Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: April 11, 2010

J. Bournelle
L. Morand
Orange Labs
S. Decugis, Ed.
NICT
Q. Wu
Huawei
G. Zorn, Ed.
Network Zen
October 8, 2009

Diameter support for EAP Re-authentication Protocol (ERP)
draft-ietf-dime-erp-02.txt

Status of This Memo

Copyright Notice

Abstract

EAP Re-authentication Protocol (ERP) defines extensions to the Extensible Authentication Protocol (EAP) to support efficient re-authentication between the peer and an EAP Re-authentication (ER) server through a compatible authenticator. This document specifies Diameter support for ERP. It defines a new Diameter ERP application to transport ERP messages between ER authenticator and ER server, and a set of new AVPs that can be used to transport the cryptographic material needed by the re-authentication server.

Table of Contents

1. Introduction

[RFC5296] defines the EAP Re-authentication Protocol (ERP). It consists in the following steps:

1. Bootstrapping: a root key for re-authentication is derived from the Extended Master Session Key (EMSK) created during EAP authentication [RFC5295]. This root key is transported from the EAP server to the ER server.

2. Re-authentication: a one-round-trip exchange between the peer and the ER server, resulting in mutual authentication. To accomplish the EAP reauthentication functionality, ERP defines two new EAP codes - EAP-Initiate and EAP-Finish.

This document defines how Diameter transports the ERP messages (Re-authentication step). For this purpose, we define a new Application Id for ERP, and re-use the Diameter EAP commands (DER/DEA).

This document also discusses the distribution of the root key (bootstrapping step), either during the initial EAP authentication (implicit bootstrapping) or during the first ERP exchange (explicit bootstrapping). Security considerations for this key distribution are detailed in [RFC5295].

2. Terminology

This document uses terminology defined in [RFC3748], [RFC5295], [RFC5296], and [RFC4072].

"Root key" (RK) or "bootstrapping material" refer to the rRK or rDSRK derived from an EMSK, depending on the location of the ER server in home or foreign domain.

We use the notation "ERP/DER" in this document to refer to a Diameter-EAP-Request command with its Application Id set to Diameter

ERP application. Similarly, we use the "ERP/DEA", "EAP/DER", and "EAP/DEA".

2.1. Requirements Language

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].

3. Assumptions

This document makes the following assumptions.

The Home EAP server of a peer that wants to use ERP is extended to support:

Cryptographic operations needed to derive the ERP root key from the EMSK. By deriving the ERP root key for a specific domain, the home EAP server implicitly authorizes the use of ERP within this domain.

Diameter operations needed to include this root key in a response message, when a request for this root key was received in a request message. The two AVP that contain the request for and the root key material are defined in this document.

(recommended) Ability to answer a DER message with EAP-Payload containing an explicit bootstrapping ERP message.

The Authenticator (NAS) is extended to support:

Allow the new ERP command codes (EAP-Initiate and EAP-Finish) in its EAP pass-through mode.

(optional) Send the EAP-Initiate/Re-Auth-Start message

(optional) Provide the local domain name via lower layer specific mechanism or via TLV in the EAP-Initiate/Re-Auth-Start message.

Encapsulate ERP message and receive corresponding Diameter answer, as described in this document.

If one of the components does not match these assumptions, the ERP mechanism will fail. In such situation, a full EAP authentication may be attempted as a fallback mechanism.

We consider at most one logical ER server entity in a domain. If several physical servers are deployed for robustness, a replication mechanism must be deployed to synchronize the ERP states (root keys) between these servers. This replication mechanism is out of the scope of this document. If several ER servers are deployed in the domain, we assume that they can be used interchangeably.

4. Protocol Overview

The following figure shows the components involved in ERP, and their interactions.

