Network Working Group M. Mealling
Request for Comments: 3405 VeriSign
BCP: 65 October 2002
Category: Best Current Practice

Система DDDS. Часть 5 – процедуры присваивания URI.ARPA

Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA

Assignment Procedures

Статус документа

Этот документ содержит спецификацию стандартного протокола, предложенного сообществу Internet, и служит приглашением к дискуссии в целях развития. Текущее состояние стандартизации и статус описанного здесь протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Тезисы

Этот документ является пятым в серии, полностью описанной в Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS (RFC 3401). Важно подчеркнуть, что понимание любого документа этой серии невозможно без прочтения других документов.

Оглавление

1. Введение

Этот документ определяет правила и процедуры добавления записей NAPTR[1] в зоны URI.ARPA и URN.ARPA с целью преобразования идентификаторов URI[2] в соответствии со спецификацией Dynamic Delegation Discovery System (DDDS) Part Four: The URI Resolution Application (RFC 3402) [2], которая задает Приложение, использующее Базу данных DDDS на основе DNS[3]. Все эти концепции определены в RFC 3401 [1]. Важно отметить, что корректное понимание этого документа невозможно без прочтения RFC 3401 и указанных там документов.

RFC 3403 определяет использование DNS в качестве Базы данных DDDS, содержащей правила передачи полномочий для URI (иногда эти правилами называют указаниями по преобразования). Этот документ указывает, что первым шагом

[1]Naming Authority Pointer - указатель на уполномоченный сервер именования
[2]Uniform Resource Identifiers – однотипные идентификаторы ресурсов
[3]Domain Name System – система доменных имен.

алгоритма является добавление суффикса 'URI.ARPA' к схеме URI и нахождение записи NAPTR для полученного доменного имени. Т. е., первым шагом преобразования http://foo.com/ будет поиск записи NAPTR для домена http.URI.ARPA. Преобразование URN поддерживает похожую процедуру, используя в качестве корневой зону 'URN.ARPA'. В этом документе описаны процедуры вставки новых правил в зоны 'URI.ARPA' и 'URN.ARPA'.

2. Преобразование URI и преобразование URN

RFC 3402 [2] определяет как работают преобразования URI [7] и URN [6], когда используется DNS в качестве базы данных правил передадачи полномочий (или указаний). В частности, этот документ говорит, что начальные инструкции (указания) для преобразования URI на основе DNS хранятся как записи о ресурсах зоны DNS 'URI.ARPA'.

Поскольку URN является схемой URI, указание по преобразованию для URI-префикса 'urn:' также будет храниться в зоне 'URI.ARPA'. Это правило говорит, что пространство имен [6] преобразуется путем добавления суффикса 'URN.ARPA' и результат используется в качестве ключа при поиске записи NAPTR [4].

3. Правила регистрации

Создание данной схемы URI или пространтсва имен URN (NID[1]) выполняется в соответствии с подходящими документами по регистрации. Схемы URI регистрируются по Registration Procedures for URL Scheme Names (RFC 2717) [10]. Пространства имен URN регистрируются по "URN Namespace Definition Mechanisms" (RFC 2611) (или обновленной версии) [9].

3.1 Регистрация URI.ARPA

3.1.1 Разрешены только схемы из дерева IETF

Для включения в зону URI.ARPA соответствующая схема URI **должна** быть зарегистрирована в дереве IETF URI. Требования для этого дерева содержатся в документе [10].

3.1.2 Сначала регистрируются схемы

Недопустимо регистрировать запись NAPTR для схемы URI до регистрации самой схемы и публикации стабильной спецификации в соответствии с [10]. IESG или указанный эксперт будут проверять запрос на предмет

1. корректности и технической обоснованности;
2. совместимости с опубликованными спецификациями URI;
3. того, что что записи NAPTR для базирующихся на DNS URI не передают полномочия преобразования никому, кроме держателя имени DNS;

Последнее правило нужно для того, чтобы данное указание по преобразованию URI не было перехватывало (по неосторожности или по иным причинам) сетевой трафик для данного домена.

3.1.3 Регистрация NAPTR может сопровождать регистрацию схемы

Запрос на регистрацию URI.ARPA **может** сопровождать запрос на регистрацию схемы URI (согласно [10]) и в таких случаях оба запроса вместе рассматриваются IESG или назначенными экспертами.

