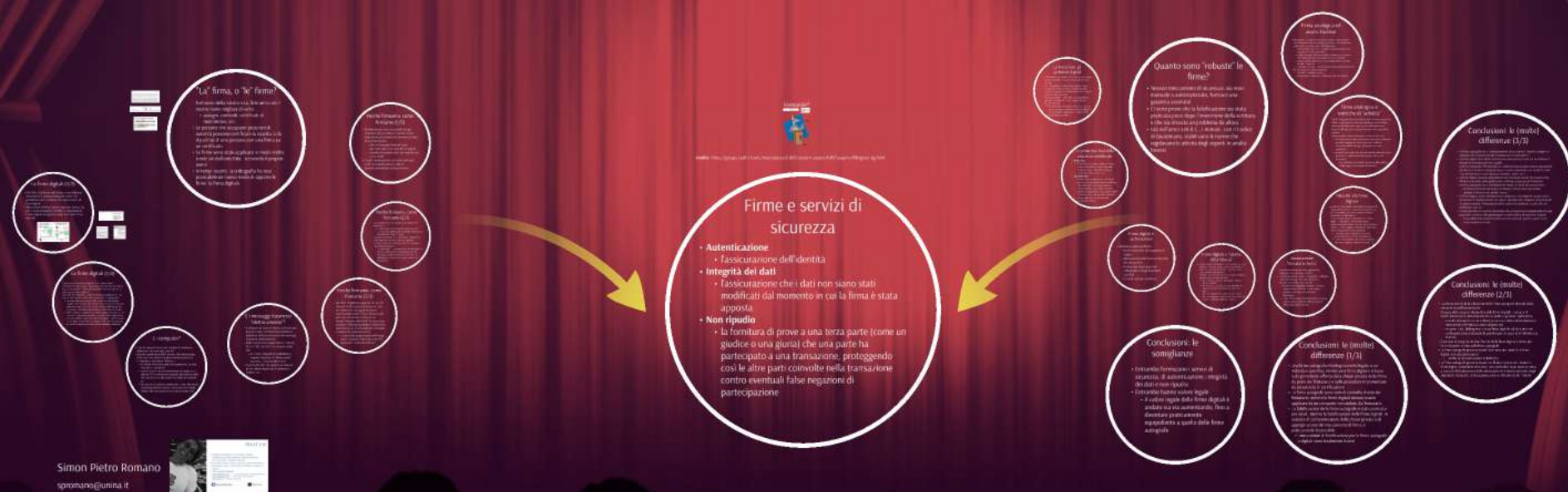


Asciutta o bagnata?

Un incontro-scontro tra firma digitale e firma grafica dal punto di vista della sicurezza





Asciutta o bagnata?

o-scontro tra firma digitale e firma grafica dal punto di vista dell



Simon Pietro Romano

spromano@unina.it



About me

- Professor at Federico II University in Napoli:
Teaching Computer Networks, Web & Real Time Communication, Network Security
- Scientific Director of the Accenture Cyber HackAdemy
- Managing Director of the Apple Developer Academy in Napoli
- Tech transfer addicted:
www.epsilononline.com —> cloud, web apps, microservices, etc.
www.meetecho.com —> real-time communication
www.secsi.io —> network security



spromano@unina.it



@spromano

- Nel corso della nostra vita, firmiamo con il nostro nome migliaia di volte:
 - assegni, contratti, certificati di matrimonio, ecc.
- Le persone che occupano posizioni di autorità possono certificare la nascita (o la dipartita) di una persona con una firma su un certificato
- Le firme sono state applicate in modo molto simile sin dall'antichità: scrivendo il proprio nome
- In tempi recenti, la crittografia ha reso praticabile un nuovo modo di apporre le firme: la firma digitale

firma

s. f. [der. di *firmare*]. – **1. a.** Il nome e il cognome con cui si sottoscrive un documento per conferma o accettazione del contenuto, una lettera o cartolina per indicare il mittente (e in questo caso può essere costituita anche dal solo nome o dal solo cognome), un'opera d'arte per attestare e garantire in qualche modo la proprietà artistica (nel caso di articoli a stampa, e di altri stampati o manifesti, il nome e cognome dell'autore stampato in calce): *mettere, apporre la propria f.; cartolina con sole f.; quadro d'autore con f., senza f.; autenticare, legalizzare una f.; falsificare, imitare una f.; avere una f. chiara, illeggibile; raccogliere (le) firme*, per una petizione, un'iniziativa, un referendum e sim.; *f. in bianco*, apposta a un documento non ancora completo; *registro delle f.*, quello che raccoglie le firme dei visitatori di una mostra, di un museo e sim.; *metterci (o farci) la f., fig., fam.*, accettare con enorme piacere un incarico, una certa condizione, ecc. (spec. in espressioni come *ci farei, ci metterei la f.!* e

dei visitatori di una mostra, di un museo e sim.; *metterci* (o *farcì*) *la f.*, fig., fam., accettare con enorme piacere un incarico, una certa condizione, ecc. (spec. in espressioni come *ci farei*, *ci metterei la f.*! e

Simon P. Roman

Fi... ..

