# Внедрение инфраструктуры открытых ключей (PKI)

**Е.Ю. Антошечкина,**
главный специалист,
«ЭОС»

**Как осуществляется внедрение инфраструктуры открытых ключей (PKI) и какие вопросы нужно решать организации в процессе внедрения и эксплуатации PKI?**

*Начальник отдела ДОУ, Тамбовская обл.*

Прежде всего дадим несколько определений и уточним, что же представляет собой инфраструктура открытых ключей, для каких целей и задач она используется, а затем уже поговорим о том, как строится процесс развертывания этой инфра-

структуры и какие вопросы предстоит решать в ходе ее внедрения и последующей эксплуатации в организации.

При этом будем исходить из того, что значения таких общих терминов, как закрытый ключ, открытый ключ, сертификат, удостоверяющий центр, шифрование, электронная подпись, криптопровайдер читателю известны.

Итак, **инфраструктура открытых ключей** (англ. **PKI** – Public Key Infrastructure) – это инфраструктура (совокупность программных и аппаратных средств, организационно-технических мероприятий и обслуживающего персонала), обеспечивающая создание доверенной среды между субъектами информационного взаимодействия, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей и сертификатов.

Такая инфраструктура создается и используется для обеспечения безопасной работы приложений в рамках распределенной информационной системы, т. е. позволяет приложению защищать собственные информационные ресурсы и безопасно взаимодействовать с ресурсами других приложений.

Основными задачами, решаемыми инфраструктурой открытых ключей, являются:

- **установление доверия (в рамках заданной модели доверия);**
- **реализация системы именования субъектов информационного взаимодействия, обеспечивающая уникальность имени каждого субъекта в рамках системы;**
- **установление связи между именем субъекта и парой ключей (закрытым и открытым) с подтверждением этой связи средствами удостоверяющего центра, которому доверяет субъект, проверяющий правильность данной связи.**

Несмотря на сложные внутренние механизмы реализации этих возможностей, преимущество PKI заключается в том, что для пользователя, взаимодействующего с PKI через то или иное приложение, эта инфраструктура является «прозрачной», т. е. позволяет использовать результат работы сервисов PKI без необходимости знания правил их функционирования. В частности, получившая в настоящее время довольно широкое распространение технология применения электронной подписи как средства обеспечения доверия при обмене электронными документами служит примером использования PKI.

Организации, принимающей решение о необходимости использования инфраструктуры открытых ключей и о сфере ее применения, следует ориентироваться на область своей деятельности, структуру, требования по безопасности (как принятые на общем законодательном уровне, так и требования, накладываемые областью и спецификой деятельности организации). Разумеется,

нельзя не учитывать и такой факт, как наличие или отсутствие необходимых для выполнения данных работ ресурсов (финансовых, кадровых, временных). PKI позволяет создать единую инфраструктуру для многочисленных сервисов безопасности, построить доверенную среду взаимодействия многих приложений.

**Такой вариант может быть востребован прежде всего крупными организациями, имеющими территориально распределенную структуру. Однако и сравнительно небольшая организация, не испытывающая острой потребности создания собственной масштабной доверенной среды, может стать заказчиком PKI (например, при необходимости вхождения в созданную с использованием PKI доверенную среду вышестоящей структуры или в целях реализации защищенного межкорпоративного взаимодействия на основе соглашения).**

После положительного принятия решения об использовании PKI в организации начинаются работы по подготовке к ее развертыванию и непосредственно внедрение инфраструктуры. Эти этапы во многом схожи с этапами внедрения в организации практически любой системы автоматизации, а компании, которые внедряли технологию использования электронной подписи, уже через них прошли.

Работы по развертыванию PKI можно разделить на следующие этапы:

1. Оценка готовности организации к развертыванию PKI и ее последующей эксплуатации.
2. Принятие решения об удостоверяющем центре.
3. Установка криптопровайдера.
4. Создание закрытых ключей и получение сертификатов.
5. Обеспечение интеграции PKI с использующими ее приложениями.
6. Опытная эксплуатация.
7. Промышленная эксплуатация.

