Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Криптографические протоколы

Практические задачи

- Обеспечение целостности сообщений
- Аутентификация источника
- Двусторонняя аутентификация
- Индивидуальная ЭЦП
- Групповая ЭЦП
- ЭЦП вслепую
- Неотрицание авторства
- Широковещательная передача
- Забывающая передача
- Доказательство с нулевым разглашением
- Распределение ключей
- Совместная выработка ключа
- Конфиденциальные вычисления
- Разделение секрета

Криптографический протокол

Криптографический протокол – алгоритм, использующий криптографические преобразования, следуя которому, участники решают некоторую задачу.

Одна и та же задача может быть решена с использованием различных криптографических протоколов.

Алгоритм Диффи-Хеллмана по выработке ключа (1976 г.)

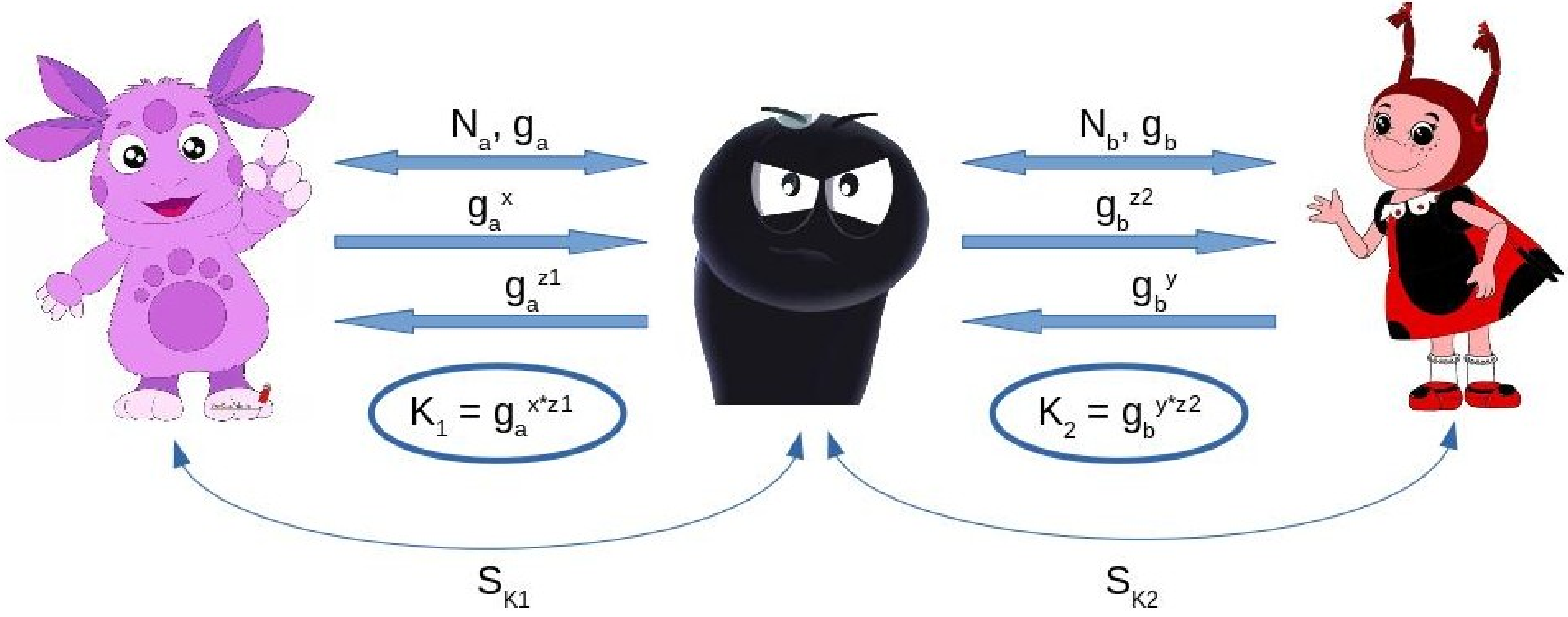
Анна				Борис		
Описание действия	Секретные данные	Открытые данные		Открытые данные	Секретные данные	Описание действия
Совместно выбирают пару чисел		N – простое, g – первообразный корень из N		N, g		
Выбирает число	x - случайное	$x_1 = g^x \bmod N$	$\Rightarrow$	x_1		
		y_1	$\Leftarrow$	$y_1 = g^y \bmod N$	y - случайное	Выбирает число
Вычисляют ключ шифрования	$K = y_1^x \bmod N$ $= g^{xy} \bmod N$				$K = x_1^y \bmod N$ $= g^{xy} \bmod N$	

