ОКС 35.040 П85

Изменение № 1 O‘z DSt 1092:2009 **Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи**

Утверждено и введено в действие постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 04.07.2014 № 05-556

Дата введения 14.07.2014

Срок действия государственного стандарта продлить до 15.10.2019 г.

Раздел 2

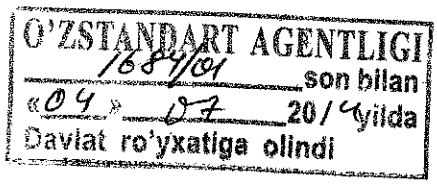
В обозначении государственного стандарта O‘z DSt 1109 год утверждения «2006» заменить на «2013».

Пункт 4.4

В последнем абзаце исключить библиографическую ссылку [1].

Библиография

Исключить.



Изменение № 1 O‘z DSt 1092:2009

Вр.и.о. директора
ГУП «UNICON.UZ» Х. Хасанов

Начальник
научно-исследовательского отдела
криптографии О. Ахмедова

Младший научный сотрудник
научно-исследовательского отдела
криптографии Д. Джаматова

Нормоконтроль Л. Шаймарданова
06.05.2014

СОГЛАСОВАНО

Начальник отдела
информационной безопасности
Государственного комитета связи,
информатизации и информационных
технологий Республики Узбекистан

А.Гафуров
письмо от 25.03.2014 г.
№ 14-8/1679

СОГЛАСОВАНО

Службой национальной
безопасности Республики Узбекистан

письмо от 24.06.2014 г.
№ 39/2199

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процессы формирования и проверки электронной цифровой подписи

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации
Ташкент

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований «UNICON.UZ» - (ГУП «UNICON.UZ») Узбекского агентства связи и информатизации

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 28.09.09 № 05-163

3 В настоящем стандарте реализованы нормы законов Республики Узбекистан «Об электронной цифровой подписи» и «Об электронном документообороте»

4 ВЗАМЕН O‘z DSt 1092:2005

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения. 1
2 Нормативные ссылки. 1
3 Термины, определения и обозначения. 2
3.1 Термины и определения. 2
3.2 Обозначения. 2
4 Общие положения. 3
5 Математические соглашения. 4
5.1 Математические определения. 4
5.2 Параметры алгоритмов электронной цифровой подписи. 6
6 Алгоритм 1. Основные процессы. 8
6.1 Вводные замечания. 8
6.2 Формирование электронной цифровой подписи и сеансового ключа. 8
6.3 Подтверждение подлинности электронной цифровой подписи 9
7 Алгоритм 2. Основные процессы 10
7.1 Вводные замечания. 10
7.2 Формирование электронной цифровой подписи 10
7.3 Подтверждение подлинности электронной цифровой подписи. 11
Приложение А (справочное) Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму 1..... 12
Приложение В (справочное) Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму 2 16
Библиография 19

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
MUASSASASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси
АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ
Электрон рақамли имзони шакллантириш ва текшириш жараёнлари

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процессы формирования и проверки электронной цифровой подписи

Information technology
CRYPTOGRAPHIC DATA SECURITY
Signature and verification processes of (electronic) digital signature

Дата введения 15.10.2009
15.10.2014

1 Область применения

Настоящий стандарт определяет алгоритм электронной цифровой подписи (АЭЦП) для формирования и подтверждения подлинности электронной цифровой подписи (ЭЦП) под заданным сообщением (электронным документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования.

Стандарт предназначен для использования в системах обработки информации различного назначения при формировании и подтверждении подлинности электронной цифровой подписи.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt 1047:2003 Информационные технологии. Термины и определения

O‘z DSt 1109:2006 Информационная технология. Криптографическая защита информации. Термины и определения

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным)

Издание официальное

O'ZSTANDART AGENTLIGI
1684 son bilan
«28» 09 2009 yilda
Davlat ro'yxatiga olindi

стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящем стандарте применяются термины по O‘z DSt 1047, O‘z DSt 1109, а также следующие термины с соответствующими определениями:

3.1.1 **аппаратный модуль** (hardware module): Модуль, составленный, прежде всего, из аппаратных средств, которые могут также содержать некоторое программное обеспечение. Аппаратный модуль включает средства генерации личного ключа владельца и снабжен механизмами защиты от извлечения информации о личном ключе владельца.

3.1.2 **гибридный модуль** (hybrid module): Модуль, криптографические функциональные возможности которого, прежде всего, обеспечиваются программным обеспечением, которое также включает некоторые специализированные аппаратные средства в пределах криптографической границы модуля.

3.1.3 **особый аппаратный модуль** (specific hardware module): Модуль, состоящий, в основном, из аппаратной части, которая содержит секретный блок с встроенным особым личным ключом уполномоченного субъекта.

3.1.4 **особый личный ключ** (specific private key): Криптографический ключ, однозначно связанный с уполномоченным субъектом и не являющийся открытым, используемый в асимметричных и симметричных криптографических алгоритмах (например, тройка параметров (R, g, κ_h), где: R – параметр степени, g – основание, κ_h – ключ хэширования).