Firmato digitalmente da

SIMON PIETRO ROMANO

CN = ROMANO SIMON PIETRO
O = UNIVERSITA DEGLI STUDI DI
NAPOLI FEDERICO II°
C = IT

Perché firmiamo, come firmiamo (1/3)

- Probabilmente non sorprende che gli inventori della scrittura, i Sumeri, siano stati anche gli inventori di un meccanismo di autenticazione:
 - essi utilizzavano intricati sigilli, applicati sulle loro tavolette di argilla cuneiformi usando rulli, per autenticare i loro scritti
- I sigilli continuarono ad essere utilizzati come principale meccanismo di autenticazione fino a tempi recenti

- Probabilmente non sorprende che gli inventori della scrittura, i Sumeri, siano stati anche gli inventori di un meccanismo di autenticazione:
 - essi utilizzavano intricati sigilli, applicati sulle loro tavolette di argilla cuneiformi usando rulli, per autenticare i loro scritti
- I sigilli continuarono ad essere utilizzati come principale meccanismo di autenticazione fino a tempi recenti

Perché firmiamo, come firmiamo (2/3)

- L'uso delle firme è documentato nel Talmud (IV secolo d.C.)
 - il testo sacro include anche le procedure di sicurezza da applicare per prevenire l'alterazione dei documenti dopo la firma
- La pratica di autenticare i documenti apponendo firme manoscritte iniziò ad essere utilizzata nell'Impero Romano nell'anno 439 d.C., durante il regno di Valentiniano III:
 - la "subscripto" - una breve frase manoscritta alla fine di un documento che dichiarava che il firmatario "sottoscriveva" il documento - fu utilizzata per la prima volta per autenticare i testamenti

- L'uso delle firme è documentato nel Talmud (IV secolo d.C.)
 - il testo sacro include anche le procedure di sicurezza da applicare per prevenire l'alterazione dei documenti dopo la firma
- La pratica di autenticare i documenti apponendo firme manoscritte iniziò ad essere utilizzata nell'Impero Romano nell'anno 439 d.C., durante il regno di Valentiniano III:
 - la "subscripto" - una breve frase manoscritta alla fine di un documento che dichiarava che il firmatario "sottoscriveva" il documento - fu utilizzata per la prima volta per autenticare i testamenti

Perché firmiamo, come firmiamo (3/3)

- Nel 1677, l'Inghilterra approvò "An Act for Prevention of Frauds and Perjuries", che richiedeva che "una qualche nota o memorandum scritto" fosse "firmato dalle parti" per alcuni tipi di transazioni
- Questo "Statuto delle Frodi" ha avuto una profonda influenza sul diritto commerciale statunitense ed è l'antecedente del Codice Commerciale Uniforme (UCC)
 - la base della maggior parte delle leggi statali e federali degli Stati Uniti che regolano le "transazioni di beni"

- Nel 1677, l'Inghilterra approvò "An Act for Prevention of Frauds and Perjuries", che richiedeva che "una qualche nota o memorandum scritto" fosse "firmato dalle parti" per alcuni tipi di transazioni
- Questo "Statuto delle Frodi" ha avuto una profonda influenza sul diritto commerciale statunitense ed è l'antecedente del Codice Commerciale Uniforme (UCC)
 - la base della maggior parte delle leggi statali e federali degli Stati Uniti che regolano le "transazioni di beni"

E i messaggi trasmessi "elettricamente"?

- Il telegrafo di Samuel Morse, utilizzato per la prima volta nel 1844, ha introdotto il problema dell'autenticazione dei messaggi trasmessi elettricamente
- Nella controversia legale Trevor v. Wood, 36 N.Y. 307, nel 1867, il tribunale stabilì che:
 - le "firme" telegrafiche soddisfano i requisiti legali per le "firme scritte" secondo lo Statuto delle Frodi
- Si potrebbe dire che questa sia stata la prima vittoria legale per il commercio elettronico!

• Nel
Prev
richi
mem
part
• Que
prof
statu
Com
• I
s
n

- Il telegrafo di Samuel Morse, utilizzato per la prima volta nel 1844, ha introdotto il problema dell'autenticazione dei messaggi trasmessi elettricamente
- Nella controversia legale Trevor v. Wood, 36 N.Y. 307, nel 1867, il tribunale stabilì che:
 - le "firme" telegrafiche soddisfano i requisiti legali per le "firme scritte" secondo lo Statuto delle Frodi
- Si potrebbe dire che questa sia stata la prima vittoria legale per il commercio elettronico!

E i computer?

- L'uso di computer in rete per condurre il commercio elettronico è iniziato negli anni '60
- Durante i primi tempi dell'Electronic Data Interchange (EDI), non c'era modo di applicare firme basate sulla crittografia ai documenti elettronici
 - le industrie facevano molto affidamento su "accordi tra partner commerciali"
 - questi accordi cartacei descrivevano le regole a cui i partner EDI si attenevano riguardo alla gestione delle richieste d'ordine, alla risoluzione delle controversie, ecc.
 - Gli accordi tra partner commerciali si sono dimostrati straordinariamente efficaci, con controversie legali relative alle transazioni EDI eccezionalmente rare

- L'uso di computer in rete per condurre il commercio elettronico è iniziato negli anni '60
- Durante i primi tempi dell'Electronic Data Interchange (EDI), non c'era modo di applicare firme basate sulla crittografia ai documenti elettronici
 - le industrie facevano molto affidamento su "accordi tra partner commerciali"
 - questi accordi cartacei descrivevano le regole a cui i partner EDI si attenevano riguardo alla gestione delle richieste d'ordine, alla risoluzione delle controversie, ecc.
 - Gli accordi tra partner commerciali si sono dimostrati straordinariamente efficaci, con controversie legali relative alle transazioni EDI eccezionalmente rare

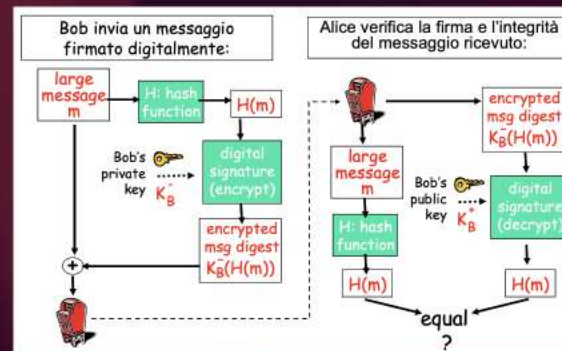
Le firme digitali (1/2)

- Il mezzo per fornire firme digitali per le comunicazioni informatiche, grosso modo equivalenti alle firme manoscritte su documenti cartacei, è divenuto disponibile con l'avvento della tecnologia a chiave pubblica
- Nel 1976, Whitfield Diffie e Martin Hellman pubblicarono il loro documento fondamentale "New Directions in Cryptography"
 - l'articolo delineava come il difficile problema di risolvere logaritmi discreti nei campi finiti potesse essere utilizzato per sviluppare coppie di chiavi asimmetriche pubbliche/private che avevano un chiaro potenziale per l'uso nelle reti di dati
 - Diffie e Hellman suggerirono, in modo piuttosto profetico, che i servizi di "autenticazione unidirezionale" offerti dagli schemi a chiave pubblica sarebbero stati di maggiore importanza per la comunità imprenditoriale rispetto ai servizi di riservatezza per cui la crittografia era stata tradizionalmente utilizzata

- Il mezzo per fornire firme digitali per le comunicazioni informatiche, grosso modo equivalenti alle firme manoscritte su documenti cartacei, è divenuto disponibile con l'avvento della tecnologia a chiave pubblica
- Nel 1976, Whitfield Diffie e Martin Hellman pubblicarono il loro documento fondamentale "New Directions in Cryptography"
 - l'articolo delineava come il difficile problema di risolvere logaritmi discreti nei campi finiti potesse essere utilizzato per sviluppare coppie di chiavi asimmetriche pubbliche/private che avevano un chiaro potenziale per l'uso nelle reti di dati
 - Diffie e Hellman suggerirono, in modo piuttosto profetico, che i servizi di "autenticazione unidirezionale" offerti dagli schemi a chiave pubblica sarebbero stati di maggiore importanza per la comunità imprenditoriale rispetto ai servizi di riservatezza per cui la crittografia era stata tradizionalmente utilizzata

Le firme digitali (2/2)

- Nel 1978, Ron Rivest, Adi Shamir e Len Adleman inventarono il sistema crittografico RSA, che permetteva sia la cifratura che l'applicazione di firme digitali
- Altri schemi di firma digitale seguirono presto, tra cui la tecnica ElGamal nel 1985 e lo Standard di Firma Digitale del governo degli Stati Uniti (DSS) nel 1991



Napoli, 28 novembre 2023

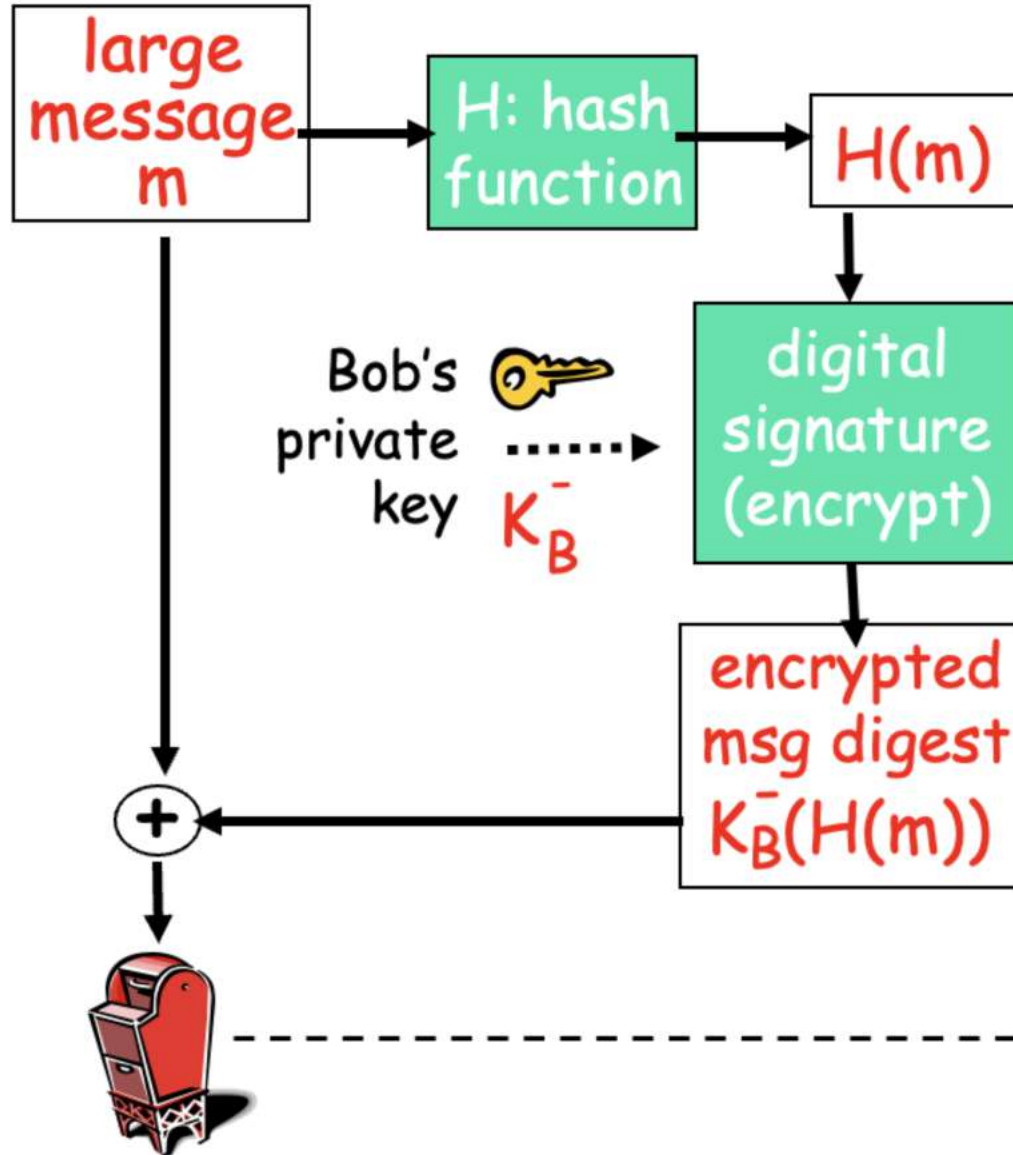
Prof. Simon Pietro Romano
Ordinario di Network Security presso
l'Università degli Studi di Napoli Federico II

