Use Identity as Raw Public Key in EAP-TLS


IETF111-2021-EMU

Meiling Chen /China Mobile
Li Su /China Mobile
Haiguang Wang/Huawei
Comments received since IETF109

1、What scenario is it for?
Internet of things devices, especially passive long-life devices.

2、Is it related to IBE?
No, only use IBS signature to solve the identity authentication problem

3、any running code?
Coding eap-tls-ibs based on eap-tls1.2 using ECCSI

4、Any cross scope of IOT OPS?
No
Updates from -00 to -02

2 updates

Abstract: Add the reference of draft-ietf-tls-dtls13

Introduction: In the draft draft-ietf-emu-eap-tls13 reads certificates can be of any type supported by TLS including raw public keys. In RFC7250[RFC7250] it assuming that an out-of-band mechanism is used to bind the public key to the entity presenting the key.

Key distribution is out of scope in my draft, if you are interested, you can consider further.

2 new adds

IANA considerations: This document registers the following item in the "Method Types" registry under the "extensible Authentication Protocol(EAP) Registry" heading.

Use case of the EAP-TLS-IBS:

- Used for authentication of Internet of Things devices
- Used for systems that do not support CA certificates
Update process
add a round trip interaction based on
draft-ietf-emu-eap-tls13-18

Figure 7: EAP-TLS mutual authentication with TLS1.3 handshake
Welcome and Thanks to Russ Housley would do the ASN.1 structures for pyasn1-modules when it becomes an RFC. will review the ASN.1 portions of the specification to make sure they are clear.

To Do

• Call for Adoption

• Comments and co-authors are welcome!

• Defines The key derivation based on EAP-TLS-IBS

• EAP-TLS based type needs to add a new type for EAP-TLS-IBS