О смене ключей в инфраструктуре открытых ключей

Белов С.В.,
Мартыненко С.В., канд.физ.-мат.наук

Внедрение Инфраструктуры открытых ключей (PKI, Public Key Infrastructure) в области банковского дела, в органах власти, а также в коммерческих предприятиях, включая электронную коммерцию, становится реальностью в Украине [1]. При этом (частично) создана иерархически структурированная инфраструктура PKI, в которой проверка действительности/ валидности X.509 сертификата зависит от сертификата корневого (Root) центра сертификации ключей (ЦСК) и цепочки подчиненных ему ЦСК (в дальнейшем – учреждения сертификации или инстанции иерархии сертификации). Корневым ЦСК в Украине является [1] Центральный удостоверяющий орган (ЦУО), и иерархическая структура цепочки ЦСК может состоять из таких уровней: ЦУО, Удостоверяющий центр (УЦ, в органах государственной власти), Аккредитованный ЦСК (АЦСК) или Зарегистрированный ЦСК (ЗЦСК).

Поскольку срок сертификата ЦСК каждого уровня цепочки не является бесконечным и периодически истекает, или сертификат может блокироваться и, тем самым, прекращается его время жизни, то существует задача/проблема выдачи нового сертификата как корневому ЦСК, то есть ЦУО, так и всем ЦСК цепочки, с последующим достоверным распределением новых сертификатов ЦСК всем участникам PKI без того, чтобы при этом ухудшились эксплуатационные характеристики.

Как показывает практика, до сих пор в Украине не рассматривались вопросы решения задачи, связанной с заменой сертификатов ЦСК в целом, и ЦУО в частности, а потому эта задача уже переходит в область проблемы. Такая «экономия» технически, видимо, связана с надеждой, что проблему можно будет решить потом, «через несколько лет», когда настанет необходимость. Но и «через несколько лет» нет эффективного плана замены, а тем более плана действий в непредвиденных обстоятельствах для случая, когда будет необходима срочная замена сертификата ЦУО, АЦСК и др. до истечения его срока их действия, например, из-за компрометации ключа. Такое положение является критическим для жизни систем электронного документооборота в государстве.

В этой публикации обсуждается ряд вопросов, связанных с заменой ключей ЦСК; обсуждаются и оцениваются возможные модели и решения.

Определения терминов

Период применимости (applicability-period) личного ключа ЦСК – это период, в котором личный ключ ЦСК является действительным и может применяться для определенных целей. Период применимости личного ключа равен периоду действительности его сертификата.

Период минимальной пригодности (availability-period) личного ключа ЦСК – это период, в котором ЦСК может выполнять операции сертификации этим актуальным личным ключом; но по истечении этого периода применимости ЦСК может только обслуживать списки отзыва и другие дополнительные службы, не связанные с выдачей новых сертификатов.

Основные требования

В настоящее время законодательство Украины предусматривает, что учреждения сертификации (АЦСК, ЗЦСК) предлагают свои услуги на основе конкуренции. Поэтому дружественность к клиентам, в отношениях с конечными пользователями, является основной предпосылкой для успешного бизнеса учреждений сертификации. Также законодательством предусматривается, что АЦСК предлагают услуги от имени (для) государственного сектора,

где дружественность к клиентам – это уже лицо государственного органа, от имени которого такие услуги предлагаются.

Клиент получает ключ электронной цифровой подписи (ЭЦП), чтобы подписывать цифровые документы. Он заинтересован в том, чтобы в любое время иметь законную цифровую подпись. Технически он должен располагать для этого в любое время действительным ключом подписи. Поэтому как минимальное требование к иерархии сертификации устанавливается такое:

Требование 1 (действительный ключ сертификации): Каждая инстанция иерархии сертификации должна быть способна в любое время располагать действительным ключом подписи/сертификации.

Для того чтобы обмен подписанными цифровыми документами, с учетом времени их передачи, был приемлемым, ключ подписи должен оставаться действительным после формирования подписи (подписывания документа) еще определенный промежуток времени. Поэтому гарантия действительности ключа подписи является критерием дружественности учреждений сертификации к клиентам.

Проверка подписи является процессом, который может быть выполнен по-разному, например:

- от имени физического лица, используя свое рабочее место и соответствующее программное обеспечение для проверки полученной подписи;
- с помощью компьютерной программы, т.е. с помощью автоматизированной процедуры.

Директива 1999/93/ЕС [3] упоминает о «данных, отображаемых для верификатора», которые могут быть истолкованы как то, что верификатор – это физическое лицо. Тем не менее, второй случай полезен в электронной коммерции, где так необходима автоматизированная проверка подписи. Таким образом, термин «отображается» следует толковать в более общем смысле, как «представлены», так как подписанные данные могут быть любыми видами носителей информации (текст, звук, видео и т.д.).

Правила процедуры верификации определены стандартом ДСТУ CWA 14171:2008 [2] как для проверки физическими лицами, так и для автоматизированной проверки подписи. Ниже перечислены основные стороны, участвующие в бизнес-транзакциях, поддерживающих электронные подписи:

- Подписант (Signer) – является лицом, которое создает ЭЦП.
- Верификатор (Verifier) – является лицом, которое проверяет ЭЦП, это может быть одно лицо или несколько лиц;
- Поставщик услуг сертификации (Certification Service Provider, CSP) – один или несколько поставщиков услуг, чтобы помочь построить доверие в отношениях между подписантом и верификатором, т.е. учреждения сертификации, ЦСК;
- Арбитр (Arbitrator) – для возможности арбитража споров между подписантом и верификатором.

Подписавшийся должен обеспечивать, по крайней мере, основную форму/ формат электронной подписи (BES, Basic Electronic Signature). Это форма не защищает против всех потенциальных угроз, вызванных отзывом сертификатов подписанта или ЦСК. Преимущество базовой подписи является то, что она может быть создана без доступа к онлайн вспомогательным услугам. Однако базовая электронная подпись может быть недостаточной в случае некоторых срочных сделок, где критичным является время транзакции (биржевые сделки и др.). Эта форма также является недостаточной для разрешения споров в долгосрочной перспективе. Для того чтобы обеспечить долговременные свойства проверки, требуется некоторая дополнительная информация после того, как электронная подпись была

сгенерирована. Поэтому, чтобы различать эти различные обстоятельства, стандарт ДСТУ CWA 14171:2008 [2] использует два разных термина: первоначальная проверка и последующая проверка.

Первоначальная проверка должна быть выполнена в удобное время после формирования электронной подписи для того, чтобы захватить дополнительную информацию, которая будет использоваться последующей проверкой, потенциально в течение длительного срока. Такой дополнительной информацией является информация относительно статуса сертификата подписанта и времени подписания. Если такие данные собраны правильно, то последующие проверки могут быть успешно выполнены через ряд лет после формирования подписи. Для архивных системы, возможно, потребуется больше данных, например, если использованная на момент подписания криптография впоследствии будет признана недостаточно сильной для того, чтобы защитить архивные данные.

