Hash Crittografici, Firma Digitale e Infrastrutture di Certificazione X.509

Francesco BUCCAFURRI
Univ. Mediterranea di Reggio Calabria
bucca@unirc.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

Indice

© CINI – 2021

Introduzione

- L'obiettivo della firma digitale è fornire autenticazione di messaggi e garantire non ripudio
- 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.**

© CINI – 2021

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 si aprono problematiche specifiche

© CINI – 2021

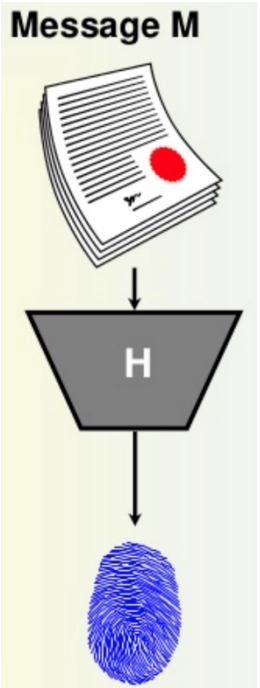
Firma come primitiva crittografica

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

© CINI – 2021

Funzioni Hash

- La funzione hash:
  - prende in input un blocco M di lunghezza variabile
  - genera un messaggio di impronta digitale a lunghezza fissa h = H(M).
- Non viene utilizzata alcuna chiave



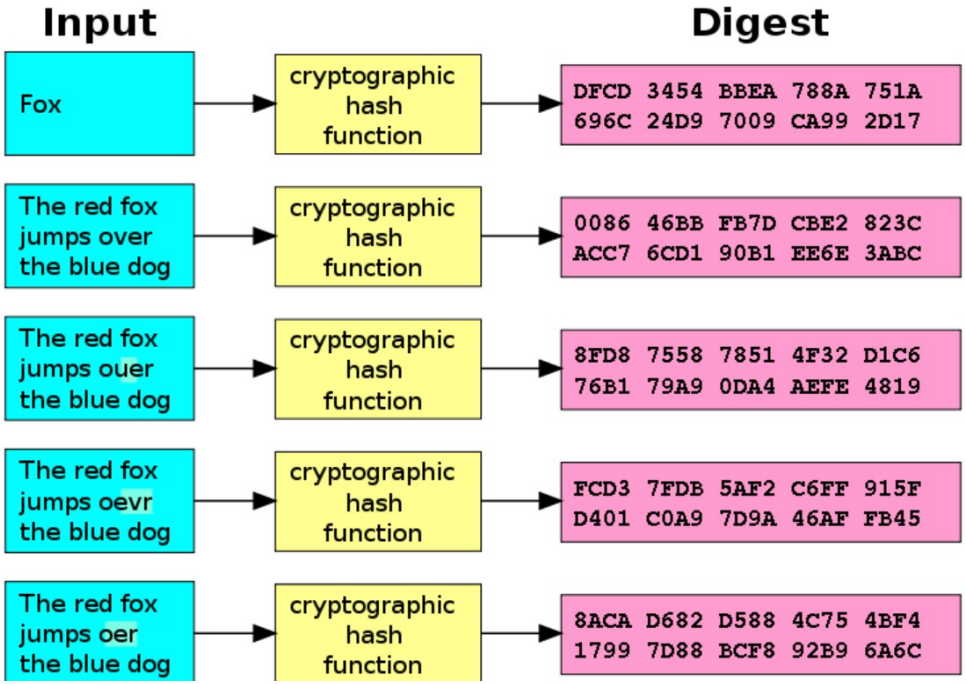
© CINI – 2021

Funzioni hash crittografiche

- Le funzioni hash di interesse per la sicurezza informatica sono le Funzioni hash crittografiche, cioè quei membri di una famiglia di funzioni che sono :
  - (1) One-way (non-invertibili)
  - (2) Weak Collision Resistance
  - (3) Strong Collision Resistance
- Se il digest è di k bit, (1) e (2) costano 2^k, (3) costa $2^{k/2}$

