Утверждены первым заместителем директора государственного предприятия «НЦЭУ»

12.01.2023

С изменениями и дополнениями от 30.03.2023, 13.12.2023 (действуют с 18.12.2023)

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ к Единой системе идентификации физических и юридических лиц

1. Общие сведения

Единая система идентификации физических и юридических лиц (далее – ЕС ИФЮЛ) является межведомственной информационной системой, предназначенной для проведения идентификации и аутентификации физических и юридических лиц, в том числе их уполномоченных представителей (далее – пользователи), с применением средств криптографической защиты информации, реализующих функцию выработки электронной цифровой подписи с аппаратными методами защиты личного ключа.

ЕС ИФЮЛ может применяться для организации получения (предоставления) из информационных систем (ресурсов), интегрированных с общегосударственной автоматизированной информационной системой (далее – ОАИС), дополнительных сведений о пользователях с их согласия.

Для взаимодействия с ЕС ИФЮЛ на стороне информационной системы (информационного ресурса) должен быть установлен Комплекс программных средств прикладной системы (далее – КПСИС), на стороне пользователя должна быть установлена Клиентская программа (далее – КП). Для получения сертифицированной копии КП и КПСИС, а также всей необходимой эксплуатационной документации, содержащей в том числе требования к аппаратным характеристикам и программному обеспечению, необходимо пройти регистрацию в облачном хранилище и заполнить соответствующие формы, размещенные по ссылке https://nces.by/service/po/.

ЕС ИФЮЛ располагается на ресурсах аппаратно-программного комплекса динамической доверенной среды (центр обработки данных Предприятия, размещенный по адресу: г. Минск, ул. Раковская, 14), разработанного в рамках мероприятия «Создание аппаратно-

программного комплекса динамической доверенной среды для размещения межведомственных информационных систем, отнесенных к разным классам объектов информатизации» Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы, утвержденной постановлением Совета Министров Республики Беларусь от 23 марта 2016 г. № 235.

Настоящие технические требования определяют перечень применяемых средств криптографической защиты информации, порядок идентификации и аутентификации пользователей, а также иные требования.

2. Описание и состав КПСИС и КП

2.1 Описание и состав КПСИС

КПСИС предназначен для обеспечения возможности предоставления информационным системам (ресурсам) различных государственных органов и иных организаций Республики Беларусь сервиса идентификации/аутентификации посредством ЕС ИФЮЛ.

КПСИС состоит из следующих компонентов:

модуля поддержки OpenID Connect (OIDC);

программного TLS-сервера;

модуля терминала;

сервиса выработки и проверки электронной цифровой подписи (далее – ЭЦП);

сервиса предварительного шифрования;

сервиса генерации псевдослучайной числовой последовательности (ПСЧП);

сервиса контроля целостности;

сервиса генерации личного ключа и выпуска запроса на сертификат открытого ключа (далее – СОК).

Для обеспечения функционирования модуля терминала из состава КПСИС необходим облегченный СОК, изданный в инфраструктуре открытых ключей облегченных сертификатов. Указанный модуль терминала используется для считывания данных из биометрических документов, удостоверяющих личность, а также при подписании данных в терминальном режиме (вне зависимости от интеграции информационной системы (ресурса) с ЕС ИФЮЛ).

При разработке КПСИС использовались следующие языки программирования: C, C++, JavaScript.

Для сборки программы из исходного кода используются:

cmake 3.17.4, cmake 3.17.5;

qmake (из состава Qt 5.15.2);

GNU Make 3.82.

При этом используются следующие основные компиляторы:

clang version 7.0.1, clang version 10.0.1;

gcc 10.2.1.

КПСИС обеспечивает:

быструю интеграцию информационных систем (ресурсов) различных государственных органов и иных организаций Республики Беларусь в Белорусскую интегрированную сервисно-расчетную систему;

защиту передаваемых персональных данных;

выработку/проверку ЭЦП;

организацию защищенного соединения.

2.2 Описание и состав КП

КП предназначена для организации взаимодействия между пользователем, его криптографическим токеном аутентификации (далее - КТА) или средством ЭЦП, КПСИС и ЕС ИФЮЛ.

