**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт компьютерных технологий и защиты информации

### КАФЕДРА СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### к выполнению Лабораторной работы № 4

на тему

**«**Обеспечение защищенности веб-сервисов**»**

Казань 2021

**ЛАБОРАТОРНАЯ РАБОТА № 4**

**Название работы:**

Обеспечение защищенности веб-сервисов

**Цель работы:**

Ознакомиться на практике с методом защиты веб-сервисов WS-Security

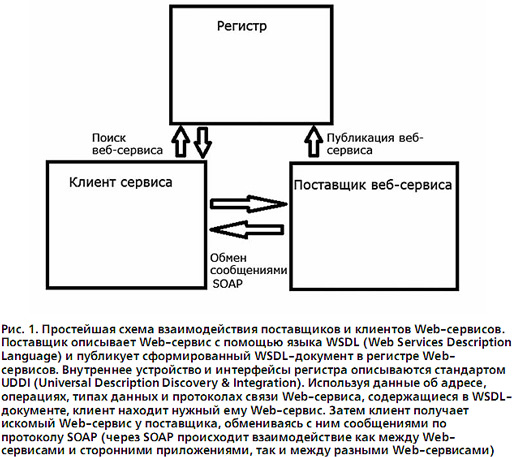
**Теоретический материал:**

**ОБЩИЕ СВЕДЕНИЯ**

1. **Веб-сервис**

Веб-сервис - это вызываемый удаленно программный компонент, имеющий заданные функциональные возможности, доступны стандартным протоколам сети Интернет и пригодный для многократного использования.

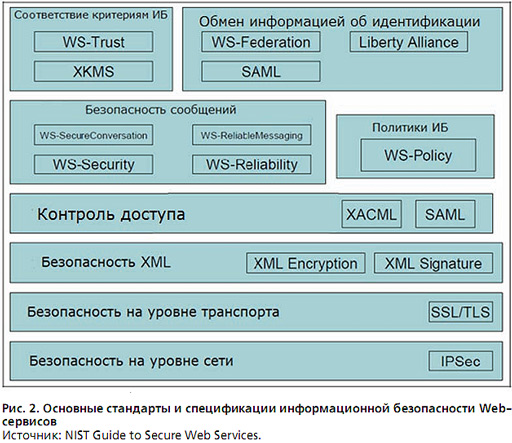
Чтобы понять принцип работы Веб-сервисов, давайте рассмотрим типичную схему взаимодействия их поставщиков и клиентов (рис. 1).



*Рис.1*

Согласно мнению аналитиков организации OASIS Веб Services Interoperability, главные угрозы, нацеленные на Веб-сервисы, - это несанкционированные изменения сообщений, потеря их конфиденциальности и аутентичности отправителей, DoS-атаки, то есть угрозы информационной безопасности Веб-сервисов, практически идентичны угрозам, направленным на другие цифровые ресурсы. Обеспечение информационной безопасности Веб-сервисов предполагает использование общепринятых технологий информационной безопасности - шифрования, цифровых подписей, парольной защиты и т.д. Можно сказать, что стандарты информационной безопасности Веб-сервисов соответствуют специфичной архитектуре ИБ Веб-сервисов, но механизмы реализации данной архитектуры вполне традиционны.

В настоящее время разработан целый ряд стандартов и спецификаций информационной безопасности Веб-сервисов (рис. 2).



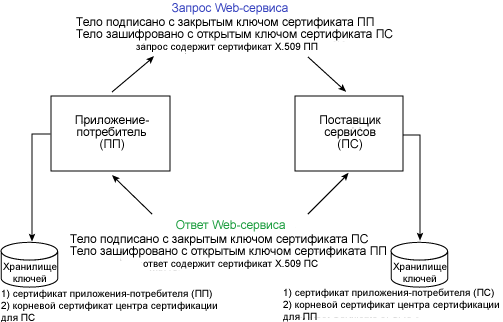
*Рис. 2*

Защита Веб-сервисов должна быть комплексной: от информационных угроз необходимо защищать не только SOAP-сообщения, но также все другие составляющие архитектуры Веб-сервисов: их интерфейсы, средства обнаружения сервисов (регистры) и т.д.