3.1.5 **проблема параметра степени** (problem of power parameter): Если в группе с параметром $(F_p; ®)$ заданы элементы g и y носителя группы F_p, найти параметр R и показатель степени x; где $y \equiv g^{[x]} \pmod p$ представляет собой x-ю степень g с параметром R по модулю p, где p – простое число, $R < p$.

3.1.6 **программный модуль** (software module): Модуль, который состоит исключительно из программного обеспечения.

3.2 Обозначения

В настоящем стандарте использованы следующие обозначения:

M – сообщение пользователя, представленное двоичным кодом, произвольной конечной длины;

p – простое число, $p > 3$;

q – простое число;

R – натуральное число - параметр;

(x, u) – пара целых чисел – закрытый ключ ЭЦП;

(y, z) – пара целых чисел – открытый ключ ЭЦП;

g – натуральное число - основание;

(r, s) – пара целых чисел – электронная цифровая подпись под сообщением M;

(R_1, y_1) – пара целых чисел – ключ обнаружения подделки ЭЦП, представляющая собой пару из контрольного и сеансового открытого ключа;

(R, g, κ_h) – особый личный ключ уполномоченного субъекта;

κ_h – ключ хэширования;

® – символ операции умножения чисел с параметром R по модулю;

$|^e$ – символ операции возведения в степень e с параметром по модулю;

$|^{-1}$ – символ операции обращения с параметром по модулю;

$^{-1}$ – символ операции обращения по модулю;

"+" – символ операции сложения в группе точек эллиптической кривой;

$[k]$ – символ k-кратного выполнения операции сложения в группе точек эллиптической кривой;

F_p – конечное простое поле, представляемое как множество из p целых чисел $\{0,1,\ldots, p-1\}$;

$b \pmod p$ – минимальное неотрицательное число, сравнимое с b по модулю p;

a, b – коэффициенты эллиптической кривой;

w – порядок группы точек эллиптической кривой;

t – порядок подгруппы группы точек эллиптической кривой;

0 – нулевая точка эллиптической кривой;

N – точка эллиптической кривой порядка t;

d – целое число, закрытый ключ ЭЦП;

T – точка эллиптической кривой, открытый ключ ЭЦП;

ЦР – центр регистрации;

ОК – открытый ключ.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

4 Общие положения

4.1 Общепризнанная схема (модель) электронной цифровой подписи охватывает три процесса:

- генерация ключей ЭЦП;
- формирование ЭЦП;
- проверка (подтверждение подлинности) ЭЦП.

4.2 При получении сообщения, получатель может осуществить проверку целостности передачи и подлинность отправителя средствами в рамках АЭЦП.

4.3 ЭЦП является электронным аналогом письменной подписи и поэтому ЭЦП может использоваться получателем или третьей стороной для удостоверения, что сообщение было действительно подписано отправителем. ЭЦП может также формироваться для сохранения данных и программ, чтобы в любое время можно было проверить целостность данных и программ.

4.4 Настоящий стандарт описывает два алгоритма (Алгоритм 1, Алгоритм 2) для формирования и подтверждения подлинности ЭЦП. Алгоритм 1 используется в двух базовых режимах:

- без сеансового ключа;
- с сеансовым ключом.

Алгоритм 2 [1] используется в классическом (без сеансового ключа) режиме. В алгоритме 1 предусмотрен резервный путь обнаружения подделки ЭЦП путем введения в процесс формирования ЭЦП процедуры сеансового ключа, используемого в процессе подтверждения подлинности ЭЦП.

4.5 Стойкость криптографического модуля, установленная в настоящем стандарте по алгоритму 1, в программном, гибридном и аппаратном типах реализации АЭЦП по отношению к несанкционированным пользователям основывается на сложности проблемы параметра степени. Это исключает возможность постановки задачи дискретного логарифмирования для подделки электронной цифровой подписи.

4.6 Установленный в настоящем стандарте алгоритм 2 должен быть реализован с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции. Криптографическая стойкость данного АЭЦП основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции.

4.7 При изложении алгоритма 2 не определен процесс генерации параметров АЭЦП. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы электронной цифровой подписи, исходя из требований к аппаратным и аппаратно-программным средствам.

5 Математические соглашения

5.1 Математические определения

5.1.1 Для определения алгоритмов электронной цифровой подписи необходимо описать базовые математические объекты, используемые в процессе формирования и подтверждения подлинности ЭЦП. В данном

разделе установлены основные математические определения и требования, накладываемые на объекты алгоритмов электронной цифровой подписи.

5.1.2 В алгоритме 1 используется ***односторонняя функция*** в группе с параметром, вычисления по которой осуществляются легко на том же уровне трудоемкости, что и в операциях возведения в степень, а инвертирование (обращение) функции требует не меньших вычислительных затрат и времени, чем в процессе решения проблемы дискретного логарифма. Главные операции умножения, возведения в степень и обращения в группе с параметром названы умножением, возведением в степень и обращением с параметром. Односторонняя функция возведения в степень является частным случаем данной односторонней функции.