Основные функции, выполняемые КП:

обеспечение взаимодействия между пользователем, его КТА или средством ЭЦП, КПСИС и сервером идентификации;

установление защищенного соединения с TLS-сервером КПСИС;

обеспечение взаимодействия со следующими программами криптопровайдера: NTCrypto БФИД.10186-01, Avest CSP BIGN РБ.ЮСКИ.12005-02 «AvPKISetup2.exe»;

обеспечение взаимодействия с любым веб-обозревателем для выработки и проверки ЭЦП с использованием средства ЭЦП;

обеспечение взаимодействия с КТА для парольной аутентификации владельца КТА с помощью протокола формирования общего ключа BPACE;

обеспечение взаимодействия с терминалами СИ и КПСИС, обеспечение взаимодействия КТА с терминалами СИ и КПСИС для установления протокола аутентификации BAUTH.

КП представляет собой локальный веб-сервис.

При разработке КП использовались языки программирования C, C++.

Для сборки программы из исходного кода используются:

cmake 3.16.2 (Windows), cmake 3.18.4 (Linux), cmake 3.81 (MacOS);

qmake (из состава Qt 5.15.2).

При этом используются следующие основные компиляторы:

Microsoft Visual C++ Compiler 16.3.29509.3 (Windows);

clang 9.0.0 (Windows), clang 11.0.0 (Linux), clang 12.0.0 (MacOs);

gcc 10.2.1 (Linux).

3. Перечень средств криптографической защиты информации, необходимых для организации взаимодействия информационной системы (ресурса) с ЕС ИФЮЛ, а также для ее использования для проведения идентификации и аутентификации.

В ЕС ИФЮЛ применяются следующие средства криптографической защиты информации:

1) клиентская программа BY.БФИД.10244-01. Сертификат соответствия № BY/112 02.01. NH027 036.01 00 223 от 18 октября 2021 г.;

2) комплекс программных средств прикладной системы BY.БФИД.10246-01. Сертификат соответствия № BY/112 02.01. TP027 036.01 00224 от 18 октября 2021 г.;

3) устройство программно-аппаратное хранения информации «AvPass» (ИЯТА.4675320.005), версия ВПО 6.00. Сертификат соответствия № BY/112 02.01. TP027 036.01 00535 от 3 октября 2022 г.;

4) устройство программно-аппаратное электронной цифровой подписи и шифрования «AvBign», версия ВПО 1.05 (ИЯТА.467532.003). Сертификат соответствия № BY/112 02.01. 036 00814 от 13 августа 2019 г.;

5) средство криптографической защиты информации «Сигма» БФИД.467379.001-01. Сертификат соответствия № BY/112 02.01.036 00266;

6) карта пластиковая идентификационная с интегральной микросхемой (ТУ BY 100093319.012-2020). Сертификат соответствия № BY/112 02.01. TP027 036.01 00164 от 25 августа 2021 г.

4. Порядок идентификации и аутентификации.

В рамках идентификации и аутентификации пользователей с использованием ЕС ИФЮЛ устанавливается соответствие предъявляемого пользователем идентификатора ранее ему присвоенному.

В качестве средств строгой аутентификации и ЭЦП могут применяться идентификационные карты, а также иные средства ЭЦП, распространяемые в рамках Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (ГосСУОК).

Для аутентификации пользователя в информационной системе (ресурсе) средствами КПСИС формируется запрос на аутентификацию, содержащий перечень утверждений (scopes), необходимых информационной системе (ресурсу) для авторизации пользователя. Запрос подписывается, шифруется и направляется в ЕС ИФЮЛ. ЕС ИФЮЛ выполняет протокол аутентификации с пользователем через КП, запрашивает недостающие сведения в информационных системах

(ресурсах) через ОАИС, возвращает в информационную систему (ресурс) данные аутентифицированного пользователя.

В результате аутентификации ЕС ИФЮЛ передает в информационную систему (ресурс) данные о физическом лице (идентификационный номер, фамилию, имя, отчество, место регистрации, атрибутный сертификат с полномочиями пользователя), сертификаты открытых ключей.