



Onion Mail

É UN HIDDEN SERVER DI POSTA



Onion Mail

PUOI COMUNICARE ANCHE CON LE MAIL DI INTERNET

SMTP + POP3 + PGP + TOR



Onion Mail

AES256 _{xN} Volte + RSA2048 _{x2} Volte + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR



Onion Mail

AES256 $\times N$ Volte + RSA2048 $\times 2$ Volte + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR



Onion Mail

AES256 _{xN} Volte + RSA2048 _{x2} Volte + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR



server@louhlbgypgktsw7.onion

Si possono mandare messaggi crittati con PGP al server per eseguire le varie operazioni ed attivare le funzionalità estese.

Onion Mail

AES256 _{xN Volte} + RSA2048 _{x2 Volte} + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR

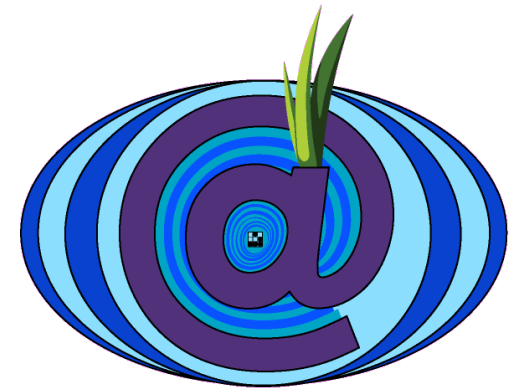
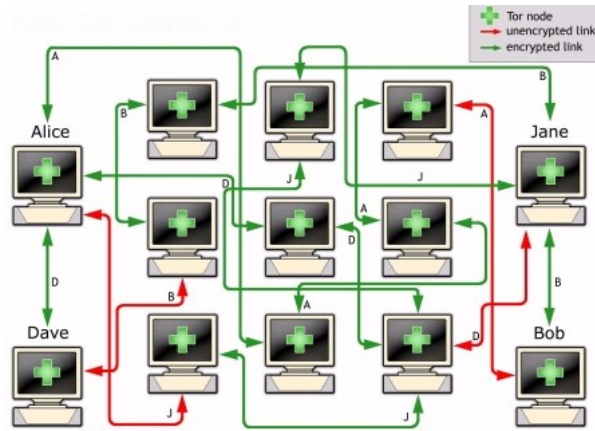
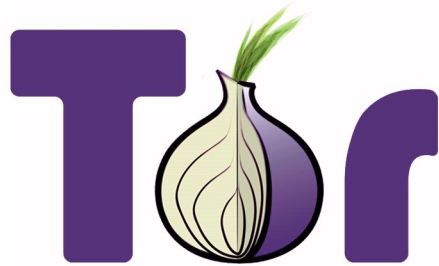


server@louhlbgypgktsw7.onion

Si possono mandare messaggi crittati con PGP al server per eseguire le varie operazioni ed attivare le funzionalità estese.

Onion Mail

AES256 _{xN Volte} + RSA2048 _{x2 Volte} + SSL + HASH + Chiavi remote F(X)



Onion Mail

É un hidden service.