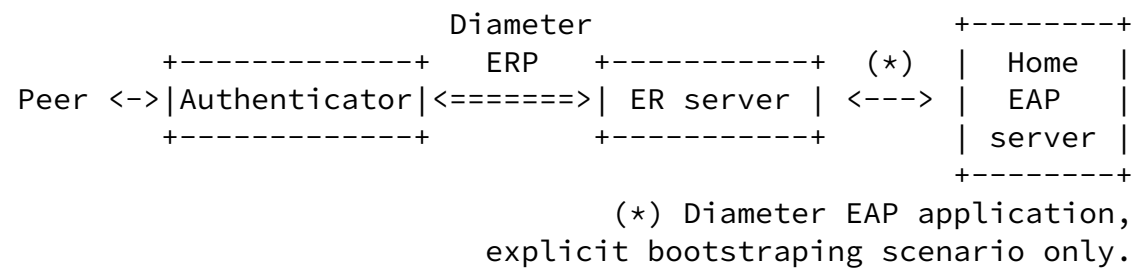


Figure. Diameter ERP overview.

The ER server is located either in the home domain (same as EAP server) or in the visited domain (same as authenticator, when it differs from the home domain).

When the peer initiates an ERP exchange, the authenticator creates a Diameter-EAP-Request message, as described in Diameter EAP application [RFC4072]. The Application Id of the message is set to Diameter ERP application (code: TBD) in the message. The exact processing to generate the ERP/DER message is detailed in section Section 6.

If there is an ER server in the same domain as the authenticator

(local domain), Diameter routing MUST be configured so that this ERP/DER message reachs this server, even if the Destination-Realm is not the local domain.

If there is no local ER server, the message is routed according to its Destination-Realm AVP content, extracted from the realm component of the keyName-NAI attribute. As specified in [RFC5296], this realm is the home domain of the peer in case of bootstrapping exchange ('B' flag is set in ERP message) or the domain of the bootstrapped ER server otherwise .

If no ER server is available in the home domain either, the ERP/DER message cannot be delivered, and an error DIAMETER_UNABLE_TO_DELIVER is generated as specified in [RFC3588] and returned to the authenticator. The authenticator may cache this information (with limited duration) to avoid further attempts for ERP with this realm. It may also fallback to full EAP authentication to authenticate the peer.

When an ER server receives the ERP/DER message, it searches its local database for a root key matching the keyName part of the User-Name AVP. If such key is found, the ER server processes the ERP message as described in [RFC5296] then creates the ERP/DEA answer as described in Section 6. The rMSK is included in this answer.

Finally, the authenticator extracts the rMSK from the ERP/DEA as

described in [RFC5296], and forwards the content of the EAP-Payload AVP, the EAP-Finish/Re-Auth message, to the peer.

If the EAP-Initiate/Re-Auth message has its 'B' flag set (Bootstrapping exchange), the ER server should not possess the root key in its local database . In this case, the ER server acts as a proxy, and forwards the message to the home EAP server after changing its Application Id to Diameter EAP and adding an AVP to request the root key. See section Section 5 for more detail on this process.

5. Bootstrapping the ER server

The bootstrapping process involves the home EAP server and the ER server, but also impacts the peer and the authenticator. In ERP, the peer must derive the same keying material as the ER server. To

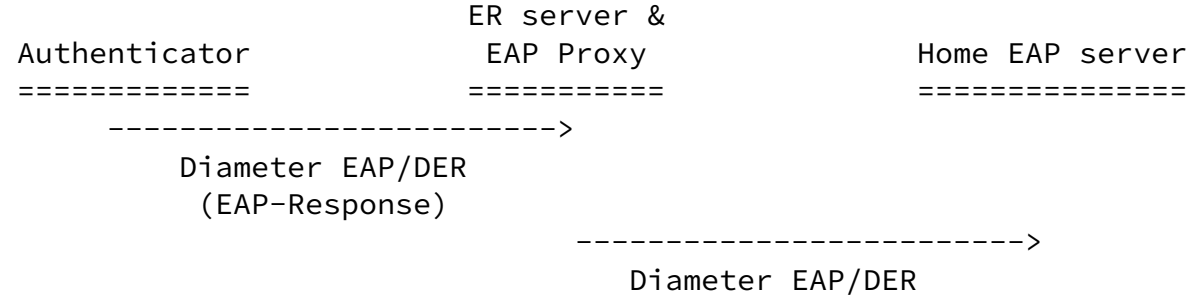
achieve this, it must learn the domain name of the ER server. How this information is acquired is outside the scope of this specification, but it may involves that the authenticator is configured to advertize this domain name, especially in the case of re-authentication after a handover.

