Internet Engineering Task Force (IETF)
Request for Comments: 8209
Updates: 6487
Category: Standards Track
ISSN: 2070-1721

M. Reynolds
IPSw
S. Turner
sn3rd
S. Kent
BBN

September 2017

Профиль для сертификатов маршрутизаторов BGPsec, списков отзыва и запросов сертификатов

A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests

Тезисы

Этот документ определяет стандартный профиль для сертификатов X.509, используемых для обеспечения возможности проверки путей AS[1] в протоколе BGP[2], с помощью расширения, названного BGPsec. BGP является стандартным протоколом междоменной маршрутизации в Internet, собирая, по сути дела, Internet в единое целое. Расширение BGPsec было разработано, как одна из компонент решения по обеспечению защиты BGP. Целью BGPsec является обеспечение полной проверки пути AS на основе использования строгих криптографических примитивов. Сертификаты конечных элементов (EE[3]), задаваемые этим профилем, выпускаются для маршрутизаторов внутри AS. Каждый из таких сертификатов выпускается с сертификатом удостоверяющего центра (УЦ или CA[4]) инфраструктуры открытых ключей ресурсов (RPKI[5]). Сертификаты УЦ и EE содержат расширение AS Resource. Сертификат EE этого типа подтверждает, что маршрутизатор или маршрутизаторы, владеющие соответствующим секретным ключом (private key), уполномочены выпускать защищенные анонсы маршрутов от имени AS, указанных в сертификате. В этом документе описан также профиль формата запросов сертификата и заданы процедуры проверки пути сертификации зависимыми сторонами (RP[6]) для этих сертификатов EE. Данный документ расширяет RPKI и, следовательно, служит обновлением профиля RPKI Resource Certificates Profile (RFC 6487).

Статус документа

Этот документ является проектом стандарта (Internet Standards Track).

Документ является результатом работы IETF[7] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[8]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке https://www.rfc-editor.org/info/rfc8209.

Оглавление

[1]Autonomous System — автономная система.
[2]Border Gateway Protocol — протокол граничного шлюза.
[3]End entity.
[4]Certification Authority — орган сертификации.
[5]Resource Public Key Infrastructure.
[6]Relying Party — зависимая сторона.
[7]Internet Engineering Task Force.
[8]Internet Engineering Steering Group.

1. Введение

Этот документ определяет профиль для сертификатов X.509 конечных элементов (EE) [RFC5280] с целью использования в контексте сертификации путей AS в протоколе BGPsec. Эти сертификаты получили название BGPsec Router Certificate (сертификат маршрутизатора BGPsec). Держатель секретного ключа, связанного с BGPsec Router Certificate, уполномочен передавать защищенные анонсы маршрутов (BGPsec UPDATE) от имени автономных систем, указанных в сертификате. Маршрутизатор, владеющий секретным ключом, уполномочен передавать (своим партнерам) защищенные анонсы маршрутов, указывающие номер автономной системы маршрутизатора (ASN[1]) в качестве источника анонсов. Обеспечиваемые BGPsec свойства (владение ключом) позволяют каждой AS на пути AS убедиться в том, что другие AS на этом пути уполномочены анонсировать данный маршрут (в следующую AS на пути AS).

Этот документ основан на [RFC6487], а тот, в свою очередь, - на [RFC5280]. Документ служит обновлением для [RFC6487]. Он устанавливает требования, предъявляемые к Resource Certificate, используемому в качестве BGPsec Router Certificate, т. е. задает ограничения для полей сертификата и расширения, приемлемые в этом контексте. Документ также описывает запросы, используемые для приобретения BGPsec Router Certificate. Кроме того, документ задает для этих сертификатов процедуру проверки пути сертификации Relying Party (RP).

1.1. Терминология

Предполагается знакомство читателя с терминами и концепциями, описанными в A Profile for X.509 PKIX Resource Certificates [RFC6487], BGPsec Protocol Specification [RFC8205], A Border Gateway Protocol 4 (BGP-4) [RFC4271], BGP Security Vulnerabilities Analysis [RFC4272], Considerations in Validating the Path in BGP [RFC5123] и Capabilities Advertisement with BGP-4 [RFC5492].

