КОБЕ – заседание по взаимодействию с сообществом: техническая группа ICANN по изучению доступа к закрытым регистрационным данным (TSG)
Понедельник, 11 марта 2019 года, 13:30 – 15:00 по JST
ICANN64 | Кобе, Япония

РАМ МОХАН (RAM MOHAN): Добрый день. Через пару минут мы начинаем заседание, посвященное технической группе по изучению доступа к закрытым регистрационным данным. Спасибо.

Добрый день. Меня зовут Рам Мохан, я координатор технической группы по изучению доступа к закрытым регистрационным данным, мы называем ее TSG-RD. На это заседание у нас запланировано примерно 90 минут.

Мы ожидаем, что примерно 45 минут из этих 90 мы будем рассматривать процесс, который мы провели, и представим вам проект технической модели, чтобы услышать ваши комментарии и отклики.

И ожидается, что это будет интерактивное заседание. Это не единственное заседание. Вчера мы встречались с группой по EPDP, а сегодня и завтра собираемся встретиться с другими группами, чтобы тоже проинформировать их о проделанной работе.

А теперь позвольте мне ознакомить вас с повесткой дня. Мы планируем рассмотреть следующие темы. Ожидается, что у нас будет достаточно времени для

обсуждения вопросов, которые у вас возникли. И, по-моему, здесь есть те, кто занимается рассмотрением комментариев от дистанционных участников, так что их мы тоже сможем прокомментировать.

Теперь позвольте я немного расскажу вам о самой Технической группе по изучению. Чтобы по-настоящему рассказать, в чем смысл, рассказать, как мы начинали, чем занимаемся и так далее, я передаю слово Йорану.

ЙОРАН МАРБИ (GÖRAN MARBY): Спасибо, Рам. Прежде чем я начну, я бы хотел поблагодарить членов группы за работу, которую вы проделали за последние три месяца в дополнение к своим остальным обязанностям. Как сторонний наблюдатель, я всегда так счастлив и рад, что есть волонтеры, готовые этим заниматься.

Итак, почему возникла такая группа? Во-первых, мы говорим об интересном правовом явлении с потенциальным техническим решением. Я должен еще раз повторить некоторые вещи, которые вы от меня, скорее всего, уже слышали раз 200.

В законе GDPR очень четко сказано по поводу роли контролера данных, стороны, ответственной за обработку данных. Те, кто собирает данные, хранит данные и

принимает решения о данных, – именно они несут ответственность согласно GDPR.

В нашем контексте они являются сторонами, связанными договорными обязательствами. У корпорации ICANN как юридического лица нет базы данных. Я знаю, это вас в свое время удивило.

И с учетом этих особенностей нам уже давно было вполне очевидно, что крайне трудно создать какую бы то ни было единую модель доступа на одной платформе, ведь стороны, связанные договорными обязательствами, как субъекты, обладают такой правовой ответственностью.

Это значит, что, даже будь у нас политика на этот счет... я вижу, г-н Крокер к нам присоединился. Хочу заметить, Стив Крокер работает со мной уже три месяца. Стив, здравствуйте.

СТИВ КРОКЕР (STEVE CROCKER): Здравствуйте!

ЙОРАН МАРБИ: Как же приятно об этом сказать. Прошу прощения. Так что тут сложилось некое убеждение, что стороны, связанные договорными обязательствами, должны принимать решение в индивидуальном порядке.

И мы начали рассматривать разные решения, как сократить правовую ответственность сторон, связанных договорными обязательствами, когда дело касается WHOIS. Я не знаю, помните ли вы, как в Барселоне мне поступило письмо, мне кажется, почти от всех сторон, связанных договорными обязательствами, где они говорили: «Может быть, вам стоит оглядеться по сторонам и поискать потенциальное решение, которое позволит сократить правовую ответственность, чтобы сформировать единую модель доступа?»

Ведь если мы не поменяем то, как DPA сейчас интерпретируют закон, или не найдем [способ изменить] план игры, как вы знаете, очень сложно сформировать единую модель доступа, ведь мы не можем принудить корпорацию ICANN делать что-то, выходящее за рамки закона. ICANN всегда действует согласно закону.

Так что мы начали эти обсуждения на основании обсуждений также внутри Европейской Комиссии, о том, какие могут быть альтернативы, когда мы начали рассматривать возможность корпорации ICANN на правовых основаниях превратиться в инстанцию, которой вы можете задавать свои вопросы. И зародилась такая идея, она была, скажем так, основана на RDAP, что вы обратитесь с вопросом к корпорации ICANN, затем вопрос, согласно принципам GDPR, будет по безопасному каналу передан сторонам, связанным

договорными обязательствами. И только сторона, связанная договорными обязательствами, сможет дать ICANN ответ на этот вопрос.

С первого взгляда это может показаться так просто, но мы поняли, что нужны реальные технические знания, чтобы сформировать такую модель. И мы, вместо того чтобы просто сидеть в корпорации ICANN и создавать модель, я принял решение – мудрое, как мне кажется, – попросить Рама собрать группу технических специалистов, которые этим займутся.

И тут, разумеется, возникает вопрос, что случится после этой презентации? Во-первых, я с нетерпением жду ваших замечаний по поводу решения, которое они разработали.

Также, после этого мы планируем, так как это компонент большой системы, то это и точка обмена, скажем так. С этой точки зрения, должен быть кто-то, кто определит, у кого есть право задавать вопросы. Ну, [неразборчиво] общие положения называли центрами аккредитации.

И существует несколько центров аккредитации. В качестве примера могу привести Europol. Я знаю, что некоторые части этого сообщества занимаются поиском различных способов создания центров аккредитации. Довольно давно мы предлагали в качестве варианта WIPO.

Смысл в том, чтобы соединить такие центры аккредитации, которые подтверждают правомочность подателя заявки, который подтверждает правомочность вопросов с помощью этого [механизма, задает] вопрос, и он поступает сторонам, связанным договорными обязательствами.

То, как мы справились с этой работой, скажем так, соединило все эти элементы. Мы намерены вернуться к органам по защите данных и задать им простой вопрос: это сокращает правовую ответственность сторон, связанных договорными обязательствами?

Если ответ «да», и тут мы используем слово «указания», и если любой DPA это будет слушать, то указания в европейских реалиях по факту являются юридически обязательными к соблюдению, в том смысле, что если DPA дает письменный ответ на вопрос, это является элементом их процесса принятия решения. То есть у него больше силы. Вот подходящее слово, вот как я считаю. Орган по защите данных не может говорить что-то без такого правового контекста.

То есть идея в том, что у сообщества ICANN таким образом, если это произойдет, появится возможность создавать политики в отношении единой модели доступа. Кто должен иметь доступ, что мы думаем насчет конфиденциальности и доступа к информации?

Смысл всего этого не в том, чтобы захватить управление работой над политиками в ICANN, а в том, чтобы иметь возможность информировать сообщество ICANN о юридических возможностях существования единой модели доступа, или как мы это все назовем.

Хочу вас предупредить, что если вы обратитесь на сайт органов по защите данных, они вам скажут: «Мы не консультируем, вы сами должны поработать». Чтобы получить правовую консультацию в любом органе по защите данных, нам приходится прилагать огромные усилия, особенно в случае Еврокомиссии.

Нам одним из немногих все-таки предоставили хоть какие-то указания в ходе последнего... как мы его называем, «процесса [Кальцоне]». Для протокола: после этого мне запретили давать названия процессам в ICANN.

В общем, это один из проблематичных [неразборчиво]. Когда мы перешли на временную спецификацию, у нас действительно были правовые указания DPA. И помните, что в них говорилось. Там говорилось, что у нас было право, мы могли собирать данные. Не указывалось, какие именно, но говорилось, что мы можем собирать данные.

Также говорилось, что они принимают, что у нас есть некая модель, где какая-то информация открытая, а какая-то – закрытая. Так что для нас эти указания были

очень важными и ценными. Без них, мне кажется, работа [неразборчиво] DPA была бы гораздо сложнее.

Сейчас ситуация такова, что у нас нет таких правовых рекомендаций относительно второй фазы, так что именно этот вопрос мы и пытаемся решить. Предлагаю вам задать вопросы.

Вопросов нет? Мне внезапно стало так одиноко.

НЕИЗВЕСТНАЯ ЖЕНЩИНА: Один вопрос. Сокращения ответственности будет достаточно? Многие компании вложат в это миллиарды. Достаточно ли оснований, чтобы утверждать, что есть хотя бы вероятность, что их ответственность будет уменьшена? Разве мы не можем получить более четкий ответ о том, что для DPIA категорически не приемлемо?

ЙОРАН МАРБИ: Ага, если бы. Это зависит от DPA. Закон... GDPR – интересная вещь. Я был регулятором и, на самом деле, GDPR интересны с технической точки зрения. Наверное, у меня плохое чувство юмора, но однажды я назвал их законом [мамочки], потому что, когда я был подростком, мама всегда говорила мне: «Пойдешь гулять, но веди себя хорошо». И я шел гулять и хорошо себя вел, и, разумеется, она под хорошим поведением понимала совсем не то, что понимал я.

И когда ей рассказывали, что я плохо себя вел, мне попадало. Ну вот и закон такой же. Там сказано, поступайте как считаете правильным. Если вы сможете все объяснить, то все в порядке. А если не в порядке, то мы вами займемся.