3.1.4 Регистрация изменений после регистрации схемы

Запрос на регистрацию записи NAPTR (или на изменение существующей записи NAPTR) **может** быть подан после того, как зарегистрирован префикс URI. Если спецификация префикса URI контролируется не IETF, IESG будет требовать одобрения владельца спецификации или поддерживающей ее стороны до того, как будет произведена регистрация. Это требование является дополнением к обычному техническому обзору при регистрации NAPTR, выполняемому IESG или назначенными экспертами.

3.2 Регистрация URN.ARPA

3.2.1 Сначала регистрация NID

Недопустимо регистрировать запись NAPTR для URN NID до регистрации NID и публикации стабильной спецификации в соответствии с [9]. Это делается для предотвращения регистрации записи NAPTR в URN.ARPA в обход процесса регистрации NID.

3.2.2 Регистрация NAPTR может сопровождать регистрацию NID

Запрос на регистрацию URN.ARPA **может** сопровождать запрос на регистрацию NID (в соответствии с [9]) и оба запросабудут рассматриваться вместе.

3.2.3 Регистрация или изменение после регистрации схемы

Запрос на регистрацию записи NAPTR (или на изменение существующей записи NAPTR) **может** быть подан после регистрации NID. Если спецификация NID контролируется не IETF, IESG будет требовать одобрения владельца спецификации или поддерживающей ее стороны до того, как будет произведена регистрация. Это требование является дополнением к обычному техническому обзору при регистрации NAPTR, выполняемому IESG или назначенными экспертами.

Отметим, что это применимо ко всем записям NAPTR для конкретного NID, даже если запись NAPTR может оказывать воздействие только на часть пространства URN, выделенного для NID

[1]Namespace id.

4. Требования к указаниям

Делегирование пространства имен может происходить двумя путями. Для большинства URI делегируемый ключ будет жестко определяться самим идентификатором (например, имя хоста для HTTP URI). Синтаксис местоположения ключа в этом случае предопределен синтаксисом схемы. В других случаях новый ключ может быть частью самого указания. Функциональный эквивалент этого можно выразить словами “если данное правило выполняется, оно всегда является ключом".

Для минимизации нагрузки по запросам в зоны URI.ARPA и URN.ARPA предлагается устанавливать для этих зон экстремально большое время жизни TTL (возможно, измеряемое годами).

Таким образом, для любого префикса URI или пространства имен URN, в которых указания по преобразованию будут склонны к изменению, актуальные правила следует хранить в какой-либо другой (менее статичной) зоне DNS, а в зоне URI.ARPA или URN.ARPA следует использовать стабильную запись NAPTR, которая будет служить для передачи полномочий в менее статичную зону.

Например пространство имен URN 'foo' имеет гибкие правила передачи полномочий. Вместо включения этих правил в зону URN.ARPA туде помещается запись, передающая полномочия хранения этих правил серверу имен с меньшим временем жизни записей. Такая запись в зоне URN.ARPA будет иметь вид:

```
foo     IN NAPTR 100 10  ""  "" "" urn-resolver.foo.com.
```

Когда клиент начинает процесс преобразования. Он сначала будет запрашивать foo.URN.ARPA для получения показанной выше записи, а на втором этапе будет запрашивать 'urn-resolver.foo.com' для получения записей NAPTR, содержащих правила преобразования. TTL на корневом уровне имеет очень большое значение. Значение TTL в 'urn-resolver.foo.com' значительно меньше.

Схема URI 'http', напротив, жестко придерживается определенного синтаксиса, который указывает, что искомый хост задан в самом значении URI. Поскольку этот синтаксис не меняется, правило можно включать в зоеу URI.ARPA. Запись будет иметь вид:

```
http    IN NAPTR 100 100 "" ""  "/http:\\/\\/([^\\/:]+)/\\2/i" .
```

Таким образом, второй шаг преобразования будет заключаться в использовании доменного имени из URI в качестве следующего ключа в цикле. Если, например, данная запись NAPTR является завершающей и содержит некое имя хоста в поле replacement, клиент может обращаться к этому хосту с запросом о данном URI.

5. Процедура подачи

Используя регистрационный механизм MIME Content-Type [8] в качестве успешной модели регистрации, процедуры 'URI.ARPA' и 'URN.ARPA' поддерживают шаблон запроса, подаваемого заинтересованной стороной в открытый список рассылки. Если в течение двух недель не поступило ни одного возражения, представители регистрационного агентства считают подачу состоявшейся и вводят соответствующую информацию в пространство имен.

- Для регистрации в зоне 'URI.ARPA' запросы направляются по адресу 'register@URI.ARPA'.
- Для регистрации в зоне 'URN.ARPA' запросы направляются по адресу 'register@URN.ARPA'.

