УДК 656.2.08

ПРОВЕРКА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РЕЖИМЕ ONLINE В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СТРУКТУРЕ С ИСПОЛЬЗОВАНИЕМ ПОДЧИНЕННОГО РЕГИСТРАЦИОННОГО ЦЕНТРА

С.П. КАЛЮТЧИК

Белорусская железная дорога
Ленина, 17, Минск, 220030, Беларусь

Поступила в редакцию 10 декабря 2008

Рассматриваются особенности проверки электронной цифровой подписи в online режиме с учетом требований законодательных и нормативных актов Республики Беларусь в условиях крупной организации (корпорации), имеющей территориально распределенную структуру с централизованным управлением на примере Белорусской железной дороги. На примере проведенных автором исследований обосновываются недостатки использования традиционной, трехуровневой системы применения электронной цифровой подписи для ее on-line проверки в условиях реальных информационно-телекоммуникационных сетей территориально распределенной структуры. Вводится понятие нового элемента системы применения электронной цифровой подписи — подчиненного регистрационного центра.

Ключевые слова: электронная цифровая подпись, удостоверяющий центр, регистрационный центр.

Введение

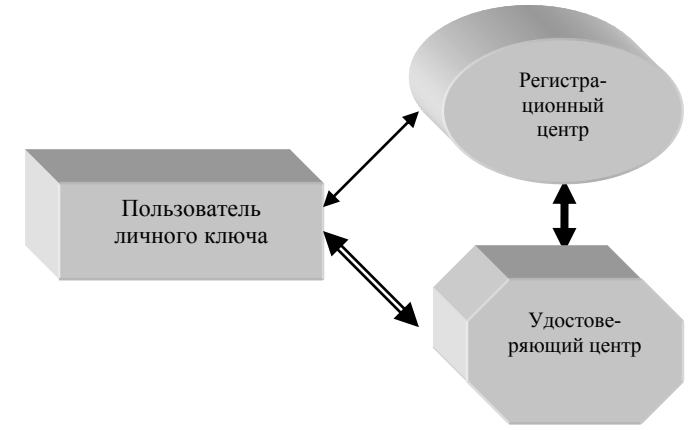
С развитием информационных технологий, их использованием в реальном секторе экономики активизируется применение элемента криптографической защиты — электронной цифровой подписи (ЭЦП) для придания юридического статуса электронным документам и иной электронной информации.

В Республике Беларусь существует достаточно полная нормативно-правовая и технологическая база, основывающаяся на законе Республики Беларусь "Об электронном документе", позволяющая создавать и эксплуатировать системы применения ЭЦП [1, 2]. Вместе с тем действующие нормативы направлены на регламентацию традиционных систем применения ЭЦП — систем общего пользования, не учитывающих ряда возможных практических аспектов подписываемой информации, например, оперативного характера электронных документов, либо их использования в критически важных процессах реального времени.

Особенности электронных документов (электронной информации), с которой применяется ЭЦП, наиболее часто проявляются в корпоративных территориально распределенных системах применения ЭЦП. Проведенные автором исследования на базе территориально распределенной информационной системы Белорусской железной дороги выявили особенности реализации ключевой задачи системы криптографической защиты информации — проверки подлинности ЭЦП в электронных документах в online режиме.

Теоретический анализ

Рассмотрим основные элементы проверки ЭЦП в традиционной системе, состоящей из трех основных уровней — удостоверяющего центра, регистрационного центра и пользователей (рис. 1).



