

ЗАО «Сигнал-КОМ»

УТВЕРЖДЁН
ШКНР.00054-01 31 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
«NOTARY-PRO 2.8»

Описание применения

ШКНР.00054-01 31 01
Листов 14

2019

АННОТАЦИЯ

Настоящий документ описывает инфраструктуру программно-аппаратного комплекса удостоверяющего центра «Notary-PRO 2.8». Документ содержит общую схему взаимодействия элементов инфраструктуры и описание их функционального назначения.

СОДЕРЖАНИЕ

1. Общие сведения	4
1.1. Список сокращений	4
1.2. Назначение программы	4
2. Функциональная схема.....	6
3. Компоненты ПАК УЦ «Notary-PRO»	7
3.1. Удостоверяющий центр	7
3.1.1. Удостоверяющий центр «Notary-PRO»	7
3.1.2. Серверная служба УЦ «Notary-PRO CA Server»	7
3.1.3. База данных УЦ	8
3.2. Регистрационные центры	8
3.2.1. АРМ оператора регистрационного центра «Notary-PRO RA»	8
3.2.2. Сервер регистрационного центра «Notary-PRO RA Server»	8
3.3. Справочник сертификатов удостоверяющего центра	8
3.3.1. Справочник сертификатов «Notary-DIR»	9
3.3.2. Транспортный модуль «Notary-TM»	9
3.3.3. База данных справочника сертификатов	10
3.4. Веб-интерфейс УЦ	10
3.4.1. Веб-приложение «Notary-PRO Web Pages»	10
3.4.2. Веб-служба «Notary-PRO Web Service»	11
3.4.3. Буферная база данных УЦ	11
3.5. Сервер штампов времени	11
3.6. Сервер онлайн-проверки статуса сертификатов	11
3.7. АРМ для разбора конфликтных ситуаций	11
3.8. Средства создания ключей ЭП и ключей проверки ЭП	12
Литература	13

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Список сокращений

АРМ	-	автоматизированное рабочее место
БД	-	база данных
ПАК	-	программно-аппаратный комплекс
РЦ	-	регистрационный центр
СКЗИ	-	средство криптографической защиты информации
СОС	-	список аннулированных сертификатов
УЦ	-	удостоверяющий центр
ЭП	-	электронная подпись

1.2. Назначение программы

Программно-аппаратный комплекс удостоверяющего центра «Notary-PRO 2.8» (далее - ПАК УЦ «Notary-PRO») предназначен для администрирования систем распределения криптографических ключей в соответствии с Рекомендациями ITU-T X.509 v3 [12] и RFC 5280 [18], а также RFC 4491[26].

ПАК УЦ «Notary-PRO» [1] имеет сертификат соответствия требованиям ФСБ России к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27.12.2011 № 796, требованиям к информационной безопасности удостоверяющих центров, установленным для класса КС2, а также требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

В ПАК УЦ «Notary-PRO» выполнение всех криптографических операций, необходимых для реализации функций удостоверяющего центра, включая создание и проверку электронной подписи (далее - ЭП), а также создание ключей ЭП и ключей проверки ЭП, обеспечивается использованием средств криптографической защиты информации (далее - СКЗИ) «СADB 2.1» (вариант исполнения 2) [23], «Signal-COM JCP 3.1» (вариант исполнения 2) [24], «Крипто-КОМ 3.3» (вариант исполнения 8) [25].

Инфраструктура открытых ключей (Public Key Infrastructure – PKI), создаваемая на основе ПАК УЦ «Notary-PRO», включает:

- удостоверяющий центр (УЦ) (см.п.3.1);
- регистрационные центры (РЦ) (см.п.3.2);
- справочник сертификатов УЦ (см.п.3.3);
- веб-интерфейс УЦ (см.п.3.4);
- сервер штампов времени (см.п. 3.5);
- сервер онлайн-проверки статуса сертификатов (см.п. 3.63.4);
- АРМ для разбора конфликтных ситуаций (см.п.0);
- средства создания ключей ЭП и ключей проверки ЭП (см.п.3.8).

Далее в документе приводится функциональная схема ПАК УЦ «Notary-PRO» (см.п. 2) и описывается функциональное назначение каждого элемента инфраструктуры, а также логика их взаимодействия (см.п.3).

Необходимые требования по обеспечению безопасности при взаимодействии элементов инфраструктуры ПАК УЦ «Notary-PRO» и их размещению приводятся в [10].

