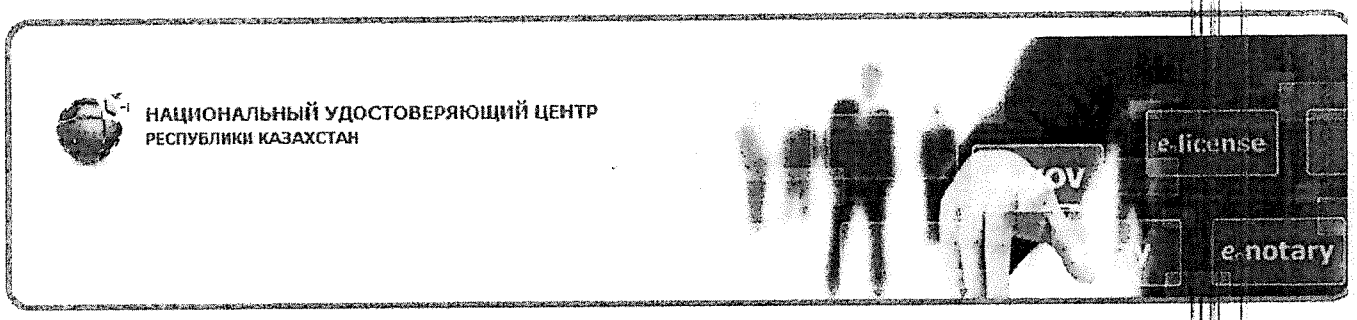
УТВЕРЖДАЮ

Директор
РГП «Государственная техническая служба»
Комитета связи, информатизации и информации
Министерства по инвестициям и развитию
Республики Казахстан

_____ Е. Есмамбетов

«_____ 2015 г.

Руководство для информационных систем при взаимодействии с Национальным удостоверяющим центром Республики Казахстан



СОГЛАСОВАНО

Заместитель директора
РГП «Государственная техническая служба»
Комитета связи, информатизации
и информации
Министерства по инвестициям и развитию
Республики Казахстан

_____ Б. Темирбаев

«_10_» _сентября_ 2015 г.

СОГЛАСОВАНО

Первый заместитель директора
РГП «Государственная техническая служба»
Комитета связи, информатизации
и информации
Министерства по инвестициям и развитию
Республики Казахстан

_____ А. Жүнісбек

«_10_» _сентября_ 2015 г.

г. Астана, 2015

1. Общие положения

1. Настоящее Руководство определяет порядок информационного взаимодействия государственных и негосударственных информационных систем с Национальным удостоверяющим центром Республики Казахстан.

2. В настоящем Руководстве используются следующие основные понятия:

1) список отозванных регистрационных свидетельств (далее – СОРС) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования);

2) удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

3) регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом;

4) электронная цифровая подпись (далее – ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

5) средство криптографической защиты информации (далее - СКЗИ) – средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами.

2. Порядок информационного взаимодействия информационных систем с Национальным удостоверяющим центром Республики Казахстан

3. Для начала работ по организации и обеспечению информационного взаимодействия с НУЦ РК владельцу информационной системы или его законному представителю необходимо получить комплект разработчика, который содержит библиотеки, тестовые регистрационные свидетельства и документацию.

4. Для получения комплекта разработчика необходимо направить на адрес электронной почты info@pki.gov.kz проект письма и акт приема-передачи для проверки корректности заполненных данных в соответствии с установленной формой согласно приложению 1 и 2 к настоящему Руководству.

5. В случае успешной проверки корректности заполненных данных уполномоченными работниками РГП «ГТС» владельцу информационной системы или его законному представителю необходимо направить официальное письмо и подписанный акт приема-передачи в двух экземплярах согласно приложению 1 и 2 к настоящему Руководству.

6. НУЦ РК в рамках взаимодействия с информационными системами предоставляет комплект разработчика согласно пункта 5, оказывает консультацию касательно официальных версий СКЗИ НУЦ РК, предоставленных в комплекте разработчика.

