Как заставить PKI работать. Опыт Минобороны США

Н.А. Храмцовская
ведущий эксперт по управлению документацией компании “Электронные Офисные Системы”, член Гильдии Управляющих Документацией и ARMA International

CNews.ru, 22 января 2008 г.
http://www.cnews.ru/reviews/index.shtml?2008/01/22/284547_1

В нашей стране вопросам использования ЭЦП в органах государственной власти уделяется повышенное внимание, и многие министерства и ведомства весьма активно занимаются внедрением в свою повседневную практику технологий, основанных на использовании инфраструктуры открытых ключей (PKI). Опыт по внедрению PKI Минобороны США, возможно, позволит заранее подготовиться к процессу, избежать многих проблемных ситуаций, а также максимально эффективно организовать внедрение.

При создании инфраструктуры открытых ключей неизбежно появляются проблемы всевозможного характера: от технологических до организационных. Эти проблемы будут "тормозить" процесс внедрения и эксплуатации PKI, что, безусловно, увеличит временные и, прежде всего, финансовые затраты на проект. Здесь показателен опыт Министерства обороны США. В нем была развернута одна из крупнейших в мире инфраструктур PKI. По мере внедрения Минобороны сталкивалось с неочевидными на первый взгляд трудностями, каждая из которых требовала оптимального, быстрого и эффективного реагирования. Из полученного опыта можно извлечь некоторые полезные советы для построения глобальной структуры PKI в России.

Одна из основных проблем, с которой столкнулось Министерство обороны США после внедрения PKI, - массовое неприятие технологии PKI пользователями. Как показала практика, причиной "негатива" стала нехватка программ и средств обучения, специально ориентированных на их интересы.

Давно известно, что большинство пользователей воспримут новую технологию быстрее и лучше, если увидят реальную для себя пользу от ее применения. Первоначально этот фактор совершенно не учитывался - курс обучения основам PKI часто начинался с подробных объяснений концепций, лежащих в основе технологии открытых ключей. В результате, когда дело, наконец, доходило до практики, большинство обучающихся уже успевали внушить себе, что все это слишком сложно. Поскольку у сотрудников была возможность вести электронную почтовую переписку и без использования электронной подписи, очень часто они покидали курсы в уверенности, что PKI освоить трудно, да и незачем. Опережающее решение использовать смарт-карты привело к тому, что многие пользователи получили CAC-карты ("карты общего доступа") за несколько месяцев до получения устройств чтения этих карт, причем еще тогда, когда ни одна из систем не требовала использования электронных подписей.

В итоге для большинства пользователей опыт использования электронной подписи свелся к ожиданию в очереди на получение карт и к использованию CAC-карт так же, как ранее использовались идентификационные карты. Такие пользователи не увидели никакой реальной отдачи от новой технологии. Даже установка огромного количества считывателей смарт-карт и появление систем, поддерживающих технологию открытых ключей, пока не смогли сделать массовой технологию электронной подписи в Министерстве обороны США.

Еще одной сложной задачей оказалось преодоление организационных трудностей: как напрямую связанных с пользователями, руководителями и разработчиками инфраструктуры, так и общеорганизационных проблем, таких как координация общих процессов в корпоративной структуре такого масштаба, налаживание рабочего взаимодействия между совершенно различными подразделениями и определение того, какая из структур Министерства должна нести основную ответственность за каждый из элементов общей архитектуры PKI.

Помимо этого, в процессе внедрения возникали разные технические и технологические трудности, однако разобраться с ними оказалось несколько проще.

Несмотря на масштабность проекта, министерству обороны США удалось осуществить внедрение PKI в достаточно короткие сроки. Так, возможность использования технологии открытых ключей для защиты информации начала изучаться в 1997 году. Уже на следующий год был реализован тестовый вариант инфраструктуры PKI, а с 2000 года началось ее массовое развертывание.