The bootstrapping of an ER server with a given root key happens either during the initial EAP authentication of the peer when the EMSK -- from which the root key is derived -- is created, during the first re-authentication, or sometime between those events. We only consider the first two possibilities in this specification, in the following subsections.

5.1. Bootstrapping during initial EAP authentication

Bootstrapping the ER server during the initial EAP authentication (also known as implicit bootstrapping) offers the advantage that the server is immediatly available for re-authentication of the peer, thus minimizing the re-authentication delay. On the other hand, it is possible that only a small number of peers will use re-authentication in the visited domain. Deriving and caching key material for all the peers (for example, for the peers that do not support ERP) is a waste of resources and SHOULD be avoided.

To achieve implicit bootstrapping, the ER server must act as a Diameter EAP Proxy as defined in Diameter Base Protocol [RFC3588], and routing must be configured so that Diameter messages of a full EAP authentication are routed through this proxy. The figure bellow captures this mechanism.



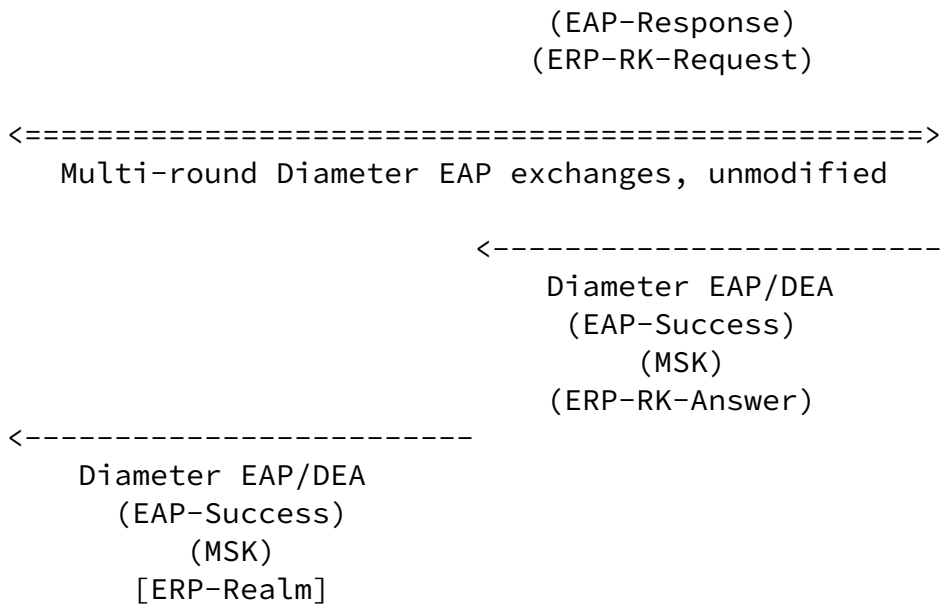


Figure. ERP bootstrapping during full EAP authentication

The ER server proxies the first DER of the full EAP authentication and adds the ERP-RK-Request AVP inside, if this AVP is not already in the message (which might happen if there are ER servers in the visited and the home domains), then forwards the request.