Мартин
Хеллман

Уитфилд
Диффи

Атака “человек посередине”

В протоколе Диффи-Хелмана ни А, ни В не могут достоверно определить, кем является их собеседник.



Протоколы обмена ключами

Распределение ключей с использованием третьей доверенной стороны.

Мастер-ключ – долговременный ключ абонента, получаемый им от центра распределения ключей.

Ключ сессии – ключ, для шифрования одного сеанса передачи информации.

Протоколы обмена ключами

Обозначения:

A, B – клиенты

KDC – центр распределения ключей

ID_A – id клиента A

ID_B – id клиента B

Ka – мастер-ключ A

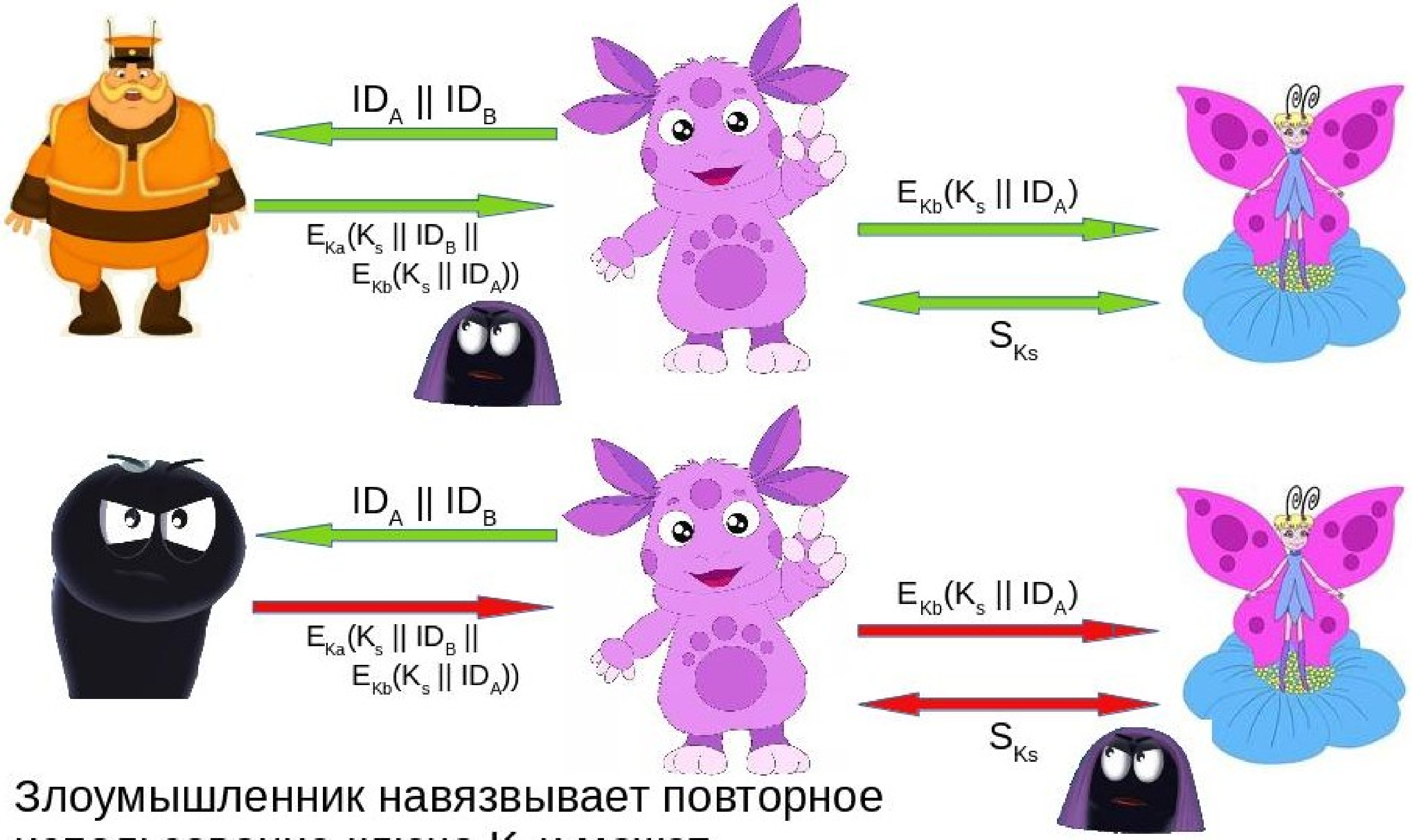
Kb – мастер-ключ B

Ks – ключ сессии

Протокол обмена ключами

$A \Rightarrow KDC$	$ID_A \parallel ID_B$
$KDC \Rightarrow A$	$E_{Ka}(K_s \parallel ID_B \parallel E_{Kb}(K_s \parallel ID_A))$
$A \Rightarrow B$	$E_{Kb}(K_s \parallel ID_A)$