© CINI – 2021

Hashing crittografico: un esempio

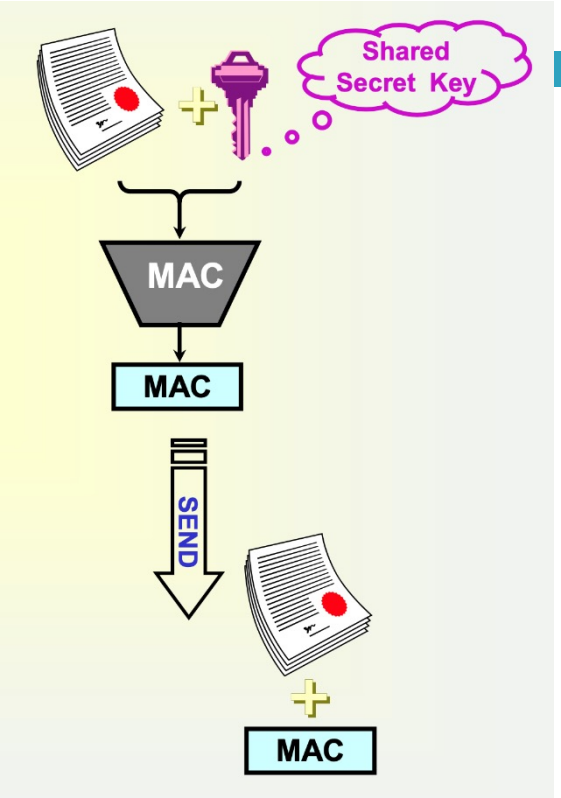


- Una funzione di hash crittografico all'opera: Un piccolo cambiamento nell'input ("over") cambia molto l'output.
- Effetto valanga se un input viene modificato legger–mente (anche di un solo bit), l'output cambia in modo significativo (metà dei bit di output).

© CINI – 2021

Autenticazione dei messaggi

- Le funzioni hash sono utilizzate per produrre *Message Authentication Codes* (MAC) per un messaggio M.
- In questo caso è necessario untilizzare una chiave segreta:
- MAC=h(f(k,M))



© CINI – 2021

HMAC

- HMAC (Hash-based MAC) è un tipo specifico di MAC che si basa sull'uso di una funzione hash crittografica e di una chiave crittografica segreta.
- HMAC può essere utilizzato per verificare contemporaneamente l'integrità dei dati e l'autenticità del messaggio.
- Qualsiasi funzione hash crittografica, come SHA-1 o SHA-2, può essere utilizzata nel calcolo di un HMAC; l'algoritmo MAC risultante è chiamato HMAC-X, dove X è la funzione hash utilizzata.

© CINI – 2021

Utilizzo degli hash

- Oltre che per l'autenticazione dei messaggi, l'hash può essere utilizzato per una serie di altri motivi:
  - Password a senso unico (one-way)
  - Rilevamento delle intrusioni
  - Generatore di numeri casuali (PRNG)
  - Firma digitale

© CINI – 2021

Password one-way

- In alcuni sistemi operativi le password non sono memorizzate per intero, ma solo il loro hash viene conservato nel file delle password.
- Chi entrasse in possesso del file di password non sarebbe in grado di ottenere la password dall'hash.
- Quando un utente digita una password, il sistema calcola l'hash e lo confronta con il valore corrispondente nel file di password.
- Quando si resetta la password e non si riceve in cambio la password in chiaro, spesso è perché il sistema non l'ha memorizzata in chiaro.

© CINI – 2021

Controllo delle differenze ottimizzato

- Intrusion Detection: Gli hash sono calcolati per ogni file di un computer, evse un virus modifica il file, la modifica può essere rilevata ricalcolando l'hash e confrontandolo con quello originale.
- Version control: Molte applicazioni permettono a diversi utenti di modificare contemporaneamente e sincronizzare la modifica sui file condivisi. I servizi di versioning utilizzano funzioni hash per determinare se i file sul server e i file locali sono gli stessi e trasferiscono solo quelli che sono stati modificati.

