Paolo Giardini
AIP Privacy Officer
Eucip Certified Informatics Professional
Consulente per la sicurezza delle informazioni
AIP – OPSI – AIPSI - CLUSIT ISSA - FORMEZ

Riservatezza,integrità,disponibilità autenticità, non ripudio.

I principi della sicurezza applicati alla posta elettronica: il certificato digitale e la posta elettronica certificata (PEC)

Agenda:

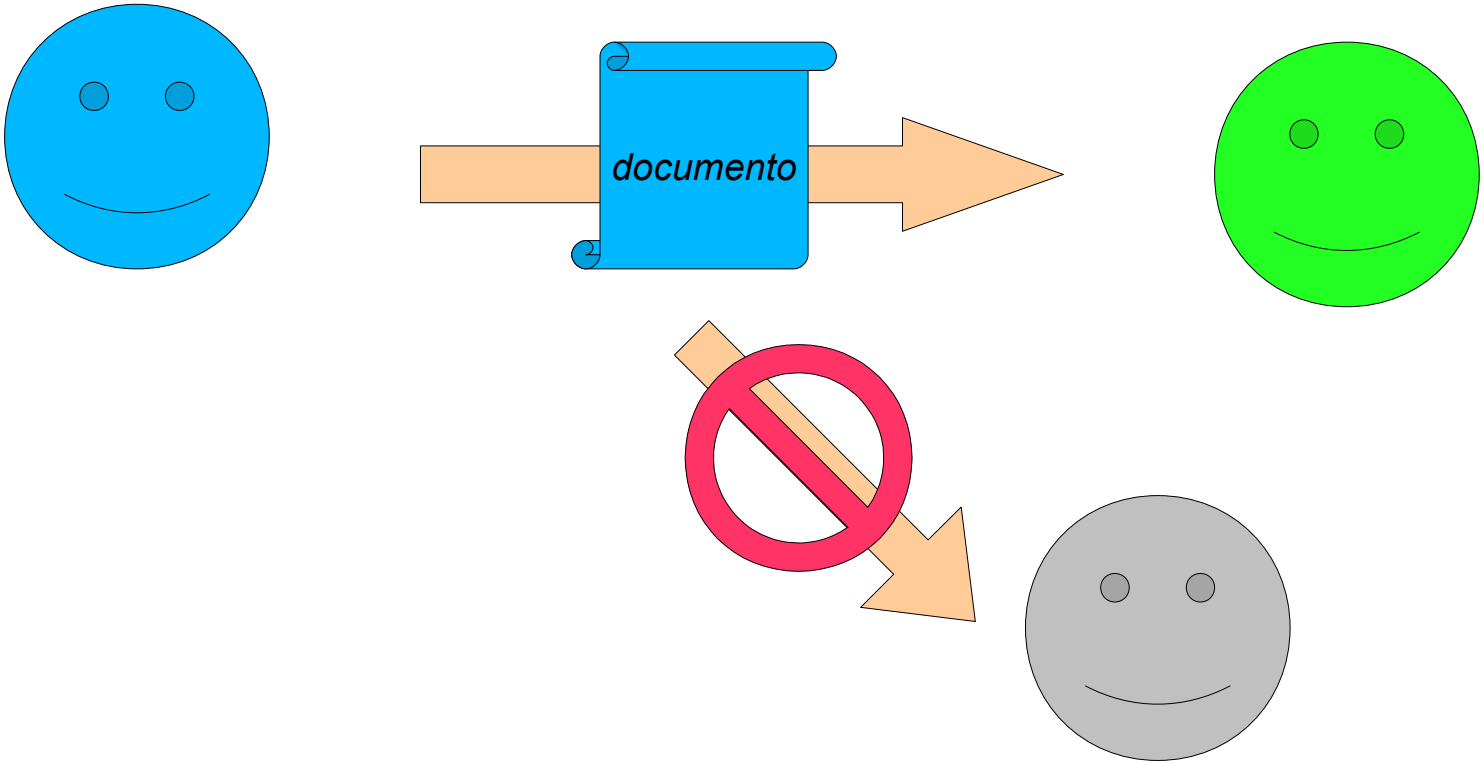
- *I principi della sicurezza informatica*
- *Cosa è il certificato elettronico*
- *Cosa è la posta certificata*
- *Come ottenere un certificato elettronico*
- *La PEC "fatta in casa" con sistemi opensource*

I principi della sicurezza informatica

- Le basi della sicurezza dell'*informazione* sono state stabilite nella BS7799, poi ISO 17799, che definisce le caratteristiche dell'informazione *sicura.*
- Queste caratteristiche sono:
  - *Riservatezza*
  - *Integrità*
  - *Disponibilità*
  - *Autenticità*
  - *Non Ripudio*