Firmato digitalmente da
SIMON PIETRO ROMANO
CN = ROMANO SIMON PIETRO
O = UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II
C = IT

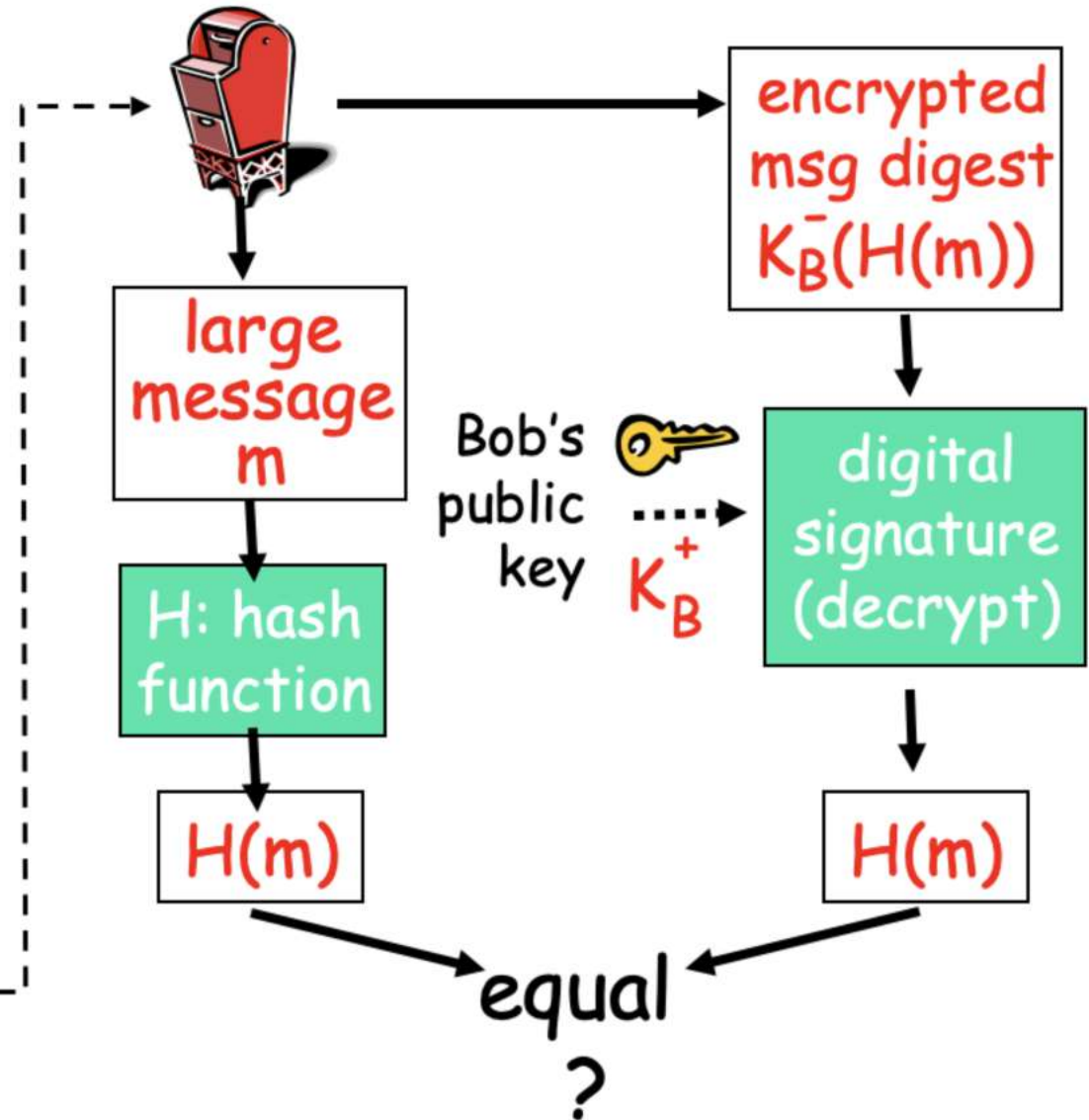


- Nel 1978, Ron Rivest, Adi Shamir e Len Adleman inventarono il sistema crittografico RSA, che permetteva sia la cifratura che l'applicazione di firme digitali
- Altri schemi di firma digitale seguirono presto, tra cui la tecnica ElGamal nel 1985 e lo Standard di Firma Digitale del governo degli Stati Uniti (DSS) nel 1991

Bob invia un messaggio
firmato digitalmente:



Alice verifica la firma e l'integrità
del messaggio ricevuto:



Napoli, 28 novembre 2023

Prof. Simon Pietro Romano
Ordinario di Network Security presso
l'Università degli Studi di Napoli Federico II

Firmato digitalmente da

SIMON PIETRO ROMANO

CN = ROMANO SIMON PIETRO
O = UNIVERSITA DEGLI STUDI DI
NAPOLI FEDERICO II°
C = IT

Proprietà firma



La firma è VALIDA, firmata da ROMANO SIMON PIETRO <spromano@unina.it>.

Ora firma: 2023/11/29 15:50:32 +02'00'

Origine affidabilità da European Union Trusted Lists (EUTL).



Firma elettronica qualificata conforme al Regolamento europeo 910/2014

Motivo:

Luogo:

Riepilogo validità

Il documento non è stato modificato dopo l'apposizione della firma.

Il certificatore ha specificato che le azioni di compilazione moduli, firma e commento sono consentite per questo documento. Non sono consentite altre modifiche.

L'identità del firmatario è valida.

L'ora della firma proviene dall'orologio del computer del firmatario.

La firma è stata convalidata all'ora della firma:
2023/11/29 15:50:32 +02'00'

Informazioni firmatario

Il percorso dal certificato del firmatario al certificato di un emittente è stato creato in modo corretto.

Il certificato del firmatario è valido e non è stato revocato.

[Mostra certificati firmatario...](#)

[Proprietà avanzate...](#)

[Chiudi](#)

[Verifica firma](#)

Visualizzatore certificati

Questa finestra di dialogo consente di visualizzare i dettagli di un certificato e dell'intera catena di emissione. I dettagli corrispondono alla voce selezionata.

