Managing Credentials via EAP-CREDS

{ **Cable**Labs® ◦ Open**CA** }

https://datatracker.ietf.org/doc/draft-pala-eap-creds/

Massimiliano Pala <m.pala@cablelabs.com>

Problem Statement

- Different types of access networks exist today that are capable of supporting EAP for authentication
- Operators tend to deploy multiple types of networks for different market segments
  - Public Access Points
  - Cellular Networks (CBRS-A, MulteFire, 5G, etc.)
  - Cable HFC Networks (e.g., DOCSIS)
- Operators should have the possibility to actively manage the credentials used to access the network to be able to address changes in the risk profile of their networks

Problem Statement (cont.)

- Different types of access networks authenticate users and devices by using different types of credentials
  - Username/Password
  - Secret Keys
  - Certificates
- Securely managing these credentials is critical for the security of the access networks
  - No easy method exists to manage these credentials
  - Some methods provide some form of credentials management for X.509 certificates, but do not handle generic types of credentials

Problem Statement (cont.)

- EAP-CREDS, by providing an encapsulating EAP method together with associated processing rules, enables network management tools to actively register, deploy, and update credentials even before providing IP connectivity
  - Solves the security and discoverability issues related to solutions like the OSU server (as defined in WFA or MulteFire) where unauthenticated devices are given (jailed) network connectivity to acquire their credentials
- Profiles can be defined for existing provisioning protocols (or only part of them – e.g., renewal) for how to use them in particular contexts and/or environments

EAP-CREDS in a Nutshell

- The protocol is organized in three different phases: initialization, management, and validation.
- The Initialization phase allows the server and the client to exchange the details about the supported EAP-CREDS version, the list of credentials, and supported management/provisioning protocols.
  - Vouchers (or Tokens) can be used to bootstrap the provisioning process
- The Management phase provides the transport messages for the selected management protocol (e.g., CMP, EST, ACME, etc.)
- The validation phase provides (optional) the possibility to verify the correct installation of the credentials

What has changed ...

- **Simplified the proposal.** Following the feedback from the thread on the mailing list, we now require the use of an outer mechanism to provide confidentiality and fragmentation support
  - We are considering further work to simplify the proposal (Next Steps...)
- **Defined a generic method for managing non-certificate credentials.** EAP-CREDS provides the definition for The Simple Provisioning Protocol (SPP)
  - Although EAP-CREDS can incapsulate existing provisioning protocols, there is no generic solution for certificate and non-certificate based credentials provisioning – SPP provides the missing piece
- However ...

Next Steps

- To further simplify the proposal, we are evaluating the removal of the SPP from the main document and provide a different “profile” for the use of SPP
  - The main document will remain the basic document for the specifications, while the second document provides the “embodiment” (i.e., the specific messages) for the SPP
- Following the feedback received on the ML and from outside, we think we can reduce the size of the document even further and make it more clear

Thanks and Acknowledgments

- We would like to thank everybody who provided feedback and suggestions for how to move forward
- We would also like to thank the WG and the WG Chairs for their support and hard work for the Charter Text

EMU WG

- There might be use-cases we are not considering that could improve the proposal's scope
  - Please Reach out if you think you have a use-case for this work
- We are currently focusing on use cases that are important to our members (i.e., managing credentials across the whole organization, independently from the type of Access Network used)
  - Cable networks (of course!)
  - Cellular Networks (i.e., CBRS-A 4G and 5G, MulteFire, 3gpp\5G)
  - Wireless Broadband Alliance (WBA)

EMU WG (cont.)

- Once this work will be done, we think the document might be ready to be evaluated for WG adoption
  - We would like to thank everybody who provided feedback and suggestions for moving forward

- ***References:***

  - EAP-CREDS I-D https://datatracker.ietf.org/doc/draft-pala-eap-creds/