технологические связи при регистрации пользователя
технологические связи при проверке ЭЦП пользователем
технологические связи между удостоверяющим и регистрационным центрами

Рис. 1. Технологические связи в классической системе применения ЭЦП

При проверке ЭЦП пользователя N, пользователи N+*k,* где *k* — целое число и $k \geq 1$, получают от пользователя N, или из удостоверяющего центра сертификат открытого ключа, содержащий значение открытого ключа, с помощью которого проверяют электронную подпись отправителя. Перед проверкой пользователь N+*k* должен проверить в удостоверяющем центре актуальность сертификата отправителя N, т.е. получить от удостоверяющего центра один из ответов:

– сертификат пользователя N находится в списке актуальных сертификатов;

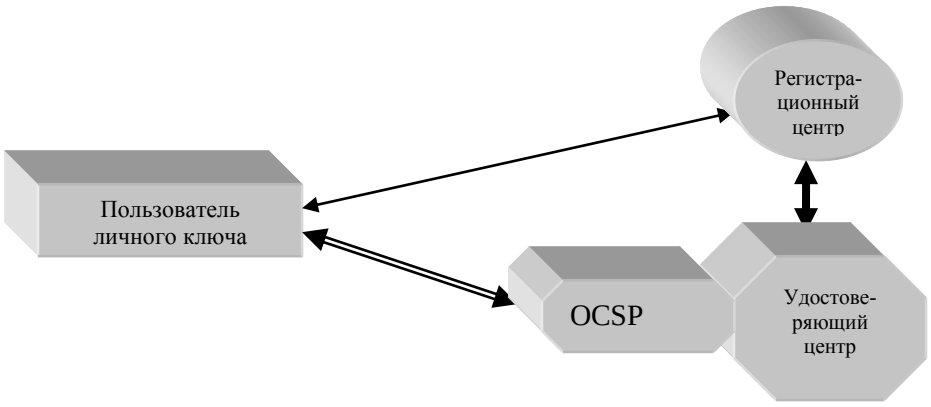
– сертификат пользователя N помещен в список отозванных сертификатов;

– сертификат пользователя N не известен удостоверяющему центру.

На практике, при использовании ЭЦП в документах не оперативного характера, такая проверка относительно каждого отправления пользователя N не проводится, т.к. требует передачи по специализированным протоколам (CAC / COC) списков актуальных и отозванных сертификатов, подписанных закрытым ключом удостоверяющего центра, пользователю N+*k* по каналам связи, что напрямую зависит от качества сетей и занимает значительное количество времени. Это обусловлено тем, что подписанные ЭЦП удостоверяющего центра файлы со списками актуальных и отозванных сертификатов занимают объем от нескольких килобайт до десятков мегабайт. Кроме того, в общих системах применения ЭЦП постоянная проверка статуса сертификата пользователя N не требуется, так как пользователи, как правило, известны друг другу и обмен осуществляется документами, в большинстве своем не оперативного характера.

С целью ускорения фактического времени проверки сертификатов открытого ключа по спискам действующих и отозванных сертификатов, при достаточно большом значении N практикуется применение объекта OCSP-респондер (Online Certificate Status Protocol), предназначенного для обработки запросов пользователей N+*k* о статусе сертификата пользователя N в соответствии с базой действующих сертификатов и списком отозванных сертификатов. OCSP-респондер, как правило, является WEB-объектом. Ускорение работы с помощью OCSP-респондера происходит вследствие выдачи ответа по запросу статуса конкретного сертификата N, а не всего списка отозванных сертификатов (рис. 2).

Так, файл ответа, передаваемый OCSP–респондером пользователю N+*k* при практической реализации на Белорусской железной дороге разработок новой технологии применения ЭЦП, имеет небольшую фиксированную длину порядка 300 байт. Вместе с тем, при проверке по классическому варианту, предусматривающему передачу полных списков актуальных и отозванных сертификатов, объем передаваемой информации на порядок больше (от нескольких килобайт до десятков мегабайт), т.к. списки содержат данные обо всех сертификатах, действующих на данный момент, и всех сертификатах, которые выпускались, но на данный момент приостановлены или аннулированы.



технологические связи при регистрации пользователя
технологические связи при проверке ЭЦП пользователем
технологические связи между удостоверяющим и регистрационным центрами

Рис. 2. Технологические связи с использованием OCSP-респондера

Сравнительные параметры методов использования CAC/COC и OCSP приведены в таблице.

