CRITTOGRAFIA

FIRMA DIGITALE

POSTA ELETTRONICA CERTIFICATA

(Gradita è la segnalazione di eventuali errori, che, chiaramente, non sono voluti)

Sommario

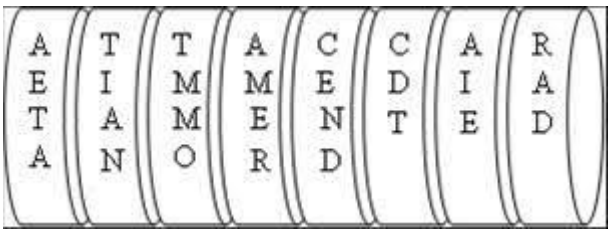
CRITTOGAFIA

La crittografia è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.

Un tale messaggio si chiama comunemente crittogramma e i metodi usati sono detti tecniche di cifratura.

La Crittografia Simmetrica

La necessità di nascondere messaggi strategici da occhi nemici è antica quanto l'uomo: ci sono tracce di cifrari antichi quanto gli Ebrei con il loro codice di atbash; gli Spartani avevano un loro particolare sistema di comunicazione dei messaggi segreti, la scitala; a Gaio Giulio Cesare si attribuisce l'uso del cosiddetto cifrario di Cesare, un sistema crittografico oggi ritenuto elementare, ma emblema della nascita di un concetto totalmente nuovo e ottimo per comprendere le idee basilari della crittografia e i primi attacchi della sua "avversaria": la crittoanalisi.

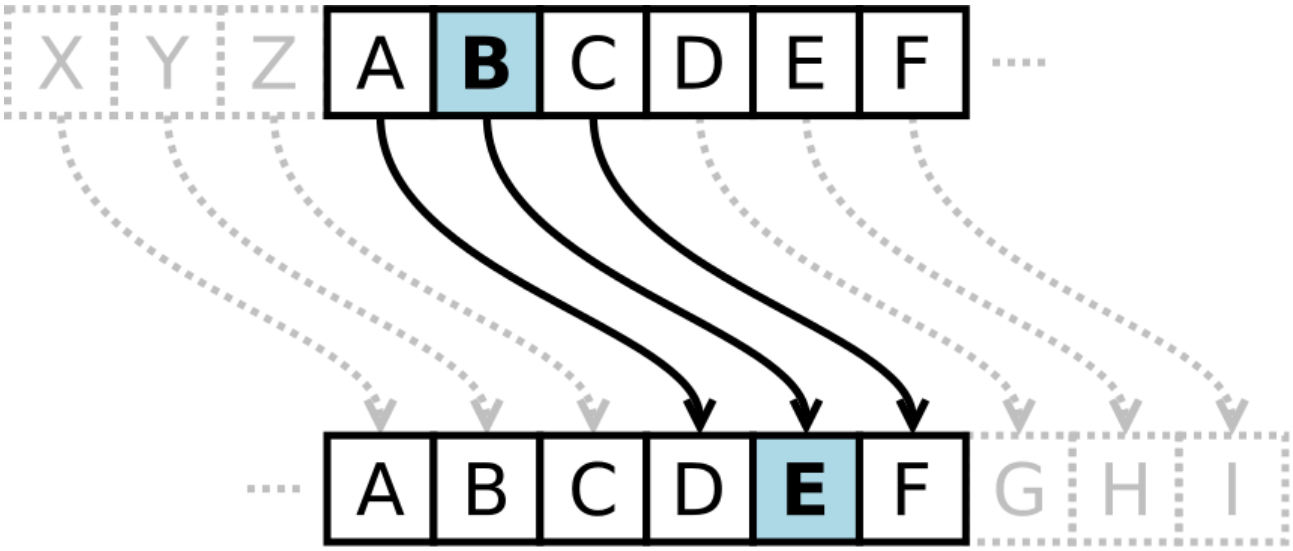


Sopra la Scitala con il messaggio in chiaro, a sx il messaggio cifrato.

A E T A T – A N T M M O A M E R C E N D C D T A _ E R A D

Cifrari a Sostituzione

In crittografia il cifrario di Cesare è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.



Il cifrario di Cesare prende il nome da Giulio Cesare, che lo utilizzava per proteggere i suoi messaggi segreti. Grazie allo storico Svetonio sappiamo che Cesare utilizzava in genere una chiave di 3 per il cifrario, come nel caso della corrispondenza militare inviata alle truppe comandate da Quinto Tullio Cicerone. Al tempo era

sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato; inoltre non esistevano metodi di crittanalisi in grado di rompere tale codice, per quanto banale.

Conosciamo anche altri che usarono questo cifrario al tempo di Cesare: Augusto, suo nipote, lo utilizzava con chiave 1, ma senza ripartire da sinistra in caso di fine dell'alfabeto. Quindi, scriveva B per A, C per B ma usava AA per Z.

Dalla scoperta dell'analisi delle frequenze da parte del matematico arabo Al-Kindi nell'XI secolo circa, tutti i cifrari di questo tipo sono divenuti molto semplici da rompere; nessuno è adatto per comunicazioni sicure allo stato tecnologico attuale, né lo è stato negli ultimi 1000 anni.

I “pizzini” di Provenzano

Un rudimentale sistema di cifratura basato sul cifrario di Cesare è stato usato anche da Bernardo Provenzano per proteggere informazioni rilevanti scritte nei suoi famosi pizzini, i piccoli foglietti di carta con i quali il boss della mafia, durante la sua latitanza, riceveva informazioni e impartiva ordini. Il sistema scelto da Provenzano era abbastanza semplice: si trattava di sostituire ad ogni lettera il numero corrispondente alla posizione nell'alfabeto sommato a 3 e di comporre così un singolo, lungo, numero. Ad esempio, i numeri "512151522 191212154" nascondono il nome di "Binnu Riina": infatti, 5 = 2 (posizione della B) più 3; 12 = 9 (posizione della I) più 3; ecc...

In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque 3), secondo il seguente schema nell'alfabeto latino con 26 caratteri:

Testo in chiaro	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Testo cifrato	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

Lo stesso si può fare con l'alfabeto italiano, che ha 21 caratteri:

Testo in chiaro	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**z**
Testo cifrato	**D**	**E**	**F**	**G**	**H**	**I**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**Z**	**A**	**B**	**C**

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga testo cifrato. Per decifrare, viceversa. Ecco un semplice esempio (coerentemente con l'uso antico di omettere gli spazi tra le parole nei papiri, nel testo questi sono omessi; questo aumenta anche la sicurezza del cifrario perché toglie un importante punto di riferimento, cioè la suddivisione in parole, a chi tentasse la decrittazione):

Testo in chiaro	attaccaregliirriducibiligalliallaorasesta
Testo crittato	DZZDFFDUHLONNUUNGAFNENONLDOONDOODRUDVHVZD

Trasposizione

In crittografia un cifrario a trasposizione è un metodo di cifratura in cui le posizioni occupate dalle unità di testo in chiaro (che in genere sono lettere o gruppi di esse) sono cambiate secondo un determinato schema, così che il testo cifrato costituisca una permutazione del testo in chiaro.

Trasposizione Colonnare

Nella trasposizione colonnare il messaggio è scritto lungo le righe di una griglia di dimensioni prefissate e poi letto lungo le colonne, secondo un ordine particolare delle stesse. Sia la lunghezza delle righe che la permutazione delle colonne sono definite da una parola chiave. Ad esempio, la parola VETRINA è lunga 7 lettere, così le righe saranno anch'esse di lunghezza 7, e la permutazione è definita dall'ordine alfabetico delle lettere della parola chiave. In questo caso l'ordine sarebbe "7-2-6-5-3-4-1" perché l'ordine alfabetico delle lettere di VETRINA è A-E-I-N-R-T-V, e le loro posizioni sono quindi A=1, E=2, I=3, N=4, R=5, T=6 e V=7, per cui V-E-T-R-I-N-A corrisponde proprio a 7-2-6-5-3-4-1.

Nei cifrari a trasposizione colonnare regolari le posizioni vuote alla fine dell'ultima riga vengono riempite con caratteri casuali, mentre in quelli irregolari sono lasciati bianchi. Alla fine, il messaggio è letto sulle colonne secondo l'ordine specificato dalla parola chiave. Ad esempio, supponendo di usare la parola chiave VETRINA e il messaggio PIANTARE IL CAMPO DIETRO LA COLLINA, in una trasposizione colonnare regolare avremmo una griglia così composta:

```
7 2 6 5 3 4 1
P I A N T A R
E I L C A M P
O D I E T R O
L A C O L L I
N A D V Y I Q
```

Con le ultime cinque lettere insignificanti (DVYIQ). Il testo cifrato è così letto:

```
RPOIQ IIDAA TATLY AMRLI NCEOV ALICD PEOLN
```

Nel caso di una trasposizione colonnare irregolare, invece, la griglia sarebbe così creata:

```
7 2 6 5 3 4 1
P I A N T A R
E I L C A M P
O D I E T R O
L A C O L L I
N A
```

E il messaggio cifrato sarebbe il seguente:

```
RPOII IDAAT ATLAM RLNCE OALIC PEOLN
```

Per decifrarlo, il destinatario risale alla lunghezza delle colonne dividendo la lunghezza del messaggio per quella della parola chiave. Poi può scrivere il messaggio riorganizzandolo in colonne e poi riordinare le colonne in base alla parola chiave.

I cifrari a trasposizione colonnare sono oggi usati solo come giochi enigmistici o per utilizzi dilettantistici: alcuni gruppi di scout, ad esempio, utilizzano un cifrario a trasposizione colonnare regolare per rendere illeggibili semplici comunicazioni.

Crittografia Asimmetrica

La crittografia asimmetrica, conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica, è un tipo di crittografia dove, come si evince dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

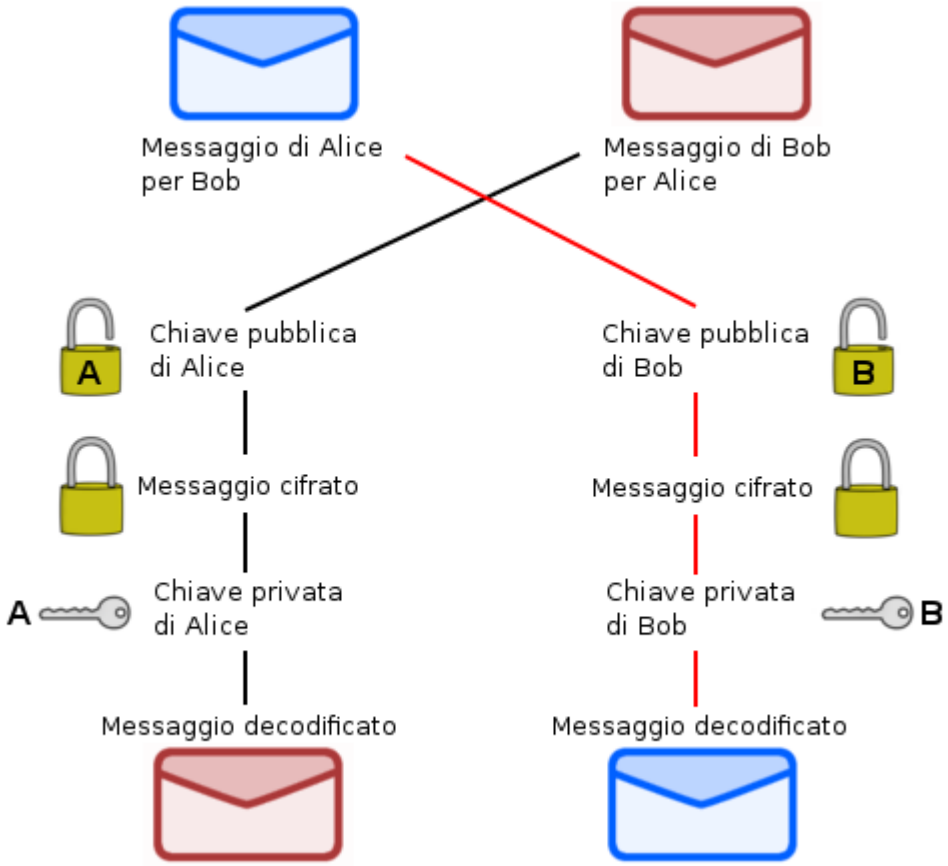
- La chiave pubblica, che deve essere distribuita
- La chiave privata, appunto personale e segreta

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

Ci sono due funzioni che possono essere realizzate: usare la chiave pubblica per autenticare un messaggio inviato dal titolare con la chiave privata abbinata; o cifrare messaggi con la chiave pubblica per garantire che solo il titolare della chiave privata possa decifrarlo.

In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.

La crittografia a chiave pubblica trova applicazione in vari campi, tra gli altri: nella disciplina di sicurezza informatica e nella sicurezza delle informazioni. La sicurezza delle informazioni si occupa di tutti gli aspetti per la protezione delle risorse informative elettroniche contro le minacce sulla sicurezza. La crittografia a chiave pubblica viene utilizzata come metodo di assicurare la riservatezza, l'autenticazione e il non ripudio delle comunicazioni e per la memorizzazione dei dati.



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

1. Alice chiede a Bob di spedirle il lucchetto già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob
2. Alice riceve il lucchetto di Bob e, con esso, chiude il pacco e lo spedisce a Bob
3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice (che lei dovrebbe aver preventivamente dato a Bob) che solo lei potrebbe aprire.

Si può notare come per mettere in sicurezza il contenuto dei pacchi ci sia bisogno del lucchetto del destinatario, mentre per aprirli viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di cifratura/decifratura asimmetrico (una chiave per cifrare ed una differente per decifrare). Chiunque intercettasse il lucchetto (aperto) o il messaggio chiuso con il lucchetto non potrebbe leggerne il contenuto poiché non ha la chiave. Uno dei vantaggi della crittografia asimmetrica sta nel fatto che le chiavi pubbliche possono essere scambiate anche utilizzando un mezzo insicuro, come Internet.

Nella crittografia simmetrica invece, che basa la sicurezza del sistema sulla segretezza della chiave di codifica/decodifica utilizzata, si rende necessario utilizzare un canale sicuro per la trasmissione della chiave, poiché l'intercettazione della stessa, da parte di terzi, vanificherebbe la sicurezza del sistema stesso.

Due degli usi più conosciuti della crittografia asimmetrica sono:

- Crittografia a chiave pubblica, nel quale i messaggi sono crittografati con la chiave pubblica del destinatario. Il messaggio non può essere decriptato da chi non possiede la chiave privata corrispondente, che viene così presupposto di essere il proprietario di quella chiave e la persona associata con la chiave pubblica. Questo è utilizzato nel tentativo di garantire la riservatezza.

- Firma digitale, in cui un messaggio viene firmato con la chiave privata del mittente e può essere verificato da chiunque abbia accesso alla chiave pubblica del mittente. Questa verifica dimostra che il mittente ha avuto accesso alla chiave privata ed è pertanto probabile che sia la persona associata alla chiave pubblica. Questo assicura anche che il messaggio non è stato manomesso.

Nella tradizionale crittografia simmetrica, viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Delle due informazioni (la chiave e l'algoritmo) necessarie a chi deve inviare il messaggio, la chiave è quindi identica a quella necessaria a chi deve riceverla, mentre l'algoritmo è facilmente reversibile in quello di decifrazione. Per concordare una chiave con il proprio interlocutore, c'è bisogno di mettersi preventivamente in contatto con lui incontrandolo di persona, telefonandogli, scrivendogli una lettera, mandandogli un messaggio o in qualsiasi altro modo. In qualunque caso, esiste il pericolo che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo.

La crittografia a chiave pubblica permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave, anche se queste non si sono mai incontrate precedentemente.

PEC

La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno, come stabilito dalla normativa (DPR 11 Febbraio 2005 n.68). Rispetto alla Posta Elettronica ordinaria, il servizio PEC presenta delle caratteristiche aggiuntive che forniscono agli utenti la certezza a valore legale dell'invio e della consegna (o mancata consegna) delle e-mail al destinatario:

- Ha lo stesso valore legale della raccomandata con ricevuta di ritorno con attestazione dell'orario esatto di spedizione.
- Grazie ai protocolli di sicurezza utilizzati, è in grado di garantire la certezza del contenuto non rendendo possibile nessun tipo di modifica nè al messaggio nè agli eventuali allegati.

La Posta Elettronica Certificata garantisce, in caso di contenzioso, l'opponibilità a terzi del messaggio. Il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la ricevuta di avvenuta consegna.
I gestori certificano quindi con le proprie "ricevute" che il messaggio:

È stato spedito ------> è stato consegnato (o non è stato consegnato) ------> non è stato alterato

In ogni avviso inviato dai gestori è inserito anche un riferimento temporale che certifica data ed ora di ognuna delle operazioni descritte. I gestori inviano avvisi anche in caso di errore in una qualsiasi delle fasi del processo (accettazione, invio, consegna) in modo che non possano esserci dubbi sullo stato della spedizione di un messaggio. Nel caso in cui il mittente dovesse smarrire le ricevute, la traccia informatica delle operazioni svolte, conservata dal gestore per 30 mesi, consentirà la riproduzione delle ricevute stesse con lo stesso valore giuridico.

A chi si rivolge

La Posta Elettronica Certificata, oltre ad essere obbligatoria per tutte le imprese (professionisti, società, ditte individuali e Pubbliche Amministrazioni), si rivolge a tutti coloro che hanno l'esigenza di inviare e ricevere comunicazioni formali (e documenti allegati) con valore legale, di attestarne data/ora di invio e di consegna e di farlo con la massima semplicità, dal proprio computer o smartphone.

Privati, professionisti, aziende e enti pubblici usano in maniera diffusa la PEC al posto di fax e raccomandate per risparmiare tempo, ma anche denaro: la Casella PEC ha infatti un costo fisso, indipendente dalla quantità/dimensione dei messaggi spediti e/o ricevuti.

Esempi di utilizzo

AZIENDE

- Sostituzione della posta cartacea per semplificare i rapporti con clienti e fornitori
- Integrazione delle trasmissioni certificate in software gestionali, paghe e stipendi, protocolli, gestori documentali, workflow
- Invio e ricezione di ordini, contratti e fatture
- Gestione di gare di appalto
- Invio di documenti alla Pubblica Amministrazione

ENTI PUBBLICI

- Invio di comunicazioni ufficiali verso altri Enti o cittadini
- Inoltro di circolari e direttive

- Convocazione di Consigli, Assemblee, Giunte
- Integrazione delle trasmissioni certificate in software gestionali, paghe e stipendi, protocolli, gestori documentali, workflow
- Invio e ricezione di ordini, contratti e fatture
- Gestione di gare di appalto

PRIVATI

- Invio e ricezione comunicazioni per riunioni di condominio
- Invio di documenti alla Pubblica Amministrazione
- Disdette polizze assicurative e contratti di fornitura servizi
- Invio e ricezione comunicazioni inerenti il rapporto di lavoro (es: busta paga)
- Comunicazioni con banche e istituti finanziari
- Prenotazione visite mediche e ritiro referti

Vantaggi

a Posta Elettronica Certificata è obbligatoria per tutte le aziende individuali e società che devono quindi associare presso il registro delle imprese un indirizzo PEC valido e attivo. Oltre a questo però, la PEC presenta diversi vantaggi.

SEMPLICITÀ

Il servizio PEC si usa come la posta elettronica tradizionale e può quindi essere gestita sia tramite un programma client (Es. Outlook Express) che via web attraverso la Webmail. Quest'ultima è anche accessibile da Smartphone e Tablet attraverso l'App dedicata.

SICUREZZA

A differenza della mail tradizionale il servizio PEC utilizza i protocolli sicuri POP3s, IMAPs, SMTPs e HTTPs. Tutte le comunicazioni sono inoltre protette perché crittografate e firmate digitalmente garantendo l'integrità e l'inalterabilità dei messaggi inviati e ricevuti e dei relativi allegati.

VALIDITÀ LEGALE

La PEC ha esattamente lo stesso valore legale di una raccomandata AR e le ricevute possono essere utilizzate come prova dell'invio, della ricezione e del contenuto del messaggio inviato, anche in caso di contenzioso. Inoltre le principali informazioni riguardanti la trasmissione e la consegna del messaggio vengono conservate dal gestore per 30 mesi.

PROTEZIONE DA VIRUS E SPAM

Il servizio PEC è pressoché immune dalla fastidiosa posta spazzatura in quanto non è possibile ricevere messaggi non certificati.

COMODITÀ

La casella PEC può essere utilizzata in qualsiasi momento da qualsiasi dispositivo (pc, tablet o smartphone) collegato ad internet.

CONVENIENZA

Rispetto a strumenti quali posta raccomandata o fax, il servizio di posta elettronica certificata ha dei costi inferiori e permette un risparmio notevole di tempo. Inoltre il costo di una casella PEC è annuale e fisso e dunque non cambia in base all'utilizzo.

Confronto delle caratteristiche del servizio PEC rispetto agli altri metodi di spedizione di documenti.

	Posta Prioritaria	Raccomand Semplice	Raccomand Ar	Fax	Corriere Espresso	Casella Email Semplice	Casella Pec**
Invio da casa/ufficio	x	x	x	s	s	s	s
Valore legale	x	si	si	s	x	x	s
Consegna immediata	x	x	x	s	x	s	s
Certificazione di avvenuta spedizione	x	si	si	s	s	x	s
Ricevuta avvenuta consegna	x	x	si	s	s	x	s
Conservazione ricevuta	x	A carico del cliente	A carico del cliente	x	A carico del cliente	x	30 mesi a carico di Aruba
Inalterabilità del contenuto	si	si	si	s	s	x	s
Utilizzabile da qualsiasi luogo	x	x	x	x	x	(tramite webmail)	(tramite webmail)
Costo unitario (per messaggio)	da **0,60€**	da **3,30€**	da **3,90€**	Secondo l'operat. telefonico	Secondo il corriere	-	-
Costo fisso	-	-	-	-	-	-	Da **5€** + IVA/anno
Protezione Spam	-	-	-	-	-	x	s

Come funziona

FRA DUE CASELLE PEC

Proprio come una raccomandata, un messaggio di Posta Elettronica Certificata, al momento della spedizione, viene racchiuso in una busta di trasporto (virtuale), sul quale viene applicata una firma elettronica (come il timbro dell'ufficio postale). Questa serve a garantirne la provenienza e l'inalterabilità, cioè che il messaggio non venga modificato da nessuno durante il suo viaggio. Prima di consegnare l'email PEC, viene effettuato un controllo sulla validità della firma apposta e in caso di esito positivo il messaggio viene consegnato al destinatario. A questo punto il mittente riceve una Ricevuta di Avvenuta consegna (come la ricevuta di ritorno) ed ha dunque la certezza che il suo messaggio è giunto a destinazione.

DA UNA CASELLA PEC A UNA CASELLA DI POSTA ORDINARIA

È possibile inviare un messaggio di Posta Elettronica Certificata ad una casella di posta elettronica ordinaria, ma in questo caso il mittente non riceverà la ricevuta di avvenuta consegna. Il destinatario può rispondere alla mail se la casella PEC del mittente è configurata in modo tale da ricevere messaggi di posta ordinaria. In caso contrario riceverà una notifica di errore (MAILER-DAEMON).

DA UNA CASELLA DI POSTA ORDINARIA AD UNA CASELLA PEC

Se una casella di posta ordinaria, quindi NON certificata, invia un messaggio ad una casella di Posta Certificata gestita da Aruba PEC, il server di posta respingerà tale messaggio senza inviare alcuna notifica al destinatario. Il mittente invece riceverà in risposta un messaggio di errore per mancata consegna (MAILER-DAEMON).

Per poter ricevere messaggi di posta elettronica sulla casella PEC basterà tuttavia modificare tale pre-impostazione attraverso il Pannello di Gestione della casella.

FIRMA DIGITALE

Cos'è la Firma Digitale

La Firma Digitale è l'equivalente informatico di una tradizionale firma autografa apposta su carta e ha le seguenti caratteristiche:

Autenticità

La firma digitale garantisce l'identità del sottoscrittore

Integrità

La firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione

Validità legale

La firma digitale attribuisce piena validità legale al documento firmato

L'utilizzo della Firma Digitale permette quindi di snellire significativamente i rapporti tra Pubbliche Amministrazioni, i cittadini o le imprese, riducendo drasticamente la gestione in forma cartacea dei documenti. È possibile firmare digitalmente qualsiasi documento elettronico, come ad esempio fatture, comunicazioni alle PA, visure camerali, contratti, etc.

La Firma Digitale è costituita da un dispositivo (smart card o chiavetta USB) che contiene un certificato digitale di sottoscrizione, tramite il quale il titolare può firmare digitalmente i propri documenti.

Cos'è la Firma Digitale Remota

I Kit di Firma Remota sono composti da un certificato di Firma digitale depositato su un server sicuro di Aruba e un dispositivo OTP (One Time Password) che permette al titolare di autenticarsi con le proprie credenziali e di firmare i propri file da qualsiasi postazione connessa a internet.

La Firma Digitale Remota si avvale dell'autenticazione OTP (One Time Password) e presenta diversi vantaggi, tra i quali la possibilità di:

- Apporre Firme Digitali senza dover installare alcun tipo di Hardware dedicato
- Sottoscrivere digitalmente documenti informatici via Web in condizioni di massima sicurezza
- Disporre in ogni momento e in ogni luogo della propria Firma Digitale su diversi ambienti (Windows, Mac) semplicemente installando il Software Aruba Sign
- Eliminare le problematiche legate all'incompatibilità di particolari dispositivi (Lettori, Smart Card e Token USB) con determinate piattaforme Hardware o Software

Vantaggi

PRATICITÀ

La firma digitale viene utilizzata attraverso dispositivi semplici da utilizzare ed installare che possono essere utilizzati ovunque.

RAPIDITÀ

L'apposizione di una firma digitale rispetto ad una firma autografa rende più veloci i tempi di trasmissione dei documenti in quanto non è necessario stampare e spedire i documenti firmati. Questo si traduce anche in un risparmio di tipo economico.

SICUREZZA

Con l'apposizione della firma digitale viene garantita l'inalterabilità del documento.

COMODITÀ

La firma digitale è composta da dispositivi semplici da utilizzare ed installare che permettono di inviare elettronicamente i documenti firmati comodamente dal proprio computer.

La firma digitale è dunque un servizio prezioso per Privati, Liberi Professionisti, Aziende e Pubblica Amministrazione che possono scambiare atti, documenti, contratti, ecc. senza dover fare lunghe code agli sportelli

Come funziona

Per poter firmare digitalmente un file è necessario essere titolare del certificato digitale di sottoscrizione contenuto nel kit di firma.

Il Kit di Firma Digitale è composto da:

- Smart Card con Certificato
- Lettore di Smart Card
- Software di Firma e Verifica

Una volta attivato il Kit sul computer, attraverso il Software di Firma è possibile selezionare il documento elettronico da sottoporre a Firma Digitale e, previa attivazione di un account, alla Marcatura Temporale. Al momento della Firma del documento, il software chiederà l'inserimento del PIN e procederà con la creazione del file firmato digitalmente.

È possibile firmare digitalmente qualsiasi tipo di file elettronico, anche file in formato pdf.

In fase di verifica della Firma da parte del destinatario del documento firmato verrà accertato che:

- Il documento non sia stato modificato dopo la Firma
- Il Certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori
- Il Certificato del sottoscrittore non sia scaduto
- Il Certificato del sottoscrittore non sia stato sospeso o revocato

Se tutte le verifiche daranno esito positivo, il documento sottoscritto digitalmente potrà essere considerato valido a tutti gli effetti di legge.

Come funziona la firma digitale remota

Grazie alla Firma Remota, per la sottoscrizione dei documenti digitali non è necessaria la Smart Card ma è sufficiente utilizzare un computer collegato ad Internet, una OTP (One Time Password), generata attraverso un apposito dispositivo (Token o app per Smartphone) ed il Software di Firma Aruba Sign, attraverso il quale è possibile selezionare il documento elettronico da sottoporre a Firma Remota.

Le OTP (password dinamiche) sono considerate il sistema più sicuro per l'accesso ai sistemi informatici e vengono generate e distrutte direttamente all'interno dei dispositivi OTP. Trattandosi di password momentanee (scadono alcuni secondi dopo essere state generate) non è necessaria la loro memorizzazione, eliminando di conseguenza i problemi ed i rischi relativi all'utilizzo delle tradizionali password statiche. Il dispositivo di Firma Remota può essere utilizzato anche per firmare documenti elettronici direttamente dal proprio iPad. È infatti disponibile l'applicazione: "Firma Digitale", scaricabile gratuitamente dall'App Store, con la quale è possibile sottoscrivere digitalmente documenti in pochi semplici passaggi. L'App "Firma

Digitale” di Aruba può essere utilizzata in abbinamento con i dispositivi di firma remota di tipo OTP con Display o OTP Mobile: è sufficiente disporre di una connessione internet.