Ordine degli Ingegneri di Pisa
Nair Congressi
Via Scornigiana 1 , loc. Ospedaletto, Pisa, PI
5 Maggio 2017 – 14:00 – 19:00

IISFA European Chapter

Dal dispositivo di firma alla SPID

corso pratico di sopravvivenza per l'Ingegnere digitale

Marco A. CALAMARI
marco.calamari@ordineingegneripisa.it

IISFA – International Information Systems Forensics Association: Italian Chapter

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/

- **Marco Calamari, classe 1955, ingegnere nucleare, si cimenta a rotazione tra attivita' di consulenza tecnica informatica, editoriali e di formazione.**
- **Qualche sigla: IISFA, AIP, Opsi, HERMES, PWS.**
- **Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.**
- **Fondatore del Progetto Winston Smith e del Centro Hermes per la Trasparenza ed i diritti digitali.**
- **In concorrenza con i veri giornalisti, dal 2003 scrive su Punto Informatico ed altre riviste la rubrica settimanale "Cassandra Crossing", che dal 2005 a oggi e' quasi arrivata alla 400ma puntata … (www.cassandracrossing.org)**

L’obbiettivo di oggi

Essere cittadino digitale richiede la conoscenza di alcuni gadget digitali; il professionista digitale e’ addirittura obbligato ad usarne alcuni. Parliamo di Firma digitale, PEC, CEC-PAC, CNS, CIE, SPID.

Se conoscete tutte queste sigle, siete dei mostri e non avete motivo per restare qui, a parte che ormai avete pagato e vi volete portare a casa i crediti formativi.

Per gli altri colleghi, professionisti tecnici, ricordo che una infarinatura di tutto e’ uno strumento utilissimo per il professionista, anche la conoscenza generale di cosa sono, a cosa servono e quando e perche’ usare quest tecnologie.

Oltretutto, sempre piu’ spesso e’ obbligatorio …..

Quindi parleremo di ...

Prima parte

Storia e fondamentali della crittografia, cifrari a chiave privata e chiave pubblica, certificati digitali.

Seconda parte

Documento elettronico, firma elettronica e certificatori.
PEC - Posta Elettronica Certificata, CEC-PAC.
CNS - Carta Nazionale del Servizi.

Terza Parte

Il problema dell'identità digitale; documento di identita' elettronico, passaporto elettronico, C.I.E.
Cosa e' SPID, come si ottiene e chi la deve avere.
Moneta elettronica, tracciabilita' dei pagamenti elettronici, Bitcoin.

Quarta parte

Cosa interessa davvero al professionista?


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Prima parte

Cenni storici...

La storia della crittografia copre quattro millenni, ma puo' essere riassunta con una manciata di nomi e di fatti.

circa 450 a.e.v. - Erodoto racconta la storia di un nobile persiano che fece rasare i capelli ad uno schiavo fidato, gli fece tatuare un messaggio sul cranio, attese fino a quando i capelli furono ricresciuti e lo invio' a destinazione con l'istruzione di rasarsi nuovamente i capelli una volta arrivato. Metodo con larghezza di banda limitata, forte latenza ed oltretutto steganografia, non crittografia.

58 a.e.v. - Gaio Giulio Cesare usa e piu' tardi descrive nel *"De Bello Gallico"* il *cifrario cesariano*, o di sostituzione monoalfabetica, per corrispondere con Lucio Cornelio Balbo Maggiore mentre era impegnato nelle sue campagne militari. Primo esempio moderno di separazione tra chiave ed algoritmo, usato oggi solo alle elementari per scambiarsi biglettini che la maestra non dovrebbe riuscire a leggere..

Cenni storici...

1586 p.e.v. - nel *"Traité des Chiffres"* **Blaise de Vigenère** descrive il primo metodo storico di sostituzione polialfabetica, che e' un metodo a chiave singola, privata.

1941 p.e.v. - Konrad Zuse costruisce lo **Z3** il primo elaboratore automatico non meccanico controllato da un programma.

1976 p.e.v.: l'NSA ed il governo americano eleggono un **algoritmo crittografico a chiave privata**, proposto in maniera non troppo indipendente da IBM, a standard crittografico FIPS federale (**DES**).

Cenni storici...

circa 1970 p.e.v. - varie persone hanno una idea rivoluzionaria, la **crittografia a chiave pubblica**. che permette di evitare lo scambio delle chiavi tra i corrispondenti e rappresenta **LA** tecnologia abilitante per le applicazioni crittografiche moderne.

