Network Working Group
Internet-Draft
Intended status: Informational
Expires: 18 March 2026

R. Ehlers
PastWipe S.L.

September 2025

RepSec Non-Reusable Data Extension (NRU)
draft-ehlers-repsec-nru-00

Abstract

NRU specifies one-time, cryptographically bound tokens that couple a dataset identifier to a requester context. Replayed or stolen datasets fail verification in the RepSec layer, preventing unauthorized reuse.

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 5 March 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Requirements 2
3. Token Format 2
4. Verification and Revocation 3
5. Security Considerations 3
6. IANA Considerations 3
7. Normative References 3
Author's Address 3

1. Introduction

NRU binds a one-time verification token to four inputs:

* _dataset_id_

* _requester_id_

* _ts_ (issuance time)

* _nonce_ (random)

Stolen copies fail verification because tokens are single-use and time-bound.

2. Requirements

Implementations MUST satisfy these requirements:

* Generate signed one-time tokens.

* Validate freshness and reject reuse.

* Consult revocation lists for compromised tokens.

3. Token Format

COSE_Sign1 payload fields are defined as follows.

dataset_id tstr or bstr.

requester_id tstr.

ts int (UNIX time).

nonce bstr (96-bit).

exp int (absolute expiry).

Ed25519 signatures are RECOMMENDED.

4. Verification and Revocation

Verifiers MUST check signature validity, single-use, freshness, and absence on a signed revocation manifest.

5. Security Considerations

TLS 1.3 [RFC8446] is RECOMMENDED for transport. Reliable time sources are REQUIRED.

6. IANA Considerations

No IANA actions.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Author’s Address

Ralph Ehlers
PastWipe S.L.
Marbella Malaga
Spain
Email: info@pastwipe.com