

# Use of Attestation with Certificate Signing Requests (CSRs)

[draft-ounsworth-csr-attestation-00](#)

Mike Ounsworth, Hannes Tschofenig

(Heavy contributions from MCR, MSJ, Carl Wallace)

# Motivation

- CA/B Ballots [CSC-13](#) and [CSC 17](#) require [code signing certificates to be generated and stored in HSMs by 1 June 2023](#).
- CSR may contain “assertions” about the storage properties of the private key as well as the platform security, such as firmware version, hardware security features, security settings, ...

# Status

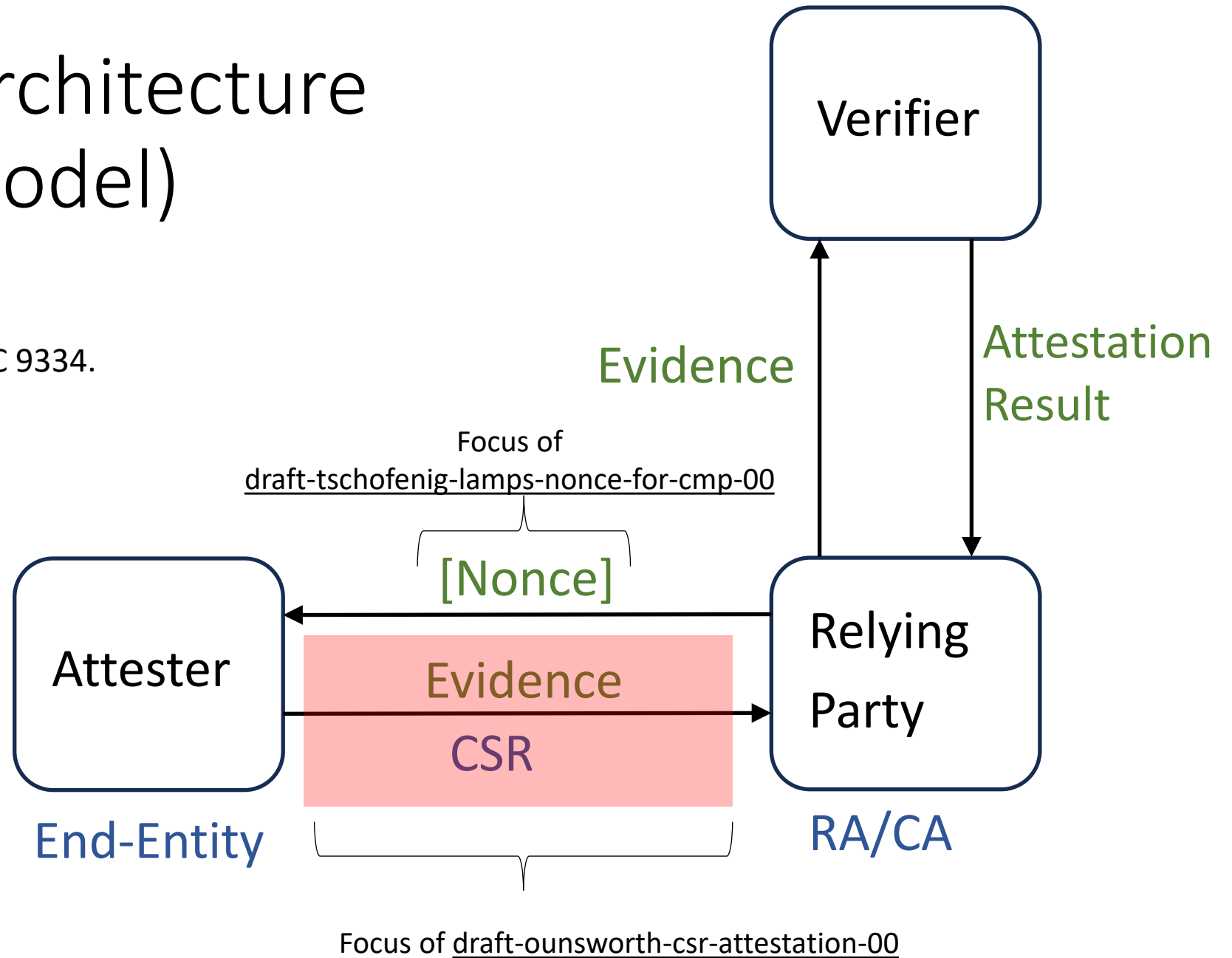
- Draft published as result of the “PKIX Attestation” design team work by  
HSM vendors: Entrust (nShield), Crypto4A, Utimaco, Thales  
CAs: Entrust, Digicert, Keyfactor

Richard Kettlewell, Chris Trufan, Bruno Couillard, Jean-Pierre Fiset, Sander Temme, Jethro Beekman, Zsolt Rózsahegyi, Ferenc Pető, Mike Agrenius Kushner, Tomas Gustavsson, Dieter Bong, Christopher Meyer, Michael StJohns, Carl Wallace, Michael Ricardson, Tomofumi Okubo, Olivier Couillard, John Gray, Eric Amador, Johnson Darren, Herman Slatman, Tiru Reddy, Thomas Fossati, Corey Bonnel, Argenius Kushner, James Hagborg, Mike Ounsworth, Hannes Tschofenig.

