

Sicurezza Informatica

Firma Digitale

DSA

ECDSA

Digital Signature Standard (DSS)

- Modifica ingegnosa dello schema di firme El Gamal
- Proposto nell'agosto del 1991 dal NIST
 - Digital Signature Standard (DSS)
 - Digital Signature Algorithm (DSA)
- Firme corte, buone per smart card
 - 160x2, 224x2, 256x2 bit
- Sicurezza basata sull'intrattabilità del problema del logaritmo discreto
- La verifica è più lenta di quella RSA

Versioni DSS

- Proposto nell'agosto del 1991 dal NIST (FIPS 186)
 - Digital Signature Algorithm (DSA)
 - Digital Signature Standard (DSS)
- Revisioni minori, in seguito a critiche, nel 1993 (FIPS 186-1)
- Rivisto nel 2000 (FIPS 186-2). Specifica altri 2 metodi:
 - Elliptic Curve Digital Signature Algorithm (ECDSA)
 - RSA (ANSI X9.31, PKCS1 v1.5 e PSS)
- Rivisto nel giugno 2009 (FIPS 186-3)
 - Incrementa lunghezza delle firme DSS
- Rivisto nel luglio 2013 (FIPS 186-4)

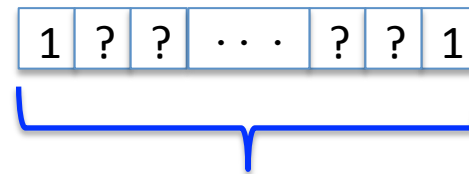
Key Generation

1. Generate a prime p with $2^{1023} < p < 2^{1024}$.
2. Find a prime divisor q of $p - 1$ with $2^{159} < q < 2^{160}$.
3. Find an element α with $\text{ord}(\alpha) = q$, i.e., α generates the subgroup with q elements. $\alpha^q \equiv 1 \pmod{q}$
4. Choose a random integer d with $0 < d < q$.
5. Compute $\beta \equiv \alpha^d \pmod{p}$.

$$k_{pub} = (p, q, \alpha, \beta)$$

$$k_{pr} = (d)$$

d appartiene a \mathbb{Z}_q^*



b bit

Primo t di b bit tale
che $2^{b-1} < t < 2^b$

Lo standard prevede anche altre combinazioni di p e q . L'algoritmo di generazione chiavi deve essere adattato in maniera opportuna

p	q	Signature
1024	160	320
2048	224	448
3072	256	512

Generazione di p e q

Il metodo suggerito dal NIST è differente

La procedura è ripetuta fino quando si trova la coppia (p,q)

```
find prime  $q$  with  $2^{159} < q < 2^{160}$  using the Miller–Rabin algorithm
FOR  $i = 1$  TO 4096
    generate random integer  $M$  with  $2^{1023} < M < 2^{1024}$ 
     $M_r \equiv M \pmod{2q}$ 
     $p - 1 \equiv M - M_r$  (note that  $p - 1$  is a multiple of  $2q$ .)
    IF  $p$  is prime (use Miller–Rabin primality test)
        RETURN ( $p, q$ )
```

Sottraendo M_r da M otteniamo un valore che è multiplo di $2q$
 $M - M_r = t \cdot 2 \cdot q$

Lo standard FIPS 186-4 indica vari modi per generare i primi p e q
Lo standard fornisce anche delle procedure per verificare che i
primi generati rispettino i requisiti richiesti

1. Check that the (L, N) pair is in the list of acceptable (L, N) pairs) (see Section 4.2). If the pair is not in the list, then return **INVALID**.
2. If $(seedlen < N)$, then return **INVALID**.
3. $n = \lceil L / outlen \rceil - 1$.
4. $b = L - 1 - (n * outlen)$.
5. Get an arbitrary sequence of $seedlen$ bits as the *domain_parameter_seed*.
6. $U = \mathbf{Hash}(\text{domain_parameter_seed}) \bmod 2^{N-1}$.
7. $q = 2^{N-1} + U + 1 - (U \bmod 2)$.
8. Test whether or not q is prime as specified in Appendix C.3.
9. If q is not a prime, then go to step 5.
10. $offset = 1$.
11. For $counter = 0$ to $(4L - 1)$ do
 - 11.1 For $j = 0$ to n do

$$V_j = \mathbf{Hash}((\text{domain_parameter_seed} + offset + j) \bmod 2^{seedlen}).$$
 - 11.2 $W = V_0 + (V_1 * 2^{outlen}) + \dots + (V_{n-1} * 2^{(n-1)*outlen}) + ((V_n \bmod 2^b) * 2^{n*outlen}).$
 - 11.3 $X = W + 2^{L-1}$. Comment: $0 \leq W < 2^{L-1}$; hence, $2^{L-1} \leq X < 2^L$.
 - 11.4 $c = X \bmod 2q$.
 - 11.5 $p = X - (c - 1)$. Comment: $p \equiv 1 \pmod{2q}$.
 - 11.6 If $(p < 2^{L-1})$, then go to step 11.9.
 - 11.7 Test whether or not p is prime as specified in Appendix C.3.
 - 11.8 If p is determined to be prime, then return **VALID** and the values of p, q and (optionally) the values of *domain_parameter_seed* and *counter*.
 - 11.9 $offset = offset + n + 1$. Comment: Increment *offset*; then, as part of the loop in step 11, increment *counter*; if $counter < 4L$, repeat steps 11.1 through 11.8.
12. Go to step 5.