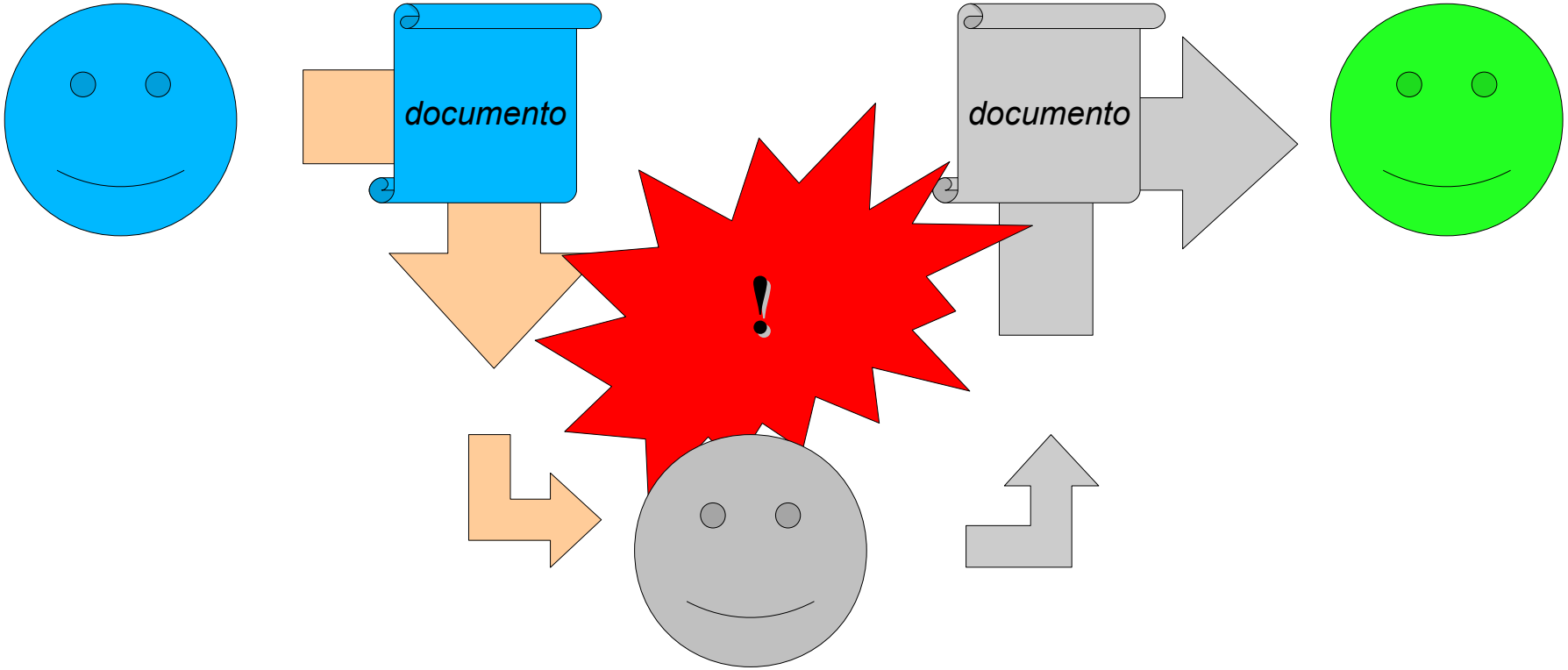
I principi della sicurezza informatica

Riservatezza: le informazioni devono essere conosciute solo da coloro che ne hanno il diritto.



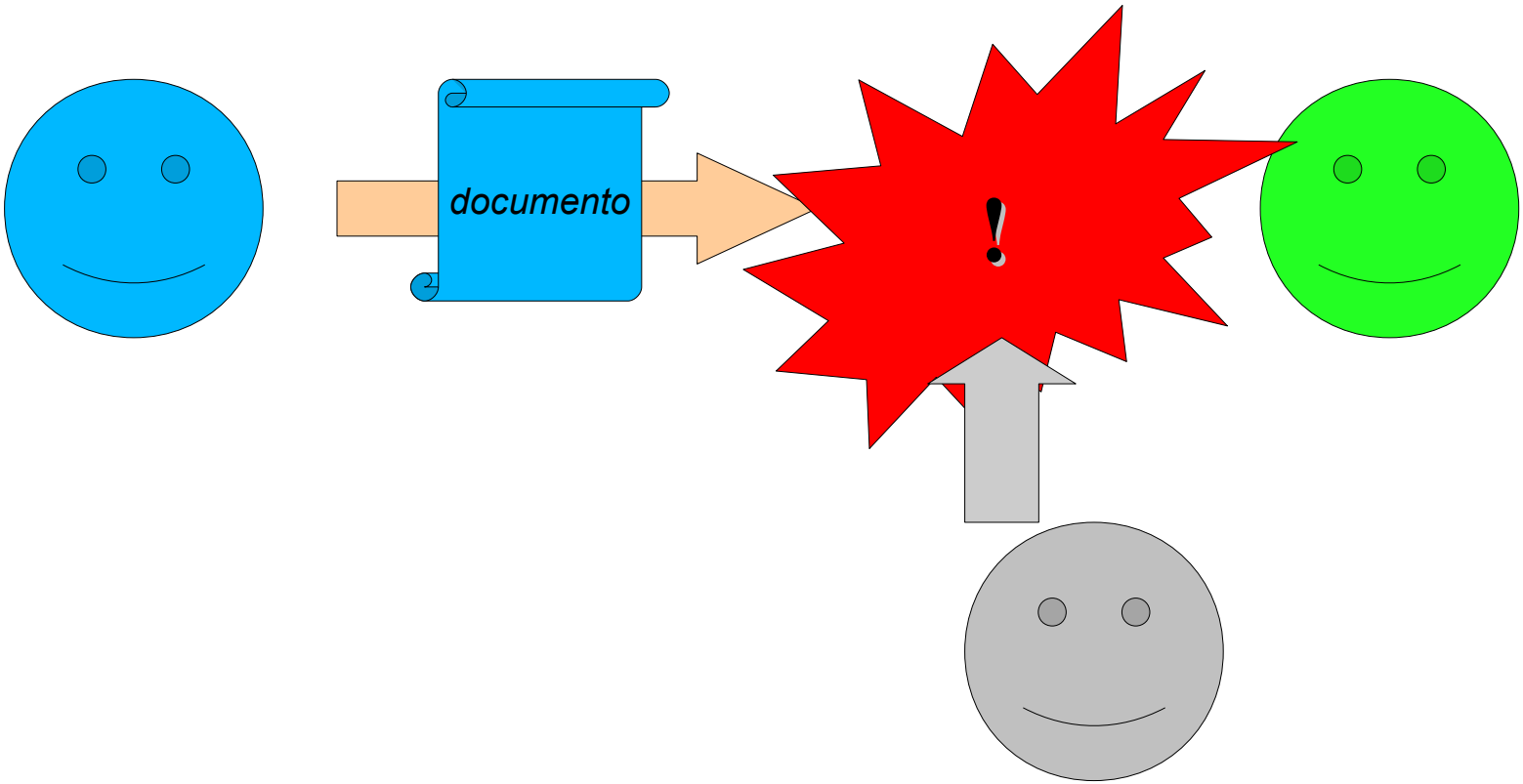
I principi della sicurezza informatica

Integrità: le informazioni devono essere protette da modifiche non autorizzate.