Сначала определяется архитектура PKI

Для начала в Министерстве обороны был создан один корневой и нескольких подчиненных удостоверяющих центров (УЦ). Корневой УЦ выпускает сертификаты только для подчиненных УЦ, а сами подчиненные - пять типов сертификатов: личности, подписи, шифрования, подписания кода и сертификат на компоненты.

Сертификаты личности и подписи используются для аутентификации пользователя программного обеспечения и для электронного подписания документов и сообщений электронной почты. Адрес электронной почты в основной сертификат личности не включается, поскольку при постоянном перемещении персонала адреса электронной почты у многих часто изменяются. Сертификаты подписи и шифрования, наоборот, содержат адреса электронной почты. Новые "почтовые" сертификаты выпускаются при предъявлении действующего сертификата личности. Сертификаты на компоненты выпускаются для веб-серверов и других устройств. Сертификаты подписания кода выдаются отдельным подразделениям МО, которые допускают использование так называемых "мобильных кодов".

Помимо удостоверяющих центров были созданы: внутренний каталог серверов и депозитарий ключей (KED). Все связанные с сертификатами шифрования закрытые ключи перед выпуском сертификатов депонируются в депозитарии.

Выпуск сертификатов осуществляется в двух вариантах: в программном варианте и на внешних устройствах. Только в 2000-2005 годах удостоверяющими центрами Министерства обороны США было выпущено 3,5 миллиона цифровых сертификатов. 85% из них составляют так называемые "карты общего доступа" (CAC), которые выпускаются на внешних устройствах и выдаются всему персоналу Министерства обороны.

Инфраструктура открытых ключей МО США

Источник: Rebecca Nielsen, Booz Allen Hamilton "Observations from the Deployment of a Large Scale PKI"

"Карта общего доступа" представляет собой смарт-карту, поддерживающую язык Java и сертифицированную на соответствие требованиям уровня 2 федерального стандарта в области обработки информации FIPS 401. Java-карта была выбрана по двум критериям: во первых, помимо PKI, она позволяет обеспечивать использование и других функциональных возможностей. Кроме того, было учтено, что данный вид карты производится достаточно большим количеством фирм-поставщиков, что позволяет ведомству проводить реальный конкурс на их поставку. Удостоверение личности и выпуск сертификатов на CAC-картах проводятся с

использование существующей в Министерстве обороны системы выпуска персональных идентификационных карт. Поскольку УЦ не имеют возможности напрямую взаимодействовать с картами CAC, для упрощения процессов генерации ключей, создания запроса на сертификат и включения выпущенных сертификатов в действие используются "порталы выдачи".

Оставшиеся 15% составляют "программные" сертификаты, которые выпускаются и для сотрудников, и для веб-серверов и используются для поддержки ряда устаревших программных приложений, не поддерживающих аппаратные "токены", а также в случае затруднений с выдачей CAC-карт.

Для публикации необходимой для работы информации в Министерстве обороны была создана Глобальная служба каталогов (GDS), представляющая собой внутрикорпоративный справочник, содержащий сертификаты подчиненных УЦ, списки отозванных сертификатов (CRL), а также сертификаты шифрования. Кроме того, сертификаты подчиненных УЦ и списки отозванных сертификатов также публикуются и во внешней директории, что обеспечивает доступ к этой информации внешних пользователей.

Отзыв сертификатов осуществляется центрами регистрации. Восстановление ключей шифрования выполняется соответствующими "агентами", которые получают доступ к депозитарию ключей.

Еще в ходе проектирования инфраструктуры было проведено "тестирование под нагрузкой" для определения того, сколько сертификатов может выпускать отдельный УЦ. Однако при этом не были учтены другие функции, которые одновременно с выпуском сертификатов должен выполнять УЦ, такие как проверка удостоверяющих личность документов доверенных сотрудников, публикация и отзыв сертификатов, создание и публикация списков отозванных сертификатов, а также исполнение запросов на поиск определенных сертификатов. В результате данные тестирования производительности УЦ оказались сильно завышенными. Министерству обороны пришлось на ходу перестраивать работу удостоверяющих центров и создавать дополнительные центры регистрации с тем, чтобы обеспечить оперативность в работе.

