

Сертификация Адресных Интернет-Ресурсов

Введение

Адресные интернет-ресурсы (АИР) или, проще говоря, IP адреса и номера автономных систем являются фундаментальным компонентом Интернет. Эту систему адресации использует универсальный протокол общения между устройствами, подключенными к Интернету, - протокол IP. Глобальная система маршрутизации также основана на АИР.

Архитектура Интернет накладывает определенные требования на то, как должны распределяться АИР между участниками. Протокол IP требует уникальности - каждая сеть должна использовать уникальное адресное пространство, а каждое устройство этой сети - уникальный адрес. Система маршрутизации накладывает требование агрегированности - насколько возможно, распределение адресов должно отражать топологию связности сетей для уменьшения числа глобальных маршрутов. Наконец для обеспечения общедоступности адресных ресурсов, учитывая их ограниченное количество, был введен принцип сохранения - распределение этих ресурсов строго по потребностям.

Лучше всего данным требованиям удовлетворяет иерархическая регионально-топологическая система распределения, образованная в середине 90-х и существующая по сегодняшний день. Пять Региональных Интернет Регистратур (РИР) - AfriNIC, APNIC, ARIN, LACNIC и RIPE NCC распределяют АИР сервис-провайдерам, выполняющим также роль Локальных Интернет-Регистратур (ЛИР). ЛИРы, в свою очередь, распределяют их далее своим клиентам - менее крупным сетям и конечным пользователям.

Однако одного только распределения АИР недостаточно. Важным аспектом деятельности РИРов и ЛИРов является регистрация интернет-ресурсов. Одно дело знать, что ресурс уже распределен, но даже более важной является информация о том, кем используется данный ресурс. Ведь структура взаимодействия сетей в Интернете в многих случаях не является иерархичной или не соответствует структуре распределения адресов. Примером являются пиринговые взаимодействия между сетями, или отношения клиент - сервис-провайдер, в случае, когда клиент имеет собственное независимое адресное пространство. Во всех этих случаях провайдеры полагаются на публично доступные регистрационные данные.

Сегодняшняя публичные регистрационные данные включают региональные регистрационные базы, поддерживаемые РИРами (whois.afriNIC.net, whois.arin.net, whois.apnic.net, whois.lacnic.net, whois.ripe.net) и многочисленные регистратуры маршрутизации (наиболее крупные - RADB и RIPE IRR). Качество информации, доступной из этих источников, очень сильно варьируется. Чем меньше объекты регистрации (сети, маршруты и т.д), чем ближе они к конечному пользователю, тем меньше доверия к этим данным. Другой проблемой является то, что достоверность данных неочевидна для «третьих лиц». Зачастую проверка достоверности превращается в детективное расследование с привлечением различных источников.

Одним из перспективных направлений улучшения доступности и достоверности регистрационных данных является применения технологий, основанных на инфраструктуре открытых ключей - PKI (Public Key Infrastructure). PKI является иерархической системой доступа к открытым (public) цифровым ключам субъектов, основанной на выпуске цифровых сертификатов, связывающих открытый ключ субъекта с определенными атрибутами субъекта - например, принадлежащее ему доменное имя. Этот цифровой документ скреплен цифровой подписью организации выдавшей сертификат. Более подробно структура сертификата X.509 описана в стандарте IETF RFC 3280 (<http://www.ietf.org/rfc/rfc3280.txt>).

В свою очередь, владелец сертификата может выдать подчиненный сертификат, скрепленный своей подписью и так далее. Во главе этой иерархии находится сертификат, также называемый «точкой доверия» (Trust Anchor). Этот сертификат не имеет «родительского» сертификата и подписан собственным ключем. Однако если пользователь уверен в достоверности этого сертификата, подлинность всех остальных сертификатов иерархии может быть легко установлена.

Примером этой технологии является использование SSL сертификатов для защищенного доступа к веб-сайтам с помощью протокола https.

Поскольку распределение АИР является иерархическим, структура PKI может полностью соответствовать структуре распределения интернет-ресурсов. Однако отличия PKI для АИР, получившей название RPKI (Resource PKI), от стандартной PKI существенны, мы остановимся на них подробно в этой статье.

Начнем с основного компонента RPKI – сертификата интернет-ресурса.

