Електронен подпис
(криптиране)

Изисквания към електронния подпис

7.1 What is a digital signature?

A digital signature is not a hand-written signature that has been scanned

By digital signature one should of course not picture a handwritten signature that has been scanned and digitally stored. This could easily be copied and misused. Instead, one understands it to be a (very large) number that, in connection with a c same attributes n a written c gnation signatur must fulfil t s:

- Да е защитен от фалшификации;
- Автентичността му да може да се проверява;
- Да не може да се прехвърля върху други документи без да бъде забелязано;
- Документът, към който принадлежи подписа, да не може да бъде променян, без да бъде забелязано;
- Дълъг живот.

Употреба на Електронния Подпис

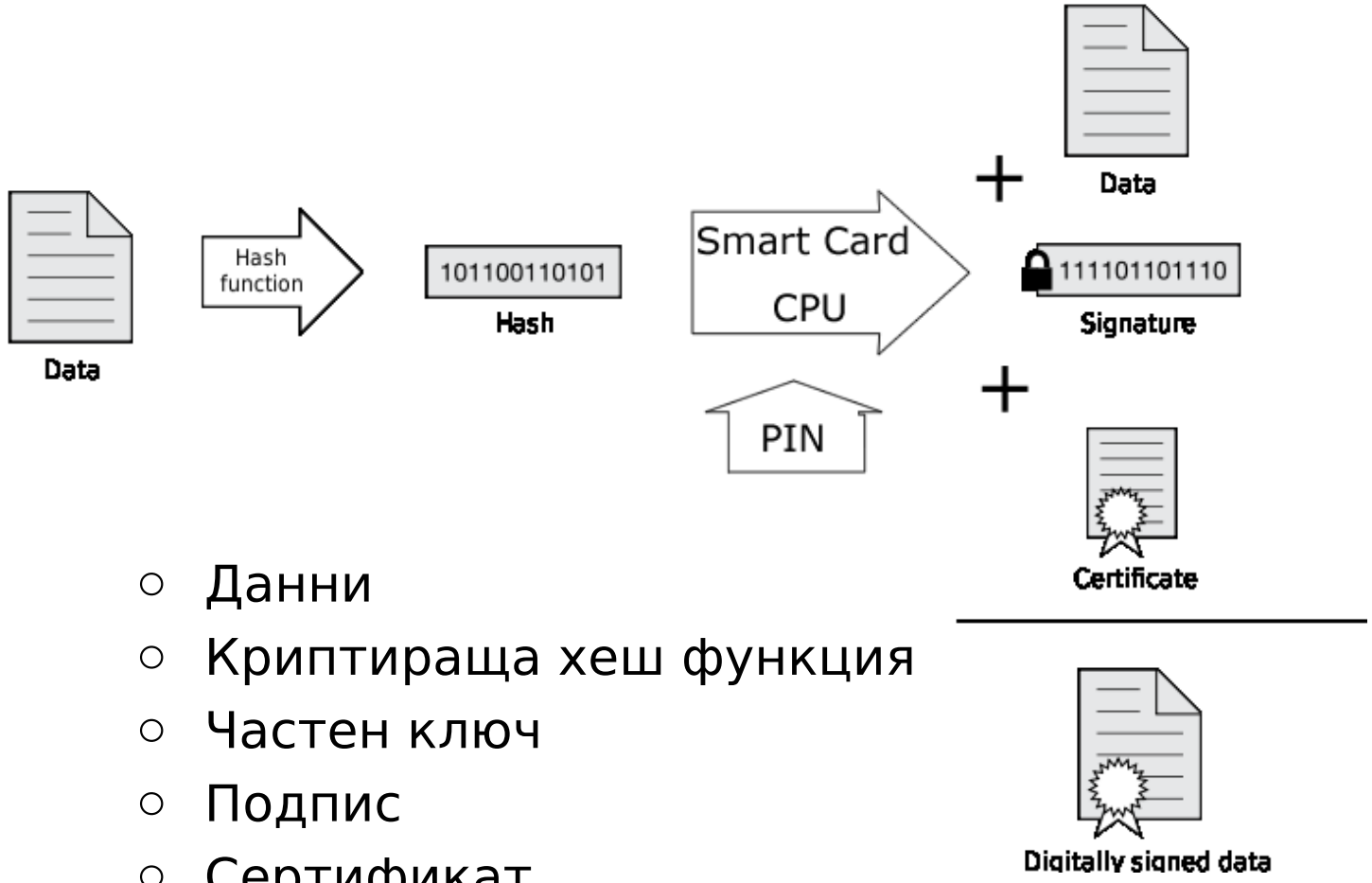
Електронният подпис осигурява доказателства за произхода, идентичността и състоянието на документа, както и гарантира съзнателно подписване.

