Сертификат ключа проверки электронной подписи

Владелец: Организация **ООО "Баба Яга и партнеры"**

Реквизиты ИНН **002145492416** ОГРН 2376272784138

Страна, область, город, улица RU , 76 Ярославская область , Ярославль , ул.Свободы, д.7

Фамилия Имя Отчество **Кощеев Иван Иванович**

СНИЛС 35345453477 E-Mail yaga@localhost.ru

Должность, Подразделение Руководитель , 0

Общее имя ООО "Баба Яга и партнеры"

Издатель: TEST-VALID-CA

Срок действия по UTC с 03.08.15 15:16:00 по 03.08.18 15:26:00

Серийный номер 60 FD E1 F4 00 00 00 00 00 91 Отпечаток C01620431A26070414AE1CA1A3ED8167BEA53AD3

Расширения сертификата X.509

Расширение 2.5.29.37 "Улучшенный ключ":

- Пользователь службы штампов времени (1.2.643.2.2.34.25);
- Пользователь службы актуальных статусов (1.2.643.2.2.34.26);
- Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6);
- Управление финансов Самарской области (1.2.643.2.23.3);
- Участник имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц (1.2.643.2.64.1.1.1);
- Управление финансов Курганской области (1.2.643.3.41.1.3.4);
- Ключ может копироваться (экспортируемый) (1.2.643.3.58.2.1.2);
- Хранение ключа на сервере (1.2.643.3.58.2.1.7);
- Ограниченная лицензия на Крипто-Про CSP (1.2.643.3.58.2.1.9);
- rkn.gov.ru (1.2.643.3.89.24);
- Департамент финансов администрации города Липецка (1.2.643.3.93.15);
- Правительство Калужской области (1.2.643.5.3.40.1);
- Управление финансов Липецкой области (1.2.643.5.3.48.1);
- Размещение сведений в сводном реестре (1.2.643.7.2.21.1.2);
- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4);

Расширение 2.5.29.32 "Политики сертификата": Класс средства ЭП КС1 (1.2.643.100.113.1) ; Класс средства ЭП КС2 (1.2.643.100.113.2) ;

Расширение 1.2.643.100.111 "Средство электронной подписи владельца": "КриптоПро CSP" (версия 3.6)

Расширение 1.2.643.100.112 "Средства электронной подписи и УЦ издателя":

Средство ЭП "КриптоПро CSP" (версия 3.6) Заключение Сертификат соответствия № СФ/121-2272 от 12.12.2013

Средство УЦ "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 Заключение Сертификат соответствия № СФ/128-2352 от 15.04.2014

Расширение 2.5.29.14 "Идентификатор ключа субъекта": 00 BA D3 50 AA 31 AE A7 85 BC 09 A1 45 79 40 4A 0D 5F 20 1C

Ключ проверки ЭП Алгоритм ГОСТ Р 34.10-2001

Значение 1F 7C 69 59 64 22 0B 54 9A 7D 52 EB 9B C6 43 A2 FA 76 0F 5B F4 13 AF FE 29 64 09 47 FB 3A 68 2D 0C 42 58 DD 53 35 FD 8A CC 57 03 8A 14 18 62 73 E9 85 DE 65 29 91 A0 B3 0F 6B EB 83 D6 6A 01 33

Подпись УЦ Алгоритм 1.2.643.2.2.3

Значение 6E B1 5D 71 EB 3E 37 14 9A F8 10 CF E3 4C 73 37 DC 48 61 80 EB 67 35 96 5F 5C D5 89 AB 13 A6 FF 38 BC D9 99 8D 9C 89 04 11 84 7F 57 F9 40 A9 A3 82 EA A7 B8 0A 04 3A BA 7F 89 A8 59 0F 6F 9E B6

Идентификатор заявки 42851715

"___"_____20___г. Сертификат получил(а): _____ /_____/

подпись расшифровка М. П.

Согласие на обработку персональных данных

Я, **Кощеев Иван Иванович**, документ, удостоверяющий личность:

_____

_____

вид документа, № документа, когда и кем выдан

в соответствии с Федеральным законом от 27.07.2006г. № 152ФЗ «О персональных данных» в целях регистрации и обслуживания в информационной системе ООО «Компания «Тензор» своей волей и в своем интересе выражаю согласие ООО «Компания «Тензор», на обработку им с использованием средств автоматизации или без использования таких средств моих персональных данных: фамилия, имя, отчество, реквизиты основного документа, удостоверяющего личность, страховой номер индивидуального лицевого счёта в Пенсионном фонде России (СНИЛС), место работы, должность, служебный телефон и иные сведения. Согласие вступает в силу с момента подписания.

"___"_____20___г. Согласие предоставил(а): _____ /_____/

подпись расшифровка М. П.

ООО «Компания «Тензор»
150001, г. Ярославль
Московский проспект, 12
(4852)262-000
www.tensor.ru

ИНН 7605016030 / КПП 760401001
р/с 40702810502910000075
в «АЛЬФА-БАНК» (ОАО) г. Ярославль
к/с 30101810200000000593
БИК 044525593

ПРАВИЛА

использования средств криптографической защиты информации и электронной подписи

1. Общие положения

Средства криптографической защиты информации (СКЗИ) и электронной подписи (ЭП), входящие в состав комплекта программного комплекса (ПК), предназначены для подписывания файлов с целью подтверждения подлинности информации и ее авторства и шифрования этих файлов при передаче по открытым каналам связи для обеспечения конфиденциальности.

СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Для работы с СКЗИ и средствами ЭП привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Должностные лица, уполномоченные соответствующим приказом руководителя организации, эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП;
- сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

В организации должны быть обеспечены условия хранения ключевых носителей и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

Пользователь несет ответственность за то, чтобы на компьютере, на котором установлены СКЗИ и средства ЭП, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ и средств ЭП.

При обнаружении на рабочем месте, оборудованном СКЗИ и средствами ЭП, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярногоучета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»(Приложение 2).

Не допускается:

а) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б) вставлять ключевой носитель в дисковод ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в дисководы других ПЭВМ;

в) записывать на ключевом носителе постороннюю информацию;

г) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭП;

д) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

3. Действия в случае компрометации ключей

Под компрометацией закрытых ключей понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Пользователь.

При компрометации ключа у Пользователя, он должен немедленно поставить в известность ООО «Компания «Тензор» о факте компрометации. Информация о компрометации может передаваться по телефону или непосредственно представителю Удостоверяющего центра в его офисе. Не позднее 1 часа после поступления сообщения о компрометации ключа, будет заблокирован ключ Пользователя в Системе. Разблокировка будет произведена только после замены скомпрометированных ключей.

Для получения новых ключей уполномоченный представитель организации- пользователя, у которой были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.