



How TLS 1.3 adoption (and disposal of SSL) is going

Jan Kopriva

jan.kopriva@alef.com

 @jk0pr

ALEF CSIRT

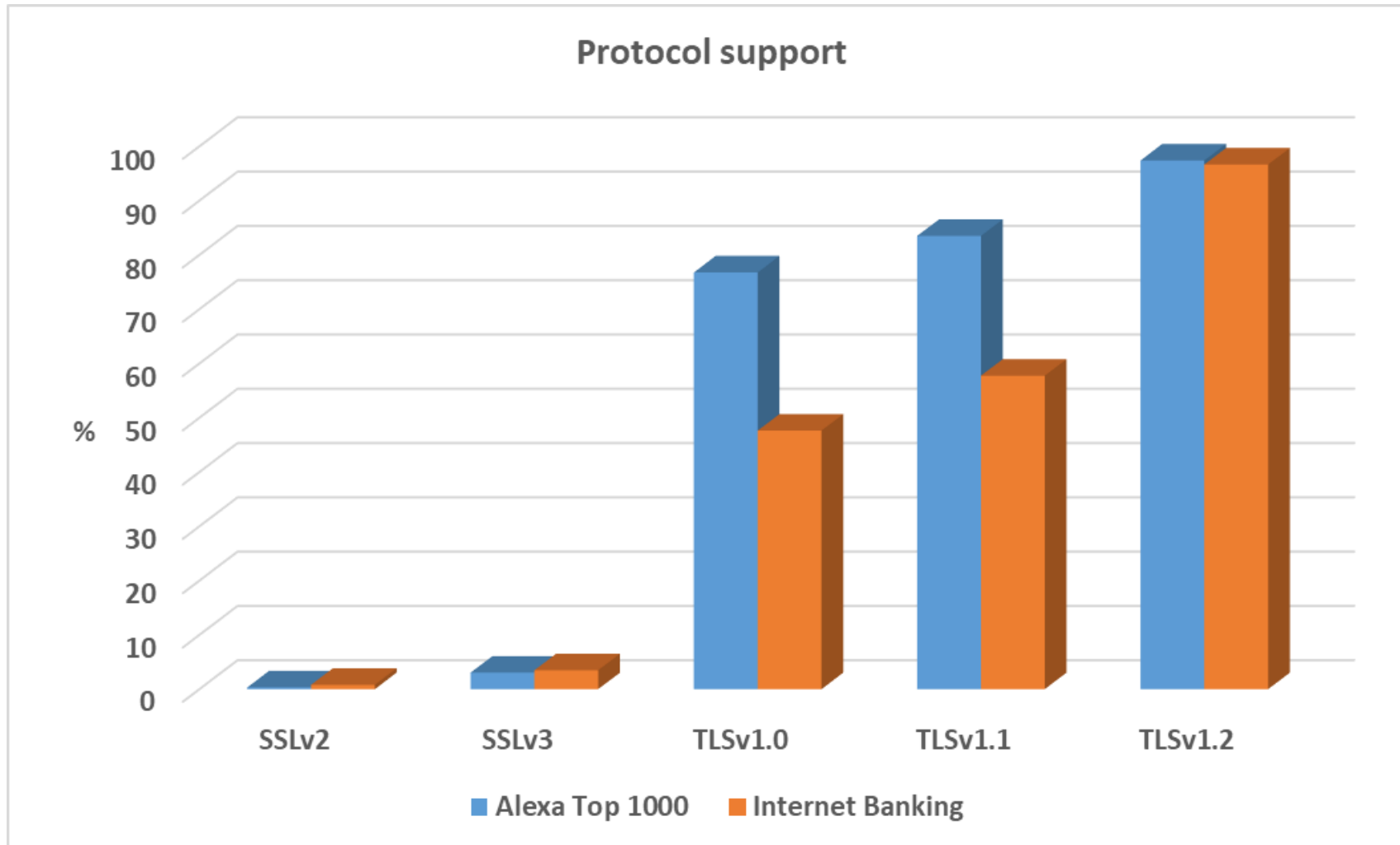


TLP: WHITE

Quick overview of SSL/TLS versions

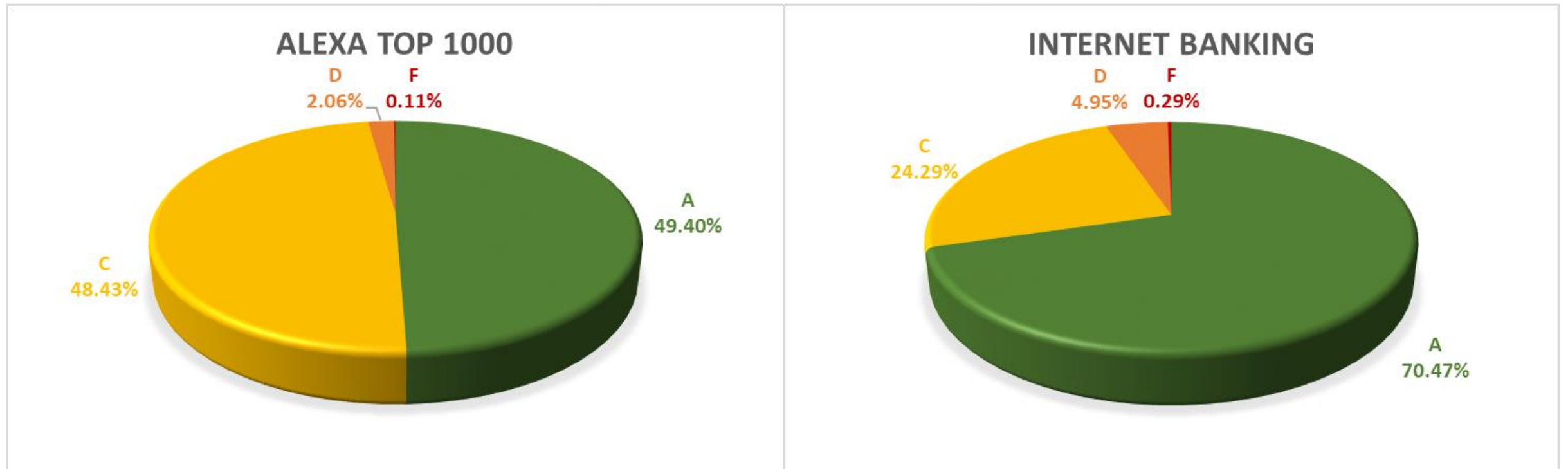
Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecated in 2020 (RFC 8996) ^{[8][9][10]}
TLS 1.1	2006	Deprecated in 2020 (RFC 8996) ^{[8][9][10]}
TLS 1.2	2008	
TLS 1.3	2018	