Scoperta da **James Ellis** impiegato dell'MI5 intorno al 1970 e chiusa in un cassetto dai suoi capi fino al 1997, prima perche' non ne avevano capito l'importanza e poi probabilmente per la vergogna o per non essere silurati.

Riscoperta in maniera sostanzialmente indipendente da **Withfield Diffie e Martin Hellmann** nel 1976 (DH), e da **Ron Rivest, Adi Shamir e Leonard Adleman** al MIT nel 1977 (RSA). Diffie vi sarebbe stato simpatico, un vero personaggio. Anche per gli standard degli anni '70 era un fricchettone eccezionale, geniale e motivato alla Stallmann o meglio alla Wau Holland.

Cenni storici...

Nel **1981** David Chaum introdusse, teorizzo' e sistematizzo' il concetto di **Mix-net**, cioe' di rete paritaria di scambio di messaggi cifrati.

Nel **1986** una famosa querelle giuridica, suscitata da una iniziativa della religione di Scientology provoca l'inizio della reazione del gruppo Cypherpunks e la nascita dei sistemi crittografici di comunicazione moderni, implementando per la prima volta in maniera crittograficamente robusta il meccanismo delle **Mixnet**.

Nel **1991** Philip R. Zimmermann, un programmatore freelance di Boulder, Colorado, pubblica in Rete **Pretty Good Privacy**, il primo **programma di crittografia forte disponibile al pubblico**. Il nome e' preso da una sitcom radiofonica dell'epoca, in cui esisteva un emporio di frutta e verdura “Pretty Good Grocery”. Il nome e' fuorviante perche la privacy garantita da PGP non e' *”piuttosto buona”* ma eccezionale.

Pgp puo’ cifrare sia mail che file generici.

Cenni storici...

Negli **anni '90 Paul Syverson** ed altri estesero l'applicazione delle **Mixnet** all'incapsulamento crittografico per il routing di pacchetti di informazioni, il cosiddetto **Onion Routing** .

Il concetto di **Blockchain** fu descritto per la prima volta nel **1991** da Stuart Haber e W. Scott Stornetta, e meglio definito nel 1996 da Ross J. Anderson e nel 1998 da Bruce Schneier and John Kelsey.

Nel 1998, **Nick Szabo** deifiniva un meccanismo per la creazione di una moneta digitale decentralizzata che battezzo' **gold**. Nel 2000 Stefan Konst pubblica una teoria generale per le blockchain ed una serie di regole pratiche per la loro implementazione

La prima blockchain fu progettata da Satoshi Nakamoto (persona che brilla per la sua inesistenza) nel **2008** e realizzata nel 2009 come parte fondamentale della moneta digitale **bitcoin**, dove e' utilizzata come pubblico registro di tutte le transazioni

Tutta la crittografia e' fatta di sole 8 pietre miliari, elaborate in 2000 anni.

Funzioni di Hash

Una **funzione di Hash** legge un file di lunghezza arbitraria e produce, usando tecniche crittografiche, una **impronta digitale** di lunghezza fissa.

As esempio, **SHA-256** produce una impronta digitale di 64 caratteri esadecimali (equivalenti a 32 byte) come questa:

73098ab8b8a3233e9166e5aca0c40261f08e55bc1585e9c6fa745e9d1cfad1fe

La proprieta' essenziale di una funzione di Hash e' che e' molto semplice calcolare l'impronta digitale di un file, ma che variando anche solo un carattere del file, l'impronta cambia in maniera non predicibile.

E' inoltre **computazionalmente impossibile** trovare un file diverso che abbia la stessa impronta digitale.

Questo significa che se il file contiene un testamento in formato PDF, non e' possibile realizzarne una versione alterata che comprenda ad esempio, un nome diverso dell'erede.

Firma Digitale

Le due chiavi di una coppia possiedono una proprieta' di simmetria totale, **quello che una cifra l'altra decifra**. Questo permette "giochetti" molto interessanti.

Calcolando l'hash di un file e criptando l'impronta con una chiave privata, si ottiene una **firma digitale** del documento originale.

Chiunque puo' prendere la chiave pubblica del firmatario, decodificare l'hash e verificare che e' proprio quello del documento.

Il firmatario quindi garantisce l'originalita' del documento, esattamente come una firma autografa.

