
КОБЕ — Совместное заседание Правления ICANN и TEG
Среда, 13 марта 2019 года, 17:00 – 18:30 по JST
ICANN64 | Кобе, Япония

ХАРАЛЬД АЛВЕСТРАНД (HARALD ALVESTRAND): Добро пожаловать на совместное заседание Правления ICANN и Группы технических экспертов. Я не Акинори. Сюрприз. Он немного опаздывает на эту встречу, но скоро придет, а тем временем я попытаюсь исполнять его роль, то есть попрошу Адизэля познакомить нас с повесткой дня.

АДИЭЛЬ АКПЛОГАН (ADIEL AKPLOGAN): Спасибо, Харальд. Я хочу кратко рассказать о повестке дня и о том, что мы будем рассматривать.

Как вы помните, на прошлых двух встречах Правления и TEG много обсуждалась структура заседания и наши возможности в плане повышения его эффективности. Поэтому мы решили испытать новый подход к составлению повестки дня и взаимодействию на сегодняшнем заседании. Если говорить конкретно, мы отправили членам TLG ряд вопросов, которые сочли интересными и важными для Правления, а затем составили повестку дня на основании полученных ответов.

Примечание. Следующий документ представляет собой расшифровку аудиофайла в текстовом виде. Хотя расшифровка максимально точная, иногда она может быть неполной или неточной в связи с плохой слышимостью некоторых отрывков и грамматическими исправлениями. Она публикуется как вспомогательный материал к исходному аудиофайлу, но ее не следует рассматривать как аутентичную запись.

Было отправлено пять вопросов, и мы получили ответы на три: от IAB, ETSI и W3C. Один вопрос был также отправлен в МСЭ. Они принесли извинения за свое отсутствие, и поэтому не смогут дать ответ.

Таким образом, мы заслушаем представителей этих трех организаций-членов TLG, их мнение по данным вопросам, и предоставим возможность членам Правления и сообщества также задать вопрос и обсудить тему.

Другой полученный нами комментарий был о необходимости предоставить Правлению более широкие возможности взаимодействия с TLG и TEG, поэтому в повестке дня был предусмотрен 30-минутный диалог между Правлением и TEG для обсуждения этих или других тем.

Планируемая структура этого заседания содержит три основных раздела. Первый — вопросы Правления или корпорации, второй — перспективный анализ, выполненный TLG, любые будущие тенденции, все, на что Правление должно обратить внимание, и последняя часть повестки дня будет посвящена взаимодействию и обсуждению.

Таким образом, мы опробуем этот подход. Мы впервые используем такую модель. Посмотрим, как она работает. И затем будем отталкиваться от поступивших отзывов.

А теперь слово снова вам, Харальд.

ХАРАЛЬД АЛВЕСТРАНД: Спасибо. И в рамках рассмотрения нашего первого вопроса, первого пункта повестки дня, мы предоставим слово IAB, которому был задан следующий вопрос: За какими самыми важными идентификаторами, определяемыми IETF, помимо доменных имен и IP-адресов, должна наблюдать ICANN? Или может быть не должна.

УОРРЕН КУМАРИ (WARREN KUMARI): У вас есть пульт?

ХАРАЛЬД АЛВЕСТРАНД: Персонал, пульт у вас?

АДИЭЛЬ АКПЛОГАН: Можете просто сказать «Дальше», и они поменяют слайд.

ТИМ ВИЧИНСКИ (TIM WICINSKI): Итак, я Тим Вичински и сегодня выступаю от имени Уоррена Кумари (Warren Kumari).

Мы передали этот вопрос IAB, Совету по архитектуре интернета и, конечно, будучи группой архитекторов, они дали нам очень подробный и содержательный ряд ответов, на основе которых мы попытались определить своего рода механизм высокого уровня. Мы просмотрим множество слайдов, значительная часть которых

адресована техническим специалистам, и затем, конечно, просто попытаемся привлечь внимание Правления к наиболее ярким моментам. Итак...