Рассмотрим подробнее каждый этап и те вопросы, которые должны быть решены в ходе выполнения его работ.

**1. Оценка готовности организации к развертыванию PKI и ее последующей эксплуатации.**

В ходе оценки готовности организации к развертыванию PKI и ее эксплуатации следует проанализировать наличие в организации ресурсов, требуемых для развертывания и сопровождения инфраструктуры PKI.

**Сюда входит оценка наличия и состава необходимых программно-аппаратных средств, сетей, обученного персонала нужной квалификации, оценка сроков выполнения работ, стоимостная оценка решения.**

Оценивая стоимость решения, нужно принимать в расчет как стоимость развертывания PKI, так и стоимость ее последующей эксплуатации (расходы на ведение операционной деятельности удостоверяющего центра, расходы на поддержание работоспособности инфраструктуры, включая оплату персонала). При отсутствии или недостаточном развитии сопутствующей ИТ-инфраструктуры следует учесть и затраты на ее модернизацию.

**2. Принятие решения об удостоверяющем центре.**

На следующем этапе работ принимается решение о том, будет ли развертывание инфраструктуры открытых ключей осуществляться силами самой организации или эти работы будет выполнять внешняя организация-исполнитель.

Принятие решения об удостоверяющем центре – ключевом элементе PKI – является одним из важнейших этапов развертывания PKI.

На это решение влияет множество факторов, в частности требования к видам используемых подписей, областям их использования, стоимости и срокам выполнения работ по внедрению, организации сопровождения. Требования к удостоверяющему центру могут быть определены законодательно, прописаны в нормативных актах, распорядительных документах или соглашениях.

**Необходимо учитывать, что деятельность удостоверяющего центра (в особенности оказывающего услуги государственным структурам) жестко регламентирована и на ее поддержание на должном уровне уходят значительные финансовые средства.**

Как правило, стоимость и временные затраты на развертывание PKI при использовании решения внешних поставщиков услуг удостоверяющего центра меньше, чем в случае реализации решения силами организации. Это объясняется тем, что стоимость этих услуг может быть распределена на нескольких заказчиков (абонентов удостоверяющего центра), типовые решения проверены и опробованы (что уменьшает вероятность ошибок и необходимость повторного проведения работ), все требуемые организационно-технические мероприятия проведены, нужные документы разработаны, персонал обучен.

**Несмотря на то что заказчик в любом случае является активным участником процесса внедрения PKI, привлечение внешних исполнителей позволяет организации-заказчику снизить квалификационные требования к собственному персоналу и инфраструктуре (работы по развертыванию PKI выполняет исполнитель с использова-**

**нием собственных мощностей, программно-аппаратных средств и персонала).**

Как правило, исполнитель, осуществляющий развертывание PKI, впоследствии выполняет работы по сопровождению внедренного решения у организации-заказчика. Основная нагрузка по сопровождению и при необходимости расширению инфраструктуры открытых ключей ложится в этом случае на плечи исполнителя.

Но следует помнить, что при этом исполнитель осуществляет также и основной контроль функционирования PKI. Для организаций, которым требуется собственный полный контроль безопасности и источника доверия, это может стать решающим доводом против использования услуг внешнего исполнителя. Создание собственного удостоверяющего центра может быть также продиктовано необходимостью реализации специфического решения в области PKI.

Таким образом, однозначно ответить на вопрос, какой вариант предпочтительнее – собственная реализация или внешний исполнитель, невозможно, решение об удостоверяющем центре принимается с учетом специфики каждого конкретного случая.

При принятии решения о выборе удостоверяющего центра нужно также учитывать, что не каждый удостоверяющий центр обслуживает всех возможных криптопровайдеров. Поэтому организациям, реализующим доверенную среду с использованием определенного криптопровайдера, следует выбирать удостоверяющий центр, предоставляющий возможность работы с этим криптопровайдером. Впрочем, большинство организаций, предоставляющих на отечественном рынке услуги удостоверяющих центров, работают со всеми наиболее популярными криптопровайдерами.