Так что интерпретация тут может быть довольно разной. Это обусловливает один из недостатков этого закона: стороны, связанные договорными обязательствами, по сути должны принимать решение самостоятельно. И ICANN как юридическое лицо посредством своих контрактов с огромным трудом может обязать стороны, связанные договорными обязательствами, соблюдать это требование.

РУБЕНС КУЛ (RUBENS KUHL): Рубенс Кул, Сетевой информационный центр Бразилии. У меня комментарий и предложение. Комментарий такой: хотя одним из стимулов будет сокращение ответственности, у этой модели есть потенциал также сократить операционные издержки при работе с единой моделью доступа. Так что тут есть и положительные, и отрицательные стимулы.

Но я предлагаю ICANN не пытаться сделать эту модель принудительной. Все, к чему принуждают, обычно встречает отпор, в духе: «Зачем это? Почему все так, почему все эдак?» Но если это носит добровольный

характер, но получает широкий охват в пространстве gTLD, то оно может быть действеннее, чем принудительные меры, именно потому, что оно оставляет право выбора. Вот такая мысль.

ЙОРАН МАРБИ: [Неразборчиво], второй момент, вообще, у нас в ICANN, в наших контрактах, уже есть так называемое разрешение на отступление от требования, когда местное законодательство преобладает над нашими договорными обязательствами. Вы можете сказать, что это очень обширное разрешение на отступление от требования. По факту, это началось в 28 странах-участницах, плюс страны ЕЭЗ, ну и так далее.

ICANN не имеет и не должна иметь полномочий... мы не можем принуждать к соблюдению, если местное законодательство это запрещает. И я говорю это... вчера я слышал, что все это просто мечты. Да, но иногда мы говорили, что мы попробуем их воплотить в реальность.

Могу ли я говорить о 100-процентной вероятности? Нет. Но мне показалось достаточно важным рассмотреть возможности сокращения правовой ответственности сторон, связанных договорными обязательствами. И, разумеется, если они примут... так как они должны будут это принять, так как об этом говорит закон... рекомендация DPA должна иметь такую юридическую

силу, чтобы они были уверены в том, что кто-то за них примет это решение. Так что сложно [неразборчиво].

С другой стороны, ICANN как институт достаточно сильно опирается на добровольное участие. Наши контракты со сторонами, связанными договорными обязательствами, основаны на политиках, сформированных сообществом по принципу «снизу-вверх». В какой-то мере мы реализуем модель на основе консенсуса, а консенсус означает, что вы принимаете это. Но я понимаю, о чем вы говорите. Мы не правительство.

НЕИЗВЕСТНАЯ ЖЕНЩИНА: У меня несколько вопросов. Простите, я не принимала участие в EPDP, так что не знаю, рассматривались ли в нем эти вопросы. Мне хотелось бы узнать две вещи. GDPR дает конечным пользователям больше доступа для большей ответственности за свои данные. Вы можете мне сказать, если, например, конечный пользователь, владелец сайта, который хочет, чтобы люди, допустим, видели его информацию, в рамках новой модели, будет ли в ней графа, где указано, что информация открыта или что ее необходимо сохранять конфиденциальной? Это первый вопрос.

Второе, я слышала, как кто-то от регистратора вчера сказал даме, просившей доступ для потребителей, желающих проверить подлинность сайта, что, к

сожалению, так как регистраторы не могут различать физическое лицо и компанию, они и не собираются их как-то разделять. Правда ли, во-первых, что в новой системе не будет такого разделения физических лиц и компаний?

ЙОРАН МАРБИ: Вы спрашиваете о политике, это относится к PDP, многие из этих вопросов. Это вопрос о политике, и ни я, ни кто-то еще на этом заседании не участвуем в работе с политиками.

Я очень четко это разграничил, так как, по-моему, эти вопросы должны рассматриваться в рамках [последующей работы с политикой и в политике, в] первой или второй. Техническое решение затрагивает один конкретный аспект, и он в том, чтобы понять, можно ли уменьшить правовую ответственность сторон, связанных договорными обязательствами.

Я признаю факт... который делает ваш вопрос очень разумным... что может случиться такое, что у законотворцев, DPA, будет собственное мнение насчет существующего PDP, что может иметь последствия. Но пока что ответа у нас нет.

Законодательство тоже довольно новое, и крайне мало судебных прецедентов, чтобы [неразборчиво], что такое закрытые данные и конфиденциальные данные. Если

говорить по вашему первому вопросу, о том, можно ли предусмотреть полное согласие, если вам потребуется, то я, если честно, не знаю ответа на этот вопрос.

БЕНЕДИКТ ЭДДИС (BENEDICT ADDIS): Здравствуйте. Меня зовут Бенедикт Эддис, я тоже участник EPDP. И, если говорить сугубо с точки зрения EPDP, а не в качестве члена этой технической группы, могу вам сказать, что мы обсуждали идею о согласии, которое владелец зарегистрированного имени может дать на публикацию сведений о себе, очень много обсуждали. Эта возможность активно рассматривалась.

Ответ – скорее всего, да, это будет возможно. Но в данный момент – нет. Так что это пока у людей в мыслях. Ответ на ваш второй вопрос о разделении на юридических и физических лиц сложно дать по ряду причин. Наверное, одна из них в том, что на первый взгляд это все кажется относительно просто, но если разбирать поэтапно, то возникает множество сложностей. Например, есть организации, имеющие право на сохранение конфиденциальности в собственной стране согласно местному законодательству. Сами подумайте, такое право может быть у клиники, где проводят аборты.

То есть в этом вопросе есть фрактальные уровни сложности, и потому мы не ответили ни да, ни нет в рамках

EPDP, а отложили принятие этого решения на вторую фазу. Но спасибо за действительно хорошие вопросы.

РАМ МОХАН: Спасибо, Бенедикт, и спасибо вам, Йоран, и благодарим за вопросы из зала. И, по мере возникновения других вопросов о политике и прочих проблемах, призываем вас задавать их нам, а мы, как посредник, направим их в одну из групп, у которых могут быть адекватные позиции по этим вопросам.

Позвольте мне просто... да, Йоран.

ЙОРАН МАРБИ: Я послушаю оттуда.

РАМ МОХАН: Конечно. Спасибо.

ЙОРАН МАРБИ: Спасибо.

РАМ МОХАН: Хорошо. Давайте немного поговорим о том, что мы сделали и как мы начинали. Йоран рассказал вам о том, как все началось. Цель TSG, Технической группы по изучению, состоит в изучении технических решений на

основе RDAP для аутентификации, авторизации и предоставления доступа к закрытым регистрационным данным третьим сторонам с правомочными интересами. Такова цель.

У TSG есть устав. Все это указано в уставе. Если вы перейдете по URL, которая указана на экране перед вами, то сможете получить доступ ко всей этой информации.

И мы очень четко, как и говорил Йоран, и как мы попытались показать, мы четко сказали, что TSG не будет принимать какие бы то ни было решения или давать рекомендации по вопросам политики. Например, вопросы о том, кто получит доступ, даже что такое доступ, если это будут назвать доступом, какие поля данных при каких условиях будут открыты при предоставлении доступа, что такое правомочный интерес. Существуют мириады проблем, мы, на самом деле, рады, что они существуют, но в большинстве случаев не в нашей компетенции их решать. Мы сосредоточились сугубо на технических аспектах.

Итак, кто является членами TSG? Как мы сказали, спонсирует все это Йоран. Он попросил меня составить группу в прошлом октябре. Я потратил какое-то время на принятие решений, вы можете посмотреть фотографии, но, самое важное, вы сейчас видите большинство членов Технической группы по изучению перед собой. По-моему,

здесь нет только Мюррея от Facebook. Но остальные участники Технической группы по изучению сейчас перед вами.

Нам очень повезло, что работу волонтеров в TSG продуктивно поддерживали совершенно великолепные сотрудники корпорации ICANN, вы сейчас видите некоторых. Элиза, Диана, Джон Крэйн, Густаво. Также Франциско Ариас, но его здесь нет. Также Иветта и Эрика невероятно помогли нам в работе.

И когда мы начинали, мне было совершенно очевидно, что для того, чтобы добиться настоящих результатов, нужно основывать работу TSG на консенсусе, надо проявлять последовательность в процедуре и сосредоточиться на технической стороне. Это было основной моделью взаимодействия, которую мы применили в работе.

И, на самом деле, вот как мы организовали процесс для формирования модели, нахождения решения: сначала мы определили ключевые вопросы и моменты, которые нужно учитывать. Затем мы определили основные предположения. После этого мы определили сценарии использования и путь пользователя, а затем требования системы: функциональные, операционные, административные и так далее. Мы провели сопоставительный анализ функциональных требований,

сформировали ряд моделей участников, определили факторы, учитываемые при реализации.

Когда мы все это сделали, это позволило нам на очном совещании в прошлом месяце, это позволило нам сформулировать предлагаемое решение. И этот процесс был очень итеративным, мы рассмотрели несколько моделей, мы могли все проработать, посмотреть, что казалось подходящим и неподходящим, и в итоге нашли предлагаемое решение, которое назвали «технической моделью».

Следующий этап нашей работы... пока мы делали всю эту работу, разрабатывали техническую модель, изучали модели участников, факторы реализации и требования, всплыло несколько вопросов, их нужно было учитывать в этом пространстве, но было понятно, что эти факторы и наши наблюдения не относились к числу вопросов, по которым мы, как Техническая группа по изучению, были уполномочены принимать решения.