Вопрос заключался в том, какие из определяемых идентификаторов наиболее важны, и мы... они, безусловно, дали нам весьма содержательный ответ. Они, конечно, разделили идентификаторы на два типа, однозначные и многозначные. Однозначные — это такие, как IP-адреса и вещи аналогичного характера. У них есть определенные значения.

Многозначные, структурные значения. Задумайтесь о таких вещах, как URI, состоящих из нескольких компонентов. Мы рассматриваем их отчасти как кубики LEGO. Кубики LEGO можно соединять друг с другом, они все определены, и когда вы их соединяете, получается что-то большее. Например, всем известно, что такое URI. Есть путь, есть доменное имя, есть путь, есть запрос. Считайте их просто небольшими кусочками. Вы их соединяете и получаете идентификатор нового вида. Все определено. Все в общем-то просто. И они растут таким способом.

Кроме того, мы говорим, что идентификаторы имеют область видимости, локальную или частную область видимости для систем, работающих самостоятельно, и глобальную область видимости. Локальная область

видимости — это вещи, которые создаются внутри программного обеспечения, с ними ни один из нас не сталкивается регулярно. Но, что касается глобальной области видимости, по-моему, ICANN занимается именно этим. Эти идентификаторы сохраняют уникальность во всех системах. Необходимое условие. И они определяются в параметрах протокола, для обслуживания которых мы используем IANA. Таким образом, это в общем-то вещи, которые собирается проанализировать ICANN.

И то, что мы видим в новой рабочей среде, по сути, является многозначными или структурными идентификаторами. Использование уже существующих вещей в качестве стандартных блоков. Мы соединяем эти блоки и создаем новые. И это, по-видимому, значительная часть работы, выполняемой в IETF. Все очень просто.

Кроме того, важная вещь для нас — IANA. Мы очень ценим IANA, потому что она обслуживает все эти реестры параметров протокола. И, по мнению ICANN, мы можем обеспечить сохранение текущего превосходного качества работы IANA, потому что нам нужна их помощь в определении этих регистров и поддержании полной синхронизации.

По существу, они задали вопрос и IAB ответил на него. Фактически, это был не ответ. Они ответили: что вы

считаете важным? Знаете ли, я прочитал то, что они написали, и хотя это очень полезная информация, она не будет... вопрос в общем-то остается открытым, потому что... немного касается ICANN, помимо вашей работы в IANA, которую, мы считаем, очень и очень ценной, и я хочу это подчеркнуть.

Такова в основном наша точка зрения.

И у нас были уточняющие вопросы там, но я полагаю, что их планируется рассмотреть в конце заседания.

ХАРАЛЬД АЛВЕСТРАНД: Спасибо.

И меня также уведомили, что из-за того, что я совсем недавно вступил в эту должность, я совершенно забыл попросить участников дискуссии... и членов Правления представиться.

Патрик, хотите начать?

ПАТРИК ФАЛЬТСТРОМ (PATRIK FALTSTROM): Патрик Фальтстром, SSAC.

ТРИПТИ СИНХА (TRIPTI SINHA): Трипти Синха, Правление ICANN.

АВРИ ДОРИА (AVRI DORIA): Аври Дория, Правление ICANN.

ШЕРИН ШАЛАБИ (CHERINE CHALABY): Шерин Шалаби, Правление ICANN.

СТИВ КРОКЕР (STEVE CROCKER): Стив Крокер, нахожусь в свободном плавании.

ГОВАРД БЕНН (HOWARD BENN): Говард Бенн, представляю ETSI.

ДЖЕЙ ДЕЙЛИ (JAY DALEY): Джей Дейли, занимаю несколько должностей.

МЕРИКЕ КАЕО (MERIKE KAEO): Мерике Каео, представитель SSAC в Правлении.

ВЕНДИ ЗЕЛЬЦЕР (WENDY SELTZER): Венди Зельцер, W3C.

ДАНИЭЛЬ ДАРДАЛЬЕ (DANIEL DARDAILLER): Даниэль Дардалье, больше не работаю в W3C, но сегодня все еще представляю W3C.

