

Working Group
Internet-Draft
Intended status: Informational
Expires: November 28, 2014

U. Chunduri
A. Tian
A. Keranen
Ericsson
T. Kivinen
INSIDE Secure
May 27, 2014

KARP KMP: Simplified Peer Authentication
draft-chunduri-karp-kmp-router-fingerprints-05

Abstract

This document describes the usage of Router Fingerprint Authentication (RFA) with public keys as a potential peer authentication method with KARP pair wise and group Key Management Protocols (KMPs). The advantage of RFA is, it neither requires out-of-band, mutually agreeable symmetric keys nor a full PKI based system (trust anchor or CA certificates) for mutual authentication of peers with KARP KMP deployments. Usage of Router Fingerprints give a significant operational improvement from symmetric key based systems and yet provide a secure authentication technique.

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 November 28, 2014.

Copyright Notice

Copyright (c) 2014 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

(<http://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.	Introduction	2
1.1.	Requirements Language	3
1.2.	Acronyms	3
2.	Router Fingerprint	4
3.	Usage of Router Fingerprints with KARP KMP	5
4.	Publishing Router Fingerprints	5
5.	Scope of Fingerprints usage with RPs	6
6.	Fingerprint Revocation	6
7.	IANA Considerations	6
8.	Security Considerations	6
9.	Acknowledgements	7
10.	Appendix A	7
10.1.	Applicable Authentications methods	7
10.1.1.	Symmetric key based authentication	7
10.1.2.	Asymmetric key based authentication	8
10.1.3.	EAP based authentication	8
11.	References	9
11.1.	Normative References	9
11.2.	Informative References	9
	Authors' Addresses	11

[1.](#) Introduction

Usage of IKEv2[RFC5996] as the KMP for with specific extensions for pair wise routing protocols (RPs) is described in [mahesh-karp-rkmp]. Also IKEv2 based KMP for group keying RPs is described in [hartman-karp-mrkmp]. With proliferation of authentication methods supported by IKEv2, this draft explores a simple and secure peer authentication method, which can be potentially used for all KARP KMP deployments.

Currently operators don't often change the manual keys deployed for protecting RP messages because of various reasons as noted in [Section 2.3](#) of KARP threat document [RFC6862]. One of the KARP WG

goals is to define methods to support key changes for all RPs which use either Manual Key Management (MKM) or KMP without much operational overhead.

Apart from Peer's identity verification, authentication and parameter negotiation, deployment of KMP can be more useful, when it comes to rekey the keys used by RPs. Rekeying can be achieved without the operator's intervention and as per the provisioned rekey policy. But for operators, usage of IKEv2 KMP opens up numerous possibilities for peer authentication and manual symmetric keys are not only used for bootstrapping KMP, but used for peer authentication. Various other peer authentication mechanisms with advantages/drawbacks of each mechanism are described in the [Section 10.1](#) of this document.

If symmetric pre-shared keys are used by IKEv2 KMP to authenticate the peer before generating the shared key(s); apart from other issues with symmetric keys, the problem still remain the same when it comes to changing these keys.

To reduce operational costs for changing keys at peering points with relatively large number of RP peers, this document describes the use of one of the available IKEv2 KMP peer authentication methods with raw public keys. The hash of these encoded public keys is called as Router Fingerprints and the authentication method is called Router Fingerprint Authentication (RFA) in rest of the document. The RFA method in conjunction with KARP KMPs require, neither out-of-band symmetric keys nor a fully functional PKI based system with trust anchor certificates as explained further in [Section 2](#).

[Section 2](#) describes the Router Fingerprints in the context of various KMPs and specifically for IKEv2 KMP. Generation and usage of the Router Fingerprints is described in [Section 3](#) and [Section 4](#) describes a reliable method for publishing the Router Fingerprints.

[1.1](#). 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 [RFC 2119](#) [[RFC2119](#)].

[1.2.](#) Acronyms

- CRL - Certificate Revocation List.
- EBGP - External BGP (BGP connection between external peers).
- EE - End Entity.
- IBGP - Internal BGP (BGP connection between internal peers).
- KMP - Key Management Protocol (auto key management).

- MKM - Manual Key management Protocols.
- PAD - Peer Authorization Database.
- RFA - Router Fingerprint Authentication.
- RP - Routing Protocol.

[2.](#) Router Fingerprint

Router Fingerprint is a sequence of bytes used to authenticate the public key before using the same public key to authenticate the peer in the context of KARP KMP.

Various forms of fingerprint mechanisms based on the public keys are already in use as defined in [[RFC4252](#)] and [[RFC4253](#)]. Fingerprints are also used primarily for root key authentication in X.509 based PKI [[RFC5280](#)]. This documents only highlights the usage of raw public key based authentication mechanism already defined in [[RFC5996](#)] for KARP deployments.

