Утверждены
Решением Правления
акционерного общества
«Национальный управляющий
холдинг «Байтерек»

Приложение № 125
к протоколу очного
заседания Правления
акционерного общества
«Национальный управляющий
холдинг «Байтерек»
от 09.04 2019 года № 18/19

Единый стандарт
хранения электронных документов акционерного общества
«Национальный управляющий холдинг «Байтерек»

Нур-Султан, 2019

1. Общие положения

1. Настоящий документ описывает стандарт хранения электронных документов (далее - Стандарт), который необходим для автоматизации процесса приема и хранения электронных документов между АО «НУХ «Байтерек» и всеми его Контрагентами, в рамках исполнения Плана мероприятий («Дорожной карты») по реализации Стратегии цифровизации АО «НУХ «Байтерек» (далее - Холдинг) на 2018-2023 годы.

Контрагентами являются все дочерние компании Холдинга и государственные органы, подключенные к Единой системе электронного документооборота государственных органов.

2. Стандарт разработан в соответствии с Законом РК от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» и Правилами электронного документооборота, утвержденными постановлением Правительства РК от 17 апреля 2004 года №430, а также с учетом Правил документирования и управления документацией в АО «НУХ «Байтерек», утвержденными решением Правления Холдинга от 30 сентября 2014 года (протокол №31/14), а также с учетом положений Правил электронного документооборота Холдинга и Политики информационной безопасности Холдинга.

3. Стандарт определяет порядок взаимодействия участников информационного обмена; сведения, подлежащие информационному обмену; порядок, режимы и способы передачи данных.

4. Действие Стандарта не распространяются на электронные документы, содержащие сведения, составляющие государственные секреты РК.

2. Системы информационного обмена

5. Системами информационного обмена являются следующие информационные системы (далее - Системы):

1) Система электронного документооборота Холдинга (далее – Система Холдинга), являющаяся платформой для загрузки и последующего хранения электронных документов;

2) Информационная система Контрагентов (далее – Система Контрагента), производящая интеграцию с Системой с целью дальнейшей загрузки и хранения электронных документов.

3. Порядок информационного обмена

6. Информационный обмен между Системами осуществляется посредством web-сервиса - по загрузке электронных документов.

7. Взаимодействие между Системами производится в синхронном режиме согласно алгоритму выполнения информационного обмена, приведенному в **Приложении 1** к настоящему Стандарту.

8. Информационный обмен осуществляется посредством электронных сообщений, формируемых и передаваемых в XML-формате с использованием Электронной цифровой подписи (далее – ЭЦП), выданных Национальным удостоверяющим центром Республики Казахстан (далее – НУЦ РК) владельцам Систем.

9. При загрузке информации должна поддерживаться передача выходных форм поступившего электронного документа вместе с прикрепленными файлами(PDF, TIFF, JPEG, JPG – графический формат; RTF, DOC, DOCX – текстовый формат; XLS, XLSX – табличный формат; PPT, PPTX – презентации; RAR, ZIP – архивированный формат).

10. Факты получения/отправки электронных документов фиксируются в протоколе информационного обмена на серверах Холдинга. Сервис информационного взаимодействия между Системами записывает в Log-журналах Системы Холдинга факт получения/отправки электронных документов с соответствующим кодом.

11. Фиксация всех временных параметров в процессе обработки сообщений производится по времени города Нур-Султан.

12. Информационный обмен производится с соблюдением технических требований согласно **Приложению 2** к настоящему Стандарту.

4. Среда и способы передачи данных

13. Информационный обмен между Системами осуществляется электронными сообщениями в XML-формате в синхронном режиме. Для передачи данных используется транспортный протокол (TCP), протокол передачи гипертекста (HTTP/HTTPS) с применением регистрационных свидетельств SSL, выданных НУЦ РК, в качестве транспортного протокола, а также стек протоколов и стандартов web-сервисов (REST, SOAP).

14. Виды сообщений, передаваемых между Системами представлены в нижеуказанной таблице 1 настоящего Стандарта.

Таблица 1 – Виды сообщений

Сообщение			**Отправитель**	**Получатель**
№	**Наименование**	**Тип**		
1	2	3	4	5
Виды сообщений при передаче информации				
1.1	Передача данных об электронном документе	Запрос	Система Контрагента	Система Холдинга

Сообщение			Отправитель	Получатель
№	Наименование	Тип		
1	2	3	4	5
1.2	Передача ответа о получении данных об электронном документе	Ответ	Система Холдинга	Система Контрагента

15. Состав сведений, форматы входных и выходных данных, подлежащих информационному обмену между Системами при автоматизации процессов приема и хранения электронных документов, указан в **Приложении 3** к настоящему Стандарту.

16. Перечень общих справочников и классификаторов, используемых в информационном обмене, указан в **Приложении 4** к настоящему Стандарту.

5. Организация защиты данных при обмене

17. Защита информации при информационном обмене должна обеспечиваться за счет подтверждения авторства подписанных XML сообщений (применение ЭЦП), а также за счет мероприятий технического и организационного характера.

