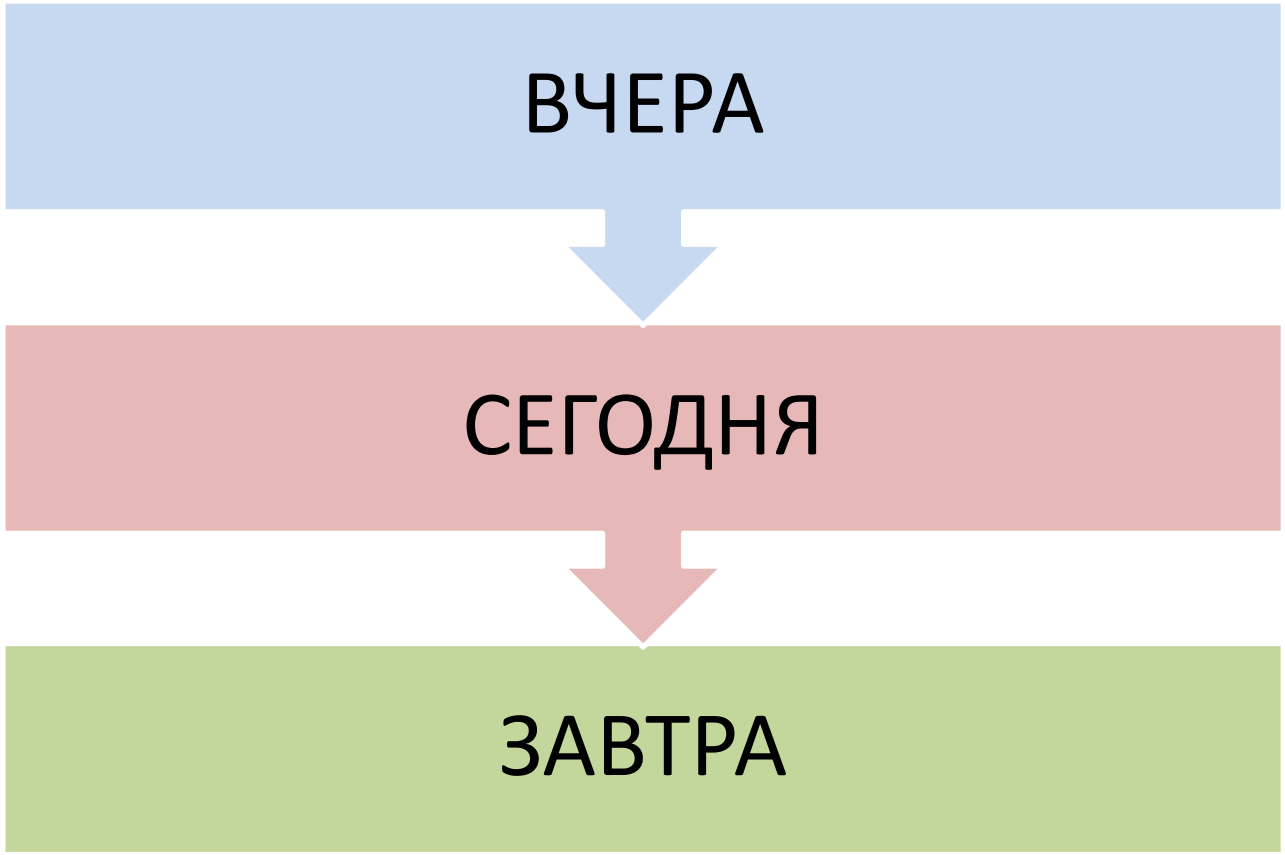
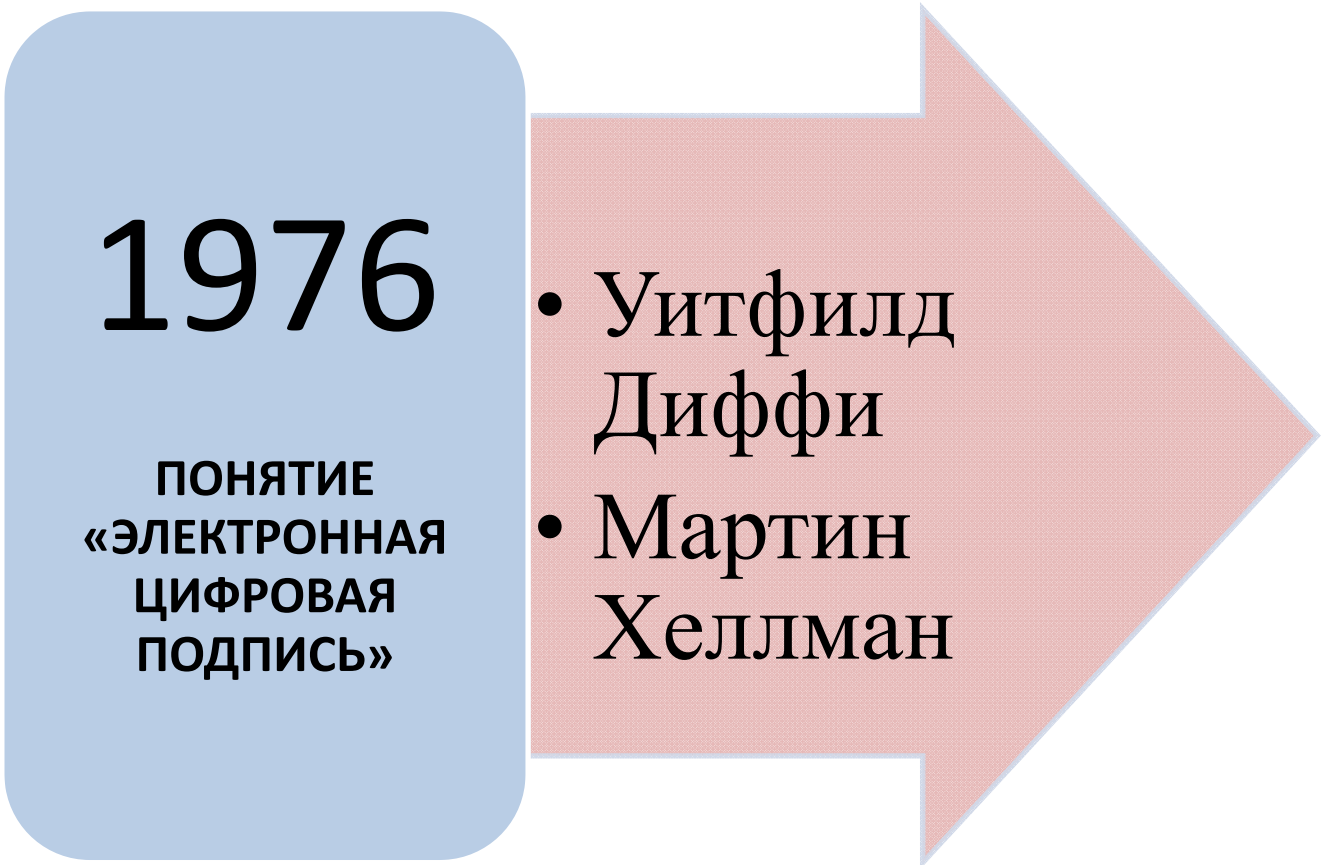
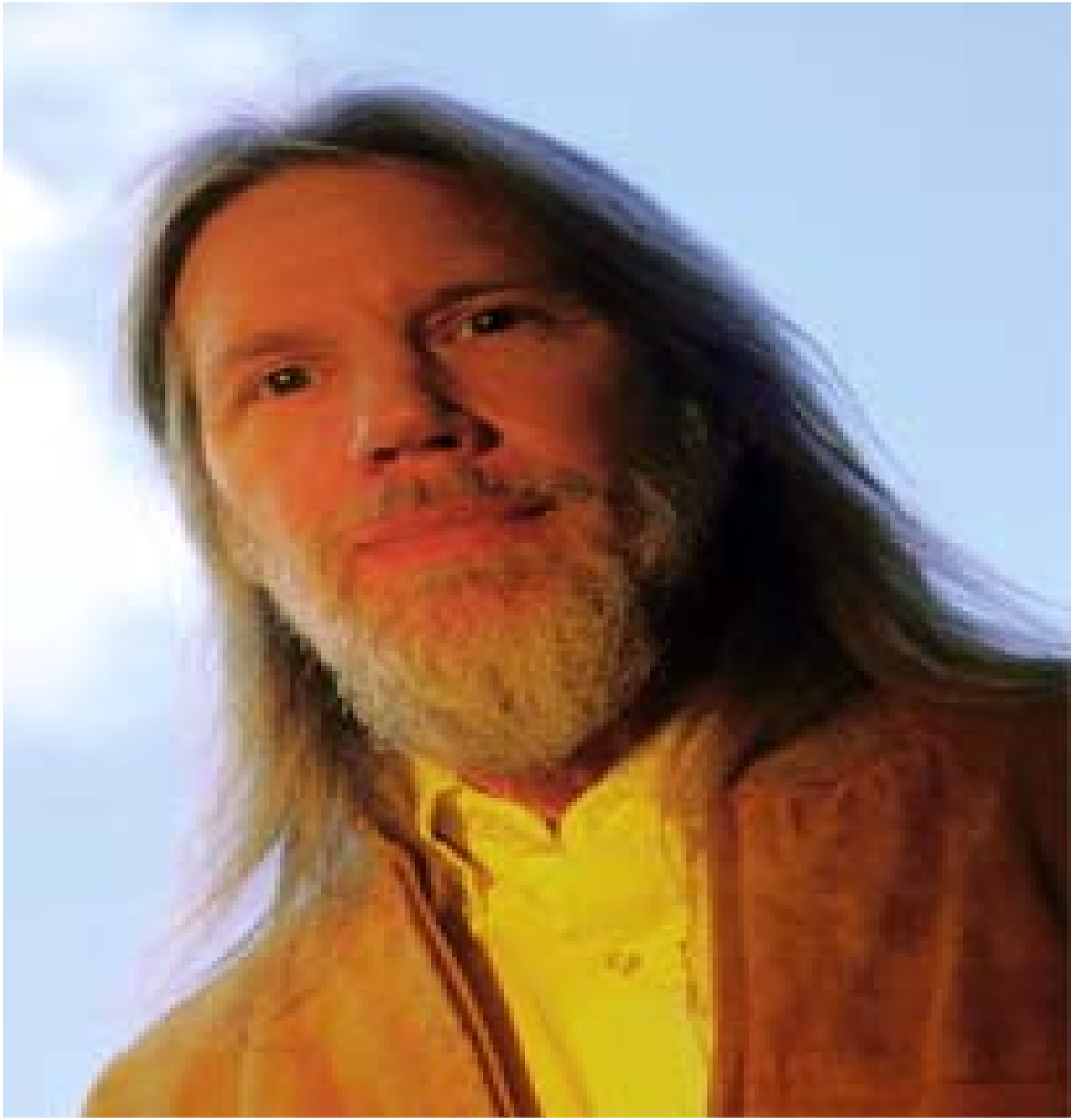
СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