От **хартиени** документи подписани с мастило към **електронни** подписани с електронен подпис;

Подписване на договори, сметки, дипломи, административни документи;

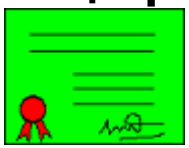
Удостоверение за самоличността на подателя и целостта на съобщението при изпращане на съобщение;
Криптиране.

Създаване на електронния подпис



- Данни
- Криптираща хеш функция
- Частен ключ
- Подпис
- Сертификат

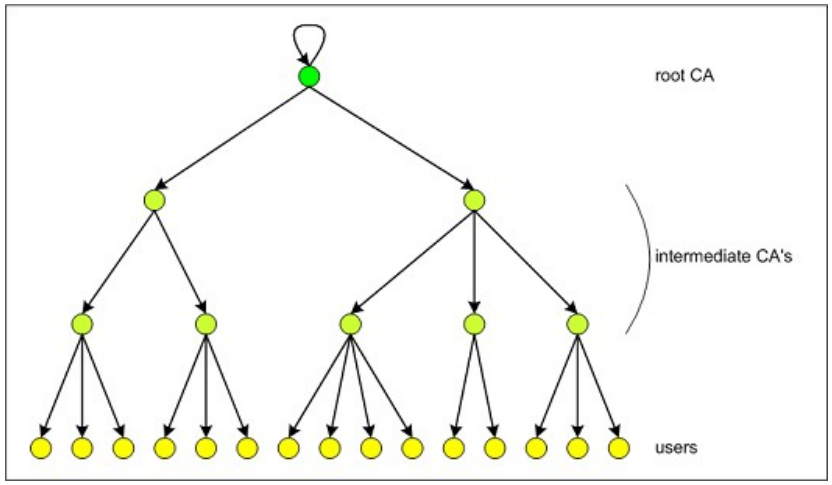
Електронен Сертификат

Удостоверяващ орган (Certification Authority). Издава (електронен) сертификат. 

Сертификат (certificate) е документ - удостоверение за електронния подпис. Сертификатът съдържа данни за притежателя на електронния подпис и
публичния му ключ.

Накратко – връзката между абонат и публичния му ключ.

Стандартът за електронен сертификат е X.509



Математика Модулна Аритметика

Права задача (Елементарна математика):

Деление	Цяла част		Дробна част
11 / 4 = = 2 + 3/4	⇔ 11 div 4 = 2	+	11 mod 4 = 3
20123 /19 = 1059 + 2/19	⇔ 20123 div 19 = 1059	+	20123 mod 19 = 2
199 /31 = __ + ___	⇔ 199 div 31 = _____	+	199 mod 31 = ___

Обратна задача (По-неясна математика – модулна аритметика):

5^-1 (mod 7) = 3, 10, 17,... (7n + 3) (5 на минус първа модул 7)

или d*5 mod 7 = 1, d = 3, проверка 3*5 mod 7 = 1

8^-1 (mod 7)= 1, 8 , 15 (7n + 1)

4^-1 (mod 8) = Ø - не съществува, защото 4 и 8 имат общ множител

7^-1 (mod 10) = ___ .

$a \perp b$ -> *a* и *b* са числа, които нямат общи множители (взаимно прости, coprime).

Несиметрично криптиране с RSA алгоритъм

*s= v*t , където v=5 и t=17 са* прости числа

φ(s) =(v-1)·(t-1))

r =u^-1 (mod φ(s)), където u>1 & u ⊥ φ(s)

s = 85, u = 7, r = 55

Ася има: private key - *R(s, r)*

Боби има от Ася: public key - *U(s, u)*

Права задача:

Боби изпраща **тайно съобщение** *C* до Ася, където *C= f(U, m)* е криптираното съобщение *m. m* = 42 (Смисълът на живота :)

C = m^u mod (s) , C = 42^7 mod(85) = 83

Ася **получава** кодираното съобщението *83*, единствено тя знае числото *55* с което ще разкодира съобщението

m = C^r mod (s), m = 83^55 mod(85) = 42

Подпис с RSA алгоритъм

Ася има *R(s = 85, r = 55)*
Валя има *U(s = 85, u = 7)*

Обратна задача:
Ася иска да изпрати на Валя **смисъла на живота**, но Валя трябва да е сигурна, че съобщението е от Ася. Ася праща
M(m, sig)
m = 42 (съобщение)
sig = *m^r mod (s), sig = 42^55 mod(85) = 83 (подпис)*

Валя получава смисъла на живота *M(m = 42, sig = 83)* и прави проверка.
C = sig^u mod(s), C = 83^7 mod(85) = 42 ⇔ m = 42
Ако *C* е равно на *m*, писмото е подписано с ключа на Ася.

