

FIRMA E CERTIFICATO DIGITALE

Testi di riferimento :

Dat@Game Hoepli - P.Camagni, R. Nikolassy
InfoChef Hoepli - P.Camagni, R. Nikolassy

Firma Digitale

La firma digitale è uno strumento che permette di firmare dei documenti **digitali**, al fine di renderli legalmente validi.

È il risultato di un procedimento crittografico che punta al raggiungimento delle seguenti **caratteristiche**:

- **AUTENTICITA'**: garantire e assicurare l'identità della persona che ha firmato il documento, imputandole la responsabilità dello stesso.
- **INTEGRITA'**: garantire la non modificabilità del documento dal momento della firma al momento dell'utilizzo.

Firma Digitale



ELENA



MARIO



Firma Digitale



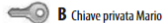
ELENA



MARIO



Cifratura



B Chiave privata Mario

Firma Digitale



ELENA



MARIO



Cifratura



 **B** Chiave privata Mario



**DOCUMENTO
FIRMATO**



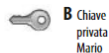
Firma Digitale



ELENA



MARIO




Decifratura



Cifratura



 **B** Chiave privata Mario

**DOCUMENTO
FIRMATO**



Firma Digitale



ELENA



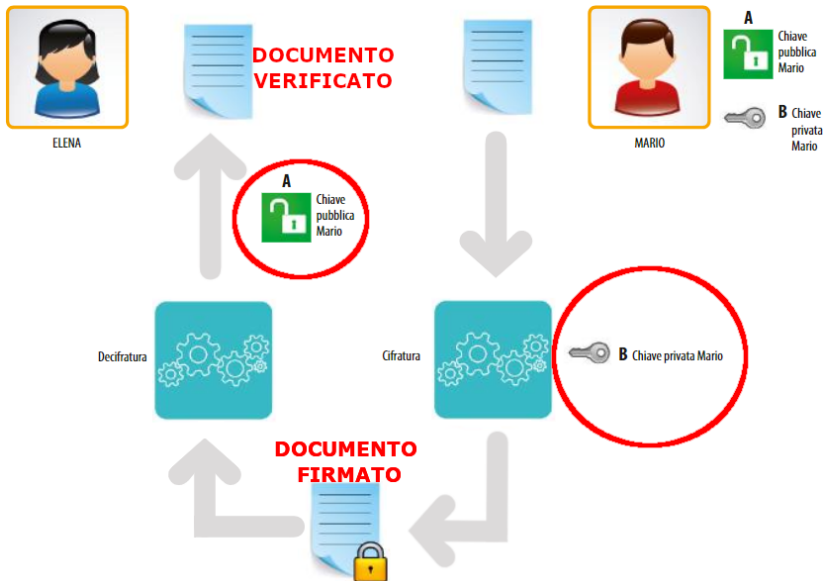
MARIO



**DOCUMENTO
FIRMATO**



Firma Digitale




Certificato Digitale



Certificato digitale

Il certificato digitale garantisce l'identità del mittente di un messaggio di posta elettronica o del proprietario di un sito Web. Vengono utilizzati soprattutto nel caso di **transazioni** economiche o per messaggi di **posta certificata**.

Certificato digitale

Il **certificato digitale**  è il corrispondente elettronico di un documento cartaceo. I certificati digitali vengono utilizzati sia per provare la propria **identità digitale**, sia per accedere a informazioni e servizi online di tipo riservato e vengono rilasciati da apposite autorità di certificazione che garantiscono l'identità dell'intestatario del sito Web.

Certificato Digitale

Come funziona il certificato digitale in pratica

La crittografia asimmetrica viene applicata al certificato digitale per renderlo uno strumento sicuro al fine di scambiare informazioni tra due computer. La **Certification Authority (CA)** è l'autorità che distribuisce i certificati digitali, ed è proprio a essa che dobbiamo rivolgerci per acquistarne uno. Quando la **CA** fornisce il certificato ne cifra le chiavi con una propria **chiave privata**: per decifrare il certificato sarà pertanto necessario possederne la corrispondente **chiave pubblica**.

Certificato Digitale

- ① Il **Client** richiede l'apertura di una connessione protetta al Server.
- ② Il **Server** risponde al Client inviandogli:
 - il proprio ID;
 - il nome della società per la quale è stato emesso il certificato;
 - il proprio common name, che contiene il nome del dominio per il quale il certificato è valido;
 - il periodo di validità del certificato;
 - il nome della CA che ha rilasciato il certificato;
 - **la propria chiave pubblica cifrata con la chiave privata della CA.**

Certificato Digitale

- ③ **Il Client verifica la validità dei dati che gli sono stati inviati dal Server e ne decifra la chiave pubblica utilizzando la chiave pubblica della CA.**
- ④ Il Client usa la chiave pubblica del Server appena ottenuta per cifrare e inviargli:
 - il proprio ID;
 - un ID di sessione (che permette al Server di distinguere un Client dagli altri).
- ⑤ Le presentazioni tra Client e Server sono finite, ora i due si conoscono e sono in grado di trasmettere e ricevere dati cifrati perchè si sono scambiati prima le chiavi per codificare la comunicazione.

