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/)

draft-groves-sakke
rfc6508
00
01
02
Jun 2010
Feb 2011
Apr 2011

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	plain text (https://www.rfc-editor.org/rfc/rfc6508.txt) pdf (https://www.rfc-editor.org/rfc/pdfrfc/rfc6508.txt.pdf) html (https://tools.ietf.org/html/rfc6508) bibtex (bibtex)
	Reviews	SECDIR Last Call Review (/doc/review-groves-sakke-secdir-lc-atkins-2011-02-02/)
Stream	**WG state (/help/state/draft/ietf)**	(None)
	Document shepherd	No shepherd assigned
IESG	**IESG state (/help/state/draft/iesg)**	RFC 6508 (Informational)
	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) 🔍 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

Table of Contents

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                       Informational                      [Page 2]
RFC 6508                         SAKKE                     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/)