Аутентификация пользователя

Электронная цифровая подпись

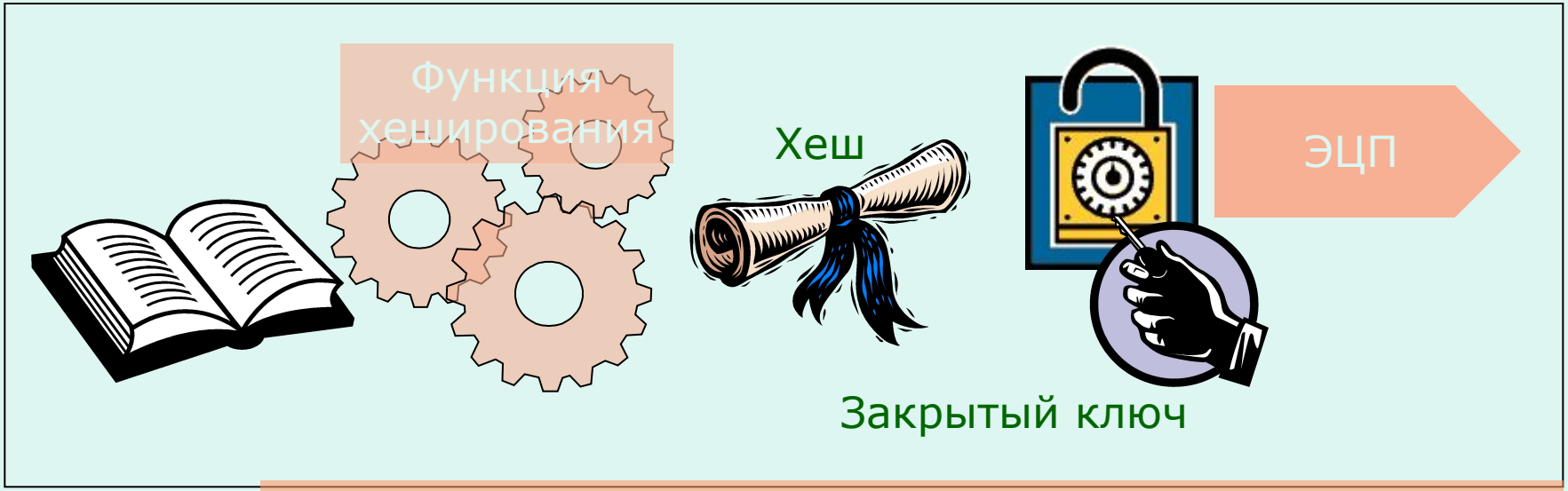
Аутентификация пользователя

Хэш-код создается функцией H:
h = H (M)
Где M является сообщением произвольной длины и h является хэш-кодом фиксированной длины.

Хэш-функция H, которая используется для аутентификации сообщений, должна обладать следующими свойствами:
1. Хэш-функция H должна применяться к блоку данных любой длины.
2. Хэш-функция H создает выход фиксированной длины.
3. H (M) относительно легко (за полиномиальное время) вычисляется для любого значения M.
4. Для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H (M) = h.
5. Для любого данного x вычислительно невозможно найти y такое, что H(y) = H (x).
6. Вычислительно невозможно найти произвольную пару (x, y) такую, что H (y) = H (x).

Электронная цифровая подпись

Цифровая подпись сообщения представляет собой контрольную двоичную последовательность. Она формируется путем специальных преобразований хэш-функции от данных сообщения и секретного ключа отправителя сообщения. Таким образом цифровая подпись, с одной стороны, несет в себе контрольную характеристику (хэш-функцию) содержимого сообщения, а с другой - однозначно указывает на связь содержимого сообщения и владельца секретного ключа. Использование хэш-функции позволяет зафиксировать подмену или модификацию данных сообщения.



Хеш-функции отображают сообщение в имеющее фиксированный размер хеш-значения.

При этом практически невозможно изменить документ так, чтобы он совпал к заданным хеш-значением.