Interesting historical data – internet banking 2019



Interesting historical data – internet banking 2019

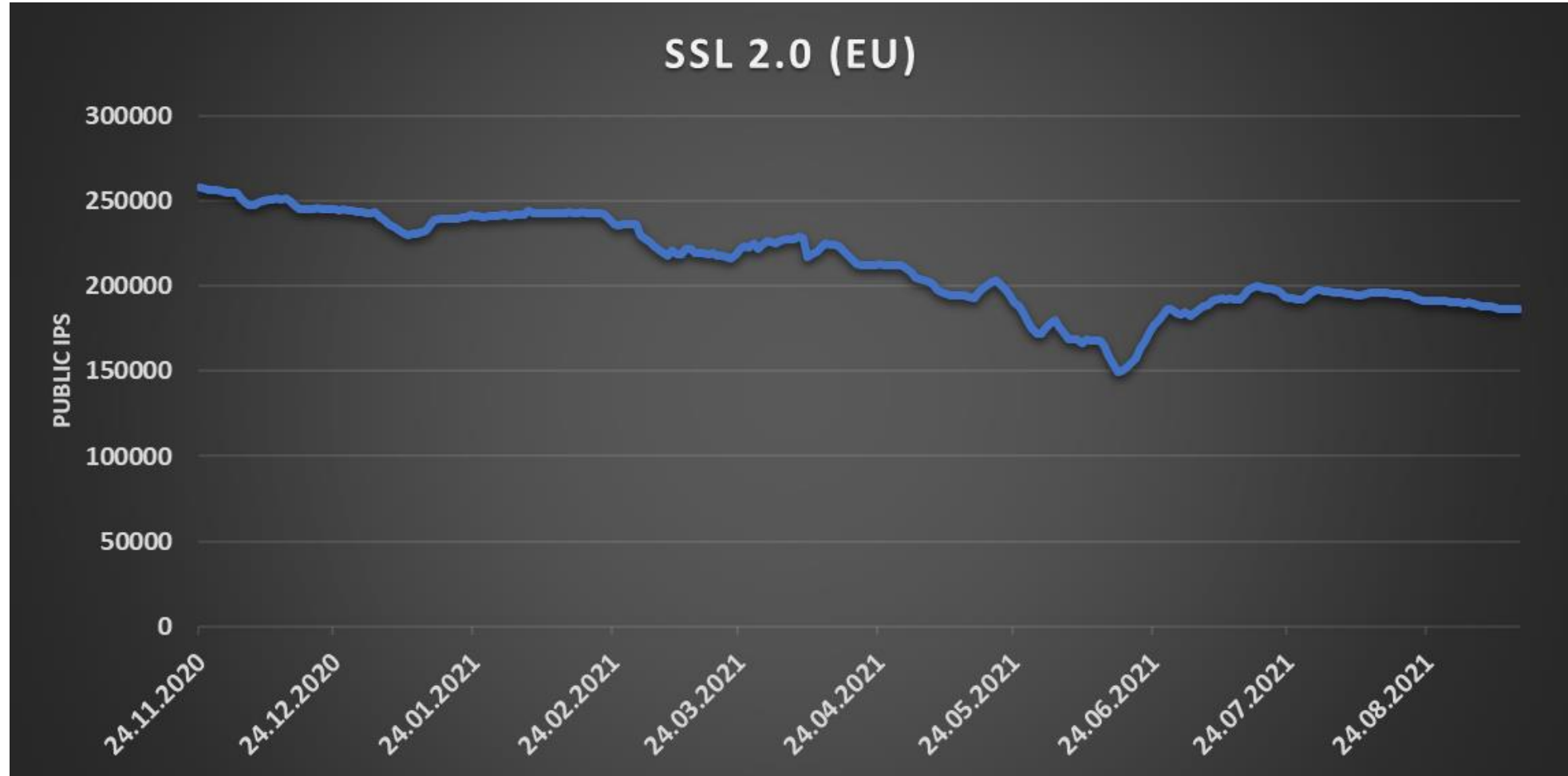
Ciphersuite with least strength



How does SSL/TLS use look now?



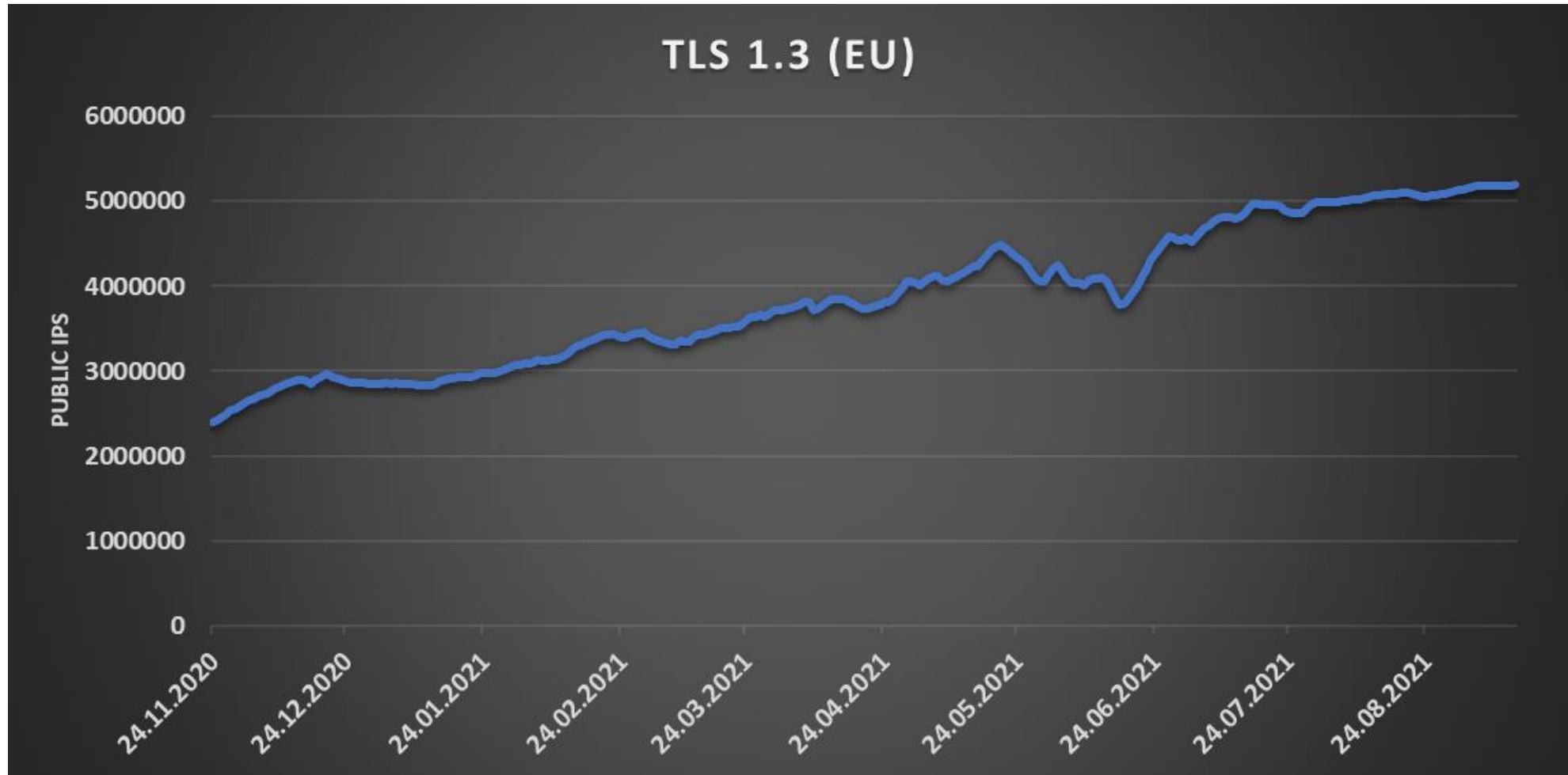
How does SSL/TLS use look now?