ХАРАЛЬД АЛВЕСТРАНД: Харальд Алвестранд, представитель IETF в Правлении ICANN.

АДИЭЛЬ АКПЛОГАН: Адизель Акплоган, Правление ICANN.

ТИМ ВИЧИНСКИ: Тим Вичински, IETF, представитель IAB.

УОРРЕН КУМАРИ: Уоррен Кумари. Я из IAB.

РОН ДА СИЛЬВА (RON DA SILVA): Рон да Сильва, Правление ICANN.

ЛИТО ИБАРРА (LITO IBARRA): Лито Ибарра, Правление ICANN.

АМИНЕ МЧАРЕК (AMINE MCHAREK): Амине Мчарек, ITU-T.

ЛАРС-ЙОХАН ЛИМАН (LARS-JOHAN LIMAN): Ларс-Йохан Лиман, оператор корневого сервера и RSSAC.

ХАРАЛЬД АЛВЕСТРАНД: Можно попросить сидящих в аудитории членов Правления помахать руками, чтобы мы увидели, где они?

Спасибо.

А теперь, я думаю, следует передать слово ETSI.

ГОВАРД БЕНН: Спасибо. В таком случае я могу получить пульт?

Спасибо. Итак, ICANN передала наш вопрос правлению ETSI, но в ETSI также есть группа, в состав которой входят все председатели наших технических органов, которая называется OCG. Я передал вопрос им тоже.

Думаю, прежде чем с головой окунуться в... есть всего лишь несколько слайдов. Они не займут много времени, но прежде чем обратиться к слайдами, пожалуй, я скажу несколько вступительных слов о том, насколько важной становится DNS для мобильного сообщества.

Думаю, что Йоран был немного неправ, когда говорил в своем вступительном докладе в понедельник утром о том, что он был на... я тоже был на Всемирном мобильном конгрессе несколько недель назад... и он указал, что на этом конгрессе прозвучало несколько комментариев о

взаимодействии между интернетом и мобильной отраслью.

Дело в том, что наши стандарты 5G полностью ориентирован на предоставление интернет-сервисов. И наша текущая работа в сетях, которые являются программно-аппаратной частью всей системы, направлена на переход от использования... ну, в них используются не столько патентованные стандарты, сколько специализированные интерфейсы между функциями. В сети мобильной связи есть много функций, охватывающих все, начиная с контроля политики, аутентификации. Их целая уйма. Определено около 25 функций. Сейчас все это движется в сторону архитектуры, больше ориентированной на интернет. То есть для каждой из них вместо специализированных интерфейсов все больше используется HTTPS и для каждой из этих функций, конечно, будет нужна DNS. Таким образом, безопасность DNS, по-моему, очень важна для нас.

Но, что интересно, когда я все рассмотрел, то понял, что это не требует изменения DNS в какой бы то ни было форме. Очевидно, DNS изначально была отлично разработана, поэтому в данный момент она полностью пригодна для использования нами.

Но я действительно обнаружил одну область в одной из групп ETSI, которая занимается электронными подписями

и инфраструктурой. И, опять-таки, если вы хотите узнать больше об этих группах и получить спецификации, просто зайдите на сайт etsi.org. Они недавно реконструировали этот сайт, и теперь он достаточно удобен для использования.

Итак, область, которую они рассмотрели, опирается на сертификат X.509. Я уверен, что большинству людей в техническом сообществе это понятно. Это сертификат, который используется для... можно увидеть небольшой символ замка в веб-браузере, который содержит определенную информацию. Очевидно, ее важный компонент — это ключ, но также в данный момент указывается URL сайта, к которому вы получаете доступ.

Еще в 2014 году Европейский союз решил, что хочет добавить дополнительную информацию, чтобы был мандат электронного идентификатора и доверие к услугам. Это требуется, чтобы сертификаты сайтов считались отвечающими требованиям. Затем ETSI работал над реализацией того мандата, занимался созданием соответствующих спецификаций. Таким образом, квалификационная часть имени — это имя владельца сайта, а также официальный регистрационный номер. Опять-таки, побродив по интернету, можно достаточно быстро найти такой мандат.

