

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 25, 2010

Y. Sheffer  
Check Point  
March 24, 2010

Password-Based Authentication in IKEv2: Selection Criteria and  
Comparison  
draft-sheffer-ipsecme-pake-criteria-02.txt

## Abstract

The IPsecME working group has been chartered with specifying a new password-based authentication method for IKEv2. This document presents a few solution alternatives, and lists potential criteria for choosing among them. It is not the author's intention to publish this document as an RFC. Moreover, it is more subjective than most IETF documents.

## Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 25, 2010.

## Copyright Notice

Copyright (c) 2010 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 BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Selection Criteria . . . . .	<a href="#">4</a>
<a href="#">3.1.</a>	Security Criteria . . . . .	<a href="#">4</a>
<a href="#">3.2.</a>	Intellectual Property . . . . .	<a href="#">5</a>
<a href="#">3.3.</a>	Other Considerations and Engineering Criteria . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Some Possible Candidates . . . . .	<a href="#">7</a>
<a href="#">5.</a>	Comparison Table . . . . .	<a href="#">7</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">8.</a>	References . . . . .	<a href="#">9</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">9</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">9</a>
<a href="#">Appendix A.</a>	Change Log . . . . .	<a href="#">9</a>
	Author's Address . . . . .	<a href="#">10</a>

## 1. Introduction

The new IPsecME WG charter defines a new work item on password-based authentication for IKEv2. This is a somewhat contentious issue, so the charter is very particular about the requirements. Quoting in full:

IKEv2 supports mutual authentication with a shared secret, but this mechanism is intended for "strong" shared secrets. User-chosen passwords are typically of low entropy and subject to off-line dictionary attacks when used with this mechanism. Thus, [RFC 4306](#) recommends using EAP with public-key based authentication of the responder instead. This approach would be typically used in enterprise remote access VPN scenarios where the VPN gateway does not usually even have the actual passwords for all users, but instead typically communicates with a back-end RADIUS server. However, user-configured shared secrets are still useful for many other IPsec scenarios, such as authentication between two servers or routers. These scenarios are usually symmetric: both peers know the shared secret, no back-end authentication servers are involved, and either peer can initiate an IKEv2 SA. While it would be possible to use EAP in such situations (by having both peers implement both the EAP peer and the EAP server roles of an EAP method intended for "weak" shared secrets) with the mutual EAP-based authentication work item (above), a simpler solution may be desirable in many situations.

The WG will develop a standards-track extension to IKEv2 to allow mutual authentication based on "weak" (low-entropy) shared secrets. The goal is to avoid off-line dictionary attacks without requiring the use of certificates or EAP. There are many already-developed algorithms that can be used, and the WG would need to pick one that both is believed to be secure and is believed to have acceptable intellectual property features. The WG would also need to develop the protocol to use the chosen algorithm in IKEv2 in a secure fashion. It is noted up front that this work item poses a higher chance of failing to be completed than other WG

work items; this is balanced by the very high expected value of the extension if it is standardized and deployed.

The charter defines some properties that a good solution is required to have. For example, despite the fact that EAP is an integral part of IKEv2, there are good reasons to avoid it in this case. But the charter does not name a specific cryptographic protocol on which to base this solution, nor does it mention a specific IETF document as a starting point. This document asserts that several such choices are possible, and attempts to provide the group with some selection criteria, in order to enable a reasoned discussion of these (and possibly other) alternatives.

## [2.](#) Terminology

This document is entirely non-normative. None of the IETF-capitalized words SHOULD be used, and if perchance they are, they MUST be ignored.

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.](#) Selection Criteria

IKEv2 is targeted at applications that require a very high level of security. Therefore, adding a new mode of operation to the protocol can only be done after careful consideration. In this section, I describe some of the criteria we can use to choose between solution candidates. Unfortunately, I am not aware of any potential solution that score a "perfect 10" under these criteria. If this paper encourages the development of new solutions that better fit the criteria, so much the better.

### [3.1.](#) Security Criteria

The primary requirement from a good solution is to have a high level of security. Unfortunately, we all know this property is extremely hard to gauge. But some data might enhance our confidence in a solution's security.

- SEC1: The protocol has good security "best practices", such as crypto agility.
- SEC2: The solution is based on a cryptographic protocol that has been (openly) published some time ago, giving the cryptographic community enough time to have reviewed it. Preferably, it was published in a location where it is more likely to be reviewed, e.g. a peer-reviewed crypto journal.
- SEC3: The protocol has undergone thorough professional analysis. It's best if protocol analyses by prominent cryptographers have been published. If issues were uncovered, we would prefer repeat analysis to have been undertaken on the fixed protocol.
- SEC4: Some modern protocols have been mathematically proven secure under various models. This is an attractive feature of such protocols.

