#### IETF 108 TLSWG

# **Delegated Credentials**

R. Barnes, S. Iyengar, N. Sullivan, E. Rescorla draft-ietf-tls-subcerts-09



### WGLC #1 and WGLC #2

- WGLC #1: draft-07
  - $\circ$  Lots of comments
  - $\circ$   $\,$  -07 was missing some updates from the list in -08  $\,$
- WGLC #2: draft-08
  - No wire changes
  - Multiple comments to be addressed
    - Minor textual tweaks based on comments from Rich
      Salz, Hannes Tschofenig, Daniel Migault
    - Test vectors PR on Github

## **Running code**

Delegated Credential-enabled certificates available from DigiCert

Cloudflare will automatically mint DCs and serve traffic

Available in Firefox 78 ESR, plans to enable by default

•••	Advance	d Preferences	× +	
$\leftrightarrow$ $\rightarrow$	ଟଳ	🖸 Firefox	about:config	☆
୍ secu	rity.tls			
secur	ity.tls.enable	e_Ortt_data	true	
secu	rity.tls.enal	ple_delegated	d_credentials true	
secur	ity the enable	a nost hands	hake auth false	

## Formal analysis

Tamarin model and results shared by Jonathan Hoyland on the mailing list.

**Questions?** 

#### IETF 108 TLSWG

# **Delegated Credentials**

R. Barnes, S. Iyengar, N. Sullivan, E. Rescorla draft-ietf-tls-subcerts-09