Мы добавили несколько дополнительных полей в сертификат X.509, и стандарт ETSI теперь поддерживает ряд из них. Я на самом деле... я понял, что стандарт... здесь не указан его номер. Так что, если это кому-то интересно, EN 319 412. Опять-таки, его можно бесплатно загрузить с сайта ETSI, и он позволяет добавить регистрационный номер компании или регистрационный номер НДС, глобальный идентификатор юридического лица или номер разрешения поставщика платежных услуг.

Таким образом, сейчас мы сотрудничаем, скажем, с Форумом разработчиков браузеров, пытаюсь реализовать это для поддержки Европейской комиссии.

На этом все. Спасибо.

ХАРАЛЬД АЛВЕСТРАНД: Спасибо, ETSI.

И последний, но не менее важный докладчик, W3C.

ВЕНДИ ЗЕЛЬЦЕР: Спасибо, Харальд, и мне не нужен пульт, потому что я не подготовила слайды, но вопрос, заданный W3C... возможно, это просто вернет на экран повестку дня.

Нет.

... был следующим: считаем ли мы, что новые виды данных, связанных с именами DNS, могут в будущем принести пользу веб-архитектуре.

И при рассмотрении этого вопроса мы провели в группе W3C небольшое обсуждение. Конечно, доменные имена — важная часть веб-архитектуры, и для веб-приложений доменные имена являются базовым элементом URL-адреса, позволяющего получить доступ к веб-странице, или URI. И они важны для безопасности интернета, устанавливая границы зоны безопасности, определяя через политику одного источника допустимый активный контент в контексте веб-приложения. Они важны для конфиденциальности пользователей, устанавливая границы использования файлов cookie. Таким образом, вопрос, могут ли дополнительные данные в регистрационной записи DNS способствовать решению каких-либо задач применительно к веб-приложениям, вызывает интерес. Кроме того, мы также рассмотрели, знаете ли, предыдущие усилия по созданию таких расширенных данных в DNS и увидели, что веб-сообщество не слишком активно их использует. То есть проекты IETF, такие как DANE и Debound, направленные на предоставление дополнительной информации о доменном центре или ассоциации получили широкого распространения в веб-среде. Почему создатели веб-

приложений не используют возможность хранения в DNS информации, относящейся к центрам сертификации?

Иногда создатели приложения обеспокоены проблемами производительности и кажущимися или реальными задержками, обусловленными необходимостью получения данных из DNS. Иногда это вопросы архитектуры приложений. Разработаны системы пограничного кэширования с целью ускорения работы веб-приложений, поэтому легче хранить дополнительную информацию, относящуюся к сайтам, в файлах .well-known, для которых используется протокол HTTP, вместо канала DNS. Иногда это трудность, реальная или кажущаяся, включения дополнительной информации в регистрационную запись домена, отсутствие поддержки со стороны регистратора... или стандартизированной поддержки хранения дополнительной информации.

Таким образом, по-моему, это хороший пример того, когда сообществам целесообразно провести мозговой штурм, чтобы определить области, в которых дополнительные данные DNS могли бы принести пользу. При этом следует учесть некоторые системные и экономические соображения, касающиеся вовлечения всех сотрудничающих сторон в процесс создания компонентов и обеспечения их эффективного функционирования в составе веб-архитектуры. Что мешает реализации вещей,

которые могли бы быть интересными? Действительно ли DNS — лучший способ устранения таких препятствий, по сравнению с использованием других веб-компонентов, например, для хранения информации о принадлежности или объеме полномочий? Вопрос в аутентификации рекламы. Таким образом, интересный вопрос, над решением которого сообществу полезно подумать, касается не только технических проблем, но также стимулов создания систем и потенциала... и изменений систем, которые должны произойти для того, чтобы это изменение стало эффективным.