If the EAP server does not support ERP extensions, it will simply ignore this grouped AVP and continue as specified in [RFC4072]. If the server supports the ERP extensions, it caches the ERP-Realm value with the session, and continues the EAP authentication. When the authentication is complete, if it is successful and the EAP method generated an EMSK, the server MUST compute the rRK or rDSRK (depending on the value of ERP-Realm) as specified in [RFC5296], and add an ERP-RK-Answer AVP in the Diameter-EAP-Request message, in addition to the MSK and EAP-Success payloads.

When the ER server proxies a Diameter-EAP-Answer message with a Session-Id corresponding to a message to which it added an ERP-RK-Answer, and the Result-Code is DIAMETER_SUCCESS, it MUST examine the message, extract and remove any ERP-RK-Answer AVP from the message, and save its content. If the message does not contain an ERP-RK-Answer AVP, the ER server MAY save this information to avoid possible

subsequent re-authentication attempts for this session. In any case,

the information stored SHOULD NOT have a lifetime greater than the EMSK lifetime

If the ER server is successfully bootstrapped, it MAY also add the ERP-Realm AVP after removing the ERP-RK-Answer AVP in the EAP/DEA message. This could be used by the authenticator to notify the peer that ERP is bootstrapped, with the ER domain information. How this information can be transmitted to the peer is outside the scope of this document.

5.2. Bootstrapping during first re-authentication

Bootstrapping the ER server during the first re-authentication (also known as explicit bootstrapping) offers several advantages: it saves resources, since we generate and cache only root key that we actually need, and it can accomodate inter-domain handovers or ER servers that loose their state (for example after reboot) . On the other hand, the first re-authentication with the ER server requires a one-round-trip exchange with the home EAP server, which adds some delay to the process (but it is more efficient than a full EAP authentication in any case). It also requires some synchronization between the peer and the visited domain: since the ERP message is different for explicit bootstrapping exchange and for normal re-authentication, explicit bootstrapping should not be used if implicit bootstrapping was already performed.

The ER server receives the ERP/DER message containing the EAP-Initiate/Re-Auth message with the 'B' flag set. It proxies this message, and do the following processing in addition to standard proxy operations:

Change the Application Id in the header of the message to Diameter EAP Application (code 5).

Change the content of Application-Auth-Id accordingly.

Add the ERP-RK-Request AVP, which contains the name of the domain where the ER server is located.

Then the server forwards the EAP/DER request, which is routed to the home EAP server.

If the home EAP server does not support ERP extensions, it replies with an error since the encapsulated EAP-Initiate/Re-auth command is not understood. Otherwise, it processes the ERP request as described

in [RFC5296]. In particular, it includes the Domain-Name TLV attribute with the content from the ERP-Realm AVP. It creates the EAP/DEA reply message following standard processing from [RFC4072] (in particular EAP-Master-Session-Key AVP is used to transport the rMSK), and includes the ERP-RK-Answer AVP.

The ER server receives this EAP/DEA and proxies it as follow, in addition to standard proxy operations:

Set the Application Id back to Diameter ERP (code TBD)

Extract and cache the content of the ERP-RK-Answer.

The DEA is then forwarded to the authenticator, that can use the rMSK as described in [RFC5296].

The figure below captures this proxy behavior:

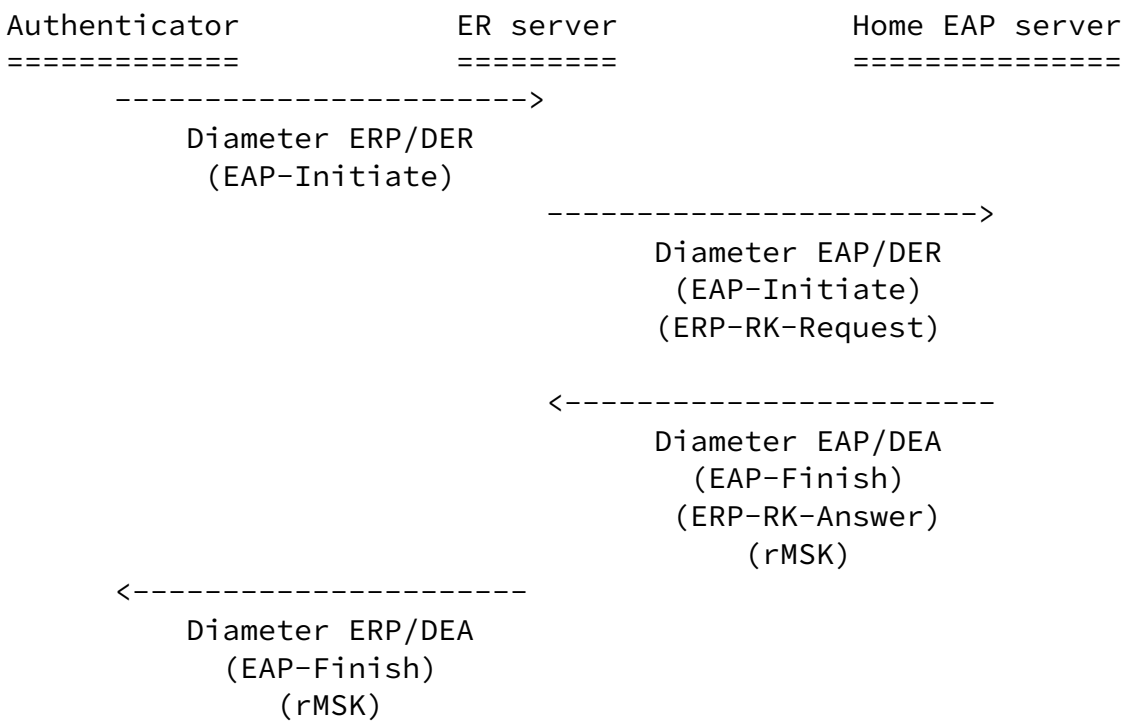


Figure. ERP explicit bootstrapping message flow

6. Re-Authentication

This section describes in detail a re-authentication exchange with a (bootstrapped) ER server. The following figure summarizes the re-authentication exchange.