**3. Установка криптопровайдера.**

Для обеспечения возможности использования инфраструктуры открытых ключей на рабочем месте пользователя должны быть установлены необходимые программные средства. В частности, выполнение действий по формированию электронной подписи и шифрованию/расшифровке данных невозможно без специальной программы – криптопровайдера. Обычно криптопровайдеры уже включены в состав современных операционных систем. Однако в ряде случаев законодательство требует применения сертифицированных государственными органами криптопровайдеров: тогда их придется покупать и устанавливать на рабочих местах пользователей, которые будут подписывать данные своей электронной подписью или проверять электронные подписи.

**4. Создание закрытых ключей и получение сертификатов.**

После установки криптопровайдеров выполняются действия по созданию закрытых ключей и получению сертифика-

тов. Каждый из сотрудников организации, являющийся конечным пользователем PKI, должен получить закрытый ключ. Процедура создания закрытых ключей может производиться по-разному: ключи могут формироваться в удостоверяющем центре и передаваться пользователям вместе с соответствующим сертификатом либо ключи могут создаваться самим пользователем на своем рабочем месте в организации, а открытая часть ключа пересылаться в удостоверяющий центр для последующего изготовления сертификата. С точки зрения гарантированного отсутствия доступа третьих лиц к закрытому ключу второй вариант предпочтительнее (никто, кроме самого пользователя, не имеет доступа к его закрытому ключу, даже сотрудник удостоверяющего центра), однако не все пользователи имеют возможность и желание заниматься формированием закрытых ключей.

Закрытый ключ подлежит ответственному хранению пользователем – владельцем соответствующего сертификата и не должен попадать в чужие руки: это ведет к его компрометации и запрету дальнейшего использования.

***На заметку!***

Закрытый ключ используется пользователем для собственной аутентификации в информационной системе, расшифровки данных и формирования электронной подписи. Данные же сертификата открыты и публичны.

**Обычно сертификаты хранятся в хранилище операционной системы (в каждом компьютере, в общем сетевом хранилище, в базе данных и т. п.). Удостоверяющий центр также хранит сертификаты. Сертификат содержит всю необходимую для проверки электронной подписи информацию, а также позволяет зашифровать данные, которые сможет расшифровать только владелец сертификата, обладающий соответствующим закрытым ключом.**

Обязанности пользователей по обеспечению сохранности закрытых ключей, порядок применения ключей для формирования электронной подписи, порядок действий пользователей в штатных ситуациях при получении, сдаче, плановой замене ключей и сертификатов, а также порядок действий в случае компрометации ключа и возникновения конфликтных ситуаций в обязательном порядке должны быть описаны в регламентирующих документах и утверждены приказом по организации.

**5. Обеспечение интеграции PKI с использующими ее приложениями.**

Мы помним, что основной интерес для пользователей представляет не сама инфраструктура открытых ключей как таковая, а возможность с ее помощью организовать защищенную работу приложений. Для этого приложение должно уметь использовать информацию, предоставляемую PKI. Обеспечение взаимодействия PKI и приложения реализуется с использованием интерфейсов прикладного программирования.

***Полезно знать!***

Для повышения конкурентоспособности своих продуктов многие разработчики предусматривают в них средства для интеграции с PKI.

**6. Опытная эксплуатация.**

Полномасштабное развертывание и последующая эксплуатация инфраструктуры открытых ключей должны предваряться этапом опытной эксплуатации.

Опытная эксплуатация, как правило, проводится в условиях реальной деятельности организации или в условиях, максимально приближенных к реальным, с ограничениями по времени и области использования решения (но ни в коем случае не ограничиваясь только ИТ-подразделениями: в процесс должны быть вовлечены пользователи, которым предстоит активно работать с инфраструктурой после ее полного развертывания). При этом важно, чтобы в период опытной эксплуатации нового решения прежняя технология работы была сохранена и продолжала выполнять свои функции.