7. Комплект разработчика содержит последнюю версию СКЗИ НУЦ РК с поддержкой текущих регистрационных свидетельств НУЦ РК, примеры использования нового СКЗИ НУЦ РК, библиотеки и тестовые регистрационные свидетельства, а также документацию по его использованию.

В соответствии с подпунктом 3) пунктом 1 статьи 10 Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи» ЭЦП используется в соответствии со сведениями, указанными в регистрационном свидетельстве.

8. При вводе в эксплуатацию государственных информационных систем, необходимо в обязательном порядке, согласно действующему законодательству Республики Казахстан, провести испытания программных продуктов, программных кодов и экспертизу нормативно-технической документации государственных информационных систем в испытательной лаборатории и принятым на территории Республики Казахстан стандартам.

9. При условии положительного результата испытаний программных продуктов, программных кодов и экспертизы нормативно-технической документации государственных информационных систем в испытательной лаборатории и принятым на территории Республики Казахстан стандартам государственной информационной системе необходимо пройти аттестацию на ее соответствие требованиям информационной безопасности согласно Правилам проведения аттестации государственных информационных систем и негосударственных информационных систем, интегрируемых с государственными информационными системами, на соответствие их требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам, утвержденных постановлением Правительства Республики Казахстан от 30 декабря 2009 года № 2280.

10. Владельцам негосударственных информационных систем рекомендуется провести испытания программных продуктов, программных кодов и экспертизу нормативно-технической документации своих информационных систем в испытательной лаборатории, аккредитованной на проведение испытательных работ в информационных системах, расположенной на территории Республики Казахстан по принятым на территории Республики Казахстан стандартам.

11. Информационной системе необходимо проверять регистрационные свидетельства подписывающей стороны согласно Правилам проверки электронной цифровой подписи и регистрационного свидетельства

пользователей Национального удостоверяющего центра Республики Казахстан для информационных систем (http://pki.gov.kz/index.php/ru/dokumentatsiya) и путем выполнения следующих проверок с использованием СКЗИ удостоверяющего центра:

1) проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельсва удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

2) проверка срока действия регистрационного свидетельства. Проверка сроков действия от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

3) проверка регистрационного свидетельства на отозванность (аннулирование). Проверка регистрационного свидетельства на отозванность (аннулирование) осуществляется одним из методов:

на основе СОРС НУЦ РК и дополнительного СОРС НУЦ РК. Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент начала срока действия СОРС НУЦ РК и дополнительного СОРС НУЦ РК.

онлайн проверка регистрационного свидетельства на аннулирование, основанная на протоколе OCSP (On-line Certificate Status Protocol). Данный метод проверки подтверждает, аннулировано ли проверяемое регистрационное свидетельство на момент формирования квитанции OCSP;

4) проверка области использования ключа. Проверка заключается в проверке значения поля регистрационного свидетельства «использование ключа» (KeyUsage). Если поле «использование ключа» содержит значения «Цифровая подпись» и «Неотрекаемость», то это регистрационное свидетельство используется для ЭЦП. А если поле «использование ключа» содержит значения «Цифровая подпись» и «Шифрование ключей», то это регистрационное свидетельство используется для аутентификации;

5) проверка номера политики регистрационного свидетельства и разрешенных способах его использования. Если политика проверяемого регистрационного свидетельства предусматривает ограничение его использования (только в одной системе), то данное регистрационное свидетельство и соответствующий закрытый ключ не использоваться в других системах;

6) проверка метки времени. Доказательством подписания документа в указанный момент времени является квитанция метки времени, полученная в удостоверяющем центре и содержащая дату на которую существовал документ. Данная проверка производится для электронных документов долговременного хранения и формируется в момент подписания документа;

Метка времени является доказательством наличия существования документа в конкретное время.

7) Проверка полномочий лица подписавшего документ. Механизмы проверки полномочий возлагаются на информационную систему. Проверку полномочий так же можно проверить, в случае наличии информации об этом в регистрационном свидетельстве.