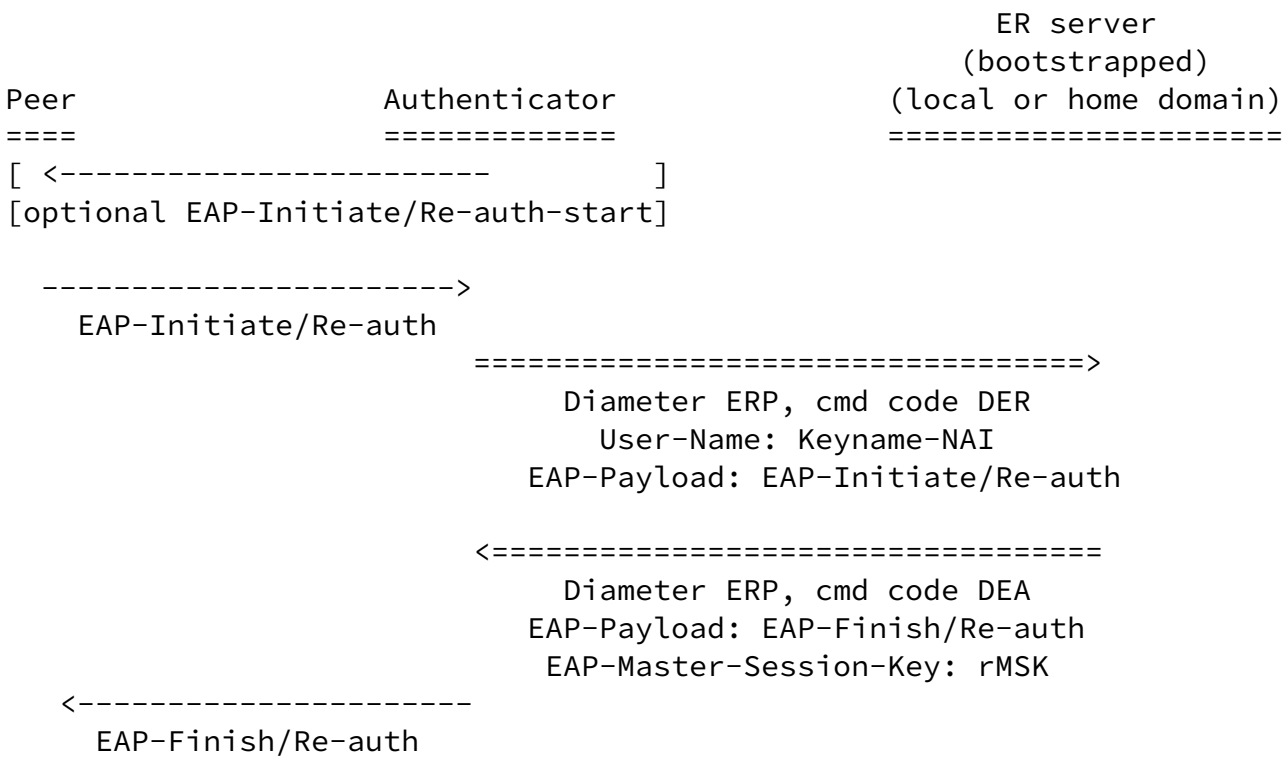


Figure. Diameter ERP exchange.

In ERP, the peer sends an EAP-Initiate/Re-auth message to the ER server via the authenticator. Alternatively, the NAS may send an EAP-Initiate/Re-auth-Start message to the peer to trigger the start of ERP. In this case, the peer responds with an EAP-Initiate/Re-auth message to the NAS.

If the authenticator does not support ERP (pure [RFC4072] support), it discards the EAP packets with unknown ERP-specific code (EAP-Initiate). The peer may fallback to full EAP authentication in such case.

When the authenticator receives an EAP-Initiate/Re-auth message from the peer, it process as described in [RFC5296] with regards to the EAP state machine. It creates a Diameter EAP Request message following the general process of Diameter EAP [RFC4072], with the following differences:

The Application Id in the header is set to Diameter ERP (code TBD).

The value in Auth-Application-Id AVP is also set to Diameter ERP Application.

The keyName-NAI attribute from ERP message is used to create the content of User-Name AVP and Destination-Realm AVP.

The Auth-Request-Type AVP content is set to [Editor's note: FFS].

The EAP-Payload AVP contains the ERP message, EAP-Initiate/ Re-Auth.

Then this ERP/DER message is sent as described in Section 4.

The ER server receives and processes this request as described in Section 4. It then creates a Diameter answer ERP/DEA, following the general processing described in [RFC4072], with the following differences:

The Application Id in the header is set to Diameter ERP (code TBD).

The value in Auth-Application-Id AVP is also set to Diameter ERP Application.

The Result-Code AVP is set to an error value in case ERP authentication fails, or to DIAMETER_SUCCESS if ERP is successful.

The EAP-Payload AVP contains the ERP message, EAP-Finish/Re-auth.

In case of successful authentication, the EAP-Master-Session-Key AVP contains the Re-authentication Master Session Key (rMSK) derived by ERP.

When the authenticator receives this ERP/DEA answer, it processes it

as described in Diameter EAP [RFC4072] and [RFC5296]: the content of EAP-Payload AVP content is forwarded to the peer, and the content of EAP-Master-Session-Key AVP is used as a shared secret for Secure Association Protocol.

7. Application Id

We define a new Diameter application in this document, Diameter ERP Application, with an Application Id value of TBD. Diameter nodes conforming to this specification in the role of ER server MUST advertise support by including an Auth-Application-Id AVP with a value of Diameter ERP Application in the of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, as described in [RFC3588].