Procedura NIST

L numero di bit di p

N numero di bit di q

Dimensione output

Hash $\geq N$

Possibili scelte

$L = 1024, N = 160$

$L = 2048, N = 224$

$L = 2048, N = 256$

$L = 3072, N = 256$

Prima scelta definita
in FIPS 186-1 e 186-2

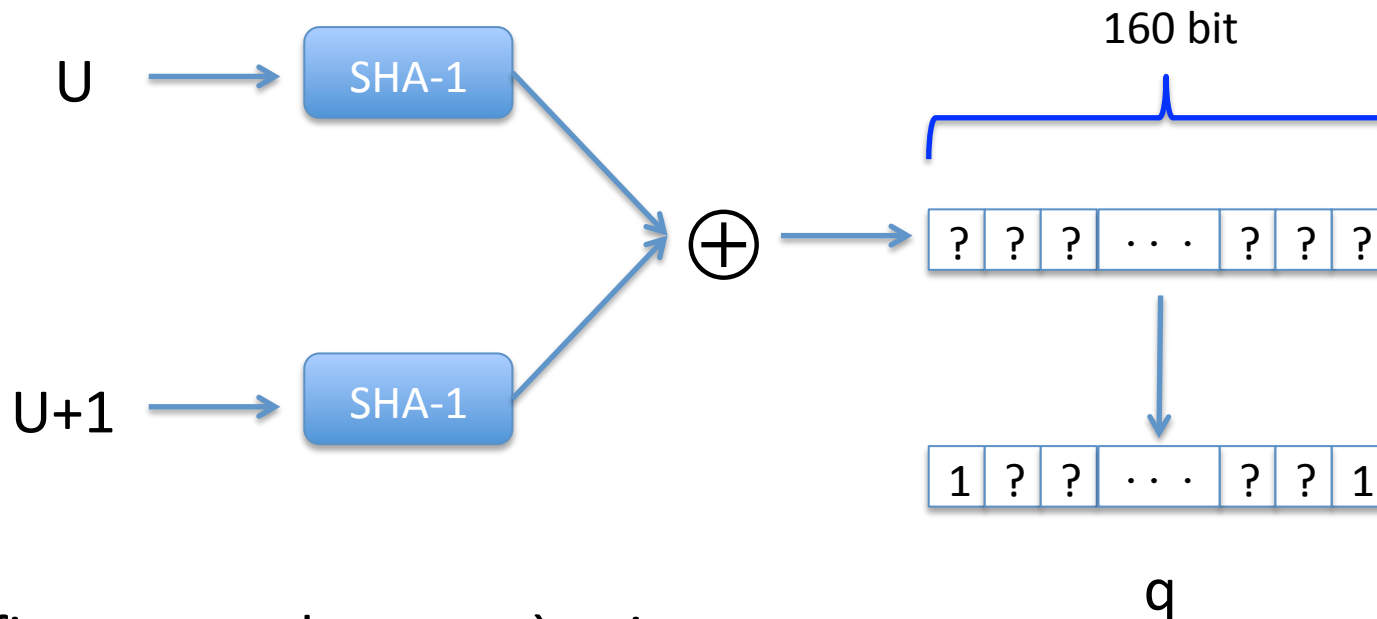
Ultime tre scelte
aggiunte in FIPS 186-3

11.2 - 11.8 simile al codice
della slide precedente

Generazione di q in FIPS 186-1 e 186-2

Scegli a caso un valore U di almeno 160 bit

U è trasformato in q

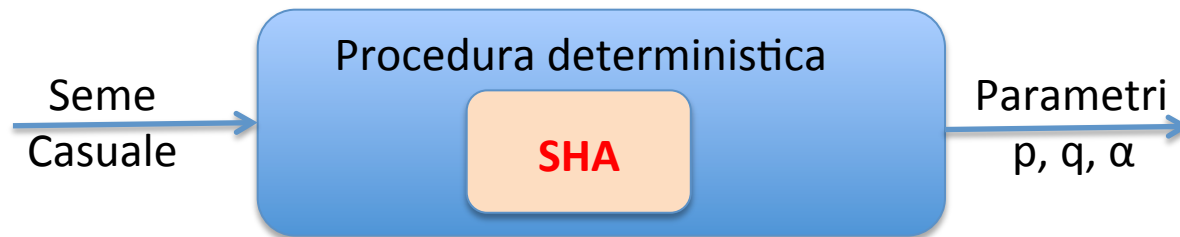


Ripeti fino a quando q non è primo

Perché nella generazione dei parametri si usa una funzione hash?

Generazione parametri DSA (NIST)

- Nelle specifiche NIST
 - FIPS 186-1, 186-2, 186-3 e 186-4
- i parametri sono generati applicando una procedura deterministica con input un seme casuale
- Il seme casuale è un testimone (*certificato*) della validità (*bontà*) dei parametri
 - Sarà difficile scegliere i parametri con una backdoor
 - Come determiniamo il seme che genera i parametri scelti?