Одним из наиболее популярных стандартов является WS-Security, описывающий процессы аутентификации и авторизации в среде обмена SOAP-сообщениями.

1. **Общая модель WS-Security**

Спецификация WS-Security предоставляет механизмы для выполнения всех трех требований (аутентификация пользователей сервисов, цифровая подпись данных, конфиденциальность данных soap запросов)безопасности между конечными точками приложения. С помощью WS-Security можно выборочно выполнять каждое из требований триады безопасности, реализуя их в решении порознь или вместе.

Система WS-Security между приложением-потребителем и поставщиком сервисов описана на Рис.3

*Рис 3*

В полную реализацию всех трех требований безопасности входят:

**Отправители запросов или ответов веб-сервисов:**

подписывают сообщения, используя закрытый ключ своих сертификатов X.509;

шифруют сообщения, используя открытый ключ сертификата X.509 получателей, что гарантирует доступ к содержимому сообщения только им.

**Получатели запросов или ответов веб-сервисов:**

проверяют подпись сообщения, используя открытый ключ отправителя, для аутентификации отправителя и проверки целостности сообщения;

дешифруют сообщение, используя закрытый ключ своих сертификатов X.509.

1. **Обработка запросов веб-сервиса c WS-Security**

### Обработка запроса веб-сервиса приложением-потребителем

Как правило, приложение-потребитель имеет прокси-сервис или компонент-заглушку JAX-RPC, создаваемые в интегрированной среде разработки (например, ВебSphere Studio Application Developer) с использованием WSDL поставщика сервиса. После вызова веб-сервиса перед отправкой запроса прокси или среда исполнения SOAP на клиентской системе выполняют функции WS-Security.

Сначала SOAP-сообщение подписывается цифровой подписью. Среда исполнения SOAP обращается к хранилищу ключей и по мере необходимости извлекает ключи защиты и сертификаты. В зависимости от предоставляемой вашей средой поддержки WS-Security можно подписывать только тело SOAP-сообщения или отдельные его элементы. Кроме того, можно подписывать блоки SOAP-заголовка. Подписание выполняется с использованием закрытого ключа сертификата X.509 приложения-потребителя. После подписания сообщения сертификат X.509 включается в SOAP-заголовок в виде двоичного маркера доступа. Сообщение шифруется при помощи симметричного алгоритма с общим ключом. Ключ, используемый для шифрования данных, шифруется при помощи асимметричного алгоритма с открытым ключом, ассоциированным с сертификатом X.509 поставщика сервиса. После шифрования сообщения и общего ключа в SOAP-заголовок включается ссылка на сертификат X.509 поставщика сервиса, которому направляется запрос. Это делается в связи с тем, что поставщик сервиса может использовать несколько сертификатов.

### Обработка запроса веб-сервиса поставщиком сервисов

После получения поставщиком сервисов запроса веб-сервиса этот запрос направляется в механизм обработки SOAP (среда исполнения SOAP) на основе URL запроса (опубликованная точка доступа к сервису). Данные сообщения и общий ключ передаются в запросе в зашифрованном виде, поэтому первым шагом является идентификация сертификата X.509, указанного в заголовке SOAP, и извлечение его закрытого ключа из хранилища ключей. После получения закрытого ключа с помощью асимметричного алгоритма дешифруется общий ключ. После дешифрования общего ключа данные сообщения дешифруются с помощью симметричного алгоритма. Теперь, когда все сообщение дешифровано, извлекается открытый ключ сертификата X.509, переданного в SOAP-заголовке. Цифровая подпись сообщения выполнена с использованием открытого ключа приложения-потребителя. Если проверка подписи проходит успешно, среда исполнения SOAP поставщика сервисов подтверждает целостность сообщения и гарантирует, что сообщение действительно подписано приложением-потребителем. Этот процесс также аутентифицирует источник (отправителя) сообщения, так как только отправитель, являясь владельцем сертификата, имеет доступ к закрытому ключу, используемому при подписании сообщения. После дешифрования сообщения и проверки подписи среда исполнения SOAP вызывает реализацию веб-сервиса.

