УДК 004.738
ББК 30

ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ В МУЛЬТИ-СЕТЕВОЙ СРЕДЕ

Асратян Р. Э.[1], Лебедев В. Н.[2]
(*ФГБУН Институт проблем управления РАН, Москва*)

Рассматривается новое архитектурное решение задачи защиты информационных запросов и обеспечения безопасных взаимодействий на базе технологии .NET в гетерогенной мультисетевой среде, основанное на применении технологии прокси-серверов. Суть решения заключается в организации специальных серверов-посредников, исполняющих роль шлюзов между информационно-управляющими системами и глобальной сетью и выполняющих функции проверки и формирования электронных подписей во входящих и исходящих SOAP-сообщениях.

Ключевые слова: распределенные системы, интернет-технологии, сетевые протоколы, веб-сервисы, электронная подпись.

1. Введение

Методам и средствам управления информационной безопасностью в территориально-распределенных информационных системах уже давно уделяется большое внимание. Интерес к ним еще более усилился в последние годы в связи с появлением систем, обеспечивающих межведомственное или транснациональное информационное взаимодействие в сложной мультисетевой среде, включающей множество сетей разного размера и

[1] *Рубен Эзрасович Асратян*, *кандидат технических наук*, *доцент* (*rea@ipu.ru*).
[2] *Виталий Николаевич Лебедев*, *кандидат технических наук*, *доцент* (*lebvini@ipu.ru*).

административной подчиненности. Вопросы, связанные с защитой и аутентификацией электронных сообщений (информационных запросов и ответов), а также с защитой информационных ресурсов от несанкционированного доступа из сети, в этих условиях стали особенно актуальны.

Однако многие разработчики подобных систем уже успели почувствовать, что созданные еще в 90-х годах универсальные интернет-технологии защиты информации в сети имеют с этой точки зрения ряд важных недостатков.

- Аутентификация и проверка целостности данных в универсальных технологиях сетевой защиты осуществляется или на уровне IP-датаграмм (IPsec), или же на уровне блоков данных, на которые разбивается информационный поток в TCP-канале (SSL и TLS [1, 4, 8]) с помощью встроенного механизма электронной подписи (ЭП). Однако в этих условиях не существует никакой связи между электронным сообщением и подобной ЭП. Зарегистрировать и сохранить документ электронного сообщения вместе с удостоверяющей его подписью попросту невозможно.
- В системах электронного документооборота уже давно сложилась практика использования сразу нескольких ЭП для подтверждения корректности одного и того же документа (например, подписи исполнителя и одной или нескольких утверждающих подписей руководителей или организаций). В последние годы возникло понимание необходимости применения подобной схемы аутентификации и для межведомственных или транснациональных электронных сообщений. Между тем, универсальные методы сетевой защиты данных не предоставляют возможности применения нескольких ЭП для удостоверения одной и той же информации.

Именно по этой причине в последние годы был разработан ряд международных стандартов на внедрение ЭП в электронные документы в формате XML, которые нашли применение в сетевой архитектуре .NET для защиты информационных запросов и ответов (так называемых SOAP-сообщений) [5, 7]. Эти стандарты вместе с соответствующим программным обеспечением,

разработанным рядом криптопровайдеров, создали основу для решения задачи защиты данных в сети на уровне электронных сообщений. Тем не менее, разработчики распределенных систем все еще сталкиваются в этой области с рядом проблем. Эти проблемы связаны с отсутствием универсальных архитектурных решений задачи встраивания упомянутых средств криптозащиты электронных сообщений в уже существующие или вновь разрабатываемые информационные системы. В этих условиях разработчики вынуждены тратить время и силы для поиска собственных ответов на следующие вопросы:

- Должны ли средства информационной защиты встраиваться в клиентские и сервисные компоненты систем или же занимать в ней какое-то особое выделенное положение?
- Каким образом осуществлять «перехват» электронных сообщений для их криптообработки (формирования и проверки ЭП)?
- Как совместить аутентификацию электронных сообщений с защитой информационных ресурсов в мульти-сетевой среде?

