Требования к взаимодействию с сервисом

Сервис передачи информации о размере базовой пенсионной выплаты

1. **Общие сведения о сервисе**

Владелец сервиса: *Государственное учреждение "Министерство труда и социальной защиты населения Республики Казахстан"*

Наименование информационной системы: *Автоматизированная информационная система «Электронное назначение пенсионных выплат и пособий» АИС «Е-Макет»*

Контур взаимодействия: *Вне ЕТС*

Ключ сервиса: *GCVPbasePens*

Назначение сервиса: *<!DOCTYPE html> <html> <head> </head> <body> Сервис предназначен для передачи порталу «электронного правительства» (ПЭП) информации о размере базовой пенсионной выплаты </body> </html>*

Бизнес описание работы сервиса:

Схема информационного взаимодействия. Форматы данных. Пояснения к схеме:

Режим взаимодействия сервиса: *Синхронный*

2. **Рекомендуемые требования по производительности и надежности**

В таблице 1 приведены требования по производительности и надежности сервиса.

Таблица 1 – Требования по производительности и надежности

№	Контролируемый показатель	Ограничение
1	Максимальное время обработки запроса при синхронном взаимодействии	30 сек
2	Среднее время обработки запроса	10 сек
3	Пиковая нагрузка	2000 запросов в час
4	Номинальная нагрузка	360 запросов в час
5	Среднее время работы без сбоев	365/7/24 доступность
6	Время на восстановление работоспособности	3 часов

3. **Требования по использованию ЭЦП**

Проверка должна осуществляться в соответствии с требованиями Приказа Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи».

Электронные сообщения между участниками информационного обмена должны проверяться по следующим правилам:

- Структура электронного документа должна соответствовать XML формату. Подпись документа должна осуществляться по стандарту XML design и спецификации консорциума W3C «XML — SignatureSyntaxandProcessing» («Синтаксис и обработка подписи XML»), см. ссылку http://www.w3.org/TR/xmldsig-core/. В случае применения стандарта хранения юридически значимых документов (CadES), должен использоваться формат XadES (XML AdvancedElectronicSignatures), спецификация которого отражена в технической документации ETSI TS 101 903 V1.2.2 (2004-04).
- При проверке электронной цифровой подписи в электронном документе должно использоваться подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого должно являться заключение о правильности или ошибочности цифровой подписи (ГОСТ 34.310-2004, определение).
- Регистрационное свидетельство должно быть выдано на имя Отправителя. Должна производиться проверка ИИН/БИН Отправителя с ИИН/БИН в регистрационном свидетельстве.
- Срок действия проверяемого регистрационного свидетельства не должен истечь. Должна быть проверка полей NotBefore и NotAfter. Проверка должна осуществляться по времени Астаны.
- Должна быть проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого со всеми промежуточными регистрационными свидетельствами. Регистрационное свидетельство должно быть удостоверено ЭЦП (выпущено НУЦ РК).
- Проверяемое регистрационное свидетельство не должно быть отозванным. Проверка должна осуществляться с помощью получения OCSP квитанции, путем обращения к сервису НУЦ РК. При повторных проверках данного ЭЦП должна быть возможность использовать ранее полученную OCSP квитанцию – в этом случае проверка должна осуществляться на дату получения квитанции. В случае недоступности сервиса OCSP должна осуществляться проверка по списку отозванных регистрационных свидетельств в Base CRL и Delta CRL (Проверка наличия серийного номера регистрационного свидетельства в Base CRL и Delta CRL НУЦ РК). Base CRL и Delta CRL НУЦ необходимо подкачивать по пути указанному в проверяемом регистрационном свидетельстве.
- Проверка поля «использование ключа» (KeyUsage). Необходимо убедиться в наличии значений «Цифровая подпись», «Неотрекаемость» – для регистрационного свидетельства, используемого для ЭЦП и «Цифровая подпись», «Шифрование ключей» – для регистрационного свидетельства, используемого для аутентификации.

Алгоритм формирования ЭЦП должен соответствовать ГОСТ 34.311-95. Закрытый и открытый ключ ЭЦП должен соответствовать ГОСТ 34.310-200.

Требования по применению ЭЦП в рамках взаимодействия

Использование ЭЦП между интегрируемыми объектами интеграции при подписании запроса/ответа в рамках взаимодействия;

Использование ЭЦП пользователя объекта интеграции при его участии в формировании запроса/ответа в рамках взаимодействия интегрируемых объектов

интеграции;

Подтверждением авторства сообщений должен быть положительный результат проверки соответствия транспортной подписи регистрационным свидетельством ЭЦП владельца объекта интеграции, направившего сообщение.

Проверка транспортной подписи осуществляется с соблюдением следующих процедур:

- проверка принадлежности ЭЦП НУЦ РК отправителю сообщения;
- проверка действительности ЭЦП НУЦ РК.

Требования к алгоритму формирования ЭЦП

Алгоритм формирования ЭЦП должен соответствовать ГОСТ 34.311-95.