The primary use of the Diameter ERP Application Id is to ensure

proper routing of the messages, and that the nodes that advertise the support for this application do understand the new AVPs defined in section Section 8 , although these AVP have the 'M' flag cleared.

8. AVPs

This specification defines the following new AVPs.

8.1. ERP-RK-Request AVP

The ERP-RK-Request AVP (AVP Code TBD) is of type grouped AVP. This AVP is used by the ER server to indicate its willingness to act as ER server for a particular session.

This AVP has the M and V bits cleared.

```
ERP-RK-Request ::= < AVP Header: TBD >
                   { ERP-Realm }
                 * [ AVP ]
```

Figure. ERP-RK-Request ABNF

8.2. ERP-Realm AVP

The ERP-Realm AVP (AVP Code TBD) is of type DiameterIdentity. It

contains the name of the realm in which the ER server is located.

This AVP has the M and V bits cleared.

8.3. ERP-RK-Answer AVP

The ERP-RK-Answer AVP (AVP Code TBD) is of type grouped AVP. It is used by the home EAP server to provide ERP root key material to the ER server.

This AVP has the M and V bits cleared.

```
ERP-RK-Answer ::= < AVP Header: TBD >
                  { ERP-RK }
                  { ERP-RK-Name }
                  { ERP-RK-Lifetime }
                * [ AVP ]
```

Figure. ERP-RK-Answer ABNF

8.4. ERP-RK AVP

The ERP-RK AVP (AVP Code TBD) is of type OctetString. It contains the root key (either rRK or rDSRK) sent by the home EAP server to the ER server, in answer to request containing an ERP-RK-Request AVP. How this material is derived and used is specified in [RFC5296].

This AVP has the M and V bits cleared.

8.5. ERP-RK-Name AVP

The ERP-RK-Name AVP (AVP Code TBD) is of type OctetString. This AVP contains the EMSKname which identifies the keying material. How this name is derived is beyond the scope of this document and defined in [RFC5296].

This AVP has the M and V bits cleared.

8.6. ERP-RK-Lifetime AVP

The ERP-RK-Lifetime AVP (AVP Code TBD) is of type Unsigned32 and contains the root key material remaining lifetime in seconds. It MUST not be greater than the remaining lifetime of the EMSK it is derived from.

This AVP has the M and V bits cleared.

9. Commands

We do not define any new command in this specification. We reuse the Diameter-EAP-Request and Diameter-EAP-Answer commands defined in [RFC4072].

Since the original ABNF of these commands allow other optional AVPs ("* [AVP]"), and the new AVPs defined in this specification do not have the 'M' flag set, the ABNF does not need any change. Anyway, a Diameter node that advertizes support for the Diameter ERP application MUST support the new AVPs defined in this specification.

Command-Name	Abbrev.	Code	Reference	Application
Diameter-EAP-Request	DER	268	RFC 4072	Diameter ERP
Diameter-EAP-Answer	DEA	268	RFC 4072	Diameter ERP

Figure. Command Codes

10. Open issues

This document does not address some known issues in Diameter ERP mechanism. The authors would like to hear ideas about how to address them.

The main issue is the use of ERP for authentication after a handover of the peer to a new authenticator (or different authenticator port). Diameter ERP is not meant to be a mobility protocol. A number of issues appear when we try to do handover in Diameter ERP (alone): how to manage the Session-Id AVP; how does the ER server provide the

Authorization AVPs; how does the peer learn the ERP domain of the new authenticator; how does the home server reachs the peer to for example terminate the session; and so on... Therefore, the management of the session for a mobile peer is not (yet) addressed in this document. It must be studied how Diameter ERP can be for example used in conjunction with a mobility application (Diameter MIP4, Diameter MIP6) to support the optimized re-authentication in such situation.