louhlbgypgktsw7.onion

SMTP + POP3 + PGP + TOR

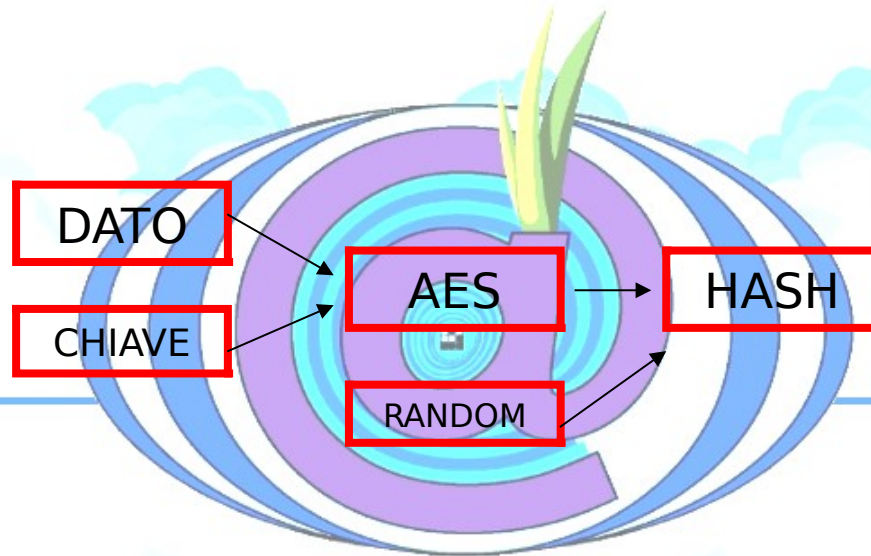


Onion Mail

AES256 _{xN Volte} + RSA2048 _{x2 Volte} + **SSL** + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR

Anche con le chiavi indietro non si torna.



Onion Mail

AES256 $\times N$ Volte + RSA2048 $\times 2$ Volte + SSL + HASH + Chiavi remote F(X)

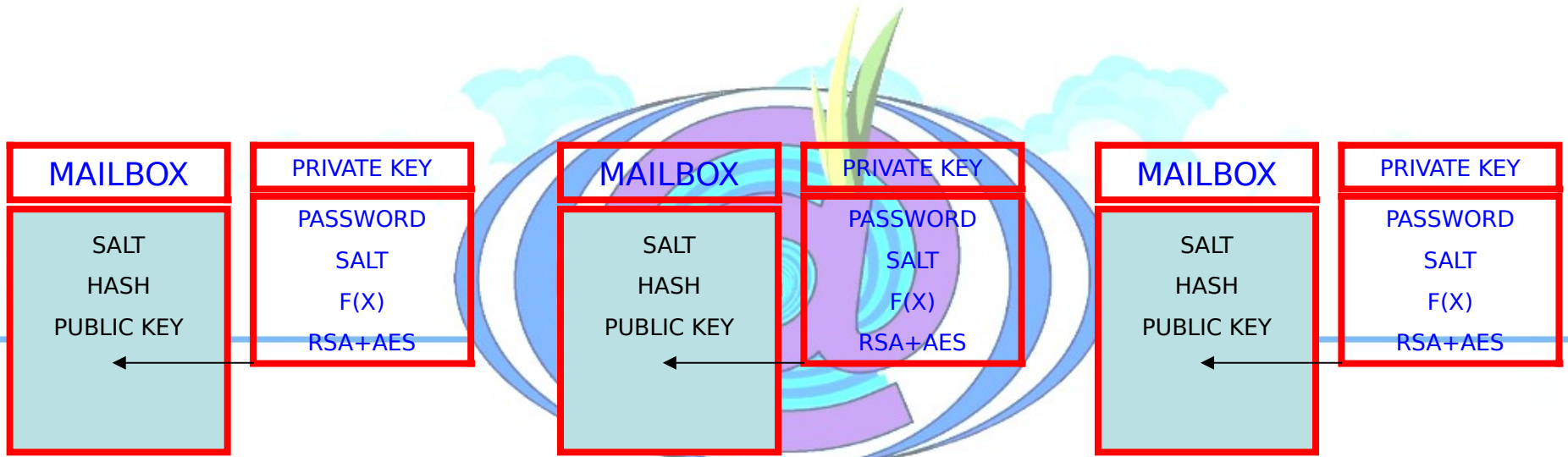
SMTP + POP3 + PGP + TOR



Onion Mail

AES256 xN Volte + RSA2048 x2 Volte + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR



Onion Mail

AES256 xN Volte - RSA2048 x2 Volte - SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR



Onion Mail

AES256 _{xN} Volte + RSA2048 _{x2} Volte + SSL + HASH + Chiavi remote F(X)