Hash Function

Ася има банкова сметка N: 2381, но всеки път като превежда пари прави грешки.

Банката добавя още една цифра към сметката на Ася:

Hash function h(N) = (N[0] + N[1] + N[2] + N[3]) mod 10 =

H = (2 + 3 + 8 + 1) mod 10 = 14 mod 10 => 4

Новата сметка на Ася е 23814.

2381 и 3281 => колизия (collision конфликт)

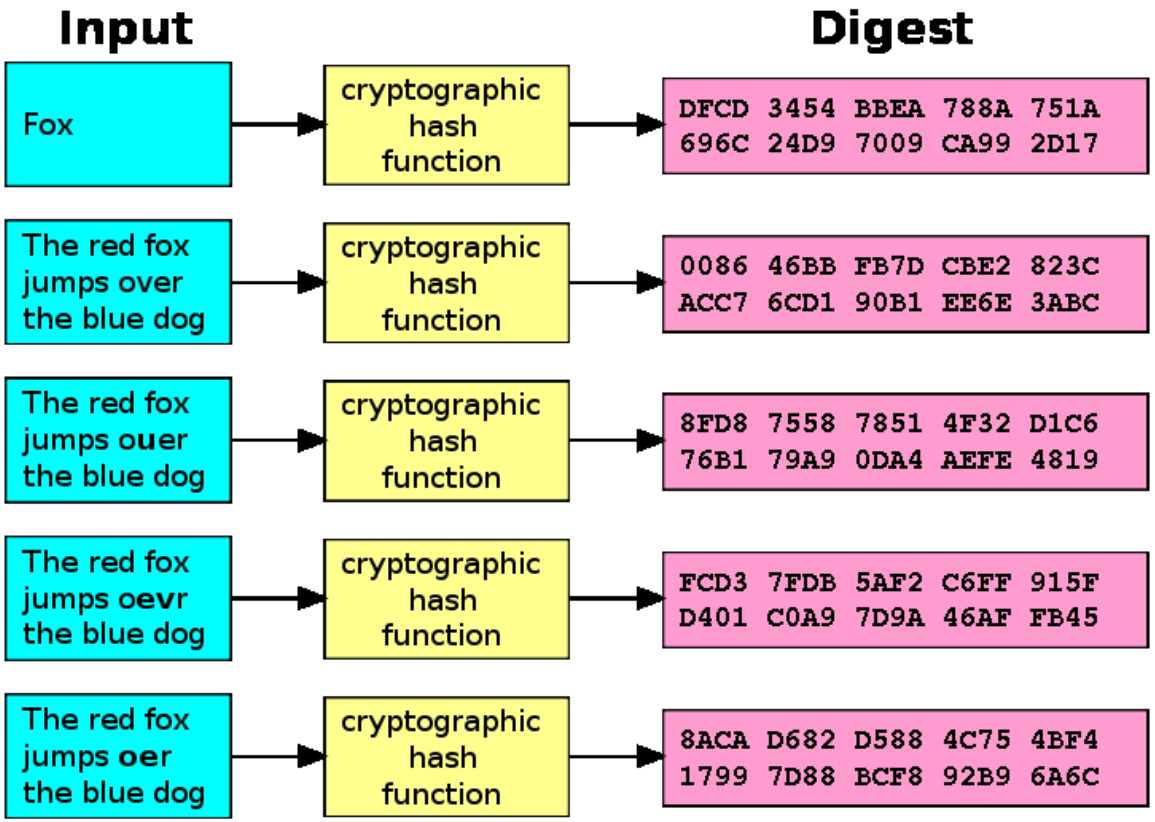
Криптираща хеш функция голяма изчислителна мощ, за да се намерят колизии. h(m1) ≠ h(m2);

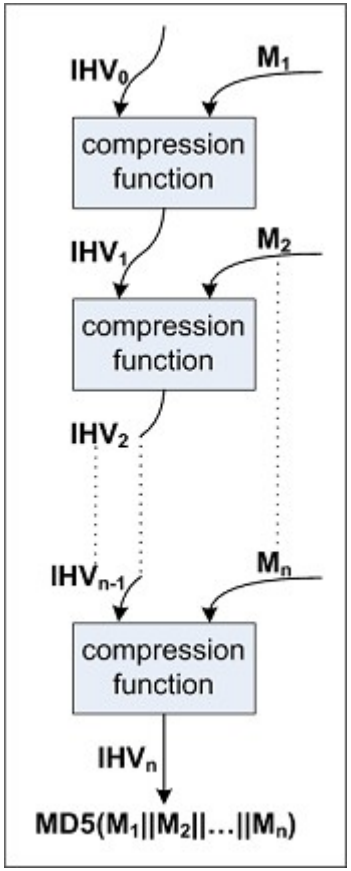
Birthday problem?!