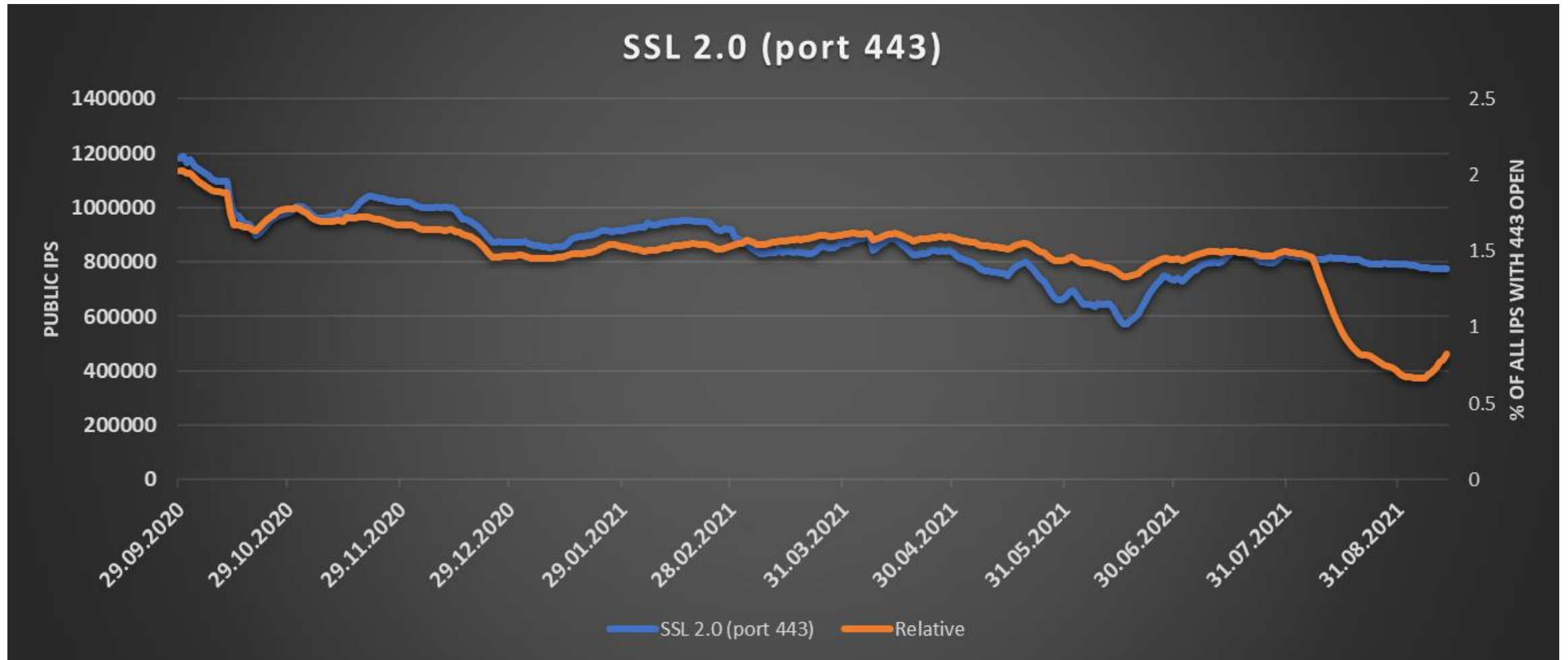
How does SSL/TLS use look now?



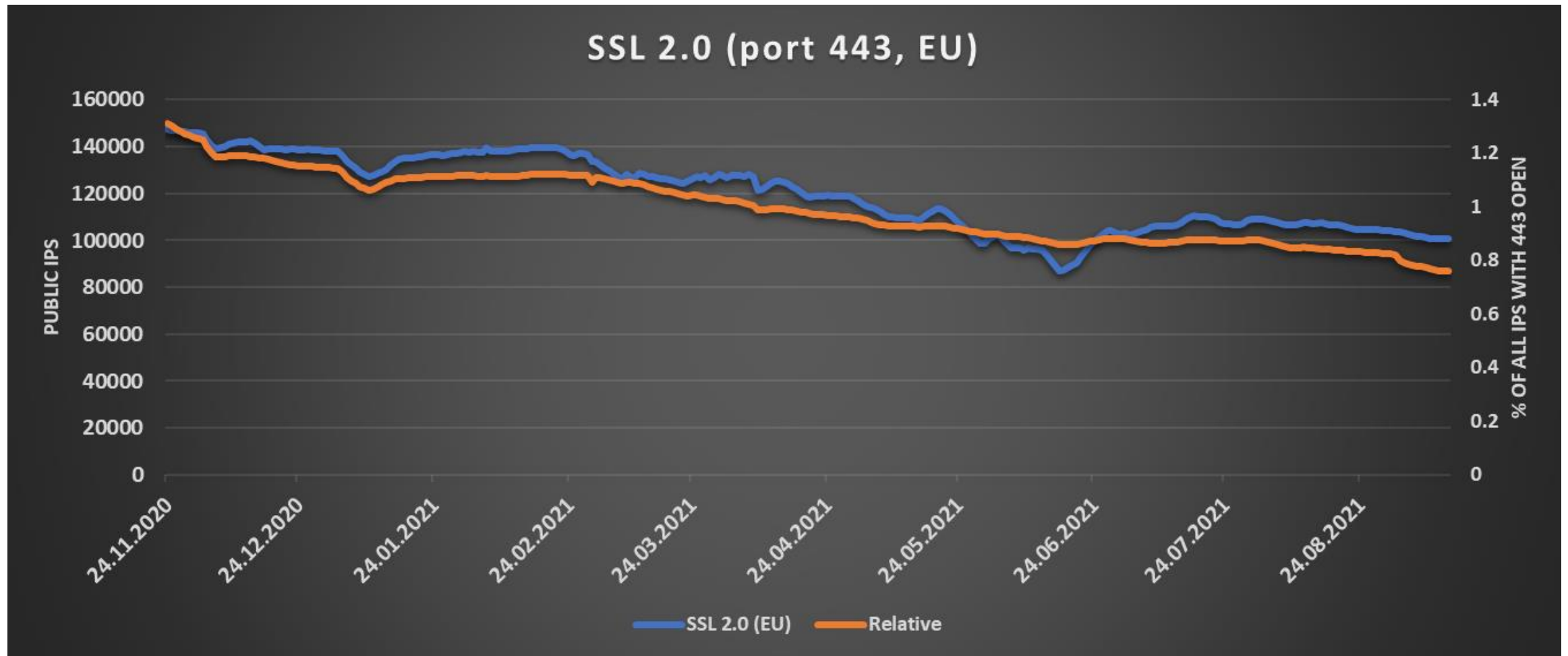
How does SSL/TLS use look now?