Generazione di α

- Input: due primi p e q tali che q divide $p-1$
 - Output: il generatore di \mathbb{Z}_q^*
1. Scegli un elemento a caso g in \mathbb{Z}_p^*
 2. Calcola $\alpha \equiv g^{(p-1)/q} \pmod{p}$
 3. Se $\alpha \neq 1$, restituisci α , altrimenti riparti da 1.

Probabilità di successo

- Se g è un generatore allora $g^{(p-1)/q} \not\equiv 1 \pmod{p}$
 - Il numero di generatori per un modulo primo p è $\phi(\phi(p)) = \phi(p-1)$
 - Risulta $\phi(p) > p/(6 \ln \ln(p))$ per $p > 4$
 - Quindi $\phi(\phi(p)) = \phi(p-1) > (p-1)/(6 \ln \ln(p-1))$
 - Probabilità successo \geq Probabilità che g (scelto a caso) è generatore $> 1/(6 \ln \ln(p-1))$
 - Numero medio di iterazioni $< 6 \ln \ln(p-1)$

512 bit	$6 \cdot \ln \ln(2^{512}) \approx 35,23$
1024 bit	$6 \cdot \ln \ln(2^{1024}) \approx 39,38$
2048 bit	$6 \cdot \ln \ln(2^{2048}) \approx 43,54$
2048 bit	$6 \cdot \ln \ln(2^{3072}) \approx 45,98$

Firma DSA

DSA Signature Generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $r \equiv (\alpha^{k_E} \bmod p) \bmod q$.
3. Compute $s \equiv (SHA(x) + d \cdot r) k_E^{-1} \bmod q$.

La firma è (r,s)

SHA funzione hash che dipende dalla *versione* dello standard

In seguito, dettagli su quale funzione hash utilizzare

Aspetti computazionali

Calcolo di r: elevamento a potenza modulare, k_E di 160 bit, in media sono necessarie

1,5x160=240 operazioni tra elevamenti al quadrato (160) e moltiplicazioni (80)

Calcolo di s: operazioni con operandi di 160 bit.

r può essere precalcolato

L'operazione più dispendiosa è il calcolo di k_E^{-1}

Verifica DSA

DSA Signature Verification

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot SHA(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$v \begin{cases} \equiv r \bmod q \implies \text{valid signature} \\ \not\equiv r \bmod q \implies \text{invalid signature} \end{cases}$$

Aspetti computazionali

Calcolo di w , u_1 e u_2 : operazioni con operandi di 160 bit.

Calcolo di v : due elevamenti a potenza modulare con esponenti di 160 bit
una moltiplicazione

Perché la verifica funziona?

$$\begin{aligned} (a) \quad & r \equiv (\alpha^{k_E} \bmod p) \bmod q. \\ & s \equiv (SHA(x) + d \cdot r) k_E^{-1} \bmod q. \end{aligned}$$

$$\begin{aligned} (b) \quad & w \equiv s^{-1} \bmod q. \\ & u_1 \equiv w \cdot SHA(x) \bmod q. \\ & u_2 \equiv w \cdot r \bmod q. \end{aligned}$$

$s \equiv (SHA(x) + d r) k_E^{-1} \bmod q$ è equivalente a $k_E \equiv s^{-1} SHA(x) + d s^{-1} r \bmod q$.

usando (b) possiamo riscrivere $k_E \equiv s^{-1} SHA(x) + d s^{-1} r \bmod q$. come $k_E \equiv u_1 + d u_2 \bmod q$.

da cui $\alpha^{k_E} \bmod p \equiv \alpha^{u_1 + d u_2} \bmod p$

Poiché $\beta = \alpha^d$, possiamo riscriverla come $\alpha^{k_E} \bmod p \equiv \alpha^{u_1} \beta^{u_2} \bmod p$.

Riducendo entrambi i membri modulo q , otteniamo

$$(\alpha^{k_E} \bmod p) \bmod q \equiv (\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q.$$

Dalla (a) $r \equiv (\alpha^{k_E} \bmod p) \bmod q$.

v , durante la verifica è calcolato come $v \equiv (\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q$.

L'espressione $(\alpha^{k_E} \bmod p) \bmod q \equiv (\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q$.

è identica alla condizione per verificare se la firma è valida $r \equiv v \bmod q$

DSA

- L'algoritmo di firma utilizza funzioni hash SHA
 - SHA-1 FIPS 180-4
 - output di 160 bit
 - SHA-224/256/384/512 Indicate con il nome SHA-2
 - output di 224/256/384/512 bit
- Se l'output è più lungo del necessario, allora è troncato opportunamente
- SHA-1 era usato in FIPS 186-1 e FIPS 186-2
 - Conservato per compatibilità con il passato
- SHA-224/256/384/512 sono state aggiunte in FIPS 180-3

Sicurezza di DSA

- Stessi argomenti usati per valutare la sicurezza dello schema di firma El Gamal
 - La sicurezza si basa sulla difficoltà di risolvere DLP (Discrete Logarithm Problem)
 - Risolvendo DLP si può estrarre d da β
 - Bisogna scegliere i parametri in maniera tale che DLP sia difficile da risolvere
- Non si può riutilizzare la chiave effimera

p	q	hash output (min)	security levels
1024	160	160	80
2048	224	224	112
3072	256	256	128