Основой для применения электронных документов, оформляемых при помощи технологии цифровой (электронной) подписи, служат в настоящее время следующие законодательные и нормативные акты государственных органов РФ

Гражданский Кодекс Российской Федерации

Федеральный Закон "Об информации, информатизации и защите информации

Официальные материалы Высшего Арбитражного Суда РФ

Федеральный закон "Об электронной цифровой подписи"

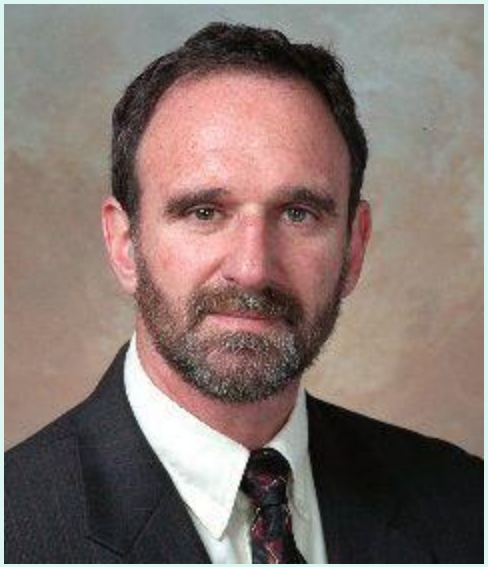
Перечень актов федерального законодательства, подлежащих признанию утратившими силу, приостановлению, изменению, дополнению или принятию в связи с принятием Федерального закона "Об электронной цифровой подписи"

ГОСТ 34.10 – 2012 Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Процессы формирования и проверки электронной цифровой подписи

Цифровая подпись сообщения представляет собой контрольную двоичную последовательность. Она получается путем специальных преобразований хэш-функции от данных сообщения и секретного ключа отправителя сообщения. Таким образом цифровая подпись, с одной стороны, несет в себе контрольную характеристику (хэш-функцию) содержимого сообщения, а с другой - однозначно указывает на связь содержимого сообщения и владельца секретного ключа. Использование хэш-функции позволяет зафиксировать подмену или модификацию данных сообщения. При удовлетворительных результатах проверки цифровой подписи получатель может быть уверен, что полученное сообщение пришло от субъекта, владеющего секретным ключом, и содержательная часть сообщения не подвергалась изменениям. Если цифровая подпись получается в соответствии с официальным государственным стандартом, то она имеет юридическую силу обычной подписи под документом.

Впервые идею цифровой подписи предложили в 1976 году американские специалисты У. Диффи и М. Хеллман. В настоящее время для получения цифровой подписи используются методы, применяемые в шифровании с несимметричными ключами.

Уитфилд Диффи (родился 5 июня 1944, Куинс, Нью-Йорк, США) — один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом.



Мартин Хеллман (род. 2 октября 1945) — американский криптограф. Получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с Уитфилдом Диффи и Ральфом Мерклем (1952г).

Первым по времени изобретения алгоритмом цифровой подписи был разработанный в 1977 году алгоритм RSA. Предложенный в 1984 году алгоритм Т. Эль-Гамаля позволял повысить стойкость подписи при ключе в 64 байта примерно в 1000 раз, но длина самой цифровой подписи увеличивалась в два раза и составляла 128 байт.

Алгоритм Эль-Гамаля послужил основой для разработки национального стандарта США DSA, введенного в 1991 году, и государственного стандарта РФ ГОСТ Р 34.10-94, введенного в действие с 1995 года. В алгоритме DSA удалось сократить длину цифровой подписи до 40 байт при сохранении ее стойкости на прежнем уровне. Дальнейшим развитием стандарта DSA стал стандарт США DSS.