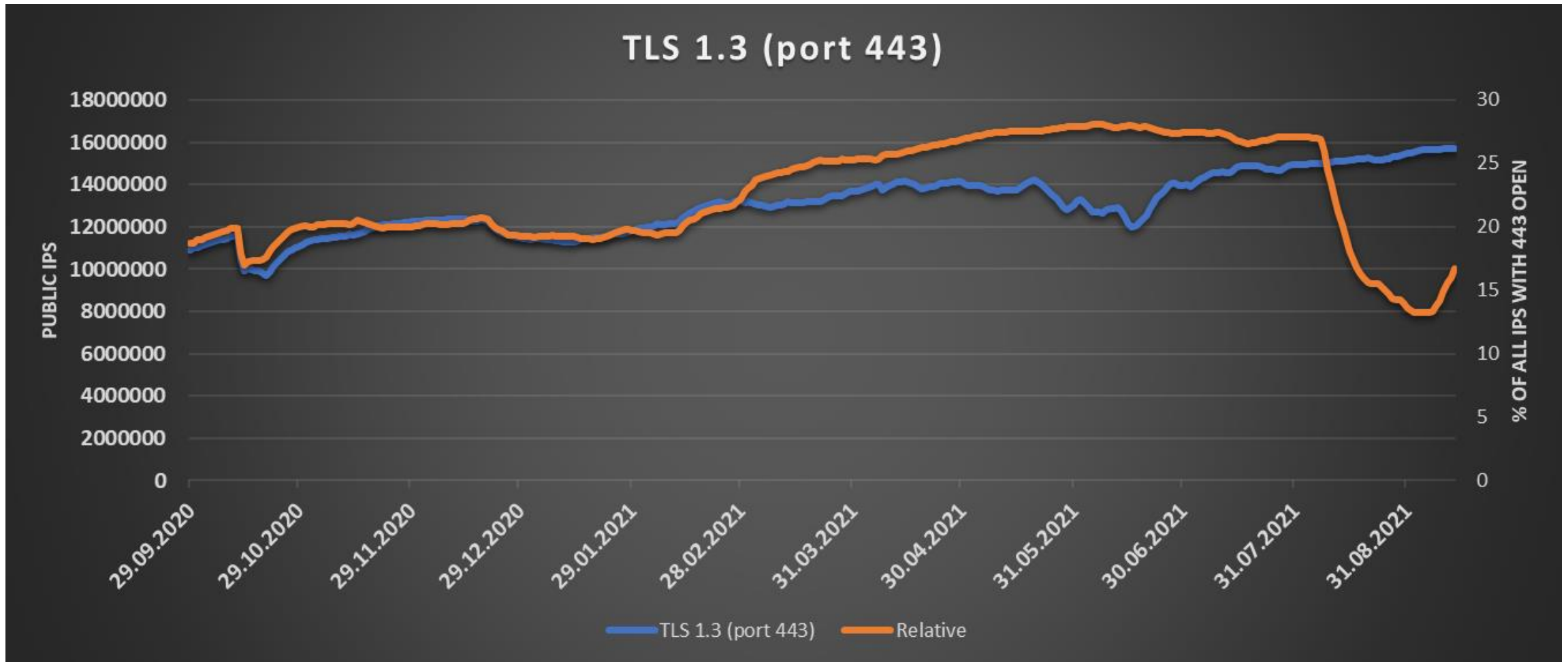
SSL/TLS on port 443



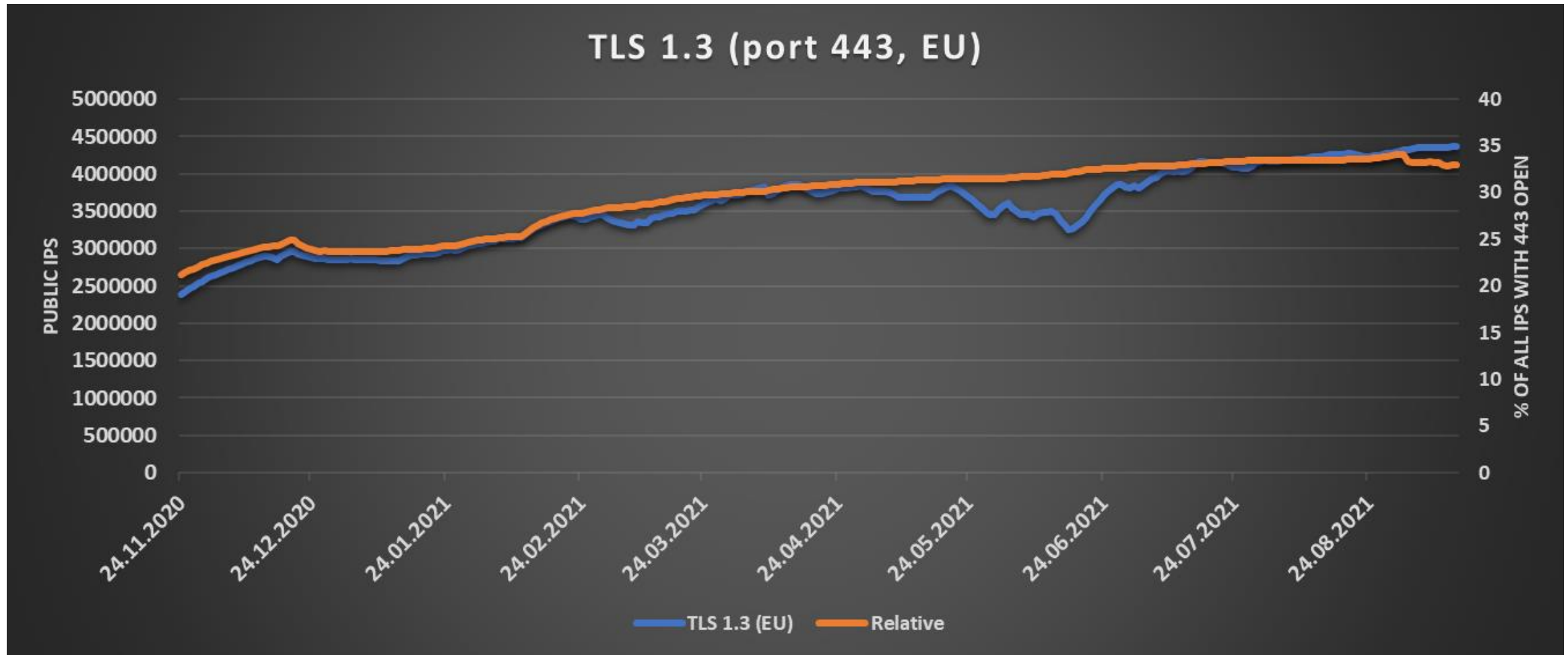
SSL/TLS on port 443



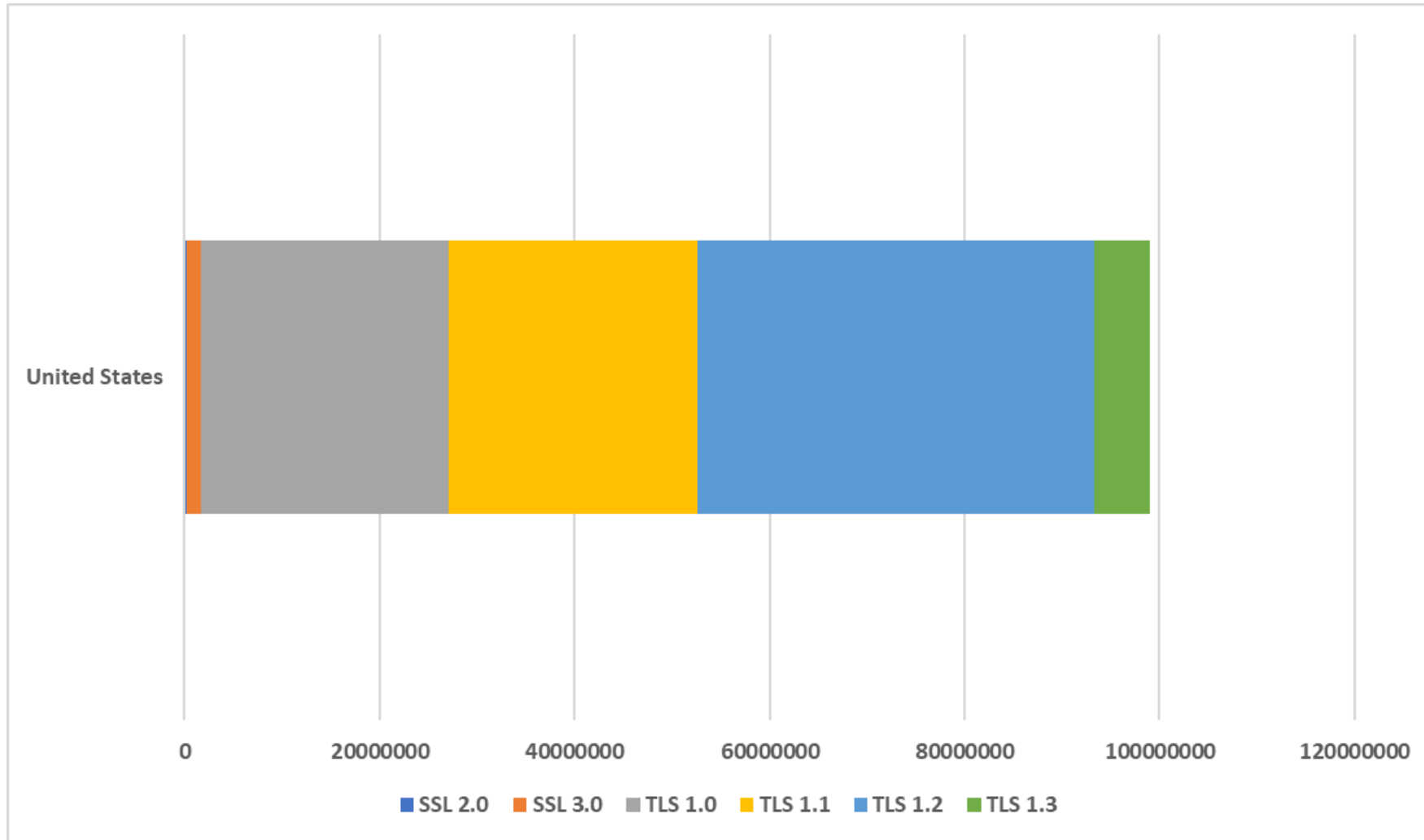
SSL/TLS on port 443



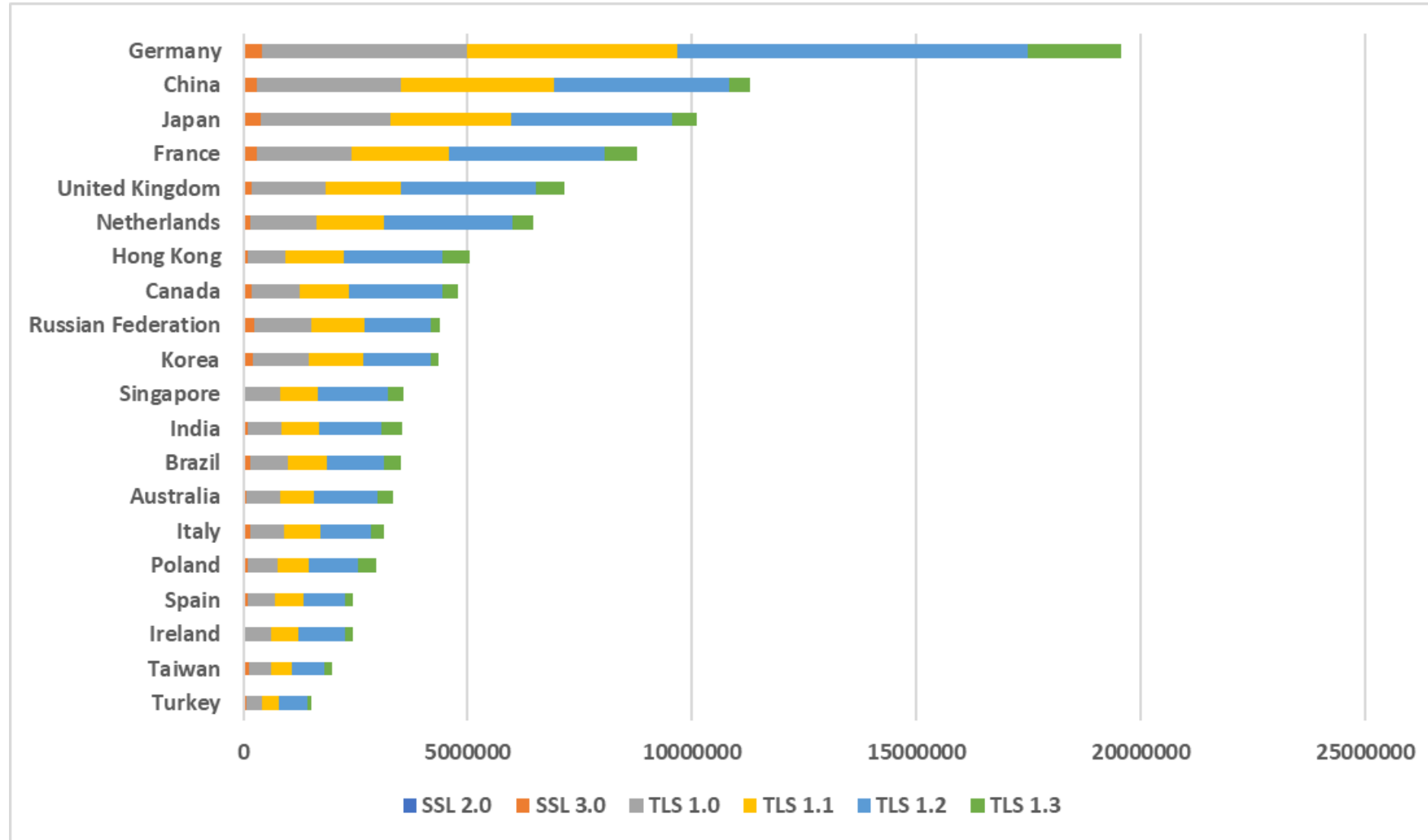