Атака повторного воспроизведения

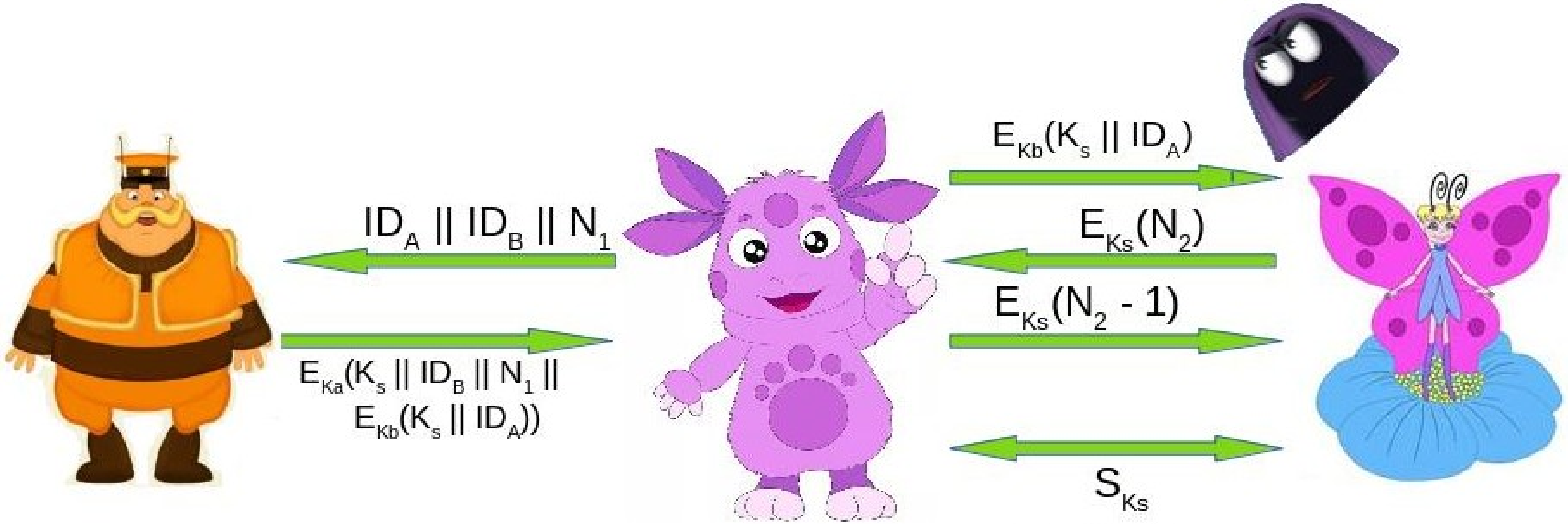


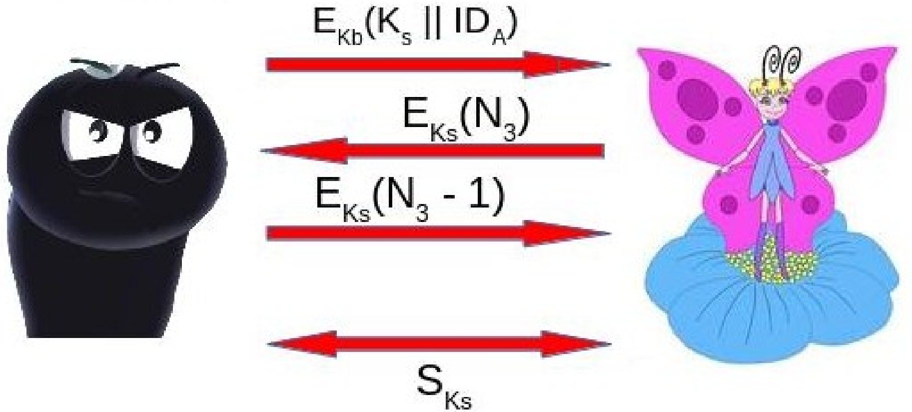
Злоумышленник навязывает повторное использование ключа K_s и может расшифровать передаваемые данные.

Протокол Нидхема-Шредера

№	Направление	Данные
1	$A \Rightarrow KDC$	$ID_A \,\|\|\, ID_B \,\|\|\, N_1$
2	$KDC \Rightarrow A$	$E_{Ka}(K_s \,\|\|\, ID_B \,\|\|\, N_1 \,\|\|\, E_{Kb}(K_s \,\|\|\, ID_A)\ )$
3	$A \Rightarrow B$	$E_{Kb}(K_s \,\|\|\, ID_A)$
4	$B \Rightarrow A$	$E_{Ks}(N_2)$
5	$A \Rightarrow B$	$E_{ks}(N_2 - 1)$

Атака повторного воспроизведения





Зная старый сеансовый ключ, злоумышленник сам инициирует соединение со второй стороной, выдавая себя за первую.

Протокол Деннинга

№	Направление	Данные
1	$A \Rightarrow KDC$	$ID_A \parallel ID_B$
2	$KDC \Rightarrow A$	$E_{Ka}(K_s \parallel ID_B \parallel T \parallel E_{Kb}(K_s \parallel ID_A \parallel T))$
3	$A \Rightarrow B$	$E_{Kb}(K_s \parallel ID_A \parallel T)$
4	$B \Rightarrow A$	$E_{Ks}(N_2)$
5	$A \Rightarrow B$	$E_{Ks}(f(N_2))$

Протоколы разделения секрета

Задача:

Имеется N различных ключей шифрования, распределенных между участниками.

Требуется, чтобы данные могли быть расшифрованы с помощью любых M ключей из этого набора (M < N).

Данные не могут быть расшифрованы при применении M-1 ключа.

Разделение секрета по схеме Шамира

$L(x) = (a_{M-1}x^{M-1}+a_{M-2}x^{M-2}+...+a_1x+S) \bmod p$ - многочлен

a_{M-1}, a_{M-2}, ..., a_1 – случайные целые числа;

S – секрет в виде числа;

p – простое число и $p > N$, $p > S$;

Если y_1, y_2, ..., y_N значения L(x) в точках x=1, x=2, ..., x=N соответственно, то **ключами будут координаты точек** $K_1 = (1, y_1)$, $K_2 = (2, y_2)$, ..., $K_N = (N, y_N)$.

