



RFC Production Center

IETF 125



Topics

- SVG
- Tools Modernization
- GitHub and markdown



SVG Guidance

- The current profile is too limiting
- RFC 9896 “SVGs in RFCs”:
 - Provides policy requirements
 - Removes requirements regarding specific SVG profiles or implementations
 - RPC responsible for decisions about SVG tooling and implementation
- The RPC is paying attention to feedback and working on providing updated guidance
- For now, previous guidance holds: <https://authors.ietf.org/en/diagrams>
- aasvg is a handy tool for converting ASCII art to SVG:
<https://github.com/martinthomson/aasvg>

Tools Modernization



Coming soon! Mid April

- The RPC expects to issue 5-digit RFC numbers by mid-June
- New rfc-editor.org website
 - New queue subsite
 - New errata subsite
- New queue management system (aka Purple)
- DraftForge editing software

New Website

The screenshot shows the homepage of the RFC Editor website. At the top left is the RFC Editor logo with the tagline "Official home of RFCs". To the right are navigation links: "The RFC Series", "For Authors", and "About Us", each with a dropdown arrow. Further right are a search icon and a user profile icon. The main heading is "The official home of RFCs". Below this is a paragraph explaining that RFCs outline computer networking and Internet foundations, published by the RFC Editor for the IETF, IRTF, IAB, and ISE. A search bar with the placeholder text "Find an RFC (number, subseries, title, author, etc.)" and a magnifying glass icon is positioned below the text. To the right of the search bar is a link "What is an RFC?". The "Latest RFCs" section features three cards. The first card is for RFC 9945: BCP 245: IETF Community Moderation, labeled as "BEST CURRENT PRACTICE", edited by L. Eggert and E. Lear, published in February 2026 in the General Area. The second card is for RFC 9939: PKCS #8: Private-Key Information Content Types, labeled as "PROPOSED STANDARD", edited by J. Mandel, R. Housley, and S. Turner, published in February 2026 in the Security Area. The third card is for RFC 9937: Proportional Rate Reduction (PRR), labeled as "PROPOSED STANDARD", edited by M. Mathis, N. Cardwell, Y. Cheng, and N. Dukkipati, published in December 2025 in the Web and Internet Transport area. A link "Looking for works in progress? Go to datatracker.ietf.org" is located to the right of the "Latest RFCs" heading.

RFC EDITOR
Official home of RFCs

The RFC Series ▾ For Authors ▾ About Us ▾ 🔍 👤

The official home of RFCs

[What is an RFC?](#) >

RFCs outline computer networking and Internet foundations, including [Internet Standards](#) and historical or informative content. They are published by the RFC Editor for the [IETF](#), [IRTF](#), [IAB](#), and [ISE](#), which collectively form the authoritative source for RFCs

Find an RFC (number, subseries, title, author, etc.) 🔍

Latest RFCs

Looking for works in progress? Go to datatracker.ietf.org

RFC 9945: BCP 245:
IETF Community Moderation

BEST CURRENT PRACTICE

L. Eggert, Ed. ♦ E. Lear, Ed.

February 2026 ♦ IETF publication

♦ General Area

RFC 9939: PKCS #8:
Private-Key Information Content Types

PROPOSED STANDARD

J. Mandel ♦ R. Housley ♦ S. Turner

February 2026 ♦ IETF publication

♦ Security Area

RFC 9937: Proportional Rate Reduction (PRR)

PROPOSED STANDARD

M. Mathis ♦ N. Cardwell ♦ Y. Cheng ♦ N. Dukkipati

December 2025 ♦ IETF publication

♦ Web and Internet Transport

5

[Home](#)

RFC 9883: An Attribute for Statement of Possession of a Private Key

R. Housley

PROPOSED STANDARD

[RFC Tips](#)

Abstract

This document specifies an attribute for a statement of possession of a private key by a certificate subject. As part of X.509 certificate enrollment, a Certification Authority (CA) typically demands proof that the subject possesses the private key that corresponds to the to-be-certified public key. In some cases, a CA might accept a signed statement from the certificate subject. For example, when a certificate subject needs separate certificates for signature and key establishment, a statement that can be validated with the previously issued signature certificate for the same subject might be adequate for subsequent issuance of the key establishment certificate.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide

[Contents](#)
[About this RFC](#)
[Erratum 1](#)

About Errata

RFC Errata are official records of technical or editorial errors found in published RFCs, which remain unchanged once issued. You can report Errata only after verifying the issue is not already documented and constitutes a genuine error in the text rather than a request for new features or protocol changes.

