Firma Digitale ed Elettronica

Crittografia, Normativa (CAD) e Applicazioni

Sistemi e Reti - Esame di Stato

25 febbraio 2026

Definizione Tecnica di Firma Digitale

In Italia, il **CAD (Codice dell'Amministrazione Digitale, D.Lgs. 82/2005)** definisce la Firma Digitale come un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche asimmetriche (una pubblica e una privata).

Garantisce tre requisiti tecnico-legali:

- **Autenticità:** Certezza matematica dell'identità del firmatario.
- **Integrità:** Immodificabilità del documento post-firma (garantita dall'uso di funzioni di *Hash*).
- **Non Ripudio:** Il firmatario non può disconoscere il documento, data l'esclusività della sua chiave privata.

Elettronica vs Digitale: La Normativa

Il Regolamento Europeo **eIDAS** e il **CAD** stabiliscono una chiara gerarchia:

Firma Elettronica (Semplice - FE)

Dati elettronici allegati ad altri dati per l'identificazione (es. PIN, firma scannerizzata). Ha **valore probatorio liberamente valutabile dal giudice**. Nessuna garanzia crittografica forte.

Firma Digitale (FD)

Sottoinsieme della Firma Elettronica Qualificata (FEQ). Usa un'infrastruttura PKI e un certificato emesso da una *Certification Authority* accreditata (es. AgID). Ha **pieno valore probatorio** (pari alla firma autografa).

Flusso della Firma Digitale

Scenario: Alice firma un contratto per Bob.

1. **Hashing:** Il software di Alice calcola il *Digest* (impronta) del PDF tramite un algoritmo (es. SHA-256).
2. **Cifratura:** Alice cifra il *Digest* usando la sua **Chiave Privata**. Questo blocco cifrato è la Firma.
3. **Trasmissione:** Alice invia a Bob: PDF + Firma + Certificato Pubblico.
4. **Verifica:** Bob ricalcola l'Hash del PDF. Decifra la Firma con la **Chiave Pubblica** di Alice. Se i due Hash coincidono, la firma è integra e autentica.

Domande Aperte per l'Esame

1. Qual è il ruolo della funzione di *Hash* nella Firma Digitale? Motivare perché si cifra il *digest* e non l'intero documento.

2. Confrontare Firma Elettronica e Firma Digitale ai sensi del CAD, spiegando la differenza di valore probatorio e di tecnologie sottostanti.

3. Descrivere il ruolo di una *Certification Authority (CA)*. In che modo il certificato digitale previene attacchi *Man-in-the-Middle*?

Esercizio Pratico: Crittografia Ibrida

Traccia

Un'azienda invia un progetto (PDF, 50 MB) a un Ente via Internet. L'Ente richiede quattro requisiti crittografici: **Autenticità, Integrità, Non Ripudio e Riservatezza**.

Richiesta: Descrivere il protocollo da adottare. Indicare in sequenza logica quali algoritmi (simmetrici/asimmetrici/hash) e quali chiavi (pubbliche/private di mittente/destinatario) usare per soddisfare i requisiti.