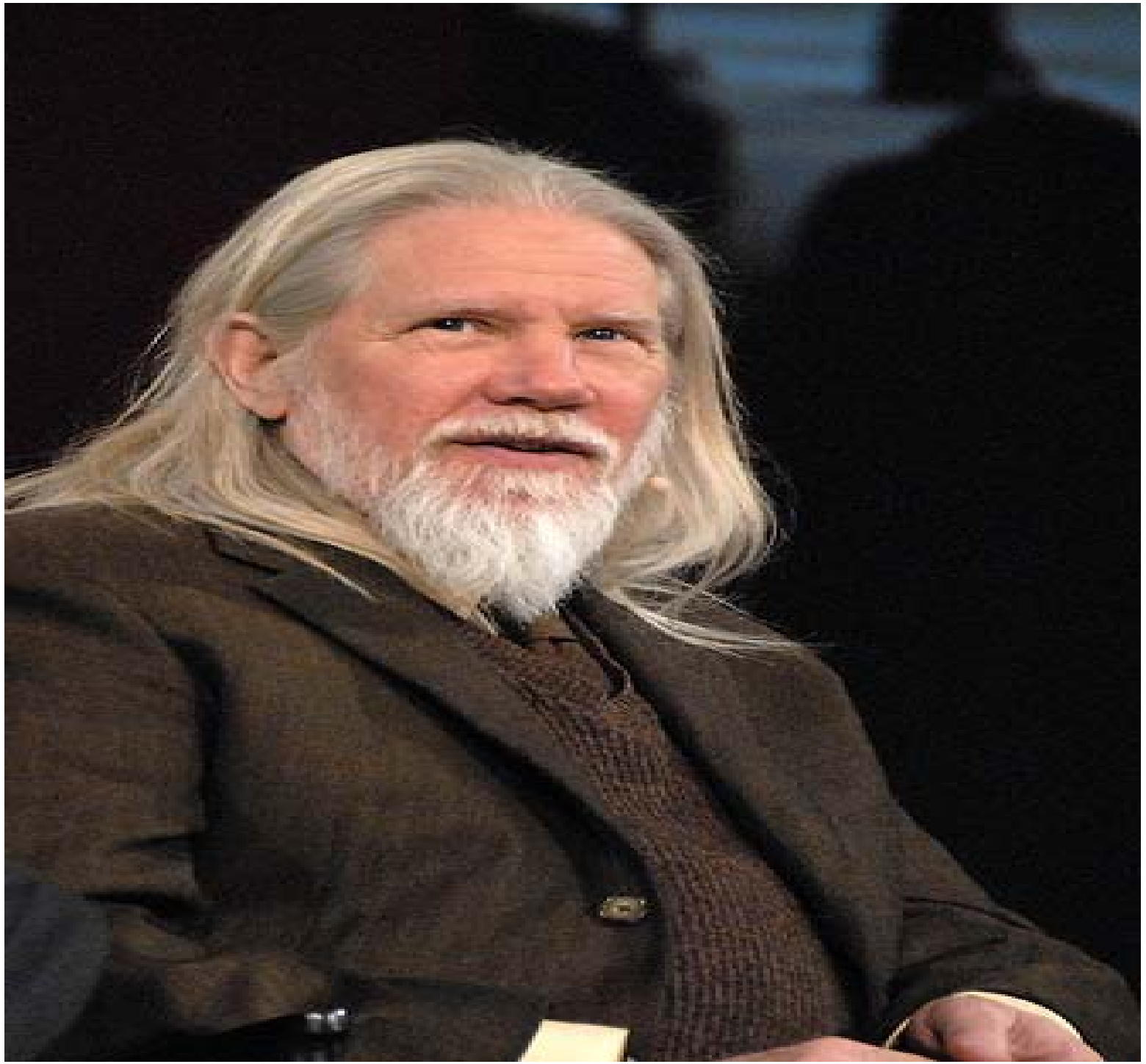
Комисаренко Владимир Владимирович - начальник группы
Оперативно-аналитического центра
при Президенте Республики Беларусь


ВЧЕРА
СЕГОДНЯ
ЗАВТРА


1976
ПОНЯТИЕ «ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ»
• Уитфилд Диффи
• Мартин Хеллман

