Firma Digitale e Non

Clizio Merli

(Versione 3)

Indice

Prefazione

Sono anni che medito di scrivere un libro sulla firma digitale: grazie alla mia pigrizia atavica questo è per ora il modestissimo risultato. Se la mia speranza di una lunga vita si avvererà, forse le generazioni future avranno il privilegio (!?!) di leggere il libro completo. Per ora i poveri lettori devono accontentarsi di queste poche pagine, nella speranza, alla fine di una rapida lettura, di aver avuto finalmente la possibilità di capire meglio cosa significa la firma digitale, e con il rischio di essersi ulteriormente complicate le idee.

La prima versione di questo libretto risale al 2005. Dopo cinque anni di profonda meditazione ho aggiunto il capitolo relativo alla marca temporale (sei pagine), e dopo altri due ho ritoccato qua e la per tentare di chiarire, nel limite del possibile, gli arcani legati alle ultime normative europee e italiane (CAdES, PadES, XadES, TSR, TSD e altre chicche).

Comunque questo che state leggendo ha la pretesa di essere un piccolo contributo chiarificatore alla comprensione del mondo che ruota intorno alla firma digitale.

Da anni si parla ormai di questo argomento, e delle mirabilia annesse e connesse. Nella pratica, sino ad ora (anno 2011) gli unici effetti visibili al grosso pubblico, perlomeno in ambito Italiano, sono due: la chiavetta che si chiude nei browser navigando in Internet, segnalando in tal modo che si entra in "siti protetti" (da cosa ?); le SmartCard e le chiavette crittografiche USB rilasciate dagli enti certificatori accreditati e utilizzati dalle aziende prevalentemente per lo scambio con l'Agenzia delle Entrate.

Per le aziende non è cambiato molto rispetto alle prime SmartCard rilasciate nei primi anni 2000 dalle Camere di Commercio per la firma digitale aziendale delle dichiarazioni dei redditi, (quelle che erano finite, quasi tutte, nelle casseforti dei commercialisti insieme alle relative password protettive - PIN). Ben poca cosa per una innovazione che avrebbe permesso, almeno potenzialmente, di eliminare gran parte della carta all'interno di organizzazioni, aziende, enti, con risparmi sensibili sia in termini economici che ecologici.

La realtà è più complessa e articolata. Diversi progetti, su scala nazionale e locale, sono in fase avanzata di realizzazione, e stanno preparando un tessuto normativo, tecnologico e organizzativo di tutto rispetto. Ma non siamo ancora arrivati al punto di innesco della reazione a catena che porterà la firma digitale a trovare una applicazione diffusa e capillare. Manca la scintilla che può scatenare la reazione, e le informazioni disponibili sono tante, frammentarie e scoordinate.

Navigando in Internet sino a qualche anno fa i motori di ricerca ritornavano uno sproloquio di siti in cui si trovava di tutto e di più, ma sopratutto miriadi di personaggi esoterici (praticoni, pseudo-esperti, maghi, chiaccheroni, avvocaticchi, aiuti contabili e simili ammenicoli) che parlavano a sproposito di algoritmi di firma, di chiavi pubbliche e segrete, di credenziali di firma, di verifica, e di tante altre cose, senza sapere di cosa stessero effettivamente parlando.

E pure avari di notizie erano i fornitori delle tecnologie sviluppate a corredo della firma digitale: SmartCard, lettori di SmartCard (che in effetti permettevano anche di scriverle, ma nessuno lo diceva), HSM, software di firma e di verifica, PKI, prodotti aderenti a tutti gli standard del pianeta (che come risultato immediato spesso non riuscivano nemmeno a essere interoperabili, ovvero compatibili, con sè stessi).

Oggi la situazione è in parte migliorata (i venditori delle bancherelle Internet sono finiti nelle ultime pagine dei motori di ricerca), ma in quanto a chiarezza ancora poca – il discorso si sta spostando sulle dematerializzazione, la Conservazione Sostitutiva, la PEC, ... – ma la firma digitale continua ad essere una grande sconosciuta, e come tale una cosa che forse è meglio evitare.

In mezzo a questo baluginare di sigle, discorsi, articoli, l'unica cosa che forse si riesce a capire, è che in un mondo sempre più rivolto all'open-source una pletora di non ben definiti professionisti e aziende stanno operando ancora in base al più misero approccio proprietario[1]. Alla faccia della tanto decantata democrazia elettronica, di cui la firma digitale dovrebbe essere una delle punte di diamante!