SSL/TLS on port 443



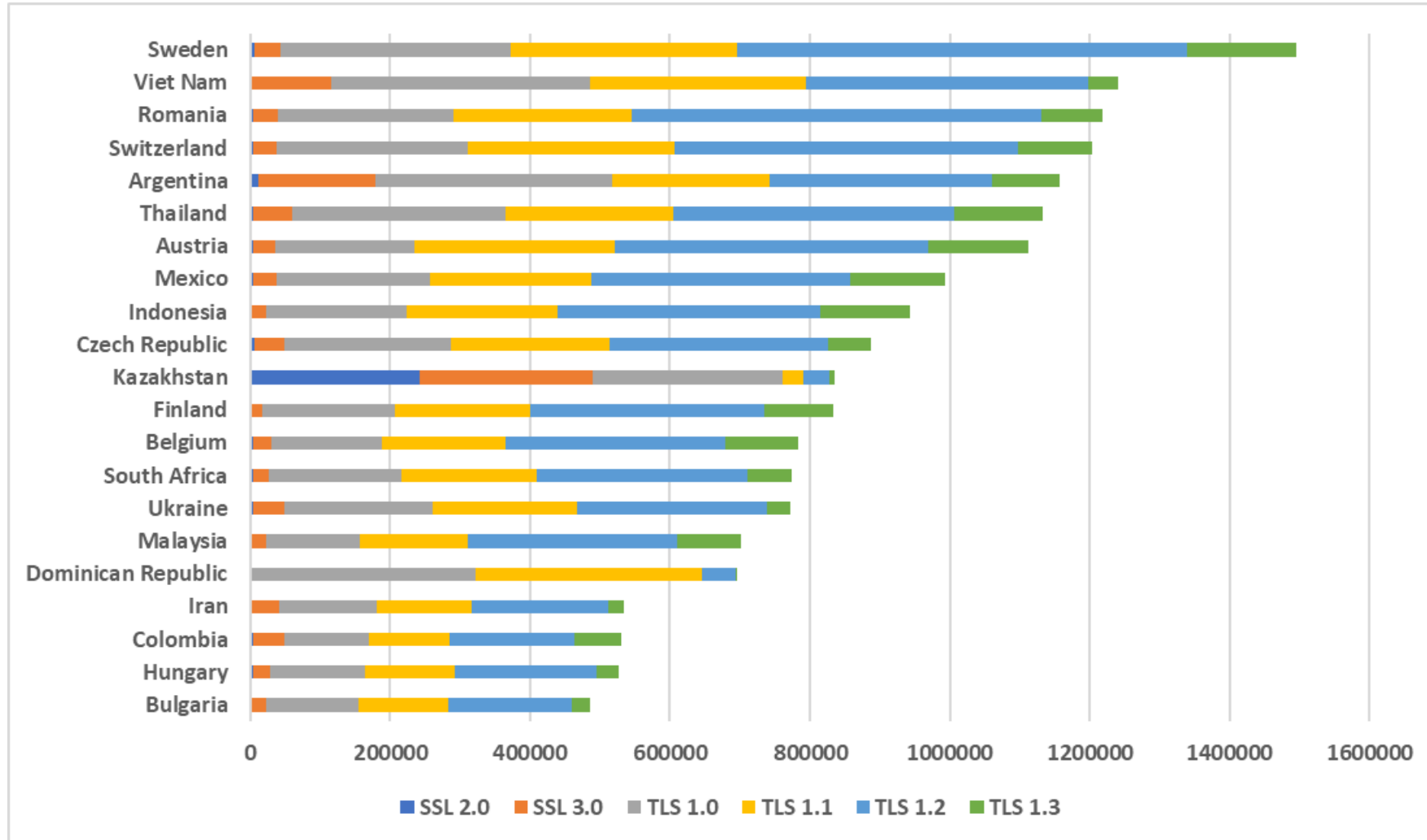
Differences between countries



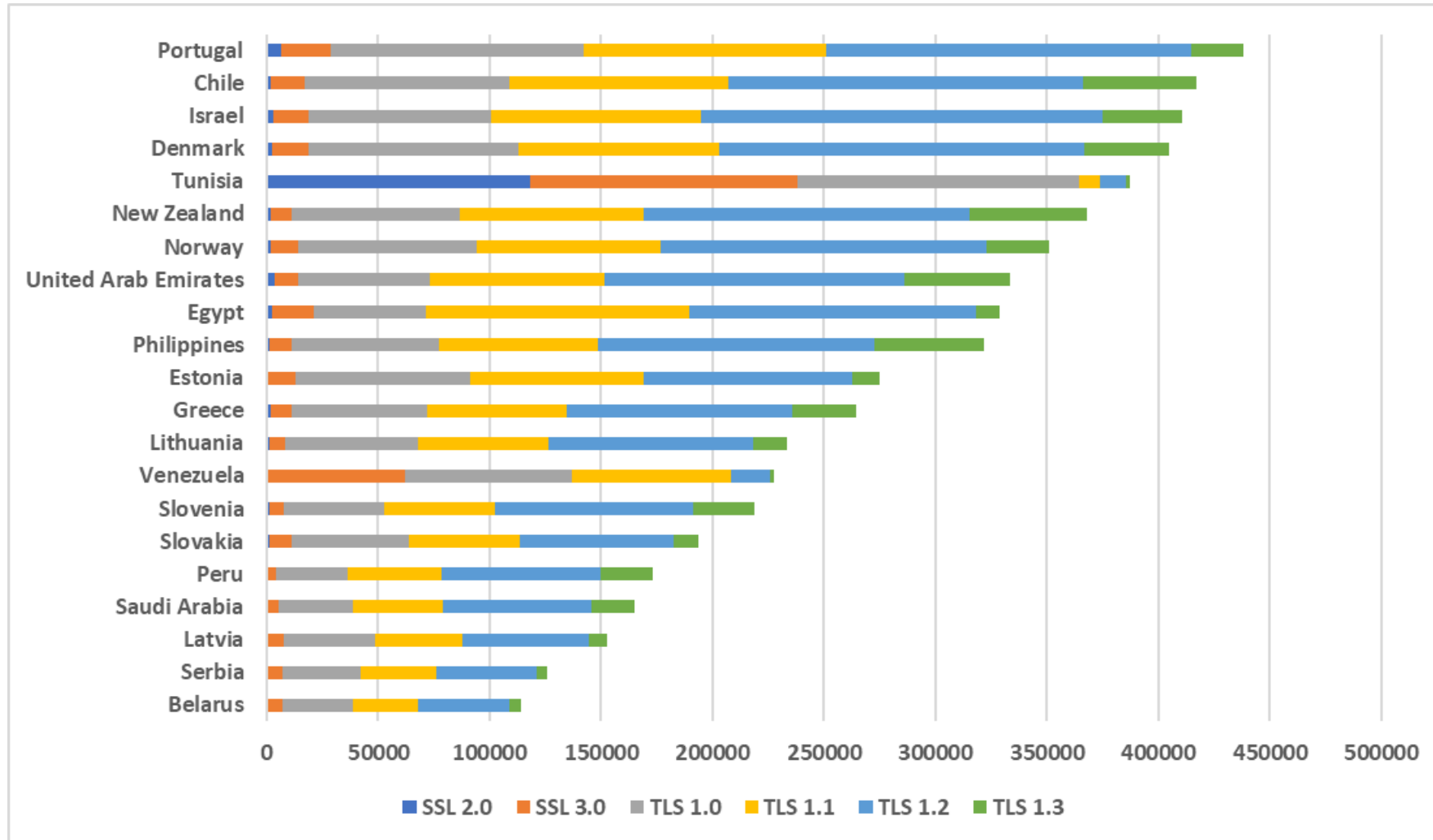
Differences between countries



Differences between countries



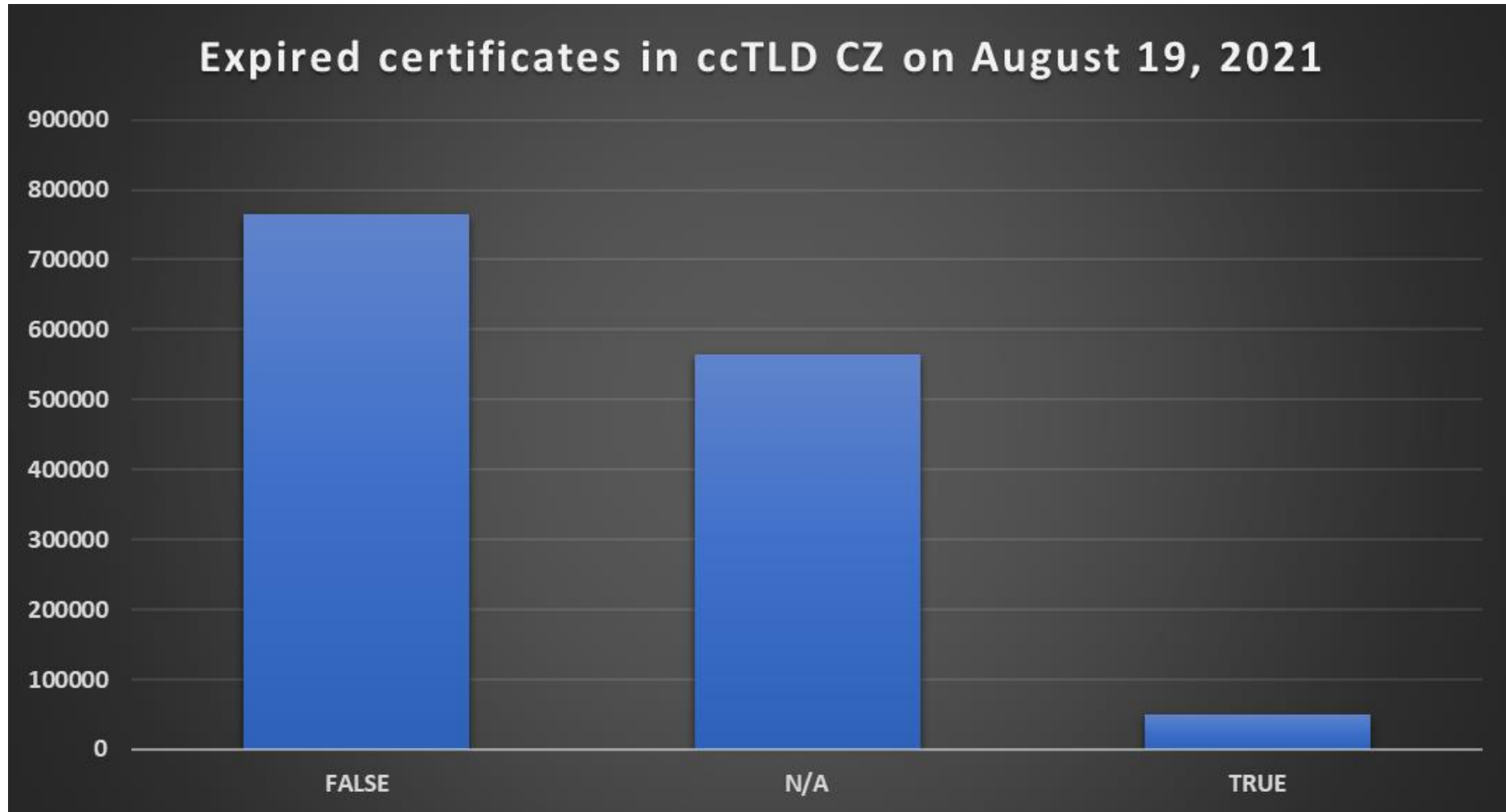
Differences between countries



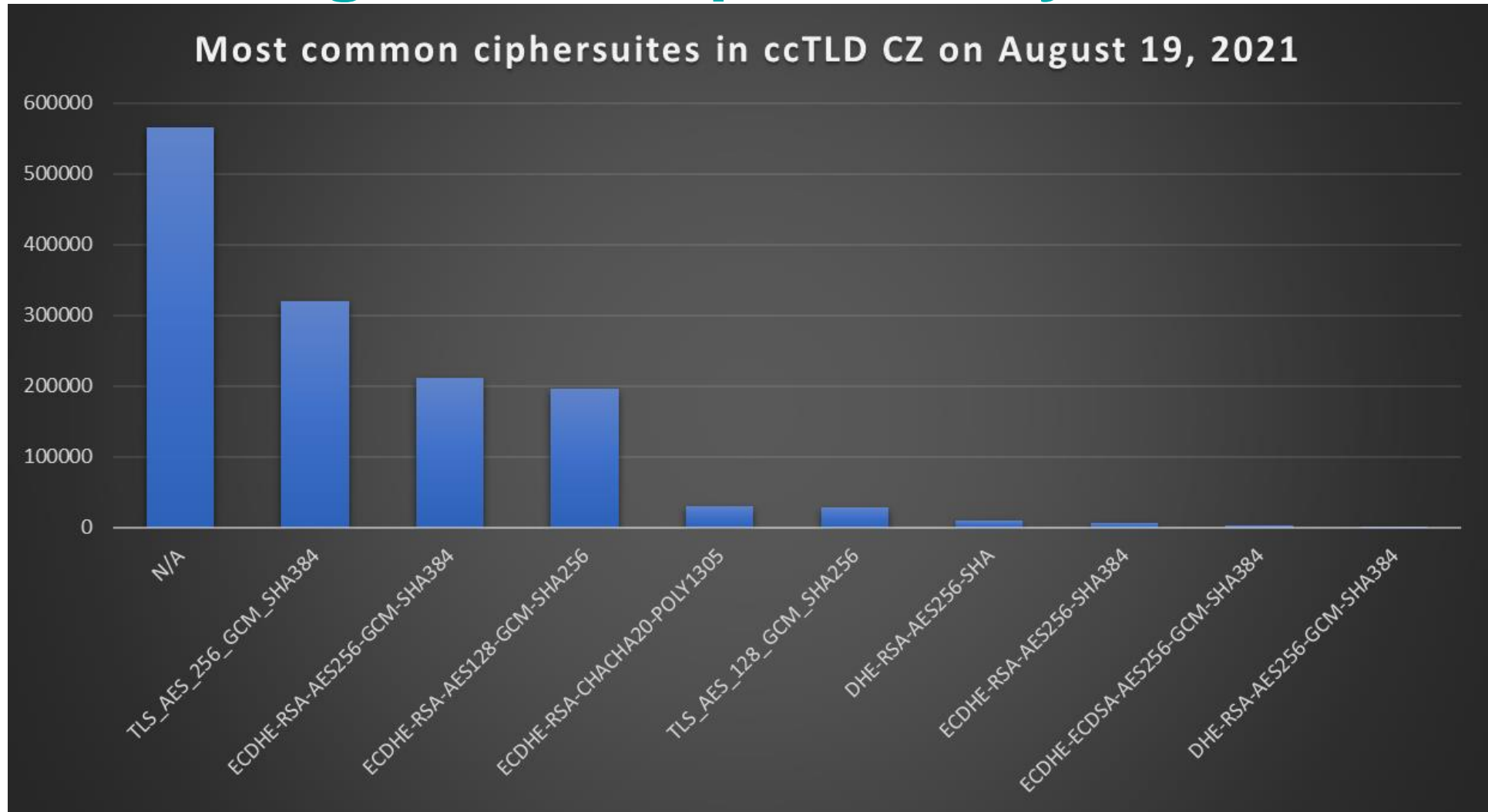
That's not all...

- To get a more thorough overview we'd need numbers for:
 - Trusted vs. Untrusted (self-signed/expired/...) certificates
 - Supported ciphersuites
 - Issuing CAs
 - ...

The remaining data can potentially be obtained



The remaining data can potentially be obtained

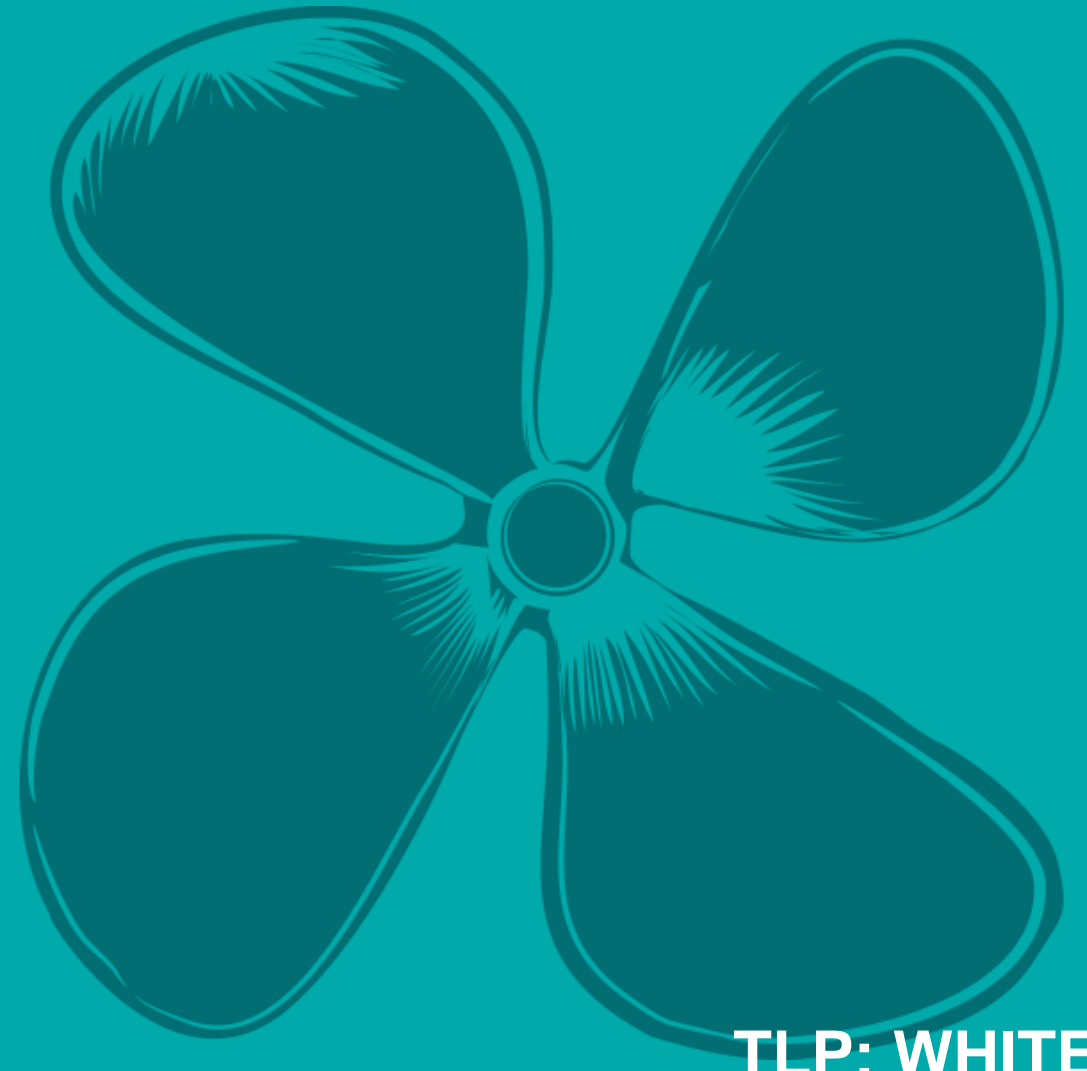


Do you want to take a look at your constituency?

- Passive option
 - Shodan (+TriOp) or similar platform
- Active option
 - Nmap or similar tool
 - ADAM from CZ.NIC

X ALEF

**Thank you for
your attention**



TLP: WHITE