ХАРАЛЬД АЛВЕСТРАНД: Спасибо, Венди.

Итак, текущий пункт повестки дня — открытое взаимодействие с Правлением. Это означает, что члены Правления от TEG теперь могут задавать вопросы.

И я начну с вопроса к ETSI, просто случайного, но отчасти (невнятно) со словами Венди о том, что сейчас с доменными именами связано больше информации, чем раньше. Это также означает, что часть такой информации может опровергать или подтверждать данные, которые хранятся в других местах, например в WHOIS, или в файлах .well-known, обычно известные организации Венди.

Как, по вашему мнению, должны взаимодействовать различные хранилища информации?

ГОВАРД БЕНН:

Это очень интересный вопрос. И на самом деле практически такой же вопрос я задал председателю группы: почему эти данные было решено включить в состав сертификата, а не в состав информации WHOIS.

По-видимому, кто-то из Европейской комиссии захотел связать это с сертификатом безопасности, а специалисты по безопасности просто сделали то, что им было велено, и составили стандарт.

Честно говоря, я действительно не понимаю причину принятия такого решения. По-моему, это решение было политическим, а не техническим. Кто мы, чтобы оспаривать действия наших политических лидеров?

Тем не менее, вопрос о противоречии между данными действительно интересный. Сейчас авторитетным источником данных в Европе должен быть сертификат. Таким образом, он... считается авторитетным источником. Если эта информация противоречит информации WHOIS, сертификат имеет преимущественную силу.

ХАРАЛЬД АЛВЕСТРАНД: Стив.

СТИВ КРОКЕР:

Спасибо.

Итак, Венди, на самом деле я потратил изрядное количество времени, думая о том, как поместить больше информации в DNS, использовать ее в различных целях. И существует целый ряд конкретных проблем. По большей части, DNS настроена так, что информация вводится администратором DNS через регистратора, если речь идет о TLD. И в случае локального администрирования с помощью локальных инструментов. По моему опыту, это не является распространенной практикой... и ситуация могла бы измениться в положительную сторону... если бы приложения помимо обычных адресов и информации о DNS-серверах обрабатывали бы данные, предназначенные для других целей. К примеру, если вы хотите создать запись DNS для каждого сотрудника своей организации и сделать их адреса электронной почты видимыми, полезно установить связь с системой управления электронной почтой. Я видел, как это было сделано в отдельном случае. Но, как я сказал, такие инструменты, по моему опыту, не являются общедоступными. Это один ключевой вопрос.

И вы немного коснулись трудности включения новой информации.

Второе препятствие, которое я увидел спустя какое-то время, это то, что в случае возникновения желания

создать новую запись DNS, новый тип RR, сейчас используется болезненный процесс: сначала определение и стандартизация, и это еще простая часть, затем получение одобрения и реализация. Поэтому на практике для внедрения чего-либо в интернете эти проблемы решаются обходным способом, поэтому текстовые записи имеются в большом количестве и получают быстрое распространение, что в некоторых отношениях считается негативным явлением, а в других отношениях — это само собой разумеющийся подход. Но он отчасти разрушает процесс стандартизации.

Это второй вопрос. У меня есть еще один или два.

Третий — то, что DNS действительно хорошо подходит для предоставления открытого доступа к множеству мелочей, доступных везде. Она не очень хорошо подходит для защиты информации, чтобы ее могли получать только уполномоченные лица. И есть много игр с предоставлением разным людям различных объемов информации с учетом географического местоположения и так далее. Но основная... базовая структура... вы знаете это и все знают это.

Есть также, пожалуй, менее важный аспект. Если вы собираетесь поместить элемент данных размером в один килобайт, это прекрасно. Если вы собираетесь поместить элемент данных размером в один гигабайт, все будет

работать не так хорошо, и я просто хочу подчеркнуть этот момент.

Какое мнение у W3C и у ETSI касательно данного класса проблем?

ВЕНДИ ЗЕЛЬЦЕР:

Спасибо, Стив.