Server federati + Verifiche reciproche



Onion Mail

Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

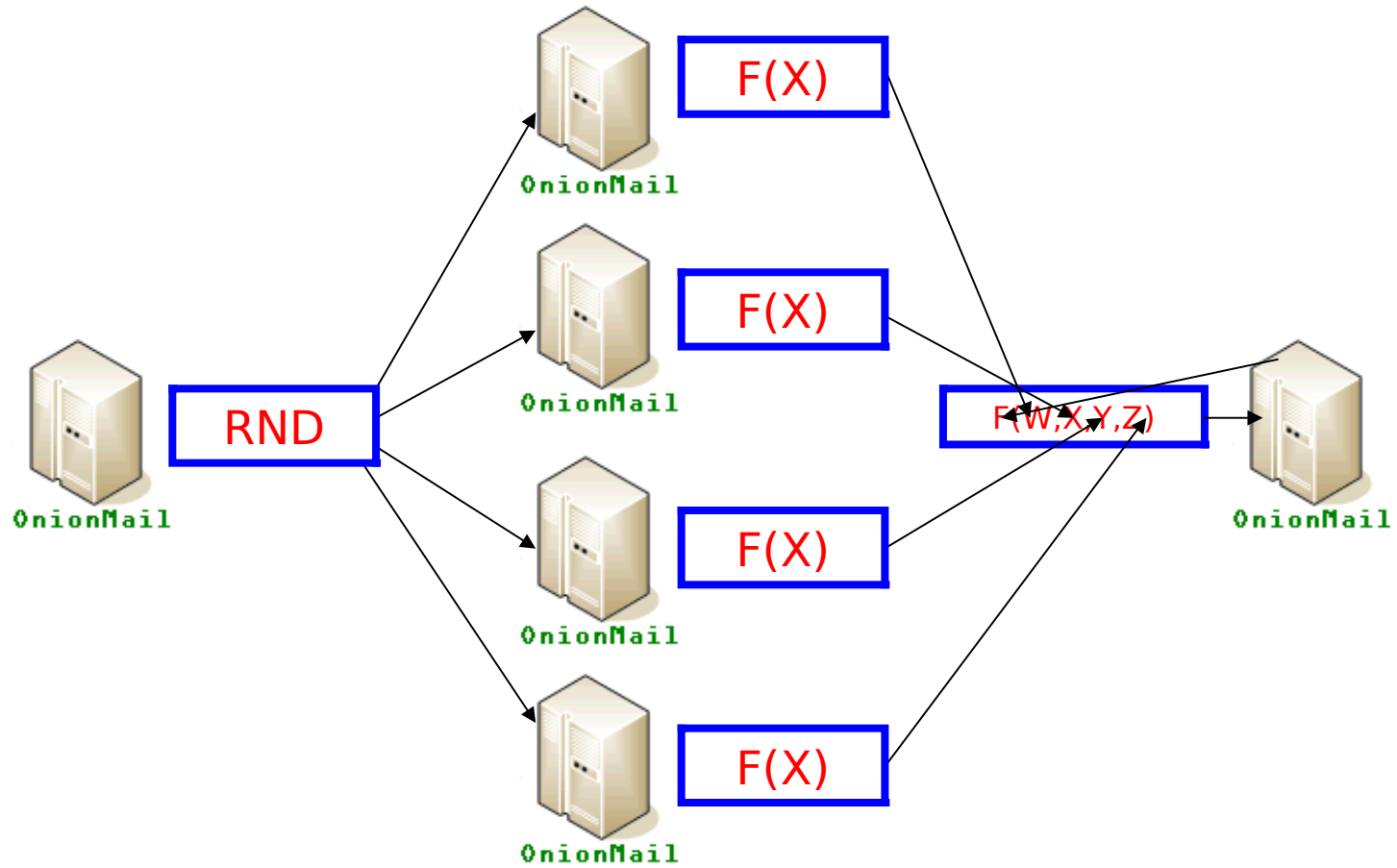
Server federati + Verifiche reciproche



Onion Mail