Pessimismo a parte, la firma digitale rappresenta una sfida formidabile (come dicono i cuginetti di oltre oceano). Credo sia giunto alfine il momento di accettarla …

Clizio Merli

[1] Mi è capitato anche di interagire con distributori che dovevano chiedere il permesso alla società costruttrice per rispondere a domande banali, quali le caratteristiche di performance di firma, o la tipologia di interfacce standard supportate dai loro prodotti.

La firma

La firma è un'**assunzione di paternità**, di un documento, un'asserzione o un evento.

La nostra vita è stata sempre caratterizzata da una continua apposizione di firme olografe su documenti cartacei, sia da parte nostra che dei nostri partner. Un fatto che da sempre comporta l'accumulo smisurato di "pezzi di carta" raccolti nei nostri archivi personali, negli archivi pubblici, nelle biblioteche e musei, negli archivi aziendali.

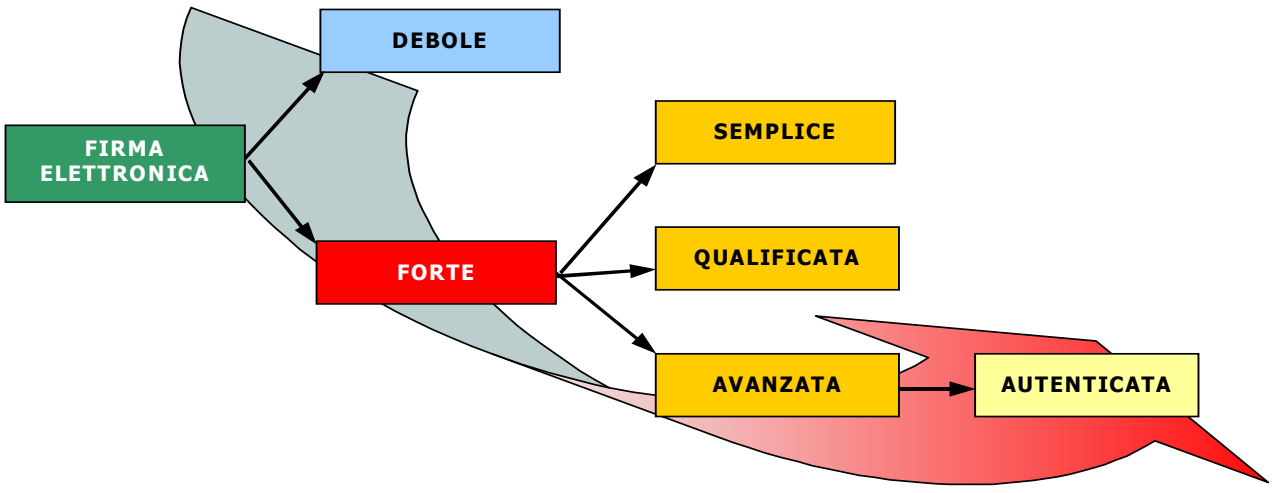
La cosa ha sicuramente un sapore romantico, specialmente per chi ama i libri e la lettura (come ad esempio chi scrive). Ma la stragande maggioranza dei pezzi di carta che firmiamo ha ben poco di romantico: scontrini delle carte di credito, richieste di ferie, documenti bancari, documenti aziendali, e altre amenità di questo tipo, per le quali sprechiamo tonnellate di carta, con buona pace delle foreste amazzoniche e delle altre depauperate zone pluviali del nostro amato pianeta.

Sin dall'avvento dei computer i vari *guru* dell'informatica hanno coltivato un sogno nel cassetto: trasformare i documenti cartacei in documenti elettronici, facili da archiviare, classificare, analizzare, ricercare. Un sogno che si è ulteriormente enfatizzato con l'avvento delle reti e con l'esponenziale aumento della capacità dei supporti di memorizzazione. Un sogno costantemente frustrato dalla impossibilità di apporre una firma sui documenti elettronici. Perchè generare documenti elettronici è facile, ma difficile è associarli ai loro autori, garantire la loro effettiva paternità, e la paternità degli atti che da questi documenti derivano.

Con l'avvento delle tecnologie di firma elettronica e digitale questo sogno può uscire dal cassetto.