В данной работе описывается новый подход к решению данной задачи, основанный на технологии прокси-серверов, т.е. серверов-посредников, размещаемых на границах сетей и обеспечивающих как аутентификацию электронных сообщений на основе сетевого протокола HTTP/SOAP [5, 7], так и защиту информационных ресурсов внутри сетей от несанкционированного доступа. Главное преимущество этого подхода заключается в его высокой универсальности, выражающейся в независимости от архитектур взаимодействующих информационных систем, их операционных и языковых платформ и средств их разработки.

2. *Аутентификации SOAP-сообщений и защита информационных ресурсов*

Основу мульти-сетевой среды распределенных информационных систем обычно составляют частные локальные сети организаций, соединенные одной или несколькими глобальны-

ми сетями. Статус частной сети предполагает высокую степень изолированности от остальной среды: прямое сетевое соединение между программами, работающими в разных частных сетях невозможно без применения специальных средств (например, трансляторов IP-адресов в датаграммах или серверов-посредников). Желание администраторов «спрятать» информационные ресурсы в частных сетях и возрастающее недоверие к низкоуровневым (т.е. основанным на IP-адресах и портах) средствам ограничения доступа - межсетевым экранам - можно признать важной тенденцией последних лет. Появление технически изощренных форм «взлома» межсетевых экранов, основанных на фальсификации IP-адресов в IP-датаграммах, значительно поколебало веру в их надежность. Сегодня многие разработчики склоняются к мнению, что высоконадежные средства информационной защиты должны быть основаны на ЭП в составе электронных сообщений (если, разумеется, удаленное взаимодействие целиком построено на технологии электронных сервисов в архитектуре .NET).

Структура SOAP-сообщения с электронной подписью, внедренной в его заголовок в соответствии со стандартами консорциумов W3C и OASIS, проиллюстрирован на рис. 1 (предполагается, что soap и wsse – префиксы пространств имен **http://schemas.xmlsoap.org/soap/envelope/** и **http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd** соответственно). Как видно из рисунка, внедрение ЭП осуществляется с помощью специальных тегов (например, тегов security) с сохранением корректной XML-структуры документа. Важно отметить, что стандарт допускает размещение любого количества ЭП в заголовке сообщения. Каждая ЭП может относиться (т.е. удостоверять) или ко всему телу сообщения или же к отдельному фрагменту тела, ограниченного каким-либо тегом.

Применение технологии прокси-серверов для аутентификации электронных сообщений и защиты информационных ресурсов в частных сетях основано на следующих принципах.

- Функции «перехвата», защиты и аутентификации SOAP-сообщений реализуются в выделенных прокси-серверах, размещаемых на границах сетей.
- Каждый прокси-сервер уполномочивается формировать ЭП организации в SOAP-сообщениях, исходящих из частной сети организации, и проверять ЭП во входящих SOAP-сообщения, т.е. поступающих в нее. Это означает, что ему должны быть доступны открытый и закрытый криптографические ключи организации, необходимые для формирования ЭП.
- Авторизация и проверка прав доступа к данным осуществляются в адресуемых электронных сервисах на основе имен подписантов, содержащихся в ЭП. Чтобы упростить им эту задачу, прокси-сервер извлекает имена подписантов (подтвержденные доверенным удостоверяющим центром) из всех проверенных ЭП и помещает их в заголовок SOAP-сообщения.
- Все входящие информационные запросы (ответы), не прошедшие аутентификацию, не только не обрабатываются соответствующими электронными сервисами (клиентами), но вообще не допускаются в частную сеть.

Другими словами, при данном подходе прокси-сервер выполняет функции своего рода высокоуровневого межсетевого экрана, работающего на уровне SOAP-сообщений и ЭП (а не на общепринятом уровне IP-датаграмм). Важно подчеркнуть, что в сочетании с жесткими мерами безопасности (отключение всех сетевых служб, кроме самого прокси-сервера, запрет на прямую маршрутизацию IP-датаграмм с одного сетевого интерфейса на другой на «пограничных» серверах) межсетевой экран подобного типа способен обеспечить наиболее высокий уровень информационной безопасности, практически исключающий возможность «взлома» с помощью технических средств. Далее в статье мы будем называть прокси-серверы, оснащенные средствами формирования и проверки ЭП в SOAP-сообщениях, «прокси-серверами с криптозащитой» (ПСК).