5.1.3 Операция возведения основания X в степень e с параметром R по модулю p обозначается в виде: $X^{\backslash e}\ (\mathrm{mod}\ p)$. Например, для $e = 37$ с параметром R имеем:

$$X^{\backslash 37} \Rightarrow X^{\backslash 32+4+1}\ (\mathrm{mod}\ p) \equiv ((((X^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR\ (X^{\backslash 2})^{\backslash 2}) \circledR\ X\ (\mathrm{mod}\ p),$$

где: $X^{\backslash 2}\ (\mathrm{mod}\ p) \equiv X\ (2 + XR)\ (\mathrm{mod}\ p)$;

операция умножения с параметром R по модулю p, определяется:

$$X \circledR Y\ (\mathrm{mod}\ p) \equiv X + (1 + X R)\ Y\ (\mathrm{mod}\ p). \qquad (1)$$

Операция обращения переменной X с параметром R по модулю p, обозначается в виде: $X^{\backslash -1}$ и определяется :

$$X^{\backslash -1} \equiv -X(1 + X R)^{-1}\ (\mathrm{mod}\ p). \qquad (2)$$

5.1.4 Пусть задано простое число $p > 3$. Тогда эллиптической кривой E, определенной над конечным простым полем F_p, называется множество пар чисел (x, y), $x, y \in F_p$, удовлетворяющих тождеству:

$$y^2 \equiv x^3 + ax + b\ (\mathrm{mod}\ p), \qquad (3)$$

где: $a, b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю p.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству:

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2}(\mathrm{mod}\ p). \qquad (4)$$

Коэффициенты a, b эллиптической кривой E, по известному инварианту, определяются следующим образом:

$$\begin{cases} a \equiv 3k(\mathrm{mod}\ p) \\ b \equiv 2k(\mathrm{mod}\ p), \end{cases} \qquad (5)$$

где: $\kappa = \dfrac{\mathrm{J(E)}}{1728 - \mathrm{J(E)}}(\mathrm{mod}\ p)$, $J(E) \neq 0$ или 1728.

Пары (x, y), удовлетворяющие тождеству (3), называются точками эллиптической кривой E, x и y – соответственно являются x и y координатами точки.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Точки эллиптической кривой будем обозначать $T(x, y)$ или просто T. Две точки эллиптической кривой равны, если равны их соответствующие x и y координаты.

На множестве всех точек эллиптической кривой E введем операцию сложения, которую будем обозначать знаком “+”. Для двух произвольных точек $T_1(x_1, y_1)$ и $T_2(x_2, y_2)$ эллиптической кривой E рассмотрим несколько вариантов.

Пусть координаты точек T_1 и T_2 удовлетворяют условию $x_1 \neq x_2$. В этом случае их суммой будем называть точку $T_3(x_3, y_3)$, координаты которой определяются сравнениями:

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod}\, p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p), \end{cases} \qquad (6)$$

где: $\lambda \equiv \dfrac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, p)$.

Если выполнены равенства $x_1 = x_2$ и $y_1 = y_2 \neq 0$, то определяются координаты точки T_3 следующим образом:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\mathrm{mod}\, p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p), \end{cases} \qquad (7)$$

где: $\lambda \equiv \dfrac{3x_1^2 + a}{2y_1} (\mathrm{mod}\, p)$.

В случае, когда выполнено условие $x_1 = x_2$ и $y_1 = -y_2 \pmod p$ сумму точек T_1 и T_2 будем называть нулевой точкой 0, не определяя ее x и y координаты. В этом случае точка T_2 называется отрицанием точки T_1. Для нулевой точки 0 выполнены равенства $T\text{“+”}0 = 0\text{“+”}T = T$,

где: T – произвольная точка эллиптической кривой E.

Относительно введенной операции сложения множество всех точек эллиптической кривой E, вместе с нулевой точкой, образуют конечную абелевую (коммутативную) группу порядка w, для которой выполнено неравенство:

$$p + 1 - 2\sqrt{p} \leq w \leq p + 1 + 2\sqrt{p}\,. \qquad (8)$$

Точка T называется точкой кратности k, или просто кратной точкой эллиптической кривой E, если для некоторой точки N выполнено равенство

$$T = \underbrace{N\text{"+"}\ldots\text{"+"}N}_{k} = [k]N\,. \qquad (9)$$

5.2 Параметры алгоритмов электронной цифровой подписи

5.2.1 Алгоритм 1 использует следующие параметры:

а) p – модуль, простое число. Верхняя граница данного числа должна определяться при конкретной реализации алгоритма электронной цифровой подписи в зависимости от типа криптографического модуля:

$p > 2^{1023}$ для программного, гибридного и аппаратного типов и $p > 2^{255}$ для особого аппаратного типа;

b) q – простое число, являющееся фактором (простым множителем) $p-1$, где $2^{254} < q < 2^{256}$;

c) R – параметр - натуральное число, удовлетворяющее условию $R < q$; R может быть открытым, совместным закрытым ключом для ограниченной группы пользователей или составляющей особого личного ключа уполномоченного субъекта;

d) $m = H(M)$ – хэш-функция, отображающая сообщение M в строку длины 256 bit; в программном, гибридном и аппаратном типах криптографического модуля используется бесключевая хэш-функция, а в особом аппаратном типе - ключевая хэш-функция.