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

2. Описание ресурсов в сертификатах

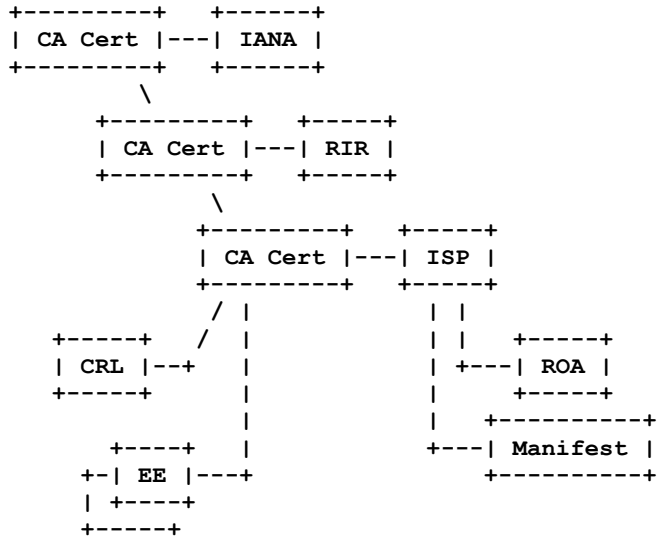

Рисунок 1

На рисунке 1 показаны некоторые элементы инфраструктуры открытых ключей ресурсов (RPKI), а также некоторые объекты, генерируемые RPKI элементами. Агентство IANA выпускает сертификат удостоверяющего центра (CA) для каждого регионального регистратора RIR[2]. В свою очередь RIR выпускает сертификаты CA для провайдеров (ISP[3]). ISP выпускают сертификаты EE для себя, чтобы обеспечить возможность проверки подписей объектов RPKI. CA также создают списки отзыва сертификатов (CRL[4]). Эти сертификаты CA и EE называют сертификатами ресурсов, для них используются профили [RFC6487]. [RFC6480] предусматривает использование сертификатов ресурсов для

[1]AS number.
[2]Regional Internet Registry.
[3]Internet Service Provider.
[4]Certificate Revocation List.

обеспечения проверки манифестов [RFC6486] и полномочий источника маршрута (ROA[1]) [RFC6482]. ROA и манифесты включают сертификаты ресурсов, используемые для их проверки.

В этот документе определяется другой тип сертификата ресурса, названный сертификатом маршрутизатора BGPsec. Цель введения этих сертификатов описана в разделе 1 и попадает в область действия, определенную в [RFC6484]. Введение сертификатов BGPsec Router оказывает минимальное влияние на RPKI CA, поскольку профильсертификатов RPKI CA и CRL не изменяется (т. е. соответствует заданному в [RFC6487]). Кроме того, алгоритмы, используемые для генерации сертификатов RPKI CA, которые служат для эмиссии сертификатов BGPsec Router и CRL, которые требуются для проверки пригодности сертификатов BGPsec Router, остаются неизменными (т. е. соответствуют спецификации [RFC7935]). Единственное влияние заключается в том, что от RPKI CA требуется возможность обработки профилированных запросов сертификатов (см. параграф 3.2), подписанных с использованием алгоритмов [RFC8208]. Сертификаты BGPsec Router используются лишь для проверки подписи в запросе сертификата BGPsec (их обрабатывают только CA) и подписи в сообщениях BGPsec UPDATE [RFC8205] (их обрабатывают только маршрутизаторы BGPsec). Сертификаты BGPsec Router не применяются для обработки манифестов и ROA, а также для проверки подписей в сертификатах и CRL.

В этом документе перечислены лишь различия между данным профилем и [RFC6487]. Отметим, что сертификаты BGPsec Router являются сертификатами EE и поэтому не влияют на процедуру смены алгоритма, описанную в [RFC6916].

3. Обновления RFC 6487

3.1. Поля сертификата BGPsec Router

Сертификат BGPsec Router согласуется с профилем [RFC6487] с учетом изменений, приведенных в этом разделе. Таким образом, это приемлемый сертификат открытого ключа X.509, соответствующий профилю PKIX [RFC5280]. Различия между этим профилем и профилем [RFC6487] указаны в этом разделе.