18. Организационные мероприятия должны регламентировать доступ персонала Холдинга и уполномоченных лиц Холдинга к серверам, активному сетевому оборудованию, системе электропитания серверов.

19. Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML).

20. При возникновении аварийной ситуации администраторы Систем должны незамедлительно принять меры по устранению последствии и выявления причин аварийной ситуации.

6. Меры по защите информации при информационном взаимодействии

21. Защита информации при информационном взаимодействии со стороны Системы Холдинга должна обеспечиваться за счет мероприятий технического и организационного характера, проводимых Департаментом информационных технологий и Комплаенс службой Холдинга.

22. Защита информации при информационном взаимодействии со стороны Системы Контрагента должна обеспечиваться за счет мероприятий технического и организационного характера проводимых Контрагентами Холдинга.

23. Для хранения закрытых ключей, а также другой конфиденциальной информации, Стороны устанавливают необходимые средства защиты информации.

24. Отправляемые данные должны быть подписаны посредством ЭЦП, сотрудником Холдинга или Контрагента, имеющим право подписи.

25. Принимаются другие предусмотренные меры по защите информации согласно действующим нормативным правовым актам Республики Казахстан.

7. Требования к мониторингу и учету событий

26. Следующие события должны подлежать обязательному учету:

– 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;

– Требования к формату файла;

– Журнал логирования – это файлы, размещенные на сервере Системы Холдинга, содержащие системную информацию работы сервера или компьютера, в которые заносятся действия пользователя или программы.

26.1. 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;

– Время начала операции;

– Время окончания операции;

– Уровень события (определяется Оператором);

– Категория события (определяется Оператором);

– Описание события.

27. Журнал логирования обязан храниться в течение срока, указанного в нормативно-технической документации в сфере обеспечения информационной безопасности, но не менее 3-х (трех) лет, а также быть в оперативном доступе не менее 3-х (трех) месяцев.

8. Блокировка соединения со стороны Системы Холдинга

28. Блокировка соединения со стороны Системы Холдинга осуществляется при следующих условиях:

– Превышение частоты запросов;

– Превышение количества ошибок (по умолчанию 10 попыток на каждой точке подключения);

– Наличие в запросах нарушений информационной безопасности в соответствии стребованиями к информационной безопасности.

9. Заключительные положения

29. Программные и аппаратные средства, используемые при подготовке и проведении обмена сообщениями в рамках информационного взаимодействия между Системами, должны поддерживаться в рабочем состоянии.

30. В случае возникновения в ходе информационного обмена проблемных ситуаций, участники информационного обмена принимают меры для их устранения.

31. В случае возникновения споров, создается специальная комиссия из числа представителей участников информационного обмена.

Приложение № 1
к Единому стандарту
хранения электронных документов
акционерного общества
«Национальный
управляющий холдинг «Байтерек»

Алгоритм выполнения информационного обмена между Системой Холдинга и Системой Контрагента

1. Система Контрагента формирует XML-сообщение с данными запроса по обращению участника процесса государственных закупок.
2. Система Контрагента осуществляет подписание XML-сообщения ЭЦП. (Согласно Закону об электронном документе и электронной цифровой подписи от 7 января 2003 года №370 и Нормативно правовым документациям Национального Удостоверяющего Центра Республики Казахстан расположенных по ссылке: http://www.pki.gov.kz/index.php/ru/dokumentatsiya).
3. Система Контрагента передает посредством веб-сервиса XML-сообщение с данными в Систему.
4. Система осуществляет проверку принадлежности ЭЦП отправителю сообщения и действительности сертификата. Выполнение шага завершается следующим образом:
5. Если проверка не пройдена, выполняется пункт 1.8.
6. Если проверка пройдена, выполняется пункт 1.5.
7. Система начинает процесс загрузки документа.
8. Система обрабатывает сообщение, формирует XML-сообщение ответа-подтверждения приема электронного документа и принятии данных в обработку.
9. Система Контрагента принимает ответ, сохраняет результат обработки запроса – ответ, полученный от Системы в журнале логирования, и изменяет статус обращения, процесс передачи данных заканчивается.
10. Система генерирует и направляет сообщение-ответ об ошибке в Систему Контрагента, сохраняет в журнале логирования результат обработки запроса – ошибка, и изменяет статус обращения, процесс передачи данных заканчивается.

Приложение № 2
к Единому стандарту
хранения электронных документов
акционерного общества
«Национальный
управляющий холдинг «Байтерек»

Технические требования к средствам электронных коммуникаций информационного взаимодействия

1. Средства электронных коммуникаций должны обеспечивать обмен информацией между Системами в электронном виде, в соответствии с принятыми в Соглашении принципами, форматами и протоколами обмена. Средства электронных коммуникаций Систем должны включать:

1.1. Канал передачи данных (выделенный или коммутируемый);

1.2. Коммуникационное оборудование;

1.3. Программную защиту данных при передаче по каналам связи от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий.