Оборудование и технологии быстро "стареют"

Сама инфраструктура PKI Министерства обороны США рассчитана на долговременное использование. Срок правомочности корневого УЦ составляет 36 лет, а каждого подчиненного УЦ – 6 лет. Подчиненные УЦ выдают сертификаты в течение первых трех лет своего срока правомочности, после чего "уходят на покой" и в течение оставшихся трех лет только выпускают списки отозванных сертификатов. Полностью закрываются УЦ только тогда, когда истекает срок действия всех выданных ими сертификатов. Срок действия выданных государственным служащим CAC-карт составляет три года, а карты, выданные персоналу подрядчиков и поставщиков действительны не более года.

Министерству обороны США удалось осуществить внедрение PKI за три года

Такой подход позволяет проводить постепенную ротацию подчиненных удостоверяющих центров, а также дает возможность значительно сократить финансовые затраты на поддержание работы УЦ. Однако срок использования инфраструктуры PKI существенно отличается от сроков обновления оборудования и программного обеспечения. В результате спустя достаточно короткое время ни оборудование, ни программное обеспечение, используемые корневым УЦ минобороны, уже не поддерживаются

соответствующими поставщиками. Более "старые" подчиненные УЦ также вынуждены работать на неподдерживаемых версиях оборудования и ПО, вследствие чего увеличивается потребность в техническом обслуживании и существенно возрастает его стоимость.

Большие трудности приносит и постоянный процесс изменения используемых технологий. Так, когда корневой УЦ был открыт, использовались ключи длиной 512 бит, а максимальная длина ключа, поддерживавшаяся поставщиками, составляла 1024 бита. Сейчас стандартом являются ключи длиной 1024 бита, а федеральное правительство США уже включило в нормативную базу требования о том, что все сертификаты, срок действия которых заканчивается позже 2008 года, должны быть выпущены с ключами длиной 2048 бит.

Решить проблему "устаревания" оборудования и технологий можно двумя способами. Первый - миграция существующего корневого УЦ на новое оборудование и программное обеспечение, а второй - создание нового корневого УЦ и выпуск действующим корневым УЦ "переходного" (rollover) сертификата для нового корневого УЦ. В краткосрочной перспективе миграцию существующего корневого УЦ осуществить проще, однако проблема 1024-битовой длины ключа при этом не решится. С другой стороны, создание нового корневого удостоверяющего центра с ключом длиной 2048 бит потребует больших затрат на распространение нового ключа по всему используемому в министерстве ПО, где употребляются сертификаты, выпущенные инфраструктурой PKI Министерства обороны. Кроме того, в этом случае придется в течение 3-6 лет поддерживать в рабочем состоянии две инфраструктуры (до тех пор, пока не будут выведены из работы все ныне существующие подчиненные УЦ).

Сертификаты и CAC-карты нельзя изменить сразу

Также со временем изменений требуют и профили сертификатов. Так, PKI Министерства обороны первоначально не поддерживала расширения, необходимые для использования цифровых сертификатов для аутентификации сетей на базе Microsoft Windows.

Сертификаты в Windows

Windows требует наличия в сертификатах следующих расширений[1]:
1. должна быть указана точка распространения списков отозванных сертификатов;
2. атрибут "применение ключа" (Key Usage) должен иметь значение "цифровая подпись" (Digital Signature);
3. атрибут "расширенное применение ключа" (Extended Key Usage, EKU) должен содержать поле “Smart Card Logon Object Identifier” (следует отметить, что если атрибут EKU присутствует, он должен также содержать идентификаторы для всех остальных видов использования сертификата, таких как "авторизация клиента" - Client Authentication);
4. поле "альтернативное имя владельца сертификата" (Subject Alternative Name) должно содержать "основное имя пользователя" (User Principal Name, UPN) в формате user@name.com.