☐ Mostra tutti i percorsi di certificazione trovati

ArubaPEC S.p.A. NG CA

ROMANO SIMON PIE

Riepilogo

Dettagli

Revoca

Affidabilità

Policy

Nota legale



ROMANO SIMON PIETRO <spromano@unina.it>

UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II°

Emesso da: ArubaPEC S.p.A. NG CA 3

Certification AuthorityC

Valido da: 2018/08/28 02:00:00 +02'00'

Valido fino a: 2024/08/28 01:59:59 +02'00'

Utilizzo: Non disconoscibilità



Certificato qualificato conforme al Regolamento europeo 910/2014 Allegato I

La chiave privata relativa a questo certificato risiede in un dispositivo per la creazione di una firma qualificata (QSCD, Qualified Signature Creation Device)

Esporta...



Il percorso del certificato selezionato è valido.

La convalida del percorso e i controlli della revoca sono stati effettuati all'ora della firma:

2023/11/29 15:50:32 +02'00'

Modello di convalida: shell

OK

Firme e servizi di sicurezza

- **Autenticazione**
 - l'assicurazione dell'identità
- **Integrità dei dati**
 - l'assicurazione che i dati non siano stati modificati dal momento in cui la firma è stata apposta
- **Non ripudio**
 - la fornitura di prove a una terza parte (come un giudice o una giuria) che una parte ha partecipato a una transazione, proteggendo così le altre parti coinvolte nella transazione contro eventuali false negazioni di partecipazione

- **Autenticazione**
 - l'assicurazione dell'identità
- **Integrità dei dati**
 - l'assicurazione che i dati non siano stati modificati dal momento in cui la firma è stata apposta
- **Non ripudio**
 - la fornitura di prove a una terza parte (come un giudice o una giuria) che una parte ha partecipato a una transazione, proteggendo così le altre parti coinvolte nella transazione contro eventuali false negazioni di partecipazione

Quanto sono "robuste" le firme?

- Nessun meccanismo di sicurezza, sia esso manuale o automatizzato, fornisce una garanzia assoluta!
- Ci sono prove che la falsificazione sia stata praticata poco dopo l'invenzione della scrittura, e che sia rimasta un problema da allora
- Già nell'anno 539 d.C., i Romani, con il Codice di Giustiniano, stabilivano le norme che regolavano le attività degli esperti in analisi forensi

e: gli
igitali

chiviazione a lungo
ati agli archivisti

o digitalmente,
omento della
zione che indica chi

responsabile di
egrità dei dati

dell'archiviazione,
e la firma digitale
i pattern di bit

Le prime due fasi della
vita di un certificato

Prima fase:

- il certificato è ancora valido e i dati di revoca dovrebbero essere disponibili tramite i canali 'normali' (directory, verifiche online, e così via)

Seconda fase:

- Gli esperti di analisi forense confrontano una firma sospetta con valide note e cercano segni di:
 - firme scritte a una velocità rispetto alle firme autentiche
 - cambi frequenti della pressione
 - Estremità delle linee smussate
 - Scarsa qualità della linea
 - Ricalchi e ritocchi
 - "Fermate" in punti in cui la scrittura non dovrebbe fermarsi
- Queste tecniche sono integrate da:
 - analisi di inchiostro e carta
 - rilevamento elettrostatico

- Nessun meccanismo di sicurezza, sia esso manuale o automatizzato, fornisce una garanzia assoluta!
- Ci sono prove che la falsificazione sia stata praticata poco dopo l'invenzione della scrittura, e che sia rimasta un problema da allora
- Già nell'anno 539 d.C., i Romani, con il Codice di Giustiniano, stabilivano le norme che regolavano le attività degli esperti in analisi forensi

Firma analogica ed analisi forense

- Gli esperti di analisi forense di documenti comunemente confrontano una firma sospetta con diversi esempi di firme valide note e cercano segni di falsificazione:
 - firme scritte a una velocità significativamente più lenta rispetto alle firme autentiche
 - cambi frequenti della presa dello strumento di scrittura
 - Estremità delle linee smussate all'inizio e alla fine
 - Scarsa qualità della linea, con ondeggiamenti e tremori
 - Ricalchi e ritocchi
 - "Fermate" in punti in cui la scrittura dovrebbe essere fluida
- Queste tecniche sono integrate da:
 - analisi di inchiostro e carta
 - rilevamento elettrostatico delle impronte di scrittura

- Gli esperti di analisi forense di documenti comunemente confrontano una firma sospetta con diversi esempi di firme valide note e cercano segni di falsificazione:
 - firme scritte a una velocità significativamente più lenta rispetto alle firme autentiche
 - cambi frequenti della presa dello strumento di scrittura
 - Estremità delle linee smussate all'inizio e alla fine
 - Scarsa qualità della linea, con ondeggiamenti e tremori
 - Ricalchi e ritocchi
 - "Fermate" in punti in cui la scrittura dovrebbe essere fluida
- Queste tecniche sono integrate da:
 - analisi di inchiostro e carta
 - rilevamento elettrostatico delle impronte di scrittura

Firma analogica e metriche di "solidità"

- È difficile quantificare la solidità delle firme manoscritte
- Il livello di garanzia che si può attribuire a una firma manoscritta dipende in gran parte dall'esperienza tecnica dell'esperto di analisi forense incaricato della verifica
- Falsari esperti hanno successo, in alcuni casi, ma...
 - le firme manoscritte continuano ad essere utilizzate perché, in generale, forniscono un livello di sicurezza sufficiente per gli scopi a cui sono applicate
 - quando sono richiesti meccanismi di autenticazione più forti, si utilizzano firme autenticate e con testimoni
 - es: "cerimonie di firma" associate alla ratifica delle leggi o alla stipula di trattati)

