RSA signature:
from
RSASSA-PKCS1-v1_5 (legacy)
to
RSASSA-PSS (PSS)

4 Nov 2015

How easy it is to upgrade to TLS 1.3?

(for multi-vendor systems)

Easy

- PSS is already supported and it works with any hash
- Raw RSA was used $\Rightarrow$ no change needed at this layer
- Tight control of software lifecycle, suppliers, components

Not so easy

- Some existing keys on secure devices assume legacy padding $\Rightarrow$ server can't be upgraded to TLS 1.3
- Smartcards don't implement PSS $\Rightarrow$ no client auth. possible with TLS 1.3
- A component with hardwired legacy padding into API
  Example: RSA CRT is hardwired with legacy padding $\Rightarrow$ performance penalty due to absent faster CRT
- The component upgrade is expensive / slow
  Example: PSS support is claimed by only $\approx 1/4$ of vendors on "RSA Validation List" (FIPS 186-4, part of FIPS 140-2 certification)
- End-users incorrectly assume that TLS 1.3 is automatic if TLS 1.2 already works

Current solution for problematic TLS clients or servers

- Don't upgrade the server to TLS 1.3, continue using legacy padding with TLS 1.2
- Don't offer TLS 1.3 in `ClientHello` when client auth. can't do PSS

A solution that makes upgrade to TLS 1.3 easier is desirable

- Add a negotiation for padding in handshake (e.g. a new enum(s) in `SignatureAlgorithm`)
- Optionally also cover legacy/PSS padding for X.509 certs