- SEC5: When integrated with IKEv2, the solution should preserve IKE's existing security properties. These include forward secrecy (disclosure of long term credentials, in this case the password, does not expose past sessions), and identity protection in the presence of passive attackers (eavesdroppers).
- SEC6: The solution should be able of generating of a cryptographic-strength credential (either a long key or a certificate) so that the weak credential needs to be used rarely or even only once.

It is noted that some features (such as support for password expiry) and some security criteria (such as resistance to server compromise) are very important for the "teleworker" use case. This document is limited to the use of password-based authentication to achieve trust between gateways, and for this use case, these features and criteria are of questionable value.

The author considers security assurance to be by far the most important criterion. The impact of a security vulnerability discovered late in the process would be extremely severe to the protocol and to deployed implementations.

### 3.2. Intellectual Property

"Intellectual property", a common euphemism for patents, is a complex issue. The existence of patents covering a specific technology is often an important consideration for vendors, and critical for open source implementers. Despite this fact, the IETF does not provide its constituency with any legal guidance or assistance in this matter.

Unfortunately, the specific area of password-based authentication is riddled with patents. This has hampered the IETF adoption of this technology for years, and caused at least one working group to fail. As a result, we (as individual implementers and as a working group) need to understand as best we can the IPR status of each proposal.

Disclaimer: I am not a lawyer, and this document should not be construed as legal advice.

IETF rules require that any participant who's aware of a patent relevant to an IETF work item should disclose the patent's existence. In practice, such disclosures are often submitted very late in the process, resulting in a long period when a document's IPR status remains unclear. Even more worryingly, filing an IPR statement against another person's technology carries no cost: in at least one case I am aware of, a company filed an IPR statement for a

competitive technology asserting their own patent, even though the technology is in fact covered by another patent, making it very likely that the company's patent does not apply to the technology. Given this background, I propose the following as selection criteria:

- IPR1: Ideally, the proposal should be unencumbered. This property is very difficult to prove, and each WG participant should attempt to review the applicable patents and determine whether in fact they do not apply to the proposal. Remember that independently invented technology might still infringe a patent.
- IPR2: In some cases the IPR situation is clear: if the protocol relies on a specific patent, and believed to not require the use of any other. This is mostly useful if the patent's licensing terms (whether free or not) are known, and/or the

patent's expiration date is near.

IPR3: Many IETF participants, and the IETF as an organization, quite naturally prefer freely licensed technology to non-free licensing terms.

Given the number and quality of encumbered protocols in this space, IPR is one area where the group might have to compromise.

### 3.3. Other Considerations and Engineering Criteria

Several additional criteria may be just as important:

- MISC1: Protocols that have been specified within standards documents should be preferred over protocols that are only described in scientific papers. Such description is typically insufficient to provide interoperability, and may not be sufficient for a thorough security analysis.
- MISC2: Likewise, cryptographic protocols that have been integrated into the IKE framework have an advantage over those described only within other security protocols.
- MISC3: The protocol should make a good fit into the minimal IPsec/IKE architecture, e.g. it should not assume a trusted third party or tight clock synchronization.
- MISC4: It is advantageous if the same algorithms and where applicable, the same Diffie-Hellman groups can be used for IKE itself and for the authentication protocol. This can simplify the implementation and eliminate spurious negotiation.
- MISC5: Performance, measured primarily by the number of round trips and number of exponentiations. Performance should remain reasonable even if the "password" is a long octet string.

- MISC6: The solution should accommodate algorithm agility relative to IKE cryptographic algorithms, e.g., transition to elliptic curve key agreement.
- MISC7: The solution must support localization of identities and passwords. In general, the scheme must support arbitrary octet strings as the input, so that any current and future character encoding can be supported.
- MISC8: Similarly, the scheme must support arbitrary octet strings as

input, so that it can be used to "boost" shared secrets that have been generated using weak methods, e.g. not-quite-random RNGs.

MISC9: The always valid, but always vague "ease of implementation".

#### [4.](#) Some Possible Candidates

This section provides background regarding some of the candidate protocols. Some pertinent properties are mentioned, but this is by no means an analysis against the criteria defined above.

1. EKE is the oldest password-authenticated key exchange (PAKE) protocol still considered secure, although some of its variants have been broken. It is covered by a patent, due to expire in late 2011.
2. SPSK (a.k.a. EAP-PWD) is a relatively new mechanism. It has been standardized within IEEE 802.11s.
3. PAK is the earliest provably-secure mechanism. A protocol description has been standardized within the IETF, but no other IETF PAK-based protocol exists. PAK is patented (IPR statement #1179).
4. SRP has been deployed in multiple products. It is described by several IETF documents, including a TLS-SRP variant. SRP is patented, and can be used under a royalty-free license (IPR statement #31, as well as additional IPR statements filed by other parties).

