

Servizi centrali per il mailing

Alessandro Brunengo

Mirko Corosu

Di cosa parleremo

- Sezione 1: Introduzione (su alcuni concetti di base)
- Sezione 2: Sicurezza (cenni)
- Sezione 3: Servizi centrali per il mailing
 - Sezione 3a: Gestione di alias nazionali
 - Sezione 3b: Servizi per la PEC

Sezione 1: Introduzione su alcuni concetti di base

Casella di posta elettronica (semplificando)

- La casella di posta elettronica e' il posto in cui vengono recapitati e conservati i messaggi
 - storage per ospitare i messaggi
 - credenziali di accesso alla casella (tipicamente **username** e **password**)
 - meccanismi di accesso ai messaggi (ad es.: imap(s), pop(s), http(s))
 - servizi accessori (filtri, automazione, address book, backup, ...)
- Ad una casella di posta elettronica e' associato un **indirizzo di posta elettronica**

Indirizzo di posta elettronica

- Una stringa del tipo **<username>@<domain>**
- Ha lo scopo di permettere la trasmissione di un messaggio di posta elettronica fino alla casella di destinazione
 - <domain> permette di individuare il o i server a cui recapitare il messaggio
 - questi si dicono **mail relay** del dominio <domain>
 - <username> individua la casella desiderata tra quelle gestite dal server
- Esempio: **brunengo@ge.infn.it**

Alias di posta elettronica

- Un alias di posta elettronica e' **un indirizzo** utilizzato come **sinonimo** (o alternativa) all'indirizzo di una casella di posta elettronica

Esempio: **alessandro.brunengo@ge.infn.it**

A questo indirizzo i server del dominio ge.infn.it associano l'indirizzo brunengo@ge.infn.it, a cui corrisponde la casella di destinazione

alessandro.brunengo@ge.infn.it --> brunengo@ge.infn.it --> casella

Configurazione tipica per gli utenti INFN

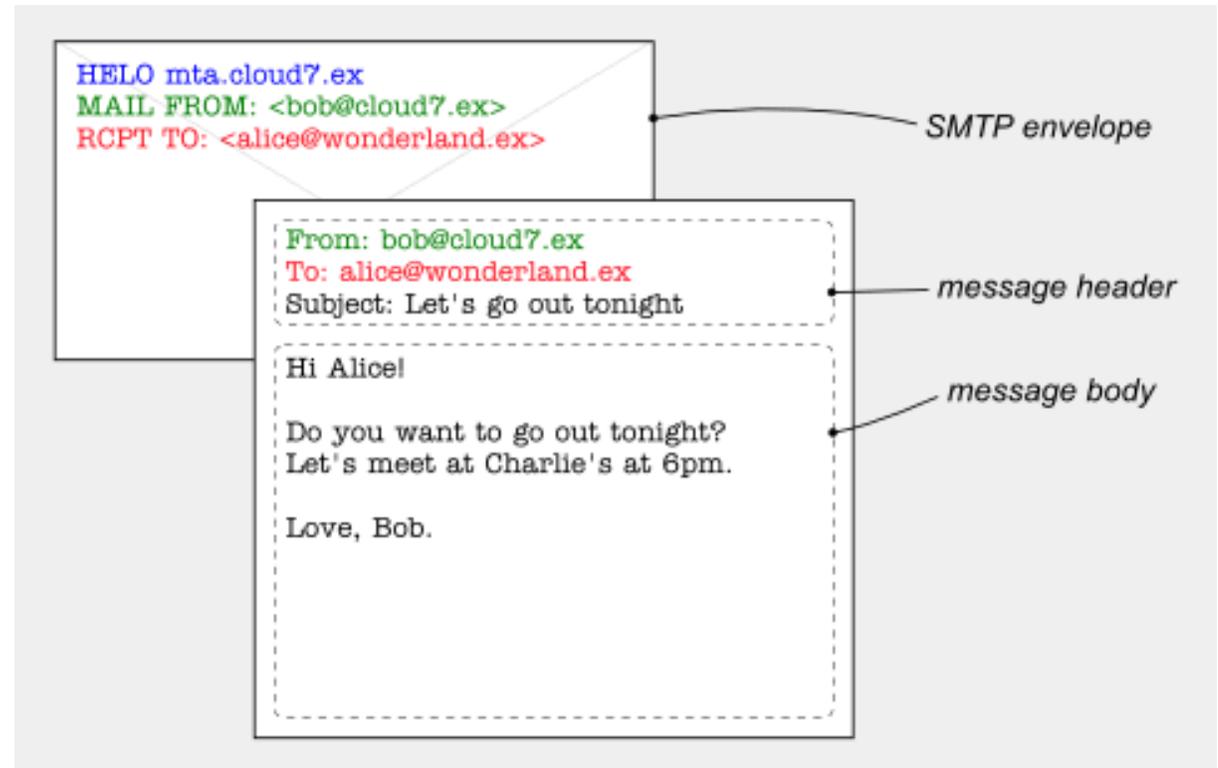
- **In ogni sede INFN esiste un servizio di posta elettronica per gli utenti afferenti a quella sede**
- Ciascun utente dispone tipicamente di:
 - una casella (nella sede di appartenenza)
 - un indirizzo associato alla casella (<username-di-sede>@<sede>.infn.it)
 - un alias esteso (<nome>.<cognome>@<sede>.infn.it)
- Quando un utente appartiene a più di una sede, tipicamente ha una casella con relativi indirizzi e alias **per ciascuna sede**