Сертификат

Сертификат интернет-ресурса (CP) является цифровым документом, связывающим список интернет-ресурсов (IP адресов и номеров Автономных Систем) с открытым (public) цифровым ключом субъекта сертификата. Посредством сертификата организация, выдавшая его, подтверждает, что субъект имеет право использования перечисленных интернет-ресурсов

CP является сертификатом стандарта X.509 и содержит так называемые критические расширения для документации АИР, стандартизованные в RFC 3779 (<http://www.ietf.org/rfc/rfc3779.txt>). Субъект может подтвердить свои права на использование указанных IP путем демонстрации владения закрытым (private) ключом, соответствующим публичному ключу, указанному в сертификате. Обычно это носит характер подписания данным закрытым ключом какого-либо документа. Получатель этого документа, в свою очередь, может удостоверить соответствие этой подписи с публичным ключом, указанным в сертификате, и как следствие достоверность документа и его ассоциацию с субъектом и его интернет-ресурсами.

Другими словами, владелец закрытого ключа, ассоциированного с CP, может продемонстрировать свои права на использование АИР, указанных в сертификате.

Цифровые сертификаты являются компонентом иерархической инфраструктуры открытых ключей - PKI (Public Key Infrastructure). Также предполагается, что структура PKI соответствует структуре распределения АИР. Сертификаты этой системы являются CP, а вся система в целом получила название RPKI (Resource PKI). Необходимо отметить, что данная система не является системой сертификации аутентичности пользователей (в отличие от большинства традиционных PKI).

Для чего нужна сертификация АИР?

Основной целью создания RPKI является расширение существующей системы регистрации интернет-ресурсов с помощью современных стандартных технологий цифровой криптографии. CP являются более надежным способом документации регистрации АИР, а система RPKI в целом позволяет пользователям независимо определить подлинность CP.

Перечислим основные достоинства использования сертификации:

- Высокая степень защиты против подложных данных. Содержимое сертификата защищено криптографической системой удостоверяющих центров сертификации (УЦС, Certificate Authority - CA) и цифровой подписью.
- Проверка достоверности сертификата основана на криптотехнологии.
- Прозрачная иерархическая система удостоверения прав, конгруэнтная текущей системе распределения АИР.
- Четкие параметры качества данных - сроки действия, удостоверение подлинности прав

Поддержка глобальной уникальности распределения АИР

Одной из основных задач системы распределения АИР является обеспечение уникальности распределенных ресурсов в глобальном масштабе. Использование в глобальном Интернете одного и того же адресного пространства несколькими сетями приведет к нарушению функционирования этих сетей, поскольку система маршрутизации Интернет основана на принципе, что каждое конечное устройство (компьютер) имеет уникальный адрес.

Существующая иерархическая архитектура и процессы системы распределения IP в должной степени обеспечивают эту уникальность, а факт, что только одна организация имеет право использования конкретного адресного пространства документируется в общедоступных базах данных whois (в системе RIPE NCC используется база данных RIPE - whois.ripe.net).

Однако предстоящее опустошение свободного пула адресов IPv4 и, как следствие, возможный процесс перераспределения существующих ресурсов, накладывает новые требования на систему регистрации АИР.

Трансфер АИР между различными организациями – новая концепция для системы распределения АИР. Передача АИР от одной организации к другой осуществлялась и прежде, но только в форме слияния или поглощения одной компании другой. Тема трансфера АИР связана с предстоящим опустошением свободного пула адресов IPv4 и, как следствие, с возможным процессом перераспределения существующих ресурсов.

Предполагается, что перераспределение будет происходить в соответствии с правилами, определенными политикой распределения АИР (в случае RIPE NCC - <http://www.ripe.net/ripe/docs/ripe-449.html#55>) и может явиться результатом свободной торговли адресами IPv4.

В то же время нельзя исключить возможность перераспределения АИР незаконным путем, посредством одностороннего присвоения и использования АИР и возможного изменения регистрационных данных в публичных базах данных whois (address space hijacking).

Можно сказать, что сегодняшняя система публичной регистрации АИР не соответствует будущим требованиям, предъявляемым к системе вследствие предполагаемой большей мобильности АИР и необходимости защиты прав использования.

В этом смысле сертификация АИР предоставляет более надежный и технологичный метод публичной регистрации.

Важно отметить, что СР не идентифицируют личность или организацию, которые владеют правами использования АИР. Заявление, представленное СР, означает, что владелец закрытого ключа СР (факт владения ключом подтверждается, например, путем подписания какого-либо документа и последующей успешной проверки правильности подписи с помощью открытого ключа, представленного в СР) является владельцем прав использования АИР, описанный в СР. Для усиления этой особенности предполагается, что поле СР, идентифицирующее субъекта, является лишь индексом во внутреннюю базу данных УЦС и не содержит значимой информации для третьих лиц.