Nella firma digitale a norma, le chiavi ed I certificati sono memorizzati nella smartcard o nel corrispondente dispositivo di firma.

In partcolare la chiave privata e' generata e memorizzata direttamente nella smartcard, e non puo' essere estratta. Una **smartcard e' un computer** con memoria permanente e difficilmente violabile).

Certificato Digitale

Un **certificato digitale** e' un tipo particolare di firma digitale.

Infatti e' la **firma digitale di una chiave pubblica**, eventualmente completata con ulteriori informazioni.

Il firmatario di una chiave pubblica viene normalmente indicato come **Autorita' di Certificazione** o **Certificatore**.

Possono esistere piu' livelli di Certificatori, in cui il certificatore di livello superiore garantisce la chiave pubblica di quello di livello inferiore

Un Certificatore garantisce che la chiave pubblica per la quale ha emesso il certificato appartiene effettivamente ad una data persona, e che le eventuali informazioni aggiuntive allegate sono corrette.

Esempi di informazioni aggiuntive sono: nome, cognome, codice fiscale, data e luogo di nascita, residenza, posta elettronica, data di emissione, data di scadenza e **per cosa il certificato puo' essere usato.**

Marca Temporale

Una **marca temporale** e' un tipo particolare di certificato digitale.

La marca temporale **certifica la data di firma di un documento**.

Il meccanismo di marcatura temporale prevede diverse fasi online:

1) il programma di firma richiede una marca temporale al certificatore

2) il certificatore "batte" una marca contenente la data e la trasmette al programma

3) il programma inserisce nella marca l'hash del documento, firma la marca, produce un documento .m7m che contiene una copia della marca e trasmette la marca al certificatore

4) il certificatore, se la marca e' stata ritornata entro un certo intervallo di tempo stabilito, la archivia come valida. La marca archiviata comprende l'hash del documento ma non il suo contenuto.

Seconda parte

Documento elettronico

Cosa e' un **Documento elettronico** (e molto altro) e' definito dal CAD – Codice dell'Amministrazione Digitale, ultimo di una lunga serie di leggi e decreti precedenti, sia italiani che UE.

http://www.agid.gov.it/cad/codice-amministrazione-digitale

Un esame di questa materia, apparentemente banale, va ben oltre gli scopi del nostro incontro.

Ruolo dei Certificatori

In ambito Firma Digitale, Marcatura Temporale, SPID ed altro, la legge italiana prevede che essi non siano emessi direttamente da un ente statale, ma da privati all'uopo certificati.

L'ente statale preposto gestisce un processo di qualificazione per le aziende che vogliono diventare **Certificatori** di uno dei suddetti servizi.

L'ente statale mantiene ed aggiorna un **albo pubblico dei certificatori** abilitati.

Firma elettronica

Anche la **firma elettronica** e' frutto di una lunga serie di leggi, decreti e recepimenti di direttive UE. In estrema sintesi, la situazione odierna prevede l'esistenza di **4 tipi diversi di firma elettronica**.

La **firma elettronica semplice** è "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*". Una semplice email con header ed indirizzo nominativo possiede gia' questo tipo di firma, perche' la legge non specifica particolari requisiti tecnici.

La **FEA - firma elettronica avanzata** non è altro che una firma elettronica con alcune caratteristiche di sicurezza addizionali. Nel decreto si legge infatti che la firma elettronica avanzata "*è apposta attraverso una procedura informatica che garantisce la connessione univoca al firmatario; è creata con mezzi sui quali quest'ultimo conserva un controllo esclusivo ed è collegata ai dati ai quali si riferisce, in modo da consentire di rilevare se gli stessi sono stati successivamente modificati*". Con una **CNS** si puo' apporre questo tipo di firma

Firma elettronica

La **firma elettronica qualificata** utilizza un **certificato digitale qualificato**, ed è realizzata mediante un dispositivo sicuro per la creazione della firma (smartcard od altro). Con una **CNS** dotata di un certificato adatto si potrebbe apporre questo tipo di firma.

La **firma digitale** (quella che ci interessa) e' definita come "*un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*".

La firma digitale prevede l'utilizzo della crittografia asimmetrica con lunghezza di chiave di 1024 bit (vecchia), o 2048 bit (conforme eIDAS).

Con una **CNS** dotata di un certificato adatto si potrebbe apporre questo tipo di firma.