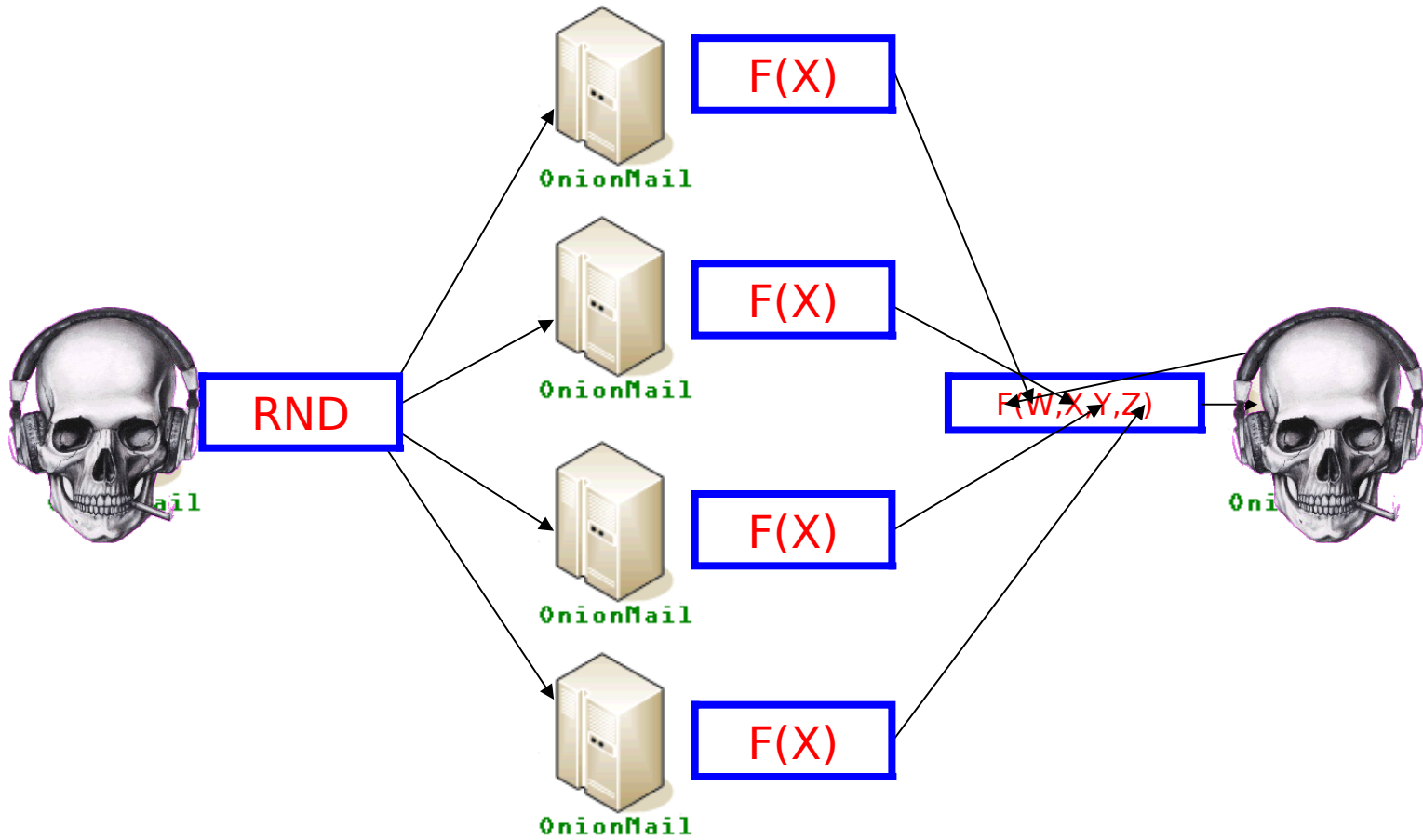
Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

SMTP + POP3 + PGP + TOR



AES256 xN Volte + RSA2048 x2 Volte + SSL + HASH + Chiavi remote F(X)