2. ФУНКЦИОНАЛЬНАЯ СХЕМА

На рис.1 приводится функциональная схема инфраструктуры открытых ключей, организованной на базе ПАК УЦ «Notary-PRO».

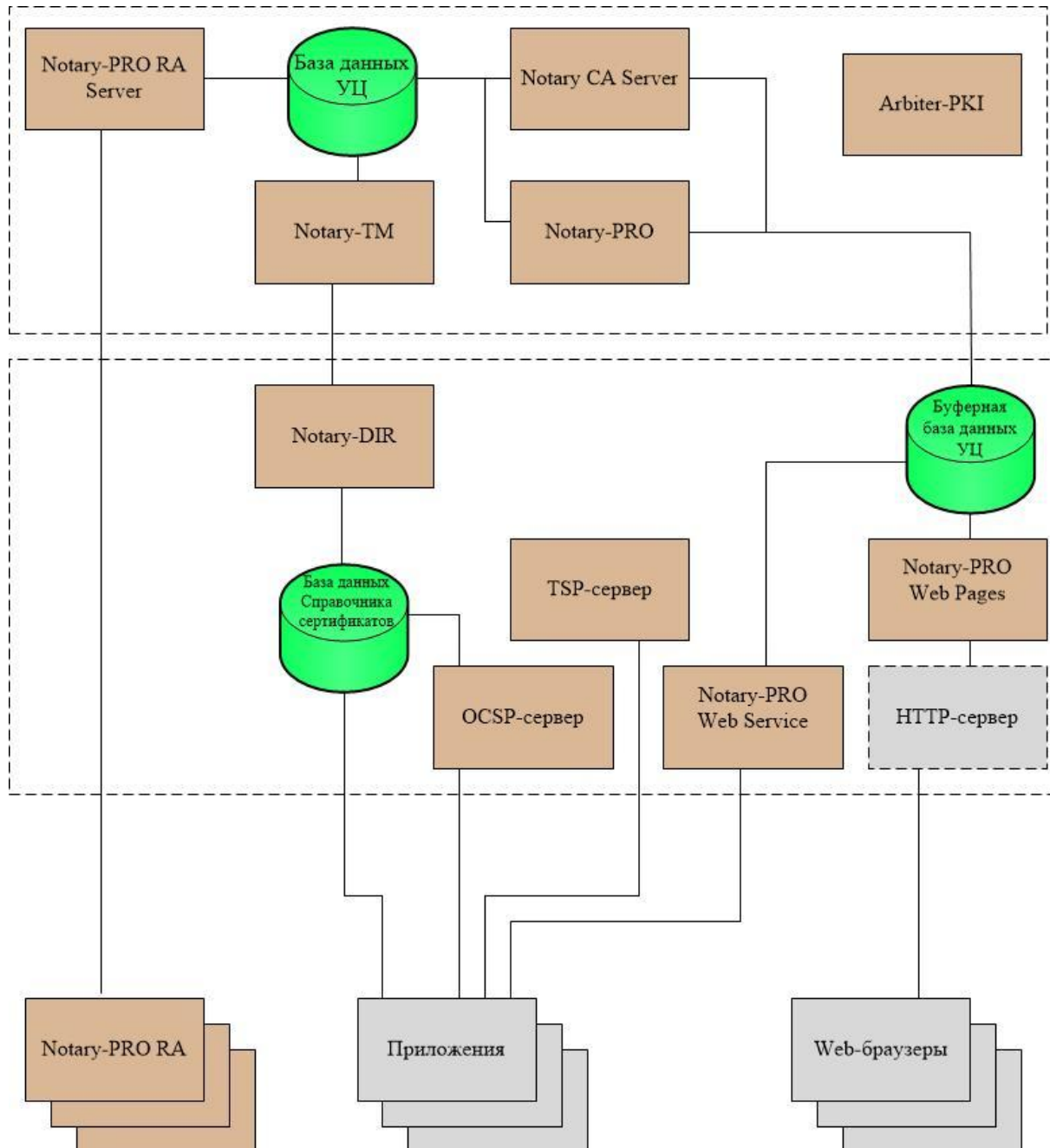


Рис. 1 Функциональная схема ПАК УЦ «Notary-PRO»

3. КОМПОНЕНТЫ ПАК УЦ «NOTARY-PRO»

3.1. Удостоверяющий центр

Удостоверяющий центр имеет модульную структуру и включает в себя следующие компоненты:

- «Notary-PRO» - удостоверяющий центр (см.п.3.1.1);
- «Notary-PRO CA Server» - серверная служба УЦ (см.п.3.1.2);
- база данных УЦ (см.п.3.1.3).