- È difficile quantificare la solidità delle firme manoscritte
- Il livello di garanzia che si può attribuire a una firma manoscritta dipende in gran parte dall'esperienza tecnica dell'esperto di analisi forense incaricato della verifica
- Falsari esperti hanno successo, in alcuni casi, ma...
 - le firme manoscritte continuano ad essere utilizzate perché, in generale, forniscono un livello di sicurezza sufficiente per gli scopi a cui sono applicate
 - quando sono richiesti meccanismi di autenticazione più forti, si utilizzano firme autenticate e con testimoni
 - es: "cerimonie di firma" associate alla ratifica delle leggi o alla stipula di trattati)

Attacchi alla firma digitale

- La falsificazione delle firme digitali, in assenza di compromissione della chiave privata di firma (o di "dirottamento" del meccanismo di firma) è praticamente impossibile
- A causa della natura crittografica delle firme digitali, i tentativi di falsificazione sono immediatamente evidenti a qualsiasi verificatore
- Tuttavia, le firme digitali richiedono l'intervento di un computer per essere applicate
 - i computer sono soggetti sia ad errori accidentali che a sovversioni malevole
 - le firme manoscritte, per la loro semplicità, non sono soggette a queste vulnerabilità

- La falsificazione delle firme digitali, in assenza di compromissione della chiave privata di firma (o di "dirottamento" del meccanismo di firma) è praticamente impossibile
- A causa della natura crittografica delle firme digitali, i tentativi di falsificazione sono immediatamente evidenti a qualsiasi verificatore
- Tuttavia, le firme digitali richiedono l'intervento di un computer per essere applicate
 - i computer sono soggetti sia ad errori accidentali che a sovversioni malevole
 - le firme manoscritte, per la loro semplicità, non sono soggette a queste vulnerabilità

Associazione "firmatario-firma"

- Una firma manoscritta è biologicamente collegata a un individuo specifico
- I sistemi di autenticazione crittografica collegano invece le firme agli individui attraverso meccanismi tecnici e procedurali
 - esistono forti legami matematici tra una chiave privata di firma, la sua chiave pubblica associata e la firma del messaggio...
 - ...ma l'associazione tra il firmatario e la sua chiave privata dipende dalla protezione offerta alla chiave privata

- Una firma manoscritta è biologicamente collegata a un individuo specifico
- I sistemi di autenticazione crittografica collegano invece le firme agli individui attraverso meccanismi tecnici e procedurali
 - esistono forti legami matematici tra una chiave privata di firma, la sua chiave pubblica associata e la firma del messaggio...
 - ...ma l'associazione tra il firmatario e la sua chiave privata dipende dalla protezione offerta alla chiave privata

o di
ei dati

Firme digitali e "catena della fiducia"

- L'associazione tra il firmatario e la sua chiave pubblica dipende dall'onestà e dalla diligenza dell'Autorità di Certificazione (CA) che rilascia il certificato della chiave pubblica del firmatario
- Pertanto, la solidità dei servizi di sicurezza forniti da una firma digitale è una funzione:
 - dei metodi utilizzati per proteggere la chiave privata di firma
 - dei metodi utilizzati dalla CA per identificare e autenticare coloro che richiedono certificati digitali
 - delle protezioni fornite contro le CA corrotte
 - delle salvaguardie contro la compromissione dei computer utilizzati dalla CA, e così via

- Un col
- I si inv me

- L'associazione tra il firmatario e la sua chiave pubblica dipende dall'onestà e dalla diligenza dell'Autorità di Certificazione (CA) che rilascia il certificato della chiave pubblica del firmatario
- Pertanto, la solidità dei servizi di sicurezza forniti da una firma digitale è una funzione:
 - dei metodi utilizzati per proteggere la chiave privata di firma
 - dei metodi utilizzati dalla CA per identificare e autenticare coloro che richiedono certificati digitali
 - delle protezioni fornite contro le CA corrotte
 - delle salvaguardie contro la compromissione dei computer utilizzati dalla CA, e così via

Firme digitali e archiviazione

- Almeno quattro problemi:
 - Deterioramento del supporto di origine
 - Obsolescenza del formato dei dati del documento
 - Evoluzione degli algoritmi crittografici e degli standard correlati
 - Ciclo di vita dei certificati

- L'as...
- dip...
- Ce...
- chi...
- Per...
- un...

- Almeno quattro problemi:
 - Deterioramento del supporto di origine
 - Obsolescenza del formato dei dati del documento
 - Evoluzione degli algoritmi crittografici e degli standard correlati
 - Ciclo di vita dei certificati

Le prime due fasi della vita di un certificato

- **Prima fase:**
 - il certificato è ancora valido e i dati di revoca dovrebbero essere disponibili tramite i canali 'normali' (directory, verifiche online, e così via)
- **Seconda fase:**
 - inizia con la scadenza del certificato
 - per un certo periodo dopo la scadenza del certificato, un'infrastruttura a chiave pubblica dovrebbe essere in grado di supportare la risoluzione delle controversie di non ripudio fornendo prove sulla storia e lo stato dei certificati emessi

- **Prima fase:**

- il certificato è ancora valido e i dati di revoca dovrebbero essere disponibili tramite i canali 'normali' (directory, verifiche online, e così via)

- **Seconda fase:**

- inizia con la scadenza del certificato
- per un certo periodo dopo la scadenza del certificato, un'infrastruttura a chiave pubblica dovrebbe essere in grado di supportare la risoluzione delle controversie di non ripudio fornendo prove sulla storia e lo stato dei certificati emessi

La terza fase: gli archivisti digitali

- I documenti che richiedono l'archiviazione a lungo termine dovrebbero essere inviati agli archivisti digitali
- Se il documento è stato firmato digitalmente, l'archivista verifica la firma al momento della ricezione e genera una dichiarazione che indica chi ha firmato il documento
- Successivamente, l'archivista è responsabile di garantire la disponibilità e l'integrità dei dati digitali archiviati
 - durante questa fase finale dell'archiviazione, non è necessario mantenere la firma digitale originariamente applicata e i pattern di bit precisi dei dati originali