Таким образом, подписанный документ является действительным при первоначальной проверке, если является действительным, в частности, сертификат подписанта. При этом законность/действительность подписанного документа является независимой от даты проверки подписи. Хотя подпись в зависимости от технического развития с течением времени может изменяться, однако, инфраструктура сертификации должна быть рассчитана таким образом, чтобы в нормальном/ штатном случае действительная подпись на определенный момент времени тестирования (проверки) не воспринималась как недействительная и наоборот.

Поэтому имеем такое требование:

Требование 2 (сертификаты «прямого» действия): Инфраструктура сертификации должна быть сконструирована таким образом, чтобы при нормальных/ штатных обстоятельствах не может действительная подпись на определенное время проверки оказаться недействительной, и наоборот. ЦСК не должен выдавать сертификаты «обратного действия», т.е. когда начало действия сертификата установлено на дату более раннюю, чем дата создания сертификата.

Это требование касается сертификатов новых ключей подписи. Продление срока жизни ключа и выпуск, в связи с этим, нового сертификата не относится к этому правилу, но подчиняется правилу 3 (ниже).

Конечно, рассматриваемую здесь проблему смены ключей ЦСК можно «решить», выпустив сертификаты ЦСК сроком на лет так 50 (по правилу Насреддина: «либо ишак, либо эмир…»). В связи с этим такое требование:

Требование 3 (надежность ключа сертификации): Срок жизни ключа ЦСК и его сертификата должен быть криптографически обоснован стойкостью ключа, с учетом возможной его компрометации в процессе эксплуатации, в том числе из-за возможных недостатков и рисков в организационных мерах безопасности.

Как известно, безопасность личного ключа не может обеспечиваться без дополнительных организационных мер безопасности, несоблюдение которых может приводить к компрометации ключа. Например, смена администратора сертификации ЦСК может иметь последствием компрометацию ключа ЦСК.

Таким образом, конечные пользователи иерархии сертификации должны иметь гарантии, что они располагают в любое время действительным ключом подписи с гарантированным сроком действия и вместе с тем с гарантированной пригодностью.

Это связано с тем, что ключ подписи любого уровня PKI действителен только, если существует цепочка действительных сертификатов от участника вплоть до корня иерархии сертификации (ЦУО). Тем не менее, клиент не имеет влияния на действительность сертификатов этой цепочки (так называемого пути сертификации), хотя действительность его ключа подписи непосредственно зависит от них. При изменении сертификата в этой последовательности может последовать принципиальная ненадежность клиентов относительно дальнейшей действительности их ключа подписи.

Модели изменения ключей в иерархии сертификации и определении действительности

Рассмотрим n-ступенчатую иерархию сертификации, при которой инстанцией уровня n является корень, а конечные пользователи являются инстанцией уровня 1 (согласно украинского законодательства n=4, если присутствует Удостоверяющий центр, иначе n=3). Для перехода от текущего уровня на следующий используется сертификат C, срок действительности которого определен от даты начала S(C) до даты окончания E(C) сертификата (в соответствии с X.509).

Обозначим через V(C) период действительности/ валидности (validity) сертификата C. Для простоты будем рассматривать арифметику с непрерывным временем, так что:

$$V(C) = E(C) - S(C).$$

Для $i<n$ обозначим через C(i) сертификат инстанции уровня i, выданный инстанцией уровня (i+1). C(n) является тогда само-подписанным сертификатом инстанции корня (корневым).

Определение действительности базируется на понятии пути сертификации:

Путь сертификации C(1), C(2)..., C(n) ключевых пар - это цепочка сертификатов, где

1) последний член C(n) - это сертификат инстанции корня,
2) первый член C(1) – это сертификат конечного пользователя, и
3) для каждого сертификата C(i), $i<n$, цепочки: открытый ключ ключевой пары C(i) удостоверяется сертификатом C(i+1) цепочки.

В соответствии с RFC 5280:2008 [3] действительность (сертификата) ключа определена, как указано ниже:

1) Ключ подписи (сертификат) ступени i, $i \leq n$, является действительным на дату t, если принадлежащий ему путь сертификации (C (i), C (i+1)..., C (n)) существует и действителен на дату t;
2) Путь сертификации действителен на дату t, если каждый появляющийся в нем сертификат действителен на эту дату;
3) Сертификат C (j) действителен на дату t, если
   a) подпись сертификата математически правильна,
   b) дата t действительности C (j) принадлежит интервалу: $S(C(j)) \leq t \leq E(C(j))$ и
   c) сертификат на дату t не указан в действительном CRL списке отозванных сертификатов.

Пусть сертификаты имеют математически правильную подпись и не указаны в действительном CRL списке отозванных сертификатов. Тогда определение действительности (сертификата) ключа сокращается до [3]:

Ключ подписи/ сертификат степени i, $i \leq n$, действителен на дату t, если для каждого сертификата C(j) принадлежащего пути сертификации (C (i), C (i+1)..., C (n)) имеет место: $S(C(j)) \leq t \leq E(C(j))$.

При таком определении действительности сертификата может иметь место случай, когда сертификат сам по себе действителен, хотя ключ его сертификации (ЦСК), больше не является действительным. Чтобы показать, когда сертификат может быть занесен в действительный путь сертификации, определим *применимости сертификата* [3]:

Сертификат действителен на дату t, если ключевая пара, которой выдавался сертификат, действительна на дату t.

Таким образом, если использовать это определение применимости, то определение действительности эквивалентно следующему рекурсивному определению:

Ключ подписи/сертификат ступени i, i ≤ n, действителен на дату t тогда и только тогда, когда он заверен применимым действительным на дату t сертификатом C(i).

Следуя [3], исследуем, какие последствия имеет изменение сертификата уровня i.

Пусть (C(1), C(2)..., C(i)..., C(n)) – действительный путь сертификации, при котором на ступени i сертификат C(i) заменяется новым сертификатом C2(i). Исследуем изменения, которые требуются (минимально), чтобы получить снова действительный путь сертификации.

При изменении сертификата либо срок действия прежнего ключа (ключевой пары) продлевается, либо ключ (ключевая пара) заменяется новым. Итак, имеем:

1 **Продление ключа**: При продлении ключа прежний открытый ключ ступени i сертифицируется подписанием документа-сертификата личным ключом ступени i+1 и получает новый период действия. Так как открытый ключ не изменяется, то остаются действительными сертификаты ступени i-1, которые сертифицировались этим ключом. Следовательно, изменение сертификата является свободным от влияний (воздействия на валидность цепочки). Поэтому без дальнейших изменений является действительным и новый путь сертификации (C(1), C(2)..., C(i-1), C2(i), C(i+1)..., C(n)).

2 **Замена ключа**: При замене ключа (ключевой пары) на уровне i все выданные прежним ключом сертификаты ступени i-1 теряют их действительность. В пути сертификации должен заменяться и C(i-1) на новый сертификат C2(i-1), который должен быть заверен сертификатом C2(i) и т.д. Новый действительный путь сертификации получается следующим: (C(1), C(2)..., C(i-2), C2(i-1), C2(i), C2(i+1)..., C2(n)).