Мы занимаемся, если говорить о полноте информации и действительно качественного управления, мы принимаем к сведению все эти наблюдения и факторы, возникающие в ходе процесса, и они войдут в итоговый документ, который мы опубликуем, но все они адресованы и должны рассматриваться другими частями сообщества, но не Технической группой по изучению.

Когда мы это сделаем, нужно будет попросить сообщество предоставить обратную связь. Это одно из заседаний, на которых мы обращаемся к вам за обратной связью, и после этого, на этой неделе, Техническая группа по изучению планирует провести очное совещание прямо здесь в Кобе и ознакомиться с полученной обратной связью, чтобы понять, нужно ли нам вносить изменения или модифицировать модель, которую мы в итоге разработали.

Потом мы пару недель... еще три или четыре недели... посвятим дальнейшим циклам работы. И мы планируем завершить работу к середине апреля и опубликовать, как мы считаем, окончательные результаты своей работы, опубликовать их к концу апреля, представить их вам и сообществу и Йорану, а затем мы наконец получим право исключить пункт 13 из своего устава.

Так что, как я уже говорил, если посмотреть на то, что мы сделали, первое – мы определили ключевые вопросы и факторы, которые нужно учитывать.

Если вернуться на страницу ICANN.org/TSG, вы там найдете устав, а в уставе будут перечислены все эти основные категории и вопросы по каждой из них. Примерно 17 или 18 вопросов для различных категорий. Это позволило нам структурировать свои мысли и понять,

что нужно изучать, что нам нужно делать по всем этим направлениям.

Первая вещь, ставшая очевидной для нас, когда мы приступили к работе, – нам нужно предельно четко определить предположения, из которых мы исходим, ведь, конечно же, если их не определить, то некоторые ключевые области работы окажутся мертворожденными, они не получат никакого развития.

И мы начали, после этого процесса, первое, что мы сделали, мы составили перечень таких предположений. Мы их уточняли по мере циклирования процесса, то есть мы начали в ноябре, по-моему, с семи или восьми предположений, а после завершения этого процесса у нас оказалось гораздо, гораздо больше. Это хороший знак. Это значит, что мы признаем дополнительные проблемы.

Итак, я также хочу отметить, что когда мы говорим о предположениях, и в документе, и на слайдах, вы должны понимать, что мы не заявляем о том, что это единственно правильные действия, которые нужно совершить. На самом деле вы тут видите, что мы просто документируем, что эти предположения или предпосылки либо были озвучены, либо сложились в этом пространстве, и основа нашей работы состоит в том, что эти предположения соответствуют истине.

Итак, естественно, если какие-то из этих предположений не соответствуют истине или нуждаются в проработке и так далее, то это окажет влияние на саму модель, и я, разумеется, очень хочу наконец оказаться в вашем пространстве, в зале, послушать следующую группу и подумать, как же развить наше техническое решение.

Одним из важных элементов всего этого также является факт, что в наших полномочиях рассматривать актуальность предположений именно с технической точки зрения. Если вы видите предположения, которые мы выдвигаем, и видите элементы политики, или вы не уверены, что эти предположения на самом деле выдержат проверку, то у нас есть несколько заявлений.

Просим вас доводить вопросы до нашего сведения, но понимать, что мы не уполномочены предоставлять авторитетные ответы об уместности этих предположений. Мы хотим выяснить, соответствуют ли эти наши предположения, возможно, мы упустили какие-то из них, номер один, номер два, соответствуют ли наши предположения действительности или полностью ложны, что может подорвать релевантность технической модели.

Итак, вот наша концепция, и теперь я передаю слово вам, Стив, и прошу объяснить слайды с предположениями.

СТИВ КРОКЕР: Спасибо, Рам. Вы видите здесь изображение базовой концепции, что запросы на конфиденциальные данные gTLD пропускаются через шлюз ICANN, который использует и имеет доступ к учетным данным, применяемым для конкретного запроса, а также процессам аутентификации и авторизации.

Есть 12 предположений. На этом слайде шесть из них я указал в скобках, а на следующем вы увидите все 12. Базовая модель: нужно использовать механизм RDAP, соответственно, доступ через порт 43 будет аннулирован, доступ к закрытым данным gTLD только в режиме такого опосредованного доступа, запросы от не аутентифицированных источников обрабатываются согласно соответствующей политике, и ICANN осуществляет надзор за защитой учетных данных и связанной со всем этим достоверностью.

На этом слайде указаны все 12 предположений. Те, что сверху, мы только что рассмотрели, а те, что снизу, – это различные предположения, затрагивающие развитие и индивидуальную корректировку, а также сопутствующие проблемы, возникающие по мере проработки модели. Так что необходим процесс для работы с изменениями в наборах данных и правилах, он должен соответствовать нормальному использованию RDAP и эволюционировать до уровня существующих практик RDAP. Нужен пилотный

запуск, нужно отразить выбор, сделанный в рамках политики, и практические аспекты реализации.

Так что пришлось эту презентацию сделать очень сжатой и компактной. Подробности вы можете узнать из отчета. Слово вам, Рам.

РАМ МОХАН: Спасибо, Стив. Итак, сделав эти предположения, давайте перейдем к следующему слайду, мы приступили к определению сценариев использования. Я вам уже рассказал о процессе, который мы применяли. Так что следующим этапом нашей работы были сценарии использования. Энди, вы не против рассказать нам об этом этапе?

ЭНДИ НЬЮТОН (ANDY NEWTON): Разумеется. Итак, мы рассмотрели такие сценарии использования... и, опять же, это был итеративный процесс, то есть мы возвращались и уточняли результаты предыдущей работы, но мы хотели поговорить об авторизованных пользователях, тех, кому мог понадобиться доступ к такой информации. Правоохранительные органы, наверное, были пользователем, к которому мы постоянно возвращались, но были и другие: исследователи по вопросам безопасности, юристы, занимающиеся интеллектуальной

собственностью, и так далее. Но им требовался доступ в рамках множественных запросов или же им нужно было делать даже единичные однократные запросы.

Также мы сказали, что пользователи, получавшие авторизацию в режиме онлайн, должны получать авторизацию как можно скорее, а еще у нас был третий сценарий использования, когда мы предусматривали возможность некоторых пользователей получать доступ к данным, связанным с ними самими. И нам даже нужно поддерживать сценарии использования, когда аутентифицированный пользователь может быть не авторизован для просмотра данных.

И, наконец, мы говорили о пользователях, являющихся субъектом данных, и о том, как они получают доступ. Исходя из этого мы вдобавок еще и разработали требования к системе. Опять же, процесс был итеративным. Сначала мы рассмотрели различные компоненты системы и немного ее, скажем так, расширили. Но в общем, мы поняли, что это должно быть основано на интернет-стандартах, должно поддерживать IPv6, должно иметь распределенную структуру или поддерживать распределенную модель, и нам нужно использовать надежные протоколы, такие как TLS и прочие применимые протоколы защиты, которые могут использоваться с системами, которые мы сейчас формируем.

Тема, которую мы начали обсуждать сразу же, касалась веб-портала для людей, которым нужны расширенные или однократные запросы, все в этом роде. Так что у нас есть требования для веб-портала на базе браузера, которым должна управлять ICANN.

Мы говорили об аутентификации и авторизации. Мы разделили два эти понятия. Мы хотели, чтобы их, по возможности, делегировали квалифицированным агентам согласно политике ICANN. Затем мы обсуждали, как это следует воплотить на практике, и у нас появилась эта концепция шлюза RDAP, управляемого ICANN, через который запросы передаются сторонам, связанным договорными обязательствами, на их серверы RDAP. И мы сказали, что нужно обеспечить поддержку множества аутентифицированных источников запросов, их идентификации и различных сопряженных с этим политик.

Шлюз должен обеспечивать точечный доступ к различным элементам данных, должен поддерживать передачу атрибутов источника запроса сторонам, связанным договорными обязательствами, а когда кто-то получает несанкционированный доступ, нужно предусмотреть место, куда будет перенаправлен такой запрос. Нам необходимо также поддерживать возможность автоматизации.

Также были серверы RDAP под управлением сторон, связанных договорными обязательствами, и они, по сути, должны были отвечать на запросы, поступающие с шлюза RDAP ICANN.

Позвольте рассказать о более общих требованиях системы. У нас есть требования, касающиеся ведения документации и аудита тех источников, в которых будут документироваться эти запросы, как мы это видим. Нам нужна некая возможность хранения данных, и нам нужен способ согласования запросов ото всех этих сторон, чтобы мы могли проводить аудит и действовать в случае неправомерного использования системы.

Еще был такой аспект общих требований всей системы: мы проанализировали эффективность и соглашения об уровне обслуживания и сказали, что должны быть соглашения об уровне обслуживания для всех подсистем, ведь без этого мы не сможем понимать, в какой части системы происходит сбой. То есть должны быть некие гарантии в отношении происходящего.

Наконец, мы рассмотрели требования по защите информации и, собственно, сказали, что необходима оценка требований к защите, также необходим способ проведения аудитов и предоставления информации об аудитах запрашивающим сторонам. И, наконец, если

происходят нарушения, должны быть способы сообщать о таких нарушениях.

И, наконец, мы рассмотрели механизмы организационного управления и сказали, что управление должно происходить согласно программе управления бесперебойной деятельностью, и нужно обеспечить максимальную эффективность и современность всех методов криптографического хранения, используемых на сегодняшний день. По-моему, это все. Скотт, не хотите ли вы рассказать о самой модели?