На рис. 2 проиллюстрирована защита SOAP-сообщений в сложной мульти-сетевой среде, включающей глобальную сеть, несколько частных сетей организаций и ведомственную сеть

(например, организованную с помощью технологии виртуальных частных сетей [1]). Как видно из рисунка, информационный запрос от рабочей станции *PC*, направленный к серверу WS_3, проходит в форме SOAP-сообщения три ПСК, размещенных на границах частной сети LAN_1 и ведомственной сети (P_1), ведомственной и глобальной сетей (P_0) и, наконец, глобальной сети и LAN_3 (P_3). Первый из серверов формирует и помещает в SOAP-сообщение подпись организации. Второй проверяет подпись организации и добавляет «утверждающую» подпись ведомства. Наконец, сервер P_3, защищающий LAN_3, проверяет обе подписи у входящего сообщения и, после успешной аутентификации, пропускает его в частную сеть к адресуемому информационному ресурсу.

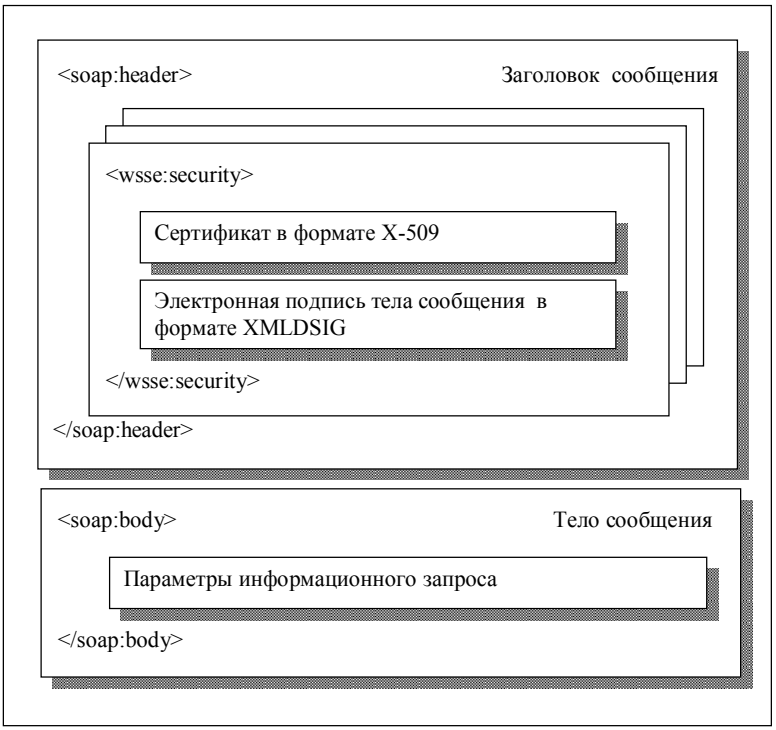

Рис. 1. Электронные подписи в составе SOAP-сообщения

Важно отметить, что документ входящего сообщения может быть не только обработан, но и зарегистрирован в WS_3 вместе со всеми содержащимися в нем ЭП.

Разумеется, приведенная в данном примере обработка электронного сообщения была бы невозможна, если бы на прокси-серверы не обеспечивали выполнение еще одной важной функции в дополнение к функциям криптозащиты: маршрутизации информационных запросов в мульти-сетевой среде. В данной статье мы не будем подробно останавливаться на данной функции; отметим лишь, что маршрутизация в данном случае осуществляется не по IP-адресам, а по символическим интернет-именам информационных ресурсов. Это позволяет обеспечить корректный доступ к электронным сервисам в удаленных частных сетях, даже если несколько сервисов имеют одинаковый IP-адрес [2, 3].

