

Sakai-Kasahara Key Encryption (SAKKE)

RFC 6508

Status (/doc/rfc6508/)	IESG evaluation record (/doc/rfc6508/ballot/)	IESG writeups (/doc/rfc6508/writeup/)
Email expansions (/doc/rfc6508/email/)	History (/doc/rfc6508/history/)	

Versions 03 (/doc/draft-groves-sakke/)



Document	Type	RFC - Informational (February 2012; No errata) Was draft-groves-sakke (/doc/draft-groves-sakke/) (individual in sec area)	
	Last updated	2015-10-14	
	Stream	IETF	
	Formats	<div>plain text (https://www.rfc-editor.org/rfc/rfc6508.txt)</div> <div>pdf (https://www.rfc-editor.org/rfc/pdf/rfc6508.txt.pdf)</div> <div>html (https://tools.ietf.org/html/rfc6508)</div> <div>bibtex (bibtex)</div>	
	Reviews	SECDIR Last Call Review (/doc/review-groves-sakke-secdir-lc-atkins-2011-02-02/)	

Stream	WG state	(None)
	(/help/state/draft/ietf)	
	Document shepherd	No shepherd assigned

IESG	IESG state	RFC 6508 (Informational)
	(/help/state/draft/iesg)	
	Consensus Boilerplate	Unknown
	Telechat date	
	Responsible AD	Sean Turner
	IESG note	Tim Polk (tim.polk@nist.gov) is the shepherd.
	Send notices to	tim.polk@nist.gov

Email authors (mailto:draft-groves-sakke@ietf.org?subject=Mail%20regarding%20draft-groves-sakke)

IPR (/ipr/search/?submit=draft&id=draft-groves-sakke)

← References (/doc/rfc6508/references/)

→ Referenced by (/doc/rfc6508/referencedby/)

! Nits (https://www.ietf.org/tools/idnits?url=https://www.ietf.org/archive/id/draft-groves-sakke-03.txt)

Q Search lists ▾

Internet Engineering Task Force (IETF)
Request for Comments: 6508
Category: Informational
ISSN: 2070-1721

M. Groves
CESG
February 2012

Sakai-Kasahara Key Encryption (SAKKE)

Abstract

In this document, the Sakai-Kasahara Key Encryption (SAKKE) algorithm is described. This uses Identity-Based Encryption to exchange a shared secret from a Sender to a Receiver.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6508>.

Copyright Notice

Copyright (c) 2012 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.

Groves
RFC 6508

Informational
SAKKE

[Page 1]
February 2012

Table of Contents

1. Introduction	2
1.1. Requirements Terminology	3
2. Notation and Definitions	3
2.1. Notation	3
2.2. Definitions	5
2.3. Parameters to Be Defined or Negotiated	6
3. Elliptic Curves and Pairings	7
3.1. $E(F_p^2)$ and the Distortion Map	7
3.2. The Tate-Lichtenbaum Pairing	7
4. Representation of Values	9
5. Supporting Algorithms	10
5.1. Hashing to an Integer Range	10
6. The SAKKE Cryptosystem	11
6.1. Setup	11
6.1.1. Secret Key Extraction	11
6.1.2. User Provisioning	11
6.2. Key Exchange	12
6.2.1. Sender	12
6.2.2. Receiver	12
6.3. Group Communications	13
7. Security Considerations	13
8. References	15
8.1. Normative References	15
8.2. Informative References	15
Appendix A. Test Data.....	17

1. Introduction

This document defines an efficient use of Identity-Based Encryption (IBE) based on bilinear pairings. The Sakai-Kasahara IBE cryptosystem [S-K] is described for establishment of a shared secret value. This document adds to the IBE options available in [RFC5091], providing an efficient primitive and an additional family of curves.

This document is restricted to a particular family of curves (see Section 2.1) that have the benefit of a simple and efficient method of calculating the pairing on which the Sakai-Kasahara IBE cryptosystem is based.

IBE schemes allow public and private keys to be derived from Identifiers. In fact, the Identifier can itself be viewed as corresponding to a public key or certificate in a traditional public key system. However, in IBE, the Identifier can be formed by both

Sender and Receiver, which obviates the necessity of providing public keys through a third party or of transmitting certified public keys

Groves
RFC 6508

Informational
SAKKE

[Page 2]
February 2012

during each session establishment. Furthermore, in an IBE system,

▼ Show full document text (?include_text=1)

ISOC (<https://www.internetsociety.org/>)

IETF Trust (<https://trustee.ietf.org/>)

RFC Editor (<https://www.rfc-editor.org/>)

IRTF

(<https://www.irtf.org/>)

IESG (<https://www.ietf.org/iesg/>)

IETF (<https://www.ietf.org/>)



IAB (<https://www.iab.org/>)

IASA & IAOC

(<https://iaoc.ietf.org/>)

IETF Tools (<https://tools.ietf.org/>)

IANA (<https://www.iana.org/>)

About (</release/about>) | IETF Datatracker | Version 6.86.0.p1 (</release/6.86.0.p1>) | 2018-10-08 | Report a bug: Tracker:  (<https://tools.ietf.org/tools/ietfdb/newticket>) Email:  (<mailto:datatracker-project@ietf.org>)

Python 2.7.13 | Django 1.11.16