Messaggio di posta e trasporto

Un messaggio di posta elettronica e' costituito essenzialmente da tre parti:

- **Envelope**: contiene le informazioni necessarie al trasporto. **Non vengono recapitate nella casella.**
- **Header**: contiene informazioni necessarie alla gestione da parte di filtri e alla visualizzazione del messaggio (**From, To, Subject, ...**)
- **Body**: il contenuto vero e proprio del messaggio (inclusi gli attachment)

Il protocollo di trasporto non si cura di headers e body, ma solo del transito dal mittente al destinatario, utilizzando la envelope, tramite protocollo SMTP



Visualizzazione del messaggio

- I client, incluso il webmail, visualizzano un messaggio in modo elaborato:
 - alcuni header sono usati per visualizzare mittente, destinatario, data, subject, eventuali destinatari in copia (CC)
 - alcuni di questi vengono ulteriormente elaborati (ad esempio, gli indirizzi rielaborati tramite eventuali presenze nella agenda e visualizzati con nickname)
 - tipicamente il corpo del messaggio contiene tutte le sezioni in formato testo o HTML (corpo principale, vCard, ...)
 - gli attachment sono mostrati in un elenco a parte, scaricabili o visualizzabili tramite previewer
 - **multi header non vengono mostrati** (inutili ai fini del contenuto)
- E' sempre possibile visualizzare il messaggio completo (*source*)
 - tramite apposite voci di menu', o shortcut (per thunderbird: CTRL^U)

[From, To] vs [MAIL FROM, RCTP TO]

- L'Envelope e' l'equivalente della "busta"
- Questa contiene i dati usati dai server per recapitare il messaggio al o ai destinatari. I principali sono:
 - **MAIL FROM:** <source address> (necessario per notificare errori)
 - **RCTP TO:** <destination address> (puo' comparire piu' volte)
- I dati di envelope sono usati per il trasporto fino a destinazione, ma **non vengono recapitati nella casella**, che conterra' solo il messaggio (header e body)
- Non c'e' relazione tra gli indirizzi indicati in **MAIL FROM** e **RCPT TO** e gli indirizzi che compaiono negli header "**From**", "**To**", "**Cc**"

Envelope e Headers

	<p>L'Envelope contiene le reali informazioni di destinazione, scambiate dai server di trasporto. Non vengono recapitate col messaggio (questo e' diverso dalla posta ordinaria)</p>	<pre>MAIL FROM: brunengo@ge.infn.it RCPT TO: corosu@ge.infn.it DATA</pre>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------

<p>Da: Brunengo A: Corosu Oggetto: Cose da fare</p>	<p>Queste informazioni non vengono usate per il trasporto. Ci si puo' scrivere qualunque cosa</p>	<pre>From: brunengo@ge.infn.it To: corosu@ge.infn.it Subject: Cose da fare</pre>
<p>Caro Mirko, per piacere, fai in prima prioritaa' tutte le cose che dovrei fare io, poi quelle che devi fare tu. Grazie. Ciao. Alessandro</p>	<p>Caro Mirko, per piacere, fai in prima prioritaa' tutte le cose che dovrei fare io, poi quelle che devi fare tu. Grazie. Ciao. Alessandro</p>	<p>Questo e' quello che viene recapitato nella casella</p>

Headers non sempre attendibili

- Di norma quando si usa un client, si specificano gli header che compariranno nel messaggio (From, To, Cc, Reply-To)
- Il client costruisce:
 - un messaggio con gli header **From**, **To**, **Cc** ... desiderati
 - una envelope corrispondente:
 - **MAIL FROM** coincidente con From:
 - un **RCPT TO** per ciascun destinatario specificato in To:, Cc: e Bcc
- E' pero' possibile (e facile) inviare un messaggio con dati di envelope diversi dai corrispondenti headers
 - quindi, ad esempio, indicare **From** fasulli.

Firma digitale ed encryption: PGP e S/MIME

- Da RFC 5321:
“Real mail security lies only in end-to-end methods involving the message bodies, such as those that use digital signatures (see [RFC 1847 \[43\]](#) and, e.g., Pretty Good Privacy (PGP) in [RFC 4880 \[44\]](#) or Secure/ Multipurpose Internet Mail Extensions (S/MIME) in [RFC 3851 \[45\]](#))”
- Entrambi i protocolli utilizzano tecniche di encryption basate su chiavi asimmetriche per permettere la firma digitale di un messaggio, in modo che il ricevente sia in grado di verificarla
 - la chiave contiene l'identificativo del mittente (l'indirizzo) e quindi costituisce verifica sul mittente del messaggio
 - entrambi i protocolli possono essere utilizzati anche per l'encryption

Firma digitale: come implementarla

- Qui parliamo di certificati x.509 (no PGP)
- Tutti i client moderni supportano la firma digitale tramite S/MIME
 - ma quasi nessun webmail lo supporta (Zimbra, Kopano)
 - comunque potrebbe introdurre un problema di security
- Per attivare la firma digitale:
 - procurarsi un certificato x.509 che certifichi **l'indirizzo di posta elettronica che usiamo come From nei messaggi che inviamo**
 - installare il certificato sul client di posta elettronica
 - configurare l'account per firmare digitalmente i messaggi (tutto o ad hoc)
 - il client chiederà quale certificato usare

To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate.

Digital Signing

Use this certificate to digitally sign messages you send:

Alessandro Brunengo [04:E1:B2:8D:93:A1:2]

Digitally sign messages (by default)

Encryption

Use this certificate to encrypt & decrypt messages sent to you:

Alessandro Brunengo [04:E1:B2:8D:93:A1:2]

Default encryption setting when sending messages:

Never (do not use encryption)

Required (can't send message unless all recipients have certificates)

click per selezionare il certificato

click per abilitare la firma dei messaggi per default

- corsoDirigenti
- mcnp
- mm_gdpr_audit
- preventivi_2019

Sezione 2: Sicurezza (cenni)

2. Security

I due problemi di sicurezza piu' comuni legati all'utilizzo della posta elettronica sono:

- Virus veicolati tramite e-mail
 - come attachment
 - come hyperlink nel corpo del messaggio
 - in altri modi (piu' complessi, piu' rari, che non vedremo)
- Accesso alle credenziali della casella di posta elettronica
 - Un caso particolare: il phishing

i) virus in attachment

- Un virus puo' essere trasferito sul nostro calcolatore tramite attachment:
 - **file eseguibili** (.com, .exe, .js, .vba, ...)
 - **macro** incluse in **documenti di office** (.doc, .docx, .xls, .xlsx, ...)
 - file che possono **sfruttare vulnerabilita'** del programma preposto a trattarli (es: .pdf)
 - **double extension** (.jpg.exe)
 - tramite ciascuno dei precedenti, ma **nascosti in file compressi** (.zip, .rar)
 - eventualmente **protetti da password, comunicata nel testo del messaggio**
- Sfruttano l'eventualita' che sia abilitato il "preview" nel client di posta elettronica
 - ed eventuali ulteriori debolezze di sicurezza degli applicativi (Office, PDF reader, etc)
- O la **fiducia malriposta sull'apparente mittente del messaggio**

i) virus in attachment: difesa

- Disabilitare il preview (o utilizzare webmail)
- Non fidarsi di messaggi inattesi con attachment
 - controllare gli header (vedi slide successiva)
 - meglio ancora: **chiamare il Servizio Calcolo**
- Diffidare di file compressi con password (se non attesi)
- Mantenere aggiornate e correttamente configurate le applicazioni che possono veicolare l'attacco
 - disabilitare **l'esecuzione automatica di macro in office**
 - disabilitare **l'esecuzione automatica di codice nei PDF reader**
 - in generale mantenere le configurazioni di sicurezza ove disponibili
- Mantenere il proprio PC con un **antivirus aggiornato**
 - eventualmente salvare l'attachment sul proprio PC e farne uno scan con l'antivirus

```
Source of: imap://brunengo@mbox.ge.infn.it:993/fetch%3EUID%3E.INBOX%3E429566

Return-Path: <alessandro.brunengo@infn.it>
Received: from mbox3.ge.infn.it ([unix socket])
  by mbox3 (Cyrus v2.3.16-Fedora-RPM-2.3.16-15.el6) with LMTPA;
  Sun, 27 Oct 2019 23:44:46 +0100
X-Sieve: CMU Sieve 2.3
Received: from dns1.ge.infn.it (dns1.ge.infn.it [193.206.144.10])
  by mbox3.ge.infn.it (Postfix) with ESMTP id 9F03814239A
  for <brunengo@mbox3.ge.infn.it>; Sun, 27 Oct 2019 23:44:46 +0100 (CET)
Received: by dns1.ge.infn.it (Postfix)
  id 80621E1166; Sun, 27 Oct 2019 23:44:46 +0100 (CET)
Delivered-To: brunengo@mail.ge.infn.it
Received: from dns1.ge.infn.it (localhost [127.0.0.1])
  by localhost (Postfix) with SMTP id 75E55E422E
  for <brunengo@mail.ge.infn.it>; Sun, 27 Oct 2019 23:44:46 +0100 (CET)|
Received: from mxge3.ge.infn.it (mxge3.ge.infn.it [193.206.144.43])
  by dns1.ge.infn.it (Postfix) with ESMTP id C2BA5E1166
  for <brunengo@mail.ge.infn.it>; Sun, 27 Oct 2019 23:44:45 +0100 (CET)
Received: by mxge3.ge.infn.it (Proxmox)
  id A192C34107B; Sun, 27 Oct 2019 23:45:00 +0100 (CET)
Delivered-To: alessandro.brunengo@ge.infn.it
Received: from mxge3.ge.infn.it (localhost.localdomain [127.0.0.1])
  by mxge3.ge.infn.it (Proxmox) with ESMTP id 9350934119C
  for <alessandro.brunengo@ge.infn.it>; Sun, 27 Oct 2019 23:45:00 +0100 (CET)
Received: from infngw1.infn.it (infngw1.infn.it [131.154.1.5])
  by mxge3.ge.infn.it (Proxmox) with ESMTP id 92BD534107B
  for <alessandro.brunengo@ge.infn.it>; Sun, 27 Oct 2019 23:44:59 +0100 (CET)
Received: by infngw1.infn.it (Postfix)
  id 7C2C56002372; Sun, 27 Oct 2019 23:44:44 +0100 (CET)
Delivered-To: alessandro.brunengo@infn.it
Received: from mxge3.ge.infn.it (mxge3.ge.infn.it [193.206.144.43])
  by infngw1.infn.it (Postfix) with ESMTP id 736216002370
  for <alessandro.brunengo@infn.it>; Sun, 27 Oct 2019 23:44:44 +0100 (CET)
Received: from mxge3.ge.infn.it (localhost.localdomain [127.0.0.1])
  by mxge3.ge.infn.it (Proxmox) with ESMTP id 2D53134119C
  for <alessandro.brunengo@infn.it>; Sun, 27 Oct 2019 23:44:59 +0100 (CET)
Received: from smtp4.ge.infn.it (smtp4.ge.infn.it [193.206.144.60])
  by mxge3.ge.infn.it (Proxmox) with ESMTP id 2A6E034107B
  for <alessandro.brunengo@infn.it>; Sun, 27 Oct 2019 23:44:57 +0100 (CET)
Received: from MACBRUNENGO.local (vpnclient54.ge.infn.it [193.206.149.184])
  by smtp4.ge.infn.it (Postfix) with ESMTPSA id F308D1A3734
  for <alessandro.brunengo@infn.it>; Sun, 27 Oct 2019 23:44:41 +0100 (CET)
DKIM-Filter: OpenDKIM Filter v2.11.0 smtp4.ge.infn.it F308D1A3734
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=ge.infn.it;
  s=default; t=1572216282; Tutorial days di CCR: i servizi nazionali della CCR
  bh=1sypoblEwSIRbEzUQ2C2cMIhZVPAvjHkEj9MTbF4I5g=;
```

i) virus puntati da hyperlink nel corpo del mail

- Un virus puo' essere trasferito sul nostro calcolatore tramite hyperlink nel corpo del messaggio:
 - il link puo' puntare ad un file eseguibile o contenente macro
 - il link puo' sfruttare bachi del browser
- Anche in questo caso l'attacco sfrutta la fiducia che il destinatario ha nei confronti dell'apparente mittente
- O la fiducia nella apparente destinazione del link presente nel messaggio
 - **Andate sempre a verificare la destinazione reale del link** posizionando il puntatore del mouse sul link e guardando la riga che compare in basso sull'applicazione client o webmail (vedi slide successiva)

Inbox - alessandro.brunengo@in

Get Messages | Write | Chat | Address Book | Reply | Reply All | Forward | Delete | Tag | Quick Filter | Search <⌘K>

alessandro.brunengo@infn.it

Inbox (14)

- Drafts (1022)
- 2014
- 2016
- 2017
- 2018 (1)
- 2019
- Account
- CasellePEC
- LicenzaAcrobat
- Phishing
- Sent
- Junk
- aaaa
 - aaa_UPS (1037)
 - backpec_log (2)
 - corso_sicurezza
 - corsoDirigenti
 - mcnp
 - mm_gdpr_audit
 - preventivi_2019
 - spam_falliti (+92)
 - techtrack
 - trendmicro (+8)
 - web_cookie
 - WindowsXP
- academia
- agenda
- Archive
- calcolo (+1602)

Subject	From	Date
Backup Error for host apcx8, dir /	root	23:35
Backup Error for host apcx8, dir /mnt_work/apcx8	root	23:35
Backup Error for host apcx9, dir /	root	23:35
Backup Error for host apcx9, dir /mnt_work/apcx9	root	23:35
Inventario	Alessandro Brunen...	23:44

From Me <alessandro.brunengo@infn.it> ★

Subject Inventario

To Me <alessandro.brunengo@infn.it> ★

This message may be a scam. Preferences X

Caro Alessandro, scarica il documento <http://www.ge.infn.it/~brunengo/inventario.xls> e dacci una occhiata.

Grazie e ciao.
Alessandro

Alessandro Brunengo
Istituto Nazionale di Fisica Nucleare - Sezione di Genova
Via Dodecaneso, 33 - 16146 - Genova - Italy
tel: +39-010-3536317
fax: +39-010-310075

Unread: 14 Total: 18564 Today Pane ^

Posiziona il mouse

Vedi la reale destinazione

Infine una informazione molto utile:

Non, ripeto: **non**, avete vinto alla lotteria
specie se non avete partecipato. Mi spiace.

ii) Accesso alle credenziali

- Il problema e' la conseguenza:
 - **viene usato il server di posta della sede** (normalmente soggetto ad autenticazione) per inviare SPAM o virus
 - in modo credibile ai contatti dell'utente
 - comunque **caricando la responsabilita' sull'utente e sul servizio di posta dell'utente**
 - come conseguenza, il sistema di posta dell'utente viene **inserito in tutte le blacklist del mondo**
 - **tutti** i messaggi inviati dai server della sede verranno rigettati per via delle black list
 - tutti i messaggi **inviati da tutti gli utenti** della sede! Il servizio risulta bloccato.
- Rimuovere i server dalle black list e' una operazione lunga, non sempre gratuita, non sempre fattibile! A volte si deve solo aspettare (settimane)
 - google e microsoft non ti ci levano, probabilmente non sanno nemmeno come fare

ii) Accesso alle credenziali: phishing

- Il phishing e' il tentativo di carpire credenziali **inducendo l'utente ad inserirle in apposite form web** tramite messaggi fasulli
 - l'attaccante simula di essere il supporto informatico dell'utente
 - comunica all'utente qualche azione imminente e preoccupante
 - hai esaurito la quota, ti disabilito l'account, ti scade la password...
 - chiede all'utente di collegarsi ad una URL e di inserire le proprie credenziali per poi eseguire una qualche operazione
 - a volte la URL ha lo stesso aspetto dei siti usati dall'utente
- Recentemente il phishing e' stato la maggiore sorgente di problemi di sicurezza

Phishing: come difendersi

Alcuni suggerimenti:

- diffida sempre di chi ti chiede di **inserire le tue credenziali ad un link proposto** nel mail
- **verifica la destinazione del link** prima di fare click (vedi slide precedenti)
- **verifica la provenienza originaria del messaggio** negli header del sorgente (vedi slide precedenti)
- se tutto sembra OK, **chiedi ugualmente al servizio calcolo**
 - il supporto non dovrebbe mandare mai mail con link in cui inserire credenziali

Importantissimo:

- Se ti sei sbagliato, e distrattamente sei caduto nel tranello...

avverti immediatamente il servizio calcolo

Sezione 3: Servizi centrali per il mailing

Servizi di mailing nazionali per gli utenti

- Gestione e registrazione di alias nel dominio @infn.it
- Servizi per la PEC

Accesso ai servizi offerti:

<https://mailing.infn.it>

I Servizi Nazionali gestiscono anche un list server nazionale
ne parlera' approfonditamente Stefano tra poco

Alias nazionale

- Perché
 - Esigenza di rappresentanza (come tutte le altre organizzazioni nel mondo)
 - Necessità di associare all'account AAI un indirizzo email valido
- Per ogni account definito in AAI viene automaticamente creato un alias <AAI-uid>@infn.it, che punta **alla casella di posta associata all'indirizzo di sede registrato in AAI**
- E' disponibile una interfaccia per poter registrare un alias nazionale esteso (piccola demo)
 - questo permette di ricevere sulla casella di sede i messaggi indirizzati all'alias scelto

Indirizzo e-mail "principale"

- Una certa importanza riveste l'indirizzo che compare nell'attributo ***mail*** di AAI
- Questo attributo e' utilizzato, in relazione al mailing, in due circostanze:
 - quando si accede alla interfaccia per ottenere un certificato x.509 da Terena
 - il certificato sara' in grado di **certificare quell'indirizzo di posta** nella firma digitale
 - quando si accede al listserver nazionale
 - il listserver ha bisogno di **associare alla persona autenticata un indirizzo di posta** per gestire le **policy di accesso alla visualizzazione o configurazione delle liste**
 - il listserver considerera' quello presente nell'attributo mail di AAI come indirizzo da usare

Selezione dell'indirizzo principale

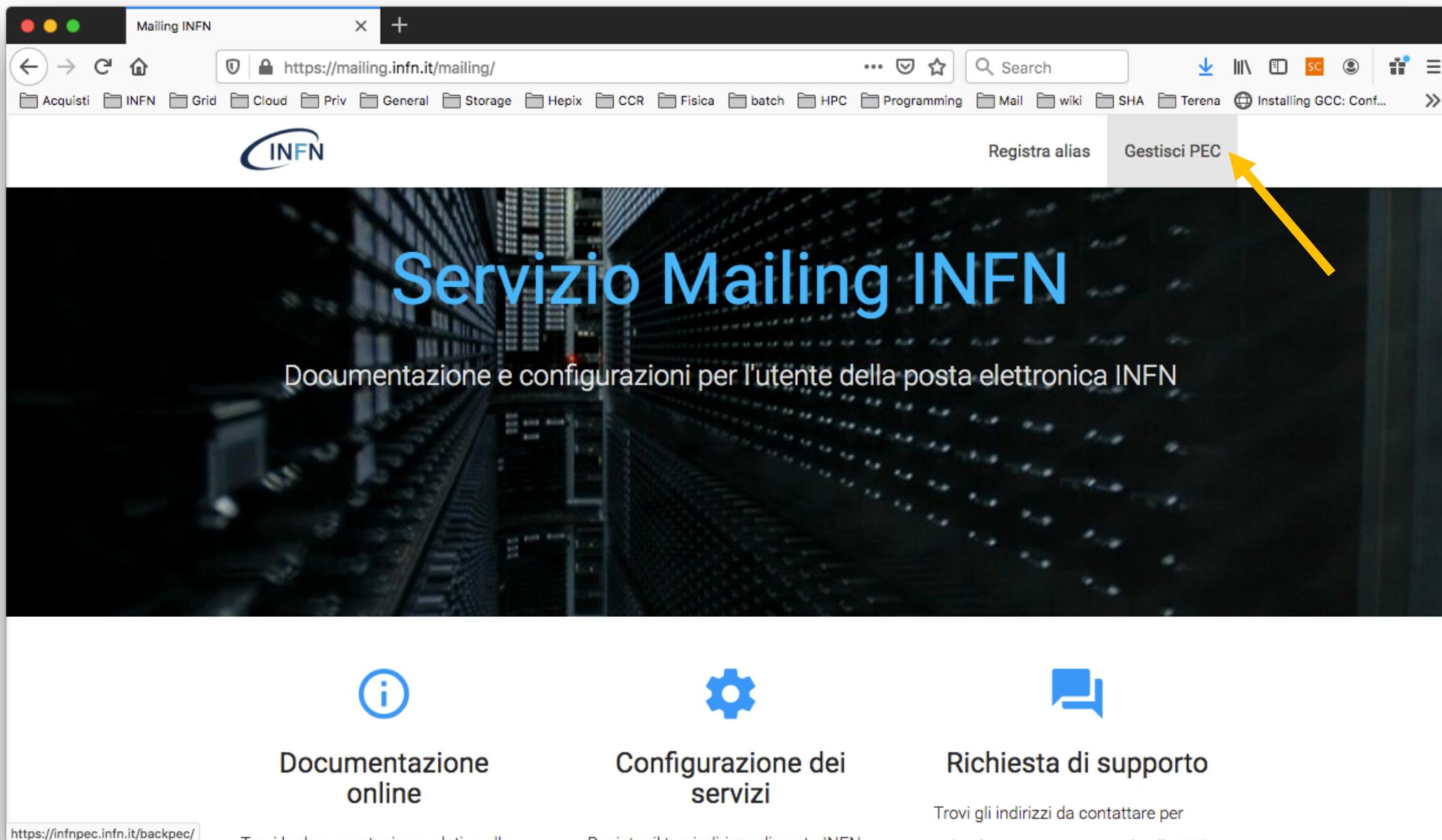
- Sara' quindi necessario assegnare all'attributo mail di AAI l'alias nazionale:
 - se si desidera inviare mail firmate con un alias nazionale come mittente
 - se si desidera usare l'alias nazionale nelle liste gestite dal list server nazionale
- E' possibile fare questa operazione attraverso il portale <https://mailing.infn.it> (piccola demo)

Servizi per la PEC

- Caselle PEC:
 - istituzionali
 - per i RUP
- La casella PEC non e' gestita da un servizio interno
 - sforzo non sostenibile (e forse inutile)
- Problemi evidenziati:
 - **attivazione** (si deve passare attraverso una procedura di acquisto...)
 - **riempimento della casella** (non esistono servizi senza quota)
 - **recupero di messaggi cancellati** per errore (i provider non offrono questo servizio)

-----> Sviluppato un servizio centrale per risolvere questi problemi

accesso al servizio: link "Gestisci PEC" del portale <https://mailing.infn.it/>

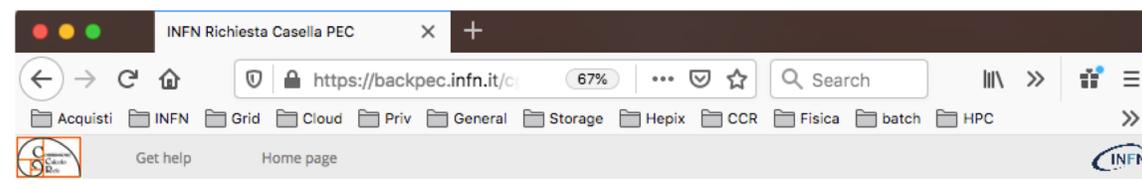
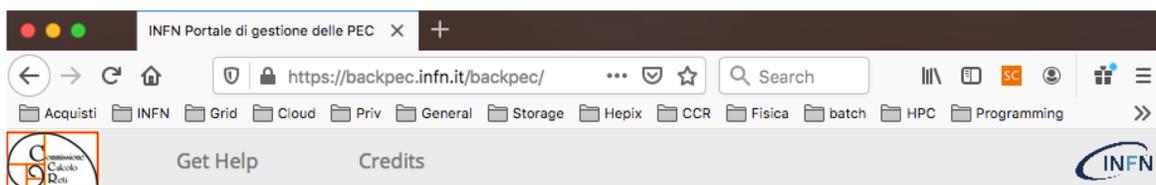


The screenshot shows a web browser window with the address bar displaying `https://mailing.infn.it/ mailing/`. The browser's address bar includes navigation icons (back, forward, refresh, home), a search bar, and a list of folders: Acquisti, INFN, Grid, Cloud, Priv, General, Storage, Hepix, CCR, Fisica, batch, HPC, Programming, Mail, wiki, SHA, Terena, and Installing GCC: Conf... The website header features the INFN logo on the left and two navigation links: "Registra alias" and "Gestisci PEC", with a yellow arrow pointing to the latter. The main content area has a dark background with a server room image and the text "Servizio Mailing INFN" in large blue letters, followed by "Documentazione e configurazioni per l'utente della posta elettronica INFN". Below this, there are three service tiles: "Documentazione online" (with an information icon), "Configurazione dei servizi" (with a gear icon), and "Richiesta di supporto" (with a speech bubble icon). The footer contains a URL `https://infnpcc.infn.it/backpec/` and a partially visible sentence: "Trovi la documentazione relativa alle...".

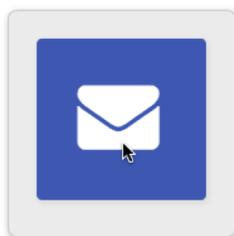
Richiesta caselle e documentazione

- Il contratto di acquisto di caselle PEC e' gestito centralmente
 - gli amministratori possono creare nuove caselle PEC sulla base di un credito disponibile presso il fornitore
 - si riducono drasticamente i tempi di creazione della casella
- La richiesta di caselle PEC va fatto attraverso il portale del mailing
 - la richiesta deve essere inoltrata necessariamente dal responsabile del servizio di direzione o dal responsabile del servizio di amministrazione
 - e' una procedura legata alla verifica (locale) dell'esigenza della casella

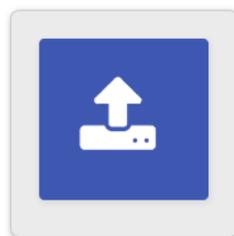
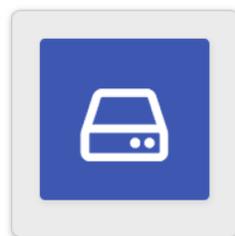
Esempio di richiesta di casella



Gestione PEC INFN



Richiedi una casella



Dati del titolare

<input type="text" value="Indirizzo PEC Richiesto (*)"/>	<input type="text" value="Nome"/>	<input type="text" value="Cognome"/>
<input type="text" value="Indirizzo"/>	<input type="text" value="Cap"/>	<input type="text" value="Provincia"/>
<input type="text" value="Comune"/>	<input type="text" value="Telefono"/>	<input type="text" value="Codice fiscale"/>
<input type="text" value="Indirizzo e-mail personale"/>		

[Avanti](#)

(*) Nella forma indirizzo@pec.infn.it

Immagine del documento di identità'

Carica un'immagine PDF o PNG

[Carica](#) ✓

Backpec: un backup della PEC

- Problemi:
 - cancellazioni involontarie di messaggi dalla casella PEC
 - necessita' di liberare spazio dalla casella PEC
 - il servizio acquistato non rende disponibile un servizio di backup/restore
 - nessuno sembra offrire questo tipo di servizio nel suo portfolio
- Sviluppata una soluzione interna per avere un backup dei messaggi della PEC
 - il backup viene fatto in modo da **preservare il formato del messaggio**, la sua firma digitale, e quindi la sua validita' legale
 - i messaggi salvati vengono resi disponibili in modalita' readonly attraverso un webmail

Accesso a backpec

- L'accesso al servizio e' possibile tramite il portale del mailing
 - scorciatoia: <https://backpec.infn.it>
 - l'accesso richiede autenticazione AAI (il sistema deve sapere chi avvisare)
 - l'esecuzione richiede l'inserimento delle credenziali della casella PEC da sottoporre a backup
- Dopo il backup viene inviato all'utente un report
 - importante: verificare che il backup abbia avuto successo
 - tutti i report dei backup eseguiti da un utente sono accessibili sul portale del mailing
- E' possibile liberare spazio dopo l'esecuzione del backup
 - ma solo messaggi ricevuti prima che l'ultimo backup iniziasse

(piccola demo)

Documentazione per la PEC

- E' disponibile su alfresco documentazione per
 - configurazione della casella PEC (filtri, avvisi, etc...)
 - configurazione dei client per l'accesso alla casella
 - best practices per la gestione dello spazio della casella
- Link disponibile attraverso il portale del mailing
 - scorciatoia: [link](#)

Coming soon

- Mirror on demand
 - backup che sia una fotografia dello stato della casella, che includa la struttura dei folder
- Backup automatizzato regolare (settimanale)
 - fare sempre attenzione ai messaggi che si possono rimuovere