Обработка ответа веб-сервиса поставщиком сервисов

После выполнения бизнес-логики реализации сервиса и получения ответа те же операции WS-Security выполняются для ответного сообщения веб-сервиса. Однако роли пар ключей X.509 для цифровой подписи и шифрования меняются местами. Среда исполнения SOAP поставщика сервисов подписывает сообщение цифровой подписью с использованием закрытого ключа своего сертификата X.509. Сертификат включается в SOAP-сообщение, а сообщение шифруется с использованием общего ключа. Ключом, используемым для шифрования данных, может быть тот же ключ, который передается в первоначальном запросе, или иной, сгенерированный случайным образом ключ, что более типично. Шифрование общего ключа осуществляется с использованием открытого ключа сертификата, который был передан в запросе; таким образом, только отправитель запроса, имеющий доступ к закрытому ключу сертификата, может дешифровать сообщение. После подписания и шифрования сообщения среда исполнения SOAP поставщика сервисов отправляет ответ приложению-потребителю.

Обработка ответа веб-сервиса приложением-потребителем

Обработка приложением-потребителем WS-Security ответа веб-сервиса очень похожа на обработку запроса поставщиком сервисов.

Приложение-потребитель получает ответ веб-сервиса с ответом, направленным в механизм обработки SOAP (среда исполнения SOAP) с учетом первоначального HTTP-сеанса. Данные сообщения и общий ключ передаются в ответ в зашифрованном виде. Таким образом, первым шагом является получение закрытого ключа сертификата, ассоциированного с соответствующим запросом, для дешифрования ключа с использованием асимметричного алгоритма. После дешифрования общего ключа данные сообщения дешифруются с помощью симметричного алгоритма. После дешифрования всего сообщения сертификат X.509, переданный в SOAP-заголовке, используется для извлечения его открытого ключа. Цифровая подпись сообщения ответа создается с использованием открытого ключа поставщика сервисов. Если проверка подписи проходит успешно, среда исполнения SOAP приложения-потребителя подтверждает целостность сообщения и гарантирует, что сообщение действительно подписано поставщиком сервисов. Этот процесс также аутентифицирует источник (отправителя) сообщения, так как только отправитель, являясь владельцем сертификата, имеет доступ к закрытому ключу, используемому при подписании сообщения. После дешифрования сообщения и проверки подписи среда исполнения SOAP передает ответ приложению-потребителю.

**Порядок выполнения работы:**

1. **Изучить теоретический материал.**

**2. По описанным алгоритмам обработки запросов и ответов веб-сервиса приложением потребителем и поставщиком сервисов, построить блок схему алгоритма функционирования.**

|  |  |
| --- | --- |
| 1 вариант | Обработка запроса веб-сервиса приложением-потребителем |
| 2 вариант | Обработка запроса веб-сервиса поставщиком сервисов |
| 3 вариант | Обработка ответа веб-сервиса поставщиком сервисов |
| 4 вариант | Обработка ответа веб-сервиса приложением-потребителем |

**3. Сделать вывод по проделанной работе.**

**4. Ответить на контрольные вопросы.**

Контрольные вопросы:

1. Что такое Веб-сервис?

2. Функции Веб-сервиса?

3. Какие стандарты защиты Веб-сервиса Вы знаете?

4. Что такое WS-Security?

5. Что такое SOAP сообщения?

6. Какие способы защиты SOAP сообщений Вы знаете?

7. Какие способы защиты SOAP сообщений реализованы в WS-Security?

8. Как обрабатывает запрос Веб-сервиса приложение-потребителя?

9. Как обрабатывает запрос Веб-сервиса поставщик сервиса?

10. Как обрабатывает ответ Веб-сервиса приложение-потребителя?

11. Как обрабатывает ответ Веб-сервиса поставщик сервиса?