3.1.1. Subject

Поддерживаемыми вариантами представления общего имени (common name) являются printableString и UTF8String. Для сертификатов BGPsec Router **рекомендуется** в качестве общего имени применять строку «ROUTER-», за которой следует 32-битовое значение ASN [RFC3779], представленное восемью 16-ричными цифрами, а в качестве атрибута порядкового номера — 32-битовое значение BGP Identifier [RFC4271] (т. е. ID) в форме восьми 16-ричных цифр. Если имеется не один номер ASN, выбор включаемого в общее имя значения отдается на откуп эмитенту (Issuer). Если один и тот же сертификат выпускается для множества маршрутизаторов (и, следовательно, все эти маршрутизаторы используют общий секретный ключ), выбор значения ID, используемого в общем имени также определяет эмитент.

3.1.2. Subject Public Key Info

См. параграф 3.1 в [RFC8208].

3.1.3. Поля расширений BGPsec Router Certificate версии 3

3.1.3.1. Базовые ограничения

Узлы BGPsec являются конечными элементами (EE), следовательно, расширение Basic Constraints присутствовать не должно, как указано в [RFC6487].

3.1.3.2. Расширение EKU

Сертификаты BGPsec Router **должны** включать расширение EKU[2]. Как указано в [RFC6487], это расширение не должно обозначаться критическим. Данный документ определяет одно расширение EKU для сертификатов BGPsec Router.

```
id-kp OBJECT IDENTIFIER ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) kp(3) }

id-kp-bgpsec-router OBJECT IDENTIFIER ::= { id-kp 30 }
```

Маршрутизатор BGPsec **должен** требовать наличия расширения EKU в полученном сертификате BGPsec Router. При наличии множества значений KeyPurposeId маршрутизатору BGPsec не требуется распознавать все эти значения, если присутствует требуемое значение KeyPurposeId. Маршрутизаторы BGPsec **должны** отвергать сертификаты без расширения BGPsec Router EKU даже при наличии в них anyExtendedKeyUsage OID, определенного в [RFC5280].

3.1.3.3. Subject Information Access

Это расширение не применяется в сертификатах BGPsec Router и **должно** быть опущено.

3.1.3.4. IP Resources

Это расширение не применяется в сертификатах BGPsec Router и **должно** быть опущено.

3.1.3.5. AS Resources

Кажый сертификат BGPsec Router **должен** включать расширение AS Resources в соответствии с параграфом 4.8.11 [RFC6487]. Расширение AS Resources **должно** включать один или множество номеров ASN, а задание «наследуемых» элементов **недопустимо**.

3.2. Профиль запроса сертификата BGPsec Router

Соответствует разделу 6 в [RFC6487]. Различия между данным профилем и [RFC6487] перечислены ниже.

[1]Route Origin Authorization.
[2]Extended Key Usage — расширенное использование ключа

- Расширение Basic Constraints.

  При наличии этого расширения CA **недопустимо** принимать во внимание установленное значение cA = TRUE.

- Расширение EKU.

  При наличии этого расширения **должно** присутствовать id-kp-bgpsec-router (см. параграф 3.1.3.2), а CA **должен** выполнять запрос для id-kp-bgpsec-router.

- Расширение SIA[1].

  При наличии этого расширения CA **недопустимо** выполнять запрос на включение расширения.

- Поле SubjectPublicKeyInfo задано в [RFC8208].

- Запрос подписывается по алгоритму, заданному в [RFC8208].

3.3. Проверка пригодности сертификата BGPsec Router

Проверка пригодности сертификатов BGPsec Router идентичная процедуре валидации, описанной в разделе 7 [RFC6487] (и всех RFC, обновляющих эту процедуру), с перечисленными ниже изменениями. Например, на этапе 3 (критерий, указанный в параграфе 7.2 [RFC6487]) слова «сертификат содержит все поля, которые **должны** присутствовать» относятся к полям, требуемым этой спецификацией.

Ниже перечислены различия:

- сертификаты BGPsec Router **должны** включать расширение BGPsec Router EKU, определенное в параграфе 3.1.3.2;

- в сертификаты BGPsec Router **недопустимо** включать расширение SIA;

- в сертификаты BGPsec Router **недопустимо** включать расширение IP Resources;

- сертификаты BGPsec Router **должны** включать расширение AS Resources;

- сертификаты BGPsec Router **должны** включать поле subjectPublicKeyInfo, описанное в [RFC8208].

