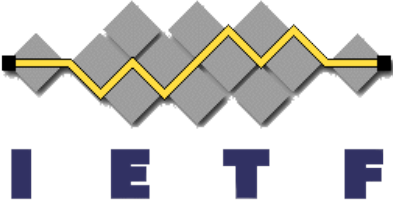


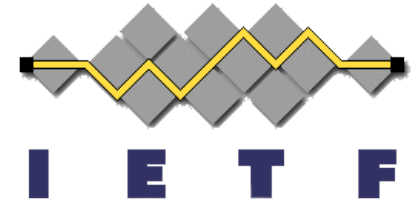
# *Split Signing Algorithms for COSE*

*draft-lundberg-cose-two-party-signing-algs*

Mike Jones, Emil Lundberg  
IETF 125, Shenzhen  
March 20, 2026



# IETF 124, Montreal Presentation

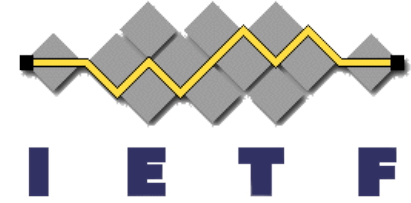


- <https://datatracker.ietf.org/meeting/124/materials/slides-124-cose-split-signing-algorithms-for-cose-00>

described

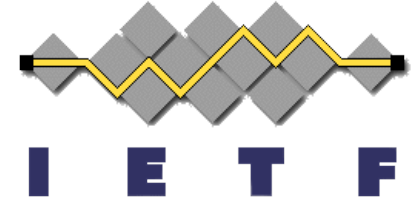
- What
  - Why
  - How
  - Context
- 
- *Not repeating that content here*

# Developments Since IETF 124, Montreal



- Great reviews from Lucas Prabel, Sophie Schmieg, David Dong
  - Incorporated their feedback
- Published drafts -04, -05, -06, -07

# Updates to the Specification (1)



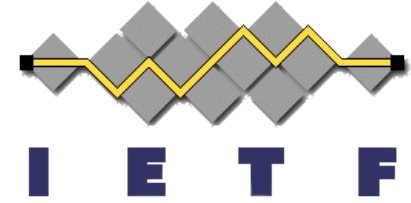
-04

- Added Implementation Status section.

-05

- Clarified that non-"-split" alg IDs defined here may be exposed to verifiers.
- Clarified that transport of digest is out of scope, but expected to be passed as data to be signed.
- Added Security Considerations section "Incorrect Use of Split Signing Algorithm Identifiers".
- Added Implementation Considerations section "Using Non-Split Signing Algorithm Identifiers in a Split Signing Protocol".
- Added section "Defining Split Signing Algorithms" with guidance for handling domain separation tags in new definitions.

# Updates to the Specification (2)



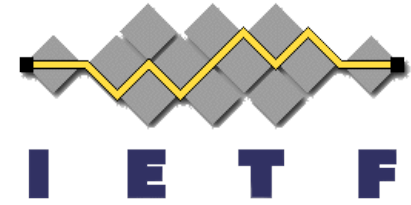
-05 (continued)

- Clarified in introduction that Ed25519 and Ed25519ph(-split) have distinct verification algorithms.
- Clarified in section "Protocol-Level Trusted Roles" why digester is necessarily trusted.
- Clarified in section "Component-Level Trusted Roles" that redundant forgeries are acceptable, and added example of key compromise concern for naively hashed FALCON.

-06

- Added "Prior Art" section to Introduction.

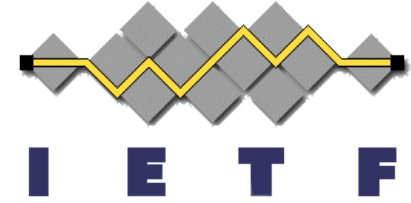
# Updates to the Specification (3)



-07

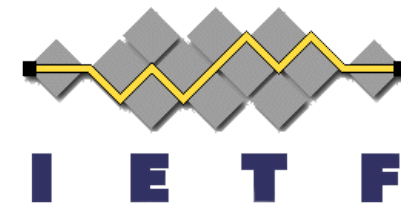
- Populated IANA Considerations sections.
- Imported COSE Algorithms registrations from draft-bradleylundberg-cfrg-arkg:  
ESP256-split-ARKG, ESP384-ARKG, ESP384-split-ARKG,  
ESP512-ARKG, ESP512-split-ARKG, ESP256K-ARKG.

# Nature of the Updates



- Explanations of rationale and mechanisms improved
- Added more background information on existing uses of split signing
- Listed implementations
- Populated IANA Considerations sections
  
- *No architectural changes since IETF 124 in Montreal*

# Status and Next Steps



## ● Status

- Draft is stable and clear
- Incorporates review feedback solicited at IETF 124
- Meets needs of a real and important use case
  - wwWallet, which won the German FUNKE wallet competition

## ● Next Steps

- Working group adoption (as discussed at IETF 124)?