Разделение секрета по схеме Шамира

$L(x) = (a_{M-1}x^{M-1}+a_{M-2}x^{M-2}+...+a_1x+S) \bmod p$

$(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), ..., (x_{iM}, y_{iM})$

$L(x) = \sum_{i=1}^{M} y_i l_i(x)$ - интерполяционный полином Лагранжа

$l_i(x) = \prod_{j=1, j\neq i}^{M} \frac{x - x_j}{x_i - x_j}$, - базисные полиномы

Разделение секрета по схеме Шамира

Пример: S = 11, N = 5, M = 3

№ п/п	Описание операции	Пример
1	Выбор простого числа **p**, которое больше количества долей **N** и секрета **S**.	p = 59
2	Выбор произвольного многочлена степени **M-1** : **f(x)** = $(a_2x^2 + a_1x + S) \bmod p$, где значения $\mathbf{a_2}$ и $\mathbf{a_1}$ выбираются случайным образом, хранятся в тайне и отбрасываются после распределения долей.	$a_2 = 10$, $a_1 = 23$ $f(x) = (10x^2 + 23x + 11) \bmod 59$
3	Определение долей ($\mathbf{x_i}$, $\mathbf{y_i}$), где $\mathbf{y_i} = f(x_i)$ и $\mathbf{x_i} = i + 1$.	$y_0 = (10{*}1^2 + 23{*}1 + 11) \bmod 59 = 44$ $y_1 = (10{*}2^2 + 23{*}2 + 11) \bmod 59 = 38$ $y_2 = (10{*}3^2 + 23{*}3 + 11) \bmod 59 = 52$ $y_3 = (10{*}4^2 + 23{*}4 + 11) \bmod 59 = 27$ $y_4 = (10{*}5^2 + 23{*}5 + 11) \bmod 59 = 22$
4	Публикация **p** и распределение долей ($\mathbf{x_i}$, $\mathbf{y_i}$) между участниками.	p = 59 $(x_0, y_0) = (1, 44)$ $(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_3, y_3) = (4, 27)$ $(x_4, y_4) = (5, 22)$

Разделение секрета по схеме Шамира

№ п/п	Описание операции	Пример
1	Сбор **M** долей.	$(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_4, y_4) = (5, 22)$
2	Определение базисных полиномов.	$l_1(x) = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = \frac{x-3}{-1} \cdot \frac{x-5}{-3} = \frac{1}{3} \cdot (x^2 - 8x + 15)$ $l_2(x) = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = \frac{x-2}{1} \cdot \frac{x-5}{-2} = \frac{1}{-2} \cdot (x^2 - 7x + 10)$ $l_4(x) = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = \frac{x-2}{3} \cdot \frac{x-3}{2} = \frac{1}{6} \cdot (x^2 - 5x + 6)$
3	Определение интерполяционного полинома Лагранжа.	$L(x) = \left[\frac{38}{3} \cdot (x^2 - 8x + 15) + \frac{52}{-2} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6)\right] \mod 59$ $L(x) = \left[\frac{76}{6} \cdot (x^2 - 8x + 15) - \frac{156}{6} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6)\right] \mod 59$ $L(x) = \left[\frac{1}{6} \cdot (-58x^2 + 374x - 288)\right] \mod 59$
4	Определение обратного числа по модулю $\mathbf{b^{-1}}$ для дробного множителя полинома **1 / b**.	$\frac{1}{b} = \frac{1}{6}$ $b^{-1} = 10$ [(6 * 10) mod 59 = 1]
5	Замена дробного множителя **1 / b** и умножение коэффициентов полинома на множитель $\mathbf{b^{-1}}$.	$L(x) = [10 * (-58x^2 + 374x – 288)] \mod 59 = (-580x^2 + 3740x – 2880) \mod 59$
6	Приведение коэффициентов полинома и определение секрета **S**.	$a_2 = -580 \mod 59 = -49 \mod 59 = 10$ $a_1 = 3740 \mod 59 = 23$ $S = a_0 = -2880 \mod 59 = -48 \mod 59 = 11$ $L(x) = (10x^2 + 23x + 11) \mod 59$

Альтернативные подходы

- N штук N-мерных некомпланарных гиперплоскостей пересекаются в одной точке. Секрет - координаты точки пересечения.
- Нельзя решить систему с N неизвестными, имея меньше N уравнений. Секрет - решение системы уравнений.