Думаю, что у всего сообщества W3C взгляды преимущественно следующие: мы используем то, что есть в DNS сейчас и встраиваем в веб-приложения и веб-серверы другие информационные компоненты. И ответ на этот вопрос заставил меня больше задуматься о том, почему это происходит, и почему даже вещи, которые кажутся структурно подходящими для включения в DNS, не были там размещены. Другая причина, которая приходит на ум, — это просто расхождение технологии с организационной структурой. Часто домен регистрирует совсем не тот человек, который управляет веб-приложениями и объемом полномочий, которые он готов дать таким вещам.

Поэтому, откровенно говоря, я не наблюдала сильного стремления включить больше информации в DNS у нашего сообщества разработчиков веб-приложений.

УОРРЕН КУМАРИ: Уоррен Кумари, представляю... на самом деле, наверное, просто свое личное мнение, чтобы попытаться ответить на некоторые ваши вопросы.

Вы упомянули такие идеи, как включение в состав данных DNS адресов электронной почты или аналогичной информации об отдельных людях.

Недавно был составлен документ... я не помню его точный статус... в котором говорится о включении в DNS таких вещей, как платежные реквизиты физических лиц. Например, если вы хотите отправить мне немного денег... и если хотите, я не возражаю... как это сделать? Вы должны отправить их с помощью чего-то аналогичного PayPal или Apple Pay или другой платежной системы, знаете ли, это лучший способ отправки мне микроплатежей. И сейчас идет обсуждение возможности использования реквизитов отдельного пользователя на уровне DNS для этой цели. Как я уже сказал, я не помню точный статус документа, но просто подумал, что это может представлять интерес... интересно за этим проследить.

И еще одна короткая новость. Да, вы правы, много обсуждалась трудность получения типа RR, знаете ли, нового типа записи в DNS. И я не помню, когда это было, но не слишком давно ситуация изменилась, то есть вместо стандарта теперь необходима просто экспертная оценка.

И это изменение связано с признанием того, что загрузка текстовых записей очень усложняет синтаксический анализ, таким образом, теперь намного легче получить тип RR. По сути, теперь нужно отправить заявку, после чего проводится процесс экспертного анализа. Таким образом, все стало намного проще.

И позвольте мне взглянуть на свое последнее примечание. А, ну да.

Да, регистрационные записи большого размера в DNS не работают. Думаю, что это намеренное архитектурное решение. Это большая распределенная база данных. И крупные объекты должны, вероятно, находиться где-то в другом месте, а в DNS — только ссылки на них или какое-то средство найти их. Это в общем-то определяется самой структурой и организацией базы данных. Большие записи должны кэшироваться в резолверах других людей, что возможно является архитектурным...

СТИВ КРОКЕР:

Рискуя продвинуться еще глубже, скажу... при определении нового типа RR, даже если вам удастся быстро пройти процесс стандартизации, реализация распознавания станет по-настоящему трудной задачей... по моему представлению, если бы мы действительно захотели сделать процесс гладким, заняться парсингом

текстовых записей и так далее, можно было бы разработать систему грамматических правил и одобрить несколько допущений, и тогда процесс распространения новой записи стал бы относительно быстрым. Это было бы похоже на текст.

Но это не так... и при синтаксическом анализе вы могли загрузить все эти грамматические правила.

Это мало чем отличается от стремления продвигать что-то по HTTP, потому что все проходит, но вы не обязаны, знаете ли.

УОРРЕН КУМАРИ:

На самом деле это поднимает очень интересный момент. Есть документ, я не помню его статус, но может быть Патрик или Сьюзан помнят, который определяет конкретный механизм этого. Способ представить описание типа RR и тем самым позволить программному обеспечению обработать это и понять. Один из очевидных вариантов использования... по-моему, Венди сказала, что часто трудно ввести в DNS новую информацию через интерфейс регистратора. У многих веб-интерфейсов есть конкретные поля. И этот новый формат позволил бы веб-системам распознать, что у данного типа RR есть два числовых значения и затем строка. Сделать так, чтобы у людей был пригодный способ введения информации.

