УТВЕРЖДЕНО

приказом ГБУ СО «РЦУП»

от «22» сентября 2011 г. № 24-21ОСН

ИНТЕГРАЦИОННАЯ ШИНА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА САМАРСКОЙ ОБЛАСТИ

СПЕЦИФИКАЦИЯ ТРЕБОВАНИЙ К МЕХАНИЗМАМ ИНТЕГРАЦИИ С ФЕДЕРАЛЬНОЙ СИСТЕМОЙ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

ЛИСТОВ 18

Самара 2011 г.

ЛИСТ СОГЛАСОВАНИЯ

Спецификация требований к механизмам интеграции с федеральной системой межведомственного электронного взаимодействия

ГБУ СО РЦУП

Должность	ФИО	Подпись	Дата
Заместитель директора	Д.П.Шевченко		15.04.2011
Начальник управления по развитию и сопровождению информационных систем и ресурсов	А.В.Ягупов		11.04.2011
Главный инженер проекта	С.А.Кузьминов		8.04.2011
Главный инженер проекта	Н.В.Кутузов		08.04.2011

Содержание

Введение

Данный документ является уточняющей и дополняющей частью основного документа «Спецификация требований к прототипу информационной системы ИШ ЭП СО», Самара, 2009 год.

Документ описывает требования, предъявляемые к механизмам взаимодействия (интеграции) интеграционной шины электронного правительства Самарской области (далее – ИШ ЭП СО) с федеральной системой межведомственного электронного взаимодействия (далее – ФСМЭВ), реализуемых в рамках работ 2010 года.

В рамках данного документа применяются следующие понятия:

- Сообщение – XML-файл установленной структуры, используемый в процессе информационного взаимодействия, проходящего с использованием ИШ ЭП СО. Существуют следующие типы сообщений:
  - Запрос – сообщение, формируемое системой-потребителем и содержащее данные, необходимые для получения услуги в электронном виде.
  - Ответ – сообщение, формируемое системой-провайдером в ответ на запрос и содержащее данные о статусе или/и результате оказания услуги в электронном виде.

1. Общие требования

Механизмы интеграции должны обеспечивать преобразование форматов сообщений ИШ ЭП СО к форматам ФСМЭВ и обратно.

Механизмы интеграции должны обеспечивать маршрутизацию сообщений, предназначенных как для использования в пределах ЭП СО, так и в пределах межведомственного взаимодействия посредством ФСМЭВ.

Механизмы интеграции должны обеспечивать возможность трансляции (проксирования) в ФСМЭВ сообщений от сервисов, опубликованных на ИШ ЭП СО.

Механизмы интеграции должны обеспечивать возможность трансляции (проксирования) в ИШ ЭП СО сообщений от сервисов, опубликованных в ФСМЭВ.

Механизмы интеграции должны обеспечивать безопасный и защищенный информационный обмен между ИШ ЭП СО и ФСМЭВ.

Должна обеспечиваться возможность получения статистики на основе логирования в разрезе сервисов и сообщений.

Должно обеспечиваться журналирование событий, связанных с обменом сообщениями между ИШ ЭП СО и ФСМЭВ.

При использовании сетевых протоколов передачи данных необходимо следовать следующим спецификациям:

- протокол передачи гипертекста HTTP v1.1 (RFC 2616);
- протокол защищённых соединений SSL v3 / TLS (RFC 2246);
- сервисы поддержки пространства имен DNS (RFC 1035).

При использовании веб-сервисов следует придерживаться следующих спецификаций:

- базовый профиль интероперабельности v1.1 (Web Services Interoperability Organization Basic Profile 1.1);
- протокол SOAP 1.1;

– язык описания веб-сервисов WSDL 1.1;

– спецификация универсального описания, обнаружения и интеграции веб-сервисов UDDI 2.0.

При описании данных, метаданных и используемых наборов символов необходимо следовать следующим спецификациям:

– расширяемый язык разметки XML;

– XML-схема (XML Schema 1.1);

– расширяемый язык таблиц стилей XSL v1.

При обеспечении безопасности информации необходимо следовать следующим спецификациям:

– базовый профиль обеспечения безопасности WS-I Security 1.0;

– стандарт безопасности веб-сервисов WS-Security.

1.1. Режимы функционирования

ИШ ЭП СО должна поддерживать два режима функционирования:

- штатный режим;
- режим системного администрирования.

Штатный режим должен являться основным режимом функционирования, обеспечивающим выполнение функций ИШ ЭП СО.

Режим системного администрирования должен являться технологическим режимом и использоваться для сопровождения ИШ ЭП СО, в том числе изменения конфигурации, параметров работы, настроек, выполнения регламентного обслуживания программно-технических средств.

Для выполнения этого требования необходимо реализовать прокси-сервер, в штатном режиме транслирующий запросы к адаптерам услуг, а в режиме администрирования – возвращающий на все запросы ответ, содержащий уведомление о ведущихся технических работах.

Ответ в режиме администрирования должен представлять собой SOAP пакет, содержащий сообщение, название которого формируется стандартным алгоритмом IBM WebSphere Process Server – название сообщения запроса с суффиксом «Response».