3.1.1. Удостоверяющий центр «Notary-PRO»

УЦ «Notary-PRO» предназначен для:

- создания ключей УЦ;
- регистрации пользователей;
- регистрации запросов на создание сертификатов ключей проверки электронной подписи;
- создания и выдачи сертификатов ключей проверки электронной подписи (далее – сертификаты);
- периодического выпуска списков аннулированных сертификатов ключей проверки электронной подписи (COC).

Подробное руководство по установке, настройке и обслуживанию УЦ «Notary-PRO» содержится в [2].

Внимание! Аккредитованный удостоверяющий центр изготавливает и обслуживает только квалифицированные сертификаты, выдаваемые по форме, утвержденной приказом ФСБ России от 27.12.2011 №795. Изготовление квалифицированных сертификатов обеспечивается настройками УЦ и правилами заполнения полей сертификата, приведенными в Приложении 1 Руководства Администратора УЦ [2].

3.1.2. Серверная служба УЦ «Notary-PRO CA Server»

Серверная служба УЦ «Notary-PRO CA Server» является опциональным компонентом ПАК УЦ «Notary-PRO», предназначенным для автоматизированного создания сертификатов ключей проверки электронной подписи конечных пользователей и периодического выпуска списков аннулированных сертификатов ключей проверки электронной подписи (COC). Серверная служба обеспечивает периодическую обработку запросов на создание сертификатов ключей проверки электронной подписи, которые поступают:

- через файловую систему;
- через веб-приложение УЦ (см.п.3.4.1);
- через веб-службу УЦ (см.п. 3.4.2);
- через регистрационные центры (см.п. 3.2.2).

Подробное руководство по установке, настройке и обслуживанию серверной службы УЦ содержится в [3].

3.1.3. База данных УЦ

Данные удостоверяющего центра хранятся в базе данных (БД) УЦ, в качестве которой могут использоваться:

- MS SQL Server;
- Oracle.

Руководство по установке, настройке и обслуживанию базы данных УЦ «Notary-PRO» содержится в [2].

3.2. Регистрационные центры

Регистрационные центры являются опциональными компонентами ПАК УЦ «Notary-PRO» и предназначены для удаленной регистрации пользователей и запросов на создание сертификатов ключей проверки ЭП.

В инфраструктуру УЦ может быть включено произвольное количество регистрационных центров.

Регистрационные центры не имеют собственной базы данных – все регистрируемые данные хранятся в базе данных УЦ (см.п.3.1.3).

Регистрационные центры включают в себя следующие компоненты:

- «Notary-PRO RA» - АРМ оператора РЦ (см.п.3.2.1);
- «Notary-PRO RA Server» - серверный компонент РЦ (см.п.3.2.2).

3.2.1. АРМ оператора регистрационного центра «Notary-PRO RA»

Автоматизированное рабочее место оператора регистрационного центра «Notary-PRO RA» обеспечивает:

- регистрацию пользователей;
- регистрацию запросов на создание сертификатов ключей проверки электронной подписи;
- регистрации запросов на аннулирование сертификатов ключей проверки ЭП.

Регистрационные центры взаимодействуют с удостоверяющим центром через сервер регистрационного центра (см.п. 3.2.2).

Подробное руководство по установке, настройке и обслуживанию «Notary-PRO RA» содержится в [4].

3.2.2. Сервер регистрационного центра «Notary-PRO RA Server»

Сервер регистрационного центра «Notary-PRO RA Server» предназначен для обеспечения доступа удаленных операторов РЦ к базе данных УЦ. Сервер РЦ может обслуживать несколько АРМ Операторов РЦ.

Взаимодействие между АРМ оператора РЦ и сервером РЦ происходит по защищенному каналу; в качестве механизмов защиты используются электронная подпись и шифрование.

Подробное руководство по установке, настройке и обслуживанию «Notary-PRO RA Server» содержится в [5].

3.3. Справочник сертификатов удостоверяющего центра

Программный комплекс справочника сертификатов удостоверяющего центра «Notary-PRO» включает следующие компоненты:

- «Notary-DIR» - справочник сертификатов на базе сервера LDAP (см.п.3.3.1;

- «Notary-TM» - транспортный модуль, обеспечивающий взаимодействие УЦ со справочником сертификатов (см.п.3.3.2);
- база данных справочника сертификатов (см.п.3.3.3).