5.2.2 Каждый пользователь алгоритма 1 должен обладать личными ключами:

a) (x, u) – парой целых чисел – закрытым ключом ЭЦП,

где: x, u – закрытые ключи, случайно или псевдослучайно генерированные целые числа, удовлетворяющие условию $1 < x$, $u < q$;

b) g – закрытый или открытый параметр, представляющий собой целое число, вычисляемый: $g \equiv h^{(p-1)/q} \pmod{p}$,

где: $h < p$ – натуральное число, удовлетворяющее условию $g^{\omega} \pmod{p} \equiv 0$, в диапазоне значений ω от $1 \div q$ тогда и только тогда, когда $\omega = q$;

c) (y, z) – парой целых чисел – открытым ключом ЭЦП,

где: y, z – открытые ключи, вычисляемые по формуле $y \equiv g^{x} \pmod{p}$ и $z \equiv g^{u} \pmod{p}$; если используется открытый параметр (основание) g, тогда $u=1$ и $z=g$;

d) (R_1, y_1) – парой целых чисел – ключом обнаружения подделки ЭЦП (только в режиме с сеансовым ключом),

где: R_1 – контрольный ключ (открытый или закрытый), выбираемый из диапазона $1 \div q-1$; если R_1 закрытый, тогда R_1 должен быть совместным секретным ключом для подписывающего лица и проверяющей стороны;

y_1 – сеансовый (открытый) ключ, вычисляемый для каждой электронной цифровой подписи как результат возведения в степень с параметром.

Простые числа p, q являются открытыми и могут быть общими для группы пользователей.

5.2.3 Алгоритм 2 использует следующие параметры:

a) простое число p – модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$. Верхняя граница данного числа должна определяться при конкретной реализации ЭЦП;

b) эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;

d) целое число w - порядок группы точек эллиптической кривой E;

O'ZBEKISTON STANDARTLASHTIRISH, MUVOFIQLASHTIRISH VA DAVLAT NAZORATI BOSHQARMASI

e) простое число t - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} w = lt, l \in Z, l \geq 1 \\ 2^{254} < t < 2^{256} \end{cases} \quad (10)$$

f) точка $N \neq 0$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $[t]N=0$;

g) хэш-функция $m=H(M)$, отображающая сообщение M, в строку длины 256 bit.

На приведенные выше параметры АЭЦП накладываются следующие требования:

- должно быть выполнено условие $p^i \neq 1 \pmod t$ для всех целых $i=1,2\ldots, B$, где B удовлетворяет неравенству $B \geq 31$;
- должно быть выполнено неравенство $w \neq p$;
- инвариант кривой должен удовлетворять условию $J(E) \neq 0$ или 1728.

5.2.4 Каждый пользователь алгоритма 2 должен обладать личными ключами:

a) закрытым ключом ЭЦП – целым числом d, удовлетворяющим неравенству $0<d<t$;

b) открытым ключом ЭЦП – точкой эллиптической кривой T с координатами (x_t, y_t), удовлетворяющей равенству $[d]N=T$.

6 Алгоритм 1. Основные процессы

6.1 Вводные замечания

В данном разделе определены процессы формирования электронной цифровой подписи и сеансового ключа под сообщением пользователя и подтверждения подлинности.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры алгоритма электронной цифровой подписи, перечисленные в 5.2.1.

Кроме того, каждый пользователь должен иметь закрытый ключ ЭЦП (x, u), параметр g, открытый ключ ЭЦП (y, z) и ключ обнаружения подделки ЭЦП (R_1, y_1), удовлетворяющие требованиям 5.2.2.

6.2 Формирование электронной цифровой подписи и сеансового ключа

Для создания электронной цифровой подписи и сеансового ключа под сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму 1.1:**

Шаг 1: вычислить хэш-функцию сообщения: $m = H(M)$ и принять $c=x$;

Шаг 2: вычислить $k=H(m+(1+mR)c)$. Если $k=0$, тогда принять $c=c+2$ и вернуться к шагу 2;

Шаг 3: вычислить $T \equiv g^{\lfloor k} \pmod p$ с параметром R;

Шаг 4: вычислить $r \equiv m + (1+mR)T \pmod p$. Если $r \pmod q = 0$, тогда принять $k \equiv k+1 \pmod p$ и вернуться к шагу 3;

Шаг 5: вычислить $s_1 \equiv k - rx \pmod q$. Если $s_1=0$, тогда принять $k \equiv k+1 \pmod p$ и вернуться к шагу 3;

Шаг 6: вычислить $s \equiv s_1 u^{-1} \pmod q$. Если $\mu = 0$, тогда выдать на выход r, s и прекратить вычисления;

Шаг 7: вычислить $r_1 \equiv R_1 + (1+RR_1)r \pmod q$. Если $r_1 = 0$, тогда принять $k \equiv k+1 \pmod p$ и вернуться к шагу 3;

Шаг 8: вычислить $x_1 \equiv (k - suR_1)r_1^{-1} \pmod q$. Если $x_1=0$, тогда принять $k \equiv k+1 \pmod p$ и вернуться к шагу 3;

Шаг 9: вычислить $y_1 \equiv (gR_1^{-1})^{\lfloor x1} \pmod p$ с параметром RR_1 и выдать на выход r, s, y_1.