MD5, SHA1 хеш функции

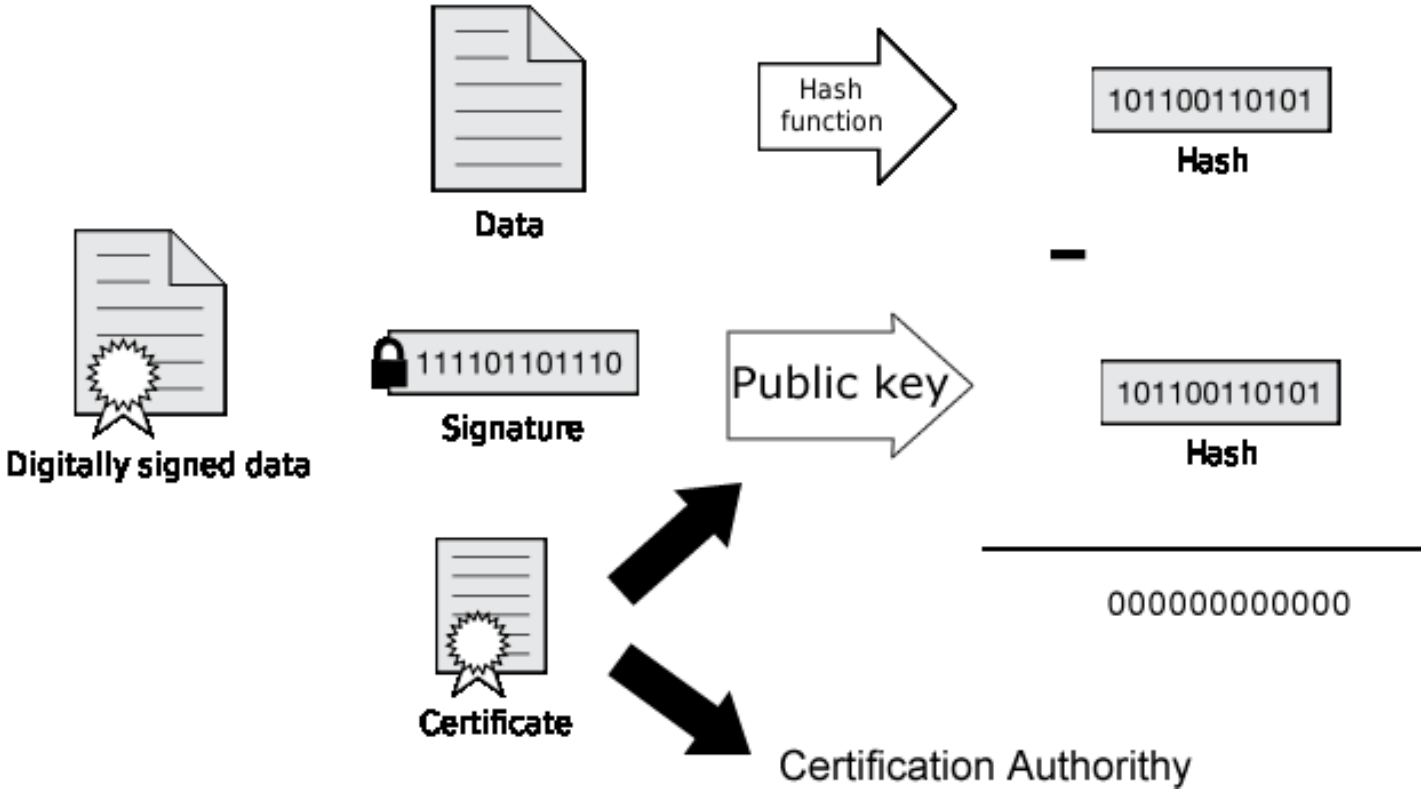
MD5 – 128 bits

SHA1 – 160 bits





Проверка


Data
Hash function
101100110101
Hash
-
Digitally signed data
111101101110
Signature
Public key
101100110101
Hash
000000000000
Certificate
Certification Authorithy