

# OAuth 2.0 Proof-of-Possession (PoP) Security Architecture

[draft-ietf-oauth-pop-architecture-08.txt](#)

Nat Sakimura

# What it is - Describes PoP Architecture

... and motivates the development of such.



## Abstract

<http://bit.ly/3ID1oN7>

The OAuth 2.0 bearer token specification, as defined in [RFC 6750](#), allows any party in possession of a bearer token (a "bearer") to get access to the associated resources (without demonstrating possession of a cryptographic key). To prevent misuse, bearer tokens must be protected from disclosure in transit and at rest.

Some scenarios demand additional security protection whereby a client needs to demonstrate possession of cryptographic keying material when accessing a protected resource. This document motivates the development of the OAuth 2.0 proof-of-possession security mechanism.

# The work started in July 2014

OAuth  
Internet-Draft  
Intended status: Informational  
Expires: January 22, 2015

P. Hunt, Ed.  
Oracle Corporation  
J. Richer  
The MITRE Corporation  
W. Mills

P. Mishra  
Oracle Corporation  
H. Tschofenig  
ARM Limited  
July 21, 2014

**OAuth 2.0 Proof-of-Possession (PoP) Security Architecture**  
**draft-ietf-oauth-pop-architecture-00.txt**

That's 9 years ago and I was assuming the work has completed and ...

I pointed out an author of an academic paper I was reviewing that they may want to refer to the RFC for the categorization of non-bearer tokens.

Then, the answer “*I cannot find it*” came back.

To my surprise,

# The draft has expired and marked “dead”

## OAuth 2.0 Proof-of-Possession (PoP) Security Architecture draft-ietf-oauth-pop-architecture-08

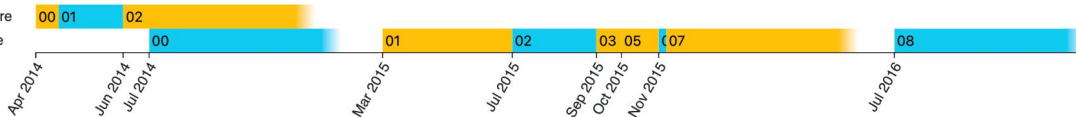
Status [IESG evaluation record](#) [IESG writeups](#) [Email expansions](#) [History](#)

### Versions:

[00](#) [01](#) [02](#) [03](#) [04](#) [05](#) [06](#) [07](#) [08](#)

draft-hunt-oauth-pop-architecture

draft-ietf-oauth-pop-architecture



Document Type Expired Internet-Draft ([oauth WG](#))

Expired & archived

Authors [Phil Hunt](#) [Justin Richer](#) [William Mills](#) [Prateek Mishra](#) [Hannes Tschofenig](#)

IESG

[IESG state](#)

Expired (IESG: **Dead**)

Action Holders

(None)

### Reviews

[OPSDIR Last Call review \(of -07\)](#)

Has Nits

[OPSDIR Last Call review \(of -07\)](#)

Ready

[GENART Telechat review \(of -07\)](#)

Almost Ready

[GENART Telechat review \(of -07\)](#)

Almost Ready

[SECDIR Telechat review \(of -06\)](#)

Ready


despite it was “Almost ready”

I still believe  
that this draft  
has useful  
information

## Table of Contents

1. Introduction	3
2. Terminology	3
3. Use Cases	3
3.1. Preventing Access Token Re-Use by the Resource Server	4
3.2. TLS and DTLS Channel Binding Support	4
3.3. Access to a Non-TLS Protected Resource	4
3.4. Offering Application Layer End-to-End Security	5
4. Security and Privacy Threats	5
5. Requirements	6
6. Threat Mitigation	10
6.1. Confidentiality Protection	11
6.2. Sender Constraint	11
6.3. Key Confirmation	12
6.4. Summary	13
7. Architecture	14
7.1. Client and Authorization Server Interaction	15
7.1.1. Symmetric Keys	15
7.1.2. Asymmetric Keys	16
7.2. Client and Resource Server Interaction	17
7.3. Resource and Authorization Server Interaction (Token Introspection)	18
8. Security Considerations	19
9. IANA Considerations	19
10. Acknowledgments	19
11. References	20
11.1. Normative References	20
11.2. Informative References	21
Authors' Addresses	22

(Source) Hunt, et al.; OAuth 2.0 Proof-of-Possession  
(PoP) Security Architecture <<http://bit.ly/3ID1oN7>>



Do we have an appetite to have it  
cross the goal line so that it can be  
referenced?

*If so, what's the next step?*