На данном этапе происходит проверка работоспособности развернутой инфраструктуры, выполнения всех функциональных требований и требований по безопасности, соответствия регламентам, обучение пользователей и обслуживающего персонала, отладка процессов и процедур информационного взаимодействия с использованием PKI между ключевыми участниками взаимодействия. Также при необходимости осуществляется корректировка решения как в аппаратно-программной части, так и в организационно-правовом плане.

**Если внедрение PKI осуществлялось внешним исполнителем и работы предыдущих этапов развертывания инфраструктуры открытых ключей выполнялись при незначительном участии персонала организации-заказчика, то на данном этапе сотрудники заказчика начинают принимать непосредственное участие в работах. Они проходят обучение и выполняют основные функции по тестированию процессов взаимодействия с использованием PKI.**

**7. Промышленная эксплуатация.**

После успешного завершения этапа опытной эксплуатации можно переходить к промышленной эксплуатации решения. К моменту начала этого этапа желательно обучить всех пользователей и обслуживающий персонал заказчика (хотя, конечно, процесс обучения можно проводить и на начальных стадиях этапа промышленной эксплуатации).

Было бы ошибкой полагать, что вопросы, нуждающиеся в решении, возникают исключительно на этапе развертывания и внедрения PKI в организации, и после этапа опытной эксплуатации организация может, не заботясь ни о чем, пользоваться результатами успешного внедрения. В процессе промышленной эксплуатации инфраструктуры PKI организация сталкивается с рядом вопросов, нуждающихся в решении. Это в первую

очередь рабочие вопросы по поддержке штатного функционирования инфраструктуры PKI, регистрации новых пользователей PKI, управлению ключами и сертификатами (выдача и замена ключей и сертификатов, приостановление и возобновление действия сертификатов, отзыв сертификатов, управление списками отозванных сертификатов, восстановление, резервное копирование и архивное хранение ключей). Также следует предусмотреть порядок действий сторон при разрешении спорных ситуаций и инцидентах, которые могут возникнуть в процессе эксплуатации инфраструктуры PKI.

При большом количестве пользователей (от сотни и выше) выполнение данных процедур требует довольно много времени. При этом крайне важно обеспечить непрерывную работу пользователей, поэтому все действия должны планироваться, выполняться своевременно и оперативно.

Если организация выбрала вариант внедрения PKI своими силами, все упомянутые вопросы в ходе сопровождения PKI она также будет решать самостоятельно. Если же организация воспользовалась услугами внешнего исполнителя, как правило, этот же исполнитель осуществляет и сопровождение, что позволит организации-заказчику уменьшить (хотя и не исключить полностью) свое участие в решении данных вопросов.

Основной ошибкой и причиной многих проблем в процессе эксплуатации PKI является, на наш взгляд, непонимание того факта, что после внедрения PKI организация-заказчик безусловно принимает непосредственное участие во всех работах по эксплуатации этой инфраструктуры и наравне с исполнителем отвечает за результат. Ответственность за выполнение работ по сопровождению PKI лежит не только на обслуживающем персонале исполнителя, но и на конечных пользователях – сотрудниках организации. В частности, процедуры выдачи новых ключей и сертификатов, замены ключей и сертификатов выполняются при непосредственном участии пользователей (даже если процедуры максимально автоматизированы). Ответственность за хранение закрытых ключей, за эксплуатацию инфраструктуры PKI и использование сервисов PKI в соответствии с регламентирующими документами также лежит на пользователях, и их некорректная работа (по незнанию или умыслу) может стать причиной серьезных проблем.

Полностью обезопасить себя от подобных ситуаций невозможно: единственным вариантом представляется тщательная регламентация и документирование всех процессов эксплуатации инфраструктуры открытых ключей, проведение полноценного обучения пользователей (желательно с тестированием качества усвоения материала и выдачей сертификатов по итогам обучения), а также организация эффективного сопровождения и технической поддержки.