Исходными (входными) данными этого процесса являются режим $\mu \in \{1, 0\}$, сообщение M, закрытый ключ ЭЦП (x, u), параметр g, контрольный ключ R_1, модуль p, число q. Выходным результатом в режиме $\mu=1$ является тройка (s, r, y_1) и k (в случае использования протокола, свойственного данному стандарту), а в режиме $\mu=0$ являются s, r. Для режима с сеансовым ключом $\mu=1$, а для режима без сеансового ключа - $\mu=0$.

Далее подписанное сообщение (сообщение и дополнение) передается приёмной стороне. Также, передается приемной стороне и сеансовый ключ, если используется режим с сеансовым ключом.

В обоих режимах, как правило, применяются общепринятые протоколы обмена сообщениями, используемые в инфраструктурах открытых ключей (PKI). В режиме с сеансовым ключом стандартом допускается использование свойственного настоящему стандарту протокола.

6.3 Подтверждение подлинности электронной цифровой подписи

Для подтверждения подлинности ЭЦП под полученным сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму 1.2**:

Шаг 1: вычислить хэш-функцию $m = H(M)$;

Шаг 2:если $L(s) <= L(q)$ AND $L(r) <= L(p)$, тогда перейти к следующему шагу, в противном случае принимается «подпись не подлинна»;

Шаг 3: вычислить $z_0 \equiv z^{\lfloor s} \pmod p$ с параметром R;

Шаг 4: вычислить $r' \equiv r \pmod q$;

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Шаг 5: вычислить $y_2 \equiv y^{|r'} \pmod{p}$ с параметром R;

Шаг 6: вычислить $z_1 \equiv z_0 + (1 + z_0 R)\, y_2 \pmod{p}$;

Шаг 7: вычислить $y_3 \equiv z_1 + (1 + z_1 R)\, r \pmod{p}$;

Шаг 8: если $\mu = 0$ и $m = y_3$, осуществляется выдача на выход "подпись подлинна"; если $\mu = 1$ и $m = y_3$, переход к следующему шагу; если $m \neq y_3$, принимается "подпись не подлинна";

Шаг 9: вычислить $g_3 \equiv z_1 R_1^{-1} \pmod{p}$;

Шаг 10: вычислить $s_1 \equiv sR_1 \pmod{q}$;

Шаг 11: вычислить $r_1 \equiv R_1 + (1 + RR_1)\, r' \pmod{q}$;

Шаг 12: вычислить $z_2 \equiv zR_1^{-1} \pmod{p}$;

Шаг 13: принять $y_4 \equiv y_1$;

Шаг 14: вычислить $z_3 \equiv z_2^{|s1} \pmod{p}$ с параметром RR_1;

Шаг 15: вычислить $y_5 \equiv y_4^{|r1} \pmod{p}$ с параметром RR_1;

Шаг 16: вычислить $g_4 \equiv z_3 + (1 + z_3 RR_1) y_5 \pmod{p}$;

Шаг 17: если $g_3 = g_4$, принимается "подпись подлинна", в противном случае принимается "подпись не подлинна".

Исходными (входными) данными этого процесса являются: подписанное сообщение M, электронная цифровая подпись s, r, открытые ключи y, z, контрольный ключ R_1, сеансовый ключ y_1, модуль p, число q, а выходным результатом – информация о подлинности или неподлинности данной ЭЦП. Ключ обнаружения подделки ЭЦП (R_1, y_1) используется только в режиме с сеансовым ключом.

В приложении А приведен контрольный пример для процессов формирования и проверки ЭЦП по алгоритму 1.

7 Алгоритм 2 . Основные процессы

7.1 Вводные замечания

В данном разделе определены процессы формирования и проверки ЭЦП под сообщением пользователя по алгоритму 2.

Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры АЭЦП, приведенные в 5.2.3.

Каждый пользователь должен иметь закрытый ключ ЭЦП d и открытый ключ ЭЦП $T(x_0, y_0)$, удовлетворяющие требования пункта 5.2.4.

7.2 Формирование электронной цифровой подписи

Для получения ЭЦП под сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму 2.1**:

Шаг 1: вычислить хэш-функцию сообщения: $m=H(M)$;

Шаг 2: вычислить $e \equiv m \pmod{t}$. Если $e=0$, то определить $e=1$;

Шаг 3: сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству $0 < k < t$;

Шаг 4: вычислить точку эллиптической кривой $C=[k]N$ и определить $r=x_c \pmod t$, где x_c – x координата точки C. Если $r=0$, то вернуться к шагу 3;

Шаг 5: вычислить значение $s \equiv (rd+ke) \pmod t$. Если $s=0$, то вернуться к шагу 3;

Шаг 6: выдать на выход r и s в качестве ЭЦП.