Функцию связи субъекта СР с реальной организацией выполняет УЦС. Решение о публикации этой информации, например на веб-сайте или в базе данных whois, остается за УЦС.

Поддержка безопасности системы глобальной маршрутизации

Система RPKI и СР, как более достоверная и технологичная система проверки достоверности информации о правах использования АИР, может существенно упростить и позволить автоматизировать сегодняшние методы взаимодействия между сетевыми операторами, а также способствовать практике надежной и безопасной маршрутизации. Конкретные процессы включают процесс установления пиринга, а также практику инспекции и фильтрации маршрутизационной информации.

Безопасность и надежность системы маршрутизации во многом зависит от возможности правильного ответа на вопросы:

- является ли префикс, полученный в сообщении BGP, правомерным (т.е. представляющим законно распределенное адресное пространство и право на его использования)?
- является ли автономная система-отправитель сообщения BGP, правомочным источником (origin) префикса?
- соответствует ли атрибут AS_PATH, полученный в сообщении BGP, действительному пути, который прошло данное сообщение в сети Интернет?

Следует отметить, что существующая практика среди сетевых операторов во многих случаях игнорирует указанные вопросы. Ряд операторов ограничиваются инспекцией (фильтрацией) префиксов, получаемых от непосредственных клиентов (по существу частично отвечая на первый вопрос). Некоторые операторы осуществляют инспекцию префиксов на основе "макро"-фильтров, отражающих, например, распределенное адресное пространство на уровне IANA.

Одной из причин такой ситуации является трудоемкость получения четких ответов на поставленные вопросы и сложность автоматизации этого процесса. Это, в первую очередь, связано с отсутствием достоверного способа документирования использования адресного пространства. Как уже упоминалось, существующие базы данных whois Региональных Интернет Регистратур содержат неполную и сильно различающуюся по качеству информацию; еще хуже состояние дел в Интернет-регистратурах маршрутизации (Internet Routing Registry, IRR). Эта проблема усугубляется отсутствием надежного способа определения достоверности данных, полученных из этих баз данных.

Прежде чем перейти к рассмотрению конкретных приложений, кратко остановимся на сегодняшних проблемах, связанных с недостаточной безопасностью системы маршрутизации.

1. Генерация трафика с использованием подложных адресов в качестве источника трафика (см. обсуждение в BCP 38 - <http://www.ietf.org/rfc/rfc2827.txt>, rfc3704.txt). Данная технология используется в атаках отказа в обслуживании DoS (Denial of Service). Например, в случае использования протокола DNS, атакуемые компьютеры играют роль отражателей и усилителей трафика, который затем поражает компьютеры, якобы являющиеся источником запросов.
2. Притягивание трафика, является одним из видов атаки DoS. Ярким примером явилось анонсирование компанией Pakistan Telecom адресного пространства серверов YouTube, с последующим игнорированием входящего трафика, что привело к невозможности доступа к сервису YouTube.
3. Перехват трафика. При этом трафик перехватывается, например для перлюстрации или модификации, и затем возвращается в прежнее русло. В этом случае получатель не подозревает, что над трафиком были произведены незаконные операции.
4. Краткосрочная незаконная деятельность с использованием присвоенного адресного пространства. Примером может служить анонсирование временной сети для атаки DoS или рассылки спама.

Система RPKI может упростить решение проблем 2-4. Следует отметить, что RPKI сама по себе не является решением проблем безопасности, поскольку решение о принятии дополнительных мер - например дополнительных проверок при предоставлении транзита сети или фильтрация маршрутов, - остается за сетевым оператором. Но система RPKI может облегчить или даже автоматизировать подобные задачи.

Установление пиринга

В настоящее время установление пиринга и предоставление услуг передачи данных сети во многих случаях не предусматривает дополнительных проверок достоверности прав использования АИР. В случаях, когда сетевой оператор все же осуществляет такие проверки, они зачастую носят характер детективной работы с привлечением нескольких баз данных (например whois, IRR), точность данных которых небезупречна.

С использованием RPKI, проверки правомерности запроса на пиринг могут быть в значительной степени упрощены. Например запрос с указанием автономной системы и адресного пространства просителя может быть подписан соответствующим сертификатом, охватывающим эти ресурсы. Определение достоверности такого запроса может быть полностью автоматизирована.