  Примечание. BGPsec RP будут требоваться для поддержки алгоритмов [RFC8208], которые используются для проверки пригодности подписей BGPsec, а также алгоритмов [RFC7935], которые требуются для проверки пригодности подписей сертификатов BGPsec, сертификатов RPKI CA и списков отзыва RPKI CRL.

3.4. Сертификаты маршрутизаторов и функции подписи в RPKI

Как указано в разделе 1, основное применение сертификатов BGPsec Router в RPKI происходит в контексте сертификации путей AS в протоколе BGPsec.

Секретный ключ, связанные с сертификатом EE маршрутизатора, может использоваться многократно для генерации подписей во множестве экземпляров Signature Segment атрибута BGPsec_PATH [RFC8205]. Т. е. сертификат BGPsec Router используется для проверки пригодности множества подписей.

Сертификаты BGPsec Router сохраняются в репозитории CA-эмитента и репозитории, соответствующие [RFC6481], **должны** использовать для сертификатов файлы с расширением имени .cer.

4. Замечания по устройству

Профиль сертификатов BGPsec Router основан на профиле Resource Certificate, определенном в [RFC6487]. В результате многие из описанных здесь вариантов выбора являются отражением выбора, сделанного в предшествующей работе. Для более полного понимания вариантов выбора читателю рекомендуется обратиться к [RFC6484].

Удостоверяющие центры CA требуются политикой сертификации (CP[2]) [RFC6484] для выпуска подобающим образом сформированных сертификатов BGPsec Router независимо от того, что присутствует в запросе сертификата, обеспечивая этим запросам некоторую гибкость.

- Сертификаты BGPsec Router всегда являются сертификатами EE, следовательно, запрос на выпуск сертификата CA приводит к выпуску сертификата EE;

- Сертификаты BGPsec Router всегда являются сертификатами EE, следовательно, запрос для расширения Key Usage значений keyCertSign и cRLSign будет выдавать сертификаты без обоих значений;

- Сертификаты BGPsec Router всегда включают значение BGPsec Router EKU, следовательно, запросы без этого значения будут возвращать сертификаты со значением;

- Сертификаты BGPsec Router никогда не включают расширение SIA, следовательно, запросы сертификата с таким расширением будут возвращать сертификаты без расширения.

Отметим, что такое поведение аналогично включению удостоверяющим центром CA расширения AS Resources в выпускаемые сертификаты BGPsec Router, несмотря на то, что это расширение не указано в запросах.

5. Вопросы реализации

Этот документ разрешает оператору включать список ASN в сертификат BGPsec Router. В данном случае сертификат маршрутизатора станет неприемлемым если любой из номеров ASN удаляется из сертификата любого «вышестоящего» (superior) CA на пути к доверенной привязке. Операторы могут предотвратить такую возможность,

[1]Subject Information Access — доступ к информации субъекта.
[2]Certificate Policy.

выпуская свой сертификат BGPsec Router для каждого отличающегося номера ASN так, что сертификаты маршрутизаторов для ASN, сохранившихся в вышестоящем CA, будут сохраняться действующими.

6. Вопросы безопасности

Для данного документа применимы вопросы безопасности, рассмотренные в [RFC6487].

Сертификат BGPsec Router не пройдет проверку пригодности RPKI, определенную в [RFC6487] по причине использования разных криптографических алгоритмов. Следовательно, RP требуется идентифицировать EKU для определения подходящего ограничения Validation.

Сертификат BGPsec Router является расширением RPKI [RFC6480] для работы с маршрутизаторами. Он является основой построения BGPsec и применяется для проверки пригодности подписей происхождения BGPsec Signature Segment в подписанных сегментах пути [RFC8205]. Таким образом, его важной защитной функцией является защищенная привязка одного или множества номеров ASN к открытому ключу, согласованная с иерархией выделения/присваивания RPKI.

