Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 16, 2012

J. Bournelle
L. Morand
Orange Labs
S. Decugis
INSIDE Secure
Q. Wu
Huawei
G. Zorn
Network Zen
January 13, 2012

Diameter support for EAP Re-authentication Protocol (ERP) draft-ietf-dime-erp-08.txt

Abstract

The 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 an ER authenticator and the ER server, and a set of new AVPs that can be used to transport the cryptographic material needed by the re-authentication server.

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 July 16, 2012.

Copyright Notice

Table of Contents

1. Introduction

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

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.

Re-authentication

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

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

This document also discusses the distribution of the root key during bootstrapping, in conjunction with either the initial EAP authentication (implicit bootstrapping) or the first ERP exchange (explicit bootstrapping). Security considerations for this key distribution are detailed in RFC 5295 [RFC5295].

2. Terminology

This document uses terminology defined in RFC3748 [RFC3748], RFC5295 [RFC5295], RFC5296 [RFC5296], and RFC4072 [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" and "ERP/DEA" in this document to refer to Diameter-EAP-Request and Diameter-EAP-Answer commands with the Application Id set to <Diameter ERP Application> Section 11.1; the same commands are denoted "EAP/DER" and "EAP/DEA" when the Application Id in the message is set to <Diameter EAP Application> [RFC4072].

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 assumes the existence of 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 multiple ER servers are deployed in the domain, we assume that they can be used interchangeably. If multiple ER servers are deployed across the domains, we assume only one ER server that is near to the peer is getting involved in the ERP.

Also this document assumes the existence of at most one EAP server entity in the home domain. In case of multiple physical home EAP servers in the same domain, if the ER server wants to reach the same home EAP server, the ER server may cache the Destination-Host AVP corresponding to the home EAP server it requests.

4. Protocol Overview

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

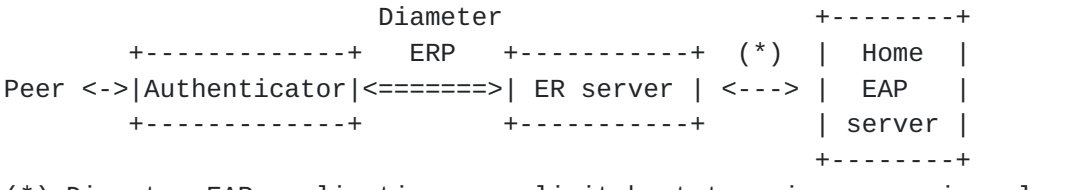


Figure 1: Diameter ERP Overview.

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 (DER) message [RFC4072]. The Application Id of the message is set to that of the Diameter ERP application Section 11.1 in the message. The generation of the ERP/DER message is detailed in Section 6.

If there is an ER server in the same domain as the authenticator (i.e., the local domain), Diameter routing MUST be configured so that this ERP/DER message reaches that server, even if the Destination-Realm is not the same as 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 [RFC5296], this realm is the home domain of the peer in the 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 MUST be generated as specified in [I-D.ietf-dime-rfc3588bis] and returned to the authenticator. The authenticator MAY cache this information (with limited duration) to avoid further attempts to execute 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 valid, unexpired 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 [RFC5296], and forwards the content of the EAP-Payload AVP, the EAP-Finish/Re-Auth message, to the peer.

The ER server may or may not possess the root key in its local database. If the EAP-Initiate/Re-Auth message has its 'B' flag set (Bootstrapping exchange) and the ER server possesses the root key, the ER server SHOULD respond directly to the peer that initiated the ERP exchange. Otherwise, the ER server SHOULD act as a proxy and forward the message to the home EAP server after changing its Application Id to Diameter EAP and adding the ERP-RK-Request AVP to request the root key. See 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 the authenticator might be configured to advertize this domain name, especially in the case of re-authentication after a