Affidandosi alla scienza della comunicazione, e alle tecnologie informatiche che ne sono derivate, il concetto di firma di documenti elettronici ha trovato varie forme di implementazione e applicazione, che sono state man mano analizzate e codificate, sia dal punto di vista tecnico che di scambi umani, e quindi legale.

Lo schema seguente illustra la classificazione cui si è arrivati nel corso degli anni, e che trova una sua codificazione nella normativa internazionale, ed europea in particolare.

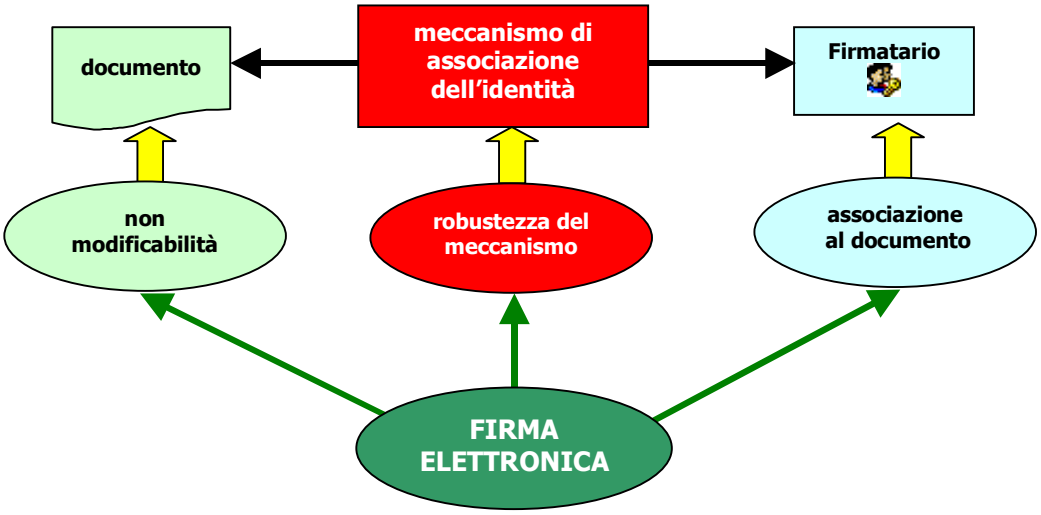


Proviamo ad analizzare il significato dei rettangolini di questa figura.

Firma elettronica

L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ed altri dati elettronici, utilizzati come metodo di autenticazione.

Questa definizione comprende qualunque meccanismo di associazione dell'identità di una persona (firmatario) ad un documento. La successiva classificazione in Firma Debole e Forte dipende dalla robustezza del meccanismo utilizzato, dalla possibilità di associare in modo non violabile l'identità del firmatario ai dati firmati, e dalla possibilità di rendere non modificabili a posteriori i dati firmati.



Firma Debole (Semplice)

Qualunque meccanismo informatico orientato ad associare l'identità di una persona a un insieme di dati registrati in formato elettronico (file di log, tecniche di crittografia a chiave semplice, …).

Ha un valore probatorio proporzionale alle caratteristiche oggettive intrinseche della qualità e della sicurezza del meccanismo adottato. La firma elettronica è in grado di fornire una prova circa la provenienza del documento ma non circa l'integrità del suo contenuto. Un documento elettronico sottoscritto con firma debole ha un'efficacia probatoria assimilabile a quello di un documento tradizionale munito di semplice sottoscrizione non riconosciuta. Ciò significa che colui contro cui è prodotto il documento può disconoscerlo, e provarne la provenienza e l'integrità del contenuto è a carico di chi intende avvalersene.

Firma Forte (Digitale)

Firma elettronica ottenuta in base alla applicazione di un sistema di chiavi asimmetriche (pubblica e segreta), che consente al firmatario di associare prova della propria identità e garantire al tempo stesso l'integrità dei dati firmati.

I meccanismi di firma forte sino ad ora elaborati e implementati si basano tutti sul principio della crittografia a chiavi asimmetriche, l'unico sinora noto in grado di supportare la prova di identità del firmatario e la non violabilità (ovvero l'integrità) dei dati firmati. In futuro potrebbero essere scoperti e implementati altri meccanismi di eguale o maggiore robustezza.

Inoltre la prova di identità del firmatario richiede ulteriori meccanismi che permettano di associare univocamente le chiavi asimmetriche di firma a una persona specifica. Questi meccanismi non sono, e non possono essere, solo informatici, ma devono coinvolgere la normativa del **Gruppo di Utenza** cui sono rivolti. Quindi per una validità certa su scala nazionale, europea o internazionale, i meccanismi devono essere supportati da norme (leggi) valide su scala nazionale, europea o internazionale[2].