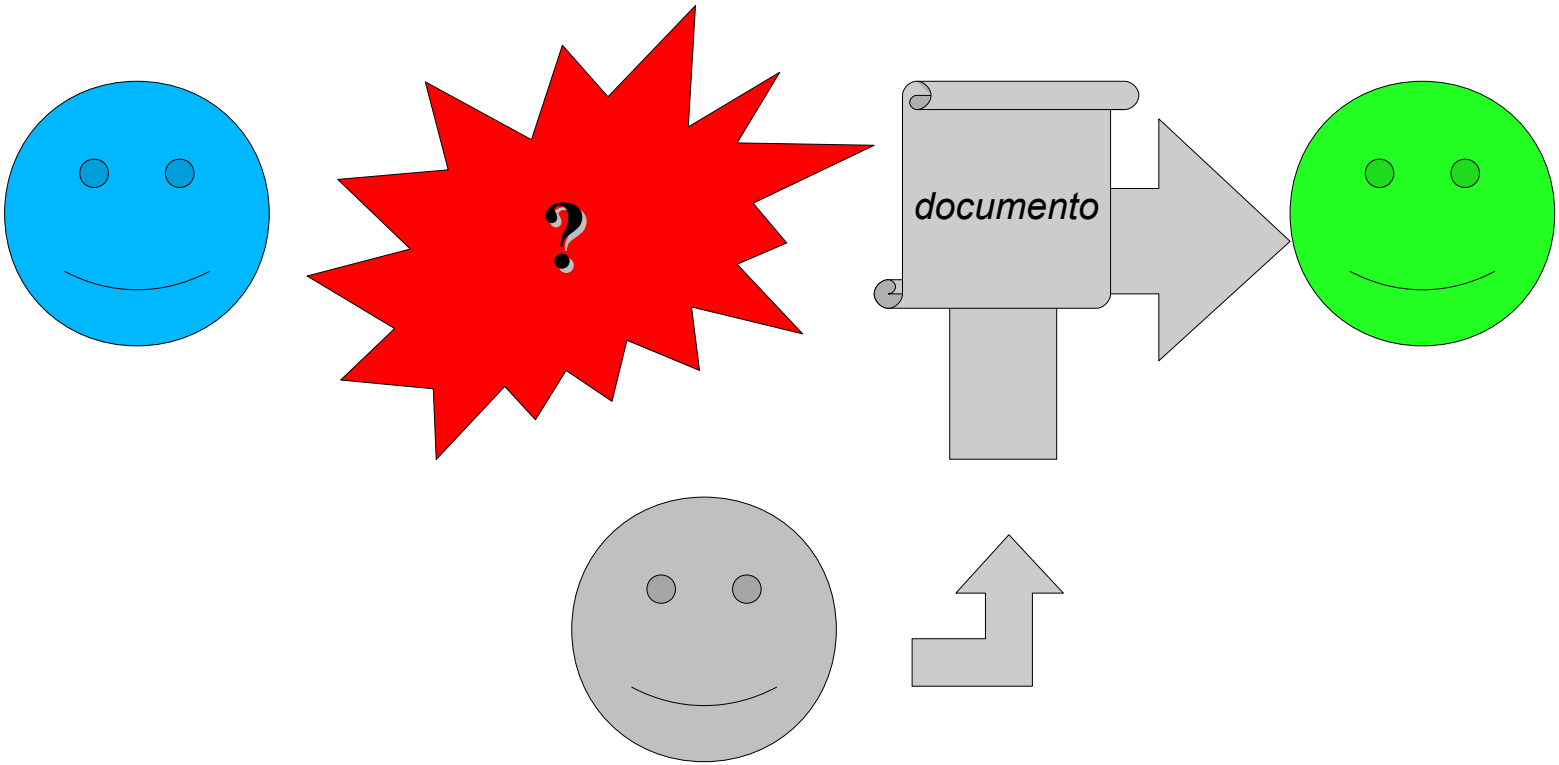
I principi della sicurezza informatica

Disponibilità : chi ha diritto di conoscere
le informazioni deve potervi accedere.