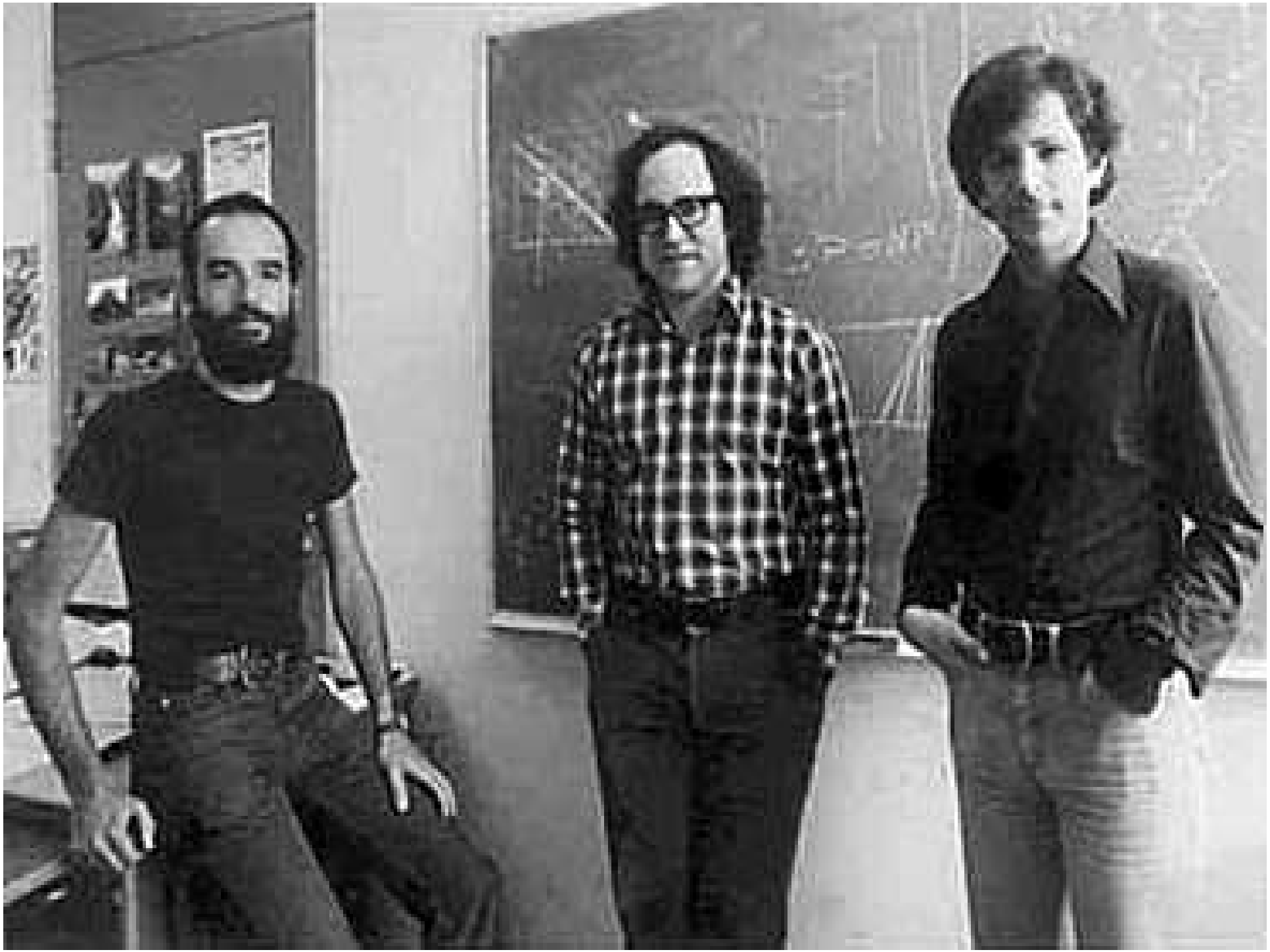
В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись». В тот момент они всего лишь предполагали, что схемы электронной цифровой подписи могут существовать.