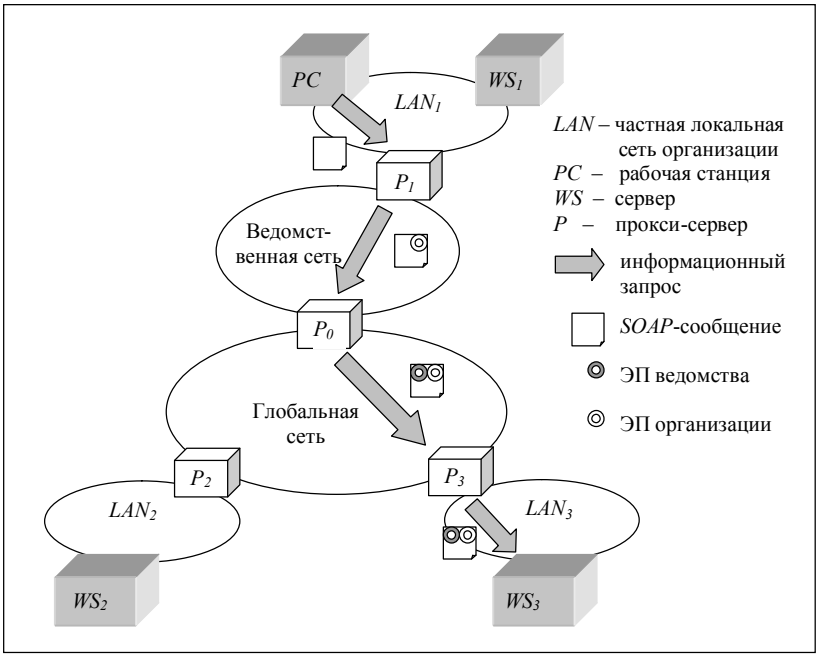

Рис. 2. Защита SOAP-сообщений в мульти-сетевой среде

К недостаткам описанного подхода следует отнести дополнительные временные задержки, вносимые ПСК и функциями формирования и проверки ЭП в электронных сообщениях. С целью оценки этих задержек была проведена серия экспериментов с опытной реализацией ПСК. Цель экспериментов заключалась в сравнении времен выполнения запросов к модельным электронным сервисам в условиях прямого обращения (без ПСК) и при обращении через ПСК, выполняющий проверку ЭП в каждом запросе и формирование ЭП в ответе на запрос. Важно подчеркнуть, что измерялось не только время выполнения одиночных запросов, но и скорость обработки (число обработанных запросов в секунду), достигаемая при одновременной обработке пакета информационных запросов. Другими словами, мы попытались провести сравнение с учетом распараллеливания обработки в множестве программных потоков (и в ПСК, и службе электронных сервисов для обработки каждого запроса создается отдельный программный поток). Скорость обработки вычислялась как частное от деления числа запросов в пакете на полное время его выполнения.

Эксперименты проводились в условиях скоростного (100 Мбит/сек.) Ethernet в среде Windows Server 2003 на достаточно скромном сервере, оснащенном одноядерным процессором Intel с частотой 2,8 Ггц и 2 Гб оперативной памяти. Размер SOAP-сообщения колебался в пределах от 2 до 4 Кб, число элементов (тегов) в сообщении – от 50 до 100.

На рис. 3 показан характерный график, который дает представление о дополнительных задержках, вносимых ПСК, при обращении к двум модельным электронном сервисам с фиксированным временем выполнения (задержкой), равным 0,5 с и 1 с соответственно. В эксперименте измерялась скорость обработки (число обработанных запросов в секунду), достигаемая при обработке группы запросов, т.е. при одновременном обращении сразу нескольких клиентов. По горизонтальной оси графика отложено количество запросов в группе, а по вертикальной – скорость обработки. Первая пара кривых (прорисованная сплошными линиями) относится к более быстрому сервису

(0,5 с), а вторая (прорисованная прерывистыми линиями) – к более медленному (1 с). При этом более тонкая кривая соответствует ситуации с прямым обращением к модельному сервису (без криптозащиты), а более толстая – с обращением через ПСК с формированием и проверкой ЭП.

