Managing Credentials via EAP-CREDS

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

Massimiliano Pala <m.pala@cablelabs.com>
CableLabs / OpenCA
The Problem

• Access network authenticates users and devices by using different types of credentials
• 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 credentials
• By providing an EAP generic method, we can enable network management tools to actively register, deploy, and update credentials even before providing IP connectivity
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, available management/provisioning protocols.

• The Management phase provides the transport messages for the selected management protocol (e.g., CMP, EST, ACME, etc.)
  • A simple EAP-CREDS specific protocol is also to be defined for managing non-certificates credentials (i.e., OTT, Passwords, Reusable Tokens, etc.)

• The validation phase provides (optional) the possibility to verify the correct installation of the credentials
Phase One: Initialization

<table>
<thead>
<tr>
<th>EAP Peer</th>
<th>EAP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>EAP-Request/Identity -</td>
<td></td>
</tr>
<tr>
<td>EAP-Response/Identity ------------&gt; (NAI=register@realm</td>
<td>NAI=manage@realm)</td>
</tr>
<tr>
<td>EAP-Request/EAP-CREDS ------------&gt; (Type=Init,Ver,Supported Protocols, Providers,Capabilities,Profiles)</td>
<td></td>
</tr>
<tr>
<td>EAP-Response/EAP-CREDS ------------&gt; (Type=Init,Ver,Proto,Provider, Crypto,Profile,token, action)</td>
<td></td>
</tr>
<tr>
<td>Phase One Begins</td>
<td></td>
</tr>
<tr>
<td>Phase One Ends</td>
<td></td>
</tr>
</tbody>
</table>
Phase Two: Credentials Management

---

Phase Two Begins

---

EAP-Request/EAP-CREDS (Type=ProtoFlow,Empty)

---

EAP-Response/EAP-CREDS (Type=ProtoFlow,ProtoData)

---

EAP-Request/EAP-CREDS (Type=ProtoFlow,ProtoData)

---

EAP-Response/EAP-CREDS (Type=ProtoFlow,EMPTY)

---

Phase Two Ends
Phase Three: Validation

Phase Three Begin

EAP Request/EAP-CREDS
(Type=Validate, Challenge)

EAP Response/EAP-CREDS
(Type=Validate, ExtraChallenge, ChallengeResponse, Challenge)

EAP Request/EAP-CREDS
(Type=Validate, ChallengeResponse)

EAP Request/EAP-CREDS
(Type=Validate, EMPTY)

EAP Success
Remaining Work

• **Simplify the proposal.** The current version of the draft assumes that EAP-CREDS should provide support for fragmentation control, and allows its use in non-tunneled mode
  
  • By requiring EAP-CREDS to be used together with a tunneling method that provides server-side authentication, encryption, and fragmentation support (e.g., EAP-TEAP, EAP-TLS/EAP-TTLS, etc.) the method’s implementation can be simplified and additional control messages can be spared.

• **Provide a generic method for managing non-certificate credentials.** Access networks use many different types of credentials: a generic method might be needed for managing these types of credentials (e.g., OTT, username/passwords, Reusable Tokens, etc.)
Next Steps

• We would like to see the proposal, at some point, to be adopted by the WG, however we do not ask for adoption at this time
  • we realize that a re-chartering is needed
  • we realize that this effort might take resources away from the current efforts

• We would appreciate feedback on the current approach, though.
  • Should we provide an authentication mechanism instead of requiring a tunneling method to be used first?
  • Should we define the EAP-CREDS credentials management in the document or shall we define it in a different document (should we define it at all?)
EMU WG

• To get a sense of the WG toward the proposal, would the WG like to work on this type of EAP method?

• If there is interest, would it be possible to start working on the text for the charter to include the development of a method for credentials management?