Поддержка текущей практики фильтрации маршрутов

К сожалению на сегодняшний день фильтрация маршрутов не является широко распространенной практикой среди сетевых операторов. Одной из причин тому - опять же отсутствие надежных достоверных и технологичных данных о принадлежности АИР определенным сетям и, как следствие, трудности принятия решения относительно допустимости того или иного маршрута.

Настоящая практика в основном предусматривает «локальную» фильтрацию - использование сетевыми операторами IRR, в которой сети-клиенты обязаны зарегистрировать т.н. объекты маршрутов (объекты "route: "), описывающие адресное пространство, которое анонсирует автономная система. Коллекция объектов «route:» всех автономных систем - клиентов оператора,

составляет его фильтр маршрутов. Следует отметить, что хотя данный метод может быть автоматизирован, надежность IRR с точки зрения достоверности данных невысока.

Некоторые сетевые операторы осуществляют «глобальную» фильтрацию: они используют базы данных распределения АИР высокого уровня (например базу данных IANA), которые являются достаточно компактными и статичными. Недостатком такого подхода является отсутствие деталей, открывающее широкие возможности обхода таких фильтров.

Идея использования сертификатов RPKI для поддержки эффективного построения фильтров является весьма привлекательной. Во-первых, сертификаты свободны от многих недостатков упомянутых баз данных и предоставляют ряд преимуществ. Например, возможность криптографического установление достоверности данных сертификата, или документа, созданного на основе сертификата, вне контекста какой-либо базы данных. Во-вторых, криптографический характер сертификатов позволяет эффективно использовать его производные - данные, подписанные сертифицированным ключом. Этими данными, так называемыми вторичными объектами, могут быть документы ROA (Route Origination Authorisation), которые позволяют удостоверять правомерность анонсирования автономной системой определенных префиксов.

Безопасность на уровне протокола BGP

Полным решением указанных проблем безопасности является определение достоверности анонсируемых маршрутов на уровне протокола BGP. Основная идея заключается в том, что на всем пути маршрута граничные маршрутизаторы связанных автономных систем «подписывают» соответствующие участки пути. В результате каждый анонсированный маршрут может быть достоверно проверен как на предмет адресного пространства и автономной системы, его анонсирующей, но также и на то, что полученный маршрут действительно был передан через автономные системы, которые в нем указаны (атрибут AS_PATH).

Данный подход получил некоторое развитие в архитектуре sBGP и soBGP, работа над которыми началась несколько лет назад. Однако в последнее время стало очевидно, что дороговизна применения (например, требуемая компьютерная мощность) и сложность внедрения (последовательное внедрение технологии не приносит ожидаемых улучшений до достижения значительной критической массы) данных технологий несоразмерны с теми преимуществами, которые они обещают (например, величина и вероятность рисков, которым они противодействуют).

В силу этого работы в этом направлении не получили достаточного развития и вряд ли можно рассчитывать на практическое внедрение безопасности на уровне протокола BGP в обозримом будущем.

Архитектура системы сертификации IP

Основные принципы RPKI

Как уже упоминалось, цифровой сертификат X.509 основан на технологии асимметричных ключей. Суть технологии заключается в том, что каждый ключ имеет секретную и открытую части. Подлинность сообщения, подписанного с помощью секретного, или закрытого ключа, может быть установлена с использованием открытого ключа. Стандартная практика предполагает, что владелец ключа предпринимает адекватные меры защиты секретного ключа, и в то же время обеспечивает как можно более широкую публикацию открытого ключа, для облегчения доступа к нему третьих лиц, например для проверки подлинности посланного владельцем сообщения.

Для эффективного применения данной технологии необходимо удовлетворить два основных условия:

- обеспечить эффективную систему распространения открытых ключей и
- обеспечить достоверную идентификацию открытого ключа с его владельцем

Данная задача успешно решается с помощью иерархической системы PKI. Основным элементом

этой системы являются сертификаты. Сертификат выдается удостоверяющими центрами сертификации, УЦС, - органами, отвечающими за установление связи между субъектом сертификата и его открытым ключом. По существу, сертификат является цифровым документом, который содержит некоторый идентификатор субъекта и его открытый ключ, подписанным органом, выдавшим сертификат. Посредством сертификатов, УЦС могут сертифицировать УЦС следующего уровня и так далее, образуя, таким образом, древовидную иерархическую структуру. Эта структура является также «структурой доверия». Если вы доверяете УЦС, сертифицировавшему другой УЦС, вы также доверяете и этой организации, и т.д. То есть, третьим лицам достаточно доверять УЦС в корне данной структуры, чтобы установить достоверность любого сертификата и, таким образом, достоверно идентифицировать связь какого-либо открытого ключа с его владельцем.