[Report a new erratum](#)

Show only

Verified (1) ▾

◆ Section 3

[Scroll to Section 3](#)
Status: Verified

Date Reported: 2025-12-22

Reported By: Wenxi Wang

Original text:

The components of the PrivateKeyStatement SEQUENCE

Correct text:

The components of the PrivateKeyPossessionStatement SEQUENCE

Notes:

The correct name is PrivateKeyPossessionStatement.



New Errata Display



Full report

RFC 9883, "An Attribute for Statement of Possession of a Private Key", October 2025

Source of RFC: lamps (sec)

Errata-ID: 8687

Status: [Verified](#)

Type: [Editorial](#)

Publication Formats: [TXT](#) [PDF](#) [HTML](#)

Reported By: Wenxi Wang

Date Reported: 2025-12-22

Verified by: Deb Cooley

Date Verified: 2025-12-28

Section 3 says:

The components of the PrivateKeyStatement SEQUENCE

It should say:

The components of the PrivateKeyPossessionStatement SEQUENCE

Notes:

The correct name is PrivateKeyPossessionStatement.

[Report New Erratum](#)

[Back to List](#)

Errata Spam Reduction



- Currently, when someone creates a report, it is sent out to multiple recipients and mailing lists
- Spam gets through, but the RPC deletes it
- The new system will send the reports to the RPC first
- The RPC will triage the reports:
 - Delete spam
 - Determine whether the report is technical or editorial
- Report notification and verification occur as usual after triage:
 - RPC verifies editorial reports
 - Stream-specific parties verify technical reports

Looking for published RFCs? Go to <https://www.rfc-editor.org>

Upcoming RFCs Queue

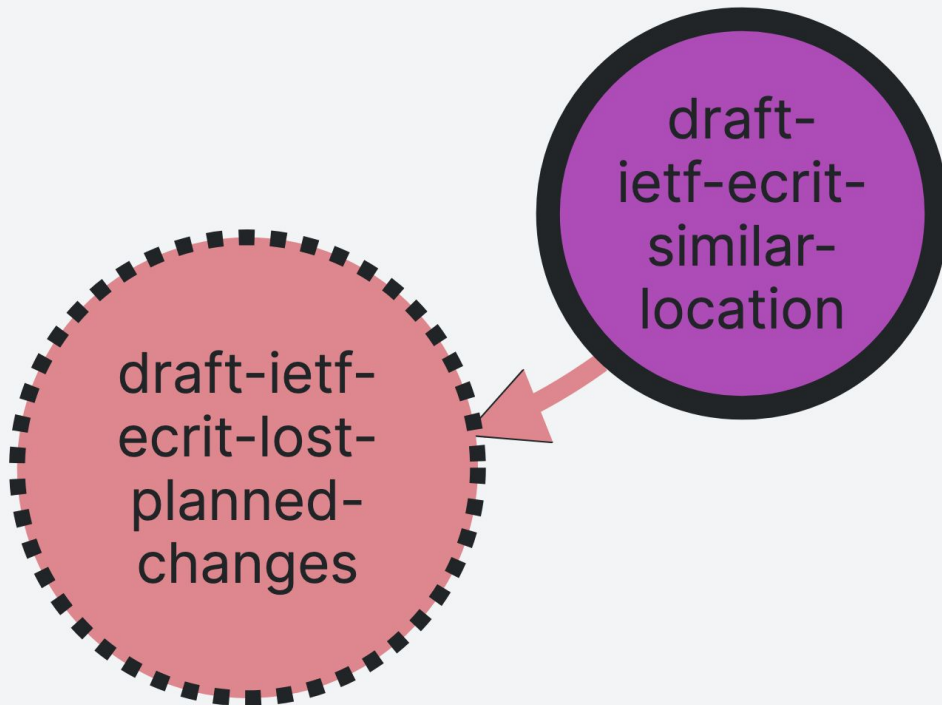
Document	Labels	Enqueue Date (Weeks in queue)	Assignments	IANA status	Cluster
draft-ietf-lsr-ospf-ls-link-infinity	Author Input Required	2026-03-15 (0 weeks)	blocked Author Input Required		
draft-ietf-lisp-geo	Author Input Required	2026-03-15 (0 weeks)	blocked Author Input Required		
draft-ietf-ccamp-optical-impairment-topology-yang		2026-03-15 (0 weeks)	blocked Reference Not Received	517	
draft-ietf-bess-evpn-unequal-lb		2026-03-15 (0 weeks)	blocked Reference Not Received	569	
draft-ietf-lamps-macaddress-on	markdown github Author Input Required	2026-03-13 (0.5 weeks)	blocked Author Input Required		
draft-ietf-ace-oscore-gm-admin		2026-03-12 (0.5 weeks)	blocked Reference Not Received	564	
draft-ietf-spring-cs-sr-policy		2026-03-12 (0.5 weeks)	blocked Reference Not Received	496	
draft-ietf-pim-updt-ipv6-dyn-mcast-addr-grp-id		2026-03-11 (0.5 weeks)	Awaiting Editor Assignment		