To generate a fingerprint:

1. A router needs to generate an asymmetric Private/Public key pair. Asymmetric crypto algorithms based on RSA [[RFC3447](#)] or for shorter and still secure keys Elliptic Curve Cryptography (ECC) [[RFC4492](#)] can be used for generating the Private/Public key pair.
2. Once the Asymmetric key pair is generated, the public key can be

encoded with any additional data (specific to the router or routing instance) and can be in the form of more easily administrable X.509 PKI Certificate profile and to be specific as specified in the SubjectPublicKeyInfo structure in [Section 4.1 of \[RFC5280\]](#). This does not force use of X.509 or full compliance with [\[RFC5280\]](#) since formatting any public key as a SubjectPublicKeyInfo is relatively straightforward and well supported by libraries.

3. The result should be hashed with a cryptographic hash function, preferably SHA-256 or hash functions with similar strength (see more discussion on choosing preferred hash function in [Section 8](#)).

The fingerprint generated is not a secret and can be distributed publicly. This is further discussed in [Section 4](#).

[3](#). Usage of Router Fingerprints with KARP KMP

To use Router Fingerprints authentication with KARP KMP, a Private/Public key-pair MUST be generated by the router as specified in [Section 2](#). To deploy RFA method more widely -

1. type of public keys supported should be generic; for e.g., support for raw Elliptic Curve public keys and
2. more generic encoding formats should be supported for carrying the raw public keys other than currently defined PKCS #1.

[I-D.kivinen-ipsecme-oob-pubkey] enhances support for other types of public keys and also defines new encoding format to carry the public key fingerprint in the CERT payload. For RPs to use Router Fingerprint Authentication in the context of IKEv2 MUST follow the encoding format as specified in [\[I-D.kivinen-ipsecme-oob-pubkey\]](#).

For RFA, the public key received is in the form of SubjectPublicKeyInfo structure of X.509 PKI profile and the Peer Authorization Database (PAD) entry [\[RFC4301\]](#) MUST contain the published fingerprint of the peer.

[4.](#) Publishing Router Fingerprints

The router fingerprint generated is not a secret and can be exchanged out-of-band or can be distributed publicly. Please refer to [Section 5](#) for the generic usage and scope of the RFA in routing environments. In the case of inter-domain routing using EBGp [\[RFC4271\]](#), if the routers are outside of the SIDR [\[I-D.ietf-sidr-bgpsec-overview\]](#) environment, fingerprint can also be exchanged out-of-band through Service Level Agreements (SLAs) at the RP peering points.

[\[RFC6920\]](#) defines a "Named Information" identifier, which provides a set of standard ways to use hash function outputs in names. As there are many ways to publish fingerprints in an unambiguous manner (e.g., as defined in [Section 5 of \[RFC4572\]](#)); on the WG consensus, KARP deployments MUST use the method described in [\[RFC6920\]](#) for interoperability. A KARP KMP deployment using router fingerprints need to resort to out-of-band public key validation procedure to verify authenticity of the keys being used. The router fingerprints MUST be part of the KMP PAD to validate the public key received in the KMP messages.

[5.](#) Scope of Fingerprints usage with RPs

The fingerprint method described in this document in general is more suitable for intra domain deployments. This includes KMP usage for e.g., for IBGP [\[RFC4271\]](#) and LDP [\[RFC5036\]](#) peers, where KARP KMP can be deployed without having to configure either manual pre-shared keys to bootstrap KMP or full PKI with trust anchor certificates. Also KMPs for group keying RPs can use this method for authenticating the peers in the group. This method also can be potentially used between EBGp [\[RFC4271\]](#) speakers outside of the SIDR ([\[I-D.ietf-sidr-bgpsec-overview\]](#)) deployment scope, where full PKI infrastructure is not available to deploy with KARP KMP and at the same time, still operators want to avoid provisioning manual keys.

[6.](#) Fingerprint Revocation

The idea of RFA in the context of KARP KMP is to deploy a better authentication method than the mutually shared symmetric keys between two routers. This SHOULD be used especially where number of peers using this method is relatively smaller and operationally manageable. Any changes in the router fingerprints SHOULD be administered manually by the operator. For e.g., to revoke the compromised key operator simply need to remove the fingerprint from the PAD, which do require and update to the PAD of all possible nodes in the network where this node was talking to. Quite often those configurations are already pushed to routers by some kind of management tool, so it is completely possible to do this quite easily.