Когда требования были сформулированы и соответствующие изменения реализованы во всех подчиненных УЦ, все вновь выдаваемые CAC-карты стали содержать сертификат подписи, в котором имелась необходимая дополнительная информация. Однако Министерство проводит все изменения постепенно, по мере замены сертификатов (то есть полная замена сертификатов требует более трех лет). В связи с этим, в Министерстве обороны еще долго существовали пользователи, в CAC-картах которых эти расширения отсутствовали.

Помимо прочего, Министерство обороны столкнулось с необходимость налаживания миграции пользовательских смарт-карт. Поскольку срок действия большинства CAC-карт составляет три года, программное обеспечение, поддерживающее работу со смарт-картами (middleware), должно поддерживать технологии смарт-карт, использовавшиеся в течение последних трех лет.

В 2005 году в смарт-картах использовались чипы с 32K памяти, но Министерство обороны уже обдумывало возможность перехода на чипы с 64K. Новые чипы, помимо PKI, будут иметь дополнительные функциональные возможности. Замену карт планировалось проводить постепенно, по мере истечения их срока действия. В результате все пользователи Министерства обороны смогут воспользоваться новыми возможностями только тогда, когда закончится нормальный процесс замены старых карт, - т.е в течение трех лет придется использовать карты с разными возможностями, что будет создавать дополнительные трудности в работе.

Сначала сертификаты – потом карты

Развертывание системы удостоверяющих центров первоначально планировалось организовать следующим образом: Министерство обороны должно было централизованно управлять удостоверяющими центрами и остальными централизованными службами, а каждая служба и каждое агентство МО должны были выделить персонал для работы в центрах регистрации. На деле подразделения, первыми осваивавшие PKI, столкнулись с повсеместным отсутствием центров регистрации. На местах упорно не желали выделять дополнительный персонал и оплачивать расходы, связанные с обучением специалистов центров регистрации. Это создало реальную угрозу всему проекту.

Надо сказать, что Министерство обороны весьма грамотно вышло из тупика. Проанализировав сложившуюся ситуацию, в ноябре 1999 года было принято политическое решение: объединить программу развертывания инфраструктуры PKI и программу выдачи новых идентификационных карт всем гражданским и военным служащим Министерства, которую в это время реализовывало кадровое управление МО. Сотрудники управления по PKI и кадрового управления совместно продумали технологию, по которой существующие пункты выдачи идентификационных карт стали использоваться и для удостоверения личности, и для выдачи сертификатов вместе с картами.

Однако по ряду причин количество пунктов выдачи персоналу идентификационных карт пришлось увеличить. Так, до появления CAC-карт идентификационные карты выдавались только военным - CAC-карты же, помимо этого, стали выдаваться также гражданским служащим и персоналу подрядчиков Министерства обороны. Кроме того, выпуск CAC-карт занимает больше времени, чем выпуск старых идентификационных карт.

В настоящее время в министерстве создано свыше 2000 авторизованных центров регистрации. Такое количество породило еще одну непростую проблему, связанную с большой текучестью кадров в центрах регистрации и необходимостью частого обновления списка авторизованных сотрудников центров регистрации.

Для того чтобы обеспечить непрерывность выпуска сертификатов, в случае, например, если один или несколько УЦ по каким-либо причинам оказались недоступны, все сотрудники центров регистрации авторизованы всеми удостоверяющими центрами. Однако лишь в ходе внедрения выяснилось, что предоставленное поставщиком ПО для управления доверенным персоналом не позволяло поддерживать работу такого большого числа сотрудников центров регистрации и частое обновление списка таких сотрудников. Эта проблема была решена с помощью специально разработанных скриптов, позволяющих быстро загрузить во все УЦ информацию об изменениях в кадровом составе центров регистрации.

