

**Credentials Provisioning and Management via EAP (EAP-CPRM)
draft-pala-eap-cprom-00**

Abstract

With the increase number of devices, protocols, and applications that rely on strong credentials (e.g., digital certificates, keys, or tokens) for network access, the need for a standard credentials provisioning layer is paramount. In particular, since EAP is deployed for authentication needs, the authors extend this use-case by including support for provisioning and management of credentials.

In particular, this specification defines how to support the provisioning of strong credentials to users and/or devices without the need for providing IP connectivity. The use of EAP not only for provisioning but also for managing network credentials provides a general conduit that can be exploited in different environments (e.g., Wired and WiFi networks credentials management).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 8, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Requirements notation	2
2.	Introduction	2
3.	Overview of existing solutions	2
4.	Scope Statement	3
5.	Protocol Overview	3
6.	IANA Considerations	3
7.	Security Considerations	3
8.	Acknowledgments	3
9.	Normative References	3
	Author's Address	4

[1.](#) Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[2.](#) Introduction

Because of the increasing number of highly available and highly utilized websites that require secure communications to protect the flow of information from the server to the client and the raising number of devices (IoT) that require strong authentication capabilities, the need for a low-cost and efficient approach to network credentials management is evident.

This specification addresses the problem of providing a simple-to-use and simple-to-deploy system for credentials management by extending the EAP protocol to support credentials provisioning and management functionality.

[3.](#) Overview of existing solutions

Currently there are many protocols that address the lifecycle of credentials. In particular, when it comes to digital certificates, some of the most deployed management protocols are:

- o Automated Certificate Management Environment
- o Certificate Management over CMS (CMC) [[RFC5272](#)] [[RFC6402](#)]
- o Enrollment over Secure Transport (EST) [[RFC7030](#)]

4. Scope Statement

This document focuses only on the definition of

5. Protocol Overview

Protocol Overview

6. IANA Considerations

This document uses a new DEAP type, CPR0M, whose value (TBD) MUST be allocated by IANA from the EAP TYPEs subregistry of the RADIUS registry.

7. Security Considerations

Several security considerations need to be explicitly considered for the system administrators and application developers to understand the weaknesses of the overall architecture.

8. Acknowledgments

The authors would like to thank everybody who provided insightful comments and helped in the definition of the deployment considerations.

9. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", [RFC 5272](#), DOI 10.17487/RFC5272, June 2008, <<https://www.rfc-editor.org/info/rfc5272>>.
- [RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", [RFC 6402](#), DOI 10.17487/RFC6402, November 2011, <<https://www.rfc-editor.org/info/rfc6402>>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed.,
"Enrollment over Secure Transport", [RFC 7030](#),
DOI 10.17487/RFC7030, October 2013,
<<https://www.rfc-editor.org/info/rfc7030>>.

Author's Address

Massimiliano Pala
CableLabs
858 Coal Creek Cir
Louisville, CO 80027
US

Email: m.pala@openca.org

URI: <http://www.linkedin.com/in/mpala>