Сообщение должно содержать стандартный блок системной информации ИШ ЭП СО (название элемента – «sysInfo»), с указанным в нем уникальным кодом ответа, соответствующим режиму администрирования, а также текстовое сообщение «ИШ ЭП СО недоступна. Ведутся технические работы».

Для формирования уникального кода ответа для режима системного администрирования необходимо воспользоваться справочником «Ответы, ошибки и исключительные ситуации», содержащегося в документе «Общесистемные справочники и классификаторы, хранимые в информационной системе ИШЭП СО».

Переключение между режимами функционирования должно производиться без перезапуска прокси-сервера.

Работоспособность ИШ ЭП СО должна автоматически восстанавливаться при перезапуске программно-аппаратных средств. Должно быть обеспечено восстановление программного обеспечения серверов в случае сбоя работы оборудования.

1.2. Требования к механизму управления и обработки событий

ИШ ЭП СО должна иметь универсальный механизм управления и обработки событий, не зависящий от типа события. Механизм обработки событий должен иметь возможность рассылки событий всем участникам взаимодействия, а также принимать события от других участников взаимодействия.

Механизм обработки событий должен быть реализован на основе существующей системы аудита. Для управления событиями должен быть реализован административный интерфейс управления событиями. Административный интерфейс управления событиями должен решать следующие задачи:

- создание событий;
- удаление событий;
- редактирование событий.

Административный интерфейс управления должен позволять управлять публикациями событий и подписками на оповещения о событиях по электронной почте. Публикация событий должна быть реализована посредством JMS.

При публикации события необходимо указать следующие атрибуты:

- событие;
- название модуля;
- услуга;
- наименование топика JMS, на который должно публиковаться событие.

ИШ ЭП СО должна иметь механизм подписки на события. При формировании подписки на оповещение о событии по электронной почте должны быть указаны:

- событие;
- название модуля;
- услуга;
- адрес электронной почты, на который должно отсылаться оповещение.

Обработка событий должна быть реализована в виде очереди JMS. В очередь JMS должны поступать события, как возникшие внутри адаптеров и модулей ИШ ЭП СО, так и от других участников взаимодействия. Должен быть реализован обработчик событий из очереди, который должен публиковать события для подписчиков и рассылать уведомления по электронной почте в соответствии с настройками оповещений.

1.3. Требования к механизму оповещений

При формировании подписки на оповещения о событиях необходимо задавать адреса электронной почты администраторов с привязкой к компонентам ИШ ЭП СО (модуль ИШ ЭП СО, услуга, событие).

При формировании подписки на оповещение о событии по электронной почте должны быть указаны:

- событие;
- название модуля;
- услуга;
- адрес электронной почты, на который должно отсылаться оповещение.

Механизм оповещений должен иметь задаваемый интервал времени, за который собираются сообщения от компонентов электронных сервисов о возникших сбоях или их устранении.

Необходимо формировать пакет уникальных сообщений за заданный интервал времени для каждого адреса электронной почты, исключающий повторные сообщения об одном и том же событии, и его отправку адресату. Пакет уникальных сообщений должен включать сообщения о событиях во всех компонентах ИШ ЭП СО, на которые подписан данный адресат.

Механизм оповещений должен осуществлять протоколирование (журналирование) всех уведомлений о возникновении событий и всех фактов рассылки.

2. Требования к прокси-интерфейсам

Прокси-интерфейсы должны осуществлять проксирование электронных сообщений, пересылаемых ФСМЭВ в ИШ ЭП СО и обратно.

2.1. Требования к структуре электронных сообщений, пересылаемых ФСМЭВ

Требования к общей структуре SOAP-сообщения:

- soap:header (заголовок электронного сообщения системы взаимодействия);
- soap:body (тело электронного сообщения системы взаимодействия);
- soap:Fault (сообщение об ошибке).

Заголовок электронного сообщения ФСМЭВ включает в том числе:

- передачу сведений об аутентификации и авторизации (WS-security),
- передачу параметров при асинхронном взаимодействии (WS-Addressing).

Тело электронного сообщения ФСМЭВ в общем случае состоит из следующих элементов:

- блок данных;
- блок присоединенных документов;
- блока ЭЦП.

Блок данных электронного сообщения должен содержать дату и время отправки электронного сообщения в систему взаимодействия.

Блок присоединенных документов может содержать информацию (текстовую, графическую и пр.), прилагаемую к электронному сообщению системы взаимодействия.

Блок ЭЦП может содержать ЭЦП ФСМЭВ или набор ЭЦП информационных систем, взаимодействующих с ФСМЭВ и самой ФСМЭВ.

Сообщение об ошибке содержит текстовое описание возникшей ошибки и ее код в рамках ИС, в рамках которой она возникла.