Помимо основной информации упомянутой выше, сертификаты могут содержать дополнительные данные, т.н. расширения, которые могут быть использованы в процессе установления подлинности сертификата.

Система РPKI основана на сертификатах стандарта X.509, содержащими критические расширения для документации AIP, стандартизованные в RFC3779. Данное расширение содержит список всех AIP (адресов IPv4 и IPv6, а также номера АС) полученных субъектом сертификата. Важно отметить, что задачей СР не является идентификация субъекта, в отличие от стандартной системы PKI. СР удостоверяет, что УЦС распределил определенные ресурсы субъекту сертификата, и данные ресурсы перечислены в расширении сертификата. УЦС удостоверяет, что любой документ, подписанный секретным ключом, соответствующим открытому ключу сертификата, подписан законным обладателем прав использования IP, перечисленных в сертификате. Данная концепция схематично представлена на рис. 1.

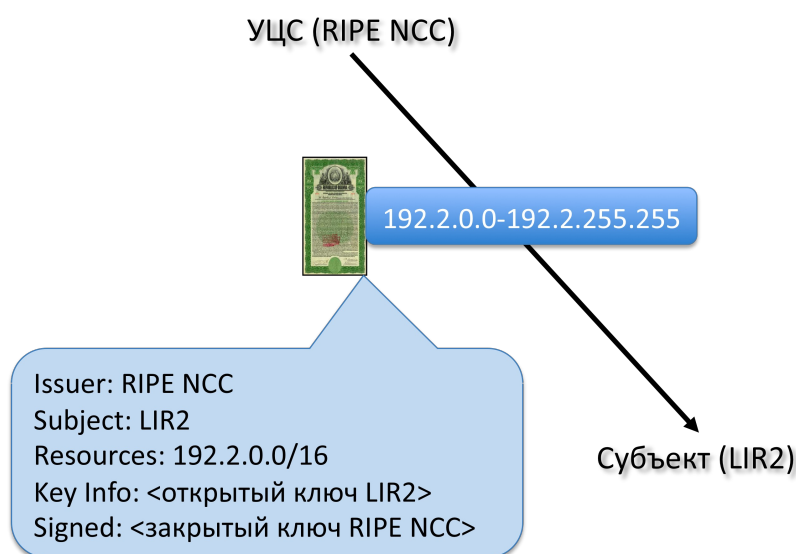


Рис.1 X.509 Сертификат Ресурсов с расширениями

Данная специфика становится более ясной в конкретном контексте, например при запросе на пиринг. Оператор сети, который хотел бы установить пиринговые отношения с другой сетью, может подписать запрос на пиринг, используя СР. Получатель запроса может проверить подлинность сертификата и удостовериться, что запрос действительно пришел от законного обладателя АС, указанной в запросе.

При этом почтовый адрес отправителя не имеет значения и не влияет на достоверность описанной проверки.

Структура RPKI

Любая система PKI имеет иерархическую структуру с корневым сертификатом во главе. Поскольку для корневого сертификата не существует родительского УЦС, данный сертификат представляет собой самоподписанный корневой ключ. Организация, которой принадлежит корневой CP, является т.н. «точкой доверия» (Trust Anchor). Важно отметить, что как и в любой системе PKI вопрос доверия данной PKI остается за третьими лицами - пользователями системы.

Хотя в случае RPKI очевидным кандидатом на роль точки доверия является IANA, можно предположить, что некоторая организация создаст CP, охватывающий все IP (все адресное пространство IPv4, IPv6 и AC). Эта организация теперь может предоставлять CP любым участниками системы распределения IP, при этом выданные сертификаты будут формально отвечать требованиям удостоверения подлинности в соответствии с RFC 3779. Единственным условием успешного использования этих сертификатов является выбор данной организации пользователями CP в качестве точки доверия. Очевидным недостатком такой системы является отсутствие надежных регистрационных данных у такого УЦС, что делает процесс сертификации менее надежным.

Более реалистичным является предположение, что процесс внедрения RPKI начнется с создания нескольких точек доверия, включающих RIR, и последующим созданием единого корневого CP.

Для этого потребуют решения вопросы контроля, управления и сопровождения корневого CP, которые затрагивают глобальное Интернет-сообщество и во многом носят нетехнический характер. Эти аспекты выходят за рамки данной статьи. Для иллюстрации работы RPKI остановимся на «идеальной» с технической точки зрения структуре.