Слепая подпись

Анна				Борис		
Описание действия	Секретные данные	Открытые данные		Открытые данные	Секретные данные	Описание действия
		N, e		N, e	d	Генерирует ключи для RSA.
Накладывает маскирующий множитель	m - сообщение, r - случайное	$m' = mr^e \bmod N$	$\Rightarrow$	m’		
		s’	$\Leftarrow$	$s' = (m')^d \bmod N$		Подписывает сообщение
Убирает маскировку		$s = s'*r^{-1} \bmod N = m^d \bmod N$				

Забывающая передача Рабина

Анна				Борис		
Описание действия	Секретные данные	Открытые данные		Открытые данные	Секретные данные	Описание действия
Генерирует ключи для RSA.	d	N, e	$\Rightarrow$	N, e		
Составляет сообщение.	m	$m^e \bmod N$	$\Rightarrow$	$m^e \bmod N$		
		v	$\Leftarrow$	$v = x^2 \bmod N$	x	Выбирает случайное число меньше N.
Вычисляет квадратный корень из y.		$y \mid y^2 \equiv v \bmod N$	$\Rightarrow$	y		Если $y \neq x$ и $y \neq -x$, то Борис сможет факторизовать N.

Квадратичный вычет $x^2 \equiv a \bmod pq$, где p,q-простые, имеет 4 корня. Поэтому вероятность расшифровки сообщения равна 0.5.

Забывающая передача 1 к 2

Анна			Борис	
Секретные данные	Открытые данные		Открытые данные	Секретные данные
m_0, m_1 - сообщения				
d – для RSA	N, e – для RSA	$\Rightarrow$	N, e	
	x_0, x_1 - случайные	$\Rightarrow$	x_0, x_1	
				k - случайное, $b \in \{0,1\}$
	v	$\Leftarrow$	$v = (x_b + k^e) \bmod N$	
$k_0 = (v - x_0)^d \bmod N$ $k_1 = (v - x_1)^d \bmod N$				
	$m'_0 = m_0 + k_0$ $m'_1 = m_1 + k_1$	$\Rightarrow$	m'_0, m'_1	
				$m_b = m'_b - k$

Забывающая передача 1 к 2

- Анна готовит сообщения (числа) m_0 и m_1 к отправке.
- Анна генерирует ключи RSA d, e, N. Открытый ключ (e, N) передает Борису.
- Анна генерирует два случайных числа x_0, x_1 и передает их Борису.
- Борис выбирает b – номер сообщения и случайное число k.
- Борис передает Анне $v = (x_b + k^e) \bmod N$.
- Анна вычисляет $k_0 = (v – x_0)^d$ $k_1 = (v – x_1)^d \bmod N$. Одно из двух чисел k_0 и k_1 равно k, но Анна не знает которое.
- Анна передает Борису $m'_0 = m_0 + k_0$ и $m'_1 = m_1 + k_1$.
- Борис вычисляет $m_b = m'_b – k$.

Электронная цифровая подпись

Отправитель

1. Вычисляет хеш-образ сообщения $r = h(T)$.
2. Шифрует хеш-образ на своем закрытом ключе и получает **цифровую подпись** $s = E_{Kp}(r)$.
3. Передает пару (T, s).

Получатель

1. Вычисляет хеш-образ сообщения $r1 = h(T)$.
2. Расшифровывает цифровую подпись на открытом ключе отправителя и получает хеш-образ $r = E_{Ko}(s)$.
3. Если $r1 = r$, то подпись верна.

ЭЦП решает задачи проверки подлинности, целостности сообщения и неотрицания авторства.

ЭЦП

Федеральный закон от 06.04.2011 г. №63

статья №6:

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, **равнозначным документу на бумажном носителе, подписанному собственноручной подписью**, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации...

ЭЦП

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Усиленная квалифицированная электронная подпись создается с привлечением криптографических средств, подтвержденных компетентными органами, а именно ФСБ РФ. Гарантом подлинности в данном случае выступает специальный сертификат, выданный аккредитованным удостоверяющим центром. В сертификате указан ключ проверки ЭП.