Firma elettronica conforme eIDAS

Il CAD – Codice dell'Amministrazione Digitale, da una lunga serie di leggi e decreti precedenti, ed infine dal regolamento eIDAS

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/il-regolamento-ue-ndeg-9102014-eidas

https://www.agendadigitale.eu/documenti/firme-digitali-ecco-cosa-cambia-con-eidas/

In estrema sintesi il recepimento del regolamento eIDAS ha causato la coesistenza di **due diversi sottotipi di firma digitale**

1) firma digitale "normale", il cui certificato usa chiavi di 1024 bit

2) firma digitale "nuova" od "eIDAS" in cui la lunghezza della chiave di firma e' unificata a livello europeo a 2048 bit

Era da molto tempo che la firma digitale veniva criticata per l'uso di chiavi troppo corte.

La conformita' eIDAS non ha niente a che fare con i "sigilli" che talvolta si vedono nei PDF firmati (es. Processo Civile Telematico).

Firma elettronica: limiti e validita’

IISFA European Chapter

Tipologia	Definizione	Valore probatorio	Tecnologia	Esempi
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	Neutra	PIN, firma biometrica, UserID e Password
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam* tranne che per i contratti immobiliari	Neutra	Firma grafometrica su tablet, PEC verso la PA.
Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	Non neutra, certificato qualificato e dispositivo sicuro	Smart-card, token USB
Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	Non neutra, certificato qualificato chiavi asimettriche e dispositivo sicuro	Smart-card, token USB, MicroSD, Firma remota

Firma elettronica remota

Per essere apposta la **firma digitale** prevede l'utilizzo di un **dispositivo di firma**, smartcard od altro, che viene fornito dal **certificatore** e la cui conservazione da parte del **proprietario** e' soggetta a ben precise norme e responsabilita' legali, come riportato sulla documentazione fornita insieme al dispositivo (leggetela!). Non va lasciato al commercialista!

Esiste un secondo tipo di firma digitale, la **firma digitale remota**; in questo caso il "dispositivo di firma" e' custodito dal Certificatore, e il proprietario lo usa via rete da remoto, utilizzando un nome utente ed una password, che puo' essere di tipo OTP (usa e getta).

Questi tipo di firma ha avuto molto successo, attualmente esistono piu' dispositivi di firma remoti che normali. L'utilizzo "di elezione" sarebbe pero' quello di firma Business-to-Business, quindi tra entita informatiche.

Per il professionista, l'utilizzo della firma remota non e' necessario, anzi.

CNS – Carta Nazionale dei Servizi

Tra le sue varie complicazioni e duplicazioni la legge italiana prevede la **CNS**, pensata in origine per permettere l'accesso a servizi pubblici di vario tipo.

La CNS piu' nota e' la tessera sanitaria, una smartcard dotata di certificato digitale e crittografia asimmetrica, che normalmente viene usata come codice fiscale in farmacia o per accedere al **Fascicolo Sanitario Elettronico**.

Tecnicamente si tratta a tutti gli effetti di un **dispositivo di firma del tutto equivalente a quelli per la firma digitale**. Puo' infatti essere usato per apporre la firma avanzata, e se dotato di certificato aggiuntivo, anche quella qualificata.

Tecnicamente anzi, potrebbe apporre anche una firma digitale.

PEC – Posta Elettronica Certificata

La **PEC** – Posta Elettronica Certificata e' una casella postale, che viene acquistata da un fornitore iscritto all'albo dei fornitori di PEC; in pratica permette di **sostituire la normale raccomandata** a tutti gli effetti legali e nei rapporti con le PP.AA.

Come la firma digitale il suo valore legale persiste sino ad opposizione di una querela di falso.

La PEC e' spesso fornita direttamente dagli albi professionali come parte dell'iscrizione, e per il professionista deve essere censita nel **REGINDE** - Registro Generale degli Indirizzi Elettronici, gestito dal Ministero della Giustizia

IL REGINDE contiene i dati identificativi nonché l'indirizzo di posta elettronica certificata (PEC) di particolari soggetti, nel nostro caso tutti I professionisti iscritti ad un Albo obbligatorio per legge. L'iscrizione e' spesso fatta dagli Ordini, ma non sempre; quindi e' meglio verificare perche' un eventuale l'obbligo e' comunque in capo all'interessato.

Mitologie della PEC

La PEC viene conservata dal fornitore della casella: no, il fornitore e' tenuto a conservare I certificati di trasmissione per due anni, ma non e' tenuto a conservare il contenuto o gli allegati. Il fatto che essi possano rimanere nella casella postale non e' rilevante.