© CINI – 2021

Generazione di numeri pseudo casuali

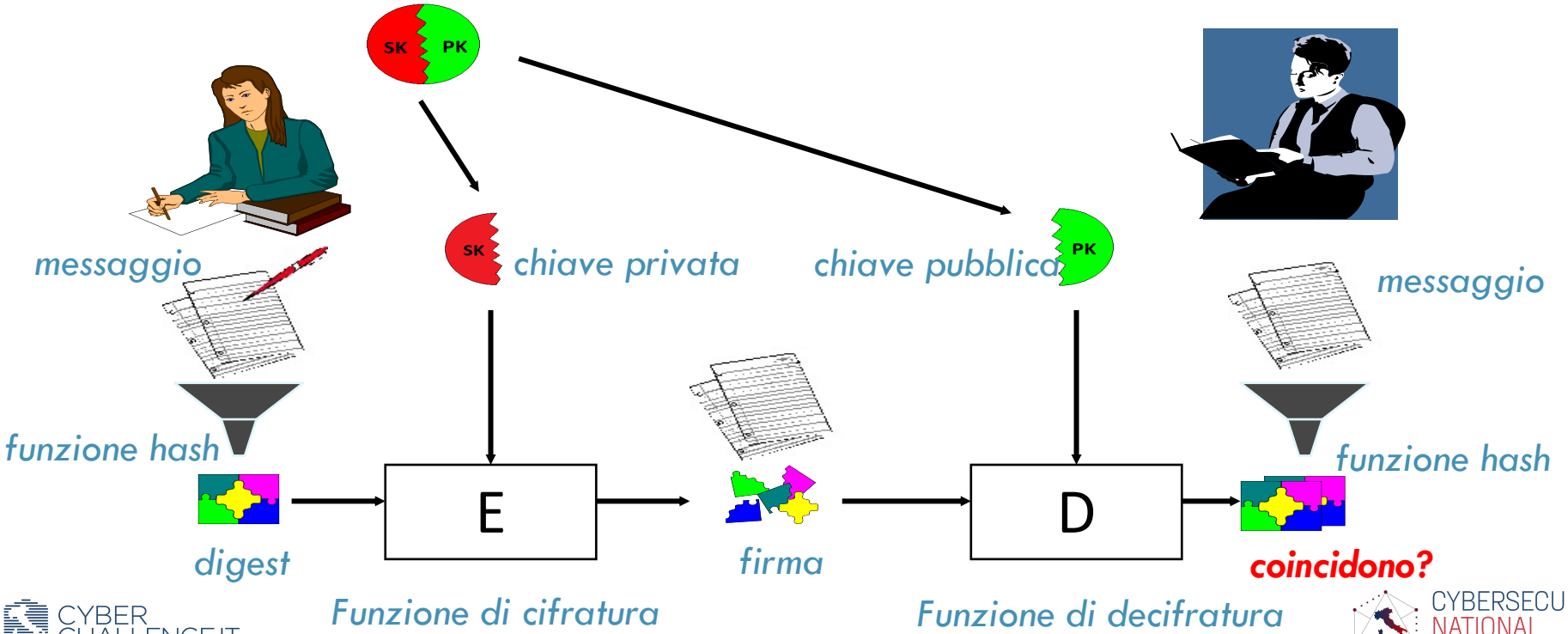
- L'hashing viene utilizzato anche per generare numeri casuali:

  n = hash(seme).

- Il risultato è un numero effettivamente pseudo-casuale perché una funzione crittografica di hash prende in ingresso una quantità variabile di dati ed emette un blocco a lunghezza fissa.
- Se il seme viene scelto con cura e dato in ingresso ad un hash crittografico, a causa dell'effetto valanga, l'uscita conterrà bit uniformemente distribuiti.

© CINI – 2021

Schema basato su crittografia a chiave pubblica e hash crittografico



© CINI – 2021

Firma Digitale e Documento Informatico

Firma come istituto giuridico

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

Documento informatico

- Funzione indicativa
- Funzione dichiarativa
- Funzione probatoria

© CINI – 2021

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.***

© CINI – 2021

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

© CINI – 2021

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

© CINI – 2021

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)

© CINI – 2021

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*
  - ASIC-S, ASIC-E (Associated Signature Container)
- I formati più utilizzati in Italia sono CADES e PADES

© CINI – 2021

Revoca dei Certificati

Il certificato può essere revocato su iniziativa del Certificatore o per richiesta del titolare. Motivi di revoca potrebbero essere i seguenti:

- Smarrimento o guasto al dispositivo di firma
- Smarrimento della chiave segreta o del codice di attivazione del dispositivo di firma
- Perdita della segretezza della chiave segreta o del codice di attivazione del dispositivo di firma
- Modifica dei dati del titolare
- Termine del contratto tra titolare e Certificatore
- Violazione da parte del titolare delle regole di utilizzo del dispositivo

© CINI – 2021

Revoca dei Certificati

- 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)

© CINI – 2021

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

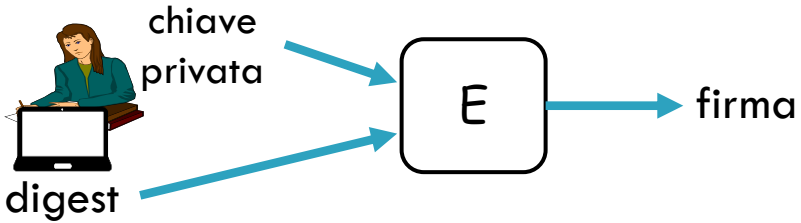
© CINI – 2021

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

© CINI – 2021

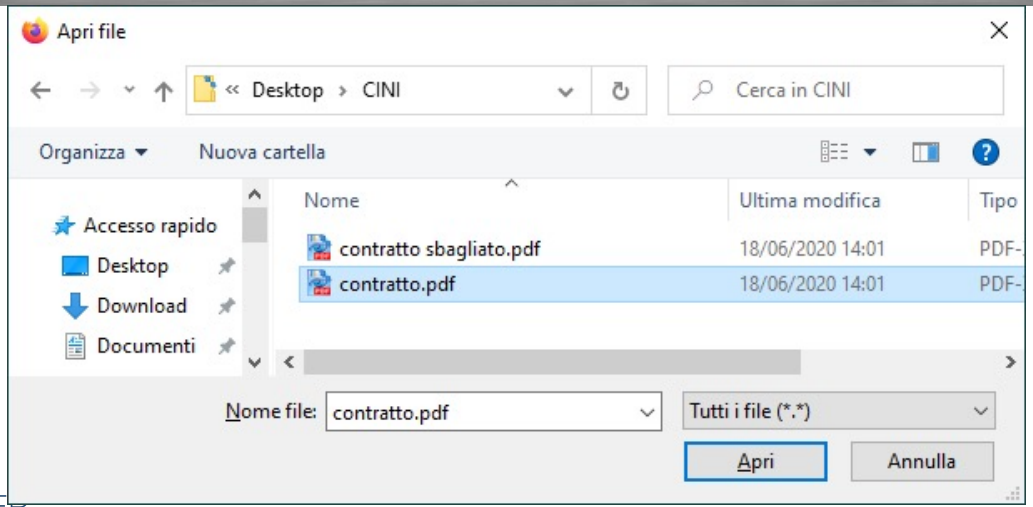
Vulnerabilità connesse al processo di generazione della firma



- Utilizzo di crittografia asimmetrica o funzione hash crittografica poco robuste
  - Stabilite dalle regole tecniche e gestite dal software

© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma



Digest
(di contratto.pdf)

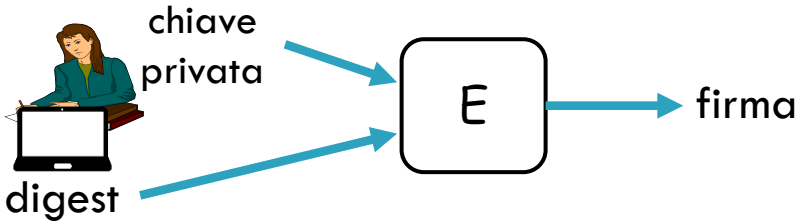
© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma

- Chi ci assicura che il file firmato sia proprio quello?
- Piattaforma software non trusted (invio malicious dell'hash alla smart card, gestione fraudolenta del controllo di validità del certificato, e molto altro)
  - Non usare piattaforme di terzi (HW,SW) se non fidati
  - Proteggere il computer (antivirus, firewall, installare solo software genuino, non condividere la piattaforma, usare credenziali di accesso, etc.)

© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma



- Segretezza della chiave
- La chiave non può essere gestita dall'utente
- La chiave non può essere gestita dal PC
  - La permanenza (anche temporanea) nella RAM del PC della chiave privata ne metterebbe a repentaglio la segretezza

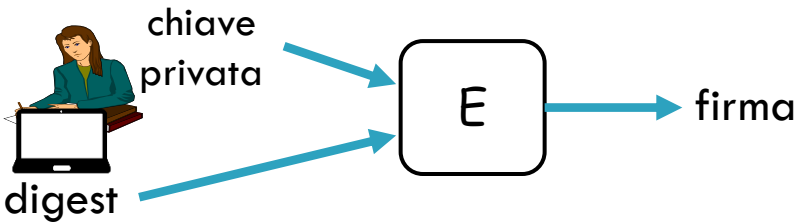
© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma: dispositivo di firma

- Viene 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

© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma: dispositivo di firma

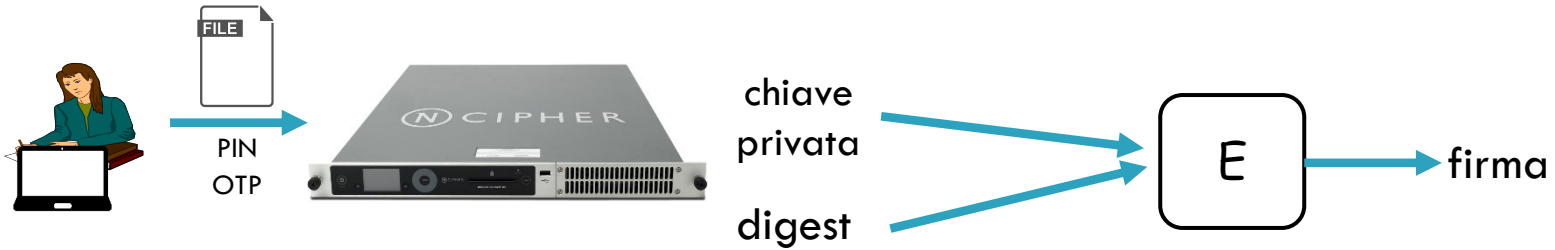


Uso token USB

- PC calcola digest
- Utente inserisce PIN
- Token USB usa la chiave privata per implementare E

© CINI – 2021

Vulnerabilità connesse al processo di generazione della firma: dispositivo di firma



- Uso Hardware Security Module (HSM)
  - elaborazione crittografica, generazione e memorizzazione delle chiavi
  - conformità normativa
  - prestazioni

© CINI – 2021

Vulnerabilità connesse alla immodificabilità del contenuto

- Un'altra minaccia deriva 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)

© CINI – 2021

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 (ad esempio in campo sanitario)
- Si pone pertanto il problema della **adeguatezza dei formati**
- Ai documenti (ai formati) è richiesta la caratteristica della **staticità**: essa 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

© CINI – 2021

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*
  - *la capacità di essere immune dall'inserimento di codice maligno*

© CINI – 2021

Vulnerabilità connesse alla immodificabilità del contenuto

- Nota bene: documento informatico, firma, chiave privata, …, sono tutte sequenze di bit

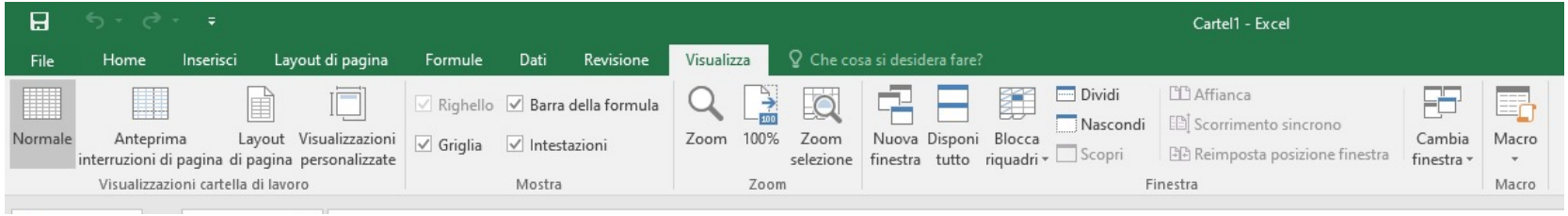
```
00111101000000010110111
10111001110111111001010
11001011101010000010100
10100110100011101001101
11101000110000111000001
01010100100000000111011
11100010011011001100010
```