Сравнение параметров использования CAC/COC и OCSP

Параметр	CAC/COC	OCSP
Время создания	Периодически через промежутки времени, настраиваемые в удостоверяющем центре	В момент запроса статуса клиентом
Время действия	Значительное (от нескольких дней до месяца), в зависимости от настроек удостоверяющего центра	Только для одного запроса. Возможно продление до нескольких минут или часов
Актуальность сведений	На момент обновления CAC / COC	На момент запроса статуса пользователем
Сертификаты, сведения о которых включены	Все отозванные сертификаты, выпущенные данным удостоверяющим центром / все сертификаты, выпущенные и аннулированные (приостановленные)	Один сертификат, статус которого запрошен
Объем	Значительный (от нескольких килобайт до десятков мегабайт) при большом количестве актуальных / отозванных сертификатов	Несколько килобайт

Принципиальным моментом при оценке рассматриваемой проблемы являются технологические особенности деятельности многих корпораций, в частности Белорусской железной дороги. Особенность заключается в том, что большинство технологических документов (технологической информации), с которыми применяется ЭЦП, являются документами оперативного характера, влекущими принятие на их основе решений в режиме реального времени либо связанных с обеспечением безопасности критических технологических процессов (на железнодорожном транспорте — безопасности движения поездов и функционирования железнодорожных предприятий). В случае конфликтной ситуации, предметом исследования в первую очередь будет являться статус пользователя системы на момент формирования ЭЦП. С учетом этого необходимым условием правовой достоверности электронной цифровой подписи таких документов является оперативная проверка статуса пользователя системы применения ЭЦП при каждой операции с закрытым ключом.

Вторым принципиальным моментом является то, что эффективность работы OCSP-респондера как сетевого объекта напрямую зависит от действенности телекоммуникационных ресурсов (качества сетей связи).

Топология существующих сетей передачи данных Белорусской железной дороги свидетельствует, что для реализации информационных задач в пределах железнодорожных узлов либо их группы применяется архитектура сетей передачи данных железнодорожных узлов, подключенных к точкам единой сети передачи данных Белорусской железной дороги.

Подавляющая часть сетей передачи данных узлов Белорусской железной дороги использует смешанные каналы передачи данных — оптоволоконные, ADSL (Asymmetric Digital Subscriber Line) и каналы тональной частоты (ТЧ). Наиболее низкими техническими параметрами при передаче информации обладают каналы ТЧ, которые и определяют предельные возможности по условиям передачи трафика.

В сетях связи ТЧ каналы объединены в группы с суммарной средней скоростью передачи 33,6 кбит/с. Учитывая приоритет передачи технологического трафика для программ, связанных с управлением движением, устройствами безопасности, финансовыми задачами и т.п., организовать online работу OCSP-респондера, централизованно размещенного совместно с удостоверяющим центром и пользователей, расположенных на периферии, оказалось практически невозможным, что подтверждено исследованиями, проведенными автором на базе информационно-телекомуникационных сетей Белорусской железной дороги.

Таким образом, можно утверждать, что в условиях отсутствия качественных сетей передачи данных, работа централизованного OCSP-респондера как сетевого объекта не обеспечивает надежности процессов online верификации статуса пользователя, что при использовании ЭЦП в технологических документах (технологической информации) грозит срывом критических производственных процессов.

Экспериментальная часть

Автором проводились измерения параметров работы объектов системы применения ЭЦП в реальных условиях функционирования информационных систем Белорусской железной дороги для пользователей, размещенных в различных точках сетей передачи данных железнодорожных узлов.