Parametri globali ed individuali

$$k_{pub} = (p, q, \alpha, \beta)$$

$$k_{pr} = (d)$$

- I parametri (p, q, α) possono essere comuni per un gruppo di utenti
 - Un'autorità fidata sceglie (p, q, α)
 - Ogni singolo utente U sceglie d_U e pubblica $\beta_U = \alpha^{d_U}$

Implementazione nel 1993 su smart card

	DSA	RSA
precomputazioni	14 sec	
firma	0.3 sec	15 sec
verifica	16 sec	1.5 sec

	DSA 1024	RSA 1024	RSA 2048
Firma	0.45	1.48	6.05
Verifica	0.52	0.07	0.16
Firma con precomputazione	0.42		

Libreria Crypto++ 5.6.0
Intel Core 2 1.83GHz
Windows Vista in 32-bit mode
Marzo 2009

Tempi in millisecondi

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Variante di DSA
- Utilizza un sottogruppo *generato* dai punti su una curva ellittica
 - Abbiamo bisogno di un punto della curva e del suo ordine
- Firme più compatte rispetto a DSA conservando lo stesso livello di sicurezza
 - Firme DSA di 360 bit hanno un livello di sicurezza di 80 bit pari a firme RSA di 1024 bit

ECDSA - Key Generation

1. Use an elliptic curve E with
 - modulus p
 - coefficients a and b
 - a point A which generates a cyclic group of prime order q
 2. Choose a random integer d with $0 < d < q$.
 3. Compute $B = dA$.
- The keys are now:
- $$k_{pub} = (p, a, b, q, A, B)$$
- $$k_{pr} = (d)$$

La curva E è definita in FIPS 186-4. La curva è descritta da una tupla

$(q, FR, a, b, \{, domain_parameter_seed\}, G, n, h)$

Curve Ellittiche per ECDSA

- $(q, FR, a, b, \{, domain_parameter_seed\}, G, n, h)$
 - q ordine del sottogruppo generato dall'elemento primitivo G
 - a e b sono i coefficienti della curva
 - FR indica la base usata per descrivere l'aritmetica nel gruppo
 - Come interpretare una stringa di bit
 - $domain_parameter_seed$
 - Seme opzionale, è presente se la curva è stata generata in una maniera verificabile
 - n è l'ordine del sottogruppo generato da G
 - h è il cofattore ($\#E = n \cdot h$)

Tipi di Curve

- Curve su campi primi $GF(p)$
 - Identificate con P-xxx
- Curve su campi binari $GF(2^m)$
 - Identificate con B-xxx
- Curve di Koblitz
 - Identificate con K-xxx

xxx indica la dimensione in bit del primo p

Parametri NIST consigliati

Bit Length of n	Prime Field	Binary Field
161 – 223	$\text{len}(p) = 192$	$m = 163$
224 – 255	$\text{len}(p) = 224$	$m = 233$
256 – 383	$\text{len}(p) = 256$	$m = 283$
384 – 511	$\text{len}(p) = 384$	$m = 409$
≥ 512	$\text{len}(p) = 521$	$m = 571$

Table 1: ECDSA Security Parameters

Bit length of n	Maximum Cofactor (h)
160 - 223	2^{10}
224 - 255	2^{14}
256 - 383	2^{16}
384 - 511	2^{24}
≥ 512	2^{32}

Curva P-256

```
 $p =$  1157920892103562487626974469494075735300861434152903141955  
33631308867097853951  
 $n =$  115792089210356248762697446949407573529996955224135760342  
422259061068512044369  
 $SEED =$  c49d3608 86e70493 6a6678e1 139d26b7 819f7e90  
 $c =$  7efba166 2985be94 03cb055c 75d4f7e0 ce8d84a9 c5114abc  
af317768 0104fa0d  
 $b =$  5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6  
3bce3c3e 27d2604b  
 $G_x =$  6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0  
f4a13945 d898c296  
 $G_y =$  4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece  
cbb64068 37bf51f5
```

$c = \text{SHA-1}(SEED)$

$a = 1$
 $b^2c \equiv -27 \pmod{p}$

$h=1$, quindi q non è necessario il sottogruppo coincide con il gruppo

Curva verificabile

ECDSA - Firma/Verifica

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $R = k_E A$.
3. Let $r = x_R$. $R = (x_R, y_R)$
4. Compute $s \equiv (h(x) + d \cdot r) k_E^{-1} \bmod q$.