Российский стандарт ГОСТ Р 34.10 схож со стандартом DSS, но предполагает более сложный алгоритм вычисления хэш-функции. Стандартом ГОСТ Р 34.10 определен следующий алгоритм вычисления цифровой подписи и аутентификации сообщения. Отправитель и получатель сообщения имеют в своем распоряжении некоторые открытые атрибуты создания и проверки цифровой подписи: начальный вектор хэширования *H* и параметры *p, q* и *a*, точка *P<>0* эллиптической кривой *E*, с координатами (x_p,y_p), удовлетворяющая равенству *qP=0*.

Параметры вычисляются в соответствии с процедурой ГОСТ. Отправитель выбирает свой секретный ключ *x* и вычисляет открытый ключ $y = a^x \pmod p$. Открытый ключ y отсылается получателю. Секретный ключ выбирается из интервала $0 < x < 2^{256}$. Число *k* генерируется в процессе получения подписи сообщения, является секретным и должно быть уничтожено после выработки подписи.

Упрощенный алгоритм процедуры выработки подписи согласно ГОСТ 34.10 – 2012 включат следующие шаги.

Для получения цифровой подписи под сообщением $M \in V^*$ необходимо выполнить следующие действия (шаги) по алгоритму I:

Шаг 1 – вычислить хэш–код сообщения $M : \overline{h} = h(M).$ (14)

Шаг 2 – вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$, и определить

$$e \equiv \alpha \pmod{q}. \quad (15)$$

Если $e = 0$, то определить $e = 1$.

Шаг 3 – сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству

$$0 < k < q. \quad (16)$$

Шаг 4 – вычислить точку эллиптической кривой $C = kP$ и определить

$$r \equiv x_c \pmod{q}, \quad (17)$$

где x_c – x-координата точки C.

Если $r = 0$, то вернуться к шагу 3.

Шаг 5 – вычислить значение

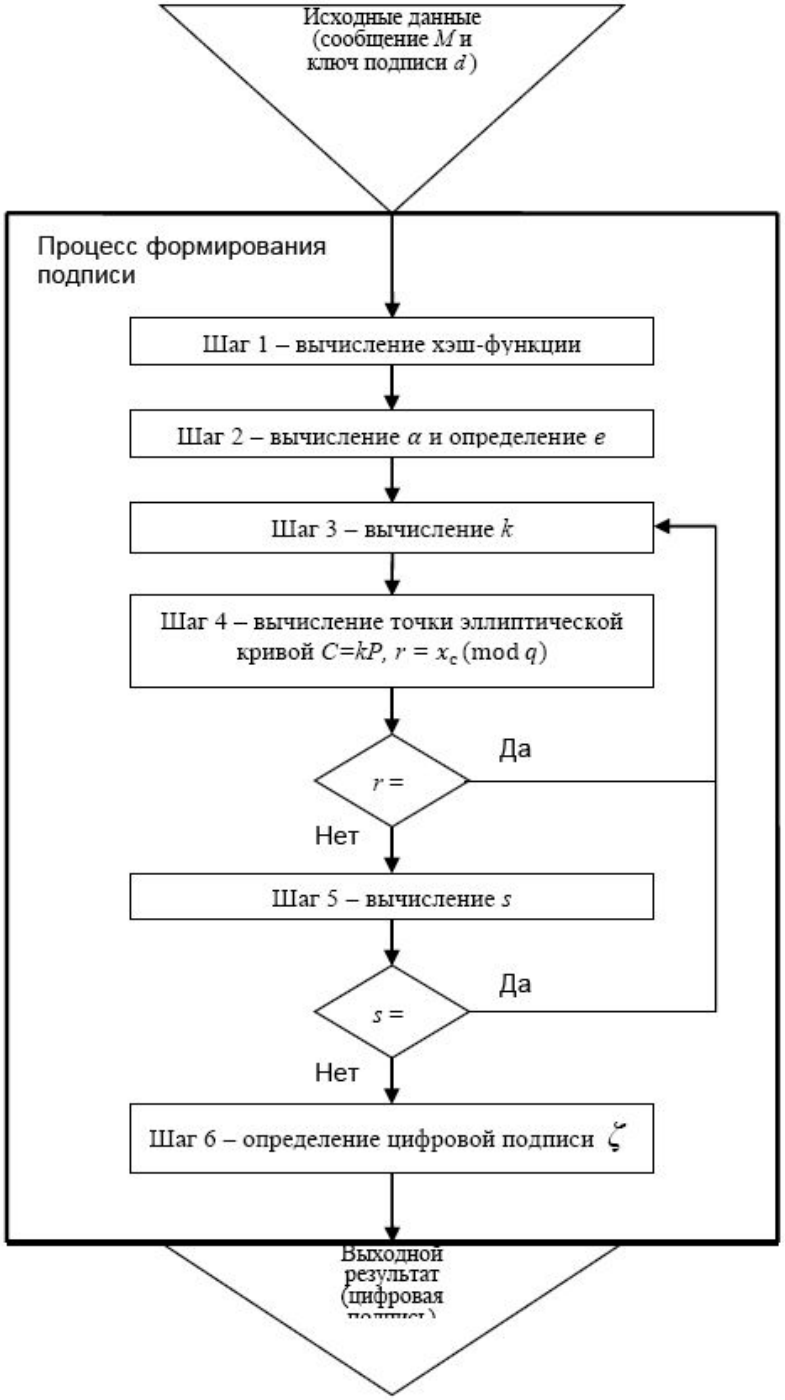
$$s \equiv (rd + ke)(\mathrm{mod}\, q). \qquad (18)$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6 – вычислить двоичные векторы $\overline{r}$ и $\overline{s}$, соответствующие r и s, и определить цифровую подпись $\zeta = (\overline{r} \parallel \overline{s})$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M, а выходным результатом – цифровая подпись ζ.