2.2. Требования к структуре электронных сообщений, пересылаемых ИШ ЭП СО

Требования к структуре электронных сообщений, пересылаемых ИШ ЭП СО должны удовлетворять требованиям, изложенным в документе «Спецификация требований к интерфейсам взаимодействия между компонентами архитектуры ЭП СО в рамках оказания электронных услуг»

2.3. Требования к обработке входящих сообщений

Прокси-интерфейсы в процессе обработки входящих сообщений должны выполнять контроль ЭЦП сообщения.

Требования к проведению контроля ЭЦП должны удовлетворять требованиям, изложенным в документе «Спецификация требований к механизмам постановки и проверки ЭЦП».

2.4. Контрольный пример

Под контрольным примером обращения к прокси-интерфейсу понимается пример запроса к прокси-интерфейсу и ответа прокси-интерфейса на указанное обращение. Контрольный пример запроса и ответа должен быть предоставлен поставщиком в формате SOAP.

Назначением контрольного примера является подтверждение работоспособности прокси-интерфейса при проведении процедуры регистрации, в рамках которой осуществляется отправка прокси-интерфейсу запроса, приведенного в контрольном примере, и сравнение полученного ответа прокси-интерфейса с ответом, приведенном в контрольном примере.

Контрольный пример не должен вызывать выполнение каких-либо операций в информационной системе, которые могут привести к возникновению событий, позволяющих информационной системе участника взаимодействия или работникам участника взаимодействия интерпретировать полученные при выполнении контрольного примера данные как реальные, а не тестовые.

Регистрация прокси-интерфейса может считаться завершенной только при условии успешного выполнения контрольного примера, которое предполагает совпадение ответа прокси-интерфейса с ответом, приведенным в контрольном примере, либо, при объективной невозможности возврата прокси-интерфейсом повторяемых данных, – его соответствие описанию логики формирования ответа, которое в подобных случаях должно сопровождать предоставляемый контрольный пример (к примеру, прокси-интерфейс возвращает номер зарегистрированного обращения, который не может повторяться, - в этом случае контрольный пример сопровождается указанием этого факта).

В дальнейшем контрольный пример может быть использован для настройки модуля системы взаимодействия, обеспечивающего проверку доступности и работоспособности прокси-интерфейса, а так же для отладки программного кода разработчиками Потребителя электронного сервиса.

2.5. Гарантированная доставка сообщений

Прокси-интерфейс должен обеспечивать гарантированную доставку неискаженных сообщений в рамках информационного обмена между информационной системой данного участника взаимодействия и системой взаимодействия.

Для реализации возможности осуществления повторных вызовов электронных сервисов при сбоях доставки сообщений необходимо обеспечить на ИШ ЭП СО настройку следующих параметров:

- количество повторных вызовов до формирования сообщения о сбое доставки сообщения;
- временной интервал, в течение которого осуществляются повторные вызовы.

3. Требования к информационной безопасности

3.1. Списки отозванных сертификатов

Программно-техническими средствами ИШ ЭП СО должна обеспечиваться возможность проверки действительности сертификатов открытых ключей ЭЦП с использованием списков отозванных сертификатов (CRL – Certificate Revocation List) и протокола получения статуса сертификата в реальном времени (OCSP – Online Certificate Status Protocol).

При отрицательном результате проверки действительности сертификата отправителю сообщения должно отправляться уведомление, а результат операции должен записываться в журнал регистрации событий.

Списки отозванных сертификатов должны соответствовать международному стандарту X.509 версии 2.

3.2. Администрирование

Доступ к интерфейсам администрирования должен осуществляться по протоколу HTTPS.

Доступ к интерфейсам администрирования должен осуществляться только с определенных IP-адресов. Перечень разрешенных IP-адресов должен определяться организацией, ответственной за эксплуатацию ИШ ЭП СО.

События аутентификации администратора при доступе к интерфейсам администрирования существующих и разрабатываемых компонентов ИШ ЭП СО, а именно, к интерфейсам просмотра статистики, подсистемы разграничения доступа, подсистемы управления событиями, подсистемы оповещений, подлежат обязательной регистрации в журнале событий.

ИШ ЭП СО должна иметь возможность удаления учетной записи администратора для доступа в администраторский интерфейс при нарушении правил доступа к ИШ ЭП СО.

В ИШ ЭП СО должен вестись журнал всех действий администратора в администраторских интерфейсах, а именно: в интерфейсах просмотра статистики, подсистемы разграничения доступа, подсистемы управления событиями, подсистемы оповещений.

4. Список используемых сокращений

Сокращение	Расшифровка
CRL	Certificate Revocation List
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
JMS	Java Message Service
OCSP	Online Certificate Status Protocol
RFC	Request for Comments
SSL	Secure Sockets Layer
TLS	Transport Layer Security
XML	Extensible Markup Language
UDDI	Universal Description Discovery & Integration
WS	Web Services
WSDL	Web Services Description Language
ИС	Информационная система
ИШ ЭП СО	Интеграционная шина электронного правительства Самарской области
ФСМЭВ	Федеральная система межведомственного электронного взаимодействия
ЭП СО	Электронное правительство Самарской области
ЭЦП	Электронная цифровая подпись

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Дата	Автор	Содержание изменения