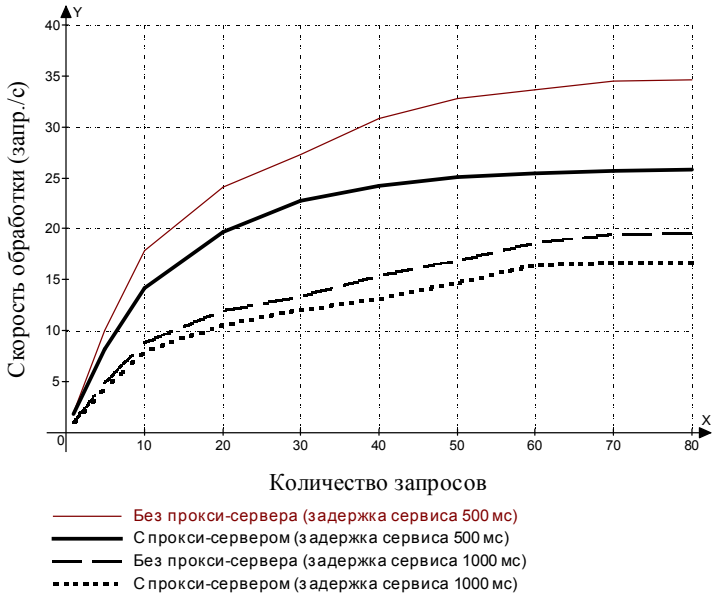

Рис. 3. Пример графика зависимости скорости обработки от числа одновременных запросов

При подаче одиночного запроса на вход сервиса со временем выполнения 0,5 с полное время обработки составило 500 мс без ПСК и 546 мс с ПСК (2 запроса в секунду и 1,88 соответственно). Как видно из графика, при росте числа одновременных запросов растет и скорость обработки, что объясняется «многоканальной» природой и ПС и электронного сервиса, т.е. положительным эффектом от распараллеливания обработки в нескольких программных потоках. Например, при одновременной подаче 10 запросов время их выполнения составило 560 мс без ПСК и 703 мс с ПСК (17,8 и 14,2 запросов в секунду соответст-

венно). Как видно из графика, при превышении числа запросов в группе значения 20-30 рост кривых сильно замедляется, а при превышении значения 70-80 – прекращается вовсе, достигая предельной производительности.

Как видно из первой пары кривых, при обращениях к быстрому (0,5 с) сервису применение ПСК существенно замедляет обработку практически при любом числе запросов в группе. Но для более медленного сервиса (1 с) относительная разница между кривыми значительно уменьшается. Другими словами, для электронных сервисов с собственным временем выполнения более 1 с влияние ПСК становится менее существенным.

На рис. 4 приведен график зависимости среднего времени выполнения информационного запроса от числа запросов в пакете при обращении к тем же двум модельным сервисам и в тех же обозначениях. В отличие от рис. 3, здесь все кривые демонстрируют устойчивый рост. Легко видеть, что и по этому важному показателю влияние ПСК является довольно ощутимым при обращении к более быстрому сервису (0,5 с) и менее ощутимым при обращении к более медленному сервису (1 с). Например, при поступлении 10 одновременных запросов соотношение значений среднего времени обработки запроса с ПСК и без ПСК равно 1,28 в первом случае и 1,12 во втором.

В целом результаты экспериментов позволяют сформулировать следующие выводы.

- Применение ПСК в целом сохраняет положительный эффект от многопоточного распараллеливания обработки.
- ПСК вполне позволяет поддерживать скорость обработки до нескольких и даже нескольких десятков запросов в секунду, что обычно бывает достаточным для большинства информационно-управляющих систем.
- Чем больше время выполнения электронного сервиса, тем менее заметна задержка, вносимая ПСК. В частности, в проведенных экспериментах наблюдалось заметное снижение скорости обработки при одновременном обращении сразу нескольких клиентов к быстрым (со временем выполнения менее 1 с) электронным сервисам через ПСК и не столь существенное при

обращении к более медленным (со временем выполнения более 1 с).