ХАРАЛЬД АЛВЕСТРАНД: Я вижу, что у ОСТО есть комментарии на эту тему?

ДАВИД КОНРАД: Да. Мы действительно... ICANN профинансировала разработку Джоном Левином (John Levine) программного обеспечения. Есть пакет, полагаю, что он написан на языке Perl. Я не знаю, здесь ли Джон. Наверное, нет. Однако, да, существует код, который делает именно то, что вы сказали. И цель этого состояла в том, чтобы людям стало намного проще реализовать новые типы RR в веб-системах. Конечно, зачастую немного трудно заставить людей на самом деле это использовать, но некоторая работа в данной области выполнена.

ДАНИЕЛЬ ДАРДАЛЬЕ: Хорошо. Даниэль Дардалье. Да, я думаю, что помимо вопросов полезности и производительности при использовании DNS для веб-данных, существует также такой вопрос, как нежелание людей повышать свою зависимость от... на... по сути, на уровне имен. Сегодня это действительно маленький интерфейс, через... знаете ли, веб-приложение должно получить адрес хоста и все, остальное выполняется на транспортном уровне. И нет необходимости знать, что происходит в DNS на один уровень выше. По-моему, люди... склоняются к тому, чтобы больше не использовать этот уровень, поскольку

это создало бы большую зависимость, чем им нужно. То есть им необходим минимум информации, знаете ли.

УОРРЕН КУМАРИ: Лиман.

ЛАРС-ЙОХАН ЛИМАН: Ларс Лиман. Краткий комментарий. Чтобы иметь возможность также устранить зависимость от... центра сертификации.

ХАРАЛЬД АЛВЕСТРАНД: К сожалению, невозможно устранить зависимость от политической власти. По-видимому, люди ведут себя смиренно. Все считают, что мы исчерпали эту тему? Думаю, у нас есть... решение, которое... в общем-то, новые имена и новая информация вызывают интерес, но нам важнее всего поддерживать в рабочем состоянии старые, потому что мы в настоящее на это рассчитываем и хотели бы сохранить уверенность в том, что на их работоспособность и впредь можно рассчитывать. Также указывалось, что многие проблемы использования идентификаторов и зависимости одних вещей от других вещей... определяются не только архитектурными, но и техническими факторами, такими как состояние реализации, степень знакомства с технологиями, юридические ограничения. Так что, по-

моему, это было самое полезное заседание. Акинори, вы готовы перейти к прочим вопросам?

АКИНОРИ МАЕМУРА: Большое спасибо. Извините за опоздание. У меня была договоренность об удаленном взаимодействии... которая совпала по времени с этим заседанием.

Хорошо. Раздел «Прочие вопросы». Есть что-нибудь у ОСТО? Нет? Хорошо.

Что-нибудь у членов TEG? Хорошо.

ХАРАЛЬД АЛВЕСТРАНД: Было ли это заседание полезным?

АКИНОРИ МАЕМУРА: Это ваш вопрос? Хорошо.

УОРРЕН КУМАРИ: Хочу поинтересоваться, не следует ли спросить, есть ли вопросы у аудитории.

АКИНОРИ МАЕМУРА: Да. Большое спасибо.

Если у кого-то есть вопрос, сейчас самое подходящее время, чтобы задать вопросы участникам дискуссии — членам Правления и TEG. Спасибо.

ПОЛ ХОФФМАН (PAUL HOFFMAN): Это Пол Хоффман. Не столько вопрос, сколько история, возвращающая к вопросу ETSI.

Фактически, IETF начал изучать предложение о введении проверенных сертификатов очень давно, приблизительно в 1999 году, и они были стандартизированы в 2001 году в рабочей группе PKIX.

Я поднимаю этот вопрос, потому что это был один из первых проектов, над которыми ETSI и IETF работали вместе. И на самом деле он относился не только к доменным именам. Он относился к... так как сертификаты PKIX в тот момент в основном рассматривались применительно к работе IETF, относящейся как раз к доменным именам. У них все же есть другие области применения, и эта технология расширяемая.

