Autenticazione dell'Utente

Classe 5ASI
ITCG Fermi

Definizioni

- **Riservatezza** (o **confidenzialità**, o **segretezza**) **dei dati**: dati leggibili e comprensibili solo dalle persone autorizzate
- **Integrità dei dati**: dati letti e/o modificati solo da persone autorizzate
- **Disponibilità dei dati**: dati devono essere disponibili in qualunque momento per le persone autorizzate per cui occorre garantire la continuità del servizio
- **Paternità** (o **non ripudiabilità**) **dei dati**: ogni dato deve essere associato ad un utente che non può ripudiare i dati da lui spediti e/o firmati.
- **Autenticazione** ("o" **autenticità**): processo di riconoscimento delle credenziali dell'utente per assicurarsi dell'identità di chi invia e/o esegue operazioni.
  Metodi di verifica dell'identità di un utente: (1) informazioni riservate (es. password), (2) oggetti elettronici (es. smart card), (3) strumenti di riconoscimento biometrici (es. impronta digitale, fondo retina ecc.)
- **Autorizzazione**: per l'utente autenticato occorre stabilire l'insieme delle autorizzazioni (azioni permesse, risorse accessibili, dati consultabili e/o modificabili)

Metodi di Autenticazione Elettronica

1. **Metodo di autenticazione basato su qualcosa (di immateriale) che l'utente ha** (password, PIN, ecc.)
2. **Metodo di autenticazione basato su qualcosa (di materiale) che l'utente possiede** (carte fisiche o elettroniche, dispositivi hardware, ecc.)
3. **Metodo di autenticazione basato su qualcosa di personale dell'utente** (dati biometrici come le impronte digitali, la conformazione della retina, ecc.)

Strumenti di Autenticazione Forte

1. **Accesso logico** (password e passphrase)
2. **OTP** (**One-Time Password**);
3. **Firma digitale**, **Posta Elettronica Certificata (PEC)**

1a Autenticazione con Password

Problemi

1. Memorizzazione delle password da parte dell'amministratore di sistema (o sistemista)
2. Scegliere e ricordarsi la password da parte dell'utente

Soluzioni al problema 1

i. Memorizzare le password in chiaro in un file protetto (es. file protetto da una password, o file protetto da cifratura); questa soluzione è sconsigliata
ii. Memorizzare le password in forma cifrata

1a Autenticazione con Password

Per accedere ad un servizio, per crittografare un documento, serve una **password** (o **parola chiave**, o **parola d'ordine**) oppure una **passphrase** (o **frase d'accesso**, o **frase segreta**) la quale è un insieme di parole o stringhe alfanumeriche.

Problema delle password: sono soggette ad **attacco a dizionario** (o **attacco forza bruta**) il quale si basa su un algoritmo che prova ad usare come password

- tutte le parole del dizionario (in diverse lingue)
- i nomi propri
- le permutazioni di ogni stringa (es. alcune permutazioni di *ciao* sono: ciao, caio, cioa, coia, ocia, ocai, iaco, ioca ecc.)

1a Autenticazione con Password

Difese dagli attacchi a dizionario (**e soluzioni al problema 2** nella slide 5)

i. **Alterare caratteri maiuscoli e minuscoli**
   Esempio: aBRAcaDAbRa invece di abracadabra
ii. **Sostituire O con 0, L con 1, S con 5, A con @ in una parola conosciuta**
   Esempio: 5egret0 invece di segreto
iii. **Deformazione di parole composte**
   Esempio: mezzaBotte, mezzaCotte invece di mezzanotte
iv. **Deformazione di parole composte + numeri** (sostituire O con 0, L con 1, S con 5, A con @) **e simboli** (sostituire doppie DD con 2D dove D è un generico carattere ripetuto due volte)
   Esempio: me2z@B02te invece di mezzaBotte
v. **Parole e numeri senza senso**
   Esempio: innestare data di nascita all'interno del nome ma995rio invece di mario995, sa19ra94 invece di sara1994

Prof. Montemurro

1b Autenticazione con Passphrase

Passphrase: insieme di parole o stringhe alfanumeriche.

Problema: scegliere e ricordarsi la passphrase da parte dell'utente.
Soluzioni

i. **Prendere una frase** (residente nella nostra memoria a lungo termine) **e ridurla a 12 caratteri** (o comunque ad un numero modesto di caratteri).
   Esempio: frase "Nel mezzo del cammin di nostra vita" diventa "nLmZdLcM" dopo aver applicato le seguenti 4 trasformazioni:
   - eliminare vocali: "Nl mzz dl cmmn d nstr vt"
   - eliminare doppie: "Nl mz dl cmn d nstr vt"
   - eliminare gli spazi e mantenere solo i primi 12 caratteri: "Nlmzdlcm"
   - alternare una lettera maiuscola ad una minuscola: " nLmZdLcM"

   Nota bene: occorre ricordarsi le trasformazioni per generare la passphrase.

Prof. Montemurro

1b Autenticazione con Passphrase

Soluzioni

ii. **Prendere frasi semplici che includono segni di punteggiatura e maiuscole**
Esempio: "A cura di LoRusso (non Lo Russo, Editore)"

iii. **Metodo Diceware**: utilizzo di 5 dadi per selezionare le parole a caso da un elenco speciale, chiamato **elenco di parole Diceware**, che contiene 7776 brevi parole, abbreviazioni, stringhe di caratteri nelle diverse lingue, facili da ricordare. Da ogni lancio dei 5 dadi si ottiene un numero di 5 cifre che corrisponde ad una parola nell'elenco di parole di Diceware.
Esempio: generazione di una passphase composta da 3 parole
- Numero "21434" → parola "gatto"
- Numero "53662" → parola "marrone"
- Numero "62352" → parola "penna"

Passphase: gattomarronepenna.

Prof. Montemurro

1b Autenticazione con Passphrase

Soluzioni

iv. **Concatenare parole brevi che piacciono all'utente numerandole e alternandole in forma maiuscola e minuscola**
Esempio: SOLE1pappa2MARE3ciccia4

Prof. Montemurro

2 Autenticazione con OTP

One-Time Password: password generata da dispositivi hardware, temporanea, cioè "usa e getta". Questa è più sicura delle password ideate dall'utente.

Metodi di generazione di OTP

i. **Lista condivisa di password OTP tra utenti e sistema di autenticazione**
ii. **Schema di Lamport**
iii. **…**

2 Autenticazione con OTP

Metodi di generazione di OTP

i. **Lista condivisa di password OTP tra utenti e sistema di autenticazione** (non viene usata): a ogni utente del sistema viene associata una lista contenente un elenco di password, ciascuna delle quali deve essere utilizzata una sola volta.

   Svantaggi:

   a. Manutenzione della lista condivisa; mantenere l'elenco aggiornato su più utenti è impegnativo e incline agli errori
   b. Appropriazioni indebite del file contenente la lista di password OTP
   c. Utente può smarrire l'elenco o non aggiornarlo

2 Autenticazione con OTP

Metodi di generazione di OTP

ii. **Schema di Lamport** (si usa uno simile a questo) basato su tre ingredienti

- $\boldsymbol{w}$, chiamato **seme**, è un valore arbitrario, scelto dall'utente, che deve essere mantenuto segreto
- $\boldsymbol{H}$, chiamata **funzione di hash**, è una funzione unidirezionale, cioè dato w, è facile calcolare $H(w)$, ma, dato $H(w)$, è impossibile calcolare w
- **n** è un numero naturale che definisce il numero di autenticazioni che devono essere eseguite basandosi sul valore segreto w (es. $n = 100$ significa che con la funzione H si potranno generare 100 password e quindi si potranno eseguire 100 autenticazioni)

Schema di Lamport: algoritmo nel quale, a partire dal valore del seme w associato all'utente, viene generato, mediante funzioni di hash, un insieme di password in sequenza, aventi come seme proprio w.

Prof. Montemurro

2 Autenticazione con OTP

La funzione H è usata per definire la sequenza di password OTP (H^i significa che la funzione H è applicata i volte; es. $H^3(w) = H(H(H(w)))$):

OTP usate dall'utente	Valori di verifica y usati dal sistema di autenticazione
Prima di usare OTP_1 il sistema sa $H^n(w)$	$y_1 = H(OTP_1) = H^n(w)$
$OTP_1 = H^{n-1}(w)$	$y_2 = H(OTP_2) = H^{n-1}(w)$
$OTP_2 = H^{n-2}(w)$	⋮
⋮	$y_{n-2} = H(OTP_{n-2}) = H^3(w)$
$OTP_{n-2} = H^2(w)$	$y_{n-1} = H(OTP_{n-1}) = H^2(w)$
$OTP_{n-1} = H^1(w) = H(w)$	$y_n = H(OTP_n) = H(w)$
$OTP_n = H^0(w) = w$	

Prof. Montemurro

2 Autenticazione con OTP: Esempio

- All'inizio, cioè prima che l'utente usi la prima password $OTP_1 = H^{n-1}(w)$, il sistema conosce $y_1 = H^n(w)$.
- Quando l'utente fornisce al sistema $OTP_1 = H^{n-1}(w)$, il sistema applica H e ottiene $H\left(H^{n-1}(w)\right) = H^n(w)$.
- A questo punto il sistema verifica se l'OTP usato dall'utente è valido eseguendo il confronto di seguito indicato (val. calcolato = val. in memoria):
  $$H^n(w) = y_1$$
  e conserva il valore $y_2 = H^{n-1}(w)$.
- Quando l'utente usa la $OTP_2 = H^{n-2}(w)$, il sistema applica H e ottiene $H\left(H^{n-2}(w)\right) = H^{n-1}$.
- A questo punto il sistema verifica se l'OTP usato dall'utente è valido eseguendo il confronto di seguito indicato:
  $$H^{n-1}(w) = y_2$$
  e conserva il valore $y_3 = H^{n-2}(w)$. E così via…

Prof. Montemurro

2 Autenticazione con OTP

Generalizzando, il confronto che il sistema di autenticazione esegue ogni volta che l'utente fornisce una password OTP è il seguente:

$$H(password\ OTP\ corrente) = password\ precedente$$

o equivalentemente:

$$H(OTP_i) = OTP_{i-1}$$

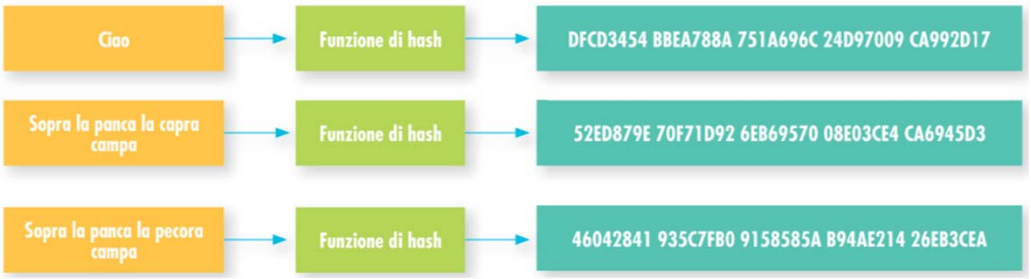
Inoltre il sistema memorizza la password OTP corrente, relativa all'autenticazione i-esima, perché sarà usata alla prossima autenticazione (la (i+1)-esima) per eseguire il nuovo confronto.

Prof. Montemurro

2 Autenticazione con OTP: Funzione di Hash

Funzione di hash H: funzione unidirezionale, cioè dato w, è facile calcolare $H(w)$, ma, dato $H(w)$, è impossibile calcolare w. Tale funzione è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria in una stringa binaria di lunghezza fissa, chiamata **valore di hash** (poi viene convertita in esadecimale per motivi di leggibilità).

Esempi



Prof. Montemurro

2 Autenticazione con OTP: Funzione di Hash

Gli algoritmi che generano le password OTP vengono inseriti in dispositivi hardware; ogni dispositivo viene associato ad un solo utente, e ogni dispositivo viene inizializzato con un suo **codice-chiave** (il seme w di cui abbiamo parlato prima).

Autenticazione a due fattori 2FA: processo di sicurezza che richiede agli utenti di fornire due diversi fattori di autenticazione per verificare la propria identità (es. password + OTP; carta di credito + PIN; password + impronta digitale). Si usa una combinazione dei tre metodi di autenticazione visti all'inizio (qualcosa di immateriale che l'utente ha, qualcosa di materiale che l'utente possiede, qualcosa di personale dell'utente).

Prof. Montemurro

3a Autenticazione con Firma Digitale

Firma elettronica: espressione priva di qualsiasi valenza tecnico-giuridica che fa riferimento a qualsiasi tecnica (1) utilizzata per l'autenticazione elettronica, e (2) che consente di associare dati ad altri dati (es. la firma ad un documento).

Metodi di autenticazione elettronica (slide 3):

1. **Metodo di autenticazione basato su qualcosa (di immateriale) che l'utente ha** (password, PIN, ecc.)
2. **Metodo di autenticazione basato su qualcosa (di materiale) che l'utente possiede** (carte fisiche o elettroniche, dispositivi hardware, ecc.)
3. **Metodo di autenticazione basato su qualcosa di personale dell'utente** (dati biometrici come le impronte digitali, la conformazione della retina, ecc.)

3a Autenticazione con Firma Digitale

Firma digitale: equivalente informatico di una tradizionale firma autografa apposta su carta; si parla di firma digitale perché riguarda un **documento digitale** (o **documento elettronico**, o **documento informatico**), non uno cartaceo.

Caratteristiche della firma digitale

1. **Autenticità**: il destinatario può verificare l'identità del mittente
2. **Integrità**: assicura che il documento non sia stato modificato dopo aver apposto la firma digitale
3. **Non ripudio**: il mittente non può disconoscere un documento da lui firmato, tale documento ha piena validità legale

3a Autenticazione con Firma Digitale

Principio di funzionamento della firma digitale: basato sulla criptografia asimmetrica; in particolare, il mittente possiede (*):

1. una chiave privata SK (Secret Key) la quale non viene condivisa, ed è usata dal mittente per cifrare la firma digitale da apporre sul documento digitale;
2. la corrispondente chiave pubblica PK (Public Key) la quale viene condivisa coi destinatari in modo tale che essi possano verificare l'identità del mittente (solo la PK associata alla SK può decifrare i dati cifrati con la SK; una generica PK associata ad un'altra SK non può farlo).

(*) Ricorda che chiave pubblica e privata vengono generate insieme a formare una coppia.

3a Autenticazione con Firma Digitale

Componenti del kit per apporre la firma digitale

3a Autenticazione con Firma Digitale

Componenti del kit per apporre la firma digitale

1. **Dispositivo sicuro di generazione delle firme digitali** il quale in genere è una **smart card** nella quale viene memorizzata la chiave privata. Tale dispositivo di firma sicuro viene rilasciato al richiedente da un ente certificatore il quale deve verificare l'identità del richiedente stesso prima di consegnargli (i) la smart card abilitata alla firma digitale, e (ii) il PIN da usare contemporaneamente alla smart card per poter usare la chiave privata
2. **Lettore di smart card**
3. **Software** che, dopo l'attivazione di un account, permette di **apporre la firma digitale** e la **marcatura temporale** sul documento digitale, e che permette di **verificare l'autenticità** e l'**integrità della firma stessa**
   Marcatura temporale: servizio che permette di associare data e ora certe, e legalmente valide ad un documento digitale.

Prof. Montemurro

3a Autenticazione con Firma Digitale

Smart card: dispositivo idoneo per apporre la firma digitale in quanto rispetta i seguenti otto requisiti:

1. apparato elettronico programmabile solo all'origine
2. fa parte del sistema di validazione
3. conserva in modo protetto le chiavi private
4. genera firme digitali al suo interno
5. non è riproducibile
6. è in parte non modificabile
7. l'accesso alla chiave privata è protetto da una procedura di identificazione del titolare (es. inserimento di un PIN)
8. evita di lasciare tracce della chiave privata sul sistema di validazione

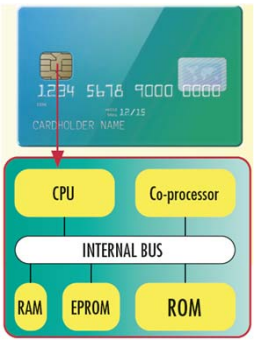
Nota bene: la **Tessera Sanitaria-Carta Nazionale dei Servizi TS-CNS** è una smart card per (i) l'identificazione dell'utente in rete, (ii) la firma digitale, (iii) l'accesso a diversi servizi resi disponibili dalle diverse amministrazioni.

Prof. Montemurro

3a Autenticazione con Firma Digitale

Smart card (continuazione): tessera plastificata, delle dimensioni di una carta di credito, su cui è integrato un **microchip programmabile** con:

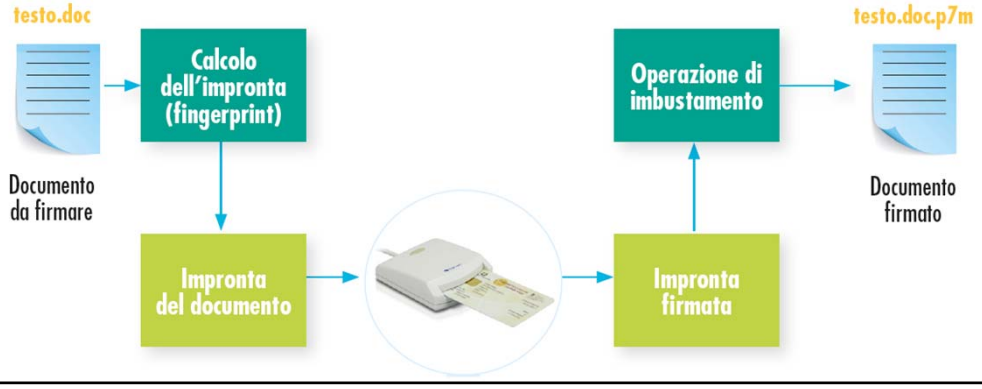
1. una memoria (Read Only Memory ROM) che contiene il sistema operativo e i programmi "fissi";
2. una memoria (Programmable Read Only Memory PROM) che contiene il numero seriale della smart card;
3. una terza memoria (Erasable Programmable Read Only Memory EPROM) che contiene i dati del proprietario e i meccanismi di protezione che ne evitano la clonazione.



Approfondimento

3a Autenticazione con Firma Digitale

Formato del documento digitale firmato digitalmente: quando si firma un documento digitale, il file viene incapsulato in una sorta di **busta criptografica**; il risultato è un nuovo file con estensione **.p7m** il quale consente di firmare qualunque tipo di file (.doc, .pdf, .xls ecc.). Le pubbliche amministrazioni sono obbligate per legge ad accettare il formato .p7m.



3b Autenticazione con PEC

Posta Elettronica Certificata PEC: sistema di comunicazione simile alla posta elettronica standard, tale che il mittente sia univocamente identificato.

- Un documento inviato con la PEC assume il medesimo valore legale di una **raccomandata con ricevuta di ritorno**.
- Un'email può essere considerata posta elettronica certificata (PEC) solo se sia la casella del mittente sia quella del destinatario sono caselle di PEC.
- Ogni impresa è obbligata per legge ad avere un indirizzo di PEC iscritto nel Registro delle Imprese INI-PEC, altrimenti l'impresa stessa viene cancellata da tale registro. Ogni ordine (ingegneri, architetti, avvocati, medici) fornisce una PEC gratuitamente.

3b Autenticazione con PEC

Elenco pubblico dei gestori accreditati: gestori riconosciuti dall'Agenzia per l'Italia Digitale AgID che:

i. certificano l'identità del mittente e del destinatario;
ii. certificano l'integrità del messaggio;
iii. datano con precisione invio e ricezione;

essi sono obbligati a mantenere per 30 mesi (2 anni e mezzo) i dati che riguardano la trasmissione dei messaggi tramite PEC.

Esempio

InfoCert è gestore accreditato di PEC iscritto nell'Elenco Pubblico dei Gestori accreditati, presente nel sito DigitPA, e il suo servizio di Posta Elettronica Certificata è **Legalmail**.

3b Autenticazione con PEC: Principio di Funzionamento

Premessa: il mittente, dopo aver predisposto il documento da inviare, deve essere identificato dal proprio provider ad esempio tramite user_ID e password.

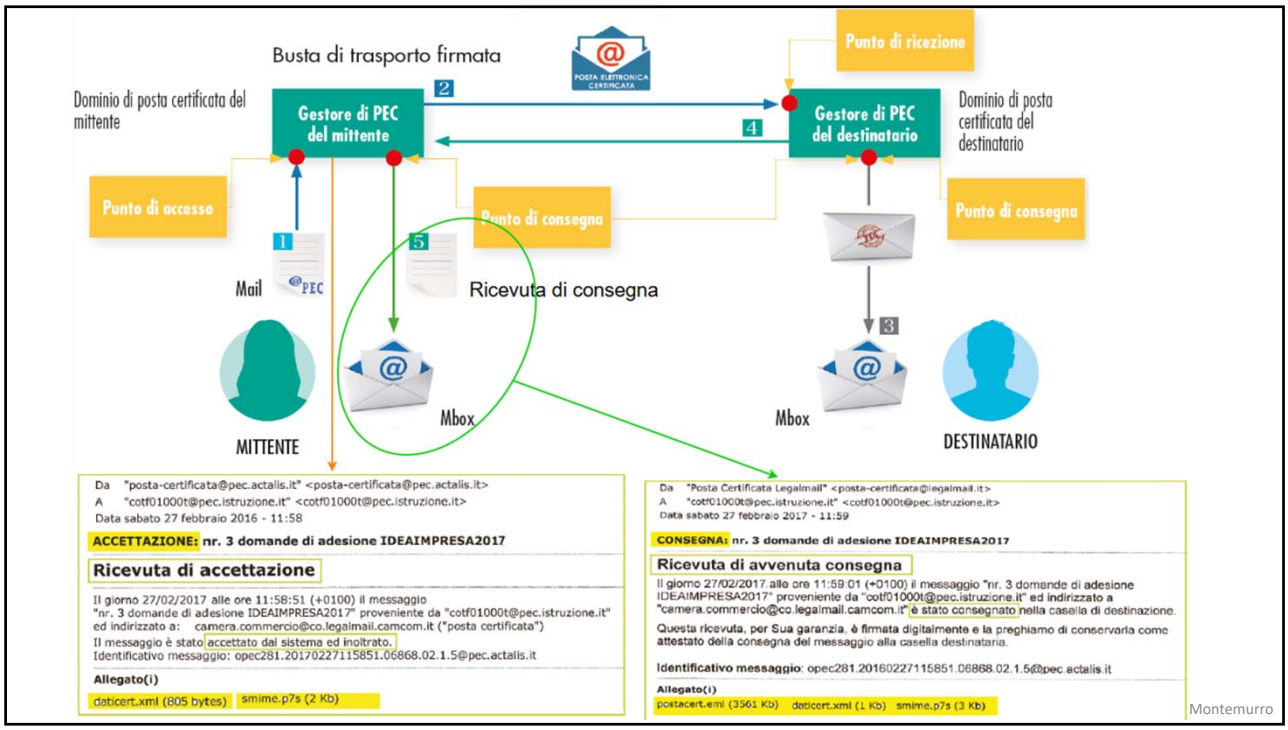
1. Quando il mittente invia un messaggio tramite PEC, egli riceve una **ricevuta di accettazione** del messaggio da parte del suo provider il quale firma tale ricevuta. Essa conferma al mittente la trasmissione del messaggio, e contiene: (i) data e ora dell'invio del messaggio; (ii) il mittente; (iii) il destinatario; (iv) l'oggetto del messaggio.
2. **Integrità del messaggio**: garantita dal provider del mittente il quale crea un nuovo messaggio, detto **busta di trasporto**, costituito (i) dal messaggio originale, e (ii) dai principali dati di spedizione. Tale messaggio viene firmato dal provider del mittente con la sua chiave privata SK; il provider del destinatario, che possiede la chiave pubblica associata alla SK, può usarla per decriptarlo e quindi per constatare la sua integrità.

Prof. Montemurro

3b Autenticazione con PEC: Principio di Funzionamento

3. Il destinatario riceve la busta di trasporto (messaggio + dati spedizione) nella propria casella PEC.
4. Se tutti i controlli fatti danno esito positivo; il provider del destinatario provvede anche a inviare al gestore del mittente la **ricevuta di consegna**, che è un normale messaggio email firmato dal gestore del destinatario che attesta: (i) la ricezione del messaggio da parte del destinatario, (ii) la data e l'ora della consegna, (iii) tutto ciò che è stato consegnato.

Prof. Montemurro



3b Autenticazione con PEC

Vantaggi della PEC

1. **Risparmio di denaro**: invio di un numero illimitato di comunicazioni senza alcun costo di spedizione; non si devono acquistare buste, lettere, francobolli; non si devono occupare spazi per conservare i documenti cartacei o le ricevute delle poste
2. **Risparmio di tempo**: si possono spedire documenti dal proprio PC e le ricevute arrivano subito; non si perde tempo a inviare fax o fare code alle poste


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
dziękuję
bedankt
obrigado
merci
go raibh maith agat
dank je
спасибо
sukriya
terima kasih
grazie
arigatô
dakujem
tapadh leat
mochchakkeram
hvala
mauruuru
sagolun
kop khun krap
takk
tack
рахмат
Баярлалаа
감사합니다
ευχαριστώ
мерси