Workgroup:
Secure Patterns for Internet CrEdentials
Internet-Draft:
draft-steele-spice-oblivious-credential-state-00
Published: 13 January 2024
Intended Status: Informational
Expires: 16 July 2024
Authors: O. Steele
Transmute

Oblivious Credential State

Abstract

Issuers of Digital Credentials enable dynamic state or status checks through the use of dereferenceable identifiers, that resolve to resources providing herd privacy. Privacy in such systems is determined not just from the size of the herd, and the cryptographic structure encoding it, but also from the observability of access to shared state. This document describes a privacy preserving state management system for digital credentials based on Oblivious HTTP that addresses both data model and protocol risks associated with digital credentials with dynamic state.

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://OR13.github.io/draft-steele-spice-oblivious-credential-state/draft-steele-spice-oblivious-credential-state.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-steele-spice-oblivious-credential-state/.

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/OR13/draft-steele-spice-oblivious-credential-state.

Status of This Memo

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

Copyright Notice

Table of Contents

1. Introduction

Digitial Credentials often have a validity period, which indicates the time at which the claims become active for the subject according to the issuer, and the time at which the issuer specifies the claims are no longer to be considered asserted by the issuer.

A typical example is a digital drivers license, which has an activation date, and an expiration date.

When the activation date is in the past, and the expiration date is in the future, we consider the license to be valid at the current time.

A verifier might wonder if such licenses are suspended or revoked, even if the validity period is acceptable.

A common solution is to the issuer of the credential to provide a resource that reflects information about the state of the credential over time.

Because issuer's track the presentation of digital credentials if a verifier where to ask the issuer about the state of a specific digital credential, it common to see credential states be merged into blocks, or herds, where an issuer can deliver the block to the verifier upon request, without learning which specific digital credential the verifier is interested in.

Unfortunatly, the metadata associated with resolving credential state can leak time and location information about the presentation of credentials over time.

This document addresses this risk by introducing a mediator which is trusted by the verifier.

2. Credential State

To simplify interpretation of resolution of credential state resources, this document uses the following aliases for the terms defined in [RFC9458].

The Verifier's Software is the Oblivious HTTP Client.

The Mediator's Credential State Resource is the Oblivious Relay Resource.

The Issuer's Gateway Resource is the Gateway Resource.

The Issuer's Credential State Resource is the Target Resource.

The critical privacy property is obtained by the verifier's client relying on the Mediator's Credential State Resource instead of Issuer's Credential State Resource.

In order to achieve this property, while preserving the property that issuer's do not know which verifier's will be interested in dynamic state information associated with their credentials, the issuer includes the identifier for their Issuer's Credential State Resource in their credential claim sets, however the verifier rewrites this URL to be their Mediator's Credential State Resource before resolution.

Editor note: is there a simpler solution here?

2.1. Identifier

While many different protocol schemes can be used to identify resources, to improve interoperability and reduce attack surface, this document requires credential state resources to be identified with https URLS, as described in [WHATWG.URL].

The following URI Templates, as described in [RFC6570] are required to improve interoperability and reduce the chances of degrading the privacy properties through the inclusion of extraneos information in the identifiers embedded in credentials.

- *issuer **MUST** support internationalizaton considerations, as described in [WHATWG.URL], for example: .example

- *mediator **MUST** support internationalizaton considerations, as described in [WHATWG.URL], for example: .example

- *resource-name **MUST** be a URN as described in [RFC4122], for example: urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

2.1.1. Issuer's Credential State Resource

```
https://{issuer}\
/credential-states/{resource-name}


https:// .example\
/credential-states/urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
```

Figure 1: Issuer Credential State Resources

2.1.2. Mediator's Credential State Resource

```
https://{issuer}.{mediator}\
/credential-states/{resource-name}


https:// .example. .example\
/credential-states/urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
```

Figure 2: Mediator Credential State Resources

2.2. Resources

Credential state resources typically rely on a similar content type as the credentials that require them.

Mixing different content types for credentials and their state, increases implementation costs and harms interoperability.

The credential state resource **MUST** be secured with the same content type that was used to secure the digital credential that has dynamic state.

For example, a JSON Web Token, [RFC7519] based digital credential must rely on a [RFC7519] based credential state resource.

There are many different content types that can be used to secure digital credentials, this document does not require a specific content type to be used.