В обоих случаях локальное изменение пути сертификации является достаточным, чтобы восстановить действительность пути. Поэтому мы можем при исследовании различных моделей гарантии ограничиваться рассмотрением изолированных двух, следующих друг за другом, уровней i и i+1 иерархии сертификации.

Локальные модели изменения ключей

В дальнейшем будем рассматривать инстанцию уровня i и обозначаем как TN (участник), а соответствующее учреждение сертификации (ЦСК) уровня i+1 коротко обозначаем как CA (Certification Authority, орган/ центр сертификации). Обозначаем C(TN) для C (i) и C(CA) для C (i+1).

Опишем разные модели изменения ключа между 2-мя смежными уровнями i, i+1 и требования к вышестоящим уровням иерархии i+1..., n, которые являются предпосылками для реализации модели.

Локальная модель №1: никакой гарантии действительности

При этой модели CA выдает сертификаты с их актуально действительным ключом, не учитывая, как долго их ключ еще будет действительным. Вследствие этого для TN получается ситуация, что срок действия ключа ограничен потенциально самым ранним сроком окончания срока действия сертификата в его пути сертификации (C (i), C (i+1)..., C (n)): min {E (C (j)): $i \leq j \leq n$}.

Рассмотрим случай, когда окончание срока действия E(C(CA)) лежит до окончания срока действия E(C(TN)) сертификата TN. После даты E(C(CA)) прежний путь сертификации больше не будет подтверждать действительность ключа TN.

TN должен сам проверять (например, поиском в перечне/каталоге CA) в этом случае, применим ли еще его сертификат, или он нуждается в новом сертификате. Он должен отслеживать изменение сертификата и разрешить/ запросить CA сертифицировать по-новому его ключ в случае изменения ключа CA.

Требования к вышестоящим этапам иерархии:

В этой модели не имеется никаких требований к инстанциям вышестоящих уровней иерархии. Инстанции каждого уровня ответственны сами за то, чтобы иметь действительный ключ подписи.

Локальная модель №1b: выполнение минимального требования иерархии

Минимальное требование, что каждая инстанция должна иметь возможность располагать в любое время действительным ключом, не выполнено в модели №1, как указывает такой пример:

TN требует в настоящее время t1 < E(C(CA)) новый сертификат с началом срока действия S(C(TN)) = E(C(CA)) таким же, как для CA, так как он знает, что CA на эту дату меняет свой ключ, и вследствие этого прежний ключ будет недействителен. CA производит свой новый ключ к дате t2. Однако, имеющегося в распоряжении периода E(C(CA)) недостаточно, чтобы выполнить требования замены сертификата TN. TN получает новый сертификат с опозданием к дате после E(C(CA)).

Причиной задержки может быть либо то, что CA с опозданием создает новый ключ, либо то, что TN несвоевременно запрашивает новый сертификат.

В модели №1b должно выполняться минимальное требование. Для этого CA должен заботиться о том, чтобы поставить к требуемой дате его новый ключ, и чтобы оставалось до конца срока действия прежнего ключа «достаточное» время для того, чтобы выполнить запрошенные пост-сертификации. Очевидно, что необходимый для этого промежуток времени зависит от того, сколько пост-сертификаций должен выполнить CA (сколько клиентов имеет CA).

При этом под пост-сертификацией мы понимаем повторную сертификацию того же ключа TN, но с новым ключом CA на остаток указанного в прежнем свидетельстве TN срока действия. Конечно, можно комбинировать пост-сертификацию с продлением срока ключа.

TN отвечает за то, чтобы своевременно запросить новый сертификат для того, чтобы он располагал в любое время действительным ключом.

Требования к вышестоящим этапам иерархии:

CA должен располагать в любое время действительным ключом сертификации. Вышестоящая инстанция должна выполнять для этого своевременно требования сертификации от CA. Поэтому рекурсивно возникает требование располагать своевременно новым ключом сертификации ко всем учреждениям сертификации, вплоть до инстанции корня.

Локальная модель №2: гарантия действительности ключа

Эта модель отличается тем, что TN через сертификат, который он получает от CA, гарантируется, что сертифицированный ключ подписи TN действителен на весь срок действия сертификата.

Тем не менее, эта гарантия относится только к ключу подписи: Как сертификат TN, так и другие сертификаты в пути сертификации ключа могут изменяться. Лишь гарантируется, что имеется в любое время действительный путь сертификации для ключа.

Если имеет место замена ключа в течение указанного в сертификате срока действия CA, то беспрерывность действия ключа подписи TN должна гарантироваться CA посредством своевременной пост-сертификации.

Ответственность за обновление/актуализацию информации, в случае ненадежности/неуверенности о действительности пути сертификации или ненадежности/неуверенности о текущей действительности сертификата, возлагается на TN.

Локальная модель №2b: гарантия действительности ключа для минимального периода времени VK (i):

По причине дружественности к клиентам, для CA невозможно, как правило, сокращать затребованные сроки действия сертификатов на сколь угодно короткие от установленных промежутков времени. Скорее должен иметься период VK (i) (VK = validity key) действительности ключа такой, что CA может выставлять в любое время сертификаты с минимальным периодом действия VK (i), для которого гарантируется действительность ключа TN.

Требования к вышестоящим уровням иерархии:

Для вышестоящих этапов иерархии получаются требования такие же, как для модели №1b.

Так как CA на уровне i+1, в противоположность модели №1b, должен проводить пост-сертификации без предварительного уведомления, то CA может лучше оценивать необходимый для этого промежуток времени. Пусть dt – это промежуток времени, который необходим CA для пост-сертификаций. Чтобы своевременно провести пост-сертификацию TN-ключа при изменении ключа CA, CA должен располагать новым ключом, начиная с даты E(C(CA))-dt. Период действия этого ключа CA должен перекрывать, по меньшей мере, период $\{ E(C(CA)),\ E(C(CA))+dt \}$, гарантируя себе, таким образом, промежуток времени для выполнения пост-сертификации.

Локальная модель №3: гарантия применимости сертификата

В этой модели CA гарантирует не только действительность ключа TN на указанный в сертификате период, а, исходя из этого периода, и применимость его сертификата. До сертификата TN путь сертификации может дальше изменяться.

К компетенции TN относится то, чтобы TN соответственно уведомлялись об актуальном пути сертификации после изменения сертификата на вышестоящих уровнях иерархии.

CA может давать эту гарантию только в случае, если общий(весь) период действия TN-сертификата лежит в пределах периода действия его (CA) ключа сертификации. Действительность ключа сертификации может гарантировать CA, однако, не за пределами периода действия, который указан в сертификате. Поэтому общий(весь) период действия сертификата TN должен лежать в пределах периода действия CA-сертификата:

$S(C(TN)) \geq S(C(CA))$ и
$E(C(TN)) \leq E(C(CA))$.