Another issue concerns the case where the home realm contains several EAP servers. In multi rounds full EAP authentication, the Destination-Host AVP provides the solution to reach the same server across the exchanges. Only this server possess the EMSK for the session. In case of explicit bootstrapping, the ER server must therefore be able to reach the correct server to request the DSRK. A solution might consist in saving the Origin-Host AVP of all successful EAP/DEA in the ER server, which is a bit similar to the implicit bootstrapping scenario described here -- only we save the server name instead of the root key, and we must then be able to match the DSRK with the user name.

Finally, this document currently lacks a description of what happens when a Re-Auth-Request is received for a peer on the authenticator.

11. Acknowledgements

Hannes Tschofenig wrote the initial draft for this document and provided useful reviews.

Vidya Narayanan reviewed a rough draft version of the document and found some errors.

Lakshminath Dondeti contributed to the early versions of the document.

Many thanks to these people!

12. IANA Considerations

This document requires IANA registration of the following new elements in the Authentication, Authorization, and Accounting (AAA)

Parameters [1] registries.

12.1. Diameter ERP application

This specification requires IANA to allocate a new value "Diameter ERP" in the "Application IDs" registry created by in [RFC3588].

Application Identifier	Value
Diameter ERP	TBD

IANA consideration for Diameter ERP application

12.2. New AVPs

This specification requires IANA to allocate new values from the "AVP Codes" registry defined in [RFC3588] for the following AVPs:

ERP-RK-Request

ERP-Realm

ERP-RK-Answer

ERP-RK

ERP-RK-Name

ERP-RK-Lifetime

These AVPs are defined in section Section 8.

13. Security Considerations

The security considerations from the following RFC apply here: [RFC3588], [RFC4072], [RFC5247], [RFC5295], and [RFC5296].

EAP channel bindings may be necessary to ensure that the Diameter client and the server are in sync regarding the key Requesting Entity's Identity. Specifically, the Requesting Entity advertises its identity through the EAP lower layer, and the user or the EAP peer communicates that identity to the EAP server (and the EAP server communicates that identity to the Diameter server) via the EAP method for user/peer to server verification of the Requesting Entity's

Identity.

14. References

14.1. Normative References

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

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

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC5295] Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", RFC 5295, August 2008.

[RFC5296] Narayanan, V. and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", RFC 5296, August 2008.

14.2. Informative References

[I-D.ietf-dime-app-design-guide] Fajardo, V., Asveren, T., Tschofenig, H., McGregor, G., and J. Loughney, "Diameter Applications Design Guidelines", draft-ietf-dime-app-design-guide-08 (work in progress), November 2008.

[I-D.ietf-hokey-key-mgm] Hoeper, K. and Y. Ohba, "Distribution of EAP based keys for handover and re-authentication", draft-ietf-hokey-key-mgm-06 (work in progress), April 2009.

[I-D.wu-dime-local-keytran] Wu, W., "Diameter support for local key transport protocol between local server and home AAA server", draft-wu-dime-local-keytran-00 (work in progress), May 2009.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", RFC 5247, August 2008.

URIs

[1] <http://www.iana.org/assignments/aaa-parameters/>

Authors' Addresses

Julien Bournelle
Orange Labs
38-40 rue du general Leclerc
Issy-Les-Moulineaux 92794
France

EMail: julien.bournelle@orange-ftgroup.com

Lionel Morand
Orange Labs

38-40 rue du general Leclerc
Issy-Les-Moulineaux 92794
France

EMail: lionel.morand@orange-ftgroup.com

Sebastien Decugis (editor)
NICT
4-2-1 Nukui-Kitamachi
Tokyo 184-8795
Koganei, Japan

EMail: sdecugis@nict.go.jp

Qin Wu
Huawei Technologies Co., Ltd
Site B, Floor 12F, Huihong Mansion, No.91 Baixia Rd.
Nanjing 210001
China

EMail: sunseawq@huawei.com

Glen Zorn (editor)
Network Zen
1310 East Thomas Street
#306
Seattle, Washington 98102
USA

Phone: +1 (206) 377-9035
EMail: gwz@net-zen.net