Объединение процесса выпуска сертификатов с выпуском идентификационных карт дало существенный выигрыш, поскольку позволило использовать при внедрении технологии ЭЦП существующую инфраструктуру идентификационных карт и минимизировать потребность служб и агентств в дополнительном персонале. Такой подход значительно упростил и процесс распространения сертификатов.

COC слишком "громоздки" для отдельного ПО

Новая технология позволила более эффективно и оперативно решать стоящие перед Министерством обороны задачи. В то же время при ее интеграции с уже используемым ПО возникли серьезные трудности. Опыт работы показал, что одной из наиболее сложных технических проблем стала проверка того, отозван сертификат или нет.

В теории "элегантным" решением могут стать списки отозванных сертификатов. Они являются документом, при помощи которого УЦ заявляет, что он более не удостоверяет связь между указанной в сертификате личностью и соответствующей парой ключей. Списки отозванных сертификатов содержат минимальное количество данных, как то серийный номер сертификата, а также дату и отзыва.

Однако сам процесс создания списков отозванных сертификатов является сложным и не очень удобным для оперативной работы, поскольку он требует значительного времени на обработку данных удостоверяющего центра. Так, при составлении списков не только определяется, какие сертификаты были отозваны, - одновременно с этим из списка отозванных сертификатов исключаются те из них, срок действия которых закончился. Для удостоверяющих центров, выпускающих большое число сертификатов, требование проверить каждый отозванный сертификат на истечение срока действия может привести к тому, что время на создание списка может превысить установленный период его обновления. Если же подобную проверку не проводить, общий размер списка увеличивается из-за того, что в него включаются сертификаты с уже истекшим сроком действия. Это еще больше затрудняет работу.

На практике списки отозванных сертификатов (COC) показали себя не очень хорошо. Так, программные продукты, использующие цифровые сертификаты, лишь в минимальной степени поддерживают использование COC. В ряде случаев отсутствует какая-либо автоматизация скачивания COC. Если же ПО предоставляет возможность автоматического обновления, часто отсутствует возможность задавать, когда именно будет производиться попытка получения нового COC. Поскольку в Министерстве обороны используется большое количество различного программного обеспечения, то часто это приводит к тому, что целый ряд программных приложений одновременно пытается получить доступ к хранилищу COC.

При разработке одного из программных приложений поставщик решил трактовать значение поля "дата следующего обновления" COC как окончание срока действия COC, что привело к тому, что это ПО не подтверждает действительность сертификатов, выданных теми УЦ, для которых отсутствуют "текущие" COC. Кроме того, содержащаяся в COC информация актуальна лишь на момент публикации, что приводит к серьезным проблемам, связанным с запаздыванием публикации информации об изменениях.

Масштаб инфраструктуры PKI Министерства обороны влечет за собой дополнительную проблему – большой размер COC. Суммарный размер COC всех УЦ Министерства обороны достигает 40 мегабайт. Когда каждое ПО в сети Министерства обороны каждый день скачивает такой объем данных, это неизбежно существенно сказывается на пропускной способности сети. Ни одно отдельно взятое ПО не имеет в качестве своих пользователей всех абонентов инфраструктуры PKI, поэтому каждое отдельное приложение нуждается лишь в подмножестве этой информации. Но поскольку корпоративная PKI заранее не знает, какое подмножество данных нужно для каждого из приложений, то всем ПО представляется общий список отозванных сертификатов.