SMTP + POP3 + PGP + TOR

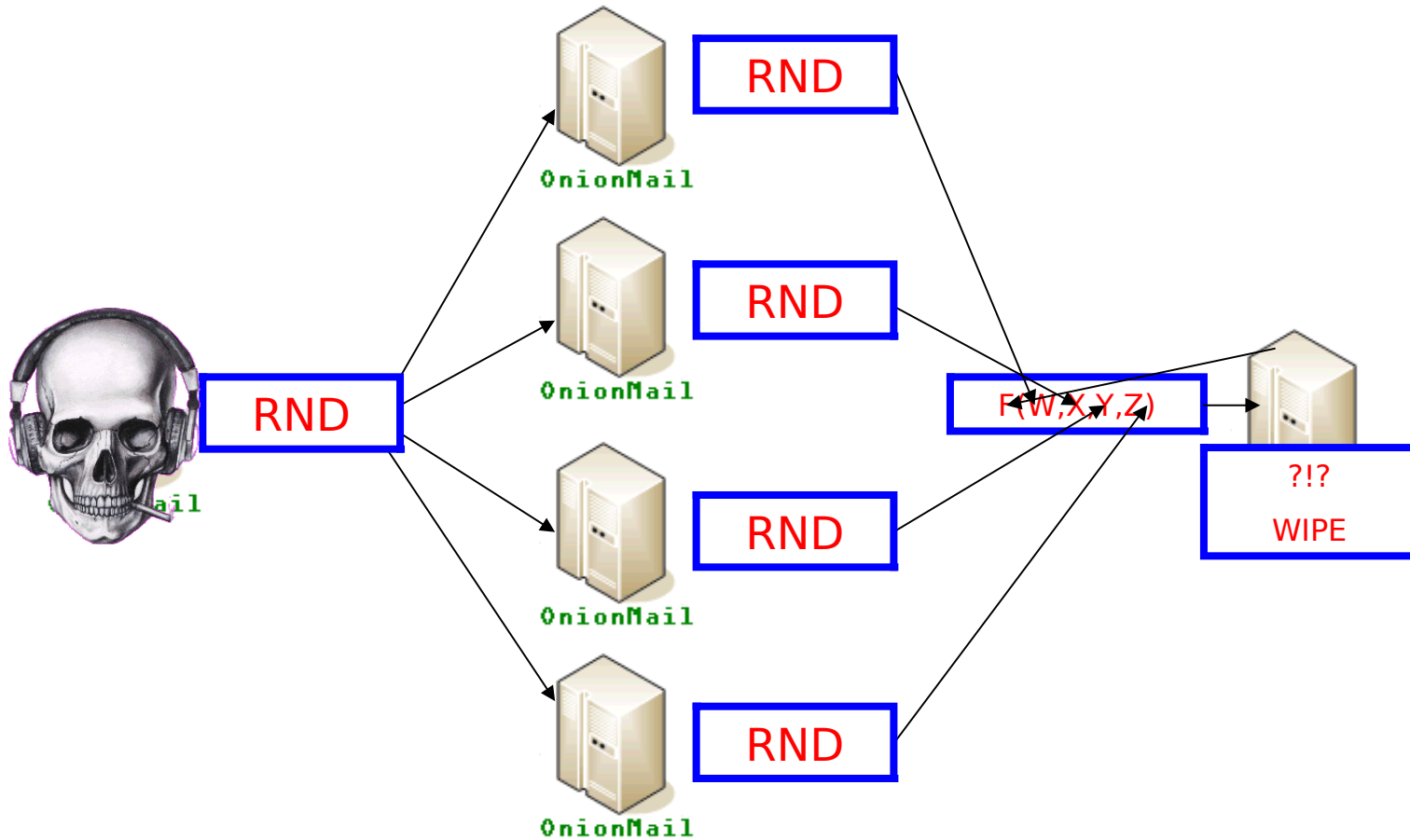


AES256 xN Volte + RSA2048 x2 Volte + SSL + HASH + Chiavi remote F(X)



AUTODISTRUZIONE

SMTP + POP3 + PGP + TOR



AES256 xN Volte + RSA2048 x2 Volte + SSL + HASH + Chiavi remote F(X)

CON LE CHIAVI

Il database degli utenti è inaccessibile .

Si possono leggere le blacklist del server senza associarle agli indirizzi.

Si possiedono i certificati SSL ma la RUN-String è diversa.

Si possono creare nuovi messaggi senza sapere se inviarli a qualcuno oppure no.

Non si possono leggere i messaggi.

I metadati sono inaccessibili.

Si può leggere la lista degli indirizzi contenuti nelle mailing list senza associarli alle mailing list stesse (dopo un attacco bruteforce).

Si accede ai log che hanno solo dati sul funzionamento del server e non sugli utenti.