2. Обмен данными между Системами должен соответствовать следующим форматам:

2.1. Использовать HTTPS, с применением регистрационных свидетельств SSL, выданных НУЦ РК, в качестве транспортного протокола;

2.2. Использовать REST протокол (Represential State Transfer) в качестве протокола взаимодействия;

2.3. Формат передаваемых данных XML для веб-методов и их параметров;

2.4. Структура подписанного ЭЦП XML-файла должна соответствовать спецификации консорциума W3C «XML - Signature Syntax and Processing» (Синтаксис и обработка подписи XML);

2.5. В рамках взаимодействия по протоколу REST, использовать ЭЦП владельца объекта информатизации, выданной НУЦ РК, в соответствии спецификации WS-security;

3. Требования по использованию ЭЦП: Использование ЭЦП интегрируемыми объектами информации при подписании запроса/ответа в рамках взаимодействия;

3.1. Использование ЭЦП пользователя при его участии в формировании запроса/ответа в рамках взаимодействия интегрируемых объектов информации;

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

4. Требования по проверке ЭЦП:

4.1. 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»;

4.2. 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/.

5. 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).

Приложение № 3
к Единому стандарту
хранения электронных документов
акционерного общества
«Национальный
управляющий холдинг «Байтерек»

Состав сведений, форматы входных и выходных данных, подлежащих информационному обмену между Системами при автоматизации процессов приема и хранения электронных документов

Описание сообщений синхронного канала

Метод отправки сообщений по синхронному каналу (SendMessage).

Запрос на предоставление Сервиса (SendMessageRequest) представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageRequest.

Таблица 1 – Формат сообщения типа SendMessageRequest

Поле	Тип	Обязанность	Описание
request	SyncsendMessagerequest	Да	Запрос
requestInfo	SyncMessageInfo	Да	Информация о сообщении запроса
messageDate	xsd: dateTime	Да	Дата создания сообщения в Системе Отправителя (Инициатора взаимодействия). Заполняется Отправителем (инициатором взаимодействия).
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой Отправителя, т.е. Инициатора взаимодействия)
sessionId	guid	Нет	Идентификатор сессии.
sender	senderinfo	Да	Объект информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Да	Пароль отправителя
properties	property	Нет	Массив свойств, можно добавить дополнительные свойства запроса

			(по согласованию с Системой получателя)
key	xsd: int		Ключ свойства
value	xsd: int		Значение свойства
data	xsd: Anytype	Нет	Данные сообщения (формат определяется системой получателя сообщения)

Ответное сообщение на запрос (SendMessageResponse) представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageResponse.

Таблица 2 – Формат сообщения типа SendMessageResponse

Поле	Тип	Обязанность	Описание
response	SyncsendMessageresponse	Да	Ответ
responseInfo	SyncMessageInfoResponse	Да	Информация об ответе
messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (заполняет система получателя запроса (система отрабатывающая сообщение)
responseDate	xsd: dateTime	Да	Дата ответа в системе получателя запроса (заполняется системой получателя запроса)
sessionId	guid	Нет	Идентификатор сессии.
status	StatusInfo	Да	Объект «Информация о статусе»
code	xsd: int	Да	Код статуса (проставляется системой получателя запроса)
message	xsd: string	Да	Сообщение о статусе
responseData	responsedata	Да	Объект «данные ответа»
data	xsd: Anytype	Нет	Объект данные сообщения (формат определяется системой получателя сообщения)

Сообщение об ошибке (SendMessageFault1_SendMessageFault) представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageFault.

Таблица 3 – Формат сообщения типа SendMessageFault

Поле	Тип	Обязанность	Описание
errorCode	xsd: string	Да	Код ошибки

errorMessage	xsd: string	Да	Сообщение ошибки
errorData	xsd: string	Нет	Дополнительное описание ошибки
errorDate	xsd: dateTime	Нет	Дата ошибки
subError	ErrorInfo	Нет	Дочерняя ошибка
sessionId	Guid	Нет	Идентификатор сессии в которой произошла ошибка

Приложение № 4
к Единому стандарту
хранения электронных документов
акционерного общества
«Национальный
управляющий холдинг «Байтерек»

Перечень общих справочников и классификаторов, используемых в информационном обмене

Состав полей информационного обмена в процессе загрузки электронного документа
Отправитель: Система Контрагента
Получатель: Система

Таблица 1 – Формат сообщения при отправке запроса на загрузку электронного документа

№	Наименование объекта	Тип поля	Обязательность	Доп. условие для обязательности	Назначение
1	metadataSystem	MetadataSystem	да		Системные поля
2	attachments	Attachment[]	да		Вложения
3	correspondent	Long	да		Идентификатор Контрагента
4	Exec_BIN	String	да		БИН организации Контрагента
5	Exec_organizationname	String	да		Наименование организации Контрагента
6	description	String	да		Краткое содержание
7	deliveryDate	Calendar	да		Дата и время отправки

В таблице 2 представлена StateDelivered – отметка о доставке сообщения в Систему Холдинга из Системы Контрагента.

Таблица 2 – StateDelivered – отметка о доставке

№	Наименование объекта	Тип поля	Обязательность	Доп. условие для обязательности	Назначение
1	metadataSystem	MetadataSystem	да		Системные поля
2	attachments	Attachment[]	нет		Вложения
3	date	Calendar	да		Дата и время доставки