Функции хэширования [RFC8208] применяются при генерации двух расширений идентификаторов ключей (т. е. Subject Key Identifier и Issuer Key Identifier), включаемых в сертификаты BGPsec. Однако, как отмечено в [RFC6818], устойчивость к коллизиям не является требуемым свойством односторонних хэш-функций при их использовании для генерации идентификаторов ключей. Несмотря на то, что коллизии возникают редко, они остаются возможными и оператора следует предупреждать о возникновении такого конфликта. Коллизия значений Subject Key Identifier может приводить к выбору из кэша неподходящего сертификата и последующему отказу при проверке подписи.

7. Согласование с IANA

Этот документ использует два значения OID из реестра SMI для PKIX. Одно значение служит для модуля ASN.1 [X680] [X690] в Приложении A и берется из реестра IANA «SMI Security for PKIX Module Identifier» (id-mod-bgpsec-eku). Другое применяется для BGPsec Router EKU, определенного в параграфе 3.1.3.2 и Приложении A и берется из реестра IANA «SMI Security for PKIX Extended Key Purpose» (id-kp-bgpsec-router). Эти значения OID были выделены до того, как управление PKIX Arc было передано IANA. Ссылки в этих реестрах были обновлены в соответствии с данным документом.

8. Литература

8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[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, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012, <https://www.rfc-editor.org/info/rfc6486>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <https://www.rfc-editor.org/info/rfc6487>.

[RFC7935] Huston, G. and G. Michaelson, Ed., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure", RFC 7935, DOI 10.17487/RFC7935, August 2016, <https://www.rfc-editor.org/info/rfc7935>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8205] Lepinski, M., Ed., and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <https://www.rfc-editor.org/info/rfc8205>.

[RFC8208] Turner, S. and O. Borchert, "BGP Algorithms, Key Formats, and Signature Formats", RFC 8208, DOI 10.17487/RFC8208, September 2017, <https://www.rfc-editor.org/info/rfc8208>.

[X680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1, August 2015, <https://www.itu.int/rec/T-REC-X.680/en>.

[X690] ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1, August 2015, <https://www.itu.int/rec/T-REC-X.690/en>.

8.2. Дополнительная литература

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/info/rfc4272>.

[RFC5123] White, R. and B. Akyol, "Considerations in Validating the Path in BGP", RFC 5123, DOI 10.17487/RFC5123, February 2008, <https://www.rfc-editor.org/info/rfc5123>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, DOI 10.17487/RFC6484, February 2012, <https://www.rfc-editor.org/info/rfc6484>.

[RFC6818] Yee, P., "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 6818, DOI 10.17487/RFC6818, January 2013, <https://www.rfc-editor.org/info/rfc6818>.

[RFC6916] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)", BCP 182, RFC 6916, DOI 10.17487/RFC6916, April 2013, <https://www.rfc-editor.org/info/rfc6916>.

Приложение A. Модуль ASN.1

```
BGPSECEKU { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-bgpsec-eku(84) }

  DEFINITIONS EXPLICIT TAGS ::=
  BEGIN
  -- EXPORTS ALL --
  -- IMPORTS NOTHING --
  -- OID Arc --
  id-kp  OBJECT IDENTIFIER  ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) kp(3) }
  -- BGPsec Router Extended Key Usage --
  id-kp-bgpsec-router OBJECT IDENTIFIER ::= { id-kp 30 }
  END
```

Благодарности

Авторы выражают свою признательность Geoff Huston, George Michaelson и Robert Loomans за их работу над [RFC6487], послужившим базой. Кроме того, в подготовке этой работы важную роль сыграли усилия Matt Lepinski. Спасибо также Rob Austein, Roque Gagliano, Richard Hansen, Geoff Huston, David Mandelberg, Sandra Murphy и Sam Weiler за их рецензии и комментарии.

Адреса авторов

Mark Reynolds

Island Peak Software

328 Virginia Road

Concord, MA 01742

United States of America

Email: mcr@islandpeaksoftware.com

Sean Turner

sn3rd

Email: sean@sn3rd.com

Stephen Kent

Raytheon BBN Technologies

10 Moulton St.

Cambridge, MA 02138

United States of America

Email: kent@alum.mit.edu

Перевод на русский язык

Николай Малых

nmalykh@gmail.com