Закрытый и открытый ключ ЭЦП должен соответствовать ГОСТ 34.310-2004.

Требования по информационной безопасности

1. Журнал событий должен вестись в соответствии с требованиями стандарта СТ РК ИСО/МЭК 27002-2015 и со схемой взаимодействия объектов информатизации посредством внешнего шлюза «электронного правительства», утвержденной приказом Вице-министра информации и коммуникаций Республики Казахстан от 23 апреля 2018 года.

ОИ должны обеспечивать возможность взаимодействия с SIEM по протоколу и в формате syslog (RFC 5424). Внешние интерфейсы взаимодействия ОИ/СПП должны быть реализованы посредством технологии WebServices с использованием протокола HTTPS.

1. Следующие события должны подлежать обязательному журналированию: авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;
    - создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;
    - неудавшиеся или отвергнутые действия пользователя;
    - получение пользователем доступа к объектам доступа (в том числе, инициирование запросов к другим ИС);
    - запросы пользователя к другим ИС;
    - Журнал логирования должен быть в текстовом формате, каждое событие должно содержать всю информацию в одной строке.
    - Журнал логирования в обязательном порядке должен содержать следующие поля
    - дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ:СС);
    - наименование источника события (сервис/служба);
    - имя учетной записи/ID пользователя;
    - IP-адрес клиента/пользователя;
    - время начала операции;
    - время окончания операции;
    - уровень события:
        - Alerts - Необходимо срочное вмешательство;
        - Critical - Критические события;
        - Errors - Сообщения об ошибках;
        - Warning - Всевозможные предупреждения;
        - Notifications - Различные важные уведомления;
        - Informational - Информационные сообщения;
        - Debug - для отладки приложений.
    - категория события;

- описание события.

2. Система должна обеспечивать возможность взаимодействия с системами SIEM по протоколу и в формате syslog.
3. Журналы необходимо хранить в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее трех лет, а также быть в оперативном доступе не менее трех месяцев;
4. При журналировании событий необходимо обеспечивать синхронизацию времени с инфраструктурой источника времени;
5. Доступ к журналу информационного обмена должен иметь только пользователь с правами Администратора.

Требования к формату Журнала логирования

- Для событий, фиксируемых в журналах необходимо определять формат записи. Значения полей необходимо разделять символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применять символы-ограничители полей;
- Журналы необходимо хранить в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее трех лет, а также быть в оперативном доступе не менее трех месяцев;
- При журналировании событий необходимо обеспечивать синхронизацию времени сервера с инфраструктурой источника времени.
- Журнал логирования должен быть в текстовом формате, каждое событие должно содержать всю информацию в одной строке. Допускается хранение журналов в формате XML, а также в табличной форме в БД;
- Для журналов должна использоваться кодировка UTF-8;
- В один файл журнала не допускается запись событий, имеющих разные форматы данных;
- В Журнале логирования необходимо использовать пары ключ-значение. Если значение содержит пробелы, их необходимо поместить в кавычки;
- В Журнале логирования необходимо использовать уникальные идентификаторы (ID). Не изменять уникальные идентификаторы (Идентификаторы транзакций, идентификаторы пользователя), и их формат, на всем пути следования транзакции;
- Уровень логирования должен быть расширенным. Необходимо добавлять информацию о входах и выходах пользователя, действия пользователя, транзакции, информацию о времени и так далее;
- В Журналах логирования необходимо использовать категории события, следующие имеющие значения:
  - INFO;
  - WARN;
  - ERROR;
  - DEBUG.

При возникновении исключительной ситуации сервис должен сохранить информацию о ней в журнале событий и сформировать ответ с информацией об ошибочной ситуации.

Доступ к журналу информационного обмена должен иметь только пользователь с правами Администратора.

Требования со стороны ШЭП/ВШЭП

Обмен данными между системами должен соответствовать следующим форматам:

1. Использовать HTTPS;

2. Использовать SOAP протокол (Simple Object Access Protocol) в качестве протокола взаимодействия;
3. В рамках взаимодействия по протоколу SOAP, использовать ЭЦП информационной системы, выданной НУЦ РК, в соответствии спецификации WS-security;
4. Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML).

Интеграция должна соответствовать положениям пп.7) и пп.11) п.139 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

Обеспечить регистрирцую события:

- журналов событий операционных систем;
- журналов событий систем управления базами данных;
- журналов событий антивирусной защиты;
- журналов событий прикладного ПО;
- журналов событий телекоммуникационного оборудования;
- журналов событий систем обнаружения и предотвращения атак;
- журналов событий системы управления контентом.

Классификатор кодов возврата конверта ШЭП/ВШЭП

№	Статус	Описание ошибки
1	SCSS001	Успешная обработка
2	SCSE002	Пояснение ошибки в бизнес-данных
3	SCSE003	Необработанное исключение

Документ подписал:
