Firma Digitale e Infrastrutture di Certificazione X.509

Indice

- Introduzione
- Primitiva Crittografica e Crittografia a Chiave Pubblica
- Documento Informatico e Firma Digitale
- Certificati e PKI
- Token Crittografici
- Minacce alla sicurezza della Firma Digitale
- Conclusioni

Introduzione

- L'obiettivo della firma digitale è fornire autenticazione di messaggi e garantire non ripudio
- La differenza con i *message authentication code* (MAC) è la verificabilità pubblica della firma
- Per garantire il non ripudio bisogna elevare il livello di sicurezza di tutto il processo e introdurre robusti meccanismi di *trust*.
- Dal punto di vista normativo dall'1 luglio 2016 ci si deve riferire al regolamento Europeo **eIDAS** (electronic IDentification Authentication and Signature) **n. 910/2014.**

Firma Digitale

Meccanismo crittografico

- Basato su crittografia a chiave pubblica
- Usato in vari contesti, anche come meccanismo standard in suite di protocolli crittografici

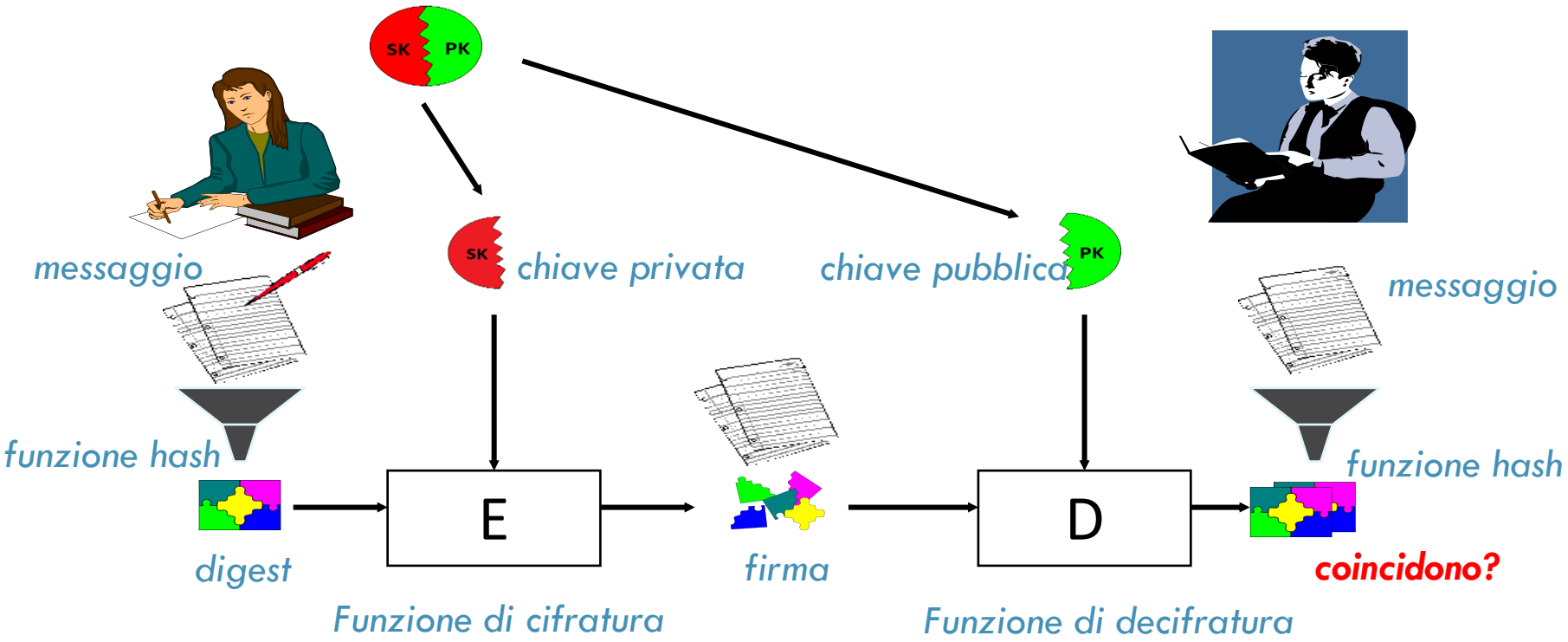
Documento Informatico

- È lo strumento che ha permesso di definire il concetto di documento informatico
- In questo contesto di aprono problematiche specifiche

Firma come primitiva crittografica

- Algoritmo di *generazione delle chiavi* (privata e pubblica)
- Algoritmo di *firma*
- Algoritmo di *verifica*
- La primitiva è tipicamente realizzata attraverso *crittografia a chiave pubblica*

Schema basato su crittografia a chiave pubblica e hash crittografico



Firma Digitale e Documento Informatico

Firma come istituto giuridico

- Funzione indicativa
- Funzione dichiarativa
- ***Funzione probatoria***

Documento informatico

- Funzione indicativa
- Funzione dichiarativa
- Funzione probatoria

Firma Digitale e Documento Informatico

Firma come istituto giuridico

- Funzione indicativa
  - *Nominativa, Autografa, Leggibile*
- Funzione dichiarativa
  - *Integrità fisica, sottoscrizione*
- ***Funzione probatoria***

Documento informatico

- Funzione indicativa: titolare chiave pubblica
- Funzione dichiarativa: il processo *hash-cifratura* è applicato al contenuto presentato al firmatario
- **Funzione probatoria**: ***è data dalla sicurezza degli algoritmi crittografici, delle tecnologie, dei processi.***

Certificazione della chiave pubblica

- La funzione indicativa è realizzata attraverso una infrastruttura di certificazione delle chiavi pubbliche (PKI)
- La PKI usata per i certificati di firma digitale segue lo standard X.509
- La chiave pubblica del titolare della firma è inclusa all'interno di un certificato digitale X.509 rilasciato e firmato (a sua volta) da una prestatore di servizi fiduciari (certificatore) – nel gergo, una terza parte fidata (Trusted Third Party)
- Per le firme a pieno valore probatorio (Firma Elettronica Qualificata o Firma Digitale), il Certificatore (Prestatore di Servizi Fiduciari) deve essere Qualificato ed Accreditato presso AGID.

Certificato X.509 (v3)

- V = Version
- SN = Serial number
- AI = Algorithm ID
- ISSUER = CA ← Certification Authority
- VALIDITY (not before, not after)
- SUBJECT
- SUBJECT PUBLIC KEY INFO (algorithm, value)
- ISSUER ID
- SUBJECT ID
- EXTENSIONS (key usage, …)
- CERTIFICATE SIGNATURE

Infrastruttura PKI e gerarchie di certificazione

- X.509 prevede una infrastruttura che realizza catene di certificati che raggiungono un punto *trusted (trust anchor)*, detto *Root*
- Date due certification authority CA-1 e CA-2, un anello della catena dalla CA-1 alla CA-2 è dato da un certificato firmato con chiave privata di CA-1 di una chiave pubblica di CA-2.
- Nel dominio delle firme eIDAS, le PKI sono realizzate a livello nazionale, ma esiste un meccanismo di *trust anchor* europeo (si veda più avanti)

Revoca dei Certificati

- Il titolare (o terzo interessato) può chiedere la revoca del certificato
- Le informazioni di revoca vengono verificate o scaricando la CRL (certificate revocation list) o attraverso OCSP (online certificate status protocol)
- Le informazioni di revoca nelle CRL (RFC 5280) sono: <`CertificateSerialNumber, Time, Extensions`>, tra le `Extensions` (opzionali) è inclusa il `ReasonCode` (fortemente raccomandato, obbligatorio per Firma Elettronica Qualificata)

Dispositivo sicuro (qualificato) di firma

- Per un effettivo non-ripudio il livello di sicurezza deve essere innalzato.
- La segretezza della chiave privata assume un ruolo fondamentale
- La permanenza (anche temporanea) nella RAM del PC della chiave privata metterebbe a repentaglio la segretezza
- Viene quindi usato un dispositivo sicuro per la generazione della firma (detto token crittografico). Il regolamento eIDAS parla di *dispositivo qualificato*.
- Esso può essere una smart card (interfacciata con driver specifico o via USB) o un Hardware Security Module (HSM).
- Gli HSM sono usati per realizzare meccanismi di firma digitale remota e sono residenti presso fornitori di servizio *trusted,* che coincidono di fatto con i certificatori.

Formati di firma

- La normativa europea prevede tre possibili formati di firma:
  - CADES (il documento è in qualsiasi formato) → PKCS#7
  - PADES (il documento è in formato PDF)
  - XADES (il documento è il formato XML) → *enveloped*, *enveloping*, *detached*
- I formati più utilizzati in Italia sono CADES e PADES

Validazione Temporale ed Estensione di validità di un documento informatico

- Una validazione temporale (qualificata):
  - collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;
  - si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato;
  - è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente
- Una validazione temporale associata ad un documento informatico che sia antecedente a scadenza o revoca del certificato, ne estende la validità

Verifica completa di un documento informatico firmato con Firma Digitale o Firma Elettronica Qualificata (PKI)

- Decifratura della firma e corrispondenza con digest
- Verifica della scadenza del certificato e delle informazioni di revoca (anche in relazione alla presenza di marcature temporali) – CRL o OCSP
- Verifica della credibilità del certificato attraverso la verifica della firma del certificato (e il certificato della chiave pubblica di certificazione installato nel sistema)
- Verifica del certificato della chiave pubblica di certificazione attraverso *Trust Service status List* nazionale pubblicata da AGID.
- Verifica dell'URL della suddetta lista nella lista pubblicata dalla Commissione Europea.
- Verifica della firma della *Trust Service status List* nazionale.
- Calcolo dell'hash SHA-256 dei certificati AGID usati per la firma della suddetta lista
- Verifica della presenza di tali digest (in formato esadecimale) nella Gazzetta Ufficiale

Minacce relative ai documenti informatici: SW/HW insicuri

- Vulnerabilità connesse alla smart card o agli HSM (recentemente documentate)
- Piattaforme SW non trusted (es. invio maliciuos dell'hash alla smart card, gestione fraudolenta del controllo di validità del certificato, etc.)
- Contromisure poco realistiche: es. visual cryptography

Immodificabilità (1)

- **Ulteriore classe di minacce:** altre minacce alla sicurezza del processo di forma derivano dalla mancanza del requisito di *immodificabilità* dei documenti

- **Immodificabilità:** caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso (DPCM 13 novembre 2014)

Immodificabilità (2)

- L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di disporre di funzionalità sempre più specializzate per rendere più facile la creazione, la modifica e la manipolazione dell'informazione

- Ciò ha portato alla diffusione di un gran numero di formati talvolta specifici di particolari domini applicativi (es. in campo sanitario)

- Si pone pertanto il problema della **adeguatezza dei formati**

- Ai documenti (ai formati) è richiesta la caratteristica della **staticità**: Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

Immodificabilità (3)

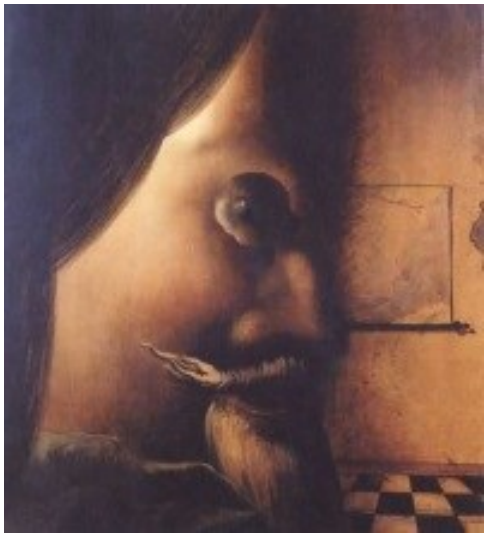
- In campo di dematerializzazione la normativa (DPCM 13/11/2014) individua i criteri di scelta:
  - Apertura
  - **Sicurezza**
  - Portabilità
  - Funzionalità
  - Supporto allo sviluppo
  - Diffusione
- Cosa intende il legislatore per «sicurezza» di un formato?
- *La sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno*

Minacce relative ai documenti informatici: contenuti dinamici

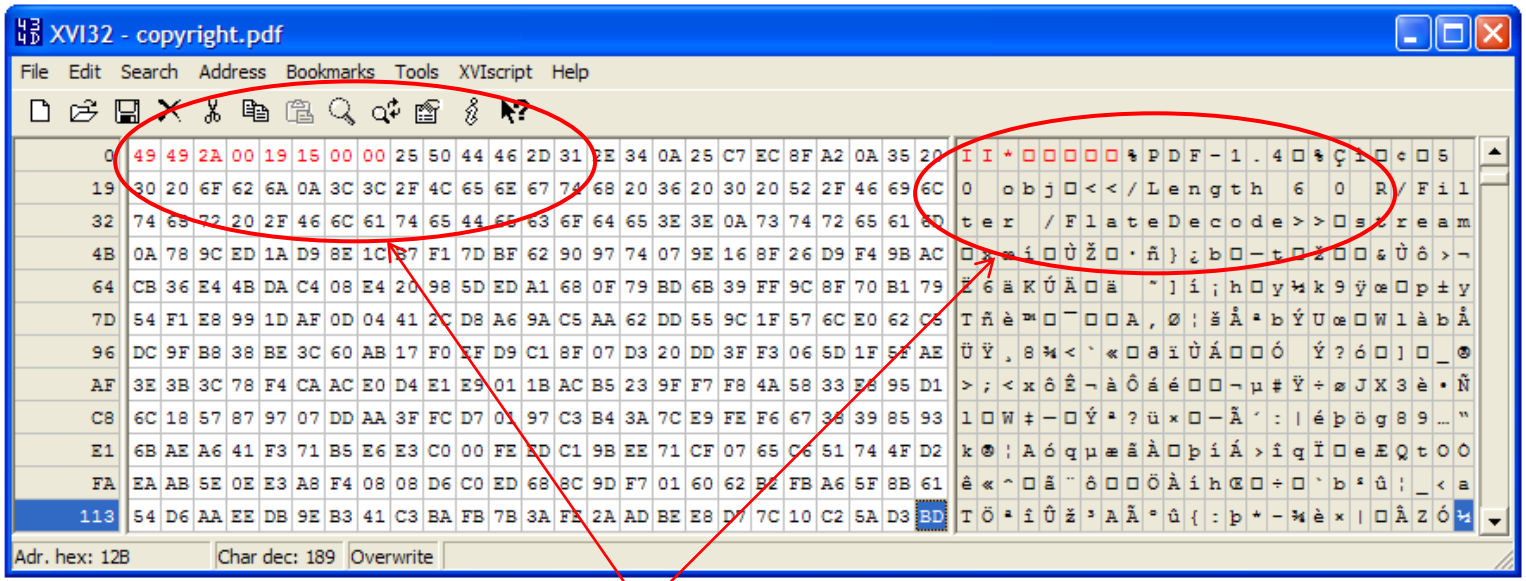
- Inclusione di macro codice, java scripts, etc. Kain, Smith, & Asokan (2002)
- Dinamicità basato su uso anomalo di font Jøsang, Povey, & Ho (2002): “Times New Roman1” scambia “A”, “i”, “c” e “e” con “C”, “a”, “r” e“k”, usando questo font se si scrive “Alice” si ottiene “Clark” e viceversa.
- Contromisure: formati statici, font hashing Jøsang, Povey, & Ho (2002), uso di sandbox Spalka et al. (2001), usare un document parser al momento della firma (Alsaid & Mitchell, 2005)

Minacce relative ai documenti informatici: file polimorfi

- L'attacco si basa sull'inserimento di due contenuti all'interno di un unico file
- Un formato di firma basato su «busta crittografica» non rileva l'anomalia ed è sufficiente una modifica di estensione
- copyright.pdf.p7m→auth.tif.p7m



Dettagli sui file polimorfi



Header *multiplo* di un file polimorfo

Conclusioni

- Firma digitale: meccanismo basilare per i processi di dematerializzazione
- Aspetti cruciali: costo, usabilità, interoperabilità, sicurezza
- Sicurezza: è necessaria consapevolezza sulle minacce esistenti per rendere il rischio trascurabile.

Approfondimento 1: autenticazione di messaggi

- Ricordiamo che autenticare un messaggio significa riuscire a dare prova della sua integrità (e cioè assenza di modifica del contenuto del messaggio) e della autenticità della provenienza del messaggio. E' ovvio che è provo di senso parlare di certezza della sorgente di un messaggio se al tempo stesso non si è in grado accertarne la sua integrità. Infatti un messaggio potenzialmente modificato non potrebbe essere ricondotto alla sorgente di provenienza per il fatto di aver perso il suo contenuto originario.
- I MAC (message authentication code), tipicamente attraverso l'uso combinato di una funzione hash crittografica e un segreto condiviso tra sorgente e destinazione del messaggio raggiungono l'obiettivo della autenticazione, ma non permettono la verificabilità del messaggio da parte di un terzo, ma solo da parte della destinazione predeterminata, con la quale la sorgente ha condiviso il segreto.
- Nel caso della firma l'obiettivo è diverso. Si vuole far si che un messaggio (o un documento) possa essere firmato digitalmente in modo tale che i destinatari (che in generale non sono determinati, ma sono tutti i soggetti interessati, anche futuri), possano verificarne integrità e autenticità, con accezione, che, come vedremo, nel caso dei documenti informatici, assumono connotati diversi.
- Inoltre nel caso di documenti informatici nel senso giuridico del termine, è necessario fornire ulteriori garanzie di sicurezza in relazione al documento firmato, che saranno esposte successivamente.
- Il non ripudio (da parte del firmatario) è un altro requisito ottenuto attraverso la firma digitale, e rappresenta il fatto che il firmatario non possa rinnegare la paternità della firma. Ovviamente, come sempre avviene, ma in particolare si verifica in questo contesto nel quale i meccanismi tecnici e tecnologici servono a determinare un istituto giuridico ben codificato, il tutto ha dei limiti ben precisi, che si traducono in vincoli di natura normativa, e che sono direttamente legati ai livelli di sicurezza di algoritmi, protocolli, tecnologie e processi utilizzati per realizzare l'infrastruttura di firma digitale, inclusi i meccanismi di trust (e gli organismi che fungono da terze parti fidate) che sono necessari per garantire autenticità della firma stessa.

Approfondimento 2: norme

- Gli aspetti normativi saranno trattati in dettaglio successivamente.
- E' però necessario già a questo stadio individuare la norma di riferimento per il contesto delle firme elettroniche, al fine di identificare le accezioni di «firma» che sono più rilevanti
- Dall'1 luglio 2016 è direttamente applicabile il **Regolamento (UE) n. 910/2014 (eIDAS)**
- Al fine di armonizzare l'insieme delle norme del settore, il Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005, n. 82), è stato ulteriormente modificato, coordinandolo con il regolamento eIDAS, attraverso D.lgs. 26 AGOSTO 2016, N. 179, D.lgs 13 DICEMBRE 2017, N. 217.
- Le norme principali da considerare sono quindi entrambe, in quanto il CAD non è un provvedimento che recepisce il regolamento eIDAS (che, come tale, non necessita di recepimento), ma è armonizzato con esso.
- Come vedremo più avanti la Firma Elettronica Qualificata (FEQ – Qualified Electornic Signature) ha valore probatorio uguale a quello della firma autografa in tutti gli Stati Membri, e deve essere garantita piena interoperabilità dei sistemi di firma dei diversi Stati.

Approfondimento 3: accezioni

- Gli schemi di firma digitale sono tipicamente basati su crittografia a chiave pubblica (es , RSA, curve ellittiche). Tuttavia esistono schemi di firma digitale (emergenti) basati su altri meccanismi (hash-based, Merkle-Ttree-based, Lattice-based, etc.), ancora però non utilizzati. Visto il fatto che la crittografica a chiave pubblica utilizzata nel contesto della firma digitale non è post-quantum, è opinione condivisa nella comunità scientifica che essa dovrà essere abbandonata in tempi non lunghi (in funzione della diffusione delle tecnologie basate su quantum computing). In tal caso gli attuali schemi alternativi post-quantum sono candidati a prendere il posto della crittografia a chiave pubblica, anche se, al momento, presentano tutti diverse limitazioni che ne ostacolano l'applicazione su larga scala. Questo problema è quindi oggetto di attenzione da parte della comunità scientifica del settore.
- La firma digitale di messaggi o pacchetti di bit è un meccanismo incluso in diverse suite di protocolli crittografici (si pensi per esempio a TLS o ai meccanismi utilizzati in blockchain). La firma digitale può essere vista come meccanismo crittografico in sé e per sé. Ma quando ci riferiamo al contesto della firma di documenti informatici, sorgono una serie di problematiche specifiche, che sono strettamente connesse al ruolo giuridico che si vuole dare al documento informatico, e quindi, per esempio, ai formati dei documenti sottoposti alla firma, ai processi di generazione e verifica della firma, e a tutto l'ecosistema che è necessario implementare per raggiungere l'obiettivo della realizzazione di un istituto giuridico.
- Partendo dall'accezione generale di firma, ci concentreremo sulla seconda accezione, pur senza approfondire gli aspetti giuridico-normativi in questa fase.

Approfondimento 4: primitiva crittografica

- L'algoritmo di generazione delle chiavi restituisce in output in maniera non predicibile una coppia di chiavi pubblica privata **(PK, SK)**.
- L'algoritmo di firma **SIG**, riceve in input un messaggio **M** (visto come sequenza di bit di dimensione arbitraria) e restituisce la firma del messaggio **F** rispetto alla chiave privata **SK**, come **F ← SIG(M,SK).**
- L'algoritmo di Verifica della firma, **VF**, riceve in input un messaggio **M**, una firma **F** e una chiave pubblica **PK** e restituisce **R**, un valore **vero** o **falso** (firma verificata, firma non verificata) **R ← VF(M,F,PK)** (si noti che la verifica usa solo informazioni pubbliche)
- Lo primitiva è tipicamente istanziata attraverso crittografia a chiave pubblica, es RSA o curve ellittiche.
- Per cui, la generazione è l'algoritmo di generazione sicuro per le chiavi dello schema crittografico considerato
- SIG è (potenzialmente) la funzione di Encryption dello schema associata alla chiave **SK, E_{SK}**
- VF è (potenzialmente) la funzione di Decryption corrispondente, e cioè associata alla chiave **PK, D_{PK}**
- Per diversi motivi legati alla sicurezza e alla efficienza dello schema, **SIG** e **VF** sono ottenuti utilizzando una funzione hash crittografica **H** (es. SHA-256).
- In particolare: SIG è ottenuta come **E_{SK}(H(M)),** quindi **F=E_{SK}(H(M)).**
- **VF** è ottenuta come segue *se* **H(M)** = **D_{PK}(F)** *restituisci* **vero**, *altrimenti restituisci* **falso**

Approfondimento 5: funzioni firma autografa

- La funzione indicativa è la capacità della firma di individuare un soggetto firmatario
- La funzione dichiarativa è la funzione per la quale il firmatario, attraverso la firma, dichiara di assumere paternità di ciò che sottoscrive, o di approvarlo o riconoscerlo. E' la semantica stessa del documento sottoscritto che determina l'effettiva declinazione della funzione dichiarativa. In un contratto, per esempio, le parti, attraverso la sottoscrizione, dichiarano di approvare le clausole del contratto, accettandone quindi le obbligazioni che ne derivano.
- La funzione probatoria rappresenta il fatto che le due precedenti funzioni, quella indicativa e quella dichiarativa, sono attuate con valore probatorio. La firma quindi costituisce prova delle *autenticità* e *genuinità* del documento firmato. Per autenticità si intende provenienza del documento, per genuinità significa non alterazione del contenuto. L'autenticità è connessa alla funzione indicativa, mentre la genuinità alla funzione dichiarativa, solo se, appunto la funzione probatoria è attuata a pieno.
- La disciplina civilistica richiede, al fine di dare valore probatorio alla funzione indicativa, che la firma sia *nominativa*, *autografa* e *leggibile*. L'ultimo requisito, spesso disatteso, è invece stringente nel caso degli atti pubblici (di fronte al notaio), caso in cui, tra l'altro, la leggibilità rappresentava originariamente contestuale prova di capacità dei sottoscrittori di leggere e scrivere, e quindi di comprendere il testo sottoscritto. Il fatto che la firma deve essere autografa, rende essa stessa un *tratto biometrico*, per il fatto che la grafia ha connotati univoci e difficilmente imitabili (il grado di robustezza di questo tipo di tratto biometrico è tuttavia non assoluto, come dimostrato dal fatto che il giudizio di periti grafologi può essere contrastante) .
- Il valore probatorio della funzione dichiarativa è di fatto ottenuto garantendo integrità fisica del documento (la carta e l'inchiostro usato per la scrittura, sia del testo che della firma – non integrerebbe la funzione probatoria in termini dichiarativi una firma apposta con la matita o apposta in calce ad un documento che però appare tagliato tra firma e testo e poi incollato). A questo si aggiunge un aspetto convenzionale, che motiva anche il termine *sottoscrizione*, per il quale la firma agisce (in termini di funzione dichiarativa) solo sul testo *precedente* alla firma. Si noti infatti che nei contratti le clausole vessatorie sono firmate in successione e sottoscritte ulteriormente, per essere considerate valide.

Approfondimento 6: funzioni firma digitale e quadro firme europeo (eIDAS)

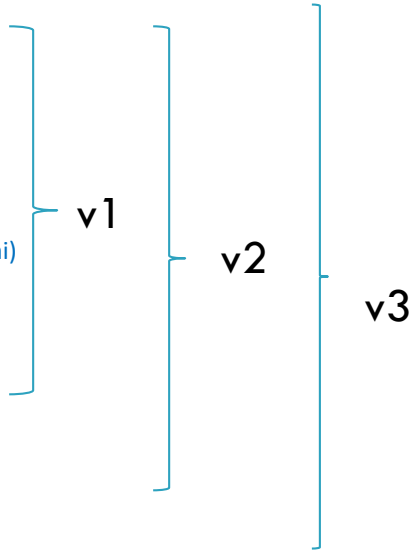
- La funzione indicativa è realizzata attraverso l'annuncio del possesso della chiave privata attraverso la pubblicazione della chiave pubblica. In linea di principio tale annuncio potrebbe avvenire in diversi modi. Potrebbe per esempio avvenire attraverso scambio diretto con i destinatari, pubblicazione in una bacheca elettronica associata ad un profilo di un social network, o pubblicazione su un sito web. Per motivi di sicurezza e trust è in realtà realizzata attraverso la produzione di un documento informatico che certifica l'associazione tra chiave pubblica e chiave privata (certificato), rilasciato da una terza parte fidata.

- La funzione dichiarativa si basa sul fatto che il sottoscrittore è consapevole di applicare una trasformazione crittografica (prima funzione hash, poi cifratura del *digest*) al contenuto binario del documento presentato (la norma impone infatti che il documento venga presentato con chiarezza al firmatario prima della firma). Nel caso di firma PADES (come vedremo), si aggiunge la convenzione della sottoscrizione attraverso la metafora della firma in calce, applicata anche a porzioni di documento.

- La funzione probatoria si basa sui requisiti di sicurezza, che sono di fatto oggetto del resto della presentazione. Quindi
  1. Sicurezza del certificato in quanto documento informatico firmato e in relazione al suo ciclo di vita (revoca)
  2. Trustworthiness del Certificatore e dell'intera infrastruttura di certificazione
  3. Sicurezza delle piattaforma hw/sw dove si genera e si verifica la firma. In particolare possibile uso di un dispositivo sicuro (esterno), di cui discuteremo in seguito.
  4. Sicurezza degli algoritmi di hash e di crittografia a chiave pubblica
  5. Sicurezza dei formati dei documenti soggetti a firma
  6. Disciplina nella custodia della chiave privata, e garanzia della sua segretezza, anche in relazione al punto 3
  7. Awareness degli utenti
- La normativa europea (Regolamento eIDAS) prevede tre tipi di Firma: Firma Elettronica, Firma Elettronica Avanzata (FEA), Firma Elettronica Qualificata. La prima è genericamente un insieme di dati associati al documento e ha baso valore probatorio. La FEA richiede connessione univoca al contenuto in modo da rilevare modifiche, connessione univoca al firmatario attraverso strumenti su cui il firmatario ha controllo esclusivo. La FEQ aggiunge i requisiti di un certificato qualificato (cioè emesso da un certificatore che rispetta requisiti di qualità e sicurezza imposti al livello europeo) e dell'uso d i un dispositivo sicuro (detto qualificato) per la creazione della firma.
- Sia FEA che FEQ rispettano il principio della neutralità tecnologica, cioè non indicano quale tecnologia si debba utilizzare ma solo i requisiti che si debbono ottenere. Al momento, la crittografia a chiave pubblica è la tecnologia adottata dagli stati membri per realizzare FEQ. In Italia la Firma Digitale è una FEQ che usa crittografia a chiave pubblica. Dal punto di vista degli effetti probatori, non vi è alcuna differenza tra FEA e FEQ (vedi Codice dell'Amm.ne Digitale). Esse hanno valore di **prova legale**, cioè pre-codificata dalla legge e non liberamente valutabile in giudizio. In sostanza, hanno valore probatorio equivalente alla scrittura privata.
- **Da qui in poi ci riferiamo implicitamente al più alto gradi di sicurezza per la firma, e cioè a FEQ e Firma Digitale.**

Approfondimento 7: campi di X.509

- V = Version: vi sono 3 versioni di X.509 (v1, v2, v3), che differiscono per i campi inclusi
- SN=Serial number: numero identificativo del certificato per una Certification Authority
- AI= Algorithm ID: ID algoritm usato per la firma del certificato (campo ridondante)
- ISSUER=CA: Nome X.500 della CA
- VALIDITY (not before, not after): tempo di validità. La scadenza è impostata per motivi di sicurezza (3 anni)
- SUBJECT: nome e cognome (o pseudonimo) del titolare della chiave
- SUBJECT PUBLIC KEY INFO (algorithm, value): valore della chiave pubblica, algoritmo (es. RSA), etc.
- ISSUER ID: ID alternativo per identificazione CA
- SUBJECT ID: ID alternativo per identificazione titolare
- EXTENSIONS (key usage, …): si veda precedenti approfondimenti
- CERTIFICATE SIGNATURE : firma del certificato, è presente in tutte le versioni



Approfondimento 8: key usage

Tra le extensions particolare importanza ha il ***key usage***. Seguono alcuni dei valori che può assumere:

- **Digital signature** : Indica che la chiave pubblica viene utilizzata con un meccanismo di firma digitale per supportare servizi di sicurezza diversi da non ripudio, firma del certificato o firma CRL. Una firma digitale viene spesso utilizzata per l'autenticazione dell'entità e l'autenticazione dell'origine dei dati con integrità.
- **Non-repudiation** : Indica che la chiave pubblica viene utilizzata per verificare le firme digitali utilizzate per fornire un servizio di non ripudio. La non ripudio protegge dall'entità firmataria che nega falsamente qualche azione (escluso il certificato o la firma CRL).
- **Key encipherment** : Indica che il certificato verrà utilizzato in un protocollo che crittografa le chiavi. Un esempio è il protocollo SSL/TLS.
- **Data encipherment** : Indica che la chiave pubblica viene utilizzata per crittografare dati, ad eccezione di chiavi crittografiche.
- **Key agreement** : Indica che il certificato è usato per lo scambio deii parametri pubblici di Diffie-Hellman.
- **Certificate signing** : Indica che la chiave pubblica contenuta nel certificato è usata per verificare una firma di un certificato.
- **CRL signing** : Indica che la chiave pubblica è usata per verificare la firma di informazioni di revoca, come una CRL.

Nota. Se le estensioni sono definite come critiche il certificato viene rigettato se le extensions non sono verificate. L'uso di estensioni critiche innalza la sicurezza applicativa perché contrasta l'uso improprio del certificato (per esempio, per ottenere una firma su un hash di un documento sfruttando un processo di autenticazione).

Approfondimento 9: Revoca (CRL)

- I motivi per effettuare la revoca possono essere diversi. Tra essi menzioniamo: (1) compromissione della chiave privata, (2) compromissione del Certificatore, (3) cessazione del Certificatore, (4) sostituzione del certificato, (5) rimozione di privilegi (tipicamente in questo caso l'istanza della revoca proviene dal terzo interessato, che è l'organizzazione nella quale il titolare aveva un ruolo connesso all'uso della firma digitale).
- La revoca può essere temporanea, in questo caso si parla di *Sospensione*, e le corrispondenti liste sono chiamate *CSL*.
- La CRL è mantenuta e pubblicizzata dal Certificatore, che la firma con una chiave di certificazione.
- La CRL è una lista di record, ognuno contentente: <(1) `CertificateSerialNumber`, `(2) Time`, `(3)Extensions`>, tra le `Extensions` (opzionali) è inclusa il `ReasonCode`.
- (1) Serial Number del certificato che individua univocamente il certificato revocato; (2) data e ora della revoca, che deve avvenire tempestivamente dopo l'invio dell'istanza da parte del titolare o da parte del terzo interessato; (3), se `ReasonCode` ragione della revoca.
- Si noti che CRL non contiene i certificati, ma solo il Serial Number per motivi di ottimizzazione dello spazio, ma anche per compliance con la normativa sulla tutela dei dati personali.
- Le CRL devono essere interamente scaricate in fase di verifica, così come in fase di firma (con HTTP o LDAP). Per motivi di efficienza può essere impostato un tempo di validità delle CRL, ma questo introduce vulnerabilità. Esiste anche una versione del protocollo che permette di scaricare solo la parte differenziale (Delta-CRL).

Approfondimento 10: OCSP

- X.509 include un protocollo client-server per la consultazione dello stato di revoca dei certificati. Il protocollo è OCSP (Online Certificate Status Protocol – RFC 2560). A differenza delle CRL, secondo OCSP non è necessario per il client scaricare l'intera lista dei certificati revocati (o una parte incrementale nella versione Delta-CRL), ma solo effettuare una richiesta che riguarda singolarmente uno specifico certificato.
- Il protocollo prevede quindi che il client invii una OCSP-request al server, che è detto OCSP-responder. La risposta può contenere tre possibili valori:
  - **Good**
  - **Revoked (**con **RevocationTime, RevocationReason)**
  - **Unknown**
- Gli RFC di riferimento sono RFC 6960, 2560 e 5019
- Lo svantaggio principale è il sovraccarico per il responder. La risposta è firmata dal server, con chiavi non necessariamente appartenenti alla catena PKI del certificato che si sta verificando. Particolare attenzione va prestata alla configurazione lato client in caso non pervenga entro il time-out la risposta. OCSP può essere più facilmente vulnerabile ad attacchi di tipo DOS. Ad ogni modo OCSP e CRL possono essere usati in combinazione (per backup, ad esempio).

Approfondimeto 11: token crittografico

- Il punto piu` critico del protocollo di firma e` la segretezza della chiave privata. Essa dovrebbe essere garantita anche in caso di attacchi sofisticati, in quanto la sua compromissione potrebbe determinare conseguenze disastrose.
- La soluzione adottata è quella di generare e mantenere la chiave privata all'interno di un dispositivo sicuro di firma, e interfacciarsi ad esso attraverso lo standard PKCS#11. Il dispositivo sicuro di firma è detto genericamente *Token Crittografico*. Esso nel concreto può essere o una smart card o un Hardware Security Module (HSM), nel caso di firma remota. Ciò che accade è che il processo eseguito sul sistema operativo del PC collegato all'applicativo di firma si occupa di generare il digest del documento da firmare, e di inviarlo al token crittografico, nel quale risiede la chiave privata. E' in esso, e cioè attraverso la CPU del token crittografico, che avviene l'esecuzione della funzione di cifratura il cui output è la firma digitale associata al documento. La chiave privata è memorizzata in un'area di memoria protetta, progettata in modo da non essere accessibile se non dal processo legittimo residente sul sistema operativo del token crittografico. Il token crittografico deve essere conforme a standard di sicurezza definiti dalla normativa vigente, per le firme con pieno valore probatorio (Qualified Electronic Signature del regolamento europeo eIDAS).
- Nel caso di firma remota, il problema si sposta, oltre che sulla sicurezza degli HSM, anche su quello dell'autenticazione del firmatario, oltre che sulla effettiva trustiworthiness del fornitore di servizio. L'autenticazione presso il servizio di generazione di firma remota deve essere forte (multi-factor) e particolare attenzione da parte dei progettisti del servizio deve essere prestata alla procedura di impostazione e modifica del numero di cellulare tipicamente associato alla autenticazione tramite OTP. Se, come spesso avviene, l'OTP è inviato come sms sullo smartphone del firmatario o con chiamata con numero mittente codificata (le ultime cifre rappresentano l'OTP), assume rilevanza anche la possibile inaffidabilità della piattaforma mobile, visti i possibili attacchi di hijacking di chiamate o sms o gli attacchi di tipo *SIM-SWAP*.

Approfondimento 12: formati di firma

- In maniera semplificativa, possiamo dire che ad un documento firmato dovranno essere associati diversi elementi: (1) la firma, (2) il certificato della chiave pubblica corrispondente alla chiave privata del sottoscrittore, (3) gli ID dell'algoritmo usato per cifrare il digest e dell'hash usato per creare il digest, (4) eventualmente certificato della chiave pubblica di certificazione, (5) eventuale marcatura temporale. Tutti questi elementi, se accessibili in modo interoperabile, permettono al software di verifica della firma di poter effettuare la verifica, dato che le informazioni di revoca dei certificati sono inclusi negli stessi. E' da osservare tuttavia che il sw di firma, indipendentemente dalla presenza del certificato della chiave di certificazione tra le informazioni sottoposte a verifica, dovrà comunque utilizzare i certificati delle chiavi di certificazione installati in modalità sicura e considerati pertanto *trusted*, perché i certificati forniti per la verifica potrebbero essere falsi.
- Il formato CADES (è basato su CMS - Cryptographic Message Syntax Authenticated-Enveloped-Data Content Type (RFC 5652, che usa la sintassi di PKCS#7), permette di creare una sorta di "busta crittografica" che contiene, oltre al documento originario, come sottoelementi, tutti gli elementi elencati prima. Pertanto in una busta crittografica è possibile includere un documento di qualsiasi formato.
- Il formato PADES, gli elementi suddetti sono integrati nel formato PDF. Pertanto I documenti firmati in modalità PADES sono solo PDF.
- Il formato XADES è XML. Può essere di tre tipi: (1) Enveloped (la firma e gli elementi associati sono sottoelementi del documento sottoposto a firma), (2) Enveloping (Il documento sottoposto a firma è un sottoelemento della firma), (3) Detached (la firma è un documento XML indipendente). In tutti I casi, nel formato XADES, il documento sottoposto a firma deve essere in formato XML. Per quanto riguarda i fogli di stile, necessari per esempio nel caso dei documenti in formato HL7 CDA Rel. 2.0, vi possono essere problemi di non immutabiltà. HL7 International ha pertanto definito un foglio di stile generico, che è disponibile nel portale web del Fascicolo Sanitario Elettronico e permette di non generare problemi di ambiguità di presentazione.

Approfondimento 13: validazione temporale (qualificata)

- La declinazione tecnica prevalente dell'istituto della validazione temporale è la marcatura temporale.
- La marcatura è una struttura dati (**TSR**) firmata digitalmente dal Certificatore (o prestatore di servizi fiduciari di validazione temporale accreditato in Italia da ACCREDIA), che contiene data e ora e l'hash crittografico dell'evidenza informatica soggetta a marcatura.
- Vi possono essere diversi formati di marcatura. I principali:
  - formato CADES-T (estensione .p7m) è il formato CADES che include nei campi PKCS#7 anche la marcatura. In tal caso l'applicazione della marcatura è contestuale alla firma
  - Formato PDF (estensione .pdf) è il formato PDF che include anche la marcatura. In tal caso l'applicazione della marcatura è contestuale alla firma
  - Formati (estensioni .m7m, .tsd) M7M e TSD: contengono il TSR e il file stesso sottoposto a marcatura. Possono pertanto essere usati per associare una marcatura temporale ad un documento in maniera differita rispetto alla firma.
  - I SW di firma permettono di estarre il .tsr (la marcatura in file separato) da tutti i formati che la includono.
- **La conservazione, da parte del prestatore di servizi fiduciari di validazione temporale, delle marcature temporali (.tsr) per periodi prolungati (20 anni) innalza il livello di sicurezza notevolmente, perché anche un ipotetica compromissione sia della chiave privata del titolare, sia della chiave privata usata per firmare la marcatura da parte del prestatore e una successiva alterazione del documento e della marcatura associata verrebbe rilevata perché la marcatura non sarebbe coincidente con quella in conservazione.**

Approfondimento 14: sigillo elettronico

- Il sigillo elettronico avanzato/qualificato è stato introdotto dal Regolamento eIDAS. Sostanzialmente consiste in una firma elettronica qualificata, con la differenza che non implementa la funzione indicativa nel senso stretto del termine perché non afferisce a una persona fisica, bensì a una persona giuridica.
- Mentre da una firma elettronica qualificata, attraverso il certificato associato, è possibile individuare il soggetto firmatario attraverso il suo nome, cognome, codice fiscale ecc., da un sigillo viene individuata una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, e non vi è alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.
- Il sigillo è quindi usato come contrassegno con valore probatorio per garantire integrità di un documento della quale una determinata persona giuridica si assume responsabilità.

Approfondimento 15: SW/HW

- Il primo problema da considerare è che se anche possiamo ritenere valida l'assunzione che il token crittografico si possa considerare una piattaforma trusted, che quindi assicura il requisito della segretezza per la chiave privata, lo stesso ovviamente non si può dire sulla piattaforma che ospita il software di firma.
- Un eventuale comportamento anomalo del SW di firma potrebbe pertanto comportare che mentre al firmatario viene presentato un certo documento, il digest inviato al token crittografico viene calcolato dal SW su un altro documento. Il risultato sarebbe quindi, da parte dell'attaccante, avere ottenuto una firma della vittima su un dato documento, all'insaputa di quest'ultimo.
- A meno quindi di non utilizzare dispositivi dedicati per la firma di documenti informatici, non è possibile, in linea di principio, escludere questa tipologia di attacco.
- Evidentemente è opportuno seguire buone prassi per mitigare il rischio di tale fattispecie, come l'uso di computer ben protetti e evitare di firmare documenti su piattaforme di terzi, se non fidati.