Схема процесса формирования цифровой подписи



Для проверки цифровой подписи ζ под полученным сообщением M необходимо выполнить следующие действия (шаги) по алгоритму II:

Шаг 1 – по полученной подписи ζ вычислить целые числа r и s. Если выполнены неравенства $0 < r < q,\ \ 0 < s < q,$ то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 – вычислить хэш–код полученного сообщения M

$$\overline{h} = h(M). \tag{19}$$

Шаг 3 – вычислить целое число α, двоичным представлением которого является вектор $\overline{h}$ и определить

$$e \equiv \alpha \pmod{q}. \tag{20}$$

Если $e = 0$, то определить $e = 1$.

Шаг 4 – вычислить значение $v \equiv e^{-1} \pmod{q}.$ (21)

Шаг 5 – вычислить значения

$$z_1 \equiv sv \pmod{q},\ \ z_2 \equiv -rv \pmod{q}. \tag{22}$$

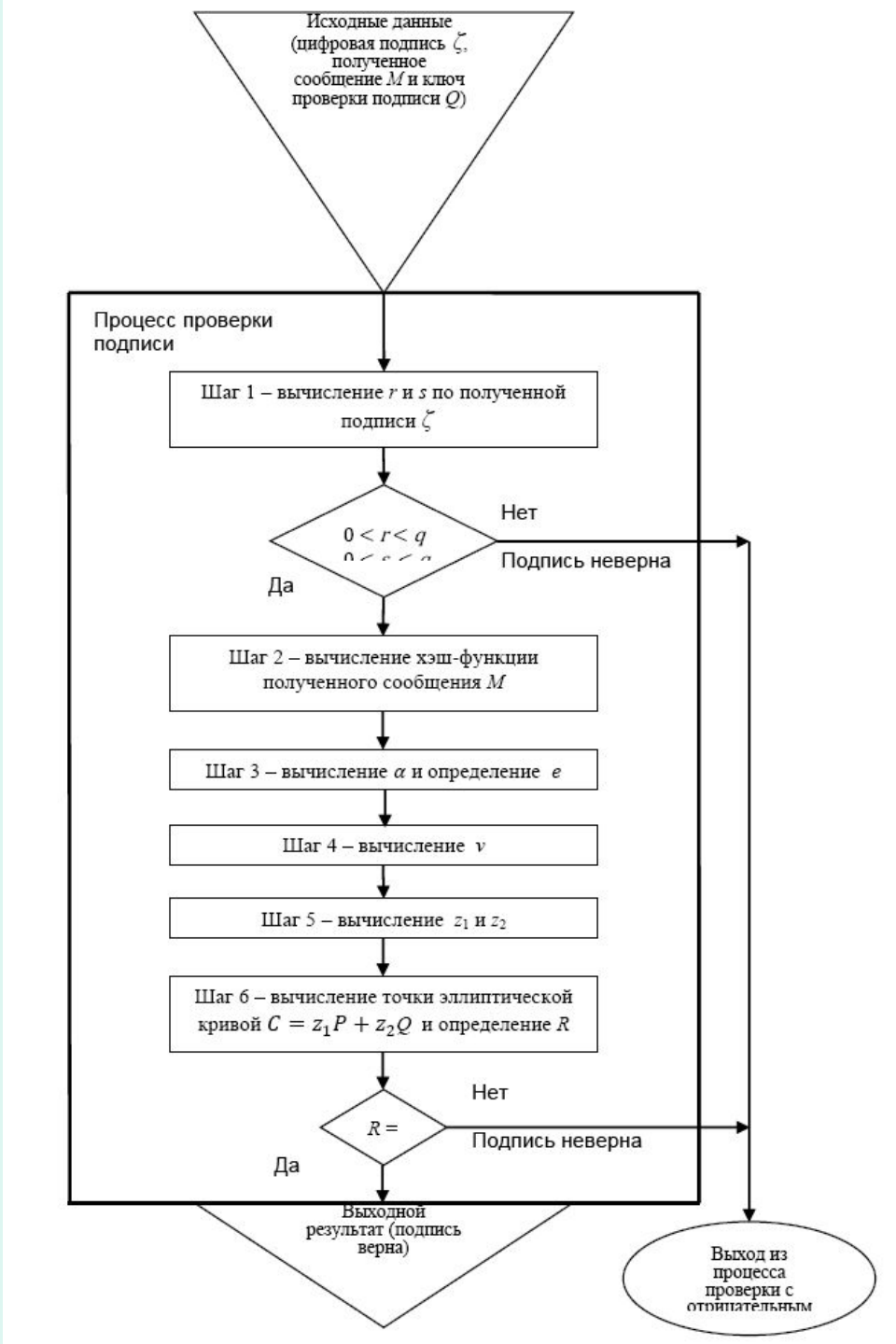
Шаг 6 – вычислить точку эллиптической кривой $C = z_1 P + z_2 Q$ и определить

$$R \equiv x_c (\mathrm{mod}\, q), \tag{23}$$

где x_c – x–координата точки C.

Шаг 7 – если выполнено равенство $R = r$, то подпись принимается, в противном случае - подпись неверна.

Схема процесса проверки цифровой подписи



Если условие выполнено, то получатель считает, что полученное сообщение подписано отправителем, от которого был получен ключ y. Кроме того, получатель считает, что в процессе передачи целостность сообщения не нарушена. В противном случае подпись считается недействительной и сообщение отвергается.

Имея открытые атрибуты цифровой подписи и тексты открытых сообщений, определить секретный ключ *x* можно только путем полного перебора. Причем при длине цифровой подписи 40 байт стандарт DSA гарантирует число комбинаций ключа 10^{21}. Для получения ключа перебором потребуется 30 лет непрерывной работы 1000 компьютеров производительностью 1 млрд. операций в секунду.

Условия использования ЭЦП

1) Средства создания подписи признаются надежными;

2) Сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены;

3) Предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам;

4) Соблюдаются правовые нормы, содержащие требования к письменной форме документа;

5) Сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства;

6) Обеспечивается охрана персональной информации.

Условия использования ЭЦП

Владельцем сертификата ключа подписи (обладателем ЭЦП) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП одписывать электронные документы.

Владелец сертификата ключа подписи обязан (статья 12):

1) Хранить в тайне закрытый ключ ЭЦП;

2) Не использовать для ЭЦП открытые и закрытые ключи ЭЦП, если ему известно, что эти ключи используются или использовались ранее;

3) Немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа ЭЦП нарушена.

Условия использования ЭЦП

Сертификат ключа подписи должен содержать:

1) Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

2) Фамилия, имя, отчество владельца сертификата ключа подписи или псевдоним владельца;

3) Открытый ключ ЭЦП;

4) Наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

5) Сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

Условия использования ЭЦП

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ

(Росинформтехнологии)

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

СЕРТИФИКАТ

КЛЮЧА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Сведения о сертификате:
Кому выдан:
Мифтахутдинов Руслан Вадимович
Кем выдан:
УЦ ОГИЦ ВУ_1
Действителен с 1 ноября 2010 г. 13:52:00 UTC по 1 ноября 2011 г. 13:53:00 UTC
Версия: 3 (0x2)
Серийный номер: 7498 6166 0000 0000 05DC
Издатель сертификата: CN = УЦ ОГИЦ ВУ_1, OU = УГУ, O = Росинформтехнологии, L = Москва, C = RU, E = uc2_1@nii.voskhod.ru
Срок действия:
Действителен с: 1 ноября 2010 г. 13:52:00 UTC
Действителен по: 1 ноября 2011 г. 13:53:00 UTC
Владелец сертификата: T = Ведущий специалист 3 разряда, CN = Мифтахутдинов Руслан Вадимович, O = ФСФР России, C = RU, E = rmiftahutdinov@fcsm.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 4010 9878 9282 0A19 435E 59A1 7118 9217 2B9C 2E92 C17B FB1B A03B A177 D7C7 0EAD EB8D 8F6F 9FC3 3D41 B576 5408 C328 9CCB 648D AEEB C257 4303 AF9B 4B89 D5B3 5C1B
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME
Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Доступ к системе обмена электронными документами ФСФР (1.2.643.5.1.31.1.1) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Система обмена электронными документами ФСФР (1.2.643.5.1.31.1)
4. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: bd e4 64 8c ec 67 7e 09 7d 80 8d 2f e0 3c 47 80 43 1f 6f f7
5. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=65 57 77 60 e1 5b ea 59 00 7a 32 6f 16 f5 4e 0d 05 0b 25 29
6. Расширение 1.3.6.1.4.1.311.21.10
Название: Политики применения
Значение: [1]Политика сертификата приложения: Идентификатор политики=Доступ к системе обмена электронными документами ФСФР [2]Политика сертификата приложения: Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент [3]Политика сертификата приложения: Идентификатор политики=Проверка подлинности клиента [4]Политика сертификата приложения: Идентификатор политики=Система обмена электронными документами ФСФР
7. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://uc.ogic.ru/CDP/UC_OGIC_VU_1.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cdp1.ogic.ru/CDP/UC_OGIC_VU_1.crl
8. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя:
URL=http://uc.ogic.ru/CERTS/UC_OGIC_VU_1.cer
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Значение: 04DA 824D 2E77 5003 C7ED 2CCF D0CB 5F72 9755 769E 1EDE 0C54 2BC1 C97D CB32 505A C21E 663F 1E2D 3A02 801F EEB4 A003 BC09 76F1 3058 871C 91F4 D064 B99A 2455 02AE
Средство ЭЦП:
Крипто Про CSP 3.0

Подпись уполномоченного лица:
М.А. Игнатьева
"2" 11 2010 г.

Подпись владельца сертификата:
Мифтахутдинов Р.В.
"23" ноября 2010 г.

Подпись руководителя удостоверяющего центра:
А.В. Лапшин
"2" 11 2010 г.

Условия использования ЭЦП

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его (статья 14 Федерального закона):

1) По истечении срока его действия;

2) При утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

3) В случае если удостоверяющему центру стало известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

4) По заявлению в письменной форме владельца сертификата ключа подписи;

5) В иных установленных нормативными правовыми актами или соглашением сторон случаях.