Специалистами были предложены два альтернативных подхода к составлению и использованию COC. Первый заключался в том, что центр, создающий COC, разделяет сертификаты на блоки заранее установленного размера (сегменты), основываясь на содержащейся в сертификате информации (такой, как серийный номер). Вместо выпуска одного списка COC, УЦ выпускает несколько COC – по одному для каждого предустановленного блока сертификатов. Когда ПО пытается проверить сертификат, оно проверяет, есть ли действующий COC для соответствующего блока сертификатов, и если нет – скачивает его. Хотя использование сегментированных COC позволяет приложениям запрашивать ограниченный объем информации, связанной с отзывом сертификатов, реализовать такое решение пока не удалось. Это связано с тем, что у УЦ отсутствует возможность поддерживать такой режим работы со списками. Кроме того, такие возможности работы должны быть заложены и в используемое для работы ПО. Идея второго подхода состоит в том, что удостоверяющий центр выпускает полный список COC лишь однажды либо периодически, а затем лишь выпускает списки, которые содержат сведения о сертификатах, отозванных с момента выпуска предыдущего. Объем таких списков, естественно, намного меньше. В то же время, в программных приложениях должен иметься механизм, обеспечивающий скачивание всех частей списка – поскольку ни одна его часть сама по себе не является авторитетным источником информации о текущем статусе отдельно взятого сертификата. Хотя инфраструктура открытых ключей Министерства обороны не поддерживает данный метод формирования COC, одно из агентств МО успешно опробовало такой подход для передачи информации об отзыве сертификатов в условиях сильно ограниченной пропускной способности сети.

В целом, списки отозванных сертификатов оказались эффективным способом передачи информации об отзыве сертификатов в сетях с высокой пропускной способностью, но при этом чересчур "громоздкими" при доставке этой информации отдельным программным приложениям.

Сертификаты проверяются онлайн

Существует и еще одна проблема. Запрашивая отзыв сертификата, большинство пользователей и руководителей не знают серийного номера сертификата, и того, каким УЦ он был выпущен. При разработке технологии работы удостоверяющих центров этот "нюансик" также не был учтен. В результате, прежде чем авторизовать отзыв соответствующего сертификата, специалисты вынуждены проводить поиск по множеству УЦ для его локализации. Это, в свою очередь, требует возможность прямого поиска во внутренних базах УЦ, что, соответственно, удлиняет время, требуемое для отзыва сертификата, влечет за собой риски его неправомочного использования, увеличивает трудозатраты на осуществление данной процедуры и загрузку внутренних сетей.

Непрекращающиеся проблемы при выполнении проверки сертификатов с использованием COC вынудили МО начать работу по организации проверки статуса сертификатов с использованием "протокола определения статуса сертификата в реальном времени" (On-line Certificate Status Protocol, OCSP). Это означает, что программные приложения, вместо скачивания COC, будут иметь возможность получать в реальном времени ответы на запросы о статусе конкретных сертификатов из глобальной системы проверки сертификатов. Хотя использование COC в качестве авторитетного источника информации об отзыве сертификатов не решает вопросов, связанных с запаздыванием получения информации, - гибридный подход, предусматривающий совместное применение списков отозванных сертификатов и возможности определения статуса сертификата в реальном времени, дает возможность использовать списки гораздо более эффективно.

Убеждение – залог успешного финансирования

Проблемы, с которыми столкнулись в Министерстве обороны США при финансировании внедрения электронных подписей можно разделить на две группы: специфические проблемы, связанные с особенностями системы финансирования органов государственной власти США, и общие проблемы финансирования, свойственные большинству органов государственной власти различных стран.

К первой группе можно отнести различие в модели финансирования. Так, финансирование компонентов ядра PKI (удостоверяющие центры и т.д.) и закупки смарт-карт осуществляется централизованно, в то время как финансирование закупок ПО (включая системы электронной почты, сети и веб-сервера) децентрализовано. И если развертывание собственно инфраструктуры PKI потребовало всего нескольких решений на уровне руководства Министерства обороны, то интеграция технологии открытых ключей в используемое ПО потребовала принятия большого числа решений многочисленных подразделений и организаций, входящих в систему Министерства обороны.