Исходными (входными) данными этого процесса являются сообщение M и закрытый ключ ЭЦП d, а выходным результатом – электронная цифровая подпись (r, s).

7.3 Подтверждение подлинности электронной цифровой подписи

Для подтверждения подлинности ЭЦП под полученным сообщением M необходимо выполнить следующие действия (шаги) по **алгоритму 2.2**:

Шаг 1: если $0 < r < t$, $0 < s < t$, перейти к следующему шагу, в противном случае принимается «подпись не подлинна»;

Шаг 2: вычислить хэш-функцию сообщения: $m=H(M)$;

Шаг 3: вычислить $e \equiv m \pmod t$. Если $e=0$, то определить $e=1$;

Шаг 4: вычислить значение $v \equiv e^{-1} \pmod t$;

Шаг 5: вычислить значения $z_1 \equiv sv \pmod t$, $z_2 \equiv -rv \pmod t$;

Шаг 6: вычислить точку эллиптической кривой $C=[z_1]N$“+”$[z_2]T$ и определить $R \equiv x_c \pmod t$, где x_c – x координата точки C;

Шаг 7: если выполнено равенство $R=r$, то принимать «подпись подлинна», в противном случае «подпись не подлинна».

Исходными (входными) данными этого процесса являются подписанное сообщение M, электронная цифровая подпись (r, s) и открытый ключ ЭЦП, а выходным результатом – информация о подлинности или неподлинности данной ЭЦП.

В приложении В приведен контрольный пример для процессов формирования и проверки ЭЦП по алгоритму 2.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Приложение А
(справочное)

Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму 1

В приведенном приложении все числа представлены в шестнадцатеричной системе счисления.

Приводимые ниже значения параметров ***p***, ***q***, а также значения закрытого ключа ЭЦП и открытого ключа ЭЦП рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте в режиме без сеансового ключа.

Для формирования и подтверждения подлинности электронной цифровой подписи должны быть использованы нижеследующие числовые значения.

В данном примере параметрам ***p***, ***q*** и ***R*** присвоены следующие значения:

p:
1F84F3905B873C8B305375882F2EF26B346EFD236F20C76070AE1FB02EF7
73CD37DF3AA46463A97FADFE7672D53C6C53897C6D7A2C4255B5AA47
0AA3D0CD50FA5392D064BBFB6D7CEFB765B3266D264E3DF1811C651A
0E344957C154037048E5B24D9B9B67D684573EA08A242699C47A49DF55F
D77B0DA4B449B37806CEDBF23

q:
A071C130A16485B29F52B17B952D1F590D758E62365494053BD0C1E71EE
73011

R:
4868CD715A93C7494D08CC52815319D803C020064556D158DD7847984FC
AD551

Считается, что пользователь обладает закрытым ключом ЭЦП ***(x, u)***, закрытым параметром ***g***, компоненты которого имеют следующие значения:

x:
03BB7BDF9ACFBECCBBF5ADE1249B0B5A36F59E88C146C14FE1FD4B6
919D81E31

u:
01F4CECD0426EAD56109D0FF23A68211C8C241FB18D860C0169DDE2170
60FCE0

g:
17B2927E70164CA06026C34C6A93DB2B6DFA0C90C981867DAE4F88E058
D8DDD5E03FA615F1C667CCDB79641B0E4177499CFBE4393CB0EFC1599
4DD50B70A67DDC8CFA6DD2C9AD3CC844E90A9BE39679DC86EFAAA2

1BF149F48916C4DBC3C8E7334B01C2636617E30A299BA8C4544B6C7DB8
95042CD7A04F7E8D6D20289C83958

Параметрам ***y, z*** присвоены следующие значения:

y:

109A0B84C75440B94869DCCF7958068037378457CDD61F27B637A6C88D2
3BECA20FC8A2045E689392E1F89C2E419C29B8D8C4D7F8D3B69395D8C
C3DD991F1FCB4D902B16660287B8F73CBBCCB7394E10C2BD81E1E4A23
2D980F071158A38FE9336E88E56E74E2C67BFB7D139AAA9A5BE3E4F484
1468E4C1B546696A879E52DE3

z:

05D0A9B8C8343F0C2E157587AA51B1227B840250D0DEFAFB250F5C7FC9
BE4CF2B46C82AB008CADAA87E2C39F833301CFA74A5110BE0E643BAC
A593DAB0F0DB1CA1D0D5B9D3B536A304D158DC4D48F5AA5A1B2B6E7
9D896FD3A918762D103243D6F5DCE88C75E91902F45505D4DBE2085302
D23DF3CE2169324228AB395549496