In addition, applicable standards to be consulted for these and additional protocols include:

- o IEEE P1363.2, Specifications for Password based Public Key Cryptographic Techniques.
- o ISO/IEC 11770-4:2006 Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets.

#### [5.](#) Comparison Table

This is a very rough attempt at a comparative analysis. Many of the

Sheffer	Expires September 25, 2010	[Page 7]
---------	----------------------------	----------

---

Internet-Draft	Password Based Authentication in IKEv2	March 2010
----------------	--	------------

details are incomplete, and/or controversial.



Name	Security Standards	Security Analysis	IPR
EKE	<a href="#">[I-D.sheffer-emu-eap-eke]</a> , <a href="#">[I-D.sheffer-ipsecme-hush]</a>	Well analyzed security, since 1992, several analysis papers published.	Patent filed 1992 (now owned by Lucent), due to expire Oct. 2011.
SRP	SRP published as <a href="#">[RFC2945]</a> , TLS-SRP is <a href="#">[RFC5054]</a> . IEEE 1363.2, ISO IEC 11770-4.	Published and unpublished analysis by Bleichenbacher.	Patent held by Stanford University, with a free license. Phoenix posted an IPR statement, but no request for reexamination.
SPSK	<a href="#">[I-D.harkins-emu-eap-pwd]</a> , <a href="#">[I-D.harkins-ipsecme-spsk-auth]</a> .	Security analysis by NIST cryptographers.	Explicitly not patented.
SPEKE	IEEE 1363.2 and ISO IEC 11770-4.	[To be completed]	Patents held by Phoenix.
PAK	Published as <a href="#">[RFC5683]</a> . IEEE 1363.2.	See <a href="#">[RFC5683]</a>	Patents held by Lucent.

## 6. IANA Considerations

This document does not require any action by IANA.

## 7. Security Considerations

This document does not define any new protocol, and has no inherent security considerations. It does discuss criteria for the selection of a security protocol, chief among them being security.

## [8.](#) References

### [8.1.](#) Normative References

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

### [8.2.](#) Informative References

- [I-D.harkins-emu-eap-pwd]  
Harkins, D. and G. Zorn, "EAP Authentication Using Only A Password", [draft-harkins-emu-eap-pwd-13](#) (work in progress), February 2010.
- [I-D.harkins-ipsecme-spsk-auth]  
Harkins, D., "Secure PSK Authentication for IKE", [draft-harkins-ipsecme-spsk-auth-01](#) (work in progress), March 2010.
- [I-D.sheffer-emu-eap-eke]  
Sheffer, Y., Zorn, G., Tschofenig, H., and S. Fluhrer, "An EAP Authentication Method Based on the EKE Protocol", [draft-sheffer-emu-eap-eke-05](#) (work in progress), March 2010.
- [I-D.sheffer-ipsecme-hush]  
Sheffer, Y. and S. Fluhrer, "HUSH: Using HUmanly memorable SHared secrets with IKEv2", [draft-sheffer-ipsecme-hush-00](#) (work in progress), March 2010.
- [RFC2945] Wu, T., "The SRP Authentication and Key Exchange System", [RFC 2945](#), September 2000.
- [RFC5054] Taylor, D., Wu, T., Mavrogiannopoulos, N., and T. Perrin, "Using the Secure Remote Password (SRP) Protocol for TLS Authentication", [RFC 5054](#), November 2007.
- [RFC5683] Brusilovsky, A., Faynberg, I., Zeltsan, Z., and S. Patel, "Password-Authenticated Key (PAK) Diffie-Hellman Exchange", [RFC 5683](#), February 2010.

## [Appendix A.](#) Change Log

### [A.1.](#) -02

Yet more criteria after the discussion in Anaheim and on the list.

Sheffer

Expires September 25, 2010

[Page 9]

---

Internet-Draft Password Based Authentication in IKEv2

March 2010

[A.2.](#) -01

Added some criteria after mailing list review.

[A.3.](#) [draft-sheffer-ipsecme-pake-criteria-00](#)

Initial version.

Author's Address

Yaron Sheffer  
Check Point Software Technologies Ltd.  
5 Hasolelim St.  
Tel Aviv 67897  
Israel

Email: [yaronf.ietf@gmail.com](mailto:yaronf.ietf@gmail.com)