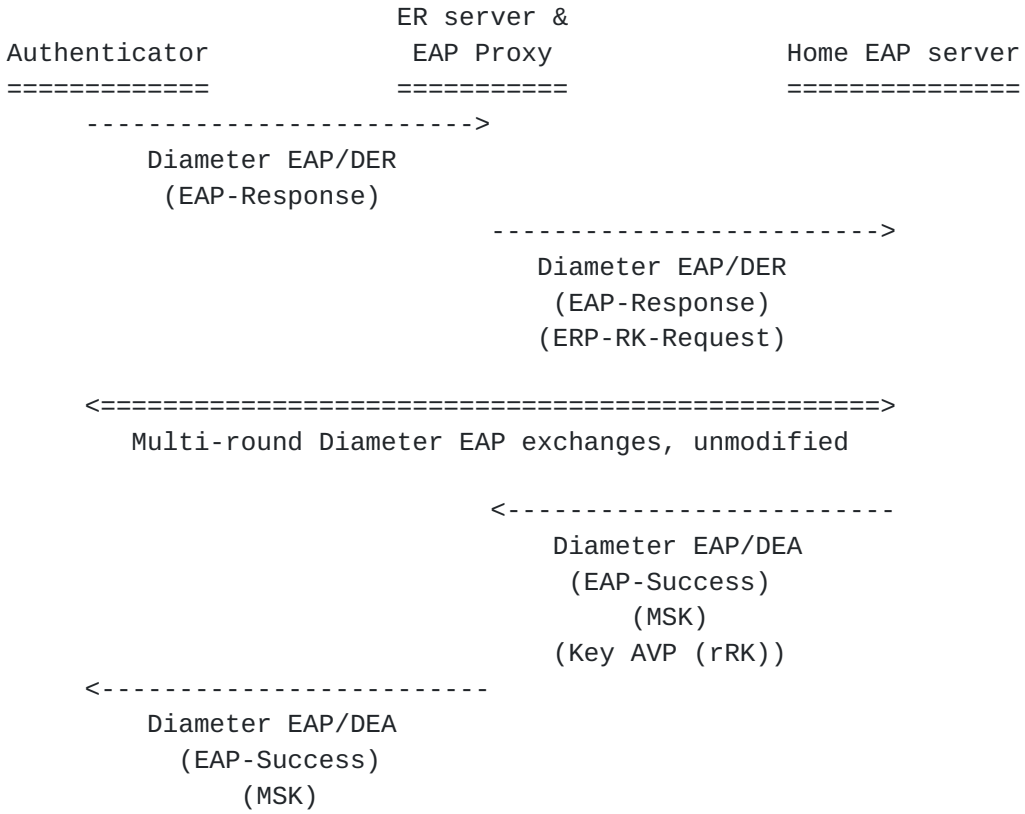
handover.

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 sub-sections.

5.1. Bootstrapping During the Initial EAP authentication

Bootstrapping the ER server during the initial EAP authentication (also known as implicit bootstrapping) offers the advantage that the server is immediately 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 acts as a Diameter EAP Proxy , and Diameter routing MUST be configured so that Diameter EAP application messages are routed through this proxy. The figure bellow illustrates this mechanism.



[ERP-Realm]

Figure 2: ERP Bootstrapping During Full EAP Authentication

The authenticator creates the first DER of the full EAP authentication and sends it to the ER server. The ER server proxies the first DER of the full EAP authentication and adds the ERP-RK-Request AVP inside, then forwards the request to the home EAP server.

If the home Diameter server does not support the Diameter ERP extensions, it simply ignores the ERP-RK-Request AVP and continues as specified in RFC 4072 [RFC4072]. If the server supports the ERP extensions, it saves the value of the ERP-Realm AVP found inside the ERP-RK-Request AVP, and continues with the EAP authentication. When the authentication completes, if it is successful and the EAP method has generated an EMSK, the server MUST derive the rRK as specified in RFC 5296 [RFC5296], using the saved domain name. It then includes the rRK inside a Key AVP (Section 8.3) with the Key-Type AVP set to rRK, before sending the DEA as usual.