In base alla robustezza dei meccanismi di firma e dei meccanismi di supporto alla prova di identità del firmatario la Firma Forte viene ulteriormente suddivisa in:

- Firma Forte Semplice
- Firma Forte Qualificata
- Firma Forte Avanzata
- Firma Forte Avanzata e Autenticata

Firma Forte Semplice

- il meccanismo di apposizione della firma digitale non è sufficientemente sicuro, in quanto il mantenimento delle credenziali[3] di firma digitale può essere violato, **oppure**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza solo nell'ambito di gruppi di utenti limitati (all'interno di organizzazioni, aziende, enti), ma non ha valore pubblico nè legale al di fuori del gruppo in cui viene riconosciuta.

Firma Forte Qualificata

- il meccanismo di apposizione della firma digitale è sufficientemente sicuro, in quanto il mantenimento delle credenziali di firma digitale non può essere violato, **e**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza nell'ambito di gruppi di utenti su scala europea, ma non ha valore per gli enti pubblici in quanto l'entità che garantisce l'identificazione si è autocertificata (non ha ottenuto una certificazione da parte di un ente di certificazione pubblica riconosciuto a livello europeo).

Firma Forte Avanzata

- il meccanismo di apposizione della firma digitale è sufficientemente sicuro, in quanto il mantenimento delle credenziali di firma digitale non può essere violato, **e**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza nell'ambito di gruppi di utenti su scala europea, con valore anche per gli enti pubblici in quanto l'entità che garantisce l'identificazione ha ottenuto una certificazione da parte di un ente di certificazione pubblica riconosciuto a livello europeo.

Firma Forte Avanzata e Autenticata

- firma forte avanzata la cui **apposizione viene autenticata da un notaio o da altro pubblico ufficiale autorizzato**. L'autenticazione della sottoscrizione consiste nella dichiarazione del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il documento sottoscritto con questo tipo di firma ha la stessa valenza probatoria della scrittura privata autenticata. L'efficacia probatoria è limitata all'elemento intrinseco della sottoscrizione (la provenienza del documento), senza alcuna interferenza sul contenuto della scrittura (la provenienza della dichiarazione).

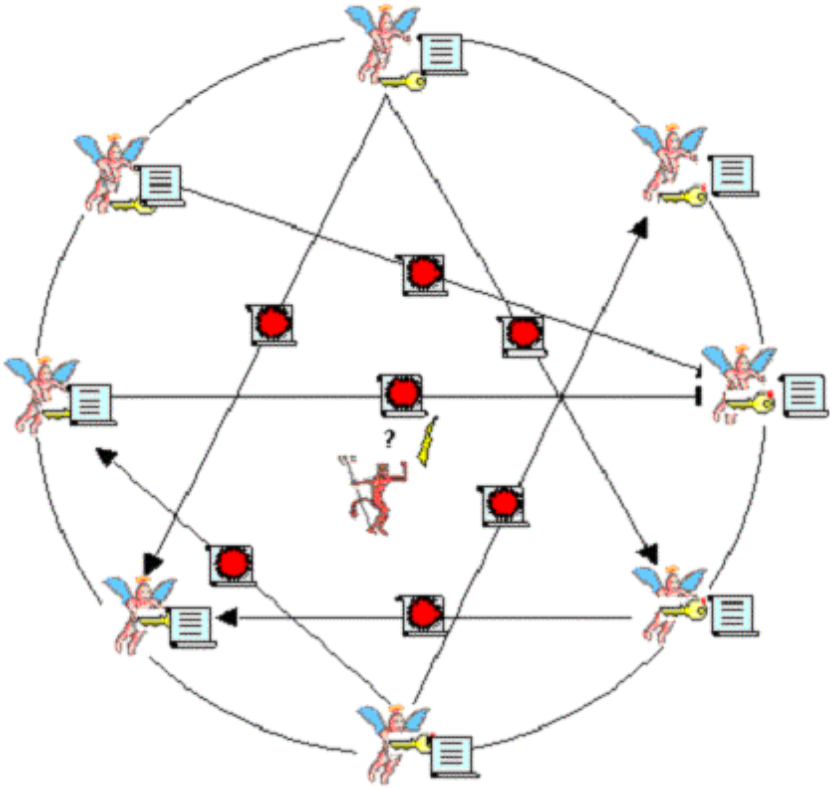
[2] Al momento il massimo grado di validità legale è quella europea (direttiva 1999/93/CE), che a livello nazionale è stata recepita da tutte le norme emanate dall'anno 2000 in poi.
[3] Il termine 'credenziali di firma' indica l'insieme delle informazioni di identità e di calcolo necessarie a eseguire il meccanismo di firma digitale (vedi capitolo successivo).

