Rats Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2020

G. Mandyam
V. Sekhar
S. Mohammed
Qualcomm Technologies Inc.

October 31, 2019

The Qualcomm Wireless Edge Services (QWES) Attestation Token
draft-mandyam-rats-qwestoken-00

Abstract

An attestation format based on the Entity Attestation Token (EAT) is described. The Qualcomm Wireless Edge Services (QWES) token is used in the context of device onboarding and authentication. It is verified in the same manner as any CBOR Web Token (CWT).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

A description of the Qualcomm Wireless Edge Services (QWES) attestation token is provided. QWES allows for service providers to manage devices that implement Qualcomm semiconductor solutions. Based on the EAT-compliant attestation token (see [I-D.ietf-rats-eat]) produced in a trusted execution environment (TEE), a service provider can verify the device identity in addition to several other security-impacting characteristics.

2. EAT Compliant Claims in QWES Token

Certain claims defined for EAT are leveraged in the QWES token.

2.1. OEM ID

The QWES token makes use of an OEM ID. However, the type is a uint (not a bstr as per the EAT specification).

2.2. nonce

The QWES token can carry a nonce. The nonce is a bstr.

3. QWES Token Augmentation to EAT

Several claims have been defined that are not currently present in the EAT base set to complete the QWES token.

3.1. DevID

The DevID is a 256-bit bstr that serves as a device identifier. It differs from the ueid (Universal Entity ID) defined in the EAT specificaation. A specific device ID can be created for ISV’s based on their identifier combined with a salt. This allows for a certain level of privacy preservation. Note that the RAND option for ueid may be a suitable substitute for this claim.

3.2. HWVer

This is a bstr claim that distinguishes different system-on-chip (SoC) models.

3.3. Context

This is a numerical (uint) index that denotes the context of the attestation. The current values defined (0-4) are: on-demand attestation, registration, provisioning, certificate issuance and proof-of-possession.

3.4. PKHash

This is a bstr containing a SHA-256 hash of a public key provisioned by the OEM. It can be used optionally in place of an OEM ID.

3.5. SPID

This is a numerical (uint) identifier of the service provider associated with the QWES token. The EAT specification’s origination claim can be a suitable substitute.

3.6. QSEEVersion

This is tstr that designates the TEE version ("QSEE" = Qualcomm Secure Execution Environment).

3.7. FWVersion

This is tstr that designates the firmware version specifically dedicated to bootstrapping.

3.8. Security State

This is tstr that contains the state of one-time programmable (OTP) memory. Bits in this field will be set as per the security-impacting section of the OTP memory. The relevant bits in OTP would normally be used to control secure boot enablement, debug disablement, debug enablement parameters, and the state of device keys (i.e. whether they are locked for reading or writing).

3.9. CSR

A Certificate Signing Request (CSR) may be carried in a QWES token as a bstr. This allows for a CA (certifying authority) to verify an attestation and provide a certificate without an extra round trip. This is an optional claim.

3.10. AppData

This is a bstr containing a hash of the associated application data. Since the QWES token can be service provider-specific, the hash that is returned can correspond to the corresponding user space application that invoked the generation of the attestation token. This is an optional claim.

4. Example

A sample QWES token payload is shown. It would be signed and/or encrypted as per COSE guidelines.

```
{
  / DevID /                     h’0a’,
  / OEMID /                     32,
  / HWVer /                     h’0e’,
  / Context /                   2, / provisioning /
  / SPID /                      10,
  / Nonce /                     h’da378321bb’
}
```

Sample QWES Token Payload

5. IANA Considerations

This memo includes no request to IANA.

6. Normative References

[I-D.ietf-rats-eat]
Mandyam, G., Lundblade, L., Ballesteros, M., and J. O’Donoghue, "The Entity Attestation Token (EAT)", draft-ietf-rats-eat-00 (work in progress), June 2019.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

Authors’ Addresses

Giridhar Mandyam
Qualcomm Technologies Inc.
5775 Morehouse Drive
San Diego, California 92121
USA

Phone: +1 858 651 7200
Email: mandyam@qti.qualcomm.com

Vivek Sekhar
Qualcomm Technologies Inc.
5775 Morehouse Drive
San Diego, California 92121
USA

Phone: +1 858 651 3557
Email: vsekhar@qti.qualcomm.com

Shahid Mohammed
Qualcomm Technologies Inc.
5775 Morehouse Drive
San Diego, California 92121
USA

Phone: +1 858 651 7975
Email: shahidm@qti.qualcomm.com