ЭЦП

Получение ЭЦП:

- Обращение в аккредитованный удостоверяющий центр.
- Предоставление необходимых данных.
- Проверка предоствленных данных удостоверяющим центром.
- Выдача ЭЦП.

Номер квалифицированного сертификата: 01D3 652F 1837 E160 0000 105F 0379 0002
Действие квалифицированного сертификата: 24 ноября 2017 г. 17:18:00 по 24 ноября 2018 г. 17:17:20

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество: Усмонов Шухратджон Фозилович
Страховой номер индивидуального лицевого счета: 18931939424

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра: ЗАО "КАЛУГА АСТРАЛ"
Место нахождения удостоверяющего центра: RU, 40 Калужская область, г. Калуга, пер. Теренинский, д. 6
Номер квалифицированного сертификата удостоверяющего центра: 23 90 81 8F 00 00 00 00 01 40
Наименование средства электронной подписи: Средство криптографической защиты информации ViPNet CSP 4.2
Реквизиты заключения о подтверждении соответствия средства электронной подписи: СФ/124-2860 от 15 марта 2016
Наименование средства удостоверяющего центра: Программный комплекс "ViPNet Удостоверяющий центр 4 (версия 4.6)"
Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: СФ/128-2932 от 10 августа 2016
Класс средств удостоверяющего центра: КС2

Сведения о ключе проверки электронной подписи

Используемый алгоритм: ГОСТ Р 34.10-2001
Класс средства электронной подписи: Класс средства ЭП КС1;Класс средства ЭП КС2;
Область использования ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных
Значение ключа:
0440 0CDB 7C06 2034 BE47 88C8 75D7 0980 86A7 39D7 AAD8
500C 6879 8F7A 8909 4BD3 2BFD B8A4 69F3 DCA3 468C D79C
05E4 F6E1 D94C E781 1903 482C F104 90CB 9440 FF36 D915

Электронная подпись под квалифицированным сертификатом

Используемый алгоритм: ГОСТ Р 34.10-2001
Значение электронной подписи:
00000 7C 05 C9 C0 7E F9 84 B1 82 B0 76 70 B5 D4 BF 43
00010 8B F2 75 C3 F0 E2 B9 A6 9D 27 54 2A 3B FC A8 E3
00020 37 AA 42 EB 02 5C 20 9E 90 F2 BF E4 B7 98 3A D9
00030 D5 33 92 BF 93 1E 9A 2A 95 83 30 33 9D 49 70 A6

Подпись уполномоченного лица ______ / Терлов П.В. /
М.П.

Подпись владельца сертификата ______ / Усмонов Шухратджон Фозилович /
М.П.

УСМОНОВ ШУХРАТДЖОН ФОЗИЛОВИЧ

ЭЦП

Хранение ЭЦП:

- Флеш-карта
- Токен – компактное usb-устройство, содержащее энергонезависимую память и сопроцессор. Предназначен для хранения ключей шифрования и возможности проведения криптографических преобразований без передачи ключей на внешние устройства. Марки изделий: “Рутокен”, “eToken”, “VdToken”, “JaCarta”, “MS_KEY K”, “Токен++” и др.

ЭЦП

Взаимодействие с токеном происходит через набор понятных ему инструкций на уровне контроллера (операции: получить сертификат, подписать данные, зашифровать данные и т.п.).

Криптопровайдер – программный модуль, обсеспечивающий интерфейс работы с ЭЦП-токеном (КриптоПРО CSP, Лисси-CSP, Signal-COM CSP).

ЭЦП

Мошенничество с использованием ЭЦП:

https://www.kp.ru/daily/26979/4038526/ - подаренная квартира

https://habr.com/en/post/453596/ - фиктивные ООО

https://habr.com/ru/post/461885/ - чужие налоги

https://47news.ru/articles/156549/ - удаленное оформление ЭЦП

Федеральный закон от 06.04.2011 г. №63

Статья 18. Выдача квалифицированного сертификата

1. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

   1) установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

2. При обращении в аккредитованный удостоверяющий центр заявитель ... представляет следующие документы либо их надлежащим образом заверенные копии и сведения...

https://sesc-infosec.github.io/