Процесс формирования электронной цифровой подписи

После выполнения шагов 1-7 по **алгоритму 1.1** были получены следующие числовые значения:

Значение хэш-функции сообщения: $m = H(M)$:

A246751D42FB22CB23F260BB77100C48E664C7438EE13B35B1496057A3D
5DE3E

Значение ***k***:

F498D14EDE9281E0DB9F367955B720EB57853DDC6DE5C4F7ADBE1486B
E6CC1DD

Значение ***T***:

14C90DED6EC16609D183E1D994EAF7932D676E4529A7267E044353438E5
8E0AA36436CAD0913981CFF8C79B7E6BE5ED787D06AE30FB4CAD8A7B
7DE0FCFE09AC79155E7B934011D0BDF9378A1BA168A94BA3CF8C9F927
DF98D3501DBC3C747DACDA91E617968F8DD334B068703636141C1519B
F8117371232AB5553653590AA94

Значение ***r***:

02B78AFE53BB1ACF3BE4B8834441AEC56E4F94D03C529B5B1BDD43A7
DDE7BCB836CD530BD97F2A86F1AE93524A5046F908B131987E8AFFFB7
E655CB72C6EAF4FCE5086C698A38A3334EF919801EF81F7C1AE82248774
374E34A96253B8902318715CD4810A8E863040241E3A831D9F8A9F527EE1
84F8367B35F1E251961C8D12

Проверка: $r \neq 0$ и $r \neq q$!

Значение s_1:

9D2E5BEA377386D12F2AC748C030F2A5AF4035BDFFF86F563BDCAB686
60FBB9D

Проверка: $s_1 \neq 0$!

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

Значение s:
521D61E03F67F32AEC5909F53C789B3E334DD12EB258D5945B5267F0FD0
F1C71

Электронная цифровая подпись

$r =$
02B78AFE53BB1ACF3BE4B8834441AEC56E4F94D03C529B5B1BDD43A7
DDE7BCB836CD530BD97F2A86F1AE93524A5046F908B131987E8AFFFB7
E655CB72C6EAF4FCE5086C698A38A3334EF919801EF81F7C1AE82248774
374E34A96253B8902318715CD4810A8E863040241E3A831D9F8A9F527EE1
84F8367B35F1E251961C8D12

$s =$
521D61E03F67F32AEC5909F53C789B3E334DD12EB258D5945B5267F0FD0
F1C71

Подтверждение подлинности ЭЦП

После выполнения шагов 1-8 по **алгоритму 1.2** были получены следующие числовые значения:

Значение хэш-функции сообщения: $m = H(M)$:
A246751D42FB22CB23F260BB77100C48E664C7438EE13B35B1496057A3D
5DE3E

Значение z_0:
1B304AF32983C97541642BAB19C881DDE63147AC903E6802BCF8613E0E
D96AA76CAA1640C8402A6DFA43D9B1F6CCD23421012B707BCEA2A184
41F45FFB03D1108AC26F06E4C71B710326E539344402069BFB02549B0C6
A8A918105FE573F6D0BD251750B85D3E96AB0C604583368C464E38448A
D2199E89AB362E01AEBEFCFAB

Значение r':
421C4D9475248E64D12EC3AF14170D2498F7A7CCD200397DE81778C86F7
121BA

Значение y_2:
0416829BB6BB8133D86118283850C33B324732FCDFF2DF6FF84931F546A
2309F0CFBC939CFAA3493171B300EE5A7D56F7F500EDA089E14C3CB042
2D0C4B022F6C180E4456CC4F2A7ADCF96C932A33C13B5AC9CE781BF25
FD6E3C348C8BFC9A5226C725B9A90A94A2C4CF22213C8191765C2B12B
B8D6E37A9C7D77785F0B4F8F0

Значение z_1:
0DF553A8C4C124E9594260CFE9AF7FFCD3ADFF73DA13C9060DC6247FA
F3ECC407E6EA0C307AAADA552E97E85FF779EDC1FDC15A3D550202F5
93B04E3B27694E4530A15A1EFE57F38DB4A0A7B8633CF2B10AEB0EF47
BF333112E9F16506A73848784B8D9413A53A373A2BFA1A1CAD2D720A85
FC2EBF5965C277CE5B582F8A0EFA

Значение y_3:
A246751D42FB22CB23F260BB77100C48E664C7438EE13B35B1496057A3D5DE3E

Подпись подлинна!!!

Приложение В
(справочное)

Контрольный пример. Процессы формирования и подтверждения подлинности электронной цифровой подписи по алгоритму 2

Приводимые ниже значения параметров p, a, b, w, t, N, а также значения закрытого ключа ЭЦП d и открытого ключа T рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритма 2, описанный в разделе 7 данного стандарта.

Все числовые значения приведены в шестнадцатеричной системе счисления.