- La firma garantisce l'immodificabilità dei bit non di come sono visualizzati

© CINI – 2021

Minacce relative ai documenti informatici: contenuti dinamici

- Inclusione di macro codice, funzioni, JavaScripts



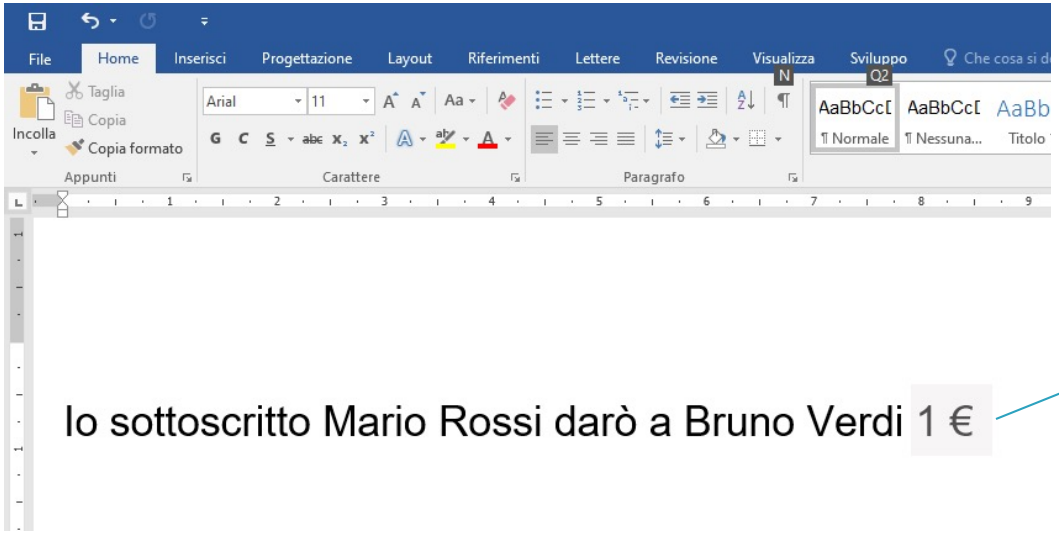

```
Private Sub Workbook_Open()
        Selection.Find.Replacement.ClearFormatting
        With Selection.Find
             .Text = "1"
             .Replacement.Text = "1000"
             .Forward = True
             .Wrap = wdFindContinue
        End With
        Selection.Find.Execute Replace:=WdReplace
End Sub
```

Kain, K., Smith, S.W., and Asokan, R. (2002). Digital signatures and electronic documents: A cautionary tale. In Advanced communications and multimedia security, pp. 293–307. Springer US.

© CINI – 2021

Minacce relative ai documenti informatici: contenuti dinamici

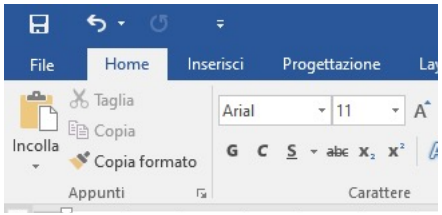
- Riferimento a risorse esterne



© CINI – 2021

Minacce relative ai documenti informatici: contenuti dinamici

- Uso improprio di font



Sostituzione di fonti	
A	C
I	A
C	R
E	K

© CINI – 2021

Minacce relative ai documenti informatici: contenuti dinamici

- Contromisure:
  - Formati statici (no Word, Excel, HTML; si PDF, PDF/A; TIF)
  - Blocco dei font
  - Uso di sandbox
  - Usare document parser

© CINI – 2021

Minacce relative ai documenti informatici: file polimorfi

Dalì attack - Buccafurri, F., Caminiti, G., & Lax, G. (2008), nome ispirato al quadro di Dalì «*the image disappears*»

- 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

© CINI – 2021

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

© CINI – 2021

Hash Crittografici, Firma Digitale e Infrastrutture di Certificazione X.509

Francesco BUCCAFURRI
Univ. Mediterranea di Reggio Calabria
bucca@unirc.it

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it