В этом случае корневой CP в качестве списка AIP охватывает все адресное пространство IPv4, IPv6 и автономных систем. С помощью этого сертификата могут быть сгенерированы сертификаты RIR в соответствии с фактически распределенным адресным пространством. В качестве примера распределения адресного пространства IPv4 см. <http://www.iana.org/assignments/ipv4-address-space/>

В свою очередь RIR могут сертифицировать AIP, которые они распределяют Локальным Регистратурам (Local Internet Registry - LIR) или конечным пользователям, которые получают AIP непосредственно от RIR. Локальные Регистратуры могут осуществлять последующее распределение, и соответствующую сертификацию. Наконец конечные пользователи - сети, фактически использующие адресное пространство, также должны иметь возможность генерирования временных сертификатов для подписания вторичных объектов RPKI - ROA, BOA, и т.д. Дело в том, что срок жизни этих объектов обычно короче, чем право на использования AIP, а их аннулирование реализуется путем аннулирования сертификатов, использованных при создании соответствующих объектов. Во избежание аннулирования всех вторичных объектов и последующего их воссоздания, для каждого объекта генерируется свой CP. Таким образом аннулирование вторичных объектов может быть осуществлено независимо.

Важным последствием такого подхода является требование, что все участники RPKI являются органами выдачи сертификатов, УЦС, со всеми вытекающими последствиями: необходимостью соответствующей защищенной инфраструктуры, процессов управления ключами и т.п.

Общая схема RPKI проиллюстрирована на рис. 2.

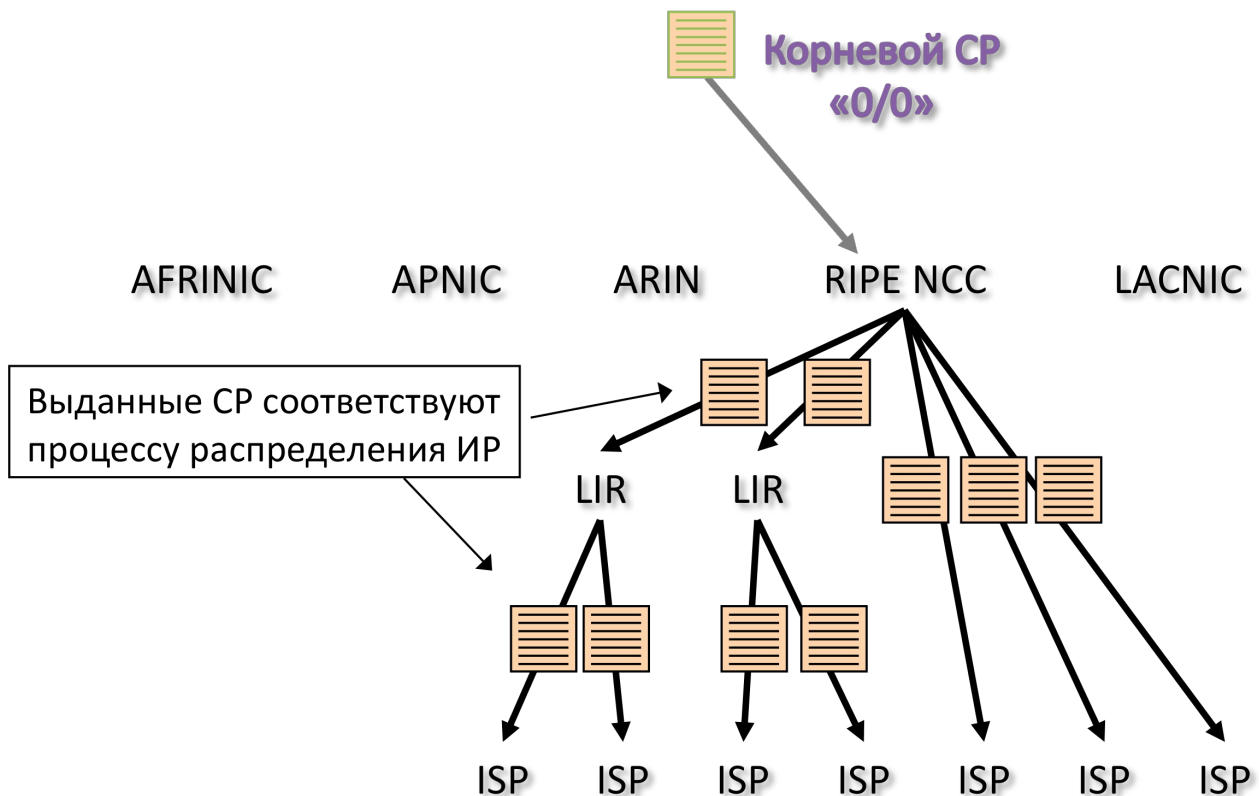


Рис. 2 Общая структура RPKI

Основные компоненты

Как и в случае традиционной PKI, в состав RPKI входят следующие компоненты:

- Служба выдачи сертификатов (Certificate Authority, CA). Основной функцией CA является генерация и публикация сертификатов и списков аннулированных сертификатов. Эта функция по существу не меняется в RPKI, за исключением того, что СР содержат расширения документирующие распределенные AIP.
- Служба регистрации (Registration Authority, RA) отвечает за проверку подлинности связи между субъектом сертификата и его ключом. В случае RPKI также удостоверяется, что субъект сертификата имеет права на использование AIP, перечисленных в расширении. По существу, эта функция неотличима от функции регистрационных услуг, выполняемых сегодня РИР. Отметим, что хотя предполагается, что УЦС удостоверяет субъекта СР, данное условие не является необходимым, и информация о субъекте в СР может не быть неявной (например, субъект может быть представлен цифровым идентификатором, имеющим значение только во внутренней структуре УЦС).

Эти две службы являются частью УЦС.

- Репозитории - открытые базы данных, в которых публикуются выданные сертификаты, списки аннулированных сертификатов и, в случае RPKI, вторичные объекты.

- Сертификаты и вторичные объекты. О структуре CP уже говорилось достаточно много. Вторичные объекты специфичны для системы RPKI и, строго говоря, не являются частью системы, а предоставляются из соображений удобства практического применения RPKI. Они являются документами, подписанными владельцем сертификата (т.е. закрытым ключом, соответствующим открытому ключу сертификата). Следует также оговориться, что ни один из вторичных объектов пока не стандартизован IETF, хотя работа над разработкой такого стандарта активно ведется.
- Разрешение на создание маршрута (Route Origin Authorisation, ROA). Одним из наиболее проработанных вторичных объектов является ROA. Использование ROA предполагается в контексте безопасности маршрутизации. Как следует из названия, ROA является разрешением, данным сетью - владельцем прав использования AIP на анонсирование данных ресурсов Автономной Системой, указанной в ROA. В соответствии со спецификацией ROA содержит номер авторизованной АС и список IP префиксов, которые эта АС имеет разрешение анонсировать. К этому "заявлению" прилагается сертификат, описывающий соответствующие AIP, и весь объект подписан с использованием ключа, указанного в сертификате. Также отметим, что наличие ROA не означает «согласие» авторизованной АС и что указанные префиксы непременно будут анонсированы данной Автономной Системой.

Использование RPKI третьими лицами (relying party)

Одной из задач создания RPKI является предоставление третьим лицам возможности независимой проверки достоверности сертификатов и вторичных объектов системы (например, ROA). Единственным условием является доверие третьих лиц корневому УЦС. Третьими лицами являются пользователи системы RPKI, задачей которых является проверка достоверности данных относительно AIP, их статуса и подлинности связи ресурсов с заявленным владельцем прав на использование.

При работе с данными RPKI, которые в общем случае являются вторичными объектами, третьему лицу в первую очередь необходимо установить соответствие данных вторичного объекта с данными CP (точнее, AIP, указанными в расширении CP). Так в случае с ROA, после проверки подлинности подписи, пользователь должен удостовериться, что ресурсы, описанные сертификатом ROA, содержат все IP префиксы, указанные в ROA.

Следующим шагом является создание т.н. «цепи доверия». Происходит это следующим образом. Как и в стандартном PKI каждый CP содержит ссылку на CP УЦС, выдавшего данный сертификат. Таким образом, можно убедиться, что сертификат действительно подписан УЦС и данные сертификата не были модифицированы. Поднявшись на ступеньку выше, таким же образом можно проверить подлинность сертификата УЦС, УЦС более высокого уровня, и т.д. вплоть до корневого УЦС, который является доверенным центром для третьих лиц. Если все проверки цепочки прошли без ошибок, можно с уверенностью сказать, что исходный сертификат является достоверным и немодифицированным. Этот процесс представлен на рис.3.