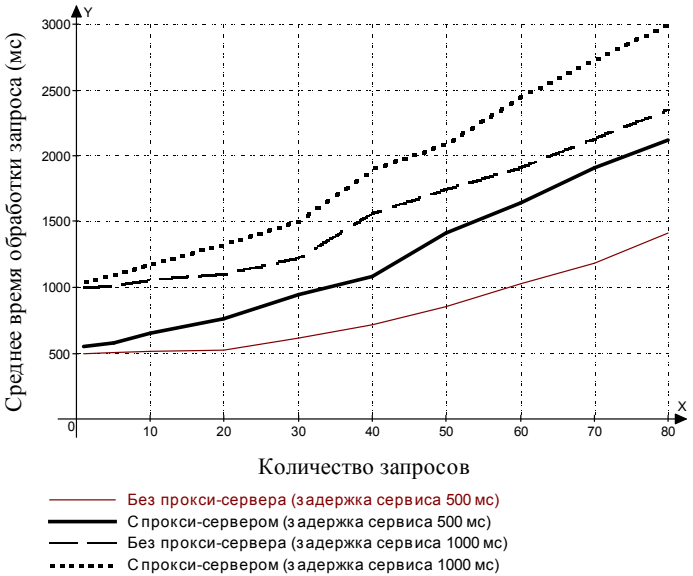

Рис. 4. Пример графика зависимости среднего времени обработки одного запроса от количества одновременных запросов

3. Проблема сохранения подписи исполнителя в частной сети

Важный недостаток описанной выше организации информационный защиты заключается в отсутствии в ней электронной подписи исполнителя – лица, непосредственно инициировавшего информационный запрос с помощью клиентского приложения. Без ЭП исполнителя, формируемой клиентским приложением одновременно с электронным документом запроса на основе личных ключей защиты, возникает угроза искажения или фальсификации запроса еще в пределах исходной частной сети. Очевидно, что безопасное поведение ПСК должно вклю-

чать проверку подписи исполнителя перед формированием подписей организации и/или ведомства в SOAP-документе. Сетевая архитектура .NET содержит специальные средства, позволяющие сформировать ЭП исполнителя в SOAP-документе запроса еще в пределах создавшего его приложения.

Однако здесь возникает важная проблема – проблема «посредников». Если между клиентским приложением и ПСК имеются один или несколько дополнительных обработчиков информационного запроса, то ЭП исполнителя может оказаться потерянной.

Рассмотрим следующий пример. Предположим, что в частной сети организации находятся одно или несколько клиентских рабочих мест для подготовки информационных запросов и сервер приложений с локальным электронным сервисом для централизованной регистрации этих запросов в БД (см. рис. 5). Логика обработки предполагает, что клиенты не обращаются непосредственно к удаленному сервису, но обращаются к локальному сервису-регистратору, который регистрирует информационный запрос, дополняет его добавочными параметрами (например, регистрационным номером, датой и временем регистрации) и уже после этого осуществляет обращение к удаленному сервису через ПСК. Результаты выполнения запроса также регистрируется в БД, после чего передаются клиенту. Очевидно, что на выходе сервиса-регистратора появляется совершенно новый SOAP-документ уже без ЭП исполнителя (сервис попросту не может сформировать ее повторно, так как не располагает необходимыми для этого личными ключами защиты).

Эффективный способ решения этой проблемы дает новый механизм – копирование ЭП исполнителя из входного SOAP-сообщения в выходное без повторного формирования в локальных электронных сервисах. Этот механизм «наследования» ЭП работает по следующим правилам:

- Клиентское приложение формирует в исходящем SOAP-сообщении одну или несколько ЭП, каждая из которых относится к какому-то фрагменту тела сообщения ограниченному опре-

деленным тегом (причем разным ЭП соответствуют разные теги).