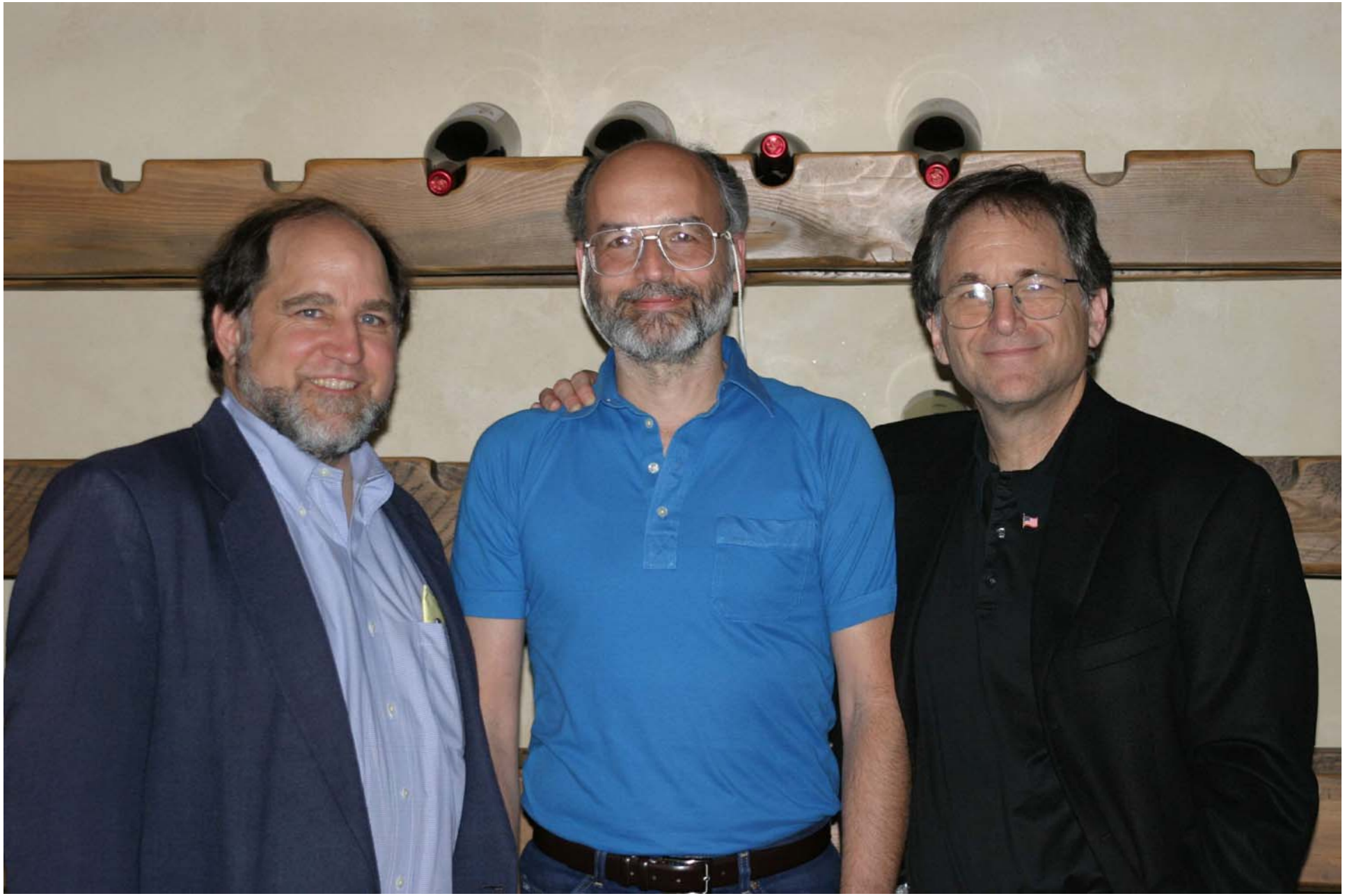




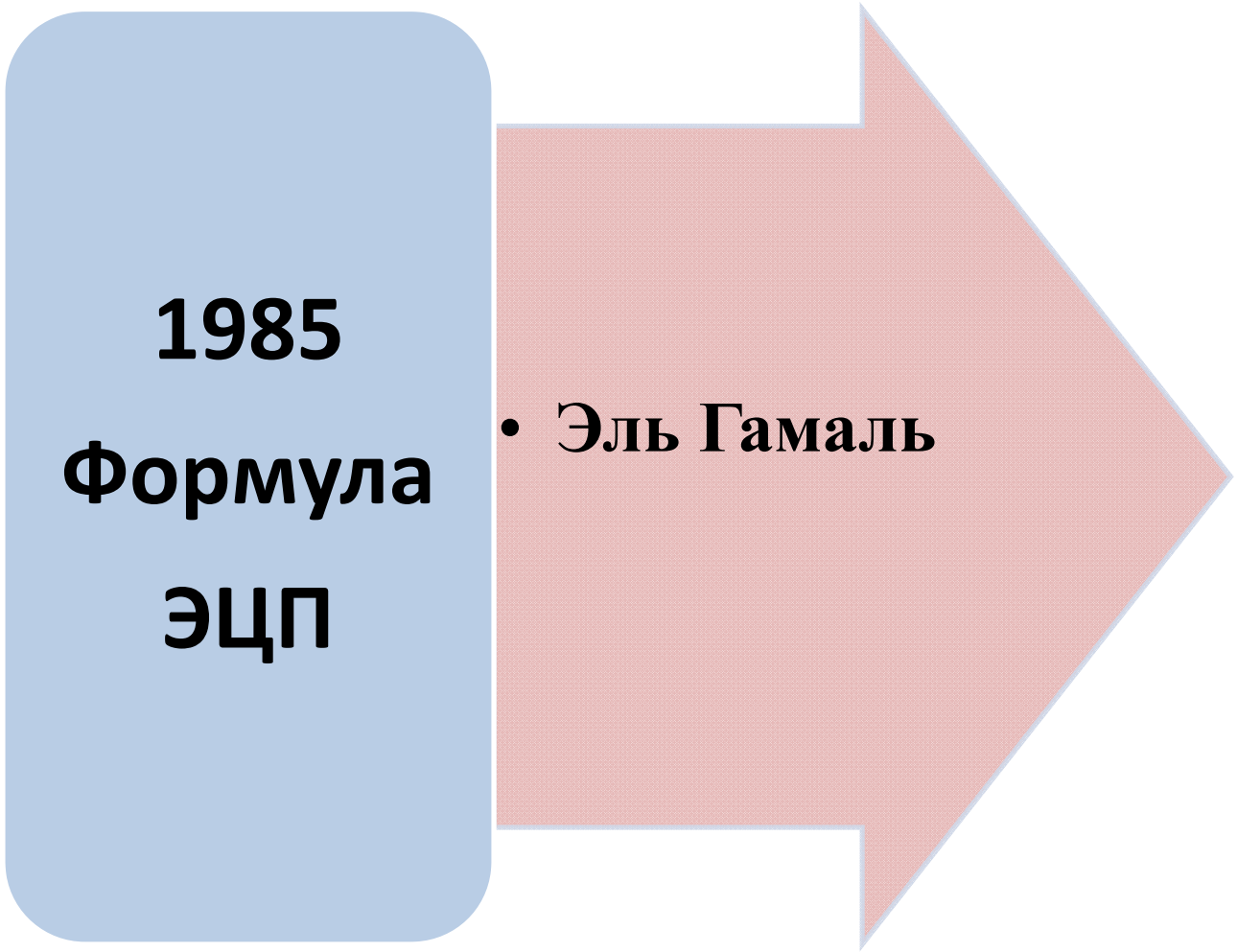

1977
RSA
• Рональд Ривест
• Ади Шамир
• Леонард Адельман

В 1977 году Рональд Ривест, Ади Шамир и Леонард Адельман разработали криптографический алгоритм RSA, который можно было использовать для создания ЭЦП.

