

Sistema distribuito per l'invio sicuro di file su rete locale



Relatori:

Angelo Raffaele Meo
Federico Di Gregorio
Pierluigi Di Nunzio

Candidati:

Emanuele Aina
Marco Barisione

Scambio di file

- La connettività è disponibile ovunque
 - Eventualmente con reti ad-hoc o meshed
 - L'accesso a Internet non è però sempre disponibile
- Spesso gli utenti desiderano scambiarsi un documento
 - Se ci si trova vicini è meglio usare la rete locale
- È più complicato di quello che dovrebbe essere
- Quindi si usano mezzi non pensati per questo scopo
- Oppure non si sfrutta la connessione di rete



Strumenti attualmente disponibili

- Cartelle condivise (FTP, Samba/condizione di Windows, WebDAV)
 - ⚠ Necessaria configurazione
 - ⚠ Eccessivo per lo scambio di singoli file
 - ⚠ Di conseguenza si usa una singola cartella pubblica
- Invio di file (e-mail, messaggistica istantanea)
 - ⚠ Necessario un server centrale
- Supporti esterni di memorizzazione (CD, penne USB)
 - ⚠ Capacità fissa
 - ⚠ Richiede lo scambio fisico del supporto



Obiettivi

- Invio di file invece che cartelle condivise
- Il destinatario deve essere una persona, non un indirizzo IP
- Se in rete locale lo scambio deve essere diretto
- Ricerca automatica dei possibili destinatari
- Integrato nell'ambiente grafico
- Basato su software libero per la piattaforma GNOME
- Ampia diffusione
 - Acquista valore all'aumentare della base utenti
- Sicuro