- Получив клиентское SOAP-сообщение, локальный электронный сервис проверяет все содержащиеся в нем ЭП и сохраняет его «как есть» перед началом обработки.
- Сформировав собственное исходящее SOAP-сообщение для обращения к удаленному сервису, локальный сервис начинает сопоставление входящего (клиентского) и исходящего сообщений.
- Для каждой ЭП, обнаруженной во входящем сообщении, локальный сервис определяет имя связанного с ним тега и отыскивает тег с таким же именем в выходном сообщении. Если выходное сообщение содержит тег с таким же именем, то соответствующий ему фрагмент тела сообщения полностью замещается аналогичным фрагментом входного сообщения (см. рис. 5), а соответствующее ЭП копируется из входного сообщения в выходное.

Как видно из приведенного описания, механизм «наследования» ЭП опирается на два предположения:

- фрагменты входного и выходного SOAP-сообщений, соответствующие «подписанным» тегам с одинаковыми именами, действительно содержат одну и ту же информацию,
- каждый «подписанный» тег не повторяется в теле сообщения несколько раз.

Вернемся к рассмотрению примера с локальным сервисом-регистратором. Предположим, что метод сервиса-регистратора, к которому обращается клиентское приложение, имеет следующую спецификацию:

int LocalQuery(ParamList QueryParams) ;

Здесь QueryParams – формальный параметр класса ParamList, содержащий набор параметров информационного запроса к удаленному сервису (структура этого класса для нас безразлична).

Предположим, также, что вызываемый метод удаленного сервиса имеет следующую спецификацию:

int RemoteQuery(string RegNum, string DateTime, ParamList QueryParams) ;

Здесь RegNum и DateTime – формальные параметры, предназначенные для передачи регистрационного номера и времени запроса, а QueryParams – формальный параметр класса ParamList, содержащий набор параметров информационного запроса. Будем считать, что описания классов ParamList на сервисе регистраторе и на удаленном сервисе совершенно одинаковы, а сервис-регистратор просто переносит полученные параметры информационного запроса в удаленный вызов. В этом случае и входящее и исходящее SOAP-сообщения будут содержать теги <QueryParams>, содержащие одинаковые данные. Если клиентское приложение сформирует ЭП для фрагмента SOAP-сообщения, ограниченного тегом <QueryParams>, то эта ЭП может быть «унаследована» выходным сообщением сервиса-регистратора.

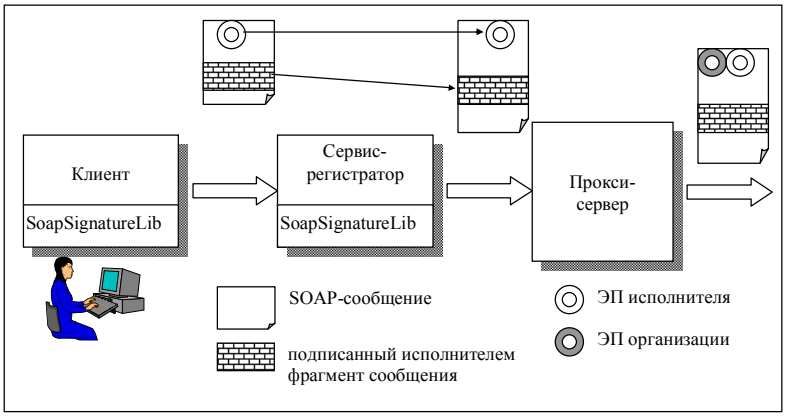

Рис. 5. Механизм наследования ЭП исполнителя в сервисе-посреднике

Описанные принципы «наследования» ЭП исполнителя были реализованы в библиотеке функций SoapSignatureLib, предназначенной для формирования и проверки ЭП непосредственно в клиентских и сервисных приложениях для организации безо-

пасного взаимодействия с ПСК (см. рис. 5). Работа библиотеки основана на механизмах Client Message Inspector и Dispatch Message Inspector в сетевой архитектуре .NET. Будучи подключенной к приложению, библиотека берет на себя такие функции, как «перехват» входящих и исходящих SOAP-сообщений, формирование и проверка ЭП, причем работа библиотеки совершенно не зависит от архитектуры приложения или структуры электронных сервисов. Следует оговориться, что библиотеку SoapSignatureLib можно использовать только в системах, ориентированных на работу в среде Microsoft Framework 4.0 или старше. Другими словами, в отличие от ПСК, она не обеспечивает платформенной независимости.