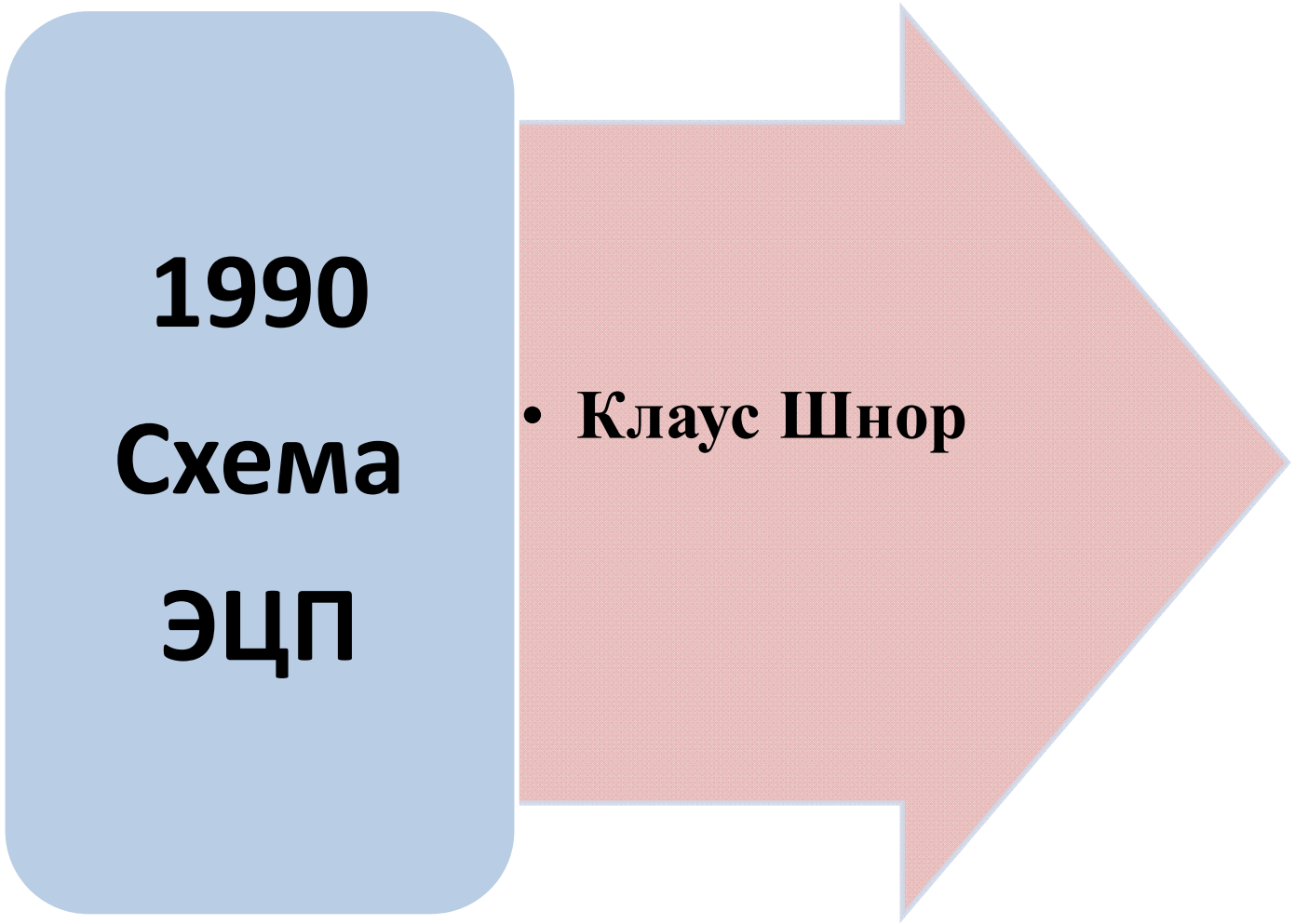


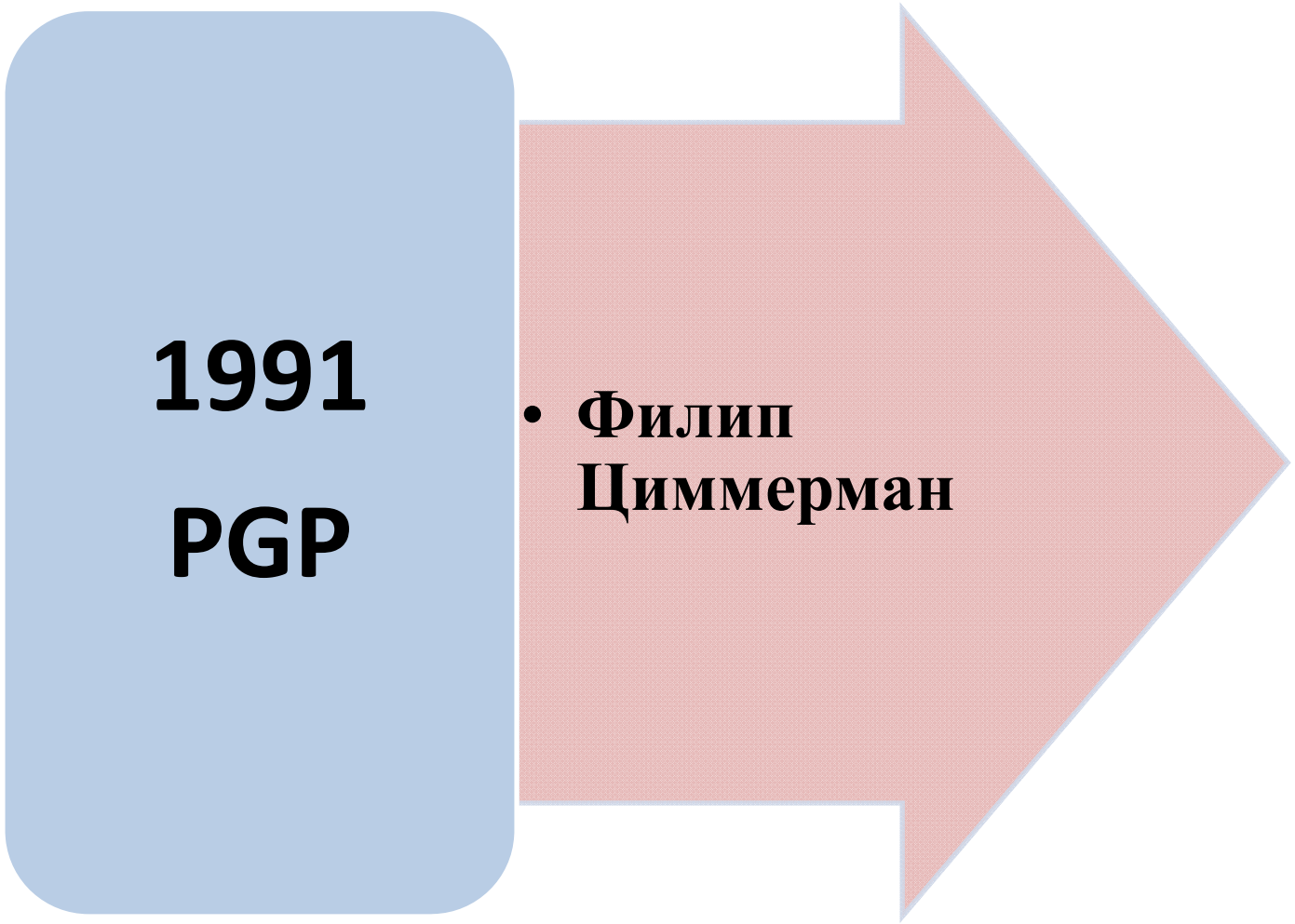


В 1984 году Шафи Гольдвассер, Сильвио Микали и Рональд Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны модели атак на алгоритмы ЭЦП, а также предложена схема, отвечающая описанным требованиям.


1985
Формула
ЭЦП
• Эль Гамаль

ЭльГамаль (T. El Gamal) в 1985г. разработал криптографическую систему, которая стала основой для создания государственных стандартов цифровой подписи как США (DigitalSignature Standard — DSS), так и России (ГОСТ 34.10).


1990
Схема
ЭЦП
• Клаус Шнор


1991
PGP
• Филип Циммерман

В эпоху триумфального шествия персональных компьютеров появилась возможность реализовать на них эти криптографические алгоритмы. Идея увлекла американского математика и программиста Филипа Циммермана (Philip Zimmermann). В 1990 году он разработал недорогую и простую коммерческую программу для массового пользователя и опубликовал ее в Интернете, назвав Pretty Good Privacy (сокращенно PGP). Эта программа стала первой практически реализованной системой, основанной на алгоритме RSA. Она и положила начало развития применения электронной цифровой подписи (ЭЦП) во всем мире.

СТАНДАРТИЗАЦИЯ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

6.1 Формирование цифровой подписи

Для получения цифровой подписи под сообщением $M \in V_\infty$ необходимо выполнить следующие действия (шаги) по **Алгоритму I**:

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

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

$$e \equiv \alpha \pmod{q}. \tag{15}$$

Если $e = 0$, то определить $e = 1$.

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

$$0 < k < q. \tag{16}$$

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

$$r \equiv x_c \pmod{q}, \tag{17}$$

где x_c – x-координата точки C. Если $r = 0$, то вернуться к шагу 3.

Шаг 5 – вычислить значение

$$s \equiv (rd + ke) \pmod{q}. \tag{18}$$

Если $s = 0$, то вернуться к шагу 3.

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

INTERNATIONAL STANDARD

ISO/IEC 15946-2

First edition
2002-12-01

Information technology — Security techniques — Cryptographic techniques based on elliptic curves —

Part 2: Digital signatures

Technologies de l'information — Techniques de sécurité — Techniques cryptographiques basées sur les courbes elliptiques —

Partie 2: Signatures digitales

5 EC-GDSA Signature Algorithm

5.2.1 Calculation of the message digest

1. Compute the hash-code $e = \boldsymbol{h}(M)$.

5.2.2 Elliptic Curve Computations (Arithmetic operations in the underlying field)

2. Select a random integer k in the interval $\{1, \ldots, n-1\}$.

3. Compute the elliptic curve point $(x_1, y_1) = kG$.

5.2.3 Computations modulo the group order of G (Arithmetic operations in $F(n)$)

4. Set $r = \pi(kG) \bmod n$.

5. Set $s = (kr - e)d_A \bmod n$.

If the signature generation process yields either $s = 0$ or $r = 0$ then the process must be repeated from step 2 with a new random value k. (But note that the probability that either $r = 0$ or $s = 0$ is negligibly small if k is chosen as described in 5.2.2.)

6 EC-DSA

6.2.1 Calculation of the message digest

1. Compute the hash-code $e = \boldsymbol{h}(M)$.

6.2.2 Elliptic Curve Computations (Arithmetic operations in the underlying field)

2. Select a random integer k in the interval $\{1, \ldots, n-1\}$.

3. Compute the elliptic curve point $(x_1, y_1) = kG$.

6.2.3 Computations modulo the group order of *G*. (Arithmetic operations in *F*(*n*))

4. Set $r = \pi(kG) \bmod n$.

5. Compute k^{-1} in $\boldsymbol{F}(n)$.

6. Compute $s = (d_A r + e)\, k^{-1} \bmod n$.

7 EC-KCDSA

7.2.1 Calculation of the message digest

1. Compute the hash-code $e = \boldsymbol{h}(z_A || M)$.

7.2.2 Elliptic Curve Computations (Arithmetic operations in the underlying field)

2. Select a random integer k in the interval $\{1, \ldots, n-1\}$.

3. Compute the elliptic curve point $(x_1, y_1) = kG$.

4. Set c to be the converted byte string of x_1.

5. Compute the hash-code $r = \boldsymbol{h}(kG) = \boldsymbol{h}(c)$.

NOTE Since the computation of r is independent of any message to be signed, r may be precomputed and stored for a later one-time use in a signing operation.

