

From: [Dang, Quynh H. \(Fed\)](#)
To: [Regenscheid, Andrew R. \(Fed\)](#)
Date: Friday, October 22, 2021 10:51:25 AM

<https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid-05>

draft-campagna-tls-bike-sike-hybrid-05

Internet Engineering Task Force M. Campagna Internet-Draft E. Crockett Intended status: Experimental AWS Expires: March 14, 2021 September 10, 2020 Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS) draft-campagna-tls-bike-sike-hybrid-05 Abstract Hybrid key exchange refers to executing two independent key exchanges and feeding the two resulting shared ...

datatracker.ietf.org