- Used several input documents:
  - draft-ietf-lamps-key-attestation-ext-00
  - draft-ounsworth-pkix-key-attestation-02
  - draft-stjohns-csr-attest-00
- Work mode: Regular conference calls + emails

# IETF RATS Architecture (Passport Model)

Terminology reused from RFC 9334.  
Nonce is optional.



# We are not running out of Attestation Technologies...

Tokens			
Yubico	✓	X.509	<a href="https://developers.yubico.com/YubiHSM2/Concepts/Attestation.html">https://developers.yubico.com/YubiHSM2/Concepts/Attestation.html</a> <a href="https://developers.yubico.com/yubico-piv-tool/Attestation.html">https://developers.yubico.com/yubico-piv-tool/Attestation.html</a> <a href="https://developers.yubico.com/PIV/Introduction/PIV_attestation.html">https://developers.yubico.com/PIV/Introduction/PIV_attestation.html</a>
Trusted Platform Module	✓	TPMS_ATTEST/PKCS#10	<a href="https://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf">https://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf</a> <a href="https://docs.microsoft.com/en-us/windows-server/identity/attestation/attestation">https://docs.microsoft.com/en-us/windows-server/identity/attestation/attestation</a> <a href="https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wcce/f596c7df-a72c-4323-b27f-3c8646604ddb?content/uploads/TNC_TAP_Information_Model_v1.00_r0.29A_publicreview.pdf">https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wcce/f596c7df-a72c-4323-b27f-3c8646604ddb?content/uploads/TNC_TAP_Information_Model_v1.00_r0.29A_publicreview.pdf</a>
Century Longmai PKI Token	✗ ⓘ	CMS/PKCS#7	
TrustSec SLCOS - Bio/PKI token	✗		
Other Devices			
Apple iOS	✓	CBOR/WebAuthn	<a href="https://developer.apple.com/documentation/devicecheck">https://developer.apple.com/documentation/devicecheck</a> <a href="https://developer.apple.com/documentation/devicecheck/dcappattestseattestkey">https://developer.apple.com/documentation/devicecheck/dcappattestseattestkey</a> <a href="https://developer.apple.com/documentation/devicecheck/validating_apps_that_connect_to_your_server">https://developer.apple.com/documentation/devicecheck/validating_apps_that_connect_to_your_server</a>
Android	✓	ASN.1	<a href="https://developer.android.com/training/articles/security-key-attestation">https://developer.android.com/training/articles/security-key-attestation</a> <a href="https://source.android.com/security/keystore/attestation">https://source.android.com/security/keystore/attestation</a>

See [Remote Key Attestation | PKI Consortium](#).

# CSR carries Evidence

- There are lots of different attestation technologies, such as TPM, Arm PSA, DICE, ...
  - Some standardized – some are proprietary.
  - Different mechanisms used for freshness (e.g. nonces, timestamps, epochs)
- CSR does not need to care about the details of the attestation technology
  - It treats evidence as an opaque blob.
  - Attester and Verifier need to understand the evidence format. RA/CA do not need to understand it.

# Conveying evidence

- CSR contains a type – value pair.
  - Type indicates what attestation technology is used.
  - Value carries the data produced by the attester (in whatever format used by the attestation technology)
- **Open Issue:** How should the type be encoded:
  - OID
  - [Conceptual Message Wrapper developed in RATS](#) group (see [issue#11](#)). Integer with values registered in IANA registry.
  - The design group started with unanimous support for “*Let’s stay within ASN.1 / PKIX modules as much as possible*” – which implies a preference for OID-based type field.

# Other Open Issues

<https://github.com/lamps-wg/csr-attestation/issues>

- Currently we define two attributes:
  - AttestAttribute
  - AttestCertsAttribute
- Should the AttestAttribute contain the certification chain need to verify it?
  - Aside: many attestation formats (ex. WebAuthn) carry their certs internally, so this is to support formats that don't (ex. TPM 2.0 attest)
  - Pro: Easier to associate certs to attestation.
  - Con: Duplication if CSR contains multiple attestations with overlapping cert chains.
- Size: We're going to embed multiple potentially long cert chains inside a CSR? Won't that make the CSR huge?
  - Yes.

# Next Steps

- Asking the working group to adopt draft-ounsworth-csr-attestation-00 and drop
  - draft-ietf-lamps-key-attestation-ext-00
  - draft-ounsworth-pkix-key-attestation-02
  - draft-stjohns-csr-attest-00
  - (we believe Carl, Sean, MSJ consider this is a friendly replacement, but need confirmation from them).
- Design team will continue its work
  - Next step / deliverable: what “evidence” is applicable across all “big iron” HSMs; “FIPS mode”, “Non-exportable”, “Dual-control”, etc.
  - Hopefully this leads to defining an attestation statement format designed for HSMs.