Non e' necessario archiviare le PEC: non in quanto tale, ma se una PEC deve rimanere a disposizione per essere opposta in un eventuale procedimento, deve essere archiviata permanentemente in modo legalmente valido (ricevute e contenuto inclusi). L'**archiviazione sostitutiva** e' particolarmente indicata, e spesso e' fornita dai fornitori di PEC coem opzione a costi contenuti.

La data della PEC ha valore legale: corretto, ma un documento allegato, se deve avere validita' legale piena, deve essere firmato digitalmente e marcato temporalmente

CEC-PAC

La **PostaCertificat@** o **CEC-PAC** (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino) **era** (per fortuna!) un servizio di comunicazione elettronica gratuito attraverso cui ogni cittadino può comunicare con gli uffici pubblici.

Defunta, con sollievo nel 2015

Era gratuita ma non poteva essere usata per altri scopi. Equivaleva ad eleggere un domicilio informatico sul quale potevano arrivare tutte le comunicazioni da una PP.AA. incluso notifiche ed atti giudiziari.

Averla al posto della PEC aveva solo un piccolo vantaggio economico. Averla insieme ad una PEC equivaleva ad avere **due domicili informatici**, un nonsenso **pericoloso**.

NOTA: Una notifica ricevuta su un domicilio informatico ma non letta o cancellata per errore **puo' costare molto cara**; un cliente sta pagando oltre 100.000 euro per aver "perso" una PEC contenente una notifica.


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Terza parte

C.I.E. ed identita' digitale

Un documento di identita' elettronico, il piu' noto dei quali, la Carta di Identita' Elettronica ha avuto ben due incarnazioni ed e' ancora poco diffusa (anche perche' costa piu' di quella cartacea), non e' altro, in buona sostanza, che una smartcard contenente un certificato ed alcune informazioni aggiuntive.

In buona sostanza, un terzo oggetto simile a CNS e Dispositivo di Firma Digitale.

Ha valore legale di documento di identita' perche emesso direttamente dallo Stato (comune o prefettura). Per il resto e' un duplicato, anzi un triplicato.

La CIE attuale, ancora in fase di avvio, contiene la fotografia, le impronte digitali dell'indice della mano sinistra e della destra ed una copia delle loro "caratteristiche". Praticamente un'"impronta digitale" di un'impronta digitale. Avete presente CSI e simili?

SPID e relativa mitologia

SPID – Sistema Pubblico di Identita' Digitale, ***e' un sistema per la creazione e gestione di credenziali di autenticazione, e per la distribuzione federata di informazioni sugli utenti***

Chiaro eh? Bene, facciamo un passo indietro, cosa NON e' la SPID

- **La SPID non e' una firma elettronica**
- **La SPID non e' un certificato digitale**
- **La SPID non e' un documento di identita'**

Ma allora cosa e' ed a cosa serve la SPID?

La SPID in pratica svolge la funzione di una CNS dematerializzata e meno sicura, che permette(ra') l'accesso a servizi sia di PP.AA. che di privati.

SPID

IISFA European Chapter

In termini pratici la SPID e' un set di credenziali di accesso, cioe' una coppia nome utente + password, eventualmente rinforzata da altri meccanismi di sicurezza, che per legge deve permettere l'accesso a tutti i siti e servizi della PP.AA.

E' gia' obbligatoria per ottenere alcuni servizi atipici tipo il Bonus Cultura (APP18) per i diciottenni del 2016, la Carta del Docente per gli insegnanti, l'accesso alla ~~famigerata~~ famosa APE ….

Quindi sostituisce tutte le password e tutti i PIN che avete per ciascun sito, quindi …la password sara' sempre la stessa! (SPID-1)

Vi viene in mente il termine "sicurezza informatica"? La SPID e' molto comoda ed usabile, ma cosa succederebbe nel caso di furto massiccio di credenziali da un fornitore? O con un uso fraudolento della vostra?
Un attaccante potrebbe impersonarvi su tutti i siti o servizi delle PP.AA. persino in quelli di cui ignorate l'esistenza.

SPID

La SPID e’ stata normata in maniera simile alla firma digitale, cioe’ viene emessa (venduta) da fornitori qualificati dallo Stato ed iscritti in un apposito albo.