3.3.1. Справочник сертификатов «Notary-DIR»

Справочник сертификатов «Notary-DIR» обеспечивает:

- публикацию, организацию свободного доступа и сопровождение актуального хранилища сертификатов ключей проверки ЭП и списков аннулированных сертификатов в формате ITU-T X.509 [12];
- обслуживание заявок на получение доступа к сертификатам ключей проверки ЭП и спискам аннулированных сертификатов по протоколу LDAP [19,20,21,22].

Актуальность информации, содержащейся в справочнике сертификатов, обеспечивает удостоверяющий центр.

Удостоверяющий центр взаимодействует со справочником сертификатов через транспортный модуль «Notary-TM» (см.п.3.3.2), используемый для автоматической публикации сертификатов и СОС в справочнике сертификатов на сервере LDAP.

Использование транспортного модуля для автоматической публикации сертификатов и СОС в справочник сертификатов «Notary-DIR» на сервере LDAP возможно только в случае гарантированной изоляции сервера со справочником от доступа злоумышленников из сетей общего пользования (см. рекомендуемые схемы размещения компонентов ПАК УЦ в Руководстве по безопасности [10]).

В противном случае, а также в случае неисправности транспортного модуля, публикация сертификатов и СОС в справочнике сертификатов должна выполняться вручную администратором УЦ, путем экспорта необходимых файлов сертификатов и СОС из удостоверяющего центра на отчуждаемый носитель и их последующего импорта в справочник сертификатов через консоль сервера LDAP.

Если сервер LDAP со справочником сертификатов не установлен или доступ к справочнику сертификатов по протоколу LDAP по каким-либо причинам невозможен, выгрузка необходимых файлов сертификатов и СОС из базы данных УЦ обеспечивается через консоль администратора УЦ на отчуждаемый носитель или в заданный сетевой каталог с ограниченным доступом (описание экспорта сертификатов и СОС из базы данных УЦ в файловую систему приводится пп.4.6.3 и 4.7.3 Руководства администратора УЦ [2]).

Один справочник сертификатов может обслуживать несколько Удостоверяющих центров.

Подробное описание справочника сертификатов «Notary-DIR» содержится в [6].

3.3.2. Транспортный модуль «Notary-TM»

Транспортный модуль «Notary-TM» предназначен для поддержания взаимодействия удостоверяющего центра «Notary-PRO» (см.п. 3.2.2) со справочником сертификатов «Notary-DIR»: публикуемые сертификаты и СОС удостоверяющий центр экспортирует в транспортный модуль, который затем передает их модулю «Notary-DIR» на сервере LDAP.

Все сообщения, передаваемые транспортным модулем справочнику сертификатов, защищаются протоколом CMS [16]. В качестве механизма защиты используется электронная подпись.

Транспортный модуль «Notary-TM» является опциональным компонентом ПАК УЦ «Notary-PRO» и может использоваться для автоматической публикации

сертификатов и СОС в справочник сертификатов только в случае гарантированной изоляции сервера со справочником от доступа нарушителя из сети общего пользования (см. рекомендуемые схемы размещения компонентов ПАК УЦ в Руководстве по безопасности ПАК УЦ [10]).

Подробное описание установки и настройки транспортного модуля «Notary-TM» содержится в [7].

3.3.3. База данных справочника сертификатов

Справочник сертификатов «Notary-DIR» строится на основе сервера OpenLDAP (<http://www.openldap.org>).

Рекомендации по установке и настройке сервера OpenLDAP содержатся в [6].

3.4. Веб-интерфейс УЦ

Веб-интерфейс удостоверяющего центра предназначен для организации взаимодействия удаленных пользователей с удостоверяющим центром «Notary-PRO» (см.п.3.1.1) и серверной службой «Notary-PRO CA Server» (см.п.3.1.2) по протоколу HTTP.

Веб-интерфейс ПАК УЦ «Notary-PRO» включает в себя следующие компоненты:

- веб-приложение (см.п.3.4.1);
- веб-службу (см.п.3.4.1);
- буферную базу данных УЦ (см.п.3.4.2).

3.4.1. Веб-приложение «Notary-PRO Web Pages»

Веб-приложение «Notary-PRO Web Pages» выполнено в виде набора динамических и статических HTML-страниц.