7.2.3 Computations modulo the group order of G (Arithmetic operations in $F(n)$)

6. Compute $w = r$ XOR e. If $w \geq n$, then $w = w - n$.

7. Compute $s = d_A(k - w) \bmod n$.

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка

ДСТУ 4145 – 2002

Видання офіційне

Алгоритм цифрового підписування:

9. Обчислюють елемент основного поля $y = hF_e$.
10. Елемент основного поля y перетворюють на ціле число r згідно з 5.8.
11. Якщо $r = 0$, то переходять до кроку 8, інакше переходять до кроку 12.
12. Обчислюють ціле число $s = (e + dr) \bmod n$.
13. Якщо $s = 0$, то переходять до кроку 8, інакше переходять до кроку 14.
14. Пару цілих чисел (r, s) перетворюють на цифровий підпис D довжини L_D згідно з 5.10.
15. Результат виконання алгоритму – підписане повідомлення (iH, T, D).

ПРЕДВАРИТЕЛЬНЫЙ
ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ П 34.101.XX–XXXX

Информационные технологии и безопасность

АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Інфармацыйныя тэхналогіі і бяспека

АЛГАРЫТМЫ ЭЛЕКТРОННАГА ЛІЧБАВАГА ПОДПІСУ НА ПАДСТАВЕ ЭЛІПТЫЧНЫХ КРЫВЫХ

Настоящий проект предстандарта не подлежит применению до его утверждения

Госстандарт
Минск

6.3.3 Алгоритм выработки ЭЦП

ЭЦП составляется из частей $S_0 \in \{0,1\}^l$ и $S_1 \in \{0,1\}^{2l}$.

выполнении следующих шагов:

1 Выработать $k \xleftarrow{R} \{1, 2, \ldots, q-1\}$.

2 Установить $R \leftarrow kG$.

3 Установить $S_0 \leftarrow h\text{BELT}_l(\text{OID}(h) \parallel \pi_{2l}(R) \parallel h(X))$.

4 Установить $S_1 \leftarrow \left\langle (k - \overline{h(X)} - (\overline{S_0} + 2^l)d) \bmod q \right\rangle_{2l}$.

5 Установить $S \leftarrow S_0 \parallel S_1$.

6 Возвратить S.

Описание схемы Шнора

Firstly, we briefly describe the protocol. For any security parameter k, an authority chooses two large prime integers p and q, such that $2^{k-1} \leq q < 2^k$ holds and q divides $p-1$ as well as an element g from $\mathbb{Z}_p^\star$ of order q. The triple (p, q, g) is published together with a public hash function f whose output domain is identified to $\mathbb{Z}_q^\star$. The security parameter k is then equal to $\lceil \log q \rceil$, whereas the size of the public key, denoted by n, is equal to $\lceil \log p \rceil$. Furthermore, we assume that $k \gg \log n$. Any user randomly chooses his secret key x in $\mathbb{Z}_q^\star$, and publishes $y = g^{-x} \bmod p$.

In order to sign a message m, the user chooses a random element K in $\mathbb{Z}_q^\star$ and computes the commitment $r = g^K \bmod p$. He gets the challenge $e = f(m, r)$ and computes $s = K + xe \bmod q$. The signature is the triple (r, e, s), which satisfies the tests $r \stackrel{?}{=} g^s y^e \bmod p$ and $e \stackrel{?}{=} f(m, r)$.

Описание реализации схемы Шнора в стандарте Республики Беларусь СТБ 1176.2-99

5.3 Алгоритм выработки ЭЦП

Алгоритм выработки ЭЦП включает в себя следующие шаги:

1 Выработать с помощью физического датчика случайных чисел или псевдослучайным методом с использованием секретных параметров число k $(1 < k < q)$;

2 $t := a^{(k)}$;

3 Представить число t в виде разложения по основанию 2^8:

$$t = \sum_{i=0}^{n-1} t_i \cdot (2^8)^i ;$$

4 $M_t := (t_0, t_1, ..., t_{n-1}, m_1, ..., m_z)$;

5 $U := h\left(M_t\right)$.

Если $U = 0$, то перейти к шагу 1;

6 $V := (k - x \cdot U) \bmod q$.

Если $V = 0$, то перейти к шагу 1;

7 $S := U \cdot 2^r + V$.

ЭЦП последовательности M является число S.

Journal of Cryptology, Volume 13, Number 3.
Pages 361–396, Springer-Verlag, 2000.

Security Arguments for Digital Signatures and Blind Signatures*

David Pointcheval and Jacques Stern

Laboratoire d'Informatique, École Normale Supérieure,
75230 Paris Cedex 05, France.
{David.Pointcheval, Jacques.Stern}@ens.fr
http://www.di.ens.fr/~{pointche,stern}

Communicated by Don Coppersmith

Received 24 October 1997 and revised 22 May 1998

Theorem 1. *(The Forking Lemma). Let $(\mathcal{G}, \Sigma, V)$ be a generic digital signature scheme with security parameter k. Let $\mathcal{A}$ be a probabilistic polynomial time Turing machine whose input only consists of public data. We denote by Q the number of queries that $\mathcal{A}$ can ask to the random oracle. Assume that, within time bound T, $\mathcal{A}$ produces, with probability $\varepsilon \geq 7Q/2^k$, a valid signature $(m, \sigma_1, h, \sigma_2)$. Then there is another machine which has control over $\mathcal{A}$ and produces two valid signatures $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$, in expected time $T' \leq 84480TQ/\varepsilon$.*

Theorem 2. *Assume that, within a time bound T, an attacker $\mathcal{A}$ performs an existential forgery under a no-message attack against the Schnorr signature, with probability $\varepsilon \geq 7Q/q$. We denote by Q the number of queries that $\mathcal{A}$ can ask to the random oracle. Then the discrete logarithm in subgroups of prime order can be solved in expected time less than $84480QT/\varepsilon$.*

Основные требования к параметрам (ГОСТ Р 34.10-2001)

5.2 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:

— простое число p - модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$. Верхняя граница данного числа должна определяться при конкретной реализации схемы цифровой подписи;

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

— целое число m – порядок группы точек эллиптической кривой E;

— простое число q - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, \ n \in Z, \quad n \geq 1 \\ 2^{254} < q < 2^{256} \end{cases}; \tag{9}$$

— точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP=O$.

— хэш-функция $h(\cdot) : V_\infty \to V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины 256 бит. Хэш-функция определена в ГОСТ Р 34.11.

5.3 Параметры эллиптической кривой

Модуль p**.** Используется простое число p, которое удовлетворяет условиям: $2^{2l-1} < p < 2^{2l}$, $p \equiv 3 \pmod 4$. Модуль определяет поле $\mathbb{F}_p$, над которым строится эллиптическая кривая. Можно использовать произвольное допустимое p, в том числе простое специального вида.

Коэффициенты a**,** b**.** Используются числа $a, b \in \mathbb{F}_p$, которые удовлетворяют условиям: $a, b \neq 0$, $b^{(p-1)/2} \equiv 1 \pmod p$, $4a^3 + 27b^2 \not\equiv 0 \pmod p$. Коэффициенты a, b вместе с модулем p определяют группу точек эллиптической кривой $E_{a,b}(\mathbb{F}_p)$.

Параметр *seed***.** Числа p и a выбираются, а b строится по ним. При построении b используется дополнительный параметр $seed \in \{0,1\}^{64}$, который может быть выбран произвольным образом.

Порядок q**.** После построения группы $E_{a,b}(\mathbb{F}_p)$ рассчитывается ее порядок $q = |E_{a,b}(\mathbb{F}_p)|$. Выбирается группа, порядок которой удовлетворяет следующим ограничениям: q — простое, $2^{2l-1} < q < 2^{2l}$, $q \neq p$, q не делит числа вида $p^m - 1$ для $m = 1, 2, \ldots, 50$.