Funzionamento

Marco



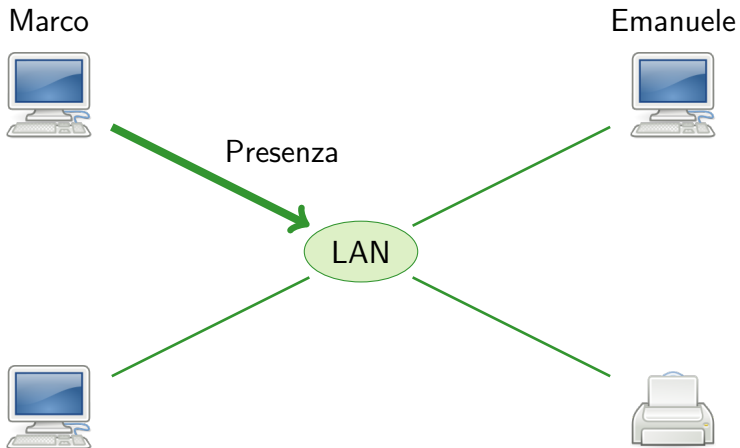
Emanuele



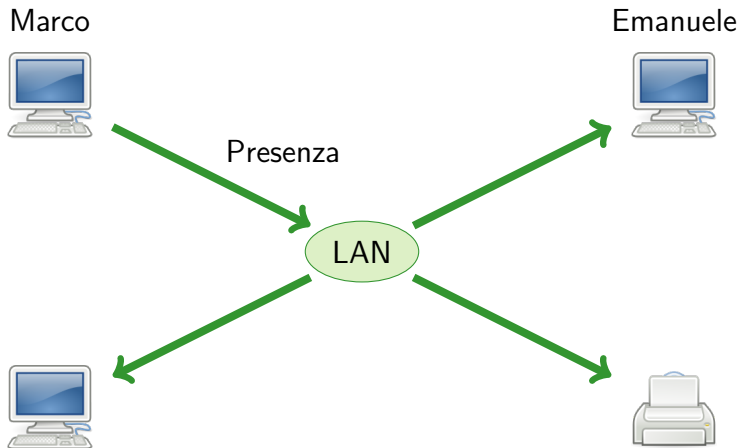
LAN



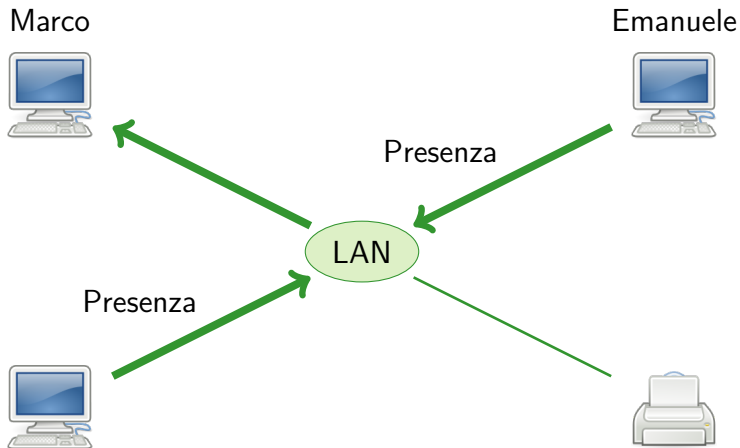
Funzionamento



Funzionamento



Funzionamento



Funzionamento

Marco



Emanuele



LAN



Funzionamento

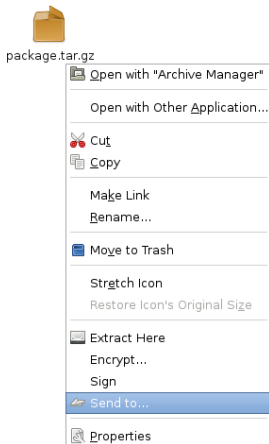


package.tar.gz

Emanuele



Funzionamento

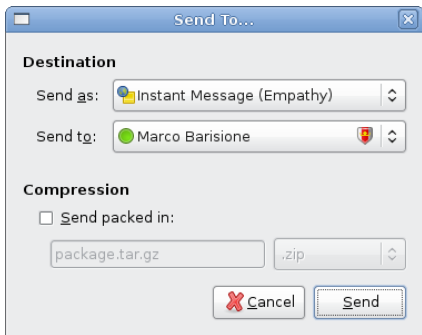


Emanuele



Funzionamento

Emanuele



Funzionamento

Marco



Emanuele



TLS

LAN



Funzionamento

Marco



Emanuele



LAN



Sicurezza

- Necessario garantire riservatezza e autenticazione
- Informare costantemente l'utente del grado di sicurezza
- Indipendenza da autorità centrali
 - Utente stesso assegna la fiducia
 - Credenziali generate automaticamente
- Tre livelli di fiducia
 - Non sicuro
 - Non fidato
 - Fidato

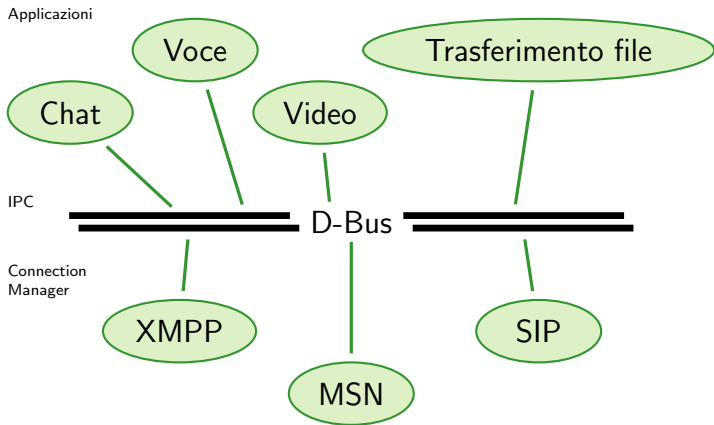


Messaggistica istantanea

- Soddisfa il maggior numero di requisiti
 - Il contatto corrisponde direttamente all'utente
 - Può supportare funzionalità di sicurezza
 - Servizi aggiuntivi (chat, voce, video)
 - Interoperabile
- Ma è necessario superare alcune limitazioni
 - Server esterno → link-local XMPP
 - Inserimento manuale contatti → ZeroConf
 - Integrazione con il desktop → Telepathy