- I documenti che richiedono l'archiviazione a lungo termine dovrebbero essere inviati agli archivisti digitali
- Se il documento è stato firmato digitalmente, l'archivista verifica la firma al momento della ricezione e genera una dichiarazione che indica chi ha firmato il documento
- Successivamente, l'archivista è responsabile di garantire la disponibilità e l'integrità dei dati digitali archiviati
 - durante questa fase finale dell'archiviazione, non è necessario mantenere la firma digitale originariamente applicata e i pattern di bit precisi dei dati originali

Conclusioni: le somiglianze

- Entrambe forniscono i servizi di sicurezza, di autenticazione, integrità dei dati e non ripudio
- Entrambe hanno valore legale
 - il valore legale delle firme digitali è andato via via aumentando, fino a diventare praticamente equipollente a quello delle firme autografe

- Una
indiv
sulla
da p
da u
- Le fir
firma
appl
- La fa
per s
asse
appr
prati
- i
e

- Entrambe forniscono i servizi di sicurezza, di autenticazione, integrità dei dati e non ripudio
- Entrambe hanno valore legale
 - il valore legale delle firme digitali è andato via via aumentando, fino a diventare praticamente equipollente a quello delle firme autografe

Conclusioni: le (molte) differenze (1/3)

- Una firma autografa è biologicamente legata a un individuo specifico, mentre una firma digitale si basa sulla protezione offerta dalla chiave privata della firma da parte del firmatario e sulle procedure implementate da un'autorità di certificazione
- Le firme autografe sono sotto il controllo diretto del firmatario, mentre le firme digitali devono essere applicate da un computer comandato dal firmatario
- La falsificazione delle firme autografe è stata praticata per secoli, mentre la falsificazione delle firme digitali, in assenza di compromissione della chiave privata o di appropriazione del meccanismo di firma, è praticamente impossibile
 - i meccanismi di falsificazione per le firme autografe e digitali sono totalmente diversi

- in questi casi la firma digitale è una soluzione valida può essere utilizzata in ambito forense
- Il servizio di intermediazione è molto forte di quello forense
- Le firme autografe sono più sicure delle firme digitali non possono essere falsificate
 - ...anche se possono essere falsificate
- Le firme autografe sono più sicure delle firme digitali possono essere falsificate a causa dell'obsolescenza dei meccanismi di crittografia standard crittografici

- Una firma autografa è biologicamente legata a un individuo specifico, mentre una firma digitale si basa sulla protezione offerta dalla chiave privata della firma da parte del firmatario e sulle procedure implementate da un'autorità di certificazione
- Le firme autografe sono sotto il controllo diretto del firmatario, mentre le firme digitali devono essere applicate da un computer comandato dal firmatario
- La falsificazione delle firme autografe è stata praticata per secoli, mentre la falsificazione delle firme digitali, in assenza di compromissione della chiave privata o di appropriazione del meccanismo di firma, è praticamente impossibile
 - i meccanismi di falsificazione per le firme autografe e digitali sono totalmente diversi

Conclusioni: le (molte) differenze (2/3)

- La rilevazione della falsificazione delle firme autografe dipende dalla competenza dell'esaminatore
- A causa della natura crittografica delle firme digitali, i tentativi di falsificazione sono immediatamente evidenti a qualsiasi verificatore
 - eccetto nei casi in cui una chiave privata sia stata compromessa o il meccanismo di firma sia stato sequestrato
 - in questi casi, distinguere tra una firma digitale valida e una non valida può essere impossibile, persino per un esperto di informatica forense
- Il servizio di integrità dei dati fornito dalle firme digitali è molto più forte di quello fornito dalle firme autografe
- Le firme autografe possono essere "testimoniate", mentre le firme digitali non possono esserlo
 - ...anche se possono essere notarizzate
- Le firme autografe possono essere verificate in perpetuo, mentre le firme digitali potrebbero diventare non verificabili dopo qualche anno, a causa dell'obsolescenza delle attrezzature di elaborazione dati, degli standard crittografici, della scadenza dei certificati e di altri fattori

- La rilevazione della falsificazione delle firme autografe dipende dalla competenza dell'esaminatore
- A causa della natura crittografica delle firme digitali, i tentativi di falsificazione sono immediatamente evidenti a qualsiasi verificatore
 - eccetto nei casi in cui una chiave privata sia stata compromessa o il meccanismo di firma sia stato sequestrato
 - in questi casi, distinguere tra una firma digitale valida e una non valida può essere impossibile, persino per un esperto di informatica forense
- Il servizio di integrità dei dati fornito dalle firme digitali è molto più forte di quello fornito dalle firme autografe
- Le firme autografe possono essere "testimoniate", mentre le firme digitali non possono esserlo
 - ...anche se possono essere notarizzate
- Le firme autografe possono essere verificate in perpetuo, mentre le firme digitali potrebbero diventare non verificabili dopo qualche anno, a causa dell'obsolescenza delle attrezzature di elaborazione dati, degli standard crittografici, della scadenza dei certificati e di altri fattori

Conclusioni: le (molte) differenze (3/3)

- Le firme autografe sono intrinsecamente sicure contro il ripudio (sempre in relazione alla competenza dell'esaminatore dei documenti)
- Le firme digitali richiedono la marcatura temporale di terzi per aumentare il servizio di sicurezza del non ripudio
- Le firme autografe offrono tutte un livello di sicurezza più o meno equivalente (anche se il loro livello di garanzia può essere aumentato con tecniche come l'uso di inchiostri e carte speciali, testimoni, notai, ecc.)
- Le firme digitali variano ampiamente nella forza dei servizi di sicurezza che offrono, a seconda della politica del certificato associato al firmatario
- Le firme autografe sono estremamente semplici e facili da comprendere
 - le tecniche forensi utilizzate per rilevare le frodi sono facilmente spiegabili ad avvocati, giudici e giurie
- Le firme digitali sono estremamente complesse, coinvolgendo arcane teorie sui numeri, il funzionamento dei sistemi operativi dei computer, dei protocolli di comunicazione, l'elaborazione delle catene di certificati, le politiche dei certificati e così via
- Ci sono pochissime persone al mondo che comprendono completamente ogni processo coinvolto nella generazione e nella verifica di una firma digitale
 - le possibilità di generare confusione tra avvocati, giudici e giurie sono estremamente elevate