В качестве регистрационного агентства выступает IANA[1].

В качестве возражений принимаются те, которые отмечают влияние на саму зону или DNS в целом. Возражения по схеме URI или пространству имен URN NID не допускаются, поскольку их следует обсуждать в соответствующих форумах. Логическим следствием из этого является то, что **должна** разрешаться регистрации **любых** санкционированных схем URI и пространств имен URN, если они соответствуют требованиям данного документа в части времени жизни и общего влияния на DNS.

6. Регистрационный шаблон

Шаблон, направляемый для регистрации в соответствующий список рассылки **должен** включать:

6.1 Ключ

Это значение URN NID или схемы URI, используемое в качестве доменной части запроса DNS. Ключ должен быть корректен с точки зрения процедур, указанных в документах по распределению пространства имен URN, а также все новым стандартам по регистрации новых схем URI.

6.2 Полномочность

Персона или организация (объект), имеющая полномочия на регистрацию записи. Эти полномочия должны быть признаны IESG или относится к числу указанных в документах по регистрации URN NID [9] или схем URI [10].

6.3 Записи

Актуальные записи DNS, представляющие набор правил для ключа. Требуемыми полями являются Preference, Order, Flags, Services, Regex и Replacement, определенные в документе RFC 3404 [4].

7. Пример шаблона

```
To: register@URN.ARPA
From: joe@foo.com

Key: foo
Authority: Foo Technology, Inc as specified in RFCFOO
Record: foo     IN NAPTR 100 100 "" "" "" urn.foo.com.
```

[1]Internet Assigned Numbers Authority – агентство по присвоению значений для Internet.

8. Регистрация URN в зоне URI.ARPA

Поскольку в этом документе обсуждаются зоны URI.ARPA и URN.ARPA, а правило URN существует в зоне URI.ARPA, это делает осмысленным приведенное ниже правило URI при регистрации URN.

```
To: register@URI.ARPA
From: The IETF URN Working Group

Key: urn
Authority: RFC2141
Record: urn     IN NAPTR 0 0 "" "" "/^urn:([^:]+)/\\2/i" .
```

9. Согласование с IANA

Агентство IANA создало зоны URN.ARPA и URI.ARPA. Иерархическая структура имен и использование имен только из этих зон обеспечивают возможность использования ключей, описанных в параграфе 6.1 этого документа. Администрирование и текущее управление для этих зон принимает на себя IANA. Записи DNS, включаемые в эти зоны, регистрируются, как описано в этом документе.

Агентство IANA также создало две почтовых конференции (списки рассылок) register@uri.arpa и register@urn.arpa для регистрации в соответствии с данным документом. Списками также управляет IANA.

10. Вопросы безопасности

Зоны 'uri.arpa' и 'urn.arpa' могут служить объектами DoS-атак[1] и подмен (spoofing) для изменения путей передачи полномочий. Любому объекту с сервером имен, на котором поддерживаются эти зоны, следует предпринять соответствующие меры по защите этих важных компонент инфраструктуры Internet. Когда станет возможным использование серверами имен цифровых подписей, записи из этих зон также следует подписывать.

11. Благодарности

Автор выражает свою признательность Ron Daniel, который был соавтором изначального варианта этого документа. Вклад Рона в разработку модели правил передачи полномочий сделал возможными описанные здесь процедуры и саму систему DDDS.

12. Литература

[1] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS", RFC 3401[2], October 2002.

[2] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", RFC 3402[2], October 2002.

[3] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403[2], October 2002.

[4] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application", RFC 3404[2], October 2002.

[5] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures", RFC 3405, October 2002.

[6] Moats, R., "URN Syntax", RFC 2141, November 1998.

[7] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[8] Freed, N., Klensin, J. and J. Postel, "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", BCP 13, RFC 2048, November 1996.

[9] Faltstrom, P., Iannella, R., Daigle, L. and D. van Gulik, "URN Namespace Definition Mechanisms", BCP 33, RFC 2611, October 1998.

[10] Petke, R. and I. King, "Registration Procedures for URL Scheme Names", BCP 35, RFC 2717, January 1999.

13. Адрес автора

Michael Mealling

VeriSign

21345 Ridgetop Circle

Sterling, VA 20166

US

EMail: michael@neonym.net

URI: http://www.verisignlabs.com

Перевод на русский язык

Николай Малых

[1]Denial of Service – атака, направленная на отказ служб.
[2]Перевод этого документа имеется на сайте www.protocols.ru. *Прим. перев.*

nmalykh@protocols.ru

14. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.