Crittografia, Riservatezza e Spudoratezza

Crittografia: l'arte della riservatezza

Crittografare un documento significa codificarlo in modo tale che risulti illeggibile a chi non conosce il meccanismo di codifica.

Lo scenario tipico è rappresentato da un gruppo di persone (entità) che vogliono comunicare tra di loro in modo riservato, senza che entità terze (aliene) possano capire il significato dei messaggi scambiati all'interno del gruppo.



Tenuto conto che ogni messaggio è una sequenza di caratteri, e che ogni carattere è rappresentabile in un numero compreso tra 0 e 255 (ovvero un byte), un meccanismo di codifica (crittografia) altro non è che una funzione matematica che permette di convertire la sequenza di caratteri che compone un messaggio (ovvero una sequenza di numeri) in una sequenza di caratteri (numeri) modificati. Il risultato è un nuovo messaggio che risulta incomprensibile a chiunque lo legga.

Ovviamente un meccanismo di semplice codifica non serve a nulla senza un meccanismo complementare di decodifica, ovvero una funzione matematica che permette di convertire il messaggio codificato nel messaggio originale.

Cosa distingue il meccanismo di codifica dal meccanismo di decodifica?

Su questo punto i matematici offrono, al momento, due possibili risposte:

1. l'utilizzo di **due funzioni matematiche** differenti, ma complementari, associate a **un solo parametro numerico**, detto **chiave** di codifica/decodifica;

2. l'utilizzo di **una sola funzione matematica** associata a **due parametri numerici** differenti ma complementari, detti rispettivamente **chiave di codifica** e **chiave di decodifica**.

In entrambi i casi i matematici ci offrono una soluzione con componenti di due tipi:

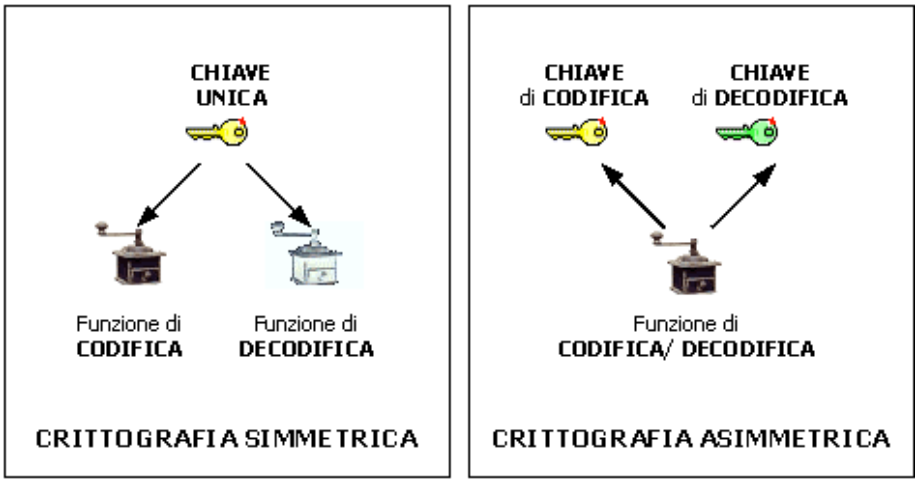
- funzione matematica
- parametro numerico (chiave)

in due possibili combinazioni:

- due funzioni e una chiave
- una funzione e due chiavi.

Poiché il vero problema non sono le funzioni matematiche in gioco, ma le chiavi:

1. nel primo caso si parla di **crittografia simmetrica** (o a chiavi simmetriche – **una sola chiave**),
2. nel secondo caso si parla di **crittografia asimmetrica** (o a chiavi asimmetriche - **due chiavi differenti**).