Если мы заменим $E(C(TN))$ в выражении

$$E(C(TN)) \leq E(C(CA))$$

на значение

$$E(C(TN)) = S(C(TN)) + V(C(TN)),$$

то получим

$$S(C(TN)) \leq E(C(CA)) - V(C(TN)).$$

Из этого неравенства можно получить 2 разных сценария:

1 В модели №3a CA определяет период действия затребованного TN-сертификата в зависимости от заявленного для этого сертификата начала срока.

2 В модели №3b мы рассматриваем затребованный TN период срока действия, в качестве заявленного, и получаем ограничение применимости актуального ключа сертификации CA.

Локальная модель №3a: гарантия зависимости от окончания срока действия CA сертификата

Если мы предполагаем начало срока $S(C(TN))$ для сертификата TN как заявленное, сертификат TN может быть выпущен максимум на период срока $V(C(TN)) = E(C(CA)) – S(C(TN))$ до окончания срока CA сертификата.

Сокращение срока сертификата на сколь угодно малые промежутки времени может выполняться CA при каждом требовании. Это, из соображения приветливости/дружественности к клиентам, представляется неприемлемым. Скорее должен иметься период $V(C(i))$ (validity certificate) такой, в котором CA выпускает только сертификаты с гарантированным минимальным сроком применимости $V(C (i))$. Поэтому модель №3a дальше не будет исследоваться.

Локальная модель №3b: гарантия применимости сертификата для минимального интервала времени

Если мы рассматриваем затребованный интервал времени действительности $V(C(TN))$ в качестве заявленного, то TN-сертификат может выпускаться только текущим CA ключом, если CA ключ, начиная с текущей даты t еще, по меньшей мере, на период $V(C(TN))$ остается действительным: $t + V(C(TN)) \leq E(C(CA))$.

Вследствие этого, срок использования текущего CA ключа ограничивается для выпуска TN-сертификатов:

CA не может выпускать никакие сертификаты, используя текущий актуальный ключ, со сроком действия V больше, чем предельная дата E(C(CA)) - V.

Пусть теперь $VC (i)$ – определенный CA период, для которого CA гарантирует TN, что он выпускает сертификаты с гарантированным периодом действия $VC(i)$. Тогда CA может применять свой текущий актуальный ключ сертификации только до даты $E(C(CA)) - VC(i)$. Мы

обозначим эту дату через EA(C(CA)), как дату окончания применимости личного ключа сертификации CA:

EA(C(CA)): = E(C(CA)) - VC(i)

После даты EA (C (ОКОЛО)) для CA возникает необходимость сертифицировать при помощи другого ключа, окончание периода действия которого лежит дальше (в будущем).

Заменой E(C(CA)) = S(C(CA) + V(C(CA) в формуле выше, мы получаем **период применимости** AP(C(CA)) (applicability-period), в котором CA может сертифицировать своим актуальным ключом (по истечении этого периода применимости, CA может только обслуживать списки отзыва и другие дополнительные службы, не связанные с выдачей новых сертификатов):

AP (C(CA)): = EA (C(CA)) - S(C(CA)) = V(C(CA)) - VC (i)

Поэтому, имеем такое требование:

Требование 4 (*управление несколькими ЦСК сертификатами): Чтобы иметь возможность сертифицировать в любое время, ЦСК должен управлять несколькими ЦСК сертификатами, которые действительны одновременно. Количество одновременно действительных ЦСК сертификатов зависит от периода действия их ключа сертификации.*

В общем, CA будет гарантировать при заявке сертификатов от инстанции ступени i+1 определенный минимум VK (i+1) периода срока действия для его ключа сертификации: V(C(CA)) ≥ VK (i+1). Так как для CA по истечении каждого промежутка времени AP(C(CA) = V(C(CA)) - VC (i) ≥ VK (i+1) - VC (i) должен назначаться заново (новый) сертифицированный ключ, то CA имеет максимально (VK(i+1) / (VK(i+1) - VC(i))) одновременно актуальных/действительных сертификатов.

Требования к вышестоящим этапам иерархии:
Относительно гарантий применимости для TN-сертификатов – CA должен гарантировать срок действия его ключа сертификации в течение указанного в его сертификате периода. Чтобы соответствовать гарантии срока для минимального промежутка времени VC(i), срок действия CA-ключа должен гарантироваться, по меньшей мере, для VK(i+1) ≥ VC(i).

Анализ сценариев замены ключей

Исследованные в предыдущем разделе локальные модели между двумя смежными уровнями i, i+1 обобщаются ниже на модели изменения ключей для всей иерархии сертификации. Эти модели представляются как «гомогенные» модели, при которых используется на каждой ступени равная локальная модель, так и «гибридные» модели, составленные из различных локальных моделей.

Модель №1: иерархия сертификации без гарантий срока
Рассматриваем применение локальной модели №1 на всех ступенях иерархии сертификации. Обратим внимание, что инстанция уровня i может только тогда гарантировать в любое время действительность ключа сертификации (локальная модель №1b), когда все вышестоящие инстанции могут исполнять своевременно требования сертификации. Как только этот момент (располагать своевременно новым ключом) упускается учреждением сертификации уровня i, то это отражается на всем подчиненном частичном дереве иерархии.

Преимущества модели:

1. Для ЦСК не существует никакой необходимости одновременно управлять больше чем одним действительным ЦСК сертификатом.
2. ЦСК не несет ответственности за выход вне интервала действия им выданных сертификатов.
3. Никакой сертификации без предварительной заявки/ запроса.
4. Для ЦСК достаточно только наблюдение за успешностью собственного пути сертификации, чтобы располагать в любое время действительным ключом.

Недостатки модели:

1. Каждый участник нижних уровней сам отвечает за действительность (за сроки действия) его сертификата.
2. Чтобы располагать непрерывно действительным ключом подписи, участник должен отслеживать все изменения сертификатов вышестоящих ступеней. Если выявленные им изменения сертификата влияют на действительность его ключа, он должен ходатайствовать своевременно о новом сертификате.
3. Поэтому непременно требуется онлайн связь с каталогами вышестоящих учреждений сертификации.
4. При изменении ключей учреждений сертификации могут встречаться ситуации, в которых они больше не являются участниками системы электронной подписи, так как к ключам не существует никаких действительных путей сертификации.

При применении локальной модели №1 на всех этапах иерархии не выполнено минимальное требование №1. Поэтому эта модель представляется неподходящей для практического применения.

Минимальное требование №1 выполняется, правда, применением локальной модели №1b на всех ступенях иерархии, тем не менее, может случиться, что изменения ключей размножаются вплоть до ступени 1.

Модель минимальной дружественности к клиентам достигает только тогда, когда все учреждения сертификации объявят при замене ключа о готовности сертифицировать по-новому/заново по заявке до сих пор действительного TN-ключа по крайней мере на остаток срока его прежнего сертификата. Только в таком случае изменения ключей остаются локальными и конечные пользователи только лишь должны установить измененные сертификаты ступеней.