СКОТТ ХОЛЛЕНБЕК (SCOTT HOLLENBECK): Разумеется. Спасибо, Энди. Итак, как понятно из названия слайда, мы предлагаем модель, которая основана на двух протоколах, опирающихся на стандарты – OAuth 2.0 и OpenID Connect.

Прежде чем я расскажу об этом слайде и засыплю вас техническими терминами, позвольте показать вам картинку. Это небольшая схема, показывающая поток данных, это некая эволюция схемы, которую вам показал Стив, но тут немного подробнее показаны взаимосвязи между пользователями и потоки между различными элементами данных.

Если вы знакомы с сервисами системы единого входа, такие места, куда вы отправляетесь, чтобы получить

доступ к веб-ресурсам, и вас просят войти через учетную запись Twitter, адрес Gmail или аккаунт Facebook, то вы понимаете принцип этой модели. Понятно, что тут больше тонкостей, но поток данных очень похож.

Давайте ненадолго вернемся назад, а потом продолжим с этим слайдом. Итак, есть пара предварительных условий, которые нужно выполнить, чтобы система единого входа могла работать. Во-первых, должны существовать такие поставщики дополнительных услуг. Должен быть некий процесс, чтобы обеспечить их появление, и, естественно, разработано ПО, чтобы эти сервисы можно было внедрить и обеспечить их работоспособность.

Источники заявок, этот термин мы позаимствовали в EPDP, чтобы называть людей, запрашивающих данные, должны располагать учетными данными, предоставленными им поставщиком идентификаторов. Такие поставщики идентификаторов – это новые участники. В их обязанности, помимо прочего, входит при предоставлении учетных данных обеспечивать привязку идентификационных атрибутов к учетным данным.

Преимуществом именно такого решения стало то, что оно сразу будет жизнеспособным и будет использовать сервисы, предоставляемые такими компаниями, как Google, Microsoft и Yahoo, которые поддерживают OpenID

и OAuth. Однако, выяснилось, что эти поставщики вообще ничего не знают о RDAP, поэтому у них пока не проводится привязка этих дополнительных учетных данных. Но скоро она начнется.

Так что после выполнения этих предварительных условий будет запущен весь процесс подачи источником заявки запроса RDAP в сервис доступа с использованием некоего клиентского приложения. Сервис доступа принимает такой запрос, и так как сервис доступа не знает, от кого запрос, он перенаправляет его на клиент для взаимодействия вот с этим так называемым поставщиком идентификаторов.

Далее человек видит некую веб-форму, предоставляемую поставщиком идентификаторов, в которую ему необходимо ввести свои учетные данные. Это могут быть имя пользователя и пароль, или будет поддерживаться использование клиентских сертификатов, если поставщик идентификаторов и клиент заранее договорились о таком варианте.

Но, просто чтобы не усложнять, скажем, что учетные данные проверены и подтверждены. И затем клиент или человек видит запрос для выбора различных фрагментов идентификационных данных, тех самых атрибутов, о которых мы говорили, и подтверждения своего согласия на предоставление этой информации главной стороне

или организации, тому сервису доступа, который управляет доступом к этой защищенной информации.

Источник запроса отвечает, заполняет все эти формы, нажимает кнопку отправки, и поставщик идентификаторов в ответ направляет так называемый код авторизации на клиент, а затем снова перенаправляет запрос, переадресацию http на так называемый сервис доступа, где запускается процесс формирования запроса RDAP.

Сервис доступа берет код авторизации и с его помощью извлекает непрозрачные куски данных, которые называют токенами, из хранилищ поставщика идентификаторов. Эти токены возвращаются клиенту. И именно в этих токенах содержится информация об идентификаторе, привязанном к источнику запроса, и некоторая информация, указывающая на авторизацию.

На клиенте есть токены, и они отправляют запрос RDAP с информацией в токенах на шлюз RDAP ICANN. А затем шлюз получает эту информацию и тогда начинает обработку самого запроса RDAP.

Шлюз получает запрос и токены, а затем отправляет оба куска информации в систему авторизации третьей стороны для проверки подлинности. В системе авторизации происходит обработка этих входных данных, проверяется достоверность идентификационной информации, соответствие запроса атрибутам, после

чего результаты проверки подлинности передаются на шлюз. Тут обычно бывают ответы типа «Да, можно продолжать» или «Нет, этот человек не авторизован для подачи подобных запросов».

Предположим, что мы авторизованы. В этом случае шлюз отправит запросы RDAP на серверы RDAP соответствующих сторон, связанных договорными обязательствами, это будут или регистраторы или регистратуры, по ситуации, для сбора всех закрытых данных, шлюз обрабатывает и фильтрует эти ответы для формирования полного ответа RDAP, который возвращается клиенту, а затем клиент отображает результаты источнику запроса.

Опять же, вот картинка, где все это показано. Некоторые основные потоки данных. Передаю слово остальным.

РАМ МОХАН: Спасибо. Скотт, не могли бы вы задержаться и показать, где поставщик аутентификации, где сервис авторизации, мы намеренно их разделили, показали их по-отдельности, и, мне кажется, было бы крайне полезно... у нас вчера была пара вопросов о том, стремимся ли мы их все объединить в одну группу, или возможно их распределение, вот такие вопросы. Поэтому, думаю, будет полезно об этом сказать.

Также у нас возникла дискуссия по поводу вот этой идеи о поставщике идентификаторов и о том, что это за роль.

СКОТТ ХОЛЛЕНБЕК: Конечно, Рам, без проблем. Да, те из вас, кто знаком с нынешними принципами работы WHOIS – а это, я так полагаю, практически все присутствующие – узнают как минимум двух участников этой модели. Клиента и серверы RDAP регистратора/регистратуры.

Ну, эта модель не так эффективна, если приходится принимать решения об идентификации, аутентификации и контроле доступа. И тут могут пригодиться те самые сервисы на базе стандартов. OpenID Connect и OAuth 2.0 разработаны для того, чтобы у нас были методы корректной идентификации клиентов, их аутентификации и принятия решений о предоставлении доступа на основании атрибутов, привязанных к их идентификаторам.

Но это означает, что нам нужно добавить промежуточных игроков в этот процесс, и первым таким игроком будет вот такой сервис доступа RDAP ICANN. В группе, между собой, мы называем его «посредник». Если вы знаете, как работают посредники, то здесь именно тот случай. Это брокер. Он получает запросы, затем решает, кого нужно вовлекать в процесс и как правильно перенаправить запрос.

Но первоочередная задача, которую должен выполнить сервис при получении запроса, – он должен узнать, с кем разговаривает, а для этого он и обращается к такому поставщику аутентификации и такому сервису авторизации.

И с учетом особенностей работы протоколов, эти услуги может оказывать одна организация, которую иногда называют поставщиком идентификаторов, или же эти функции можно распределить среди разных участников. Модель, которую мы описали, поддерживает оба способа работы и, по сути, вопрос о том, как именно будет выполнено разделение и какой участник какие функции будет выполнять, скорее всего будет решен уже в рамках политики.

Но, как вы видите из показанных взаимосвязей, поставщик аутентификации получает запрос от сервиса RDAP. По факту сам он не взаимодействует с клиентом. Это веб-интерфейс, о котором я уже рассказал. Именно тут клиент сообщает свои учетные данные. Их ему выдает именно поставщик аутентификации, поэтому он и может проводить аутентификацию, и сервис RDAP никогда не будет взаимодействовать с такой информацией. Он просто получает подтверждение от поставщика аутентификации о том, прошел клиент полную проверку идентификаторов и аутентификацию или нет.

Но тут мы подходим к сервису авторизации. Когда сервис доступа RDAP понимает, что взаимодействует с кем-то, кто надлежащим образом идентифицирован и аутентифицирован, ему требуется принять решение о том, обладает ли источник запроса необходимым уровнем доступа, чтобы видеть данные, которые запрашивает. И, как я сказал, стандартно такая функция предусмотрена в OAuth, она выполняется поставщиком идентификаторов, но у нас есть возможность отделить эту функцию и поручить ее службе третьей стороны. В этой модели мы показываем такую возможность, и она работает так: отправляется запрос, выполняется сравнение согласно тем же политикам, которые еще предстоит сформировать, и ответ типа «можно/нельзя» возвращается в сервис, который потом действует согласно этому ответу при формировании и отправке запросов на серверы RDAP сторон, связанных договорными обязательствами. Вам достаточно подробностей, Рам?

РАМ МОХАН: Да, отлично. Спасибо, Скотт. Еще одно: был вопрос по поводу этой предусмотренной службы доступа RDAP ICANN, предполагает ли наша модель, что если данные находятся в разных источниках, будет ли ICANN включать копию этих данных в эту модель или нет. Стоит об этом сказать.

СКОТТ ХОЛЛЕНБЕК: Разумеется. Данные в этой модели остаются в авторитативных источниках. Я должен пояснить, что значит «авторитативный», так как, я знаю, что в политике по расширенному варианту записи данных WHOIS, к примеру, говорится, что регистратура – «авторитативный» источник данных.

Мы используем несколько иной подход, и под «авторитативным» подразумеваем орган, у которого есть отношения с субъектом данных. То есть это вопрос происхождения, ближайшей точки к месту сбора данных или месту их генерирования.