В ходе технологического обмена, связанного с проверкой сертификата при авторизации пользователя и проверке ЭЦП в online режиме, осуществлялось измерение скорости передачи информации при каждой транзакции. OCSP-респондер разворачивался в месте размещения удостоверяющего центра на базе управления Белорусской железной дороги (г. Минск). В качестве пользователей задействовались клиентские места, подключенные к серверам Брестской и Могилевской узловых сетей передачи данных. Измерения параметров осуществления передачи при одной транзакции показали, что время осуществления информационного обмена для клиентов, подключенных к ТЧ-каналам, доходило до 30 с. Указанные сверхдлительные временные интервалы в условиях использования систем обработки технологических электронных документов приводили к системным сбоям, поскольку оценивались центральными серверами систем в качестве "ошибки связи".

Вместе с тем исследования показали, что с учетом сопоставления каналов нагрузке объектов узловых сетей передачи данных, а также использования мощных центральных серверов, устройств передачи и маршрутизации, такие сети в пределах узла обеспечивают приемлемые параметры передачи данных при операциях авторизации и проверки ЭЦП. Так, при размещении OCSP-респондера в узле Брестской сети передачи данных, время транзакции при авторизации пользователей и проверке ЭЦП для клиентов узловой сети лежит в пределах нескольких миллисекунд.

Таким образом, основываясь на экспериментальных данных можно утверждать, что в пределах сети передачи данных железнодорожного узла Белорусской железной дороги имеются условия, удовлетворяющие требованиям функционирования OCSP-респондера для объектов, включенных в узловую сеть передачи данных. Следовательно, для верификации пользователя при каждой операции с закрытым ключом в информационно-телекоммуникационной сети территориально распределенной структуры необходимо решить следующие задачи:

1. Создать OCSP-респондер как объект локальной сети передачи данных, входящей в корпоративную сеть передачи данных территориально распределенной структуры, совместимый с технологическими задачами корпорации, решаемыми с помощью субъектов локальной сети передачи данных, удовлетворяющий следующим условиям:

– OCSP-респондер либо содержащий его объект являются штатными объектами локальной сети передачи данных;

– OCSP-респондер либо содержащий его объект совместимы со всеми технологическими объектами локальной сети передачи данных;

– OCSP-респондер либо содержащий его объект обеспечивают удовлетворяющую технологическим потребностям корпорации оперативность взаимодействия между собой и удостоверяющим центром (между локальной сетью передачи данных и единой корпоративной сетью) в условиях недостаточной повсеместной пропускной способности единой корпоративной сети либо в условиях аварийного прерывания связи сервер локальной сети – центр управления единой корпоративной сетью.

2. Обеспечить правовую основу функционирования OCSP-респондера как объекта технологической локальной сети передачи данных с учетом требований нормативов функционирования систем криптографической защиты информации.

Результаты и их обсуждение

В ходе проведенного автором изучения практики построения разветвленных открытых систем криптозащиты с открытыми ключами (систем применения ЭЦП), ее анализа с учетом действующей республиканской правовой и нормативной базы сделан вывод о том, что для разработки юридически корректного OCSP-респондера локальной сети передачи данных он должен представлять собой объект, определенный действующей нормативной базой применения ЭЦП, либо являться составной частью такого объекта.

Как белорусские, так и международные нормативы применения ЭЦП указывают в качестве основных объектов систем криптозащиты, использующих открытые ключи, три объекта — удостоверяющий и регистрационный центры, а также пользователей.[1–3]. Эти объекты в достаточной степени определены в нормативно-технологическом плане, что позволяет использовать их в качестве базиса правовой поддержки всех остальных элементов системы применения ЭЦП, в том числе OCSP-респондера локальной вычислительной сети.

