

Secure Patterns for Internet CrEentials  
Internet-Draft  
Intended status: Informational  
Expires: 8 January 2026

B. Zundel  
M. Prorock  
Tradeverifyd  
7 July 2025

Use Cases for SPICE  
draft-ietf-spice-use-cases-02

## 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 CrEentials (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 CrEentials 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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 January 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Definitions . . . . .	3
3. SPICE Common Patterns . . . . .	3
4. SPICE Use Cases . . . . .	3
5. Use Case Discussion . . . . .	4
5.1. Roles . . . . .	4
5.2. Microcredentials in Education . . . . .	4
5.3. Physical Supply Chain Credentials . . . . .	5
5.4. IoT, Control Systems, and Critical Infrastructure Credentials . . . . .	6
5.5. Credentials related to Authenticity and Provenance . . . . .	7
5.6. Offline exchange of credentials . . . . .	7
5.7. Attribute Sharing for Trusted Telephone Interactions . . . . .	8
5.8. Embedding Credentials . . . . .	8
5.9. Digital Wallets . . . . .	8
6. Security Considerations . . . . .	8
7. IANA Considerations . . . . .	8
8. Normative References . . . . .	8
Acknowledgments . . . . .	9
Document History . . . . .	9
Contributors . . . . .	9
Authors' Addresses . . . . .	10

## 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 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 CBOR based verifiable credentials
- \* Cryptographic agility support via 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 utilizing HTTP

## 4. SPICE Use Cases

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

- \* Microcredentials, particularly in education
- \* Digitization of physical supply chain documents in multiple jurisdictions:
  - CBOR credentials

- High-volume system-to-system exchange of credentials
- Regulatory data and business-driven information
- \* Credentials related to IoT, Control Systems, and Critical Infrastructure
- \* Credentials related to authenticity and provenance, especially of digital media
- \* Offline exchange (in person) of credentials that may have been internet issued
- \* Attribute sharing for trusted telephone interactions
- \* 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 digitization 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 asynchronously, 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 assisted, 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. Embedding Credentials

TODO embedding credentials use case

### 5.9. 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

- 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](mailto:songyurong1@huawei.com)

Lun Li  
Huawei  
Email: [lilun20@huawei.com](mailto:lilun20@huawei.com)

Donghui Wang  
Huawei  
Email: [wangdonghui124@huawei.com](mailto:wangdonghui124@huawei.com)

Fei Liu  
Huawei  
Email: [liufei19@huawei.com](mailto:liufei19@huawei.com)

Authors' Addresses

Brent Zundel  
Tradeverifyd  
Email: brent.zundel@gmail.com

Michael Prorock  
Tradeverifyd  
Email: mprorock@tradeverifyd.com