Это одна из причин, почему вы здесь видите разделение функций регистратуры и регистратора. Регистраторы будут поддерживать актуальность данных, в отношении которых они авторитативны. Служба RDAP ICANN не поддерживает актуальность копий данных. Данные передаются через службу так, чтобы их можно было обработать, но не ведется никакая документация, кроме журналов доступа. Сами данные не копируются, их актуальность не поддерживается, они не кэшируются. Здесь речь лишь о передаче и не более того.

РАМ МОХАН: Большое спасибо. Я знаю, вы все пытаетесь передать мне слово. Но я хотел бы подольше поговорить на эту тему, ведь именно ради этого нашу группу и

сформировали. Еще задавался такой вопрос, Скотт, эта служба доступа RDAP ICANN, вопрос касался нашей модели, мы ожидаем, что это все будет происходить централизованно? Мы ожидаем, что для этого будет использоваться только сайт, или же у нас есть другие автоматизированные механизмы? Это первое. А второе, если не аутентифицированный и, возможно, даже не авторизованный запрос поступает в отношении открытых или конфиденциальных данных, и эти данные не относятся к gTLD, каков наш план, что мы предусматриваем в такой ситуации? Есть начальная загрузка, переадресация, это тоже может оказаться чем-то полезным.

СКОТТ ХОЛЛЕНБЕК: Разумеется. Что ж, служба доступа RDAP, ее мы себе представляем как веб-интерфейс, но с двумя лицами. Как говорил Энди, нам требуется автоматизированный онлайн-доступ, но также требуется асинхронный доступ, то есть, например, если у кого-то даже нет учетных данных, но есть правомочные основания запрашивать информацию. Тут будет некая поддержка клиента, возможно, заполнение веб-формы, и эта форма будет проходить проверку и обработку, а ответ будет направлен каким-то другим способом.

Но как веб-служба, служба доступа RDAP может быть реализована любыми способами, которыми обычно реализуются веб-службы. Необязательно один сервер. Разумеется, можно это распределить по нескольким точкам, чтобы решить такие задачи, как, например, балансировка нагрузки. Тут вопрос только в оптимальных практиках поддержки служб http.

Функции поставщика аутентификации и сервиса авторизации можно централизовать, но их же можно и распределить. А модель, которую мы, скажем так, продвигаем, не предполагает централизации функций, наоборот, в ней они распределены надлежащим образом. Крайне логично, чтобы эти функции выполняли органы, у которых есть отношения с источниками запросов, так как эти органам известно, кто такие эти источники запросов. Например, они могут выдавать такие учетные данные и принимать адекватные решения об аутентификации идентификаторов на основании ранее имевшихся отношений.

И, если говорить об открытых данных, вы увидите, что тут есть такой момент, как ожидания, что стороны, связанные договорными обязательствами, предусмотрят у себя интерфейсы общего пользования для открытых данных, чтобы клиенты могли отправлять запросы напрямую в регистратуры и регистраторам. А в ответ они будут

получать такие данные, которые согласно политике будут считаться открытыми. Я ответил на вопрос?

РАМ МОХАН: Да.

СКОТТ ХОЛЛЕНБЕК: Хорошо. Спасибо.

НЕИЗВЕСТНЫЙ МУЖЧИНА: Если позволите, в нашем документе мы рассматриваем разные комбинации разбиения или сочетания поставщиков идентификаторов и тех, кто выносит решение об авторизации, и мы это называем моделями участников. И у нас есть набор комбинаций, фактически описываемых в документе. По-моему, их там четыре.

Еще есть такой момент, касающийся не аутентифицированных или не авторизованных пользователей, в целом, мы просили, чтобы шлюз RDAP ICANN, когда на него поступает запрос от таких пользователей, работал скорее как стандартный сервер начальной загрузки RDAP, чтобы он мог выполнить переадресацию на уровне HTTP на источник, который указан в файлах начальной загрузки IANA.

Одна из причин, почему мы об этом просили, – RDAP применяется не только в контексте gTLD ICANN, но и в других контекстах типа RIR, а также пространстве ccTLD.

РАМ МОХАН: Спасибо. Спасибо, Скотт. Я передаю слово вам, Гэвин. Расскажите, пожалуйста, о факторах, которые нужно было учитывать.

ГЭВИН БРАУН (GAVIN BROWN): Спасибо, Рам. Да, и Рам уже говорил об этом вначале, но я все-таки повторю. Продвигаясь в своих обсуждениях, мы выявили ряд вещей, которые, как нам кажется, до начала нашей работы еще не до конца сформировались. И нам их решение показалось выходящим за круг наших полномочий, так как мы уделяем пристальное внимание техническому решению, и нас не слишком интересовало участие в работе над политикой.

Так что я просто скажу о них в общих чертах. Им посвящена пара слайдов. Мы их рассмотрим.

Мы уже вкратце обсудили хранение данных. Как уже сказали, мы не предполагаем, что шлюз доступа будет хранить данные о регистрации, говоря на жаргоне, это обратный прокси-сервер, но не кэширующий. Он ничего не хранит, он просто передает все, что получает с серверов сторон, связанных договорными обязательствами.

Но все же будут сохраняться определенные элементы данных. Например, ключевым элементом станут журналы. И мы понимаем, что с этими журналами могут быть сопряжены риски и ценность, и что с точки зрения политики будет разумно применять к этим журналам правила хранения данных, и это стоит предусмотреть.

Очевидно, в системе должны быть различные вещи, которые позволят, например, обеспечить... мы поговорим о транспарентности на следующем слайде. Важно иметь возможность проводить аудит системы, чтобы контролировать надлежащий порядок работы. Поэтому регистрация в журналах – это залог возможности аудита, но также есть и потребность сначала сократить риск разглашения, ведь тот факт, что кто-то направил запрос, уже может быть ценной информацией сам по себе, и поэтому крайне важно иметь политику по сокращению риска разглашения подобной информации.

Также ранее говорили о соглашениях об уровне обслуживания. Разумеется, будет ряд зависимых сторон. В описываемой нами модели есть ряд потенциально автономных органов, каждый из которых зависит от доступности сервисов других таких органов при выполнении своих функций в системе. Очевидно, в конечном счете, есть конечные пользователи системы, источники запросов, которые также зависят от доступности этой системы при выполнении необходимых

им действий и правомочном обращении для получения доступа.

Так что мы пришли к заключению, что необходимо определить ряд соглашений об уровне обслуживания и внедрить их, чтобы гарантировать доступность и стабильность системы.

Также мы рекомендовали корпорации ICANN обеспечить транспарентность с точки зрения действенности этих соглашений об уровне обслуживания, например, предусмотреть некую страницу статуса, на которой источник запроса может сразу увидеть статус системы.

Нам показалось, что важно, чтобы ICANN проанализировала потенциальные последствия того, что она возьмет на себя ответственность за управление подобной системой, особенно учитывая ее роль как координирующей стороны, пункты три и четыре в этом списке можно сложить вместе.

Очевидно, есть юридические риски, но также и операционные риски потенциально крупных масштабов. Опять же, в зависимости от того, каким будет решение в рамках политики о методе развертывания системы, есть и ряд других рисков, которые нужно учитывать. Очевидно, мы уже сказали о рисках, связанных с безопасностью информации.

И нам было важно обратить внимание корпорации ICANN и сообщества ICANN, что должны проводиться определенные проверки и оценка, чтобы понять, как работать с этими рисками.

Нам действительно показалось важным обратить внимание на проблему сокращения ответственности сторон, связанных договорными обязательствами. Мы, конечно, просто технари, далеко не юристы, и не можем ответить, действительно ли система, которую мы предлагаем, обеспечивает сокращение ответственности. Но нам кажется важным призвать стороны, связанные договорными обязательствами, высказывать собственные точки зрения, уверен, они так и поступят.

Вкратце насчет транспарентности. Мы определенно считаем, что ключевым фактором обеспечения доверия к системе будет активное стремление ICANN, если она решит взять на себя управление такой системой, обеспечивать транспарентность методов управления и использования этой системы. Очевидно, мы не говорим, что конкретные запросы нужно публиковать или раскрывать, но статистическая информация о том, как используется система, мне кажется, будет ключевой точкой данных, обеспечивающей хорошую репутацию системы, поэтому мы предлагаем регулярно составлять отчеты о транспарентности для соблюдения интересов сообщества.

И, наконец, мы также признаем, что процесс авторизации любого рода завершается неким результатом, и источник запроса может быть не согласен с этим результатом, и поэтому необходимо внедрить механизм обработки жалоб, чтобы жалобы насчет процессов или проблем в системе можно было получать, переводить их рассмотрение на необходимый уровень и разрешать в рамках процесса обработки жалоб, и сюда, вероятно, также войдут запросы об удалении согласно статье семь GDPR и подобных законов, когда субъекты данных могут обратиться в ICANN и потребовать удалить данные о себе. Рам.

РАМ МОХАН: Спасибо, Гэвин. Вы не могли бы переключить на следующий слайд, или у нас опять самообслуживание? Отлично. Спасибо. И на этом мы в целом завершаем свои заранее подготовленные комментарии к сегодняшнему заседанию. Мы работаем точно по плану. Предусмотрен вклад сообщества, и мы надеемся, что вы его нам предоставите до этой среды, и, на самом деле, даже после среды, но нам очень нужны ваши отзывы и замечания. Мы хотели бы их проанализировать и включить в техническую модель. Мы планируем еще несколько телеконференций и одно очное совещание в середине апреля, чтобы окончательно оформить результаты своей работы, и планируем опубликовать

итоговую техническую модель 23 апреля. Когда мы это сделаем, эта группа будет расформирована, и наша задача будет выполнена.