В качестве HTTP-сервера для «Notary-PRO Web Pages» используется MS Internet Information Server.

Для хранения данных, передаваемых от удаленных пользователей в УЦ и обратно, используется специальная буферная база данных (см.п.3.4.2).

Пользователи могут пополнять базу данных запросами на создание сертификатов ключей проверки ЭП, заходя на соответствующие страницы веб-сервера УЦ.

Удостоверяющий центр и серверная служба периодически опрашивают буферную базу данных и импортируют в БД УЦ поступившие запросы, а в буферную базу данных помещают созданные сертификаты ключей проверки ЭП.

Пользователи могут получить созданные удостоверяющим центром сертификаты ключей проверки ЭП на соответствующих веб-страницах.

«Notary-PRO Web Pages» является опциональным компонентом ПАК УЦ «Notary-PRO» и может использоваться для доставки запросов пользователей в контролируемую зону ПАК УЦ только в случае гарантированной изоляции сервера с буферной базой данных от доступа нарушителя из сетей общего пользования (см. типовые схемы размещения компонентов ПАК УЦ в Руководстве по безопасности [10]).

Подробное описание «Notary-PRO Web Pages» содержится в [8].

3.4.2. Веб-служба «Notary-PRO Web Service»

Веб-служба «Notary-PRO Web Service» выполнена в виде сервиса, предоставляющего программный интерфейс по протоколу SOAP. В качестве HTTP-сервера для «Notary-PRO Web Service» используется Apache.

Функции компонента «Notary-PRO Web Service»:

- предоставление интерфейса конечным пользователям к функциям УЦ по протоколу SOAP.

Следующие функции УЦ доступны через компонент «Notary-PRO Web Service»:

- регистрация запросов на создание сертификатов ключей проверки ЭП по протоколу СМС, полученных от заявителей;
- регистрация запросов на аннулирование сертификатов ключей проверки ЭП по протоколу СМС, полученных от заявителей;
- выдача сертификатов ключей проверки ЭП и списков аннулированных сертификатов ключей проверки ЭП заявителям.

Доступ заявителей к компоненту «Notary-PRO Web Service» должен быть разрешён только из локальной вычислительной сети или по выделенной сети связи.

Подробное описание «Notary-PRO Web Service» содержится в [14].

3.4.3. Буферная база данных УЦ

Для хранения данных, передаваемых от удаленных пользователей в УЦ и обратно, используется специальная база данных, которая может быть развернута на следующих СУБД:

- MS SQL Server;
- MSDE;
- MySQL;
- Oracle.

Руководство по установке и настройке буферной базы данных УЦ содержится в [8].

3.5. Сервер штампов времени

Компонент «TSP Server» ПАК УЦ «Notary-PRO 2.8» предназначен для выдачи по запросу штампов времени в формате RFC 3161.

Подробное описание компонента «TSP Server», а также руководство по его установке и настройке содержатся в [13].

3.6. Сервер онлайн-проверки статуса сертификатов

Компонент «OCSP Server» ПАК УЦ «Notary-PRO 2.8» предназначен для выдачи по запросу информации о текущем статусе сертификатов ключей проверки ЭП согласно RFC 6960.

Подробное описание компонента «OCSP Server», а также руководство по его установке и настройке содержатся в [12].

3.7. АРМ для разбора конфликтных ситуаций

АРМ для разбора конфликтных ситуаций «Arbiter-PKI» является компонентом ПАК УЦ «Notary-PRO», предназначенным для разбора конфликтных ситуаций,

возникающих в связи с применением электронной подписи (ЭП) в автоматизированных защищенных системах, связанных с доказательством авторства электронного документа.

Подробное описание АРМ разбора конфликтных ситуаций «Arbiter-PKI» содержится в [9].

3.8. Средства создания ключей ЭП и ключей проверки ЭП

В инфраструктуре открытых ключей, создаваемой на основе ПАК УЦ «Notary-PRO», создание ключей ЭП, ключей проверки ЭП и запросов на создание сертификатов ключей проверки ЭП конечных пользователей должно выполняться с помощью специализированного программного обеспечения, разработанного с использованием СКЗИ, имеющих сертификат соответствия ФСБ России.

Выбор конкретного ПО для формирования ключей и запросов на сертификаты определяется по согласованию с Удостоверяющим центром и зависит от защищенной прикладной системы, в которой должен использоваться запрашиваемый сертификат ключа проверки ЭП.