Queue subsites

- Clearer labels
- More details
- Visualizations of cluster dependencies



Cluster info



Pan and zoom the dependency graph after the layout settles.

Document ↕

Labels

Enqueue Date ↕
(Weeks in queue)

Assignments ↕

IANA status

Cluster ↕

[draft-ietf-ecrit-similar-location](#) @

2022-03-07
(209.5 weeks)

blocked Reference Not Received

🔍 452



DraftForge

- VS Code plugin
- Available for testing: Details at draftforge.ietf.org
- Checkers for common typos, placeholders, inconsistent hyphenation and capitalization, use of abbreviations
- Split screen: Edit RFCXML on the left, see the HTML output on the right

DraftForge

- List of checkers and tools
- An analysis of abbreviation use

The screenshot displays the DraftForge application interface. The top bar shows the workspace name "workspace [Dev Container: rfcd @ desktop-linux]". The main window is titled "IETF DRAFTFORGE" and contains two tabs: "rfc9888.xml 3" and "rfc9888.notprepped.xml". The left sidebar is divided into "VALIDATION CHECKS" and "TOOLS". Under "VALIDATION CHECKS", the "Typos Check" is selected. Under "TOOLS", "List Abbreviations" is selected. The main editor area shows the XML content of "rfc9888.xml", including the root element and a link to the document. The bottom panel displays a list of abbreviations and their usage statistics, such as "PASSporT" used 4 extra times and "STIR" used 5 extra times.

```
<?xml version='1.0' encoding='utf-8'?>
<rfc xmlns:xsi="http://www.w3.org/2001/XMLSchema" version="3"
category="std" docName="draft-ietf-stir-servprovider-oob-08"
number="9888" consensus="true" ipr="trust200902" obsoletes=""
updates="" submissionType="IETF" xml:lang="en"
tocInclude="true" tocDepth="4" symRefs="true" sortRefs="true"
prepTime="2026-03-02T18:56:26" indexInclude="true"
scripts="Common, Latin">
<link href="https://datatracker.ietf.org/doc/
draft-ietf-stir-servprovider-oob-08" rel="prev"/>
<link href="https://dx.doi.org/10.17487/rfc9888"
...
Filter (e.g. text, lexcl... DraftForge
P - "Provider" used 24 times but never abbreviated as "P"
PASSporT - used before the expansion "Personal Assertion Token" and
expansion used 4 extra time(s) after initial expansion of "PASSporT"
PM - "Pervasive Monitoring" used 2 times but never abbreviated as "PM"
PSTN - expanded as "Public Switched Telephone Network"
REST - expanded as "Representational State Transfer"
RFC - is well known and not expanded
SF - not expanded
SIP - is well known, expanded as "Session Initiation Protocol", and
expansion used 2 extra time(s) after initial expansion of "SIP"
SP - expanded as "Service Provider" and expansion used 21 extra time(s)
after initial expansion of "SP"
SPC - not expanded
STIR - expanded as "Secure Telephone Identity Revisited" and expansion
used 5 extra time(s) after initial expansion of "STIR"
```

GitHub and kramdown-rfc for AUTH48

- Goal: To further support the authoring community and facilitate author reviews using tools they are familiar with.
- The RPC is accepting 5 GitHub documents and 5 kramdown-rfc documents a month. Authors can choose to do both.
- GitHub: The RPC shares its proposed edits with authors in an RPC-created repo and a pull request made against the approved source file. Authors, WG chairs, doc shepherd, and responsible AD invited to the repo.
- kramdown-rfc: AUTH48 starts with a md file. When content changes are approved, the doc is converted to RFCXML.

This Week



Come by the desk Monday - Thursday!