Onion Mail

Server federati + Verifiche reciproche



Onion Mail

Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

Server federati + Verifiche reciproche



Onion Mail

Alias + Exit/Enter + **Anti Spam** + Wipe + Mailing List + Internet

Server federati + Verifiche reciproche



Onion Mail

Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

Server federati + Verifiche reciproche



sysop.list@louh1bgyupgktsw7.onion

Onion Mail

Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

Server federati + Verifiche reciproche



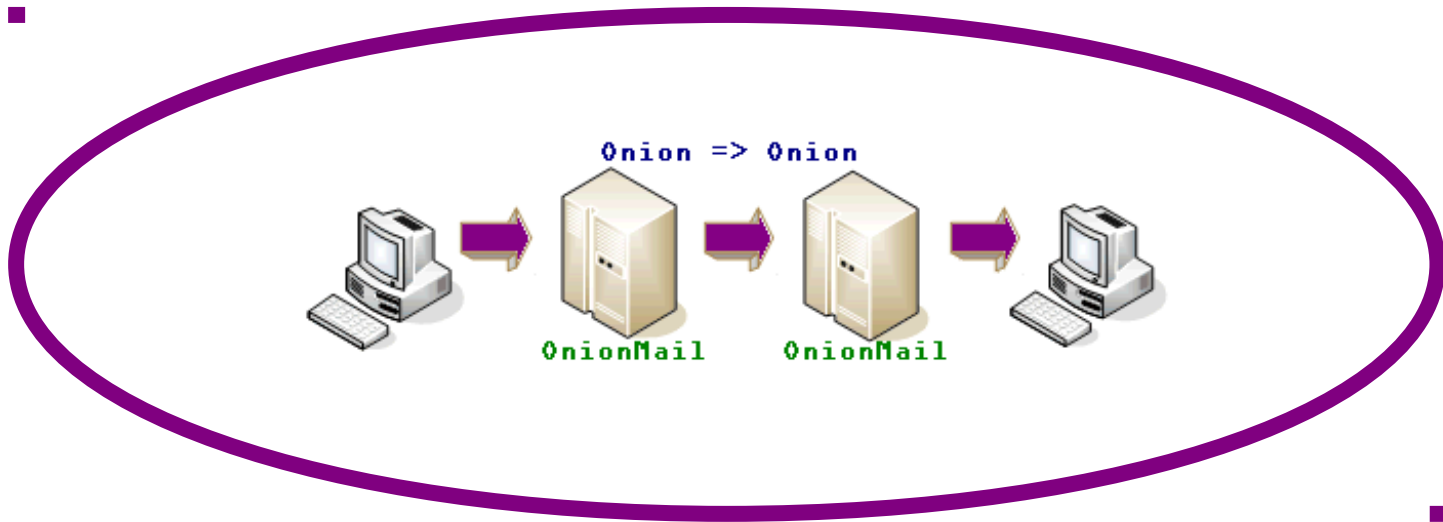
sysop.list@louhlbgypgktsw7.onion

Onion Mail

