Secure Patterns for Internet CrEdentials
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

B. Zundel
M. Prorock
Tradeverifyd
M. B. Jones
Self-Issued Consulting

20 October 2025

Use Cases for SPICE
draft-ietf-spice-use-cases-03

Abstract

This document describes various use cases related to credential exchange in a three party model (issuer, holder, verifier). These use cases aid in the identification of which Secure Patterns for Internet CrEdentials (SPICE) are most in need of specification or detailed documentation.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ietf-wg-spice.github.io/draft-ietf-spice-use-cases/draft-ietf-spice-use-cases.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-spice-use-cases/.

Discussion of this document takes place on the Secure Patterns for Internet CrEdentials Working Group mailing list (mailto:spice@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spice/. Subscribe at https://www.ietf.org/mailman/listinfo/spice/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-spice/draft-ietf-spice-use-cases.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

There is a need to more clearly document digital credentials that utilize the issuer-holder-verifier model across various work at IETF, ISO, W3C, and other SDOs. This need particularly arises in use cases for verifiable credentials that do not involve human-in-the-loop interactions, require strong identifiers for business entities, call for the benefits of CBOR encoding, or leverage the cryptographic agility properties of JOSE or COSE. This document covers multiple use cases for verifiable credentials that help inform both the required architecture and components, as well as to frame needs for clearly defined message formats or supporting mechanisms.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. SPICE Common Patterns

Within SPICE there are a few common patterns that continually arise:

* Selective disclosure with verifiable credentials

* Cryptographic agility support via JOSE or COSE, including support for PQC, and to permit use of the same signature algorithms with both selective disclosure as well as fully disclosed credentials

* Strong and long-lived identities that may be correlated with public key material for verification and permit binding to DNS or existing x509 certificates, as well as providing ready access to public keys for verification.

4. SPICE Use Cases

There are several expanding use cases and common patterns that motivate the working group and broader community, including:

* Microcredentials in education

* Physical supply chain credentials

* IoT, control systems, and critical infrastructure

* Credentials related to authenticity and provenance

* Offline exchange of credentials

* Attribute sharing for trusted telephone interactions

* Mobile driving licenses

* Embedding credentials in other data formats

* Digital Wallet Initiatives

5. Use Case Discussion

5.1. Roles

An "issuer", an entity (person, device, organization, or software agent) that constructs, secures, and shares digital credentials.

A "holder", an entity (person, device, organization, or software agent) that stores issued credentials and controls their disclosure.

A "verifier", an entity (person, device, organization, or software agent) that receives, verifies, and validates disclosed digital credentials.

5.2. Microcredentials in Education

Microcredentials provide a flexible and verifiable way to recognize skills, achievements, and competencies in education. Unlike traditional degrees or certifications, microcredentials offer a modular and portable format that can be tailored to specific learning outcomes. They enable lifelong learning, career advancement, and industry-aligned skill validation while allowing learners to demonstrate their achievements in a verifiable and interoperable manner.

Common use cases:

* Microcredentials for industry-specific skills such as cloud computing, cybersecurity, or data analytics, enabling verifiable skills on job applications, LinkedIn profiles, or digital resumes.

* Recognizing individual competencies as learners progress through a program, which allows institutions and employers to verify achievements more granularly.

* Stackable microcredentials that allow learners to accumulate and combine microcredentials into a larger qualification.

* Work-integrated learning and apprenticeships: skills and competencies gained through internships, apprenticeships, or on-the-job training, enabling employers to issue digital credentials for workplace learning experiences.

* Recognition of informal learning, community-based education, or non-degree programs to support individuals without access to traditional higher education.

5.3. Physical Supply Chain Credentials

Physical supply chains provide several unique scenarios and requirements for implementers of digital credentials. There is a strong movement toward digitization of physical supply chain documents which are typically exchanged on paper or scanned pdf form today using legacy approaches. Some steps have been taken towards digitatization of supply chain documents using XML, however this has proved problematic over native binary formats due to the complexity, size, and volumes of transmission often involved.

Common use cases for physical supply chains include:

* Regulatory data capture and exchange with governmental bodies

* Requirements around capturing specific types of data including:

  - Inspection information

  - Permits

  - Compliance certification (both regulatory and private)

  - Traceability information, including change of control and geospatial coordinates

* Providing the ability for 3rd parties to "certify" information about another actor in the supply chain. e.g., Vendor A is an approved supplier for Company X

* Passing of data between multiple intermediaries, before being sent along to customs agencies or consignees.

* Moving large amounts of signed data asyncronously, and bi-directionally over a network channel

* Identifying actors in a supply chain and linking them with legal entity information

5.4. IoT, Control Systems, and Critical Infrastructure Credentials

The deployment of digital credentials in constrained systems such as IoT, control systems, and critical infrastructure environments introduces challenges. These systems often operate in environments with strict security, latency, and interoperability requirements. Digital credentials play a role in ensuring secure device identity, access control, and trusted data exchange between interconnected systems.

Common use cases include:

* Device identity and authentication ensuring only authorized IoT devices can connect to a network or control system.

* Restricting access to critical systems, such as industrial control systems, SCADA networks, and energy grid controllers, to only authorized personnel and devices.