Опыт Министерства обороны США показал, что для того, чтобы руководитель организации в условиях достаточно ограниченных финансовых ресурсов принял решение о финансировании интеграции PKI в используемую в его подразделении или организации систему, ему нужна подробная информация, необходимая для принятия этого решения. Кроме того, требуется заранее создать достаточную внутреннюю нормативную базу, основываясь на которой, руководитель любого подразделения или организации мог бы грамотно обосновать необходимость финансирования данной работы. В организации обязательно должна быть разработана внутренняя политика в отношении использования технологии открытых ключей и ее интеграции со всеми имеющимися информационными ресурсами. Наличие такого документа позволяет тем, кто первыми внедряет новую технологию, обосновать свои инвестиции.

Желательно, чтобы средства на интеграцию технологии открытых ключей в информационные системы выделялись в рамках обычного процесса составления бюджета организации. В противном случае, скорее всего, придется пожертвовать ради PKI другими запланированными расходами, на что многие руководители идут неохотно. Необходимо заранее изучить существующие информационные системы, чтобы на реальных примерах показать, какие слабые места в них имеются и каким образом использование PKI может помочь исправить положение.

Нельзя аргументировать внедрение PKI одной только необходимостью обеспечения безопасности систем. Нужно выявить и убедительно обосновать деловые преимущества применения PKI, включая более эффективное управление пользователями, упрощение управление паролями и новые функциональные возможности.

Отдачу покажет использование технологий в информационных системах

Использование технологии в информационных системах является ключевым этапом, позволяющим показать отдачу от инвестиций в PKI. Основным вопросом является организация получения пользователями ключевых сертификатов. Когда в конце 90-х годов были сделаны первые попытки применения PKI в ряде имеющихся в Министерстве обороны систем, во всех случаях интеграция PKI задержалась из-за того, что пользователи не смогли вовремя пройти регистрацию и получить сертификаты.

На основе опыта по внедрению инфраструктуры PKI специалистами Министерства обороны США были сделаны несколько важных выводов, которые являются достаточно универсальными и поэтому могут рассматриваться как общие рекомендации, применимые, в том числе, и теми органами государственной власти нашей страны, которые планируют широкомасштабное развертывание аналогичных инфраструктур.

Так, при развертывании инфраструктуры PKI Министерство обороны США столкнулось с рядом технических проблем, однако с проблемой масштабирования PKI справляется гораздо успешнее других технологий. Благодаря интеграции процесса выпуска сертификатов с существующими процессами управления персоналом, PKI Министерства обороны смогло осуществить удостоверение личности при личном присутствии более трех миллионов пользователей. Единственным базовым блоком инфраструктуры PKI, который не удалось успешно масштабировать, оказались списки отозванных сертификатов, однако Министерство обороны планирует преодолеть это препятствие за счет использования протокола OCSP. Для достижения успеха при внедрении PKI кроме всего прочего требуется, чтобы сначала были решены проблемы, существующие в деловых процессах.

Министерство обороны США рассматривает внедрение PKI как долговременные инвестиции, поскольку владельцы информационных ресурсов не желают приступать к использованию сертификатов до тех пор, пока не убедятся, что все их пользователи в состоянии получить эти сертификаты. Отдача от инвестиций в PKI ощущается тогда, когда начинается широкое использование этой технологии. На этом пути встречаются трудности, но потенциал технологии открытых ключей важен для обеспечения доверия к информации и улучшения деловых процессов[2].

---

1 "Guidelines for Enabling Smart Card Logon with Third-Party Certification Authorities", Microsoft Knowledge Base Article 281245. http://support.microsoft.com/default.aspx?scid=kb;en-us;281245

2 По материалам Rebecca Nielsen, Booz Allen Hamilton "Observations from the Deployment of a Large Scale PKI" in: Proceedings of the 4-th Annual PKI R&D Workshop: "Multiple Paths to Trust", April 19-21, 2005, NIST, Gaithersburg MD, http://middleware.internet2.edu/pki05/proceedings/nielsen-large_pki.pdf