ABFAB Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 17, 2013

S. Winter
RESTENA
J. Salowey
Cisco
October 14, 2012

# Update to the EAP Applicability Statement for ABFAB
# draft-ietf-abfab-eapapplicability-01

## Abstract

This document updates the Extensible Authentication Protocol (EAP) applicability statement from RFC3748 to reflect recent usage of the EAP protocol in the Application Bridging for Federated Access Beyond web (ABFAB) working group.

## 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 http://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 April 17, 2013.

Table of Contents

## 1. Introduction

The EAP applicability statement in [RFC3748] defines the scope of the Extensible Authentication Protocol to be "for use in network access authentication, where IP layer connectivity may not be available.", and states that "Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED.".

While some of the recommendation against usage of EAP for bulk data transport is still valid, some of the other provisions in the applicability statement have turned out to be too narrow. Section 2 describes the example where EAP is used to authenticate application layer access. Section 3 provides new text to update the paragraph 1.3. "Applicability" in [RFC3748].

### 1.1. Requirements Language

In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. [RFC2119]

## 2. Uses of EAP for Application-Layer Access

Ongoing work in the IETF (abfab working group) specifies the use of EAP over GSSAPI for generic application layer access. In the past, using EAP in this context has met resistance due to the lack of channel bindings [RFC6677]. Without channel bindings, a peer cannot verify if an authenticator is authorized to provide an advertised service. In most network access use cases all access servers that are served by a particular EAP server are providing the same or very similar types of service. The peer does not need to differentiate between different access network services supported by the same EAP server.

However as additional services use EAP for authentication, the distinction of which service is being contacted becomes more important. Application services might have different properties. Consider an environment with multiple printers some of which provide a confidential service to output documents to a controlled location. If a peer sent a document to the wrong service then potentially sensitive information might be printed in an uncontrolled location and be disclosed. In addition, it might be more likely that a low-value service is compromised than some high value service. If the high-value service could be impersonated by a low-value service then the security of the overall system would be limited by the security of the lower value service.

This distinction is present in any environment where peers' security depends on which service they reach. However it is particularly acute in a federated environment where multiple organizations are involved. It is very likely that these organizations will have different security policies and practices. It is very likely that the goals of these organizations will not entirely be aligned. In many situations one organization could gain value by being able to impersonate another. In this environment, authenticating the EAP server is insufficient: the peer must also validate that the contacted host is authorized to provide the requested service.

For these reasons, channel binding MUST be implemented by peers, EAP servers and AAA servers in environments where EAP authentication is used to access application layer services. In addition, channel binding MUST default to being required by peers for non-network authentication. If the EAP server is aware that authentication is for something other than a network service, it too MUST default to requiring channel binding. Operators need to carefully consider the security implications before relaxing these requirements. One potentially serious attack exists when channel binding is not required and EAP authentication is introduced into an existing non-network service. A device can be created that impersonates a Network Access Service to peers, but actually proxies the authentication to the service that newly accepts EAP authentications may decrease the security of this service even for users who previously used non-EAP means of authentication to the service.

It is REQUIRED for the application layer to prove possession of the EAP MSK between the EAP Peer and EAP Authenticator. Failing to validate the possession of the EAP MSK can allow an attacker to insert himself into the conversation and impersonate the peer or authenticator. In addition, the application should define an channel binding attributes that are sufficient to validate that the application service is being correctly represented to the peer.

## 3. Revised EAP applicability statement

The following text is added to the EAP applicability statement in [RFC3748].

In cases where EAP is used for application authentication, support for EAP Channel Bindings is REQUIRED on the EAP Peer and EAP Server to validate that the host is authorized to provide the services requested. In addition, the application MUST define channel binding attributes that are sufficient to validate that the application service is being correctly represented to the peer. It is important for the protocol carrying EAP to prove possession of the EAP MSK between the EAP Peer and EAP Authenticator.

## 4. Security Considerations

In addition to the requirements discussed in the main sections of the document applications should take into account how server authentication is achieved. Some deployments may allow for weak server authentication that is then validated with an additional existing exchange that provides mutual authentication. In order to fully mitigate the risk of NAS impersonation when these mechanisms are used, it is RECOMMENDED that mutual channel bindings be used to bind the authentications together as described in [I-D.ietf-emu-crypto-bind]. When doing channel binding it is REQUIRED that the authenticator is not able to modify the channel binding data passed between the peer to the authenticator as part of the authentication process.

## 5. IANA Considerations

This document has no actions for IANA.

## 6. Acknowledgements

Large amounts of helpful text and insightful thoughts were contributed by Sam Hartman, Painless Security.

## 7. References

### 7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC6677] Hartman, S., Clancy, T., and K. Hoeper, "Channel-Binding Support for Extensible Authentication Protocol (EAP) Methods", RFC 6677, July 2012.

### 7.2. Informational References

[I-D.ietf-emu-crypto-bind] Hartman, S., Wasserman, M., and D. Zhang, "EAP Mutual Cryptographic Binding", draft-ietf-emu-crypto-bind-00 (work in progress), June 2012.

Authors' Addresses

Stefan Winter
Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
Luxembourg 1359
LUXEMBOURG

Phone: +352 424409 1
Fax: +352 422473
EMail: stefan.winter@restena.lu
URI: http://www.restena.lu.

Joseph Salowey
Cisco Systems
2901 3rd Ave
Seattle, Washington 98121
USA

EMail: jsalowey@cisco.com