L'architettura di Telepathy



Utilizzatori di Telepathy



MIT One Laptop Per Child
chat, video, giochi, editing
collaborativo

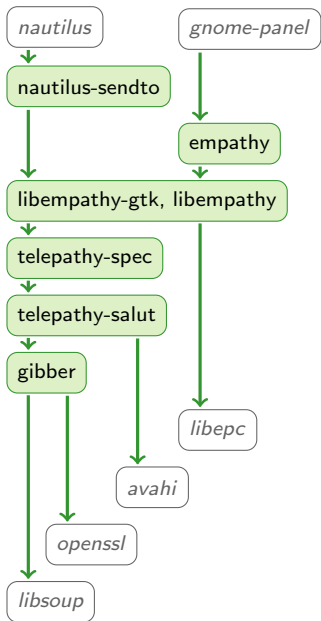
Nokia Internet Tablet
chat e video



Lo stack del progetto

- Telepathy è altamente modulare
- Le modifiche hanno riguardato tutto lo stack
- Correzioni a bug apportate anche in componenti esterni





ambiente desktop

invio file integrato nel file manager

chat e invio file

widget e classi per chat e invio file

definizione interfaccia IPC su D-Bus

connection manager per XMPP link local

libreria XMPP

generazione di chiavi auto firmate

librerie e servizi per mDNS/DNS-SD

libreria crittografica

libreria HTTP

Esempio di invio di un file

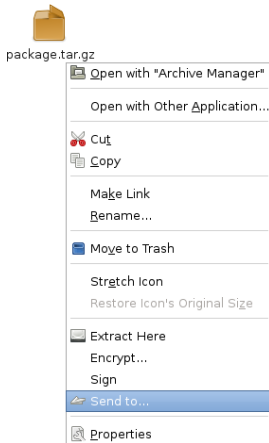
nautilus-sendto



package.tar.gz

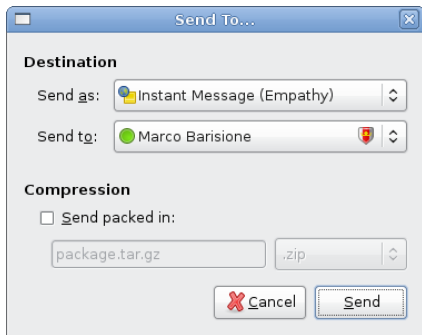