Crittografia: le chiavi

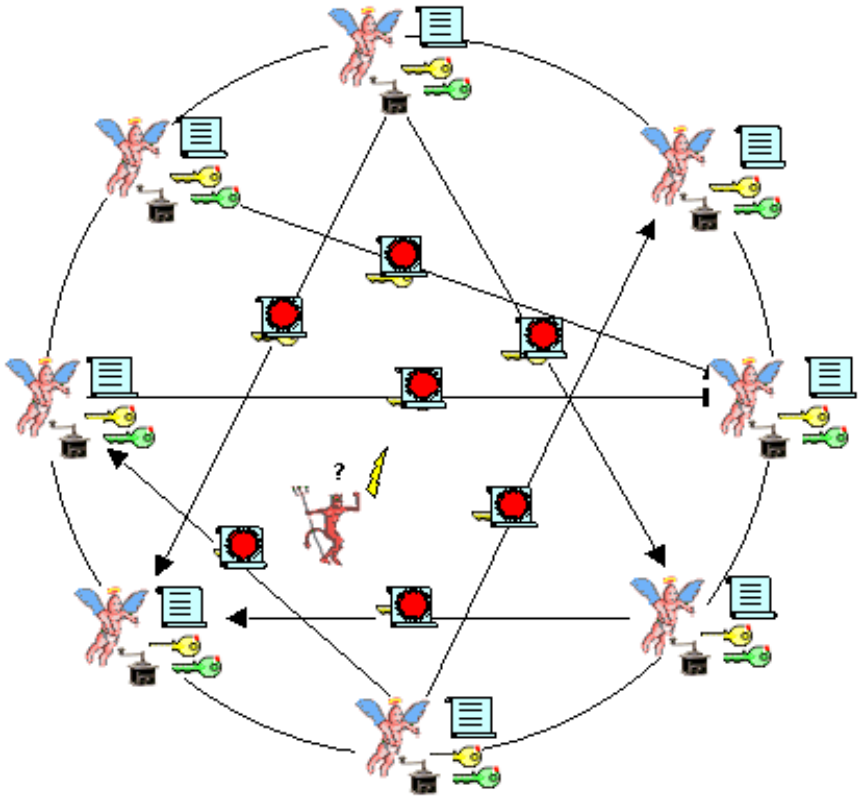
Perché il vero problema è rappresentato dalle chiavi e non dalle funzioni?

La risposta è di tipo economico.

Creare nuove chiavi è un processo poco costoso, che può essere ripetuto più e più volte senza particolari problemi. Per contro sviluppare una funzione di crittografia è un processo costoso, e non è ipotizzabile lo sviluppo di una nuova funzione per ogni messaggio che deve essere trasmesso.

Ora nel primo caso (crittografia simmetrica), sia le chiavi che le funzioni utilizzate devono essere conosciute a tutte le entità del gruppo. Purtroppo quando si trasmettono le chiavi a tutte le entità si corre il rischio che entità terze (aliene) intercettino la chiave, vanificando lo sforzo di rendere sicura e riservata la comunicazione.

Nel secondo caso (crittografia asimmetrica), questo problema non si pone, in quanto ogni entità del gruppo crea due chiavi: una viene comunicata a tutte le altre entità, e una viene mantenuta rigorosamente segreta. La chiave trasmessa a tutti è di fatto pubblica. In virtù di questo fatto la crittografia asimmetrica viene anche detta crittografia a chiavi pubbliche.



L'uovo di Colombo!

Non proprio.

Quando una entità trasmette a tutte le altre la propria chiave pubblica, deve corredarla di alcune informazioni relative alla propria identità (nominativo). Ora se una entità aliena si maschera da entità del gruppo e trasmette una chiave pubblica falsa dotata di un nominativo vero, le altre entità del gruppo possono essere tratte in inganno, ed essere convinte di parlare con una entità buona invece che con l'aliena.

Tuttavia la crittografia asimmetrica ci offre una possibilità in più rispetto alla crittografia simmetrica. Se al momento di trasmettere un messaggio, dopo aver codificato il messaggio con la chiave pubblica del destinatario (in modo tale che solo lui possa decodificarlo con la propria chiave segreta), codifichiamo ulteriormente il messaggio con la nostra chiave segreta, il destinatario non solo ha la ragionevole certezza che nessun altro ha letto il messaggio durante la trasmissione, ma ha anche la ragionevole certezza che ad inviarlo siamo stati proprio noi, in quanto riesce a decodificarlo con la nostra chiave pubblica (che lui possiede) solo se lo abbiamo codificato noi con la nostra chiave segreta (che solo noi possediamo).

Questo piccolo (!) accorgimento è di fatto una firma, la nostra firma.