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot h(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $P = u_1 A + u_2 B$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$x_P \begin{cases} \equiv r \bmod q \implies \text{valid signature} \\ \not\equiv r \bmod q \implies \text{invalid signature} \end{cases}$$

in DSA

$$v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$$

Sicurezza ECDSA

- Stessi argomenti usati per valutare la sicurezza dello schema di firma El Gamal e DSA
 - La sicurezza si basa sulla difficoltà di risolvere DLP (Discrete Logarithm Problem) in un gruppo generato da una curva ellittica
 - Risolvendo DLP si può estrarre d da $B = d \cdot A$
 - Attualmente, il miglior algoritmo richiede tempo proporzionale a $O(q^{1/2})$
 - Per prevenire alcuni tipi di attacchi, durante la fase di verifica è necessario controllare che r ed s appartengano a $\{1, 2, \dots, q\}$
 - La chiave effimera k_E non deve essere riutilizzata
 - Stesso attacco di El Gamal e DSS

PS3 e ECDSA

Dettagli su <https://fail0verflow.com/>

- Sony utilizzava una firma ECDSA per proteggere la PS3
 - Il software è firmato con ECDSA
- La chiave effimera è sempre la stessa

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
              // guaranteed to be random.  
}
```

<https://xkcd.com/221/>

La firma digitale in Italia

- Un documento sottoscritto con firma digitale ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma
 - Decreto Legislativo 7 marzo 2005, n. 82 **Codice dell'Amministrazione Digitale**, e modifiche successive
 - Decreto Legislativo 26 agosto 2016, n. 179
- Le prime *norme* sulla firma digitale risalgono al marzo 1997

Legge 15/03/1997 N. 59, Art. 15, comma 2

Gli atti, dati e **documenti formati** dalla pubblica amministrazione e dai privati **con strumenti informatici** o telematici, **i contratti stipulati nelle medesime forme**, nonché la loro archiviazione e trasmissione con strumenti informatici **sono validi e rilevanti a tutti gli effetti di legge**; i criteri di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con **specifici regolamenti da emanare**, entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2 della legge 23 agosto 1988 n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei Deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni.

Regolamento **Decreto del Presidente della Repubblica 10 novembre 1997, n. 513**

Regole tecniche **Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999**

	Definizione	Valore probatorio	Esempi