Esempio di invio di un file

nautilus-sendto

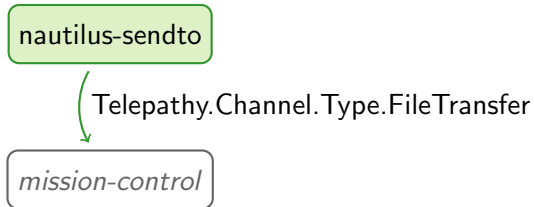


Esempio di invio di un file

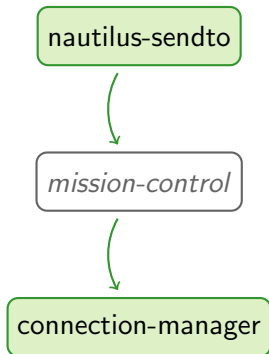
nautilus-sendto



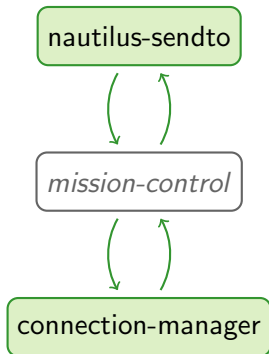
Esempio di invio di un file



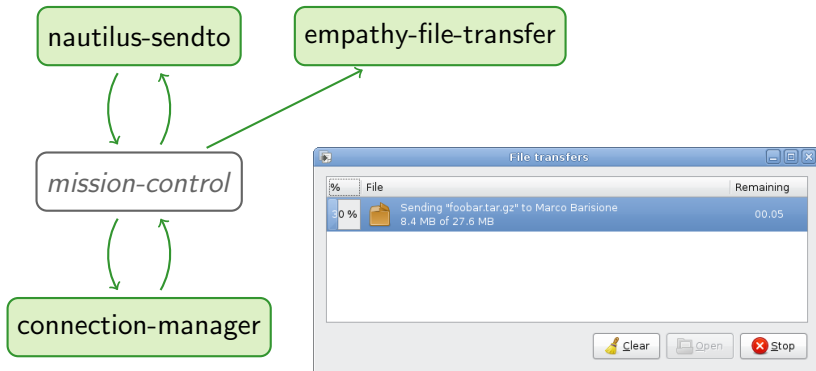
Esempio di invio di un file



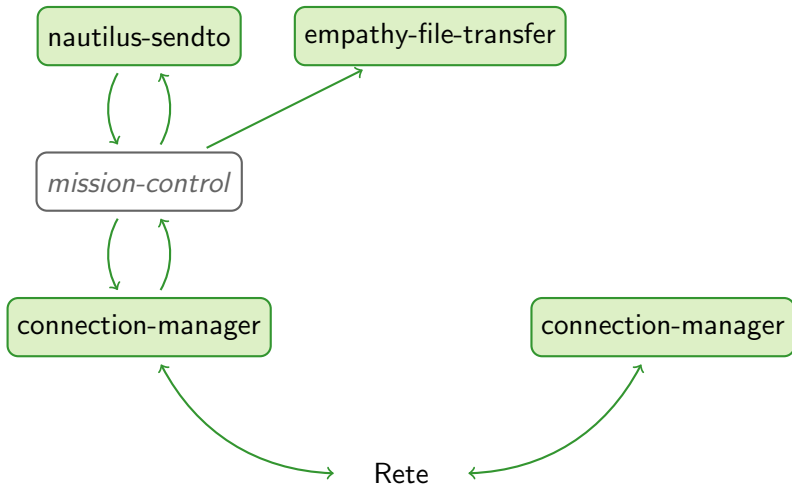
Esempio di invio di un file



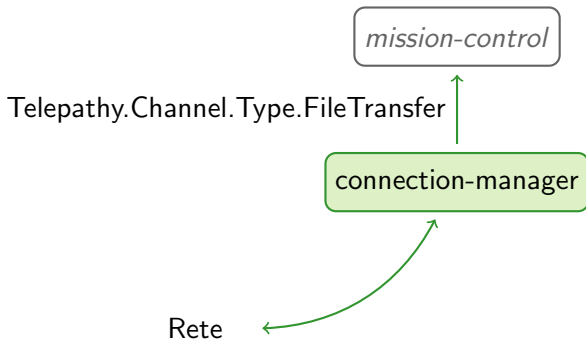
Esempio di invio di un file



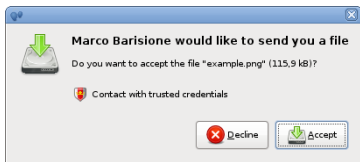
Esempio di invio di un file



Esempio di invio di un file



Esempio di invio di un file



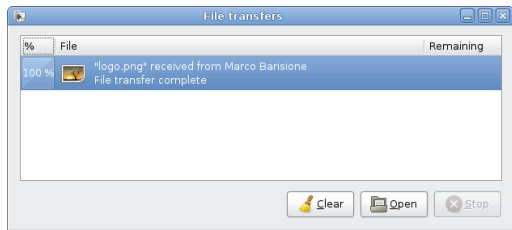
empathy-file-transfer

mission-control

connection-manager

Rete

Esempio di invio di un file



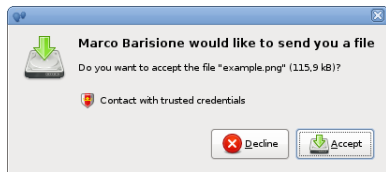
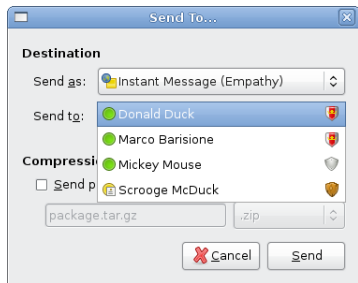
empathy-file-transfer