Это был один из случаев, когда ETSI сказал: «Нас интересуют не только доменные имена. Нас интересует и другая проверенная информация». И тогда IETF в общем-то пришлось согласиться на расширение.

И возвращаясь к тому, что Тим сказал о важности IANA, позже... в тот момент реестр расширений для сертификатов PKIX хранился только на сайте, а не в IANA. Рабочая группа PKIX в общем-то вела собственный реестр.

И затем, когда намного позже расширение проверенного сертификата переехало в IANA, оно вошло в состав этих данных. Это на самом деле демонстрирует возможности сотрудничества этих организаций, когда совместно изучаются предложения внешних групп, связанные с DNS, а затем выполняется вся эта работа, конечный результат которой попадает в регистратуры IANA. Спасибо.

АКИНОРИ МАЕМУРА: Кто-то еще?

ПАТРИК ФАЛЬТСТРОМ: Патрик Фальтстром, SSAC.

Думаю, что работа над сертификатами X.509 — превосходный примером того, что IETF и ETSI могут сотрудничать. Если продолжить анализ того... как связать доменные имена с сертификатами, просто потому что было такое широкое обсуждение интернационализированных доменных имен не только здесь в ICANN, но также и в IETF сейчас. IETF также долго

работала над этим вопросом, но эта работа завершилась в 2011 году созданием RFC 6125, конкретно, как оценивать интернационализированные доменные имена и как сравнивать их, когда они входят в состав данных сертификата. Это означает, что IETF разрабатывает вещи, которые затем влияют на содержание самих сертификатов. Спасибо.

АКИНОРИ МАЕМУРА: Уоррен.

УОРРЕН КУМАРИ: Спасибо. Уоррен Кумари. Как я сказал, очень короткое дополнение. Думаю, что это также логично приводит к сообщению Тима/IAВ о том, что у нас теперь есть своего рода основание «системы счисления»: идентификаторы, IP-адреса, доменные имена и так далее, и многие текущие и будущие инновационные решения подразумевают объединение этих существующих систем и их подключение друг к другу для создания более крупной и удобной системы.

АКИНОРИ МАЕМУРА: Большое спасибо.

Еще замечания? Хорошо.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: (Говорит не в микрофон.)

АКИНОРИ МАЕМУРА: Пожалуйста.

ГОВАРД БЕНН: Так как у нас осталось немного времени, еще одной интересной областью, которая обнаружилась в результате текущей работы в ETSI, в общем-то она с этим не связана, но возможно имеет к этому некоторое отношение, мы очень активно изучаем квантовые вычисления. И квантовые вычисления действительно интересны, если удастся сделать эту технологию работоспособной, потому что она разрушит TLS и всю систему безопасности, на которую мы опираемся сегодня.

Таким образом, есть группа в TC CYBER, которая занимается вопросами кибербезопасности и пытается разработать защищенные на квантовом уровне методы шифрования.

Опять-таки, эта работа находится на начальной стадии. Но если кто-то заинтересовался, на сайте ETSI можно получить свежую информацию об этой работе.

И думаю, что в будущем, если квантовые вычисления действительно получат широкое распространение, это

могло бы оказать радикальное влияние на ICANN в долгосрочной перспективе.

АКИНОРИ МАЕМУРА: Большое спасибо.

ТИМ ВИЧИНСКИ: По-моему, на самом деле работа в области квантовых вычислений также идет в IRTF, в Инженерной исследовательской группе интернет-технологий. Я посмотрю, какие есть параллели в работе обеих групп. Такие дела.

АКИНОРИ МАЕМУРА: Итак, квантовые вычисления будут... войдут в повестку дня будущих заседаний TEG? Вполне ожидаемо.

Еще замечания? Если нет, отлично. Большое спасибо членам TEG, ВТС и Правления. Совместное заседание Правления ICANN и TEG закрыто. Большое спасибо.

[КОНЕЦ РАСШИФРОВКИ]