Базовая точка G**.** Используется базовая точка $G \in E^*_{a,b}(\mathbb{F}_p)$ вида $G = (0, y_G)$, где $y_G = b^{(p+1)/4} \bmod p$. Кратные G, $2G$,..., $(q-1)G$ базовой точки пробегают все элементы $E^*_{a,b}(\mathbb{F}_p)$, а $qG = O$.

МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

DECISIONS

COMMISSION DECISION

of 25 February 2011

establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

(notified under document C(2011) 1081)

(Text with EEA relevance)

(2011/130/EU)

ANNEX

Specifications for an XML, CMS or PDF advanced electronic signature to be technically supported by the receiving Member State

Within the following part of the document the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 ([1]).

SECTION 1 — XAdES-BES/EPES

The signature is conform with the W3C XML Signature specifications ([2])

The signature MUST at least be a XAdES-BES (or -EPES) signature form as specified in the ETSI TS 101 903 XAdES specifications ([3]) and complies with all the following additional specifications:

The ds:CanonicalizationMethod that specifies the canonicalization algorithm applied to the SignedInfo element prior to performing signature calculations identifies one of the following algorithms only:

Canonical XML 1.0 (omits comments):	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML 1.1 (omits comments):	http://www.w3.org/2006/12/xml-c14n11
Exclusive XML Canonicalization 1.0 (omits comments):	http://www.w3.org/2001/10/xml-exc-c14n#

Other algorithms or of 'With comments' versions of the above listed algorithms SHOULD NOT be used for the signature creation but SHOULD be supported for residual interoperability for the signature verification.

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102 176 ([4]) and to the ECRYPT2 D.SPA.x report ([5]) for further recommendations on algorithms and parameters eligible for electronic signatures.

XAdES - BES (EPES)		Common Minimum Requirements
(ETSI TS 103 903 applies with the following profiled elements)		
M=Mandatory; O=Optional; R=Recommended; N=Not used		
ds: Signature ID	M	
ds: SignedInfo	M	
ds: CanonicalizationMethod	M	*All the following algorithms MUST be supported for signature verification, creation SHOULD restrict to one of these:* *- Exclusive XML canonicalization 1.0: http://www.w3.org/TR/xml-exc-c14n/* *- Canonical XML 1.0: http://www.w3.org/TR/2001/REC-XML-c14n-20010315* *- Canonical XML 1.1: http://www.w3.org/2006/12/xml-c14n11* *Other methods or "#WithComments" versions of the above methods SHOULD NOT be used.*
ds: SignatureMethod	M	***Algorithms:*** *refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.*
ds: Reference URI	M	One reference to every original data object to be signed (URIs can point to external object as well), + reference to SignedProperties element
ds: Transforms	O	*Verifying applications MUST support all following transforms while signature creation application SHOULD restrict the use of those transforms to the following ones:* *- Canonicalization transforms: see above* *- Base64 encoding* *- XPath and XPath Filter 2.0* *- Enveloped signature transform* *- XSLT transforms*
ds: DigestMethod	M	***Algorithms:*** *refer to applicable national laws and for guidelines purposes to ETSI TS 102 176 and to ECRYPT2 D.SPA.7 report for further recommendations.*
ds: DigestValue	M	
/ds: Reference		
/ds: SignedInfo		
ds: SignatureValue	M	
ds: KeyInfo	M	MUST contain X509 certificate (SigningCertificate signed property MUST contain the digest value of this signer's certificate) Signer's certificate certification chain are RECOMMENDED to be provided as a hint for facilitating the validation process (X.509 certificates MUST be provided in this case).
ds: Object		
QualifyingProperties	M	
SignedProperties	M	M
SignedSignatureProperties	M	M
SigningTime	M	UTC (xsd: dateTime)

SECTION 2 — CAdES-BES/EPES

The signature is conform with the Cryptographic Message Syntax (CMS) Signature specifications ([1]).

The signature uses CAdES-BES (or -EPES) signature attributes as specified in the ETSI TS 101 733 CAdES specifications ([2]) and complies with the additional specifications as indicated in Table 2 below.

All attributes of CAdES which are included in the archive timestamp hash calculation (ETSI TS 101 733 V1.8.1 Annex K) MUST be in DER encoding and any other can be in BER to simplify one-pass processing of CAdES.

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines to ETSI TS 102 176 ([3]) and to the ECRYPT2 D.SPA.x report ([4]) for further recommendations on algorithms and parameters eligible for electronic signatures.

The signed attributes MUST include a reference to the signer's X.509 v3 digital certificate (RFC 5035) and *SignedData.certificates* field MUST include its value.

The SigningTime signed attribute MUST be present and MUST contain the UTC expressed as in http://tools.ietf.org/html/rfc5652#section-11.3.

The ContentType signed attribute MUST be present and contains id-data (http://tools.ietf.org/html/rfc5652#section-4) where the data content type is intended to refer to arbitrary octet strings, such as UTF-8 text or ZIP container with MimeType sub-element.

In case the signatures used by Member States are based on a qualified certificate, the PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures are verifiable using the Trusted List, in accordance with Commission Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

SECTION 3 — PAdES-PART 3 (BES/EPES)

The signature MUST use a PAdES-BES (or -EPES) signature extension as specified in the ETSI TS 102 778 PAdES-Part3 specifications ([1]) and complies with the following additional specifications:

MD5 (RFC 1321) MUST NOT be used as a digest algorithm. Signers are referred to applicable national laws, and for the purposes of guidelines, to ETSI TS 102 176 ([2]) and to the ECRYPT2 D.SPA.x report ([3]) for further recommendations on algorithms and parameters eligible for electronic signatures.

The signed attributes MUST include a reference to the signer's X.509 v3 digital certificate (RFC 5035) and *SignedData.certificates* field MUST include its value.

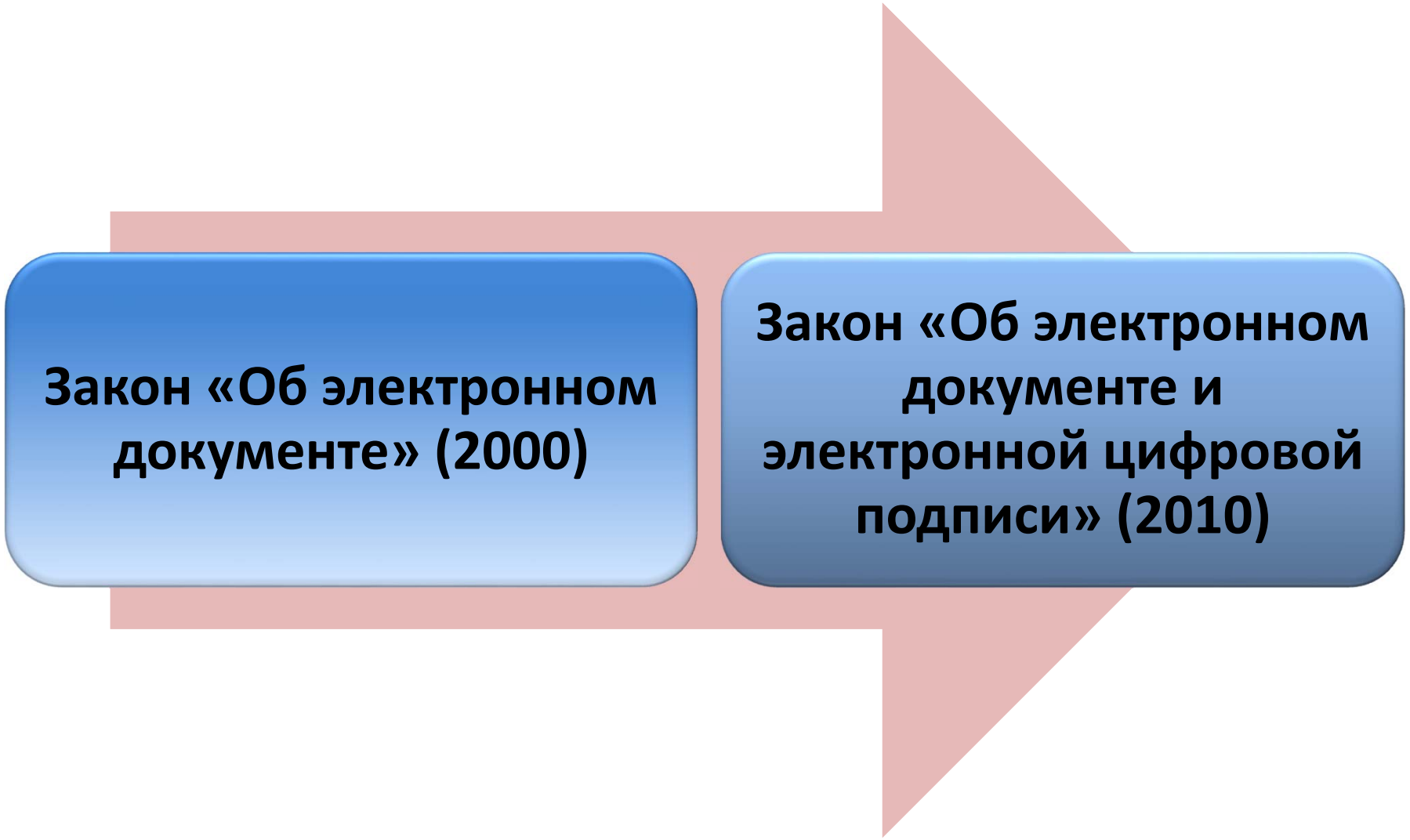
The time of signing is indicated by the value of the **M** entry in the signature dictionary.