Модель №2: гарантия действительности ключей для всех этапов иерархии

Исследуем применение локальной модели №2 на всех ступенях иерархии сертификации. Ситуация компетентности «переворачивается» (является инверсной) по сравнению с моделью №1: Здесь конечный пользователь TN не должны больше своевременно ходатайствовать о пост-сертификации, а ЦСК сам обязан проводить их своевременно.

Рассмотрим сначала подробнее проблемный случай, который встречается тогда, когда в пределах указанного в TN-сертификате периода действия, CA-ключ становится недействительным из-за истечения срока действия его CA-сертификата.

При продлении срока CA-ключа новым сертификатом, никакая пост-сертификация TN-сертификатов не требуется. Однако необходимо располагать непрерывно действительным CA-ключом. Для этого продление ключа новым сертификатом должно уже произойти, в частности, прежде чем будет достигнуто окончание срока действия прежнего сертификата.

При замене CA-ключа должен существовать (уже быть в наличии) новый, сертифицированный CA-ключ до даты окончания срока его текущего CA-сертификата. Исходя

из этого, пост-сертификация всех затронутых TN-сертификатов должна произойти до этой даты. Если CA сгенерировал свой новый ключ, пост-сертификации могут происходить временно параллельно с заявкой сертификации его нового ключа. При этом начало срока действия как TN-сертификатов, так и нового CA-сертификата должно соответствовать окончанию срока действия прежнего CA-ключа.

Чтобы избежать пересечения времени пост-сертификации, каждый CA должен гарантировать, начиная с конца срока действия его прежнего ключа, действительность нового CA-ключа, по меньшей мере, на необходимый для TN-сертификатов промежуток времени.

Преимущества модели:

1. Управление действительным CA-ключом достаточное.
2. Перенос компетентности/ответственности за пост-сертификации на CA.

Недостатки модели:

1. Необходима онлайн связь с каталогами для участника, так как сертификат изменяется при замене CA-ключа. Исходя из этого, изменяется путь сертификации, как только один из сертификатов пути достигает даты окончания срока действия.
2. На самой низкой ступени иерархии между конечными пользователями и учреждением сертификации пост-сертификация потенциально очень большого числа ключей подписи в пределах короткого промежутка времени может привести к проблемам, или вообще быть нереальной. При каждом изменении ключей CA дополнительно необходима потенциально высокая пропускная способность в пост-сертификациях, в сравнении с нормальной/обычной эксплуатационной пропускной способностью. Таким образом, возникают пиковые нагрузки, которые могут распределяться только более ранней по времени генерацией нового ключа CA.

Модель №3: видоизменение модели №2 для самой низкой ступени иерархии

Чтобы ограничить проблематичность пост-сертификаций, рассмотрим модель №2 с модифицированной самой низкой ступенью иерархии. Для ступеней 2,...,n локальная модель №2 назначается как раньше. Ступень 1 модифицируется в этом отношении так, что учреждение сертификации уровня 2 имеет в любое время более двух одновременно действительных ключей сертификации. Ключи имеют равный срок действия V = V(C1(2)) = V(C2(2)). Изменение одного ключа, соответственно, происходит в середине периода срока действия другого ключа:

$$S(C1(2)) = S(C2(2)) + V / 2.$$
$$S(C2(2)) = S(C1(2)) + V / 2.$$

Учреждение сертификации сертифицирует с использование его соответственно более нового ключа. Этим способом оно может гарантировать конечному пользователю, что сертификат остается применимым, по меньшей мере, в течение периода V/2 (см. локальную модель №3). Тем не менее, эта гарантия может происходить только тогда, когда для использованного CA-ключа гарантируется срок действия в течение надлежащего промежутка времени.

Для TN-сертификатов, которые выпускаются на период действия V/2, не требуется пост-сертификация. Обусловленная пост-сертификациями дополнительная нагрузка делится пополам путем распределения на 2-й ключ сертификации.

Модель №4: гарантия применимости/действительности сертификата для конечного пользователя

Модель №4 гибридная: На уровне 1 гарантируется применимость сертификата (локальная модель №3). Предпосылкой для этого является то, что на уровне 2 гарантируется срок действия ключа, использованного на этом уровне сертификации. Соответственно на уровне 2 действует модель №2b. Требование этой модели к вышестоящим уровням является таким, что на уровне 3 существуют в любое время, по меньшей мере, действительный ключ сертификации и пост-сертификации происходят своевременно. Однако, чтобы избежать проблем при пост-сертификациях, должны быть обеспечены гарантии действительности ключа в течение достаточного для этого промежутка времени. Соответственно, для уровней от 3 до n могут использоваться выборочно локальные модели №2b или №1b.

Недостатки модели:

1. Учреждения сертификации уровня 2 должны управлять несколькими ключами одновременно.
2. Путь сертификации от TN-сертификатов может изменяться. Поэтому требование доступа к перечню/ каталогу существует в этой модели также для конечного пользователя.
3. Необходима гарантия действительности для ключа сертификации уровня 2.
4. Требуется пост-сертификация CA-ключей уровней 2,..., n-1. Однако это является некритичным, так как количество CA по сравнению с количеством конечных пользователей значительно меньше.

Преимущества модели:

1. Хотя несколько ключей действительны одновременно, для сертифицирования должен использоваться только соответственно недавний (более новый).
2. До тех пор пока не будет блокирован ключ сертификации, никакая пост-сертификация сертификатов конечного пользователя не требуется. Однажды выданные сертификаты не должны обрабатываться снова.
3. Гарантированная применимость сертификата в течение указанного в сертификате периода для конечного пользователя.
4. При применении локальной модели №3b на уровне 1: минимальная гарантированная действительность для сертификатов конечных пользователей.

Модель №5: гарантия действительности общего/всего пути сертификации

Рассматриваем гомогенную модель применения модели №3b на каждом уровне иерархии сертификации.

Каждое учреждение сертификации иерархии для выданных им сертификатов гарантирует применимость в течение указанного в них периода. Этим способом может гарантироваться конечному пользователю действительность его пути сертификации в течение всего срока действия его сертификата. Из этого получаются следующие неравенства:

$$E(C(n)) \geq E(C(n-1)) \geq ... \geq E(C(1))$$
$$S(C(1)) \geq S(C(2)) \geq ... \geq S(C(n))$$
$$V(C(n)) \geq (C(n-1)) \geq ... \geq V(C(1))$$

При запросе сертификата учреждением сертификации уровня i у инстанции уровня (i+1), учреждение сертификации уровня i знает заранее, что сертификат, который оно получает, применим, по меньшей мере, на период VC (i). Следовательно, период VC (i) может гарантироваться также, как период применимости VC (i-1) выданным сертификатам: $VC(i) \geq VC(i-1)$.