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	<i>Pin, firma biometrica</i>
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i> tranne che per i contratti immobiliari	<i>Firma su tablet</i>
Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	<i>Smart-card, token</i>
Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	<i>Smart-card, token</i>

Osservatorio Fatturazione Elettronica e Dematerializzazione

Firme previste dal CAD

Codice dell'Amministrazione Digitale

- **Firma elettronica**

- l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

- username e password utilizzate come credenziali di accesso
- pin associato ad un bancomat

- **Firma elettronica avanzata**

- Ottenuta dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione penna,...) della firma tramite penna elettronica



Firme previste dal CAD

Codice dell'Amministrazione Digitale

- **Firma elettronica qualificata**

- Firma Elettronica Avanzata apposta attraverso strumenti che permettono l'identificazione certa del firmatario e la certificazione dell'integrità dei dati del documento firmato.
- L'apposizione della firma elettronica qualificata avverrà tramite un “dispositivo sicuro per la creazione della firma” (e.g., token usb o smart card).

- **Firma digitale**

- Firma elettronica qualificata basata su coppia di chiavi crittografiche

Diffusione firma digitale in Italia

Dati Agenzia Digitale per l'Italia

<http://www.agid.gov.it/>

Anno	Certificati qualificati di firma digitale attivi	Percentuale certificati di firma remota	Marche temporali emesse
2014	5.319.800	-	-
2015	8.104.615	55% (stima)	584.610.193
2016	11.170.257	60%	
Data rilevazioni: maggio 2014, luglio 2015, aprile 2016			

Firma Digitale Remota

Tipologia di firma digitale, accessibile via rete per la quale la chiave privata del firmatario viene conservata, da parte di un certificatore accreditato, assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM - Hardware Security Module).




I verbali di esame su ESSE3 sono firmati dal docente tramite Firma Digitale Remota

Dispositivi di Firma Remoti






- Hardware che firma i documenti su delega dell'utente
- I dispositivi di firma devono essere certificati da un Organismo di Certificazione della Sicurezza Informatica (OCSI)
- In Italia tale organismo è l'ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) del Ministero dello Sviluppo Economico
 - <http://www.ocsi.isticom.it/>

HMS accertati (novembre 2016)

<http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/dispositivi-accertati>



Organismo di Certificazione della Sicurezza Informatica