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-Request AVP, and the Result-Code is DIAMETER_SUCCESS, it MUST examine the message and save and remove any Key AVP (Section 8.3) with Key-Type AVP set to rRK. If the message does not contain such Key AVP, the ER server may cache the information that ERP is not possible for this session to avoid possible subsequent attempts. In any case, the information stored in ER server concerning a session should not have a lifetime greater than the EMSK for this session.

If the ER server is successfully bootstrapped, it should also add the ERP-Realm AVP after removing the Key AVP with Key-Type of rRK in the EAP/DEA message. This ERP-Realm information can be used by the authenticator to notify the peer that ER server is bootstrapped, and for which domain. How this information can be transmitted to the peer is outside the scope of this document. This information needs to be sent to the peer if both implicit and explicit bootstrapping mechanisms are possible, because the ERP message and the root key used for protecting this message are different in bootstrapping exchanges and non-bootstrapping exchanges.

5.2. Bootstrapping During the First Re-authentication

Bootstrapping the ER server during the first re-authentication (also known as explicit bootstrapping) is only needed when there is no local ER server in the visited domain and there is an ER server in the home domain. It is less resource-intensive, since the EMSK generated during initial EAP authentication is reused to derive root

keys. On the other hand, the first re-authentication requires a one-round-trip exchange with the home EAP server, since the EMSK is generated during the initial EAP authentication and never leaves the home EAP server, which is less efficient than the implicit bootstrapping scenario.

The EAP-Initiate/Re-auth message is sent to the home ER server. The home ER server receives the ERP/DER message containing the EAP-Initiate/Re-Auth message with the 'B' flag set. It creates the new EAP/DER message using the received DRP/DER message and performs the following processing:

Set the Application Id in the header of the message to <Diameter EAP Application> [RFC4072]

Extract the ERP-RK-Request AVP from the ERP/DER message, which contains the name of the domain where the ER server is located and add it to the newly created ERP/DER message.

Then the newly created EAP/DER is sent and routed to the home Diameter EAP application server.

If the home Diameter server does not support ERP extensions, it replies with an error since the encapsulated ERP-RK-Request AVP is not understood. Otherwise, it processes the DSRK request as described in [RFC5296]. In particular, it includes the Domain- Name TLV attribute with the content from the ERP-Realm AVP. The server creates the EAP/DEA reply message [RFC4072] including an instance of the Key AVP (Section 8.3) with Key-Type AVP set to rRK and an instance of the Domain-Name TLV attribute with the content from the ERP-Realm AVP.

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

Set the Application Id back to Diameter ERP Application Id (Section 11.1)

Extract and cache the content of the Key AVP with Key-Type set to rRK, as described in the implicit scenario (Section 5.1).

The ERP/DEA message is then forwarded to the authenticator, that can use the rMSK as described in RFC 5296 [RFC5296].

The figure below captures this proxy behavior:

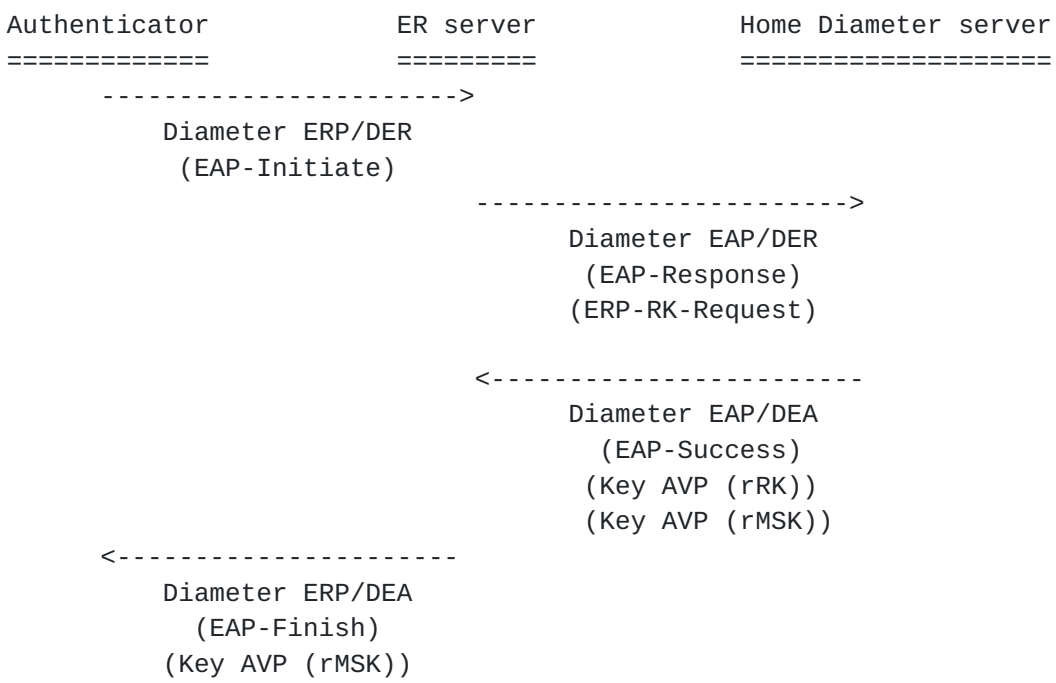


Figure 3: ERP Explicit Bootstrapping Message Flow

6. Re-Authentication

This section describes in detail a re-authentication exchange with an ER server that was previously bootstrapped. The following figure summarizes the re-authentication exchange.

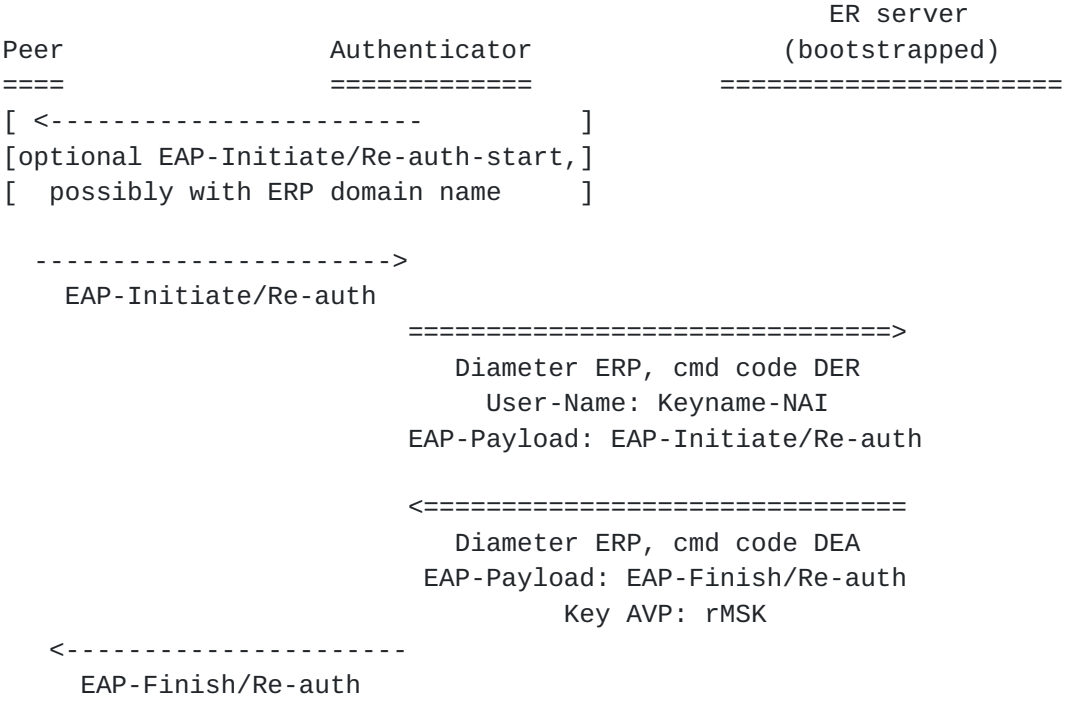


Figure 4: Diameter ERP Re-authentication Exchange

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

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

When the authenticator receives an EAP-Initiate/Re-auth message from the peer, the message is processed as described in [RFC5296] with regard to the EAP state machine. It creates a Diameter ERP/DER 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>.