Наиболее значимые функции в системе применения ЭЦП принадлежат удостоверяющему центру. Именно удостоверяющий центр обладает необходимыми государственными разрешениями (лицензиями), придающими юридическую значимость ЭЦП и, следовательно, подписанному с ее помощью документу [1]. Выступая своего рода нотариусом относительно конкретного пользователя системы и формируемого им пользователя, удостоверяющий центр должен быть по возможности избавлен от всех иных функций, что явилось одним из оснований практики применения OCSP-респондера — объекта, снимающего с удостоверяющего центра и берущего на себя функцию непосредственного общения с пользователями для передачи информации на основе списка актуальных сертификатов и списка отозванных сертификатов.

Таким образом, в ходе развертывания системы применения ЭЦП на Белорусской железной дороге автором разработана схема, предполагающая использование регистрационного центра в качестве объекта базирования OCSP-респондера в локальной сети передачи данных. Для этого введены понятия головного и подчиненных регистрационных центров со следующим разграничением функционала.

Головному регистрационному центру удостоверяющим центром переданы функции регистрации пользователей системы применения ЭЦП, генерации закрытых ключей, передачи пользователям информации на основе списка актуальных сертификатов и списка отозванных сертификатов.

Подчиненные регистрационные центры содержат OCSP-респондер, посредством которого передают пользователям информацию на основе списка актуальных сертификатов и списка отозванных сертификатов. Право проводить регистрационные действия у подчиненных регистрационных центров отсутствует, т.е. их деятельность не связана с лицензируемыми правами и полномочиями удостоверяющего центра по изданию и распространению сертификатов открытых ключей. С учетом того, что подчиненные регистрационные центры размещаются в локальной (узловой) сети передачи данных территориально распределенной структуры, они используют имеющиеся возможности взаимодействия с удостоверяющим центром для осуществления принудительного обновления списков актуальных и отозванных сертификатов незамедлительно по факту внесения любых изменений в указанные списки.

Понятие подчиненного регистрационного центра является новым элементом системы применения ЭЦП в силу того, что в отечественной практике нет прецедентов развертывания подобных систем широкого применения в крупных организациях с территориально распределенной структурой, предполагающих организационно-техническую централизацию. Использование подчиненных регистрационных центров, наряду с применением интегрированных в них OCSP-респондеров, позволяет совместить централизованные генерацию ключей и управление сертификатами с вынесением в зоны сосредоточения абонентов функций, направленных на максимально оперативную проверку ЭПЦ.

Заключение

Результаты работ, ведущихся в данной области на Белорусской железной дороге (являющейся территориально распределенной структурой), показывают, что реализация изложенных в статье принципов создает основу для создания и успешного функционирования системы применения ЭЦП в самых различных технологических задачах оперативного характера, либо связанных с управлением критическими процессами. Использование нового объекта системы применения ЭЦП — подчиненного регистрационного центра с функционалом, описанным в статье, позволяет обеспечить максимально быструю проверку статуса ЭЦП в условиях недостаточно качественных сетей передачи данных территориально распределенной структуры.

ONLINE CHECK OF THE ELECTRONIC DIGITAL SIGNATURE IN THE ORGANIZATIONS, THAT HAVE TERRITORIALLY ALLOCATED STRUCTURE WITH USE OF THE SUBORDINATED REGISTRATION CENTER

S.P. KALIUTCHYK

Abstract

Features of the electronic digital signature check in online mode are considered in view of requirements legislative and statutory acts of the Republic of Belarus in conditions of corporation with territorially allocated structure and the centralized management by the example of the Belarusian railway. Lacks of use of traditional, three-level system of application of the electronic digital signature for its online check in conditions of real information-telecommunication networks of territorially allocated structure are proved. The concept of a new element system of the electronic digital signature — the subordinated registration center, is entered.

Литература

1. Закон Республики Беларусь "Об электронном документе" от 10.01.2000 г.
2. Руководящий документ Республики Беларусь "Банковские технологии. Технология электронной цифровой подписи. Термины и определения", РД РБ 07040-2004.
3. *Полянская О.Ю.* Стандарты и спецификации в области инфраструктур открытых ключей. Безопасность информационных технологий. Вып. 1. МИФИ, 2003.