home | contatti | cerca | mappa

ORGANISMO

LABORATORI

ASSISTENTI

FORMAZIONE

DOCUMENTAZIONE

ELENCHI CERTIFICAZIONI

DISPOSITIVI DI FIRMA

- Procedura di Accertamento
- Dispositivi accertati
- In corso di accertamento

EVENTI



DOMANDE FREQUENTI

Dispositivi di firma per i quali è stato rilasciato l'Attestato di Conformità

Sono stati rilasciati da questo Organismo Accertamenti di Conformità per i seguenti dispositivi di firma.

[Espandi tutto](#) | [Chiudi tutto](#)

CoSign v8.2

Fornitore: **ARX**
Data emissione attestato: **12 settembre 2016**
Attestato di Conformità:  [ac_rda_cosign_82_v1.0.pdf](#)
Traguardo di Sicurezza:  [st_arx_cosign_82_v2.6.pdf](#)

nShield HSM Family v11.72.02

+

CoSign v7.5

+




CoSign v7.1

+

Luna® PCI Configured for Use in Luna® SA 4.5.1 (RF)

+

Luna® PCI Configured for Use in Luna SA 4.1

Fornitore: **SafeNet**
Data emissione attestato: **12 dicembre 2012**
Attestato di Conformità:  [ac_rda_safenet_v1.0.pdf](#)
Note interpretative:  [note_rda_safenet_v10.pdf](#)
Traguardo di Sicurezza:  [st_luna_pci_cr-2386_11.pdf](#)

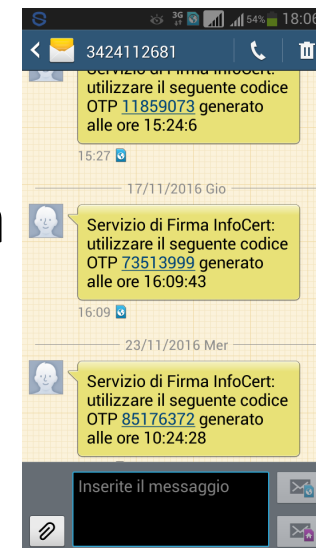
-

Firma Digitale Remota

- Il firmatario è identificato dal servizio remoto che autorizza la firma del valore hash del documento
- Il valore hash è firmato dall'HSM **Dispositivo di Firma**
- Il firmatario è identificato tramite
 - PIN
 - Token OTP **OTP: One Time Password**
 - Riconoscimento grafometrico della firma autografa
 - Token OTP + PIN di Firma (come per ESSE3)

Come ottenere un OTP?

- generarlo con token con display
 - L'utente deve ricopiarlo in un'apposita casella di testo
- generarlo con token usb
 - Automaticamente inserito nella casella di testo
- riceverlo tramite SMS (tipo ESSE3)
 - L'utente deve ricopiarlo in un'apposita casella di testo



Generarlo con un'app

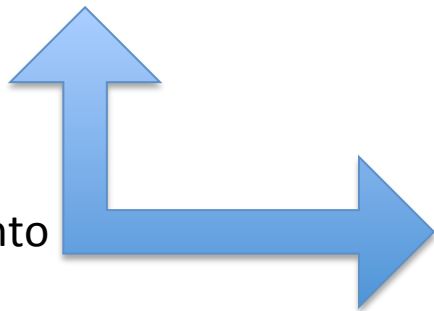
Firma Remota con Aruba



Autenticazione utente



Scelta documento



Formati di Firma

- La normativa italiana prevede tre formati di firma (*busta crittografata*)
- I formati appartengono alla famiglia di formati di firme digitali AdES (Advanced Electronic Signature) improntata sugli standard ETSI
- CAdES
 - Cryptographic Message Syntax AdES
- PAdES
 - PDF AdES
- XAdES
 - XML AdES

ETSI: European Telecommunications
Standards Institute

CAdES

- Permette di firmare qualsiasi tipo di file. Il file firmato ha estensione .p7m
- Il contenuto del file è visualizzabile (ed estraibile) solo attraverso idonei software in grado di *sbustare* il documento firmato
