

## Добавление расширенных порядковых номеров (ESN) в области интерпретации IPsec (DOI) для протокола управления защитными связями и ключами (ISAKMP)

### Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)

#### Статус документа

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Допускается свободное распространение документа.

#### Авторские права

Copyright (C) The Internet Society (2005).

#### Тезисы

Протоколы AH<sup>1</sup> и ESP<sup>2</sup> используют порядковые номера для детектирования попыток повторного использования пакетов. В этом документе описано расширение области интерпретации (DOI<sup>3</sup>) для протокола управления защищенными связями и ключами (ISAKMP<sup>4</sup>). Это расширение поддерживает согласование использования традиционных 32-битовых порядковых номеров или расширенных (64 бита) порядковых номеров (ESN<sup>5</sup>) для конкретной защищенной связи AH или ESP.

## 1. Введение

Спецификации протоколов AH [AH] и ESP [ESP] описывают опцию использования расширенных (64 бита) порядковых номеров. Эта опция обеспечивает возможность передачи очень больших объемов данных с высокими скоростями через защищенные связи (SA) без смены ключей, связанной с исчерпанием пространства порядковых номеров. В этом документе описано дополнение к IPsec DOI для ISAKMP [DOI], которое требуется для поддержки согласования опции ESN.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [Bra97].

## 2. Атрибут SA

Описанный здесь атрибут SA используется во второй фазе (Phase II) согласования протокола IKE<sup>6</sup>. Атрибут относится к базовому типу - Basic (B). Кодирование этого атрибута определено в базовой спецификации ISAKMP [ISAKMP]. Атрибуты, описанные в качестве базовых, **недопустимо** кодировать, как переменные. Более подробное описание кодирования атрибута в IPsec DOI приведено в документе [IKE]. Все ограничения, перечисленные в [IKE], применимы к IPsec DOI и настоящему дополнению.

#### Тип атрибута

Класс	Значение	Тип
Extended (64-bit) Sequence Number	11	B

#### Значения класса

Этот класс показывает, что защищенная связь SA будет использовать 64-битовые порядковые номера (описание расширенных порядковых номеров содержится в документах [AH] и [ESP]).

Резерв	0
64-битовый порядковый номер	1

<sup>1</sup>Authentication Header — заголовок идентификации.

<sup>2</sup>Encapsulating Security Payload — инкапсуляция защищенных данных.

<sup>3</sup>Internet IP Security Domain of Interpretation — область интерпретации защиты IP.

<sup>4</sup>Internet Security Association and Key Management Protocol — протокол управления защищенными связями и ключами в Internet.

<sup>5</sup>Extended Sequence Number.

<sup>6</sup>Internet Key Exchange - протокол обмена ключами.

### 3. Согласование атрибута

Если реализация получает определенный атрибут IPsec DOI (или значение атрибута), который не поддерживается, **следует** передать сигнал ATTRIBUTES-NOT-SUPPORT, а организация защищенной связи **должна** быть прервана.

Если реализация получает любое значение атрибута, отличное от значений для 64-битовой нумерации, организация защищенной связи **должна** быть прервана.

### 4. Вопросы безопасности

Этот документ связан с протоколом обмена ключами [IKE], который объединяет ISAKMP [ISAKMP] и Окли [OAKLEY] для распространения криптографических ключей с обеспечением защиты и идентификации сторон. Обсуждение различных протоколов защиты и преобразований, описанных в этом документе, можно найти в упомянутых ниже базовых документах и документах по шифрованию.

Добавление атрибута ESN не меняет параметров безопасности IKE. При использовании ESN с протоколом ESP важно выбрать режим шифрования, который обеспечит достаточную защиту при шифровании очень большого объема данных с использованием одного ключа. В этом смысле такие алгоритмы, как DES<sup>1</sup> в режиме CBC<sup>2</sup> **не** подходит для использования с ESN, поскольку с использованием одного ключа DES не следует шифровать более 2<sup>32</sup> блоков в таком режиме. Аналогично, с протоколами ESP и AH следует использовать алгоритмы контроля целостности, обеспечивающие должную защиту при больших объемах передаваемой информации. Во избежание возможных проблем с защитой, порождаемых ограничениями алгоритмов, время жизни SA можно ограничивать по объему информации, защищаемой с использованием одного ключа, до того, как будет достигнут предел ESN в 2<sup>64</sup> пакетов.

### 5. Согласование с IANA

В этом документе задано «магическое» число, поддерживаемое IANA. Для этого атрибута не выделяется дополнительных значений. Агентство IANA выделило значение IPsec Security Attribute для Attribute Type (тип атрибута). Это значение указано в колонке «Значение» таблицы раздела 2.

### Благодарности

Автор благодарит членов рабочей группы IPsec. Автор также признателен Karen Seo за помощь при редактировании этой спецификации.

### Нормативные документы

[Bra97] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119<sup>3</sup>, March 1997.

[AH] Kent, S., "IP Authentication Header", RFC 4302<sup>3</sup>, December 2005.

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407<sup>4</sup>, November 1998.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303<sup>3</sup>, December 2005.

[IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409<sup>4</sup>, November 1998.

[ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408<sup>4</sup>, November 1998.

### Дополнительная литература

[OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

### Адрес автора

Stephen Kent

BBN Technologies

10 Moulton Street

Cambridge, MA 02138

USA

Phone: +1 (617) 873-3988

E-Mail: [kent@bn.com](mailto:kent@bn.com)

### Перевод на русский язык

Николай Малых

[nmalykh@protocols.ru](mailto:nmalykh@protocols.ru)

### Полное заявление авторских прав

Copyright (C) The Internet Society (2005).

<sup>1</sup>Data Encryption Standard — стандарт шифрования данных.

<sup>2</sup>Cipher Block Chaining — сцепка шифрованных блоков.

<sup>3</sup>Перевод этого документа имеется на сайте [www.protocols.ru](http://www.protocols.ru). Прим. перев.

<sup>4</sup>В настоящее время этот документ утратил силу и заменен RFC 4306. Прим. перев.

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### **Интеллектуальная собственность**

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

#### **Подтверждение**

Финансирование функций RFC Editor обеспечено Internet Society.