Если выясняется, что ЭЦП или регистрационное свидетельство не соответствует требованиям хотя бы одного из критериев вышеописанных проверок, за исключением проверки метки времени, то ЭЦП или регистрационное свидетельство считается недействительным.

12. Проверка ЭЦП на электронном документе производиться путем использования открытого ключа ЭЦП, который содержится в регистрационном свидетельстве подписывающей стороны. Электронный документ должен содержать регистрационное свидетельство подписывающей стороны.

Проверка ЭЦП осуществляется в обратном порядке, по которому производилось подпись документа по следующей схеме:

1) с помощью открытого ключа ЭЦП отправителя дешифруется хэш сообщения (подпись отправителя);

2) с помощью хэш-функции вычисляется контрольная сумма оригинального сообщения;

производится сверка двух контрольных сумм, если они равны, то подпись считается верной, если не равны, то подпись считается не действительной.

13. Техническая реализация проверки подлинности ЭЦП и регистрационного свидетельства возлагается на информационную систему, путем использования высокоуровневых функций разработки с применением СКЗИ удостоверяющего центра.

14. В случае положительного результата проверки ЭЦП к электронному документу, сам документ признается действительным.

15. В случае отрицательного результата проверки ЭЦП к электронному документу, сам документ признается не действительным.

16. Информация по доступу к боевым и тестовым службам OCSP, TimeStamp, CRL, DeltaCRL и сервису по получению регистрационных свидетельств пользователей на модернизированном программном обеспечении НУЦ РК приведена согласно Приложению 3 к Руководству.

17. Для решения технических вопросов информационного взаимодействия информационных систем с НУЦ РК необходимо обращаться по адресу электронной почты knca@pki.gov.kz, info@pki.gov.kz или по тел. 55-27-70, 55-99-99 (вн. 394).

Приложение 1 к Руководству для информационных систем при взаимодействии с Национальным удостоверяющим центром

Шаблон письма

РГП «Государственная техническая служба» Комитета связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан

«Наименование ГО или организации» для начала работ по организации и обеспечению информационного взаимодействия с Национальным удостоверяющим центром Республики Казахстан просит предоставить комплект разработчика, который содержит библиотеки и тестовые регистрационные свидетельства.

Первый руководитель

«наименование ГО или организации»*

**Письмо направляется от владельца информационной системы или от разработчика информационной системы (по согласованию с владельцем информационной системы)*

Приложение 2 к Руководству для информационных систем при взаимодействии с Национальным удостоверяющим центром

Акт приема передачи

г. Астана _____ 2015 г.

Настоящим актом РГП «Государственная техническая служба» передает, а _____ получает средство интеграции с НУЦ РК и тестовые регистрационные свидетельства необходимые для проведения интеграционных работ.

Наименование организации: _____;

Информационная система: _____;

Владелец информационной системы: _____;

Контактные данные: _____
(Фамилия Имя Отчество)
тел. 77172-_____, сот. +7_____,
mail: _____

Планируемое количество пользователей и их месторасположение: _____, г.Астана, _____

Данное средство интеграции предназначено для использования только на территории Республики Казахстан.

Передал: _____ Получил: _____

_____ _____
МП МП

ЛИСТ СОГЛАСОВАНИЯ

к Руководству для информационных систем при взаимодействии с Национальным удостоверяющим центром Республики Казахстан

№ п.п.	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5
1	Жантайлаков Б.С.	главный специалист		03.09.15г.
2	Калдыбеков А.С.	главный спец.		03.09.15г
3	Сайгулова А.О.	глав спец		03.09.15г.
4	Жаксыбекова А.К.	Начальник сект		03.09.15г.
5.	Сагиев С.В.	гл. спец. прогр.		03.09.15
6	Сулейменов А.К	р-р дел-т		03.09.15г
7.	Бекеев А.И.	гл. спец		08.09.15г
8	Хан Л.Г.	Зам.нач. СД		08.09.15г
9	Корнев Г.В	Зам.дир. ДИБ		01.04.15г.
10	Баянкулов Н.Т.	дир. ДИБ		08.09.15г