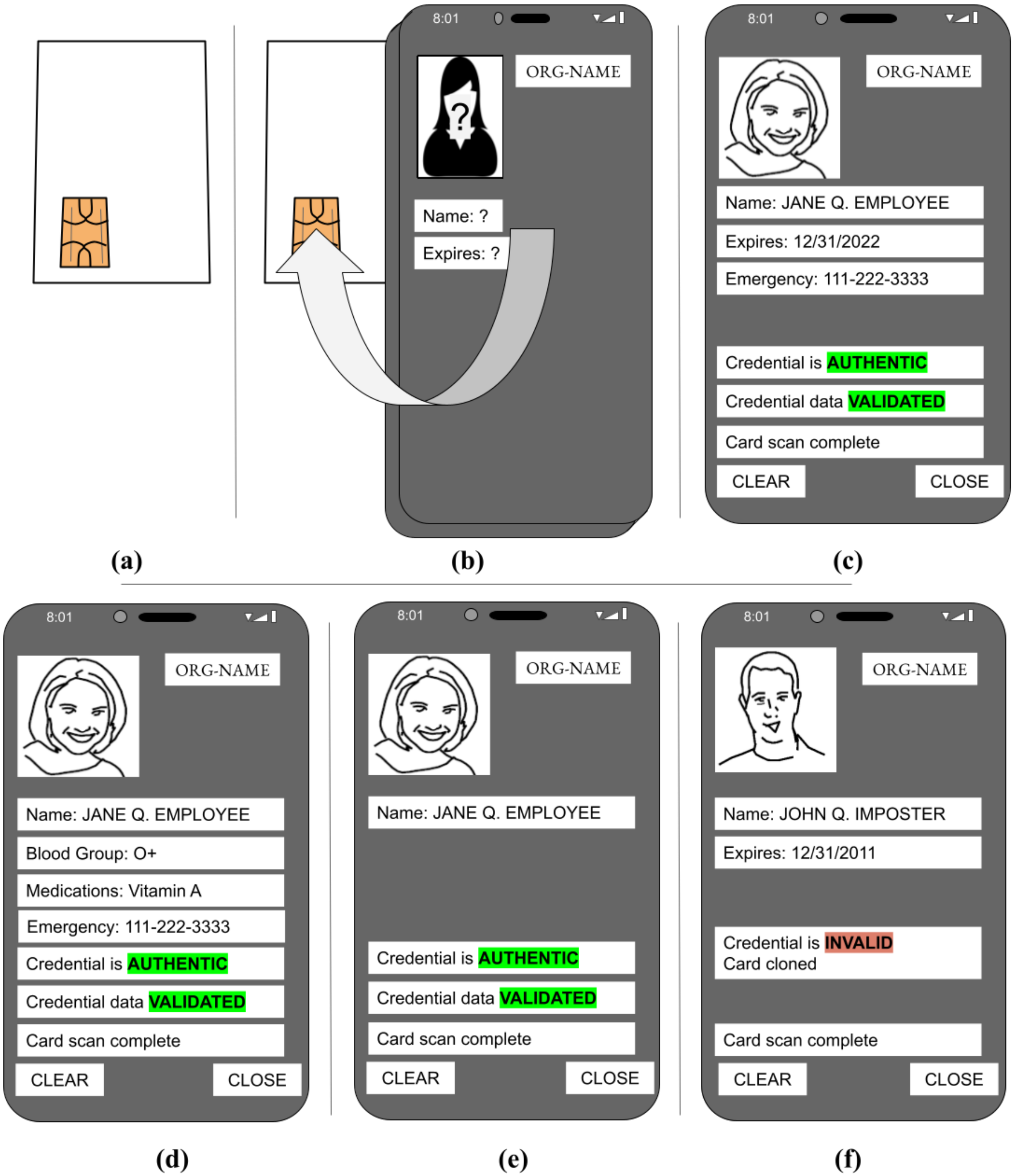
BACKGROUND

Traditional access control credentials require authentication against a backend and have no mechanism to work offline. In the event of a network connectivity failure, it is infeasible to determine if the credential (which can be in the form of a badge, smart card, mobile device, smartwatch, etc.) is valid or to obtain information about the holder of the credential.

Additionally, traditional credentials have a photo and/or other identifying information on them to identify the credential holder and/or the credentials-issuing organization. The forgery of the outward appearance of a credential to the extent that it likely passes a visual inspection is easily possible, even when modern anti-forgery techniques are employed. This poses challenges for a security officer visually verifying the validity of a credential. Besides, the appearance of a photograph on a credential can be undesirable from a privacy perspective. Also, as credentials transition away from the traditional badge or smart card form-factor to wearables, mobile phones, etc., adding physical indications (e.g., photos) of the user's identity or that of the issuing entity is infeasible.

