Network File System Version 4
Internet-Draft
Intended status: Standards Track
Expires: 1 February 2026

R. Macklem
FreeBSD
C. Lever, Ed.
Oracle

31 July 2025

Remote Procedure Call Identity Squashing via x.509 Certificate Fields
draft-cel-nfsv4-rpc-tls-othername-00

Abstract

This document extends RPC-with-TLS, as described in [RFC9289], so that a client's x.509 certificate may carry instructions to the RPC server to execute all RPC transactions from that client as a single user identity.

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://chucklever.github.io/i-d-rpc-tls-othername/#go.draft-cel-nfsv4-rpc-tls-othername.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-cel-nfsv4-rpc-tls-othername/.

Discussion of this document takes place on the nfsv4 Working Group mailing list (mailto:nfsv4@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/nfsv4/. Subscribe at https://www.ietf.org/mailman/listinfo/nfsv4/.

Source for this draft and an issue tracker can be found at https://github.com/chucklever/i-d-rpc-tls-othername.

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/.

Copyright Notice

Table of Contents

1. Introduction

1.1. Background

The Remote Procedure Call version 2 protocol (RPC, for short) has been a Proposed Standard for three decades (see [RFC5531] and its antecedents). Several important upper layer protocols, such as the family of Network File System protocols (most recently described in [RFC8881] are based on RPC.

In 2022, the IETF published [RFC9289], which specifies a mechanism by which RPC transactions can be cryptographically protected during transit. This protection includes maintaining confidentiality and integrity, and the authentication of the communicating peers.

1.2. Problem Statement

Section 4.2 of [RFC9289] states that:

> RPC user authentication is not affected by the use of transport layer security. When a client presents a TLS peer identity to an RPC server, the protocol extension described in the current document provides no way for the server to know whether that identity represents one RPC user on that client or is shared amongst many RPC users. Therefore, a server implementation cannot utilize the remote TLS peer identity to authenticate RPC users.

Mobile devices such as laptops are typically used by a single user and do not have a fixed, well known IP host address or fully qualified DNS name. The lack of a well known fixed IP host address or fully qualified DNS name weakens the verification checks that may be done on the client's X.509 certificate by the server. As such, this extension allows the client to be restricted to a single user entity on the server, limiting the scope of risk associated with allowing access to the server.

When a service is running in a dedicated VM or container, it often runs as a single assigned user identity. Handling this user identity using Kerberos is problematic, since Kerberos TGTs typically expire in a matter of hours and the service is typically a long running task. This extension allows the client to specify the single assigned user identity to the server in a manner that will not expire for a significant period of time.

When an RPC server replaces incoming RPC user identities with a single user identity, for brevity we refer to this as "identity squashing".

1.3. Summary of Proposed Solution

In the interest of enabling the independent creation of interoperating implementations of RPC identity squashing, this document proposes the use of the x.509 SubjectAltName otherName field to carry a RPC user identity. For these user squashing instructions, this document establishes a fixed object identifier carried in the "type-id" part of the otherName field, and specifies the format of the "value" part of the otherName field when "type-id" carries the new object identifier. The document also provides normative guidance on how the "value" is to be interpreted by RPC servers.

1.4. Open Questions

* Should this be an NFS-only feature, or should it be an RPC-layer feature?

* Standardizing a fixed OID is necessary for interoperability, but are we required to allocate that OID from a particular arc?

2. Requirements Language

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. x.509 Certificate SubjectAltName Field

As specified in Section 4.2.1.6 of [RFC5280]:

> The subjectAltName MAY carry additional name types through the use of the otherName field. The format and semantics of the name are indicated through the OBJECT IDENTIFIER in the type-id field. The name itself is conveyed as value field in otherName.

This document specifies new uses of the otherName field to carry an RPC user identity. The receiving system (an RPC server) then converts all RPC users (as carried in the RPC header credential and verifier fields) to the user identity specified in the certificate.

3.1. AUTH_SYS Identities

3.1.1. otherName OID for AUTH_SYS

> | State the Object Identifier to be used to indicate this form of
> | RPC user identity

3.1.2. Format of the otherName Value

> | This will be a set of 32-bit integers that specify a numeric
> | UID, and a counted list of 32-bit integers that specify numeric
> | GIDs.

3.2. Kerberos V5 Principals

3.2.1. otherName OID for AUTH_SYS

> | State the Object Identifier to be used to indicate this form of
> | RPC user identity

3.2.2. Format of the otherName Value

The otherName value contains a principal name as described in Section 4 of [RFC2743].

3.3. NFSv4 User @ Domain String Identities

3.3.1. otherName OID for String Identities

> | State the Object Identifier to be used to indicate this form of
> | RPC user identity

3.3.2. Format of the otherName Value

> | Follow recommendations of draft-ietf-nfsv4-
> | internationalization-latest to form an internationalized
> | "user@domain" string similar to NFSv4 ID map strings.

4. Extending This Mechanism

It is possible that in the future, RPC servers might implement other forms of RPC user identity, such as Windows Security Identifiers (SSIDs) [SSID]. This section describes how standards action can extend the mechanism specified in this document to accommodate new forms of user identity.

> | Provide the base level of general requirements that we will
> | have to meet in this document as instructions to future
> | authors. I’m not sure yet exactly what those are.

5. Implementation Status

> | This section is to be removed before publishing this document
> | as an RFC.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs.

Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

5.1. FreeBSD NFS Server and Client

Organization: FreeBSD

URL: https://www.freebsd.org (https://www.freebsd.org)

Maturity: Complete.

Coverage: The mechanism to represent user@domain strings has been implemented using an OID from the FreeBSD arc.

Licensing: BSD 3-clause

Implementation experience: None to report

6. Security Considerations

7. IANA Considerations

> | Insert request for allocations of a SubjectAltName : otherName
> | object identifiers

8. References

8.1. 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>.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, DOI 10.17487/RFC2743, January 2000, <https://www.rfc-editor.org/rfc/rfc2743>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/rfc/rfc7942>.

[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>.

[RFC9289] Myklebust, T. and C. Lever, Ed., "Towards Remote Procedure Call Encryption by Default", RFC 9289, DOI 10.17487/RFC9289, September 2022, <https://www.rfc-editor.org/rfc/rfc9289>.

8.2. Informative References

[RFC5531] Thurlow, R., "RPC: Remote Procedure Call Protocol Specification Version 2", RFC 5531, DOI 10.17487/RFC5531, May 2009, <https://www.rfc-editor.org/rfc/rfc5531>.

[RFC8881] Noveck, D., Ed. and C. Lever, "Network File System (NFS) Version 4 Minor Version 1 Protocol", RFC 8881, DOI 10.17487/RFC8881, August 2020, <https://www.rfc-editor.org/rfc/rfc8881>.

[SSID] Microsoft, "Security Identifiers", n.d., <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers>. Replace this with a reference to an MS standards doc

Acknowledgments

The authors are grateful to Jeff Layton, Greg Marsden, and Martin Thomson for their input and support.

Special thanks to Area Director Gorry Fairhurst, NFSV4 Working Group Chairs Brian Pawlowski and Christopher Inacio, and NFSV4 Working Group Secretary Thomas Haynes for their guidance and oversight.

Authors' Addresses

Rick Macklem
FreeBSD Project
Canada
Email: rmacklem@uoguelph.ca

Chuck Lever (editor)
Oracle Corporation
United States of America
Email: chuck.lever@oracle.com