- Le firme autografe sono intrinsecamente sicure contro il ripudio (sempre in relazione alla competenza dell'esaminatore dei documenti)
- Le firme digitali richiedono la marcatura temporale di terzi per aumentare il servizio di sicurezza del non ripudio
- Le firme autografe offrono tutte un livello di sicurezza più o meno equivalente (anche se il loro livello di garanzia può essere aumentato con tecniche come l'uso di inchiostri e carte speciali, testimoni, notai, ecc.)
- Le firme digitali variano ampiamente nella forza dei servizi di sicurezza che offrono, a seconda della politica del certificato associato al firmatario
- Le firme autografe sono estremamente semplici e facili da comprendere
 - le tecniche forensi utilizzate per rilevare le frodi sono facilmente spiegabili ad avvocati, giudici e giurie
- Le firme digitali sono estremamente complesse, coinvolgendo arcane teorie sui numeri, il funzionamento dei sistemi operativi dei computer, dei protocolli di comunicazione, l'elaborazione delle catene di certificati, le politiche dei certificati e così via
- Ci sono pochissime persone al mondo che comprendono completamente ogni processo coinvolto nella generazione e nella verifica di una firma digitale
 - le possibilità di generare confusione tra avvocati, giudici e giurie sono estremamente elevate

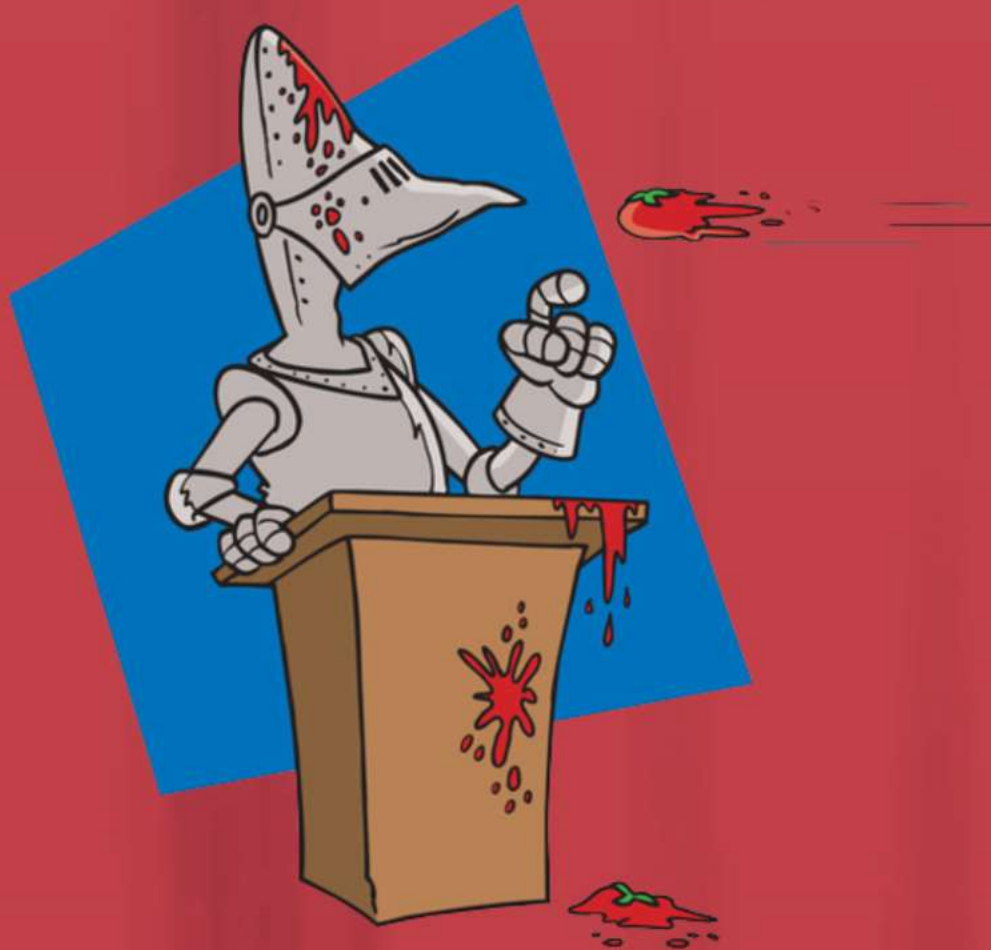
Domande?

Simon Pietro Romano

Firmato digitalmente da

SIMON PIETRO ROMANO

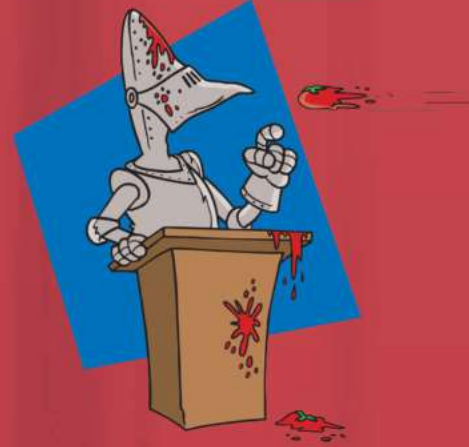
CN = ROMANO SIMON PIETRO
O = UNIVERSITÀ DEGLI STUDI DI
NAPOLI FEDERICO II
C = IT



Domande?

Simon P. Romano

Firmato digitalmente da
SIMON PIETRO ROMANO
DN: c=ROMA, o=SIMON PIETRO
ROMANO, ou=STUDIO
2 - IT



Credits: <https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html>

Firme e servizi di

Asciutta o bagnata?

Un incontro-scontro tra firma digitale e firma grafica dal punto di vista della sicurezza