Alias + Exit/Enter + Anti Spam + Wipe + Mailing List + Internet

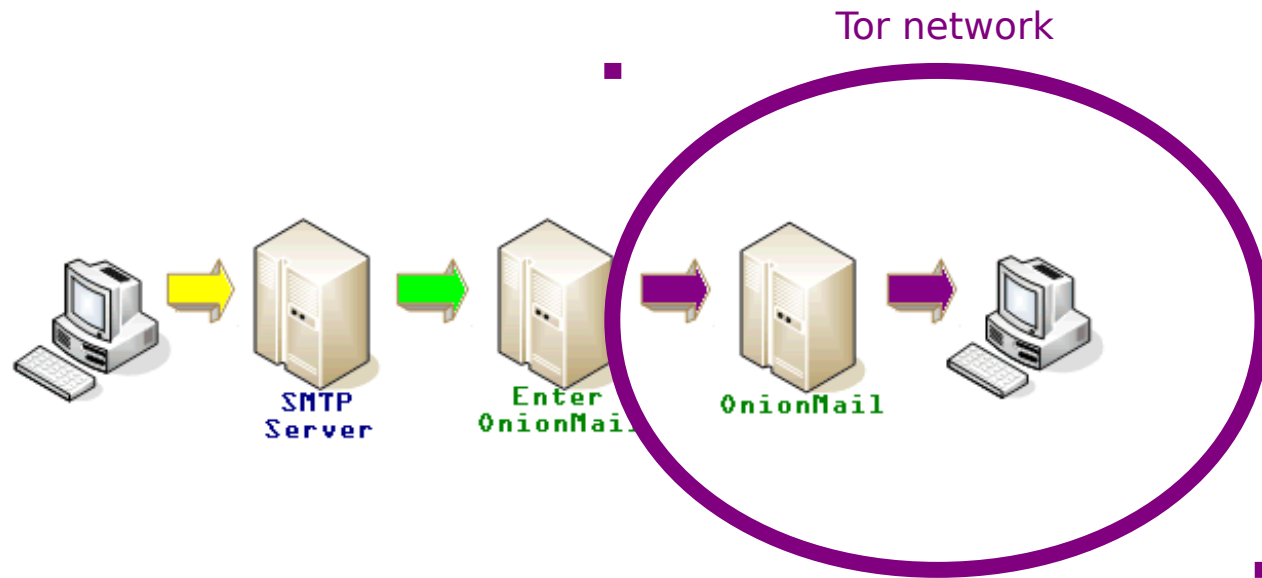
ONION => ONION

Tor network



alice@louhlbgypgktsw7.onion => bob@5b2edtzvosbfdztn.onion

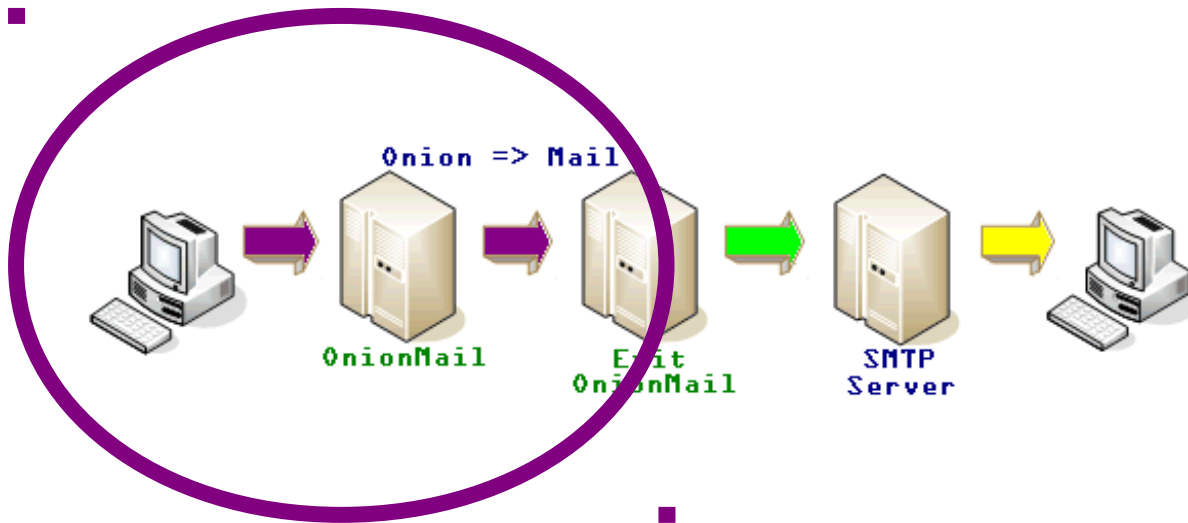
INTERNET => ONION



alice@example.org => bob.5b2edtzvosbfdztn.onion@onionmail.info

INTERNET => ONION

Tor network



`bob.5b2edtzvosbfdztn.onion@onionmail.info => alice@example.org`

PROTOCOLLO M.A.T.



Onion Mail

bob@5b2edtzvosbfdztn.onion uscendo da onionmail.info

diventa **bob**.5b2edtzvosbfdztn.onion@onionmail.info

PROTOCOLLO M.A.T.



Onion Mail

Diventa **bob.5b2edtzvosbfdztn.onion@onionmail.info** ?