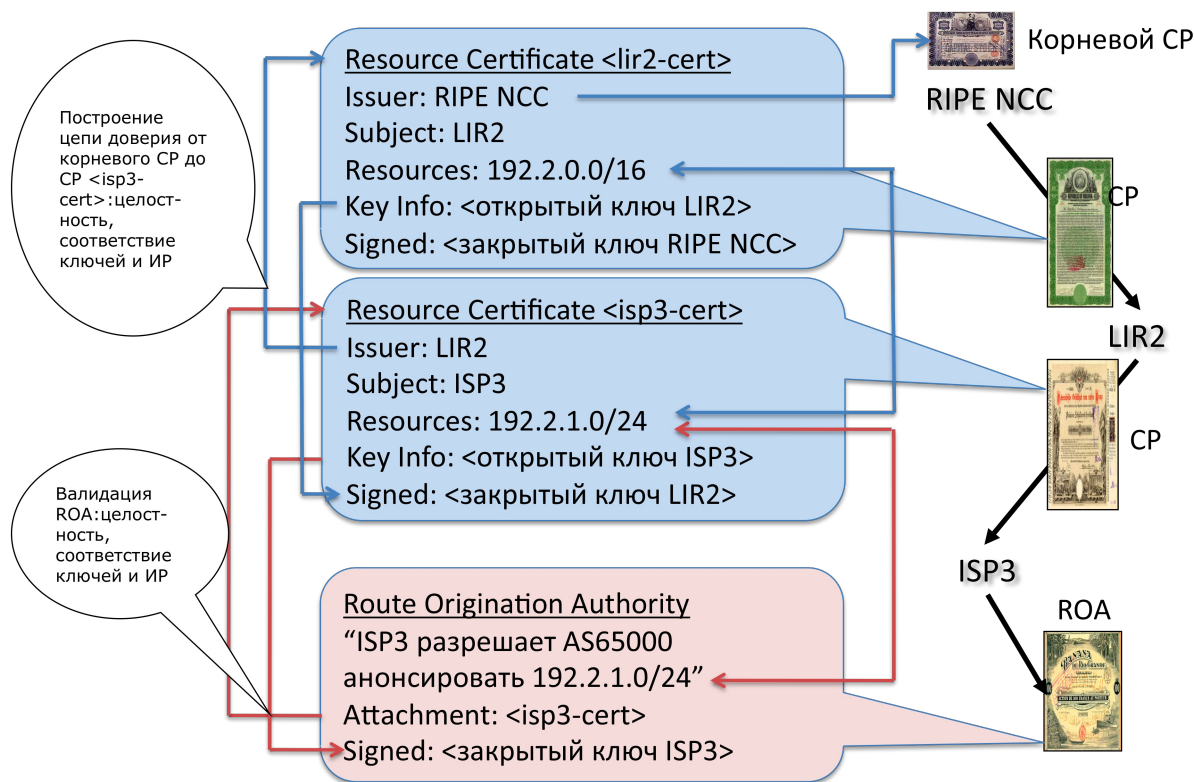


Рис. 3. Построение цепи доверия для проверки подлинности вторичных объектов и CP

Реализация системы Сертификации Региональными Интернет Регистратурами

РИР начали заниматься вопросами сертификации АИР с 2006 года. Пионером в этом отношении являлся APNIC, который предложил основные принципы построения системы RPKI. В 2007 году к работе активно подключился ARIN и совместная группа RESCERT, в состав которой также входили специалисты других РИР, разработала основные компоненты системы.

RIPE NCC начал работу над сертификацией почти одновременно с APNIC. В отличие от APNIC первоначально основная деятельность была направлена на выработку общей позиции относительно целей сертификации АИР, а также на вовлечение сообщества в процесс выработки требований к системе RPKI. В ноябре 2006 была создана рабочая группа (Certification Task Force - <http://www.ripe.net/ripe/tf/certification/index.html>).

Одновременно началась разработка программного обеспечения. Первоначально основной фокус был направлен на разработку пользовательских интерфейсов, в отличие от других РИР, работавших над внутренними компонентами. Целью RIPE NCC являлось облегчить понимание системы и практическая демонстрация ее работы сообществу и рабочей группе.

На сегодняшний день RIPE NCC предоставляет функциональный прототип сертификационного портала, через который Локальные Регистратуры имеют возможность запросить сертификаты АИР, полученных от RIPE NCC, генерировать и аннулировать ROA, а также осуществлять трансфер АИР между собой. По окончании разработки инфраструктуры, отвечающей требованиям безопасности RPKI, планирующейся в течение 2009, пользователям будет предоставлен полностью функционирующий портал.

Технический директор RIPE NCC Андрей Робачевский

Мнения, представленные в статье, не обязательно отражают официальную позицию RIPE NCC