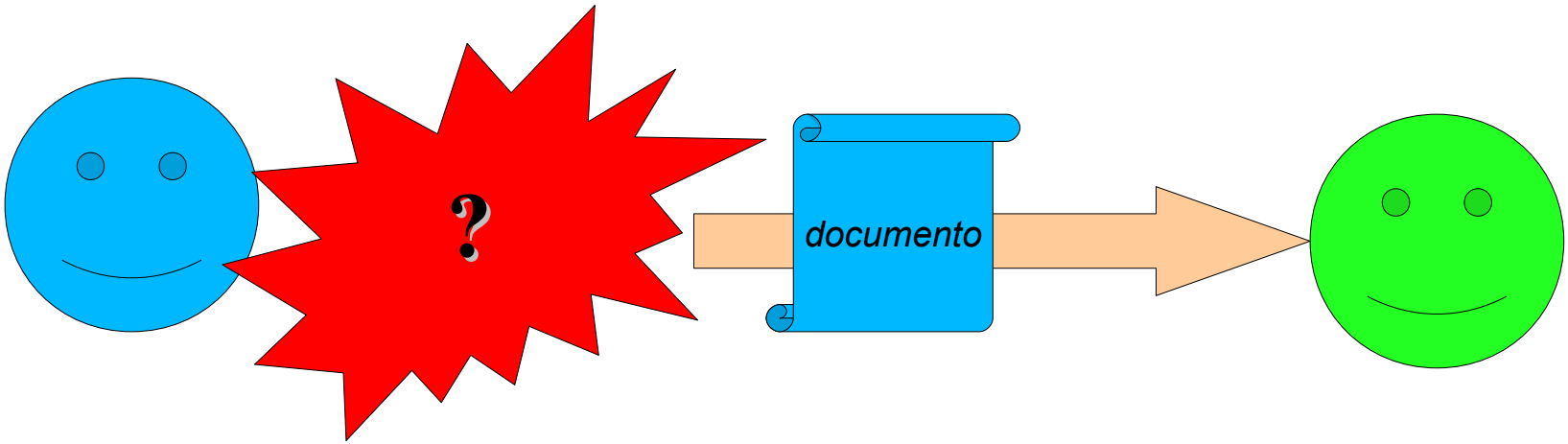
I principi della sicurezza informatica

Autenticità: il destinatario dell'informazione deve poter verificare l'identità del mittente.



I principi della sicurezza informatica

Non Ripudio: Il mittente di un messaggio non può negare di averlo inviato.



Posta elettronica e Sicurezza

Domanda:

La posta elettronica risponde ai principi della sicurezza?

Posta elettronica e Sicurezza

risposta:

Posta elettronica e Sicurezza

Riservatezza?

I messaggi sono trasmessi in chiaro.

Posta elettronica e Sicurezza

Integrità?

Il messaggio può essere modificato durante il percorso.

Posta elettronica e Sicurezza

Disponibilità?

Nessuno può assicurare che un messaggio venga effettivamente ricevuto dal destinatario.

Posta elettronica e Sicurezza

Autenticità?

La falsificazione del mittente
è alla portata di chiunque.

Posta elettronica e Sicurezza

Non ripudio?

Come puoi dimostrare che un messaggio è stato inviato da me? Io non ti ho mandato nulla!

Posta elettronica e Sicurezza

Integrità
Riservatezza
Disponibilità
Autenticità
Non Ripudio

Ma allora...

Perché continuiamo a fidarci della posta elettronica?

Posta elettronica e Sicurezza

Integrità
Riservatezza
Disponibilità
Autenticità
Non Ripudio

E soprattutto...

Come posso risolvere questi problemi?

Crittografia asimmetrica e certificato digitale

Cosa è, a cosa serve, come ottenerlo, come usarlo

Crittografia asimmetrica e certificato digitale

Problema: la posta elettronica è comoda, ma posso essere certo che quella mail è stata inviata proprio da chi sembra essere il **Mittente**?

Problema: la posta elettronica è comoda, ma posso essere certo che quella mail possa essere letta solo dal **Destinatario**?

Crittografia asimmetrica e certificato digitale

Quello che serve è un sistema di **crittografia asimmetrica** od a "chiave pubblica"

Crittografia asimmetrica e certificato digitale

la crittografia asimmetrica

• La crittografia asimmetrica è conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica.
Come si evince dal nome, ogni attore coinvolto possiede una coppia di chiavi:

- la chiave privata, personale e segreta, viene utilizzata per decodificare un documento criptato;
- la chiave pubblica, che deve essere distribuita; serve a crittare un documento destinato alla persona che possiede la relativa chiave privata.

Crittografia asimmetrica e certificato digitale

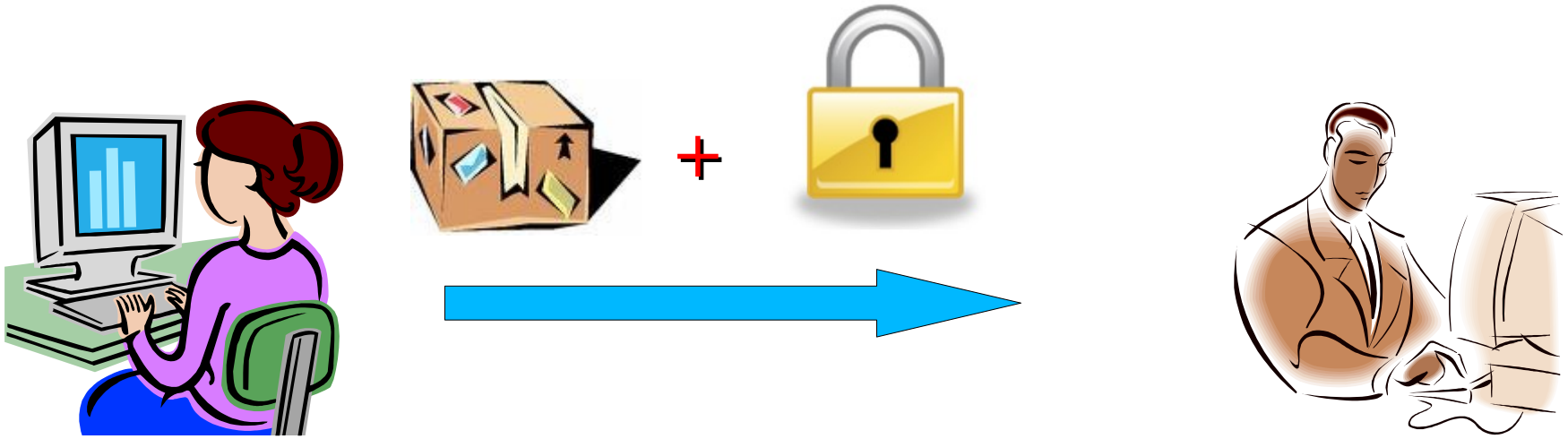
L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob.
I **lucchetti** fanno le veci delle *chiavi pubbliche* e le **chiavi** recitano la parte delle *chiavi private*:

Crittografia asimmetrica e certificato digitale

1) Alice chiede a Bob di spedirle il suo ***lucchetto***, già aperto. La ***chiave*** dello stesso verrà però gelosamente conservata da Bob.