Certificato Digitale

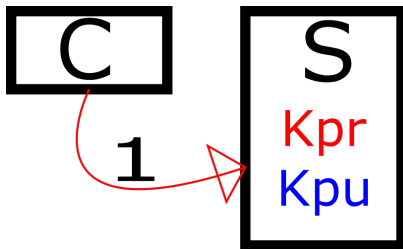
C

S
Kpr
Kpu

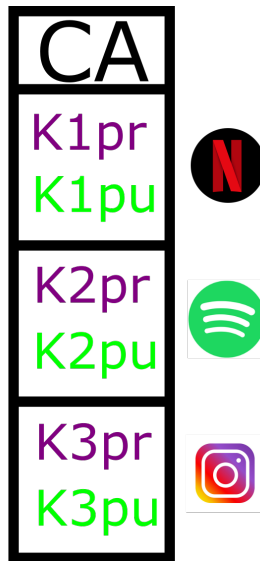
CA
K1pr
K1pu
K2pr
K2pu
K3pr
K3pu



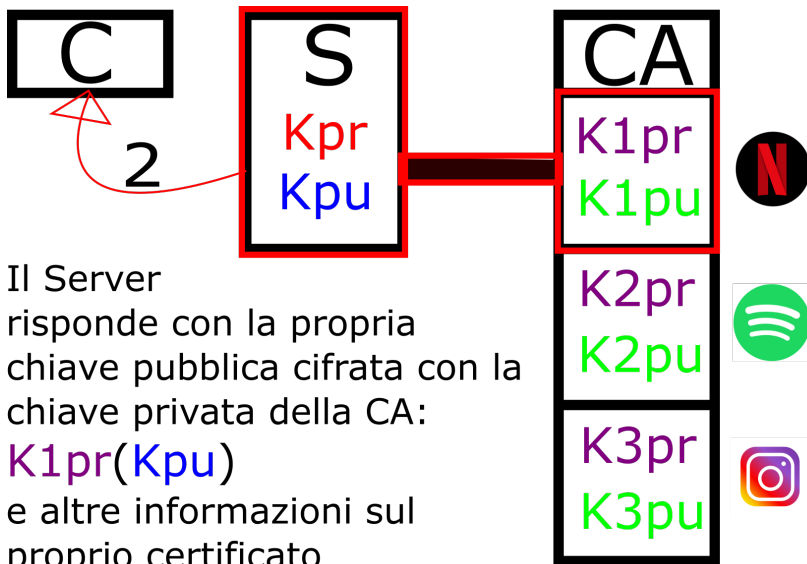
Certificato Digitale



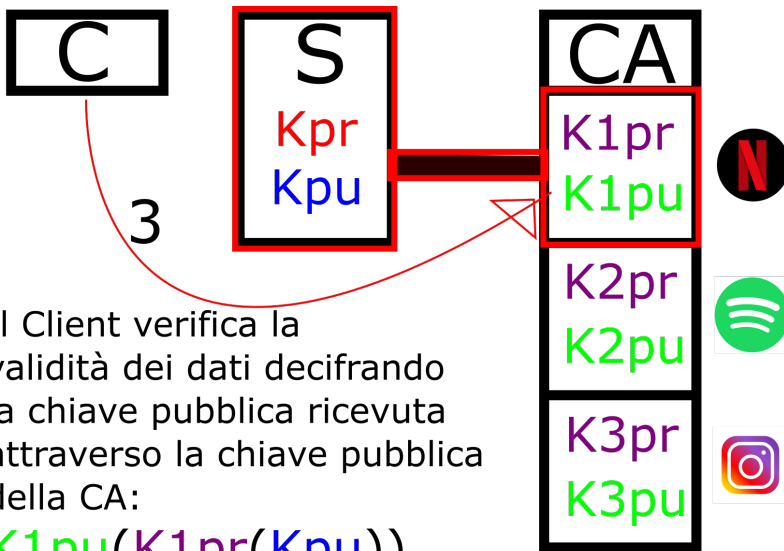
Il Client richiede l'apertura
di una connessione
protetta al Server.



Certificato Digitale



Certificato Digitale



Certificato Digitale

