

TLS BCP

draft-ietf-uta-rfc7525bis

Yaron Sheffer, Peter Saint-Andre, Thomas Fossati

IETF 112

A large yellow triangle is positioned in the bottom right corner of the slide, pointing towards the top right.

Since IETF-111, published -02 and -03

- Adjusted text about ALPN support in application protocols
 - A plea to support ALPN!
- Incorporated text from draft-ietf-tls-md5-sha1-deprecate
- Cipher integrity and confidentiality limits
 - draft-irtf-cfrg-aead-limits
- Require ***extended_master_secret***
 - Published post RFC 7525, well supported
- A few [open issues](#) remain

Require
supported_versions
in TLS 1.2

RFC 8446 allows TLS 1.2
implementations to use this
extension

Do we require support?

To our understanding, support in
TLS 1.2 servers has no effect on TLS
1.2 or 1.3 clients

No benefit?

TLS 1.2 version
downgrade
protection

Again, coming from RFC 8446
SHOULD requirements for TLS 1.2
servers re: setting/checking the
ServerHello.Random field

RSA-PSS in TLS 1.2

As well as support for
signature_algorithms_cert

PSS already a SHOULD for
handshake message signatures

Do we add a requirement to support
PSS in certificates?

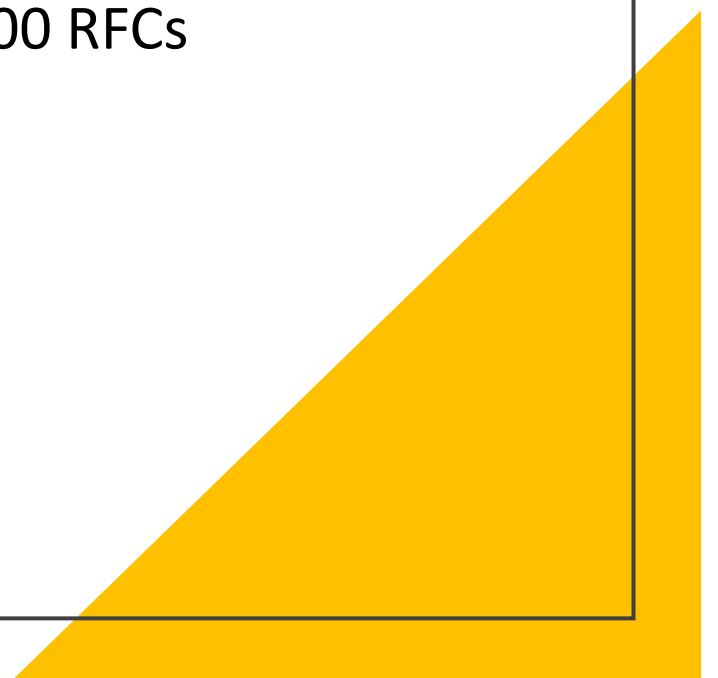
To advance support of almost
nonexistent PSS certs?

Waiting for
*draft-aviram-
tls-deprecate-
obsolete-kex*



Do we break
"consumer"
documents?

Still pending review of ~100 RFCs



Thank You!