Учреждение сертификации может использовать его актуальный ключ сертификации для сертифицирования на время $AP(C(i)) = V(C(i)) - VC(i-1)$. Если учреждение сертификации

использует сертификат с минимальным временем применимости V(C(i)) = VC(i), то получается, что минимальный промежуток времени AP (i), в котором оно может использовать свой ключ для сертификации, равен: AP(i): = VC(i) - VC(i-1). Так как по истечении каждого периода AP(i) на уровне i должен использоваться заново сертифицированный ключ, максимальное количество одновременно управляемых CA-сертификатов соответствует VC(i) / AP(i). Это «максимальное количество» относится к случаю, когда CA стремится управлять одновременно как можно меньшим числом CA-сертификатов.

Недостатки модели:

1. Продление промежутков времени действия от уровня к уровню по отношению к AP(i):
   $VC(2) \geq AP(2) + VC(1)$
   $VC(3) \geq AP(3) + VC(2)$
   $\geq AP(3) + AP(2) + VC(1)$
   $VC(n) \geq AP(n) + AP(n-1) + ... + AP(2) + VC(1)$
2. Необходимо несколько одновременно действительных ключей на каждом уровне.
3. Длинные промежутки времени действия для сертификатов верхних уровней. Вследствие этого имеет место повышенная вероятность компрометации, которая должна минимизироваться дополнительными организационно-техническими мерами.

Преимущества модели:

1. В течение общего/всего срока действия сертификата путь сертификации для ключа подписи остается постоянным.
2. После выдачи сертификата, как правило, не требуется больше никакого общения между конечным пользователем и учреждением сертификации.
3. Все преимущества модели №4 имеют место и для этой модели.

Модель представляется хорошо приемлемой для инфраструктур, у которых онлайн доступ к каталогам не обеспечивается для большой части конечных пользователей. Это имеет место, к примеру, когда многие из конечных пользователей не располагают необходимыми онлайн коммуникациями, или если учреждениями сертификации не предлагаются никакие службы каталога.

Из-за того, что промежутки времени действия ключа продлеваются от уровня к уровню, мы доходим до такого целевого конфликта:

а) Если прирост срока действия от уровня к уровню установить незначительным, то время пригодности AP (i), i> 1 личного ключа на каждом уровне является коротким, и это приводит одновременно к большому количеству действительных, управляемых ключей сертификации.

б) С другой стороны, если количество одновременно действительных ключей ограничивается, то период AP(i) минимальной применимости личного ключа должен занимать относительно большую долю в гарантированном минимальном периоде применимости VC(i). Прирост от уровня к уровню минимальной гарантированной применимости VC (i) приведет к относительно большому значению в отношении к сроку действия сертификата конечного пользователя. Наконец, из этого следует, что должны устанавливаться относительно большие сроки действия сертификата для верхних уровней.

Для методов с открытыми ключами, когда в течение соответствующих промежутков времени криптографическая стойкость ключа не вызывает сомнений, эта модель представляется наиболее применимой и выгодной.

Рекомендации по применению модели

При организации безопасного использования подписей в течение больших промежутков времени, в сравнении со сроком действия сертификатов конечных пользователей, требуется гарантия действительности общего/всего пути сертификации. Здесь имеет место конфликтная ситуация между сроком действия сертификатов конечных пользователей, организацией удобства использования, безопасностью подписи и эффективностью практического выполнения подписи.

Поэтому баланс между дружественностью к клиентам и дополнительными организационными мерами представляется оптимальным в гибридной модели №4, у которой гарантируется конечным пользователям применимость их сертификатов в течение их срока действия, и гарантируется действительность ключей вышестоящих уровней иерархии на промежутке времени срока действия соответствующих сертификатов.

Таким образом, учитывая вышеизложенное, можно сделать вывод, что модель №4 представляется наиболее применимой с точки зрения применимости/действительности сертификата конечного пользователя. Модель №5 представляется наиболее применимой с точки зрения не только применимости/действительности сертификата конечного пользователя, но и гарантии действительности общего/всего пути сертификации, что важно для систем электронного документооборота с юридически значимыми электронными документами. Обе эти модели удовлетворяют Требованию 1 (действительный ключ сертификации), Требованию 2 (сертификаты «прямого» действия), указанным выше. Отказ от этих моделей приведет к недружественной по отношению к клиентам модели, которая определяет пассивность учреждений сертификации и возлагает ответственность за срок действия ключа подписи на конечных пользователей.

Для выполнения Требования 3 (надежность ключа сертификации) при реализации модели №4 или №5 требуются дополнительные организационные и, возможно, технические меры для минимизации риска, связанного с повышенной вероятностью компрометации из-за больших промежутков времени действия сертификатов верхних уровней учреждений сертификации. При этом, как сказано, ответственность за срок действия сертифицированного ключа конечного пользователя переносится с конечного пользователя на учреждения сертификации, что повышает не только дружественность к клиентам учреждений сертификации, но и уменьшает проблематичность дорогостоящих пост-сертификаций уже выданных сертификатов в случае замены ключа учреждений сертификации.

Реализация модели №4 или №5 также предполагает выполнение Требования 4 (управление несколькими CA сертификатами). Недостатки управления несколькими ключами сертификации представляются вообще не достойными внимания из-за их незначительности, если только не…

Учитывая текущий уровень Национальной системы ЭЦП Украины, можно сделать уверенное предположение, что отдельные АЦСК и/или ЗЦСК спроектированы и созданы не ориентированными на дружественность к клиентам, поэтому не способны управлять несколькими CA сертификатами одновременно. В этой ситуации следует сделать выбор – «угодить» нескольким «не дружественным» участникам рынка, или создать приемлемые и безопасные условия работы с ЭЦП сотням тысяч, а в дальнейшем миллионам, клиентов, конечных пользователей ЦСК.

Итак, учитывая вышеизложенное, считаем, что в Национальной системе ЭЦП Украины должна применяться модель №5 (гарантия действительности общего/всего пути сертификации).

Рассмотрим вопрос о сроках действия ключей учреждений сертификации, т.е. период действительности/ валидности сертификата учреждения сертификации (и соответственно

личного ключа) V(C(i)) и период AP(i) минимальной применимости личного ключа учреждения сертификации.

Задача – определить количество одновременно действительных, управляемых ключей сертификации учреждения сертификации для каждого уровня иерархии.

Согласно Постановлению Кабинета министров Украины от 13.07.2004 г. №903 [8]

1) Личный ключ АЦСК может быть действительным не более 5-ти лет (п.4.4.1 Постановления КМУ);
2) Личный ключ конечного пользователя может быть действительным не более 2-х лет (п.5.3.2 Постановления КМУ).

Учитывая введенные обозначения (для уровней иерархии):
VK (i) (VK = validity key) – период действительности личного ключа уровня i,
для выбранной модели, согласно Постановлению КМУ, имеем такие периоды (в годах):

VK (1) = 2;
VK (2) = 5.

И пусть для примера:
VK (3) = 7;
VK (4) = 10.