This disclosure describes techniques that extend security credentials to provide secure, authenticated, offline access, e.g., available and operative without network connectivity. Fig, 1 illustrates a credential provided as a badge and the selective access to various stored data objects stored on the credential when accessed by different credential readers.

DESCRIPTION



Name: ?
Expires: ?

Name: JANE Q. EMPLOYEE
Expires: 12/31/2022
Emergency: 111-222-3333
Credential is AUTHENTIC
Credential data VALIDATED
Card scan complete

Name: JANE Q. EMPLOYEE
Blood Group: O+
Medications: Vitamin A
Emergency: 111-222-3333
Credential is AUTHENTIC
Credential data VALIDATED
Card scan complete

Name: JANE Q. EMPLOYEE
Credential is AUTHENTIC
Credential data VALIDATED
Card scan complete

Name: JOHN Q. IMPOSTER
Expires: 12/31/2011
Credential is INVALID
Card cloned
Card scan complete

Fig. 1: Reading a credential, e.g., a badge, with an authenticated reader such that the information displayed is based on the access class of the reader: (a) A physical badge; (b) Placing an authenticated badge reader over the badge; (c) Credential validated by a security officer; (d) Credential validated by a medical service provider; (e) Credential validated by a receptionist; (f) Credential that is detected as invalid.

As illustrated in Fig. 1, an authorized person can validate a badge (Fig. 1a) or other credential (e.g., smart card, mobile device, smartwatch, etc.) by tapping it against an authenticated credential reader, e.g., a mobile device (Fig. 1b), issued by the credential-issuing organization. Data on the credential is containerized such that specific data objects are accessible by specific classes of credential readers. For example, a security officer can have access to the facial image, personal information, and emergency contact information stored on the credential (Fig 1c); a medical service provider can additionally have access to medical information stored on the credential (Fig 1d); a receptionist can have access only to the name and facial image (Fig. 1e). Fig. 1(f) illustrates an example of an invalid credential that the reader is unable to validate.

Data extracted from the credential is secured such that it is tamper-evident and access to such data is limited to authorized devices based on access class (e.g., security officer vs. medical service provider), thus protecting the privacy of the credential holder. Effectively, a need-to-know rule is enforced, disclosing information stored on the credential based on the access class of the credential reader.

Per the techniques, the FIPS-201 data model (or similar information-security data model) is extended to include an extensible data object holding personal information in both structured and unstructured format. The data object is digitally signed using a secret, private key secured by a trusted certificate authority, rendering the data object clone-proof and tamper-evident.

A credential reader, e.g., a mobile device issued by the credential-issuing organization, requests to read the data object, using e.g., near-field communications (NFC). An authentication mechanism based on, e.g., public key cryptography, authenticates the requesting device (credential reader) to the credential such that the credential establishes trust in the requesting device before permitting it to access the data object.

When the credential reader receives the data object, it verifies the authenticity of the data object using public key cryptography. Access control restrictions are placed on other data objects (e.g., facial image, printed information, etc.) on the credential such that they can be read only when a credential reader is authenticated to the credential. As mentioned before, access to specific data objects is limited to specific classes of devices.

When an authorized device (e.g., a security officer’s mobile device provided by the credentials-issuing organization) taps a badge, the mobile device authenticates itself to the badge; reads those data objects from the badge appropriate to its access class; verifies their authenticity; and displays them to the security officer.

The techniques apply to any situations where offline or non-federated verification of credentials information is sought. For example, physical driver’s licenses typically presented for visual inspection prior to boarding an aircraft are forgeable. Per the techniques, boarding gate agents are issued credential readers, which can be, e.g., a mobile-device application. A credential reader reads and verifies a passenger’s credential (e.g., a smartcard or smartphone-based ID) issued and cryptographically signed by a trusted third party after the credential reader has authenticated itself to the passenger’s credential.

In this manner, the techniques of this disclosure provide secure, containerized data objects (e.g., name, photo, emergency information, etc.) on a credential (e.g., badge, smart card, smartphone, etc.) such that selective access to data objects is granted to different classes of credential readers. Prior to a credential reader receiving a data object, it authenticates itself to the credential and declares its class, such that the credential releases the appropriate data objects to the credential reader.

CONCLUSION

This disclosure describes techniques that extend security credentials to provide secure, authenticated, offline access. An authorized person can validate a badge or other credential by tapping it against an authenticated credential reader. Data on the credential is containerized such that specific data objects are accessible by specific classes of credential readers. For example, a credential reader operated by a security officer may have access to name, image, and emergency contact information stored on the credential while a credential reader operated by a receptionist can have access to only the name and image.

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.