ЛИТЕРАТУРА

1. ПАК УЦ «Notary-PRO 2.8». Формуляр. ШКНР.00054-01 30 01. ЗАО «Сигнал-КОМ», 2019.
2. ПАК УЦ «Notary-PRO 2.8». Notary-PRO. Автоматизированное рабочее место администратора удостоверяющего центра. Руководство оператора. ШКНР.00054-01 34 01. ЗАО «Сигнал-КОМ», 2019.
3. ПАК УЦ «Notary-PRO 2.8». Notary-PRO CA Server. Сервер удостоверяющего центра. Руководство системного программиста. ШКНР.00054-01 32 02. ЗАО «Сигнал-КОМ», 2019.
4. ПАК УЦ «Notary-PRO 2.8». Notary-PRO RA. Автоматизированное рабочее место оператора регистрационного центра. Руководство оператора. ШКНР.00054-01 34 02. ЗАО «Сигнал-КОМ», 2019.
5. ПАК УЦ «Notary-PRO 2.8». Notary-PRO RA Server. Сервер регистрационного центра. Руководство системного программиста. ШКНР.00054-01 32 03. ЗАО «Сигнал-КОМ», 2019.
6. ПАК УЦ «Notary-PRO 2.8». Notary-DIR. Справочник сертификатов. Руководство системного программиста. ШКНР.00054-01 32 04. ЗАО «Сигнал-КОМ», 2019.
7. ПАК УЦ «Notary-PRO 2.8». Notary-TM. Транспортный модуль. Руководство системного программиста. ШКНР.00054-01 32 05. ЗАО «Сигнал-КОМ», 2019.
8. ПАК УЦ «Notary-PRO 2.8». Notary-PRO Web Pages. Веб-приложение удостоверяющего центра. Руководство системного программиста. ШКНР.00054-01 32 06. ЗАО «Сигнал-КОМ», 2019.
9. ПАК УЦ «Notary-PRO 2.8». Arbiter-PKI. Автоматизированное рабочее место для разбора конфликтных ситуаций. Руководство оператора. ШКНР.00054-01 34 04. ЗАО «Сигнал-КОМ», 2019.
10. ПАК УЦ «Notary-PRO 2.8». Руководство по безопасности. ШКНР.00054-01 90 03. ЗАО «Сигнал-КОМ», 2019.
11. ПАК УЦ «Notary-PRO 2.8». Типовой регламент. ШКНР.00054-01 90 02. ЗАО «Сигнал-КОМ», 2019.
12. ПАК УЦ «Notary-PRO 2.8». OCSP Server. Сервер онлайн-проверки статуса сертификатов. Руководство системного программиста. ШКНР.00054-01 32 08. ЗАО «Сигнал-КОМ», 2019.
13. ПАК УЦ «Notary-PRO 2.8». TSP Server. Сервер штампов времени. Руководство системного программиста. ШКНР.00054-01 32 09. ЗАО «Сигнал-КОМ», 2019.
14. ПАК УЦ «Notary-PRO 2.8». Notary-PRO Web Service. Веб-служба удостоверяющего центра. Руководство системного программиста. ШКНР.00054-01 32 07. ЗАО «Сигнал-КОМ», 2019.
15. ITU-T Recommendation X.509, «Information Technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks», August 2005.
16. R.Housley, «Cryptographic Message Syntax (CMS)», RFC 3852, July 2004.
17. J.Schaad, M.Myers, «Certificate Management over CMS (CMC)», RFC 5272, June 2008.
18. D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W. Polk, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», RFC 5280, May 2008.
19. K. Zeilenga, «Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map», RFC 4510, June 2006.
20. J. Sermersheim, «Lightweight Directory Access Protocol (LDAP): The Protocol», RFC 4511, June 2006.

21. K. Zeilenga, «Lightweight Directory Access Protocol (LDAP): Directory Information Models», RFC 4512, June 2006.
22. R. Harrison, «Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms», RFC 4513, June 2006.
23. СКЗИ «CADB 2.1». Формуляр. ШКНР.00053-01 30 01, 2019.
24. СКЗИ «Signal-COM JCP 3.1». ШКНР.00049-01 30 01, Сигнал-КОМ, 2019.
25. СКЗИ «Крипто-КОМ 3.3». Формуляр для вариантов исполнения 7, 8. ШКНР.00035-07 30 08, Сигнал-КОМ, 2018.
26. S.Leontiev, D.Shefanovski, «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», RFC 4491, May 2006.