When there are a large number of peers, the need for router fingerprint changes may increase. This may be for reasons of key compromises or other potential changes to the routers. In such environments, operators SHOULD look to full PKI with trust anchor certificates and CRL profiles as specified in the [\[RFC5280\]](#). In this context, RFA mechanism should be only seen as substantial improvement from mutually shared manual keying authentication methods.

[7.](#) IANA Considerations

This document defines no new namespaces.

[8.](#) Security Considerations

If collision attacks are perceived as a threat, the hash function to generate the fingerprints MUST also possess the property of collision-resistance. To mitigate preimage attacks, the cryptographic hash function used for a fingerprint MUST possess the property of second preimage resistance.

For deploying RFA authentication method, generated fingerprints MUST not be truncated to make those short as to preserve the relevant properties of the hash function against brute-force search attacks.

Considering the above facts, it's recommended to use SHA-256 or similar hash functions with good security properties to generate the fingerprints.

[9.](#) Acknowledgements

The authors would like to thank Jari Arkko for initial and valuable discussions on operationally simplified authentication methods in general and RFA mechanism as described in this document in particular. Authors would like to acknowledge Joel Halpern for supporting this work and providing continuous feedback on the draft, including the usefulness of this approach in routing environments.

[10.](#) [Appendix A](#)

[10.1.](#) Applicable Authentications methods

One advantage that IKEv2 provides is the largest selection of key management and parameter coordination authentication methods suitable for various environments. The goal of this section is to look at various KMP authentication options available and recommend suitable options for use in negotiating keys and other parameters for routing protocol protection.

As some of the authentication mechanisms are optional in IKEv2, one mandatory authentication mechanism from the list below needs to be selected for routing environments to ensure inter-operability and quicker adoption. This section attempts to summarize the available options and constraints surrounding the options.

[10.1.1.](#) Symmetric key based authentication

IKEv2 [[RFC5996](#)] allows for authentication of the IKEv2 peers using a symmetric pre-shared key. For symmetric pre-shared key peer authentication, deployments need to consider the following as per [[RFC5996](#)]:

1. Deriving a shared secret from a password, name, or other low-entropy source is not secure. These sources are subject to dictionary and social-engineering attacks, among others.
2. The pre-shared key should not be derived solely from a user-chosen password without incorporating another source of randomness.

3. If password-based authentication is used for bootstrapping the

IKE_SA, then one of the EAP methods as described in [Section 10.1.3](#) needs to be used.

One of the IPsecME WG charter goals is to provide IKEv2 [[RFC5996](#)] a secure password authentication mechanism which is protected against off-line dictionary attacks, without requiring the use of certificates or Extensible Authentication Protocol (EAP), even when using the low-entropy shared secrets. There are couple of documents which try to address this issue and the work is still in progress.

[10.1.2](#). Asymmetric key based authentication

Another peer authentication mechanism IKEv2 uses is asymmetric key certificates or public key signatures. This approach relies on a Public Key Infrastructure using X.509 (PKIX) Certificates. If this can be deployed for IKEv2 peer authentication, it will be one of the most secure authentication mechanisms. With this authentication option, there is no need for out-of-band shared keys between peers for mutual authentication.

Apart from RSA and DSS digital signatures for public key authentication provided by IKEv2, [[RFC4754](#)] introduces Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. ECDSA provides additional benefits including computational efficiency, small signature sizes, and minimal bandwidth compared to other available digital signature methods.

[10.1.3](#). EAP based authentication

In addition to supporting authentication using shared secrets and public key signatures, IKEv2 also supports authentication based on the Extensible Authentication Protocol (EAP), defined in [[RFC3748](#)]. EAP is an authentication framework that supports multiple authentication mechanisms. IKEv2 provides EAP authentication because public key signatures and shared secrets are not flexible enough to meet the requirements of many deployment scenarios. For KARP KMP, EAP-Only Authentication in IKEv2 as specified in [[RFC5998](#)] can be explored.

By using EAP, IKEv2 KMP can leverage existing authentication infrastructure and credential databases, because EAP allows users to choose a method suitable for existing credentials. Routing protocols today use password-based pre-shared keys to integrity protect the routing protocol messages. The same pre-shared key can be used to bootstrap the KMP and as a potential authentication key in KMP. With appropriate password based EAP methods, stronger keys can be generated without using certificates.

For authenticating the nodes running routing protocols, EAP and the IKEv2 endpoints are co-located (so no separate EAP server required). When EAP is deployed, authenticating the IKEv2 responder using both EAP and public key signatures could be redundant. EAP methods that offer mutual authentication and key agreement can be used to provide responder authentication in IKEv2 completely based on EAP.

