

mar.16 00:36
draft-scott-neurovix-synodo-aegis-00

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 17, 2026

C. Scott
NeuroVix Systems
March 16, 2026

Synodo-Aegis Protocol: Post-Quantum Inter-Sovereign Immunity
draft-scott-neurovix-synodo-aegis-00

Abstract

This document specifies the Synodo-Aegis protocol, a post-quantum PKI federation between national sovereignties where each country maintains total autonomy over its infrastructure.

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/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 17, 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

The Synodo-Aegis protocol establishes a post-quantum federated PKI architecture. Trust is established through bilateral cross-certification, ensuring that the compromise of any individual CA does not compromise the entire federation.

2. Technical Standards

The protocol integrates several existing standards:

- * STIX 2.1 and TAXII 2.1
- * RFC 5272 Cross-PKI
- * CRYSTALS-Dilithium5
- * seL4 Microkernel Integration

3. Sovereignty Guarantees

The architecture ensures that NeuroVix Systems cannot access private keys of any participating country. Security is mathematical and independent of political trust.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

Security relies on CRYSTALS-Dilithium5 resistance against Shor's algorithm. The seL4 microkernel minimizes the attack surface. Participating nations must ensure physical HSM integrity.

Author's Address

Clebson Scott
NeuroVix Systems
Brasilia, DF
Brazil

Email: clebsoncamposdearaujo@gmail.com