PROTOCOLLO M.A.T.



Onion Mail

CHE BRUTTO!!!!

Diventa bob.5b2edtzvosbfdztn.onion@onionmail.info ?

UTILIZZA ANCHE INDIRIZZI “POTABILI”

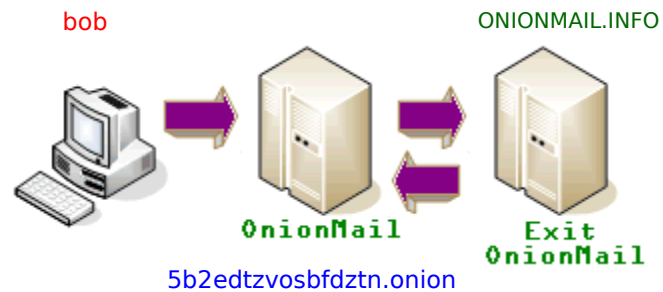


Onion Mail

PROTOCOLLO M.A.T. vs V.M.A.T.

PROTOCOLLO V.M.A.T.

Iscrizione indirizzo VMAT presso un nodo di uscita.



Messaggio VMAT al server

PROTOCOLLO V.M.A.T.

Iscrizione indirizzo VMAT presso un nodo di uscita.



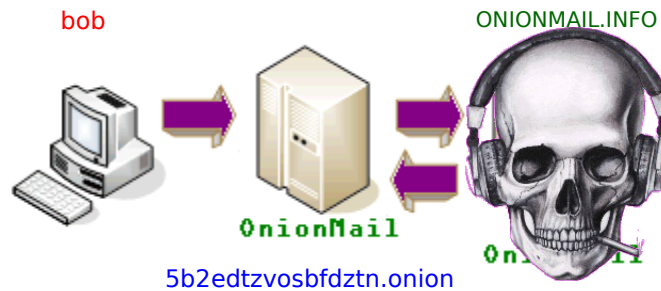
Diventa **bob@onionmail.info**

Può anche iscriversi come **tizio@onionmail.info**

Si possono usare i nuovi indirizzi al pari di quelli MAT oppure ONION.

PROTOCOLLO V.M.A.T.

Iscrizione indirizzo VMAT presso un nodo di uscita.

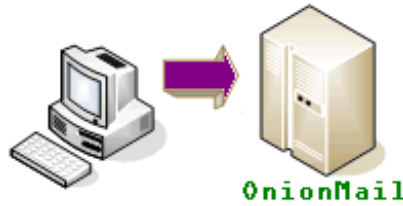


Diventa **bob@onionmail.info**

Può anche iscriversi come **tizio@onionmail.info**

Non si scandalizza e funziona ancora.

CARO SERVER TI SCRIVO



`server@louhlgypgktsw7.onion`

RULEZ	Risponde con la guida.
IDENT	Da le informazioni sul server.
VMAT	Iscrive gli indirizzi VMAT.
MYKEY	Imposta la chiave pubblica.
PGP	Esegue le funzioni con PGP.
SPAM	Modifica i filtri anti spam personali.
EXIT	Sceglie il nodo di uscita.
LIST	Gestisce le mailing list.
REBOUND	Rimbalza il messaggio.
NEWUSER	Crea un utente.

É UN HIDDEN SERVER DI POSTA



Onion Mail

É orientato alla privacy degli utenti, il gestore potrebbe non sapere quali utenti ci sono e non può in alcun modo leggere i messaggi.

LIMITAZIONI



Onion Mail

- Solo un destinatario per messaggio
- Non ci sono le DSN
- I messaggi rimangono sul server N giorni e poi sono eliminati.

POTENZIALITÀ



Onion Mail

- Non supporta alcun sistema di intercettazione.
- I messaggi sono salvati solo sul server del destinatario.
- Si possono aprire più server indipendenti con un solo processo di OnionMail attivo.

<http://onionmail.info>

<http://louhlbgypgktsw7.onion>



Onion Mail

***«In futuro forse implementeremo il caffè anonimo!
Oggi, solo [OnionMail](#) ;) »***

<http://onionmail.info/reqmail>

<http://louhlbgypgktsw7.onion/reqmail>