mission-control

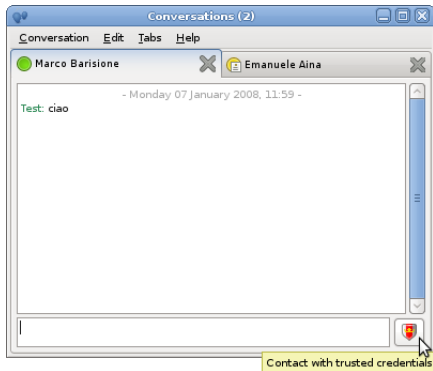
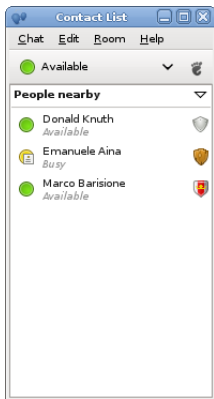
connection-manager

Rete

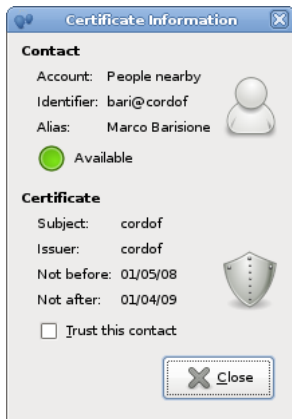
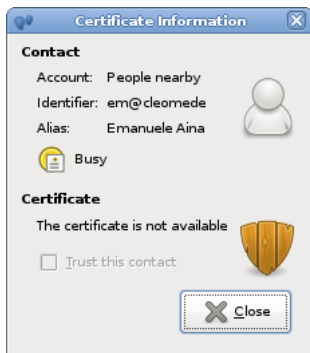
Interfaccia grafica per la sicurezza



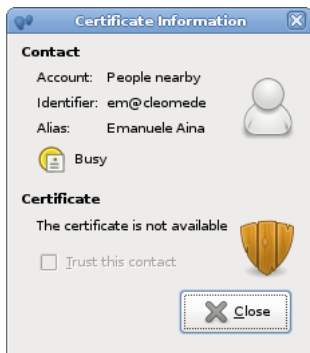
Interfaccia grafica per la sicurezza



Interfaccia grafica per la sicurezza



Interfaccia grafica per la sicurezza



Tecnologie per la sicurezza

- Autenticazione con certificati X.509
- Transport Layer Security (RFC-2246)
 - Scambio dei certificati
 - Protezione delle comunicazioni
- Generazione automatica delle chiavi private
- Certificati auto-firmati
 - Resta possibile ricorrere a una certification authority
- Informazioni di presenza firmate



Tecnologie per segnalazione e trasferimento file

- eXtensible Messaging and Presence Protocol (XMPP/Jabber)
 - Messaggistica e presenza (RFC-3920 e RFC-3921)
 - Basato su XML
 - Modello client-server
- Link-local XMPP per messaggistica senza server (XEP-0174)
 - Segnalazione della presenza in rete locale (ZeroConf)
 - DNS su multicast/anycast senza server (mDNS)
 - Pubblicazione e ricerca di servizi tramite DNS (DNS-SD)



Tecnologie per segnalazione e trasferimento file

- Diversi meccanismi (XEP-0096)
- Out of Banda Data (XEP-0066)
 - Negoziazione su XMPP
 - Trasferimento reale su canale esterno
 - HTTP o HTTPS (RFC-2616 e RFC-2818)
 - Il più efficiente in rete locale
 - Unico supportato da Apple iChat