На этом, думаю, можно перейти к вашим вопросам. Вижу, уже кто-то готов. Если есть другие вопросы, прошу вставать в очередь. С обеих сторон есть микрофоны, и я постараюсь руководить процессом максимально эффективно. Сэр.

РУБЕНС КУЛ: Скажите, группа рассматривала такой сценарий, когда ICANN будет предоставлять токен только с использованием OAuth и OpenID, после чего клиент будет напрямую спрашивать сторону, связанную договорными обязательствами? Так как это предотвратит поток данных через системы ICANN. Это бы предотвратило большую часть проблем, связанных с SLA. И пусть это не кэширующий прокси-сервер, все равно несанкционированный доступ на прокси-сервер приведет к утечке данных.

То есть была возможность не делать поток данных централизованным, но ее почему-то не использовали. По какой причине?

ЭНДИ НЬЮТОН: Да, мы это обсуждали. Причина, почему мы не пошли по этому пути, – когда мы рассматриваем механизмы распространения политики среди всех сторон, связанных договорными обязательствами, вы в этом случае возлагаете гораздо более тяжелое бремя на эти стороны, вынуждая их соблюдать и постоянно обновлять политику. Нам показалось, что проще сделать корпорацию ICANN таким местом фильтрации политики. Вот причина, по которой мы выбрали эту модель, это упрощенная модель по сравнению с получением доступа [неразборчиво] напрямую сторонам, связанным договорными обязательствами.

Что же касается SLA, не думаю... я не знаю, думает ли так кто-то в этой группе... что это по факту меняет какие-либо SLA в принципе.

РУБЕНС КУЛ: Даже при наличии централизованной платформы политики в ICANN поток данных можно было не централизовать. Поэтому одно решение не должно никак влиять на другое.

ЭНДИ НЬЮТОН: Я понимаю, что вы имеете ввиду, но если говорить о SLA, по-прежнему будет составлено SLA для ICANN, любых служб, которыми управляет ICANN. Так что, полагаю, что

проблемы с SLA никак не меняются, какой бы тип системы мы ни выбрали.

ГЭВИН БРАУН: Если позволите добавить, по-моему, использование ICANN как единой точки доступа также разрешает некоторые сомнения, о которых нам сообщали правоохранительные органы, что они не хотят, чтобы слишком много информации об их собственных запросах передавалось сторонам, связанным договорными обязательствами. Может, Бенедикт нам расскажет об этом или Стив. Но, по-моему, когда мы это обсуждали, было одно соображение, которое для меня стало самым ключевым, что от правоохранительных органов поступило четкое замечание о том, что, хотя они не возражают против соображений о транспарентности, есть опасения, что... тот факт, что конкретный правоохранительный орган или конкретное должностное лицо в правоохранительных органах, что они направляют запрос, и это становится известно регистратору, этот факт вызывает у них обеспокоенность.

БЕНЕДИКТ ЭДДИС: Я буду немного более осторожен, и скажу, коллеги из EPDP во второй фазе, прямо сейчас мы активно обращаем ваше внимание на этот факт, так как нужен некий баланс между использованием псевдонима в

запросах, когда все запросы останавливаются в ICANN и ICANN несет ответственность за регистрацию в журналах, и большей степенью раскрытия данных, меньшей степенью в отношении сторон, связанных договорными обязательствами, и это должно обсуждаться в рамках дискуссии о политике, которую правоохранительные органы должны провести со сторонами, связанными договорными обязательствами, насчет анонимности запросов или использования псевдонимов и возможности сторон, связанных договорными обязательствами, видеть, кто подает запрос, что может сыграть свою роль в увеличении ответственности. Но это совершенно вне нашей компетенции, если вас такой ответ устроит.

РАМ МОХАН: Спасибо.

БЕНЕДИКТ ЭДДИС: Есть еще одно преимущество: с точки зрения транспарентности, централизованная служба позволяет вам вести журналы и составлять отчеты о транспарентности, а это, думаю, все согласятся, очень хорошо.

РАМ МОХАН: Спасибо. Участник слева от меня.

КЛАУС ШТОЛЛ (KLAUS STOLL): Большое спасибо. Клаус Штолл, [неразборчиво] Group. Только краткое замечание и предложение. Факты под номером шесть, транспарентность, может быть, вам следует упомянуть научно-исследовательскую деятельность, так как многим будет очень интересно, а это выходит за рамки статистики. Было бы неплохо, если бы об этом тоже сказали. Спасибо.

РАМ МОХАН: Большое спасибо. Мы примем это к сведению и обсудим.

ВИТТОРИО БЕРТОЛА (VITTORIO BERTOLA): Здравствуйте. Витторио Бертола из [неразборчиво]. Кажется, у меня был очень похожий вопрос. Я хотел понять, почему вы действительно хотите внедрить централизованную систему [посередине], в частности, является ли это техническим решением, то есть вы пришли к такому техническому решению, что с технической точки зрения так будет лучше, или это политическое решение, ведь с технической точки зрения, если бы я что-то подобное создавал, мне кажется, что-то децентрализованное было бы гораздо лучше, просто децентрализовать [неразборчиво] и передачу, чтобы их подлинность могли проверять стороны, связанные договорными обязательствами, и мы можем об этом побеседовать. Я даже мог бы составить ряд предложений, если хотите.

Но с другой стороны, когда был задан вопрос, две причины, которые я услышал, были политическими, что мы хотим все отслеживать ради транспарентности, или что правоохранительные органы хотят, чтобы мы работали как посредник, чтобы стороны, связанные договорными обязательствами, не видели, что они запрашивают. Это все политические решения.

Но в своей презентации вы сказали, что не можете сказать, лучше ли они с точки зрения политики или правовой ответственности сторон, связанных договорными обязательствами. И теперь я немного не понимаю, пытаетесь ли вы решить техническую проблему, предлагая оптимальное техническое решение, или у вас есть ряд политических требований, которые делают такую централизованную структуру необходимой, и в таком случае что это за требования и можно ли их обсудить?

ГЭВИН БРАУН: Да, я с вами согласен, насчет некоторых ответов вы можете сказать, что там замешана политика. Но у нас были достаточные технические основания, а именно мы стремились сократить техническую и операционную сложность системы.

Распространение политики и возложение на стороны, связанные договорными обязательствами, обязанности постоянно обновлять политику и понимать, как ее нужно

формулировать и как ее нужно распространять, каким бы вы способом это ни сделали, – это сложное техническое мероприятие, и одна из причин, почему мы поступили так, как поступили, – мы пытались сократить сложность, техническую сложность системы.

Второе, и я об этом еще не говорил, – и мы это включили в документ – способ, которым мы все это определили, предполагает, что стороны, связанные договорными обязательствами, должны просто использовать взаимную TLS, чтобы понимать, кому верить, а если бы мы внедрили механизмы управления доступом с помощью токена, который клиент просто напрямую передает сторонам, связанным договорными обязательствами, то это бы усложнило задачи, которые предстоит решать сторонам, связанным договорными обязательствами.

РАМ МОХАН: Спасибо. Сэр.

АЛЕКС ДИКОН (ALEX DEACON): Спасибо. Да, я хотел задать вопрос, связанный с вопросом Рубена, он касается конкретно требований системы 4 E и 4 F, где сказано о передаче атрибутов и информации идентификатора сторонам, связанным договорными обязательствами. И по-моему, там явно

указано, что это политика. Я думаю, вы тут переходите к разделению политики и технологии.

И мне интересно, если бы приняли решение, что мы выбираем модель два, и мне кажется, это правильное решение, и эта модель описывает ICANN как единственную систему авторизации, то мне непонятно, зачем мы будем отправлять эти данные сторонам, связанным договорными обязательствами. Не могли бы вы предоставить некий контекст, основания, почему эти требования... я не говорю, что они плохие или хорошие, и не возражаю против них, мне просто интересно понять ход мыслей, почему в итоге эти требования [неразборчиво].

ЭНДИ НЬЮТОН: Да. Хороший вопрос. Требования в том, что в системе должна быть возможность это делать, располагать такими идентификаторами и атрибутами источника запроса, и она должна иметь возможность поддержки их передачи сторонам, связанным договорными обязательствами, если этого требует политика.

То есть не говорилось, что политика именно в этом. Вот что мы тут пытаемся донести. Речь о такой функции системы, которая позволит это сделать, если некая новая политика того потребует.

АЛЕКС ДИКОН: Я понял, то есть, если согласно политике это все должно будет происходить на этом прокси-сервере ICANN, то эти атрибуты не понадобится вносить. Система должна поддерживать такую возможность, но мы ее не будем использовать.

ЭНДИ НЬЮТОН: Именно. У нас должна быть возможность ее поддерживать, вот почему у нас четыре разных модели участников. Но мы не знаем пока, какую лучше всего использовать и не будет ли их сразу несколько. Поэтому сегодня мы их показали так, как показали.

АЛЕКС ДИКОН: Хорошо. Спасибо.

РАМ МОХАН: Спасибо.

