Running code

Delegated credentials: Improving the security of TLS certificates

Delegated Credentials for TLS

By Subodh Jaygar, Kyle Nekritz, Alex Guzman

Validating Delegated Credentials for TLS in Firefox

By Kevin Jacobs, J.C. Jones, Thyla van der Merwe

November 1, 2019 9:00 PM
Proposal: Added algorithm flexibility

Problem: The Client Hello supported_algorithms extension is overloaded to apply to both DC SPKIs and leaf certificate SPKIs, PKIX stack is intolerant of unknown SPKIs.

Proposed solution:
Advertise set of “supported_algorithms” for use with delegated credential handshakes in the delegated credentials extension.

Alternative: Live with it.
Next Steps

Security analysis underway (J Hoyland)

WGLC in conjunction with security analysis?