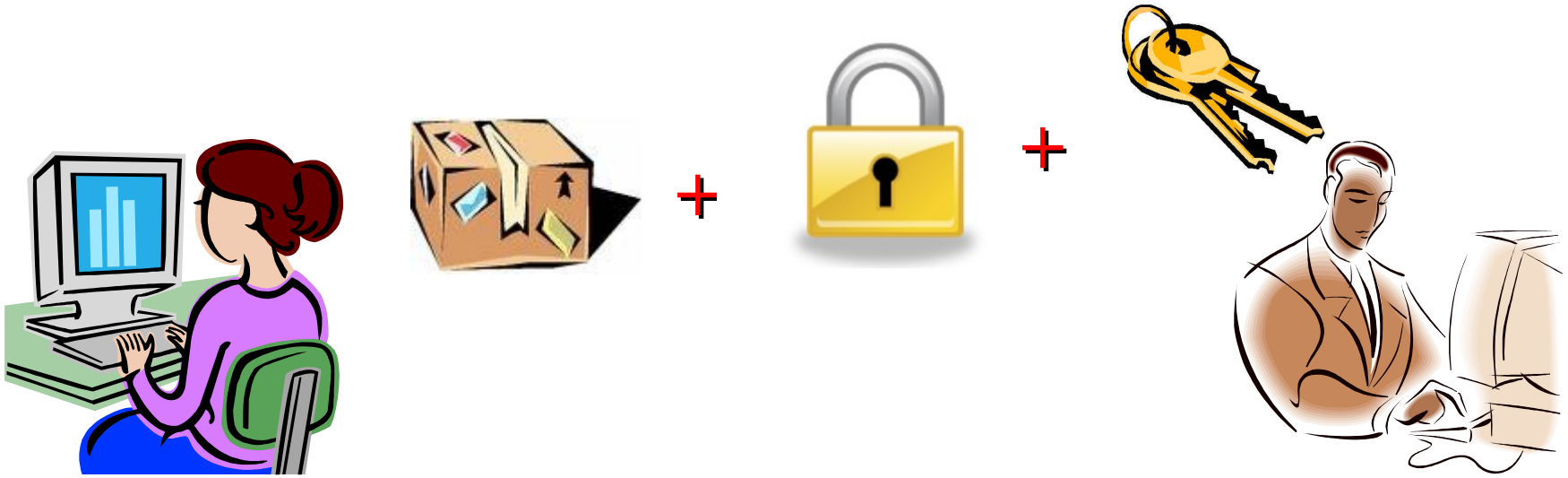
Crittografia asimmetrica e certificato digitale

2) Alice riceve il ***lucchetto*** e, con esso, chiude il pacco e lo spedisce a Bob.



Crittografia asimmetrica e certificato digitale

3) Bob riceve il pacco e può aprirlo con la ***chiave*** di cui è l'unico proprietario.



Crittografia asimmetrica e certificato digitale

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il ***lucchetto*** di Alice, che lei dovrebbe mandare a Bob e che solo lei potrebbe aprire.

Si può notare come per "*chiudere*" i pacchi ci sia bisogno del *lucchetto* del destinatario mentre per ricevere viene usata esclusivamente la propria *chiave* segreta, rendendo l'intero processo di criptazione/decriptazione asimmetrico.

Crittografia asimmetrica e certificato digitale

Ricapitoliamo:

Una **chiave pubblica** è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni **chiave pubblica** è associata ad una **chiave privata**.

La caratteristica dei crittosistemi asimmetrici è che ogni coppia di chiavi è formata in modo tale che ciò che viene cifrato con una, può essere decifrato solo con l'altra.

Le due chiavi sono, a priori, perfettamente interscambiabili, ma generalmente una delle due viene definita "pubblica" e una "privata" perché il poter distribuire una (e una sola!) delle due è il principale vantaggio dei crittosistemi asimmetrici.

Le chiavi pubbliche *possono essere scambiate anche su un canale non sicuro* (via e-mail, tramite un key server, su una pagina web o quant'altro), l'importante è sapere che una chiave pubblica non è di per sé associata a una "persona", ma esclusivamente ad una chiave privata. Per associarla ad una persona si fa generalmente uso di un **certificato digitale**

Crittografia asimmetrica e certificato digitale

Ricapitoliamo:

Una **chiave privata** è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni **chiave privata** è associata ad una **chiave pubblica**.

La caratteristica dei crittosistemi asimmetrici è che ogni coppia di chiavi è formata in modo tale che ciò che viene cifrato con una, può essere decifrato solo con l'altra.

Le due chiavi sono, a priori, perfettamente interscambiabili, ma generalmente una delle due viene definita "pubblica" e una "privata" perché il poter distribuire una (e una sola!) delle due è il principale vantaggio dei crittosistemi asimmetrici.

Le chiavi private *non devono essere scambiate né conosciute da nessuno* che non sia il legittimo proprietario. Per maggiore sicurezza la maggior parte dei programmi memorizza su disco la chiave privata solo cifrata con una password definita dall'utente.