4. Заключение

В условиях отсутствия общего архитектурного решения для задачи криптозащиты электронных сообщений в мульти-сетевой среде разработчики вынуждены расходовать время и силы для создания собственных технических решений, привязанных к особенностям конкретных систем, платформам и средствам программирования. Авторы попытались показать, что технология прокси-серверов может послужить основой общего решения этой задачи.

Описанный подход был реализован в форме дополняющих друг друга программных продуктов для среды Win32: ПСК (в форме Windows-службы [1, 6]) и библиотеки функций SoapSignatureLib для обработки ЭП в клиентских приложениях и электронных сервисах. Оба продукта реализованы на языке C# в среде Microsoft Visual Studio с использованием сертифицированных криптосредств компании «КриптоПро».

В данной работе не рассматривались вопросы шифрования электронных сообщений в сети. Однако следует отметить, что предложенный подход вполне совместим со средствами шифрования, реализованными в IPsec или TLS/SSL.

Разработанные методы и средства управления информационной безопасностью прошли испытания в составе Системе

межведомственного электронного взаимодействия (СМЭВ), представляющей собой федеральную государственную информационную систему, предназначенную для интеграции информационных ресурсов федеральных органов государственной власти на базе единых стандартов защиты информации и сетевых технологий. Испытания показали, что описанный подход может быть использован в качестве типового решения для задачи организации безопасного взаимодействия в СМЭВ и других территориально-распределенных информационных системах, базирующихся на сетевой архитектуре .NET.

Литература

1. АНДРЕЕВ А.Г., БЕЗЗУБОВ Е.Ю., ЕМЕЛЬЯНОВ М.М. И ДР. *Widows 2000: Server и Professional.* – СПБ.: «БХВ-Санкт-Петербург», 2001. – 1055 с.
2. АСРАТЯН Р.Э., ЛЕБЕДЕВ В.Н. *Организация защищенного http-взаимодействия в мульти-сетевой среде* // Управление большими системами. – 2012 - №36. - С. 285-300.
3. АСРАТЯН Р.Э., ЛЕБЕДЕВ В.Н. *Прокси-серверы в распределенных гетерогенных мульти-сетевых средах* // Проблемы управления. – 2013 - №2.- С. 45-50.
4. ДЖАМСА К., КОУП К. *Программирование для Internet в среде Windows.* – СПб.: Питер, 1996. – 659 с.
5. МАК-ДОНАЛЬД М., ШПУШТА М. *Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов.* - М.: Вильямс, 2009. – 1408 с.
6. СНЕЙДЕР Й. *Эффективное программирование TCP/IP. Библиотека программиста.* – СПб.: Символ-Плюс, 2002. – 320 с
7. ШАПОШНИКОВ И.В. *Web-сервисы Microsoft .NET*. – СПб.: БХВ – Петербург, 2002. – 336 с.
8. ХАНТ К. *TCP/IP. Сетевое администрирование.* – СПб.: Питер, 2007. – 816 с.

ORGANIZATION OF PROTECTED HTTP-INTERACTION IN MULTI-NETWORK ENVIRONMENT

Ruben Asratian, Institute of Control Sciences of RAS, Moscow, Cand.Sc., assistant professor (rea@ipu.ru).
Vitali Lebedev, Institute of Control Sciences of RAS, Moscow, Cand.Sc., assistant professor (lebvini@ipu.ru).

Abstract: We suggest an architectural solution based on proxy servers technology for the problem of query protection and the.NET technology-based interactions security in the heterogeneous multi-network environment. The idea is to use special intermediary servers playing the role of gateways between information systems and a global network and carrying out functions of digital signature generation and verification for input and output SOAP messages.

Keywords: distributed system, Internet technology, network protocol, Web-service, digital signature.

Статья представлена к публикации членом редакционной коллегии М.В. Губко

Поступила в редакцию 08.05.2013.
Опубликована 30.09.2013.