 - Sul sito dell'Agenzia per l'Italia Digitale si può trovare un elenco aggiornato dei software disponibili (www.digitpa.gov.it)
 - Sul sito è indicato anche un elenco di software per la verifica della firma digitale

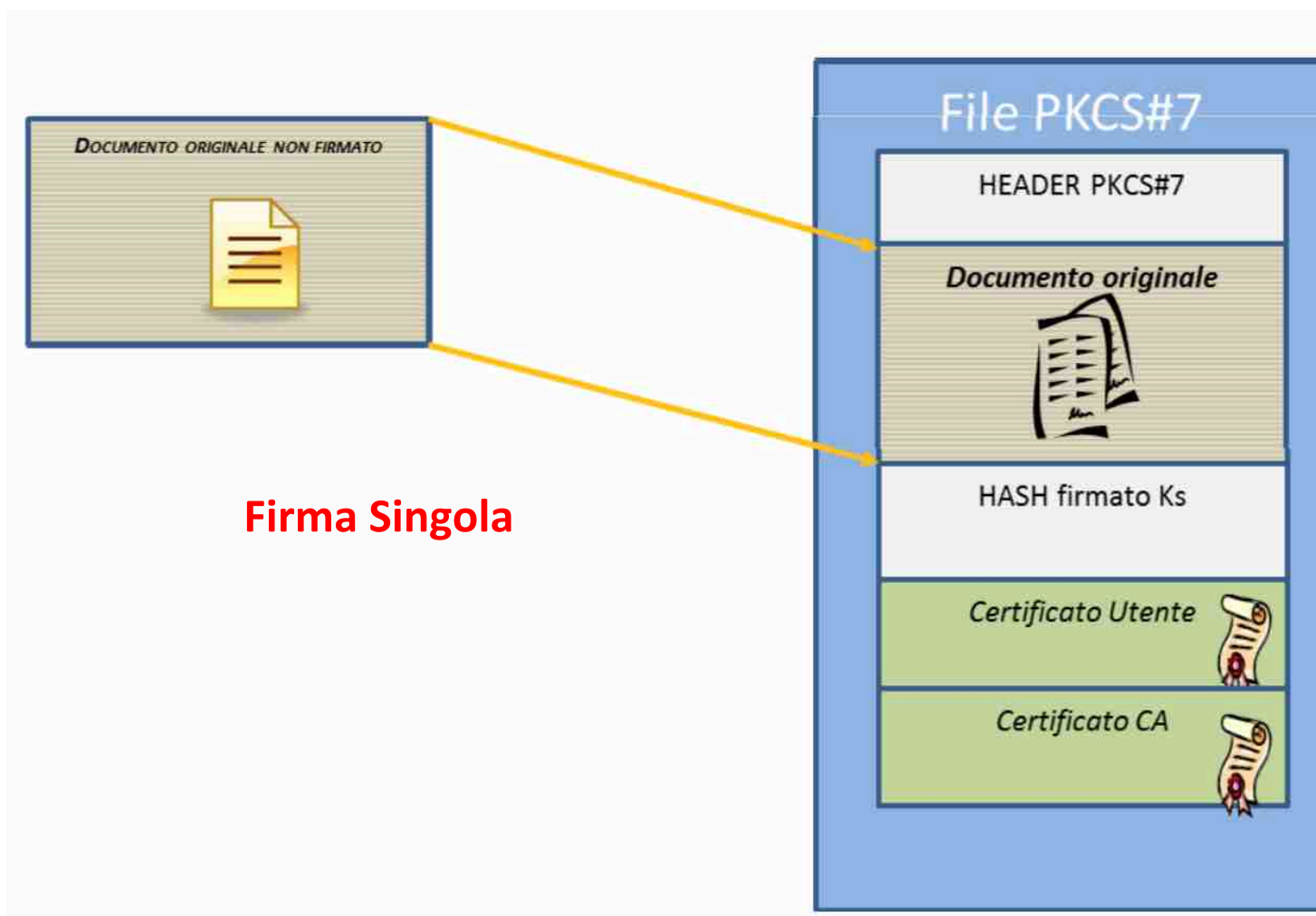
Software disponibili - novembre 2016

- [Digital Signature Service](#)
- [DigitalSign Reader](#)
- [Firma OK!](#)
- [PkNet](#)
- [DIKE](#)
- [Firma Certa](#)
- [DSTK](#)
- [View2Sign](#)
- [MnISignVerifier](#)

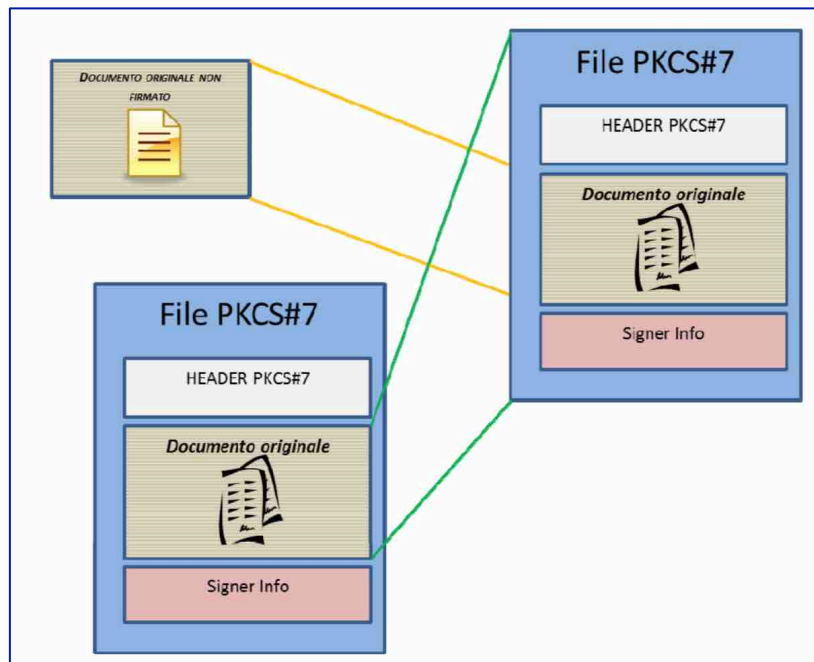
Software per verifica - novembre 2016

- [AgID](#)
 - applicazione DSS (Digital Signature Service) per la verifica di firme europee
- [Consiglio Nazionale del Notariato](#)
- [Infocert](#)
 - Verifica anche le firme PDF (PAdES)
- [DigitaSign Cloud](#)
 - Verifica anche le firme PDF (PAdES) e XAdES (XML), consente di aprire e verificare le Fatture PA con gli appropriati fogli di stile
- [Namirial](#)
 - Verifica anche le firme PDF (PAdES) e le firme basate su certificati rilasciati da certificatori qualificati stabiliti nell'Unione Europea

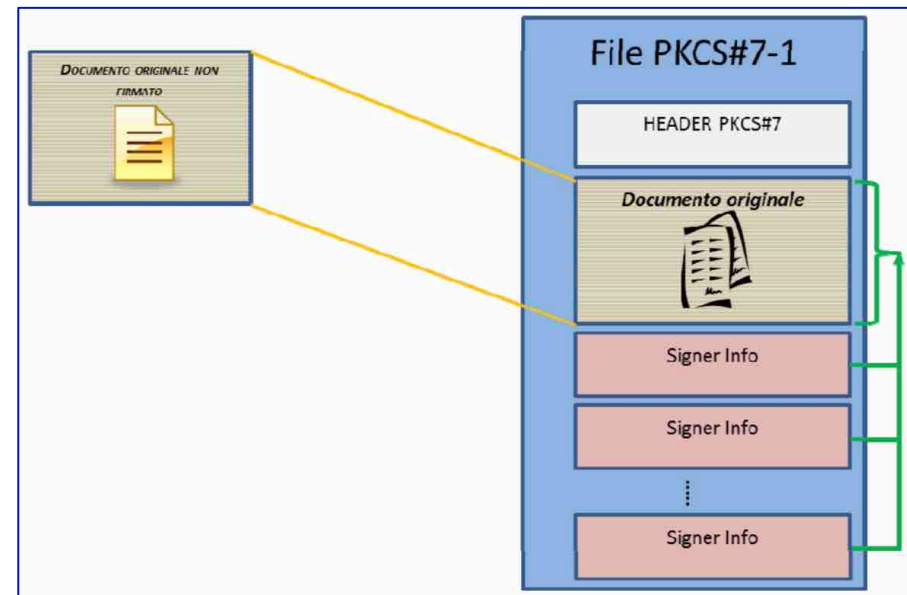
Formato CAdES **Firma Singola** basato su PKCS#7



Formato CAdES **Firma Multipla** basato su PKCS#7



Firma a matryoska



Firme congiunte

In entrambi i casi è presente un'unica versione del documento, che pertanto può solo essere oggetto di ulteriori firme digitali senza modificarne il contenuto

Formato PAdES

- Permette di firmare esclusivamente file in formato pdf
- Il file firmato (nomeOriginale_signed.pdf) potrà essere aperto con comuni lettori pdf
- La firma apposta potrà essere visibile o invisibile
- Si possono apporre firme ulteriori senza invalidare quelle precedenti
 - Il formato implementa la funzione della gestione delle versioni (versioning)



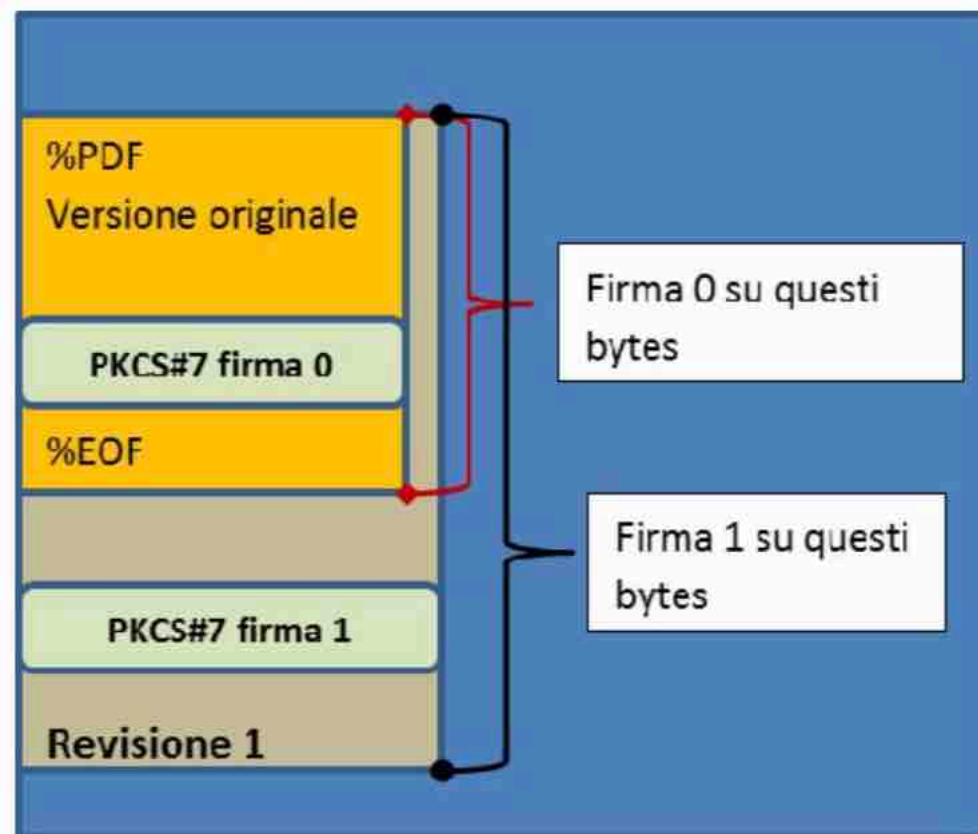
Firma PAdES

- La firma è inclusa nel file pdf

```
57 0 obj
<</F 132/Type/Annot/Subtype/Widget/Rect[39 109 146 212]/FT/Sig/DR<</
XObject<</FRM 55 0 R>>>>/T(Signature1)/V 49 0 R/P 2 0 R/AP<</N 56 0 R>>>>
endobj
```

Il documento originario firmato
è sempre incluso nel documento
finale

Si può produrre una nuova
versione del documento e
firmarla



Riferimenti

Christof Paar and Jan Pelzl
Understanding Cryptography
Capitolo 10 **Digital Signatures**
Paragrafi 4, 5 e 6

Centro Nazionale per l'Informatica nella Pubblica
Amministrazione (CNIPA)
Guida alla Firma Digitale, Versione 1.3, 2009

[http://www.agid.gov.it/agenda-digitale/
infrastrutture-architetture/firme-elettroniche](http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche)