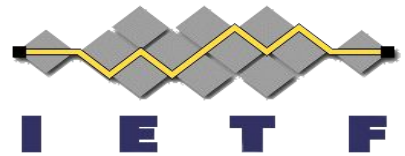
OAuth2.0 Nonce Endpoint

draft-demarco-oauth-nonce-endpoint

Giuseppe De Marco, Orie Steele

IETF 119, Brisbane
March 21, 2024



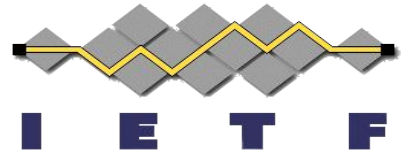
Why the Nonce is important

- Unique, one-time use, number or string (a "nonce").

- It ensures that each transaction/request is unique.

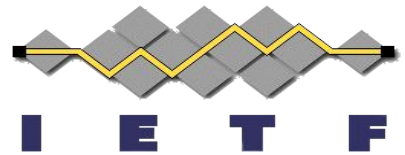
- it protects against replay attacks by making each request verifiably unique.

What's the Nonce Endpoint?



- A RESTful endpoint for issuing Nonces
- It is usable in OAuth 2.0 and any other protocols that requires the issuance of Nonces
- It can be protected or unprotected
- It overcomes, integrating, the *provisioning-by-error* we have in other specifications
- It can be used for public audiences or for internal infrastructure, as a microservice

What Does the Nonce Endpoint Do?



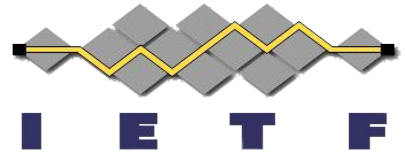
- Generates a unique, one-time use number or string (a "nonce").
- Provides nonces of particular scopes or audiences (if requested)

```
GET /nonce HTTP/1.1
Host: server.example.com
…

HTTP/1.1 200 OK
Content-Type: application/json
{
  "nonce": "d2JhY2Nhb"
}
```

```
GET /nonce?scope=pizza&aud=mario
HTTP/1.1
Host: server.example.com
…
HTTP/1.1 200 OK
Content-Type: application/json
{
  "nonce": "d2JhY2NhbG91cmVqdWFuZGFt"
}
```

Why Do It? (Purpose and Benefits)



- Cleaner API design to not overload error messages (no provisioning-by-error).
- Simple endpoints provide value to protocols other than just OAUTH, such as RATS, SCITT and SPICE.
- Nonce design considerations can be useful when considering privacy, security or availability issues associated with random, encrypted or signed nonces.
- Protecting nonce endpoints may open the opportunity to create new flows

Status

- Just recently published -00
- Some discussion and interest from SCITT, SPICE and RATS, as a building block for credential exchange or credential status apis.

… A straightforward and versatile specification for broad applications.

Next Steps

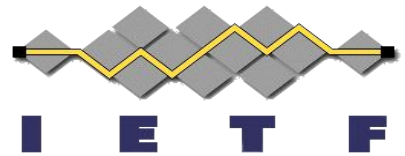
- Encourage use beyond OAuth 2.0.
- Support multiple payload formats, not just JSON.
- Enhance Nonce guidance: random, signed, encrypted.
- Include use case examples.
- Reevaluate architectural strategy.
- Is our future monolithic or modular?
- New direction?

OAuth Status Attestations

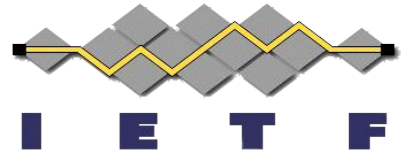
draft-demarco-oauth-status-attestations

Giuseppe De Marco, Orie Steele, Francesco Marino

IETF 119, Brisbane
March 21, 2024



What’s the Status Attestation?



- It is a signed artifact (JWT) demonstrating the validity of a digital credential, ensuring it hasn't been revoked or expired.
- It is issued by the same Issuer of the digital credential.

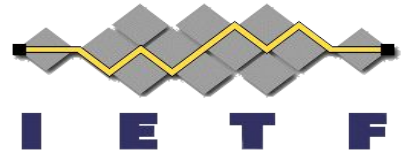
Purposes and Benefits

Enhances Privacy
Designed to protect user privacy by minimizing data exposure and ensuring transactions cannot be linked back to status requestors.

It allows verifiers to trust the authenticity and current status of presented credentials without direct contact with the issuer.

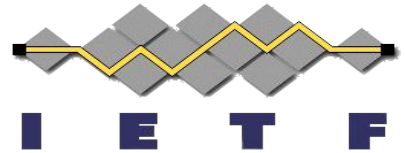
Offline Flows
It enables the verification of a credential's status without needing real-time access to the credential issuer, supporting use cases with limited connectivity.

Example: *A Digital Credential with a Status*




```
{
    "vct": "https://credentials.example.com/identity_credential",
    "given_name": "John",
    …
    "birthdate": "1990-01-01",
    "is_over_18": true,
    "is_over_21": true,
    "is_over_65": false,
    "status": {
       "status_attestation": {
           "credential_hash_alg": "sha-256",
       }
    }
}
```

Example: *Holder Requesting a status attestation*



Request

```
POST /status HTTP/1.1
Host: issuer.example.org
Content-Type: application/x-www-form-urlencoded
// it might consume a nonce
credential_pop=$digitial_credential_pop
```

Response

```
HTTP/1.1 201 OK
Content-Type: application/json
{
  "status_attestation": "eyJhbGciOiJFUzI1Ni ...",
}
```

Why Do It?

Address network security and privacy issues with anonymous access status lists: because **Anonymous is not entirely anonymous**, due to tools like WHOIS, reverse DNS, and GeoIP that can uncover information about the entity behind an internet protocol address.

All credentials and their status attestation are presented by holders under user control.

Simplify verification process for presentations of credentials with dynamic state.

Status

Just published -00

Editor's copy as well here with several fixes.

Implementer interest for COSE based digital credentials.

Next Steps

- Improve privacy considerations
- Address RATS terminology “Evidence / Endorsements”
  - Discussion about name change:
    - Attestation is an abused term
    - Status Assertions seems the way to go
    - Suggestions are welcome.
- Considerations for CWT
- Explain relationship to Nonce Endpoint
- Adopt?