The Accept header **MUST** be supported, and the application/cose content type **SHOULD** be supported.

2.3. Processing Credential State Resources

Validation of the digital credential state **MUST** occur after verification.

Validation of the digital credential validity period **MUST** occur before credential state checks.

Implementers are cautioned that concepts like "suspended" or "revoked" are interpretted differently and used differently by issuers.

All dynamic claims provided through credential state resources **MUST** be considered issuer defined, and cannot be interpretted globally.

Interpretting the structure of the Issuer's Credential State Resource is outside the scope of this document.

However, other documents describe this process in detail.

[W3C.VC-BITSTRING-STATUS-LIST] provides guidance on processing resources that secure the content type application/vc+ld+json, such as application/cose.

[I-D.draft-ietf-oauth-status-list] provides guidance on processing resources of the content type application/cwt, and application/jwt.

2.4. Techniques

2.4.1. CRL Distribution Points

[RFC5755] described a mechanism for verifiers to check the revocation status of attribute certificates.

2.4.2. Online Certificate Status Protocol

[RFC2560] described a protocol useful in determining the current status of a digital certificate without requiring CRLs.

2.4.3. Bitmaps

In this approach, the size of the herd is the length of the bitmap, and the state of a digital credential claim is the value of the bit at a given index.

Scaling this approach can be difficult, as a seperate list is needed for each dynamic claim in a digital credential.

This scalling challenge can be partially addressed by consuming multiple bits at a given index, however, the resulting enumeration needs to be consistently understood.

A common solution to consistent interpretation of enumerations is the establishment of a registry, however this can become impractical depending on the nature of the issuer's need to express dynamic state.

Publishing a dictionary per issuer, or per sets of issuer's can help address these challenges for some use cases.

2.4.4. Cryptographic Accumulators

[ZKA] describes an approach to expressing proofs of set membership.

2.4.5. Bloom Filters

Appendix B.2.7 of [RFC8932] mentions an application of bloom filters, that can be applied to communicating credential state assuming the probabilistic nature of bloom filters is acceptable to the verifier.

2.4.6. Transparency Services

Tree structures, such as described in [I-D.draft-mcmillion-keytrans-architecture] can be used to provide advanced membership proofs, such as proving inclusion, consistency, non inclusion, and freshness.

3. Terminology

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.

4. Security Considerations

TODO Security

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. 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>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/rfc/rfc4122>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/

RFC6570, March 2012, <https://www.rfc-editor.org/rfc/rfc6570>.

[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>.

[RFC9458] Thomson, M. and C. A. Wood, "Oblivious HTTP", RFC 9458, DOI 10.17487/RFC9458, January 2024, <https://www.rfc-editor.org/rfc/rfc9458>.

[WHATWG.URL] "URL - Living Standard", n.d., <https://url.spec.whatwg.org/>.

6.2. Informative References

[I-D.draft-ietf-oauth-status-list] Looker, T., Bastian, P., and C. Bormann, "OAuth Status List", Work in Progress, Internet-Draft, draft-ietf-oauth-status-list-00, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-status-list-00>.

[I-D.draft-mcmillion-keytrans-architecture] McMillion, B., "Key Transparency Architecture", Work in Progress, Internet-Draft, draft-mcmillion-keytrans-architecture-01, 4 December 2023, <https://datatracker.ietf.org/doc/html/draft-mcmillion-keytrans-architecture-01>.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, DOI 10.17487/RFC2560, June 1999, <https://www.rfc-editor.org/rfc/rfc2560>.

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", RFC 5755, DOI 10.17487/RFC5755, January 2010, <https://www.rfc-editor.org/rfc/rfc5755>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC8932] Dickinson, S., Overeinder, B., van Rijswijk-Deij, R., and A. Mankin, "Recommendations for DNS Privacy Service

Operators", BCP 232, RFC 8932, DOI 10.17487/RFC8932, October 2020, <https://www.rfc-editor.org/rfc/rfc8932>.

[W3C.VC-BITSTRING-STATUS-LIST] "Bitstring Status List v1.0", n.d., <https://www.w3.org/TR/vc-bitstring-status-list/>.

[ZKA] "Zero-Knowledge Accumulators and Set Operations", n.d., <https://eprint.iacr.org/2015/404.pdf>.

Acknowledgments

TODO acknowledge.

Author's Address

Orie Steele
Transmute

Email: orie@transmute.industries