Параметры электронной цифровой подписи

Для формирования и подтверждения подлинности ЭЦП должны быть использованы следующие параметры:

Модуль эллиптической кривой

Параметру p присвоено следующее значение:

$p =$
8000000000000000000000000000000000000000000000000000000000000431

Коэффициенты эллиптической кривой

Параметры a и b принимают следующие значения:

$a = 7$

$b =$
5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514COCE9D AE23B7E

Порядок группы точек эллиптической кривой

Параметр w принимает следующее значение:

$w =$
800000000000000000000000000000150FE8A1892976154C59CFC193ACCF 5B3

Порядок циклической подгруппы группы точек эллиптической кривой

Параметр t принимает следующее значение:

$t =$
800000000000000000000000000000150FE8A1892976154C59CFC193ACCF 5B3

Коэффициенты точки эллиптической кривой

Координаты точки N принимают следующие значения:

$x_n = 2$

$y_n =$
8E2A8A0E65147D4BD6316030E16Dl9C85C97F0A9CA267122B96ABBCEA 7EFC8

Закрытый ключ ЭЦП

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI

Считается, что пользователь обладает следующим закрытым ключом ЭЦП d:

$d =$
7A929ADE789BB9BE10ED359DD39A72C11B60961F49397EEE1D19CE9891EC3B28

Открытый ключ ЭЦП

Считается, что пользователь обладает открытым ключом ЭЦП T, координаты которого имеют следующие значения:

$x_t =$
7F2B49E270DB6D90D8595BEC458B50C58585BA1D4E9B788F6689DBD8E56FD80B

$y_t =$
26F1B489D6701DD185C8413A977B3CBBAF64DlC593D26627DFFB101A87FF77DA

Процесс формирования электронной цифровой подписи

Пусть после выполнения шагов 1-3 по **алгоритму 2.1** были получены следующие числовые значения:

$e =$
2DFBC1B372D89A1188C09C52EOEEC61FCE52032AB1022E8E67ECE6672B043EE5

$k =$
77105C9B20BCD3122823C8CF6FCC7B956DE33814E95B7FE64FED924594DCEAB3

При этом кратная точка $C = kN$ имеет координаты:

$x_c =$
41AA28D2F1AB148280CD9ED56FEDA41974053554A42767B83AD043FD39DC0493

$y_c =$
489C375A9941A3049E33B34361DD204172AD98C3E5916DE27695D22A61FAE46E

Параметр $r = x_c (\mathrm{mod}\, t)$ принимает значение:

$r =$
41AA28D2FlAB148280CD9ED56FEDA41974053S54A42767B83AD043FD39DC0493

Параметр $s = (rd + \kappa e) (\mathrm{mod}\ t)$ принимает значение:

$s =$
1456C64BA4642A1653C235A98A60249BCD6D3F746B631DF928014F6C5BF9C40

Процесс подтверждение подлинности ЭЦП

Пусть после выполнения шагов 1-3 по **алгоритму 2.2** было получено следующее числовое значение:

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
METROLOGIYA VA
MILLIY BANK
MUASSASASIDA

$e =$
2DFBC1B372D89A1188C09C52E0EEC61FCE52032AB1022E8E67ECE6672B
043EE5

При этом параметр $v = e^{-1} \pmod{t}$ принимает значение:

$v =$
271A4EE429F84EBC423E388964555BB29D3BA53C7BF945E5FAC8F38170
6354C2

Параметры $z_1 = sv \pmod{t}$ и $z_2 = -rv \pmod{t}$ принимают значения:

$z_1 =$
5358F8FFB38F7C09ABC782A2DF2A3927DA4077D07205F763682F3A76C9
019B4F

$z_2 =$
3221B4FBBF6D101074EC14AFAC2D4F7EFAC4CF9FEC1ED11BAE336D27
D527665

Точка $C = [z_1]N'' + [z_2]T$ имеет координаты:

$x_c =$
41AA28D2F1AB148280CD9ED56FEDA41974053554A42767B83AD043FD3
9DC0493

$y_c =$
489C375A9941A3049E33B34361DD204172AD98C3E5916DE27695D22A61F
AE46E

Тогда параметр $R = x_c \pmod{t}$ принимает значение:

$R =$
41AA28D2F1AB148280CD9ED56FEDA41974053554A42767B83AD043FD3
9DC0493

Поскольку выполнено равенство $R = r$, принимается “подпись подлинна”.

Библиография

[1] ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

УДК: ОКС 35.040 Группа П85

Ключевые слова: электронный документ, электронная цифровая подпись, подписанное сообщение, открытый ключ, закрытый ключ, сеансовый ключ, обработка данных, криптографический алгоритм

Заместитель директора
ГУП «UNICON.UZ» Х. Хасанов

Главный научный сотрудник
ГУП «UNICON.UZ», д.т.н. проф. П. Хасанов

Начальник научно-исследовательского
отдела криптографии к.т.н. О. Ахмедова

Начальник научно-исследовательской
лаборатории криптоанализа А. Давлатов

Нормоконтроль Н. Травина

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH,
MUVOFIQLASHTIRISH
VA DAVLAT NAZORATI
BOSHQARMASI

СОГЛАСОВАНО

Службой национальной
безопасности Республики Узбекистан

Письмо от 27 марта 2009 года
№39/657