In case the signatures used by Member States are based on a qualified certificate, the PKI objects (certificate chains, revocation data, time-stamps) that are included in the signatures are verifiable using the Trusted List, in accordance with Decision 2009/767/EC, of the Member State who is supervising or accrediting the CSP having issued the signatory's certificate.

ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ ЭЛЕКТРОННОГО ДОКУМЕНТА И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

2000, январь	• Республика Беларусь
2000, июнь	• США
2002, январь	• Россия

РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА В РЕСПУБЛИКЕ БЕЛАРУСЬ



ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ

Государственная система управления открытыми ключами предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах и их владельцах в Республике Беларусь и представляет собой систему взаимосвязанных и аккредитованных в ней удостоверяющих и регистрационных центров.

Основными функциями Государственной системы управления открытыми ключами являются:

регистрация владельцев личных ключей;

издание, распространение и хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

создание и сопровождение баз данных действующих и отозванных сертификатов открытых ключей;

внесение сертификатов открытых ключей в базу данных действующих сертификатов открытых ключей;

обеспечение доступности баз данных действующих и отозванных сертификатов открытых ключей;

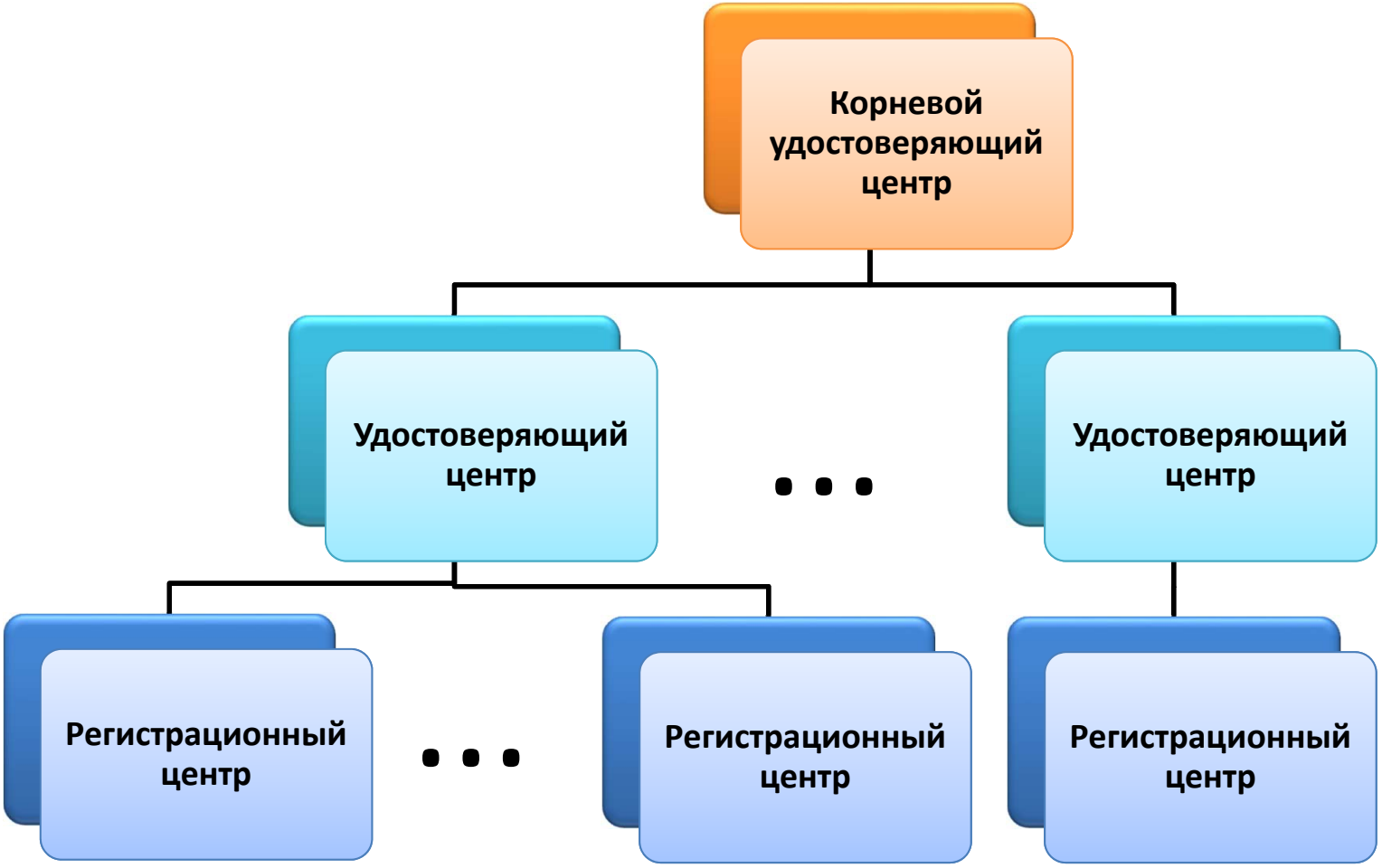
отзыв сертификатов открытых ключей;

достоверное подтверждение принадлежности открытого ключа определенной организации или физическому лицу;

хранение карточек открытых ключей.

ЕДИНАЯ ИОК – ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ

ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ



Межведомственный координационный совет по развитию Государственной системы управления открытыми ключами

- Национальный банк Республики Беларусь
- Оперативно-аналитический центр при Президенте Республики Беларусь
- Аппарат Совета Министров Республики Беларусь
- Министерство связи и информатизации Республики Беларусь
- Министерство по налогам и сборам Республики Беларусь
- Министерство юстиции Республики Беларусь
- Министерство труда и социальной защиты Республики Беларусь
- Государственный таможенный комитет Республики Беларусь
- Национальный статистический комитет Республики Беларусь
- Государственное учреждение «Главное хозяйственное управление Управления делами Президента Республики Беларусь»
- Государственное учреждение «Белорусский научно-исследовательский центр электронной документации»
- Белорусский государственный университет

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ОБРАЩЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