Максимальное количество одновременно действительных, управляемых ключей сертификации K(i) учреждения сертификации i-го уровня определяется по формуле:

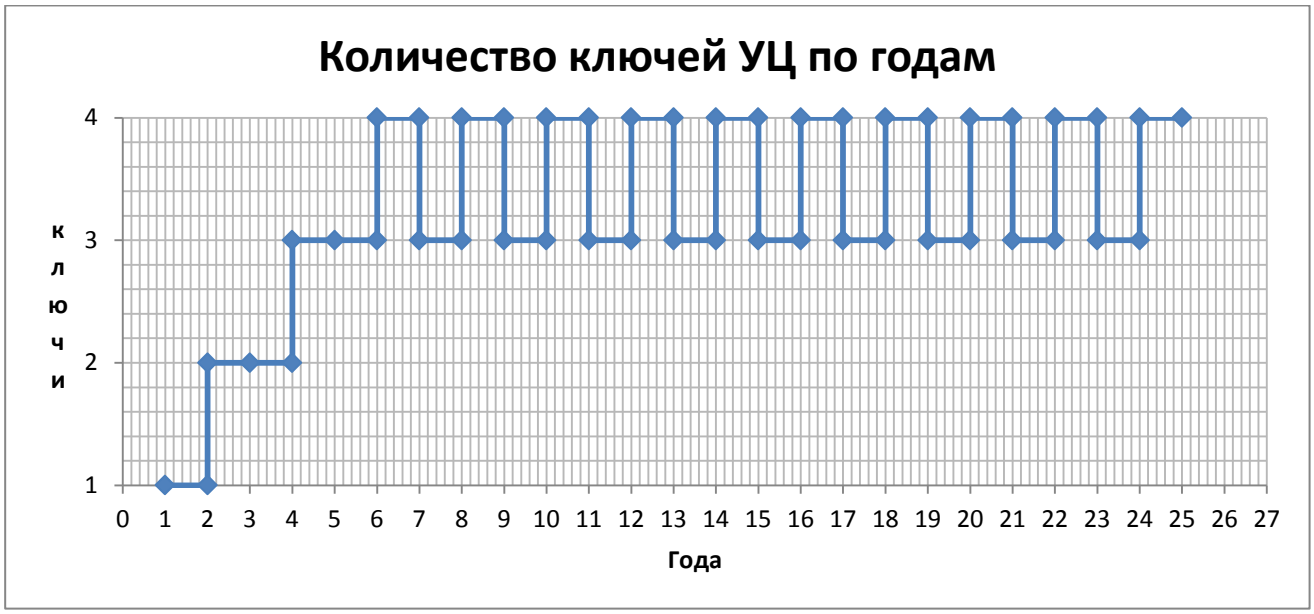
$K(i) = \lceil VK(i)/ (VK(i) – VK(i-1)) \rceil$, при i = 2, …,
где
VK(i) > VK(i-1).
$\lceil .. \rceil$ - обозначает операцию округления до большего целого.

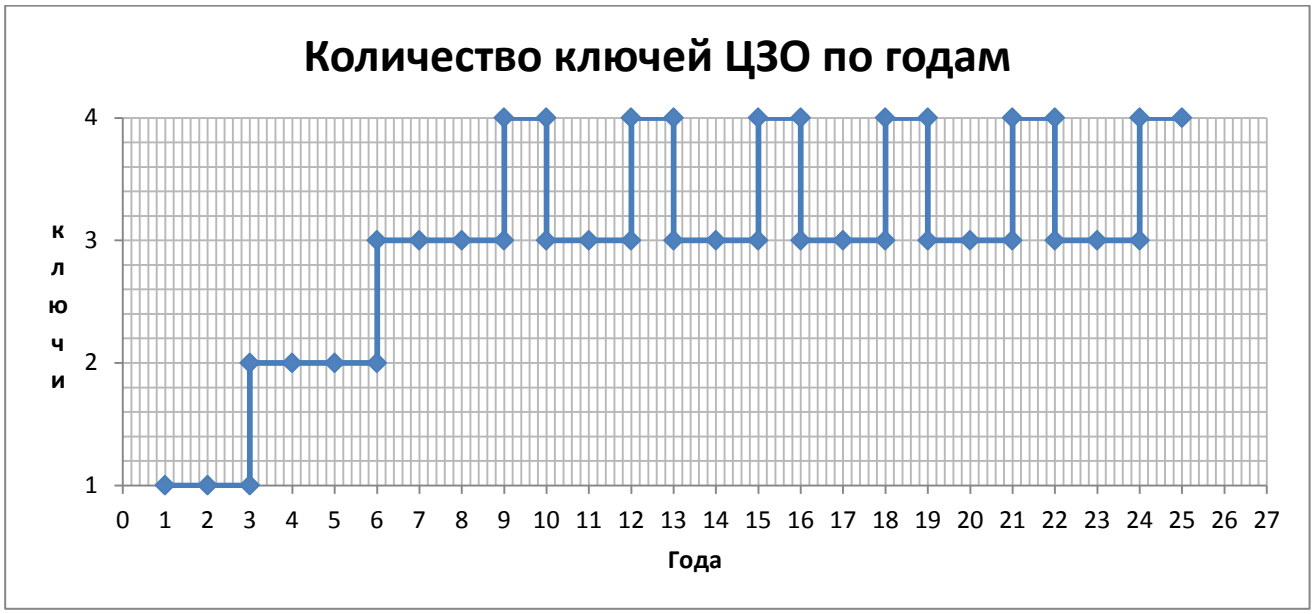
Таким образом, для заданных выше VK(i) имеем максимальное количество одновременно действительных, управляемых ключей сертификации K(i) учреждения сертификации i-го уровня:

Уровень (i)	**Период действительности VK(i) в годах**	**Макс. количество одновременно действительных ключей K(i)**
1 (пользователь)	2	**1**
2 (АЦСК/ЗЦСК)	5	**2**
3 (УЦ)	7	**4**
4 (ЦЗО)	10	**4**

На диаграммах ниже приведено фактическое количество одновременно действительных, управляемых ключей сертификации K(i) учреждения сертификации i-го уровня по годам:


Количество ключей АЦСК по годам
Ключи
2
1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
Года


Количество ключей УЦ по годам
Ключи
4
3
2
1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
Года


Количество ключей ЦЗО по годам
Ключи
4
3
2
1
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
Года

Изменения сертификата через цикл продукта

В завершение вопроса замены сертификата нельзя не отметить такой вопрос, как замена сертификата через цикл продукта [9]. Этот вопрос базируется на том, что сертификаты распределяются их пользователям вместе с приложением(и), и соответственно уже твердо в него(них) установлены. Это особенно актуально для приложений, которые используют криптомодули (программные или программно-аппаратные), не интегрированные со стандартными хранилищами ключей/сертификатов. Разработчики таких приложений жестко «прошивают» в свои хранилища не только сертификат пользователя, но и всю его цепочку – сертификаты вышестоящих уровней сертификации.

При этом считаем, что жизненный цикл продукта программного обеспечения до замены или обновления, в общем, является короче, чем срок действия сертификата, так что модернизированной версией или новой инсталляцией приложения заменяется своевременно и сертификат(ы). В противном случае, конфликтов не избежать.