[Section 4 of \[RFC5998\]](#) lists safe EAP methods to support EAP_ONLY_AUTHENTICATION. For routing protocols deployment, because an EAP server is co-located with IKEv2 responder, channel binding capability of the selected EAP method is irrelevant. Various qualified mutual authentication methods are listed in [\[RFC5998\]](#); of these, a password based methods [\[RFC4746\]](#), [\[RFC5931\]](#), [\[RFC6124\]](#) can offer potential EAP alternative for pre-shared key only authentication.

[11.](#) References

[11.1.](#) Normative References

- [I-D.chunduri-karp-using-ikev2-with-tcp-ao]
Chunduri, U., Tian, A., and J. Touch, "A framework for RPs to use IKEv2 KMP", [draft-chunduri-karp-using-ikev2-with-tcp-ao-06](#) (work in progress), February 2014.
- [I-D.kivinen-ipsecme-oob-pubkey]
Kivinen, T., Wouters, P., and H. Tschofenig, "More Raw Public Keys for IKEv2", [draft-kivinen-ipsecme-oob-pubkey-07](#) (work in progress), May 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 5996](#), September 2010.

[11.2.](#) Informative References

- [I-D.hartman-karp-mrkmp]
Hartman, S., Zhang, D., and G. Lebovitz, "Multicast Router Key Management Protocol (MaRK)", [draft-hartman-karp-mrkmp-05](#) (work in progress), September 2012.
- [I-D.ietf-karp-ops-model]
Hartman, S. and D. Zhang, "Operations Model for Router

Keying", [draft-ietf-karp-ops-model-10](#) (work in progress), January 2014.

[I-D.ietf-sidr-bgpsec-overview]

Lepinski, M. and S. Turner, "An Overview of BGPSEC", [draft-ietf-sidr-bgpsec-overview-04](#) (work in progress), December 2013.

[I-D.mahesh-karp-rkmp]

Jethanandani, M., Weis, B., Patel, K., Zhang, D., Hartman, S., Chunduri, U., Tian, A., and J. Touch, "Negotiation for Keying Pairwise Routing Protocols in IKEv2", [draft-mahesh-karp-rkmp-05](#) (work in progress), November 2013.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), February 2003.

[RFC3618] Fenner, B. and D. Meyer, "Multicast Source Discovery Protocol (MSDP)", [RFC 3618](#), October 2003.

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

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", [BCP 107](#), [RFC 4107](#), June 2005.

[RFC4252] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol", [RFC 4252](#), January 2006.

[RFC4253] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol", [RFC 4253](#), January 2006.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", [RFC 4271](#), January 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites

for Transport Layer Security (TLS)", [RFC 4492](#), May 2006.

- [RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", [RFC 4572](#), July 2006.
- [RFC4746] Clancy, T. and W. Arbaugh, "Extensible Authentication Protocol (EAP) Password Authenticated Exchange", [RFC 4746](#), November 2006.

Chunduri, et al.

Expires November 28, 2014

[Page 10]

Internet-Draft KARP KMP: Simplified Peer Authentication

May 2014

- [RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", [RFC 4754](#), January 2007.
- [RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", [RFC 5036](#), October 2007.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 5280](#), May 2008.
- [RFC5440] Vasseur, JP. and JL. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)", [RFC 5440](#), March 2009.
- [RFC5931] Harkins, D. and G. Zorn, "Extensible Authentication Protocol (EAP) Authentication Using Only a Password", [RFC 5931](#), August 2010.
- [RFC5998] Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", [RFC 5998](#), September 2010.
- [RFC6124] Sheffer, Y., Zorn, G., Tschofenig, H., and S. Fluhrer, "An EAP Authentication Method Based on the Encrypted Key Exchange (EKE) Protocol", [RFC 6124](#), February 2011.
- [RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for Routing Protocols (KARP) Design Guidelines", [RFC 6518](#), February 2012.

- [RFC6862] Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", [RFC 6862](#), March 2013.
- [RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", [RFC 6920](#), April 2013.

Authors' Addresses

Chunduri, et al. Expires November 28, 2014 [Page 11]

Internet-Draft KARP KMP: Simplified Peer Authentication May 2014

Uma Chunduri
Ericsson
300 Holger Way
San Jose, California 95134
USA

Phone: +1 (408) 750-5678
Email: uma.chunduri@ericsson.com

Albert Tian
Ericsson
300 Holger Way
San Jose, California 95134
USA

Phone: +1 (408) 750-5210
Email: albert.tian@ericsson.com

Ari Keranen
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: ari.keranen@ericsson.com

Tero Kivinen
INSIDE Secure
Eerikinkatu 28
Helsinki 00180
Finland

Email: kivinen@iki.fi