* Role-based access control (RBAC) and attribute-based access control (ABAC) policies using digital credentials.

* Encrypted and authenticated data exchange between industrial sensors, actuators, and control systems.

* Verifying software updates and firmware integrity using signed credentials to prevent unauthorized modifications.

* Tamper-resistant logging and auditing: digitally signed operational logs and sensor data to enable post-incident forensic analysis.

* Temporary access credentials for emergency personnel and automated response systems during critical incidents.

5.5. Credentials related to Authenticity and Provenance

Due to a proliferation of AI-generated or modified content, there is an increased need to provide the ability to establish the provenance of digital materials. Questions of authenticity and the means of creation (human created, machine assited, machine created) also abound. In cases where an AI created the content, providing the model information related to the generation of that content is becoming increasingly important.

Common use cases include:

* Determining whether a received piece of media is human created, and that the content is authorized for certain uses.

* Providing the ability to trace training materials for LLMs and similar models to output

* Understanding if media was created by an authoritative or trustworthy source

5.6. Offline exchange of credentials

Many real-world scenarios require credentials to be disclosed, verified, and validated without continuous or immediate access to online services. This can be due to network limitations, privacy concerns, or operational constraints in environments where connectivity is intermittent or unavailable. Some digital credential frameworks assume online verification mechanisms, which may not be suitable for offline-first environments where entities must verify credentials using locally-available data and cryptographic techniques.

Common use cases include:

* Identity verification in disconnected environments, such as remote regions, military operations, or disaster recovery efforts.

* Travel and border security, where credentials such as visas, vaccination records, or national IDs must be verified in locations with limited or no network connectivity.

* Access control in secure facilities, such as industrial sites, research labs, or private events.

* Device authentication in air-gapped systems.

* Peer-to-peer credential sharing.

5.7. Attribute Sharing for Trusted Telephone Interactions

When a user subscribes to a telecom operator, a subscription identifier is issued that enables the operator to identify the user. However, the subscription information is limited. Operators or Over-the-Top (OTT) providers with the capability to verify user VCs, which serve as reliable proofs of users' attributes, enable a user to share those attributes over a telecom network.

Common use cases include:

* Bank employees taking calls from customers can receive digitally signed account information, which enables a smoother experience for the customer and a higher level of assurance for the bank.

* Identification of the user across network domains supports mobility in a larger area (e.g., cross-border traveling, studying abroad) by endorsing attributes (e.g. , “subscriber of a legal operator”).

* Disclosure of a user’ s role or affiliation to other parties during a phone call by presenting the attributes endorsed by the operator or OTT providers.

* Operator or OTT provider service provisioning by verifying user attributes (e.g., subscription status)

5.8. Mobile Driving Licenses

The primary purposes of a driving licence are to confirm identity and convey driving privileges. In order to be trustworthy, issuers take duty to do identity proofing seriously. The trusted identity attributes (e.g., photo, address, date of birth/age, full name) confirmed by these issuers are of value to establishments that need to verify a customer’ s age, identity, current contact information, or driving privileges.

The primary use case envisioned is defined as follows:

* Holders can transmit sets of data attributes to a verifier over any communication channel supported by both parties. Data resides on the mobile device and it arrives intact with proof that there was no tampering.

5.9. Embedding Credentials in Other Data Formats

Embedding credentials within other data formats allows for the direct integration of verifiable attestations into the content itself. This binds the proof of provenance directly to the data object, allowing the the credential to travel with the content. This makes the data self-authenticating. Common data formats for embedding include PDFs, images, media files, and other structured documents.

Common use cases include:

* A news organization embedding a credential within a PDF of a news article that attests to its authenticity.

* A photographer’s digital camera embedding a credential in each digital image to show provenance.

* Scientific researchers embedding credentials in a research paper to attest to the integrity of the data and the validity of the research findings.

* Manufacturing companies embedding credentials in digital twins or 3D models of physical parts to prove their authenticity and supply chain provenance.

5.10. Digital Wallets

TODO digital wallet use case

6. Security Considerations

There are no security considerations for this document.

7. IANA Considerations

This document has no IANA actions.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgments

The authors would like to thank the following individuals for their contributions to this specification: Yurong Song, Lun Li, Donghui Wang, Fei Liu

Document History

-03

* Added Mobile Driving Licenses use case.

* Described Embedding Credentials in Other Data Formats.

* Added Michael B. Jones as an author.

-02

* Added telecom use case

* added contributors

* added acknowledgements

* added security considerations

-01

* Added offline use case

* Added IoT use case

* Added microcredentials use case

* Changed author affiliations

-00

* Initial individual draft

Contributors

Yurong Song
Huawei
Email: songyurong1@huawei.com

Lun Li
Huawei
Email: lilun20@huawei.com

Donghui Wang
Huawei
Email: wangdonghui124@huawei.com

Fei Liu
Huawei
Email: liufei19@huawei.com

Authors' Addresses

Brent Zundel
Email: brent.zundel@gmail.com

Michael Prorock
Tradeverifyd
Email: mprorock@tradeverifyd.com

Michael B. Jones
Self-Issued Consulting
United States
Email: michael_b_jones@hotmail.com
URI: https://self-issued.info/