Quando si teme che una chiave privata sia stata letta da terzi, la cosa migliore da fare è revocarla.

Crittografia asimmetrica e certificato digitale

Un **certificato digitale** è un documento elettronico che associa l'identità di una persona ad una chiave pubblica.

Viene emesso da una autorità di certificazione riconosciuta secondo standard internazionali (X.509) e viene firmato con la chiave privata dell'autorità. Gli enti che fanno da autorità devono sottostare a regole rigidissime per quanto riguarda la gestione dei dati personali, pertanto si possono considerare sicuri.

I certificati garantiscono la tutela delle informazioni personali su Internet e consentono di proteggere il sistema da programmi software non sicuri.

Un certificato è un attestato che consente di verificare l'identità di una persona o la protezione di un sito Web.

Come metto in pratica tutto questo?

Soluzione 1: con PGP creo autonomamente le mie chiavi pubblica e privata e distribuisco ai miei corrispondenti la chiave pubblica, raccogliendo le loro chiavi pubbliche (ad es. durante i *key signing party*)

Problema: in realtà la sicurezza si basa sulla fiducia, infatti ognuno certifica agli altri "di essere se stesso"

Come metto in pratica tutto questo?

Soluzione 2: mi rivolgo ad una *autorità di certificazione* (CA, Certification Authority) la quale, dopo aver accertato la mia identità, rilascia un certificato digitale assumendosi la responsabilità di garantire la mia identità.

Problema: le infrastrutture costano, pertanto le aziende che rilasciano certificati digitali si fanno pagare!

Come metto in pratica tutto questo?

Soluzione 3: ovvero come ottenere un certificato digitale gratuito.

Come metto in pratica tutto questo?

Thawte nasce nel 1995 a Cape Town in Sudafrica e nel 1996 è la prima Certification Authority a vendere certificati al pubblico.Nel 1999 raggiunge il 40% del mercato e l'anno dopo viene acquisita Verisign.

Thawte offre come servizio ai propri utenti la possibilità di creare uno o più certificati di firma digitale in modo gratuito.

Ovviamente Thawte vende anche certificati a pagamento per siti e per applicazioni e-commerce ecc.

Come metto in pratica tutto questo?

Registrandosi al sito e facendo richiesta si può avere un certificato **NON nominativo** in pochi minuti (al posto del nome e cognome reali verrà visualizzato "*Thawte Freemail Member*").

Inoltre, attraverso dei "Notai" sparsi in tutto il mondo, è possibile anche rendere la chiave **nominativa**, incontrandosi DI PERSONA e fornendo al notaio fotocopie dei propri documenti d'identità.

Ogni notaio vale da 10 a 35 punti, totalizzando 50 potete rendere la certificazione nominativa, totalizzando 100 diventate notai a vostra volta e potrete a vostra volta assegnare punti validi per ottenere un certificato digitale nominativo.

Come metto in pratica tutto questo?

Potete richiedere il vostro certificato tramite i notai presenti oggi!

Resta ancora un problema da risolvere...

Ma adesso...

Come posso essere certo che il mio messaggio abbia raggiunto il destinatario?

...Il destinatario, potrebbe dire di non aver ricevuto nulla?

La posta elettronica certificata (PEC)

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale al mittente viene fornita documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

Attraverso la PEC chi invia una email ha la certezza dell'avvenuta (o mancata) consegna del proprio messaggio e dell'eventuale documentazione allegata.

E' nata con lo scopo di offrire in formato digitale l'equivalente della raccomandata postale con ricevuta di ritorno.

La posta elettronica certificata (PEC)

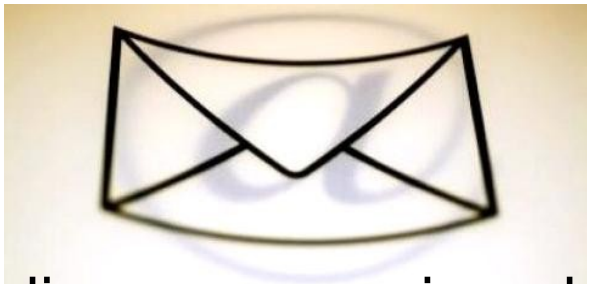
I messaggi di posta certificata possono includere testo, immagini, audio, video o qualsiasi tipo di file.

Per l'utente non esiste differenza fra l'utilizzo di una casella di posta certificata e quello di una casella di posta normale.

Possono essere utilizzati i normali programmi di posta (Outlook, Thunderbird, ecc.

Per utilizzare il servizio PEC, sia il mittente che il destinatario debbono essere in possesso di un indirizzo di posta certificata.

La posta elettronica certificata (PEC)



La certificazione dell'invio e della ricezione di un messaggio e dell'eventuale allegato avviene per mezzo di ricevute emesse dai gestori degli indirizzi certificati del mittente e del destinatario.

Quando si invia una mail certificata, il proprio gestore di posta rilascia una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegato.

Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale.

La posta elettronica certificata (PEC)

Ogni operazione che viene effettuata riceve una marca temporale che attesta gli istanti di invio e ricezione.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

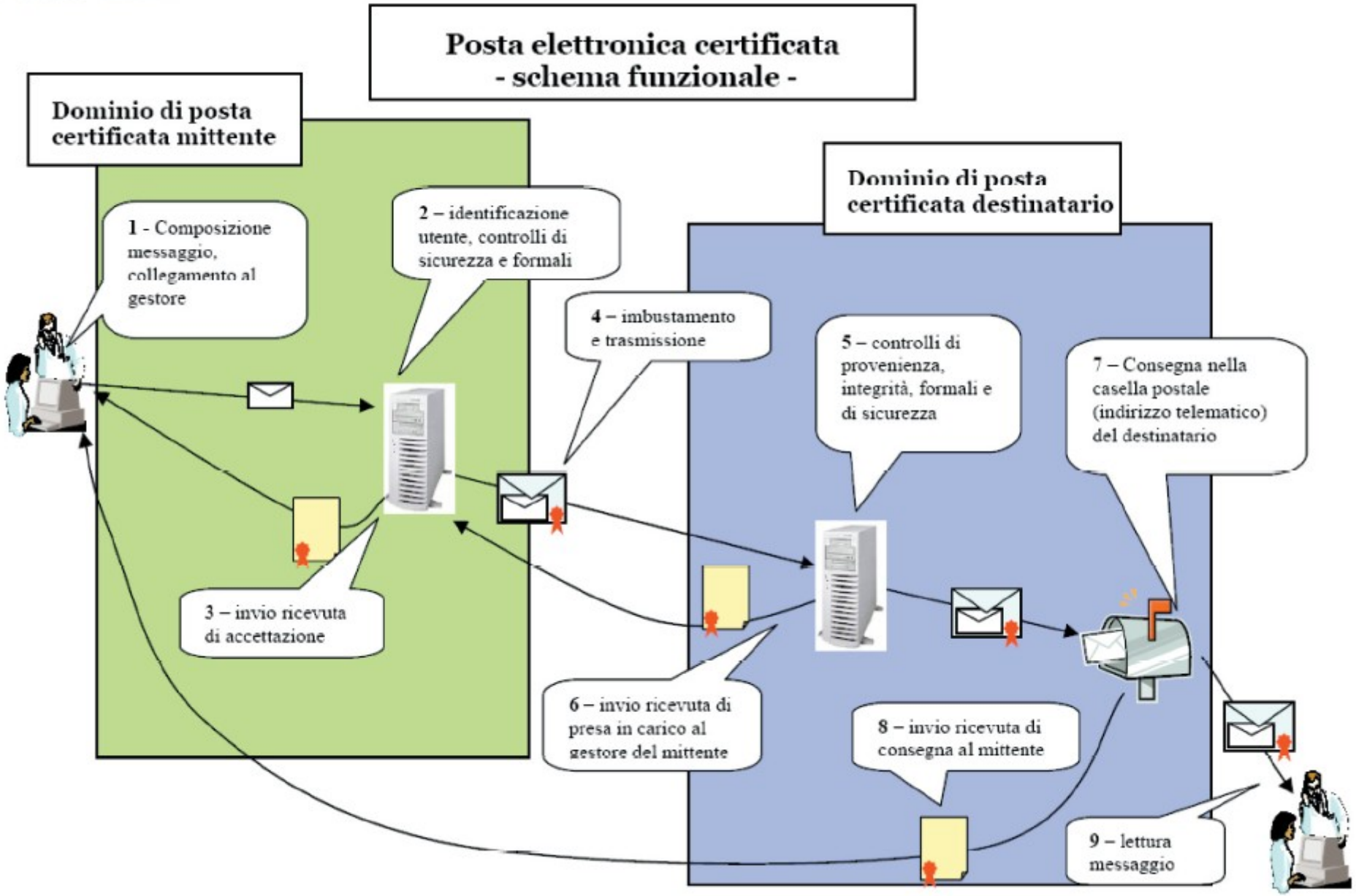
Per garantire la qualità del servizio il Centro Nazionale Informatica per la Pubblica Amministrazione (CNIPA) ha istituito un indice pubblico dei Gestori di PEC che possono essere sia Enti Pubblici che soggetti privati.

La posta elettronica certificata (PEC)

Possono divenire Gestori accreditati le aziende interessate devono presentare domanda al CNIPA ed avere determinati requisiti:

- mettere in opera un sistema di PEC rispondente ai requisiti tecnici, logistici ed organizzativi previsti dalla normativa
- predisporre uno staff ed una struttura tecnico/amministrativa per l'erogazione del servizio
- avere 1.000.000 euro di capitale sociale interamente versato
- essere in possesso di certificazione di qualità ISO 9001
- stipulare una polizza assicurativa per la copertura dei danni di esercizio (solo per aziende private)

La posta elettronica certificata (PEC)



Fonte: www.cnipa.it

La posta elettronica certificata (PEC)

Note all'uso della PEC

- Entrambi gli utenti, mittente e destinatario, debbono avere una casella PEC anche se di Gestori diversi.
- La ricevuta prodotta con la PEC in ogni caso garantisce la consegna del messaggio ma non che il destinatario lo abbia letto.
- L'uso della PEC garantisce mediante la firma con il certificato digitale del Gestore che il messaggio non venga alterato durante il percorso.
- le caselle di PEC rilasciate da pubbliche amministrazioni sono valide ai sensi della legge limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cittadini cui sono rilasciate (Art. 16 - DPR 11/2/05, n.68).
- Tale limitazione non è estesa alle caselle di PEC rilasciate da fornitori privati certificati.
- Il DPR 445/2000 obbliga le PA a provvedersi di casella PEC. Potete verificare sul sito http://indicepa.gov.it/
- L'elenco dei gestori accreditati si trova sul sito del CNIPA.

La posta elettronica certificata (PEC)

Tabella Comparativa

Caratteristiche e vantaggi della Posta Certificata a confronto con quelle dei tradizionali sistemi di invio di comunicazioni.

	Posta prioritaria	Raccomandata semplice	Raccomandata AR	Fax	Corriere espresso	Casella email semplice	Casella PEC => Casella semplice (*)	Casella PEC => Casella PEC (*)
Invio da casa/ufficio	✗	✗	✗	✓	✓	✓	✓	✓
Valore legale	✗	✓	✓	✓	✗	✗	✓	✓
Consegna immediata	✗	✗	✗	✓	✗	✓	✓	✓
Certificazione avvenuta spedizione	✗	✓	✓	✓	✓	✗	✓	✓
Avviso ricezione	✗	✗	✓	✓	✓	✗	✗	✓
Mantenimento ricevuta	✗	✓	✓	✗	✓	✗	✓ (30 mesi)	✓ (30 mesi)
Inalterabilità del contenuto	✓	✓	✓	✓	✓	✗	✓	✓
Uso da qualsiasi posto	✗	✗	✗	✗	✗	✓ (tramite webmail)	✓ (tramite webmail)	✓ (tramite webmail)
Costo unitario (per messaggio)	a partire da **€ 0,60** (120x235 mm x 50gr)	a partire da **€ 2,80** (x 20gr)	a partire da **€ 3,40** (x 20gr)	a seconda dell' operatore telefonico	a seconda del corriere	-	-	-

Fonte: http://pec.aruba.it

La posta elettronica certificata (PEC)

Normativa di riferimento

- DPR 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"
- Direttiva per l' utilizzo della posta elettronica nelle pubbliche amministrazioni, emanata il 27 novembre 2003 dal Ministro dell' Innovazione e le Tecnologie di concerto con il Ministro per la Funzione Pubblica.(G.U. 12 gennaio 2004, n. 8)
- Codice dell' amministrazione digitale: artt. 6, 45 e seguenti (Capo IV)
- DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l' utilizzo della posta elettronica certificata, a norma dell' articolo 27 della legge 16 gennaio 2003, n. 3" (G.U. 28 aprile 2005, n. 97)
- Decreto 2 novembre 2005 recante le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (G.U. 15 novembre 2005, n. 266). **Nasce ufficialmente la PEC**
- Circolare Cnipa CR/49 recante le modalità di accreditamento all'elenco pubblico dei gestori di PEC (G.U. 5 dicembre 2005, n. 283)

Openpec, la posta certificata Open Source

OpenPEC è un progetto Open Source nato per realizzare un sistema di Posta Elettronica Certificata conforme alle linee guida indicate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

Il suo sviluppo avviene in forma collaborativa sfruttando le infrastrutture del sito Sourceforge.net incoraggiando quindi a contribuire alla sua realizzazione, uso e diffusione.

OpenPEC è stato rilasciato sotto licenza Gnu GPL.

Openpec, la posta certificata Open Source

OpenPEC non è un sistema di posta elettronica sviluppato completamente da zero ma si propone come estensione dei mail server Open Source più diffusi sul mercato; in quest'ottica può essere visto come un "plug-in" di questi sistemi.

Secondo le modalità specifiche legate all'implementazione dei singoli server, OpenPEC può anche essere "aggiunto" ad un sistema già installato e funzionante: in questo modo si garantisce una naturale evoluzione dei sistemi esistenti evitando difficili e spesso costose operazioni di migrazione o di conversione. Questa è sicuramente una caratteristica molto importante per chiunque debba adottare un sistema di PEC per lo scambio dei documenti.

Openpec, la posta certificata Open Source

OpenPEC è sviluppato in Perl e progettato in modo da essere modulare per permettere facili estensioni e adattamenti. Dal punto di vista implementativo si basa su un "branch" del progetto Open Source AMaVIS, che estende i mail server più diffusi con funzionalità di antivirus nei messaggi di posta elettronica.

E' stato testato sulle distribuzioni Linux RedHat ES e CentOS 4.2 / 4.3 e si può liberamente scaricare da sourceforge o dal sito ufficiale del progetto, insieme alle istruzioni per l'installazione.

Abbiamo finito...

Domande?

Link utili

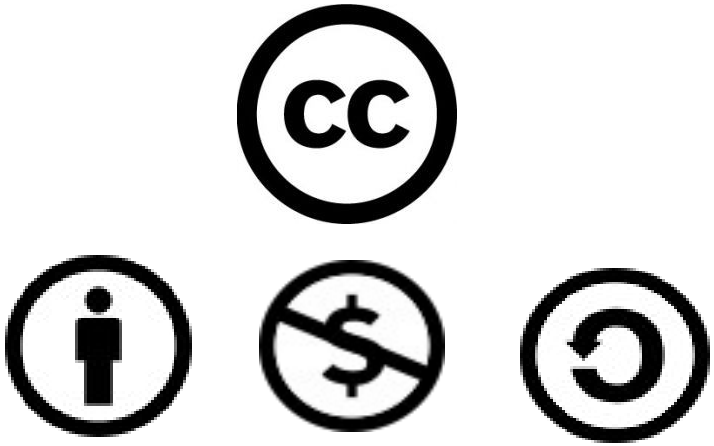
http://www.openpec.org
http://sourceforge.net/projects/openpec/
http://it.wikipedia.org/wiki/Certificato_digitale
http://www.thawte.com
http://punto-informatico.it/p.aspx?i=2017120
http://punto-informatico.it/p.aspx?i=2019484
http://punto-informatico.it/p.aspx?i=2022767
http://www.adusbef.it/consultazione.asp?Id=2976&Ricerca=cita
http://punto-informatico.it/p.aspx?i=1853010&p=1
http://www.exentrica.it/offerta-caselle-exentrica.shtml
http://cnipa.gov.it (tutta la normativa e la documentazione tecnica)
http://www.cacert.org

Grazie dell'attenzione

Paolo Giardini
pgiar@solution.it - http://www.solution.it

Licenza d'uso

Questo lavoro viene distribuito sotto
licenza Creative Commons 3.0



Sei libero di copiare, distribuire, trasmettere quest'opera e di modificarlo a condizione di: attribuirne la paternità all'autore originale, non usare quest'opera per fini commerciali, condividerla allo stesso modo.