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

The Auth-Request-Type AVP content is set to the appropriate value.

The EAP-Payload AVP contains the EAP-Initiate/Re-Auth meassge.

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 an ERP/DEA message following the general process described in RFC4072 [RFC4072], with the following differences:

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

The value of the Auth-Application-Id AVP is also set to <Diameter ERP>.

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

If authentication is successful, an instance of the Key AVP containing the Re-authentication Master Session Key (rMSK) derived by ERP is included.

When the authenticator receives this ERP/DEA answer, it processes it as described in Diameter EAP [RFC4072] and RFC5296 [RFC5296]: the content of the EAP-Payload AVP is forwarded to the peer, and the contents of the Keying-Material AVP [I-D.ietf-dime-local-keytran] is used as a shared secret for a secure association protocol specific to the lower-layer in use.

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 in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [I-D.ietf-dime-rfc3588bis].

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 8, although these AVP have the 'M' flag cleared.

8. AVPs

The following sub-sections discuss the AVPs used by the Diameter ERP application.

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 5: 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. Key AVP

The Key AVP [I-D.ietf-dime-local-keytran] is of type "Grouped" and is used to carry the rRK or rMSK and associated attributes. The usage of the Key AVP and its constituent AVPs in this application is specified in the following sub-sections.

8.3.1. Key-Type AVP

The value of the Key-Type AVP MUST be set to 2 for rRK or 3 for rMSK.

8.3.2. Keying-Material AVP

The Keying-Material AVP contains the rRK sent by the home EAP server to the ER server, in answer to a request containing an ERP-RK-Request AVP, or the rMSK sent by the ER server to the authenticator. How this material is derived and used is specified in RFC 5296 [RFC5296].

8.3.3. Key-Name AVP

This AVP contains the EMSKname which identifies the keying material. The derivation of this name is specified in RGC 5296 [RFC5296].

8.3.4. Key-Lifetime AVP

The Key-Lifetime AVP contains the lifetime of the keying material in seconds. It MUST NOT be greater than the remaining lifetime of the EMSK from which the material was derived.

9. Contributors

Hannes Tschofenig wrote the initial draft of this document.

Lakshminath Dondeti contributed to the early versions of the document.

10. Acknowledgements

Hannes Tschofenig provided useful reviews.

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

Many thanks to these people!

11. IANA Considerations

This document requires IANA registration of the following new elements in the Authentication, Authorization, and Accounting (AAA) Parameters [1] registries.

11.1. Diameter Application Identifier

This specification requires IANA to allocate a new value "Diameter ERP" in the "Application IDs" registry using the policy specified in Section 11.3 of RFC 3588 [RFC3588].

11.2. New AVPs

This specification requires IANA to allocate new values from the "AVP Codes" registry according to the policy specified in Section 11.1 of Fajardo, et al. [I-D.ietf-dime-rfc3588bis] for the following AVPs:

ERP-RK-Request

ERP-Realm

These AVPs are defined in Section 8.

12. Security Considerations

The security considerations from the following documents apply here:

- Fajardo, et al. [I-D.ietf-dime-rfc3588bis]
- RFC 4072 [RFC4072]
- RFC 5296 [RFC5296]
- Zorn, Wu and Cakulev [I-D.ietf-dime-local-keytran]

13. Normative References

[I-D.ietf-dime-local-keytran] Zorn, G., Wu, W., and V. Cakulev, "Diameter Attribute-Value Pairs for Cryptographic Key Transport", draft-ietf-dime-local-keytran-14 (work in progress), August 2011.

[I-D.ietf-dime-rfc3588bis] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", draft-ietf-dime-rfc3588bis-29 (work in progress), August 2011.

[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.

[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
INSIDE Secure
41 Parc Club du Golf
Aix-en-Provence 13856
France

Phone: +33 (0)4 42 39 63 00
EMail: sdecugis@freediameter.net

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
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thailand

EMail: glenzorn@gmail.com