Однако при непредвиденном нарушении, при котором должен быть отозван сертификат (компрометация или др.), это решение не практично, так как в этом случае приложение должно (срочно!) по-новому инсталлироваться или модернизироваться, что, как правило, связано с высокими организационными издержками, и при этом все равно не может быть выполнено своевременно (в разумное время после отзыва сертификата).

Кроме того, модернизация версии приложения не устраняет еще такую проблему - приложение должно после изменения сертификата иметь возможность проверять ранее подписанные валидные документы (созданные до отзыва сертификата).

Ну и конечно, если разработчики жестко «прошивают» в свои хранилища только одну ключевую пару с ее цепочкой, то это делает вообще невозможным реализацию любой дружественной к клиентам модели замены ключа в иерархии сертификации, т.к. любая такая модель предполагает одновременное существование нескольких доверенных корневых сертификатов и, соответственно, цепочек сертификатов для сообщества клиентов в целом.

Дополнительные организационно-технические мероприятия

К таким мерам, в частности, относится продуманная политика и практика выпуска сертификатов всех уровней сертификации. Например, следует помнить, что не все приложения, даже известных производителей (например, Microsoft) позволяют корректно выбирать сертификат из хранилища, если есть несколько сертификатов с одинаковыми атрибутами субъекта. То есть, при выпуске двух сертификатов с одним и тем же полем Subject системы поиска сертификата (например, при построении цепочки и проверке подписи сертификата) могут выдавать всегда первый в списке, что приводит в результате к ошибке.

К организационно-техническими мерам, с целью минимизации риска компрометации ключа корневого ЦСК, можно отнести возможность построения инфраструктуры PKI с несколькими корнями доверия [9]. Это решение базируется на том, что несколько корней доверия (корневых сертификатов ЦУО) будут применяться одновременно параллельно, и отмена одного корня доверия «перехватывается» остальным(и) корнем(и) доверия (временно). При необходимости может параллельно устанавливаться полная инфраструктура PKI (все уровни иерархии), вплоть до многократной выдачи ключей и сертификатов для конечного пользователя. Для этого решения предлагается устанавливать параллельные структуры PKI на различных криптографических процессах (алгоритмах) или, по меньшей мере, выбирать различные длины ключей, чтобы мочь реагировать на атаки на алгоритмы. Например, решение FlexiPKI фокусируется на этом аспекте [10]. Естественно, что это подход очень трудоемкий и затратный, и требует более детального анализа.

К организационно-техническим мерам также относится вопрос фактически установки на стороне клиента нового корневого сертификата при его замене, и установлению доверия пользователей со старым (но еще действительным) корневым сертификатом в отношениях с пользователями с новым корневым сертификатом (особенно, если может одновременно действовать, как показано выше, до четырех корневых сертификатов ЦУО). Этот процесс, как правило, требует участия пользователя (установить флажок «Доверять»), что делает его предрасположенным к ошибкам взаимодействия с пользователем. Целью организационно-технических мер является проводить установку доверия к новому корневому сертификату автоматически, что можно обеспечить механизмом кросс-сертификации. До истечения срока одного корневого сертификата выставляется другой (новый) корневой сертификат, который взаимно кросс-сертифицируется с актуальным (для этого пользователя) сертификатом. Новый корневой сертификат и оба кросс-сертификата распределяются пользователю и другим участникам, после чего возможна автоматизированная проверка подлинности для участников с разными корневыми сертификатами. При этом следует подчеркнуть, что в случае нарушения, например, при компрометации ключа и пропаже/потере актуального корня доверия, это решение не предлагает никаких преимуществ - созданный после компрометации новый корень доверия не может заверяться через кросс-сертификацию со старым, скомпрометированным корнем доверия, так как не может обеспечивать подлинность кросс-сертификатов. Для внедрения механизма кросс-сертификации программное обеспечение клиента должно поддерживать соответствующую проверку (нового сертификата, подписанного ключом старого, и соответственно, старым ключом подписанный кросс-сертификат для нового ключа). Это решение стандартизировано международными стандартами, например, RFC 4210:2005 [10], однако в Украине не регламентировано и поэтому пока неприменимо.

К организационным мерам, в частности, относится более четкая/строгая регламентация порядка использования ключа ЦСК, политик формирования/ проверки подписи и др.

Для практической организации и эффективного контроля за выполнением организационно-технических мер можно обратиться к опыту США. Так, согласно стандарту NIST SP 800-57 [7] (Appendix A. National Key Management Infrastructure) в государстве существует «Центральный орган надзора» (Central Oversight Authority), - орган, который осуществляет общий для всей Инфраструктуры управления ключами сертификации (KMI, Key Management Infrastructure) надзор за синхронизацией данных, надзор системы безопасности организации или совокупности организаций сертификации. Центральный орган надзора (основные функции):

1) координирует политику защиты и практику (процедуры),
2) может функционировать как держатель данных, предоставленных ЦСК, и
3) выступает в качестве источника общего и системного уровня информации, требуемой для ЦСК всех уровней, например, рекомендации/ требования по выбору ключевого материала (алгоритмы, длины ключей и др.), информации о регистрации, каталог данных, спецификаций системной политики, информация о компрометации ключей, информации об отзыве сертификатов и др.
4) в соответствии с требованиями живучести или политики операционной непрерывности, Центральный орган надзора может функционировать (в соответствующем удаленном узле) как система резервного копирования для ЦСК всех уровней.

Перечень литературы

1. Закон України “Про електронний цифровий підпис” від 22.05.2003 N 852-IV.

2. ДСТУ CWA 14171:2008 Загальні рекомендації для верифікації електронних підписів.

3. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures - Official Journal L 013 , 19/01/2000 P. 0012 – 0020.

4. RFC 5280:2008 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

5. Fritz Bauspieß, Alfred Scheerhorn: Zertifikatswechsel und Schlüsselgültigkeiten. Schlüsselwechsel-Szenarien auf der Basis von RFC 1422. - Datenschutz und Datensicherheit, 21(6):334–340, 1997.

6. Ingmar Camphausen, Stefan Kelm, Britta Liedtke, Lars Weber: Aufbau und Betrieb einer Zertifizierungsinstanz - März 2000 (http://www.dfn-cert.de/dokumente/ca-handbuch.pdf);

7. NIST SP 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization.

8. Постанова Кабінету Міністрів України "Про затвердження Порядку акредитації центру сертифікації ключів" від 13 липня 2004 року №903.

9. Ingmar Camphausen, Dr. Holger Petersen, Claus Stark: Root CA Zertifikatswechsel. Secorvo White Paper, Version 1.0 - Stand 30.September 2002, Secorvo Security Consulting GmbH.

10. Hartmann, M.; Maseberg, S.: „Fail-Safe-Konzept für FlexiPKI“, in: Horster, P. (Hrsg.): Kommunikationssicherheit im Zeichen des Internet, Vieweg Verlag, 2001, S. 128ff.

11. RFC 4210:2005 – Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), September 2005.