НИЛ МАКФЕРСОН (NEAL MCPHERSON): Здравствуйте. Нил Макферсон от 1&1 Ionos. У меня вопрос по историческим данным. По-моему, Стив говорил, что весь процесс не обязательно должен проходить в реальном времени, будут такие сценарии использования, когда потребуется отвлечься, собрать запросы, информацию и тому подобное, и все это может занять долгое время. Так есть ли временная метка или

что-то подобное, что вы должны предоставить данные сегодня или вчера или когда запрос поступил в первый раз? И по поводу запросов, множество запросов, которые мы получаем, выглядят как «привет, а кто владелец домена [неразборчиво]».

РАМ МОХАН: Не могли бы вы ближе подойти к микрофону? Я расслышал сценарии использования, исторические данные, а дальше приходится догадываться, а я бы предпочел этого не делать.

НИЛ МАКФЕРСОН: Ладно. Так намного лучше. По поводу временных меток, да, процесс может выйти за [рамки], занять долгое время. Какие временные метки данных WHOIS или данных RDAP вы должны выдавать на основании процесса, который не происходит в режиме реального времени? И еще я сказал, что у нас много запросов на исторические данные. Как это учитывается в процессе, когда источник запроса говорит, что ему нужны данные полугодовой давности, кто тогда был владельцем домена.

ЭНДИ НЬЮТОН: Ну, я работаю в ARIN, и у нас есть такая штука «WHOWAS», то есть «Покажите, как регистрационные данные выглядели шесть месяцев назад» и тому

подобное. Мы обсуждали такие вещи, как массовые сервисы WHOIS, WHOWAS, и мы их, скажем так, исключили из рассмотрения, по крайней мере на данный момент, так как это все настолько усложняет, что мы уже не можем понять, входит это в нашу компетенцию или нет.

Но мы эти вещи обсуждали, и решили, что нет, давайте пока их отложим. Я ответил на ваш вопрос?

НИЛ МАКФЕРСОН: Спасибо. Да.

РАМ МОХАН: Следующий вопрос, пожалуйста.

ГРЕГОРИ МУНЬЕ (GREGORY MOUNIER): Привет, это Грег Мунье из Europol, я хочу задать вопрос, относящийся к этому, но насчет другой функции, которой постоянно пользуются следователи, 80% их работы, и это обратный поиск. Если кто-то не знает, что это, то в целом это возможность перекрестных ссылок или определения всех доменов, которые были зарегистрированы с указанием конкретной информации. Допустим, адреса или имени владельца домена.

В ваших отчетах я прочитал, что технически это можно обеспечить, но по какой-то причине, которую я не понял, TSG не сказала, что это нужно разработать. И мой первый

вопрос: что заставило бы вас включить этот момент в свое исследование? Ну и какова причина, почему это не вошло в исследование. Спасибо.

ЭНДИ НЬЮТОН: Да, в общем-то главная причина, почему этого здесь нет, – обратный поиск не является частью RDAP на данный момент. В IETF есть проект, и его будут обсуждать в Праге через две недели, касающийся обратного поиска, и это просто никогда не входило в RDAP, начнем с этого.

Помимо того, что говорится в проекте, и как это будет обеспечено, есть вопросы о том, как вы будете обеспечивать сбор таких данных ото всех сторон, связанных договорными обязательствами, в пространстве. Вы хотели что-то сказать, Бенедикт? Да, вот по этой причине мы это не рассматриваем.

ГРЕГОРИ МУНЬЕ: Если позволите, я думаю, что будет очень жаль, если в итоге, в политике будет сказано, что да, вы это можете сделать, и с технической стороны мы скажем: «Ой, а мы это почему-то даже не рассматривали». Так что было бы хорошо, если бы в итоге мы реально могли это сделать с технической точки зрения.

РАМ МОХАН: Спасибо. Мы к вам вернемся через минуту, оставайтесь у микрофона. Сейчас 2:46. 11 марта 2011 года в 2:46 по местному времени землетрясение силой 9,1 балла произошло в Тихом океане недалеко от северо-западного побережья японского острова Хонсю.

Землетрясение, известное как Великое восточнояпонское землетрясение, вызвало крупный цунами с волнами высотой до 40 метров, которые прошли расстояние до десяти километров по суше.

Это было самое мощное землетрясение, зарегистрированное в Японии за все время, и четвертое по силе землетрясение во всем мире.

По оценкам, 20 000 человек погибло и 500 000 человек пришлось эвакуировать. В память о жертвах Великого восточнояпонского землетрясения мы объявляем минуту молчания.

Спасибо. Энди, вы хотели бы ответить на второй вопрос?

ЭНДИ НЬЮТОН: Извините, я потерял мысль. Какой был второй вопрос?

ГРЕГОРИ МУНЬЕ: Это был не второй вопрос, скорее заявление, что будет очень жаль, если технически это окажется невозможным, в то время как политика объявит это возможным.

ЭНДИ НЬЮТОН: Надеюсь, функции RDAP, которые он приобретет в будущем, окажутся полезны для этого. Да. Это может стать вопросом политики. Некоторые технические аспекты могут потребовать доработки, но да, будет хорошо, если в будущем мы это обеспечим, если сообщество решит, что ему это нужно.

РАМ МОХАН: Спасибо.

СЕВЕРИН УОТЕРБЛИ (SÉVERINE WATERBLEY): Здравствуйте. Добрый день. Это Северин Уотербли из Бельгии. Я являюсь членом GAC. Если я правильно понимаю, ICANN будет пунктом обработки, как это понимается в GDPR, а службы авторизации будут пунктом обработки для пункта обработки. То есть предусматриваются ли договорные отношения между регистратурами и службами для предоставления нам авторизации или аутентификации? Спасибо.

РАМ МОХАН: По-моему, очень хороший вопрос, но не думаю, что мы уполномочены на него отвечать. Но мы все-таки можем сделать следующее: чтобы этот вопрос не затерялся, мы внесем его в протокол и обязательно передадим коллегам в корпорации ICANN, так как правовым

аспектам всего этого мы не уделяли свое время, во всяком случае уделяли не так много времени и сил.

БЕНЕДИКТ ЭДДИС: [И это достаточно активно обсуждается в EPDP.] И опять же, если я буду говорить как член EPDP, то мы проводили много обсуждений реальной природы юридического соглашения внутри ICANN и сторон, связанных договорными обязательствами. И я знаю, что юридический отдел ICANN высказал свое мнение по этому вопросу. Думаю, что в EPDP, особенно во второй фазе, что довольно удобно, пройдут обсуждения, в этом же самом зале, через 40 минут.

ТИМ ЧЕН (TIM CHEN): Хорошо. Спасибо. Тим Чен из DomainTools. Прежде всего, спасибо за проделанную работу. Думаю, крайне полезно учитывать технические реалии воплощения всего этого в жизнь параллельно с разработкой политики, поэтому мои аплодисменты вам, как и всем волонтерам, за работу. Поэтому спасибо вам за ответ.

Всего два коротких технических вопроса. Первый: внизу одного из первых слайдов с факторами, которые необходимо учитывать, было примечание, где упоминался, если не ошибаюсь, термин «запросы многократного использования». Я хотел бы узнать, что

это значит. Это было вначале... Рам, может быть, в ходе вашего выступления... или сразу же за ним. Там был длинный список, 13 вроде. Да, вот оно: запросы многократного использования. Извините.

Вы не могли бы объяснить, что это, внизу слайда?

РАМ МОХАН: Разумеется. Ну это было еще на этапе начальной разработки. Мы тогда рассматривали различные формы, которые может принимать запрос на данные. Одна форма может быть, когда сторона авторизована только для доступа к одному элементу данных один раз, а в других случаях, возможно авторизация более долгосрочная, но опять же, она долгосрочная лишь для одного класса запросов или для доступа только к конкретному количеству элементов данных.

На том этапе обсуждений мы еще не понимали, что следует ограничить модель только до однократной обработки запроса на один элемент данных и один раз для одного объекта, как в долгосрочном, так и в кратковременном формате. Вот об этом все вопросы, касающиеся запросов многократного использования.

ТИМ ЧЕН: Хорошо. Спасибо. Если позволите, еще вопрос. Служба начальной загрузки упоминалась вчера на вашем

совещании со сторонами, связанными договорными обязательствами, и потом уже сегодня. [Я не технический специалист,] я попробовал обратиться к RFC для этого [на пару минут,] но, по-моему, мы уточнили самый большой вопрос, что это все как-то не охватывает – я думаю, вчера использовался такой термин – не охватывает стороны, связанные договорными обязательствами. Это не обеспечивает услугу в обратном направлении. Похоже, что главный смысл службы начальной загрузки в том, чтобы определить, к какому авторитативному источнику обращаться. И, возвращаясь к комментариям насчет начальной загрузки, по-моему, Скотт говорил об этом: была ли заявка о том, что эта служба будет обрабатывать запросы на информацию за пределами данных доменного имени gTLD? Не могли бы вы пояснить?

СКОТТ ХОЛЛЕНБЕК: Разумеется. Теоретически это возможно. Знаю, мы шутя говорили, как было бы прекрасно, если бы internic.net на самом деле и сегодня оказывал хоть какие-то полезные услуги, да ведь? Но нет, по факту, чем все это закончится в результате, определит только сформированная и реализованная политика. Но теоретически это абсолютно возможно.

ТИМ ЧЕН: Спасибо.