Per ottenerla si parte da qui:

https://spid.gov.it/richiedi-spid

La SPID esiste in tre tipologie:

SPID-1: Username e password
SPID-2: Username, password e OTP (app oppure token)
SPID-3: Token crittografico con PIN (smartcard)

Non e’ nemmeno il caso di dire che l’unica veramente sicura e’ la SPID-3; peccato che nessuno, dopo oltre un anno, la venda ancora.

SPID - funzionamento

La SPID permette al fornitore di accesso ad un servizio di richiedere se l'autenticazione e' corretta direttamente al fornitore della particolare indentita' digitale che cerca di connettersi.

Il fornitore di accesso puo' anche chiedere alcune informazioni di cui necessita per fornire il servizio (ad esempio, codice fiscale).

Il fornitore dell'identita' digitale puo' anche possedere e distribuire in maniera selettiva altre informazioni non pubbliche sull'identita' digitale che cerca di connettersi (per esempio se e' iscritta ad un albo). Questa funzionalita' ad oggi non e' utilizzata

Per favorire la diffusione iniziale della SPID essa e' fornita gratis per 1 o 2 anni. Successivamente si paghera' annualmente come la firma digitale o la PEC.

La registrazione si puo' fare in diversi modi a seconda del fornitore, e quelli piu' facili sono a pagamento. Usare la CNS e' gratuito.

SPID – il problema “identificazione”

Il rilascio della SPID, come quello della firma digitale e della PEC, prevede l’identificazione del richiedente.

Per fortuna, o meglio purtroppo, la legge fornisce ai fornitori di SPID molti metodi per svolgerla, e molta liberta’ nel realizzarli in pratica.

Un nota videoinchiesta giornalistica descrive bene i problemi che possono derivare da alcuni di essi.

Si noti che metterla in pratica configurerebbe 3 diversi reati – non fatelo a casa, nemmeno per gioco!

Come impossessarsi dell'identita' digitale di un altro

SPID – approfondimenti ed opinioni

Perche' SPID-1 e' da evitare e SPID-2 come e' adesso non ci piace?
http://punto-informatico.it/4313602/PI/Commenti/lampi-cassandra-spid-nato-morto.aspx

I dettagli del perche SPID-2 senza token e' insicura
http://punto-informatico.it/4330925/PI/Commenti/lampi-cassandra-spid2-opinione-del-nist.aspx

Perche' la SPID-3 non esiste ancora?
http://punto-informatico.it/4373413/PI/Commenti/cassandra-crossing-difendiamo-spid3.aspx

Perche la SPID non e' un successo (per usare un eufemismo) ...
http://punto-informatico.it/4370831/PI/Commenti/cassandra-crossing-numeri-dell-egov-spid.aspx

L'opinione ufficiale sulla SPID e su tuttal'Italia Digitale la trovate su Agenda Digitale (schierato, ben fatto e ricco di informazioni)
https://www.agendadigitale.eu/

Moneta Elettronica

Una moneta elettronica (da non confondersi con un pagamento elettronico) e' un sistema che permette di assegnare, generare, scambiare e tracciare una valuta sintetica.

Una valuta sintetica e' una valuta accettata in un sistema economico che le riconosce un valore di scambio.

Bitcoin e' la piu' nota moneta elettronica, che ha la bizzarra caratteristica di essere stata progettata e realizzata da un programmatore anonimo, Satoshi Nakamoto, puo' essere scambiata anche in maniera anonima e difficilmente tracciabile.

E' realizzata come sistema peer-to-peer che permette di coniare nuova moneta, e rende conveniente contribuire tecnicamente alla gestione del sistema.

Non e' una cosa per nerd o criminali; un bitcoin oggi (3/5/2017) vale circa 1500 dollari, ed il circolante e' di 24 miliardi di dollari.

Quarta parte

Cosa interessa al professionista ?

Al professionista interessa lavorare velocemente, correttamente e senza spendere piu' dello stretto necessario

Ovviamente interessa anche lavorare in maniera perfettamente legale ed aderente alla normativa.

Ed interessa anche la certezza di poter fare a meno dei servizi cartacei e/o tradizionali.

Ne vogliamo parlare?

Cominciamo a farci due domande e discutiamone:

1) conviene fare la SPID solo per impedire che la rubi un malintenzionato?

2) Ho un solo dispositivo di firma. E' corretto?


International Information Systems
iisfa
Forensics Association
IISFA
European Chapter

Q&A time

Grazie per l'attenzione

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu ------------+