Approfondimento 16: attacchi alla immodificabilità (contenuti dinamici)

- Un'altra ben nota vulnerabilita` e` derivante dalla possibilita` per i documenti di incorporare macro-istruzioni o codice eseguibile (si pensi ad esempio alle *macro* dei documenti Word, oppure al codice Javascript dei documenti PDF). Un documento contenente istruzioni non e` statico, nel senso che la visualizzazione (la presentazione) del suo contenuto dipende da variabili legate all'ambiente in cui avviene la presentazione del documento. Ad esempio, si consideri il caso di un contratto (malicious) che include un valore dipendente dalla data del sistema (attraverso macrocodice), in modo tale che, dopo una certa data, la quantita` sia per esempio incrementata. La firma digitale dovrebbe garantire integrità non solo della rappresentazione binaria del documento, ma anche degli atti, fatti o dati in esso rappresentati. Nell'esempio in questione si comprende facilmente che la firma digitale non è in grado di raggiungere questo obiettivo, operando solo sulla rappresentazione binaria del documento (e quindi in questo caso delle macroistruzioni stesse) e non garantendo integrità della presentazione del documento.
- Questa classe di vulnerabilita` e` ben nota ed il modo per contrastarla e` banalmente quello di forzare l'utente a verificare il documento prima della firma, assumendo che egli sia consapevole circa gli strumenti capaci di rilevare e rimuovere possibili istruzioni malevole contenute nel documento. Un'ulteriore metodo suggerito e` quello di restringere i formati permessi per i documenti a quelli che non supportano l'inclusione di istruzioni, come il testo (es. ASCII) o PDF/A (PDF *Archive*), formati che non permettono l'inclusione di (macro)istruzioni e che siano *self-contained* (anche relativamente ai font).
- Gli attacchi sopra descritti sono possibili nel formato di firma CADES e, relativamente al formato PDF anche nel formato di firma PADES.

Approfondimento 17: attacchi alla immodificabilità (file pomimorfi)

- L'attacco qui descritto opera solo su formati di firma CADES, quindi in presenza di busta crittografica.
- In questo caso non si sfrutta la presenza di istruzioni nel documento né il fatto che la presentazione del documento è basata su font esterni. Non è richiesto quindi che il formato del documento abbia tale caratteristica di dinamicità. In altre parole, come vedremo, formati totalmente statici possono manifestare presentazioni ambigue.
- Il documento ambiguo (detto *polimorfo*) è ottenuto attraverso un'originale tecnica di *steganografia iniettiva* che permette al documento di essere visualizzato in accordo a due diversi formati, e presenta un diverso contenuto, in dipendenza dal formato scelto. L'effetto può essere in un certo senso accostato a quello di alcuni quadri del celebre pittore Salvator Dalì, tra i quali quello intitolato "*L'immagine scompare*") in cui due immagini, quella di una giovane donna e quella del ritratto di un baffuto anziano sono rappresentate allo stesso tempo, ciascuna conservando tuttavia la propria indipendenza. Tale ambiguità (che è stata pertanto denominata "*attacco Dalì*") può essere attivata, nella maggior parte dei sistemi operativi, semplicemente cambiando l'estensione nel nome del file, e non è certamente rilevata da un'eventuale firma digitale generata a partire dal documento stesso, come sopra evidenziato. Inoltre, se il formato del documento non è inserito negli attributi firmati della busta crittografica (cosa che avviene per esempio nel sistema di firma adottato dal nostro Paese), la modifica del nome della busta (ad esempio, da *contratto.pdf.p7m* a *contratto.tif.p7m*) consente di attivare l'ambiguità di presentazione del documento in fase di verifica della firma, in quanto l'applicazione invocata dal software di verifica della firma per visualizzare il documento sarà individuata semplicemente dall'estensione che appare nel nome della busta crittografica prima dell'estensione *.p7m*. Nel caso dell'esempio il software di verifica crederà che sia stato firmato un file in formato TIFF, quando invece il sottoscrittore intendeva firmare esclusivamente la "controparte" PDF.
- In particolare, è possibile realizzare un documento PDF che presenta un contenuto diverso se riconosciuto (e dunque visualizzato) come se fosse di tipo TIFF. In altri termini è possibile realizzare documenti polimorfi che mostrano diversi contenuti, pur apparendo sempre in formati ritenuti affidabili (PDF e TIFF). Si pensi, a titolo di esempio, ad un bilancio redatto da un dipendente infedele che utilizzi questa tecnica e presentato al firmatario nel formato PDF. Tale documento potrebbe essere archiviato, dopo la generazione della firma, nel formato TIFF (semplicemente cambiando il nome della busta crittografica da *bilancio.pdf.p7m* a *bilancio.tif.p7m*) e mostrare pertanto un contenuto diverso da quello sottoscritto ogni qual volta la firma sarà verificata e la busta "aperta".

Approfondimento 18: struttura di un file polimorfo

- La struttura di un file pdf standard è la seguente:
- **Header** (versione del PDF… %PDF -1.5)
- **Body** (il contenuto)
- **Xref** (una tabella contenente puntatori e altre info relativi agli oggetti del body)
- **Trailer** (contiene dove è localizzato Xref e un'oggetto speciale del body, e termina con %%EOF)
- Lo standard prevede che il %PDF appaia nei primi 1024 byte del file (retrocompatibilità)
- L'attaccante produce il "bad content" in un file tiff che è suddiviso in due parti (Head di pochi byte e Tail, con il contenuto malevolo)
- Un file tiff è una lista concatenata di oggetti, ognuno descritto da un IFD (image File Directory)
- L'attaccante nell'header modifica l'offset fino al primo IFD creando un "buco" dove inserire il file pdf…
- Siccome il reader pdf trova I puntatori a Xref e quindi al Body nel trailer, il file polimorfo dovrà avere il trailer alla fine del file. Quindi il contenuto tiff è incluso tra Xref e Trailer.

- Ulteriori dettagli possono essere trovati in: *Francesco Buccafurri, Gianluca Caminiti, Gianluca Lax:* ***Fortifying the dalì attack on digital signature*** *- Proceedings of the 2nd International Conference on Security of Information and Networks, SIN 2009, Gazimagusa, North Cyprus, October 6-10, 2009. ACM 2009, ISBN 978-1-60558-412-6*