ЭНДИ НЬЮТОН: Я хочу к этому кое-что добавить. Очень даже вероятно, что будут люди, которые будут писать клиентам RDAP, что не хотят самостоятельно проводить процесс начальной загрузки. Они, наверное, уже так делали с [Kerl] и Bash или чем-то таким, и они просто выберут источник начальной загрузки, и возможно это будет ICANN. В таком случае будет отлично, если ICANN выступит в роли стандартного сервера начальной загрузки и будет использовать файлы IANA.

РАМ МОХАН: Спасибо. Да, пожалуйста.

НЕИЗВЕСТНАЯ ЖЕНЩИНА: Просто одно наблюдение. Мне кажется, единственной стороной, которую не включили в эту модель и в EPDP, оказался конечный пользователь. Я знаю, что у вас есть сценарий использования, когда можно проверять собственные данные, но эта модель, по-моему, конечный пользователь тут как канарейка в шахте, нас всегда приносят в жертву. Я всего лишь конечный пользователь, я не вхожу ни в какие группы, к сожалению. Мне кажется, что нам постоянно приходится бороться, и все равно нас постоянно не берут в расчет, нам постоянно

достаются худшие условия, и все стороны найдут механизм, чтобы получать нужные данные с ограничениями, юридическим путем, с помощью авторизации, а мы единственные остались не у дел.

Очень жаль. Такое ощущение, что нам придется за это побороться, и это только начало. Спасибо.

РАМ МОХАН: Благодарю вас. Ну вообще это довольно странное заявление в наш адрес, потому что во всех обсуждениях... если вы обратитесь к ним, послушаете записи и прочитаете стенограммы и тому подобное, то вы увидите, что мы посвятили существенное количество времени рассмотрению этого вопроса с точки зрения конечного пользователя, подающего запрос. И хотя, если убрать из всю воду, то у нас будет пять сценариев использования, на самом деле велись обширные обсуждения о конечных пользователях, на самом деле, тот принцип, о котором говорил Энди, сохранять простоту, не внедрять множество служб сразу и не заставлять конечного пользователя обращаться сразу в несколько мест, чтобы получить информацию. Путь пользователя и его опыт при этом как раз и были основным ориентиром.

Так что, по крайней мере я сам, я считаю, что мы учли интересы конечного пользователя. Но, конечно, в процессе в целом, я согласен, что всем нам необходимо

рассмотреть потребности и нужды конечных пользователей. Еще будут вопросы? Стив, вы подняли руку.

СТИВ КРОКЕР: Да. Я бы немного хотел добавить по этому вопросу. В чем тут, собственно, проблема? Предполагается, что владелец домена может войти в учетную запись вместе с регистратором и узнать всю информацию и подтвердить ее подлинность. И таким образом у них есть прямой доступ.

Поэтому я искренне озадачен, можно ли вообще тут говорить о какой-то проблеме, актуальной с точки зрения поддержки конечного пользователя.

РАМ МОХАН: Бенедикт мне помог, он сказал, что, наверное, вы говорите не о фактическом конечном пользователе, а скорее всего о субъекте данных?

НЕИЗВЕСТНАЯ ЖЕНЩИНА: Да. Именно так.

РАМ МОХАН: Ну это и есть сценарий использования номер пять, про который мы говорили.

НЕИЗВЕСТНАЯ ЖЕНЩИНА: Позвольте добавить, что до этого я не знала о WHOIS? Теперь, когда мне известно, что существует WHOIS, я бы лучше использовала ее. Жаль, что тогда я ей не пользовалась. Коллега из GAC, дама из Франции, которая сказала, что боролась за то, чтобы у потребителей был доступ к информации о компаниях, – это одно. Это важно для нас.

И мне кажется, если бы решение действительно принималось ради нас, если бы в его центре стояли именно мы, то оно бы состояло в разработке способов использования WHOIS в качестве средства защиты, а не в ее ликвидации. Да.

БЕНЕДИКТ ЭДДИС: Понимаете, преодолев недопонимание насчет терминов, и я скажу не как член технической группы, а снова как член EPDP, думаю, что вы сделали разумнейшее замечание. И было бы очень жаль видеть, как эта система превращается в элитный клуб для узкого кружка людей, перепрыгнувших через законодательные барьеры.

По-моему, прелесть этой модели в том, что она обладает гибкостью, и, опять же, мы снова будем оспаривать это слово, если сообщество решит, что его нужно использовать в таком значении в отношении обычных интернет-пользователей, чтобы понять, с кем они

проводят обмен данными. Это политика, это вещь, с которой вам нужно обратиться к сообществу.

НЕИЗВЕСТНАЯ ЖЕНЩИНА: Да. Да. Я буду за это бороться.

БЕНЕДИКТ ЭДДИС: Спасибо.

РАМ МОХАН: Спасибо. Последний вопрос от Вас.

НЕИЗВЕСТНЫЙ МУЖЧИНА: Спасибо. Я постараюсь быть кратким. Это, скажем так, касается, и это комментарий, который я хотел бы сделать по поводу раздела о пути пользователя, раздел 4.1 вашего отчета. Тут говорится о пути пользователя, с которым я не знаком, и я уже долгое время использую RDS WHOIS, особенно второй пункт. Я его пару раз перечитал, и мне кажется, тут можно внести уточнения, чтобы реально поместить путь пользователя в контекст пользователя WHOIS или RDS, ну или как мы все это скоро назовем, и действительно внести ясность, о каком пользователе мы говорим и о каком пути, и реально представить себя на месте того, кто будет пользоваться службой, чтобы найти данные RDS.

РАМ МОХАН: Спасибо. Великолепный комментарий. Благодарю вас. Это заседание практически подошло к концу. Сейчас мне бы хотелось ненадолго передать микрофон различным членам Технической группы по изучению, на случай если вы хотите что-то сказать, прежде чем мы закончим. Скотт, начнем с вас.

СКОТТ ХОЛЛЕНБЕК: Разумеется. Спасибо, друзья. Не забывайте, это консультация. Мы вам все это показали. Нам кажется, что это сработает, но мы, разумеется, очень ждем ваших замечаний. Пожалуйста, предоставьте нам свои комментарии, мы очень хотим услышать ваши соображения.

РАМ МОХАН: Энди?

ЭНДИ НЬЮТОН: Да, я просто хочу повторить то, что сказал Скотт. Ждем ваши комментарии, пожалуйста, присылайте их нам, а мы их обсудим. Спасибо.

РАМ МОХАН: Бенедикт?

БЕНЕДИКТ ЭДДИС: Вот это команда. Спасибо всем, спасибо, что пришли нас послушать.

РАМ МОХАН: Хорхе?

ХОРХЕ КАНО (JORGE CANO): Я хочу поблагодарить вас за комментарии. Мы очень признательны.

РАМ МОХАН: Джоди?

ДЖОДИ КОЛКЕР (JODY KOLKER): Мне нечего добавить. Все здорово.

РАМ МОХАН: Гэвин.

ГЭВИН БРАУН: Мне бы кое-что хотелось сказать, по поводу предыдущих комментариев об использовании регистрационных данных для защиты потребителя, для обеспечения защиты потребителя. Одной из замечательных особенностей RDAP является гораздо более простой доступ к регистрационным данным через RDAP, а не через WHOIS через Порт 43. Если вы пишете веб-

приложение на JavaScript или приложение для мобильного телефона, у вас практически нет шансов получить доступ к данным через Порт 43, если вы не используете какой-нибудь прокси-сервер, который вам придется установить и использовать до конца жизни. RDAP работает в интернете, и данные предоставляются как JSON. Любой программист знает, что такое JSON.

Думаю, что внедрение... и это, в некотором роде, отклоняется от предмета TSG, но это касается RDAP, который сейчас внедряется. Думаю, оно может потенциально открыть множество преимуществ для потребителей, которые хотят доверять тем идентификаторам, которые они используют, ведь это обеспечит более простой доступ конечных пользователей к основной информации об этих доменных именах и прочих ресурсах, которые предоставляет RDAP. Мне видятся такие вещи, как расширение для браузера, где можно нажать на значок в адресной строке, и браузер загрузит эти данные из службы RDAP регистратуры или регистратора и отобразит их, и не придется использовать всю эту сложносочиненную систему с Портом 43. И можно использовать... преимущества онлайн-структуры позволяют нам предусмотреть такие функции, как кэширование и защита, что обеспечит высокую надежность такой системы.

РАМ МОХАН: Спасибо, Гэвин. Томофуми.

ТОМОФУМИ ОКУБО (TOMOFUMI OKUBO): Большое спасибо, что не заснули до конца совещания. С нетерпением жду...

НЕИЗВЕСТНЫЙ МУЖЧИНА: Кое-кто заснул.

РАМ МОХАН: Стив.

СТИВ КРОКЕР: Я со всем согласен. Спасибо. Диана? Элиза, Густаво? Джон.

ДЖОН КРЕЙН: Еще кое-что: огромное спасибо этой группе. Мы, инженеры, просто ненавидим строить системы, не зная требований, и именно это поручили сделать этой группе. И мне кажется, они великолепно с этим справились, и все эти люди, как и вы, тоже волонтеры. Нужно очень постараться, чтобы построить что-то, что, мы надеемся, было, как я это называю, «независимым от политики». Это не очень хороший термин, но довольно гибкий, поэтому переживет нападки, которые точно будут в

ближайшие годы, и много упорного труда. Великолепная работа, друзья.

РАМ МОХАН: Спасибо. На этом заседание завершается. Спасибо всем, кто пришел. Спасибо.

[КОНЕЦ СТЕНОГРАММЫ]