Messaggi crittografati per trasmissioni riservate

e-privacy XXXVII

23 e 24 ottobre 2025
sala conferenze dell'Infopoint
piazza della Stazione, 4 Firenze

Messaggi crittografati per trasmissioni riservate

Prospettive innovative e soluzioni pratiche

L’analisi preliminare condotta ci ha permesso di individuare una serie di vincoli da rispettare che, se attuati correttamente, permettono di azzerare il rischio di intercettazione e decriptazione de dati trasmessi.

E’ stata ridotta al minimo la superfice esposta a potenziali attacchi: Nessun Server Centrale.

Client mai esposti in rete: azzerato il rischo di intrusione da connessione remota.

Boot loader e successivo software precaricato con solamente il minimo necessario allo scopo del dispositivo: Azzeramento di potenziali backdoor di sistema

Operazioni critiche svolte esclusivamente dal client non esposto in rete: Connessione seriale o wi-fi con certificati: nessun login interattivo abilitato.

Server preconfigurato con relazione 1 a 1 con il proprio client. NON è in grado di decriptare il messaggio ma può solo trasmettere o ricevere l’informazione criptata.

Messaggi crittografati per trasmissioni riservate

Pubblico di destinazione

Sono potenzialmente interessati alla nostra soluzione tutti quei soggetti (organizzazioni, banche, enti, privati cittadini) che necessitano della assoluta certezza che ciò che trasmettono sia leggibile solo e unicamente dai destinatari ai quali le informazioni vengono inviate.

Principi di base fondamentali

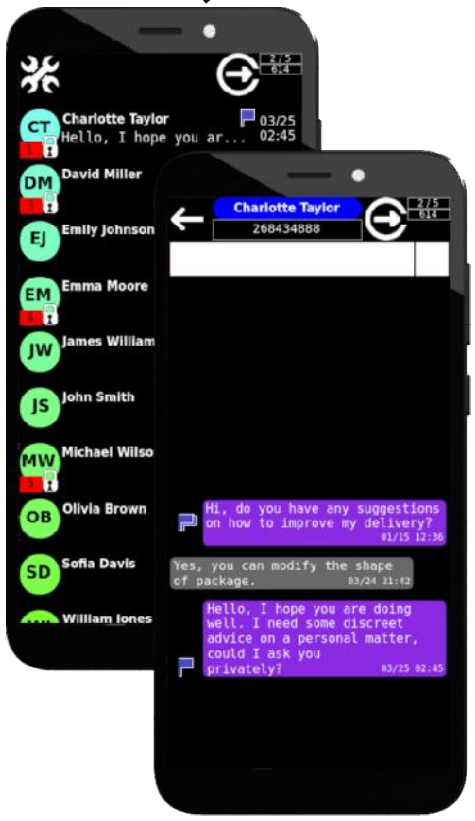
- Chiavi di criptazione simmetriche univoche e non riutilizzabili **OTP** (**O**ne **T**ime **P**assword).
- **Proprietà completa di hardware e software:** nessun dispositivo intermedio di terze parti
- Il sistema opera nella sola memoria RAM: **nessun dato viene memorizzato permanentemente.**

Messaggi crittografati per trasmissioni riservate

Due Proposte per un’unica soluzione

Postazione Fissa (PC Notebook+Server)
con connessione di rete tramite cavo.
Client **E-mail** dedicato.

Postazione Mobile (SmartPhone)
con connessione tramite rete GSM.
Chat **SMS** dedicata.



Messaggi crittografati per trasmissioni riservate

Postazione Fissa

I NODI

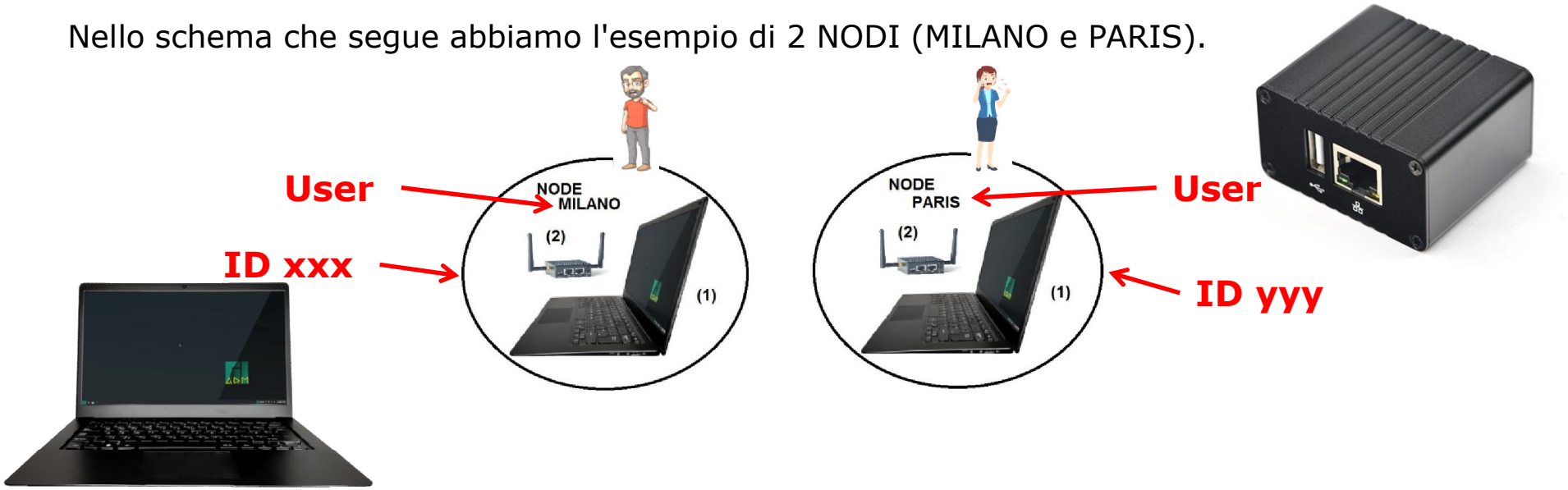
Il **NODO** è l'insieme di Hardware e Software utilizzato dal singolo **UTENTE**.

Ogni **NODO** ha un nome che lo identifica univocamente all'interno del gruppo.

Il NODO è composto da 2 unità fisiche distinte:

(1) **Client**
(2) **Server**

Nello schema che segue abbiamo l'esempio di 2 NODI (MILANO e PARIS).



Messaggi crittografati per trasmissioni riservate

Postazione Fissa

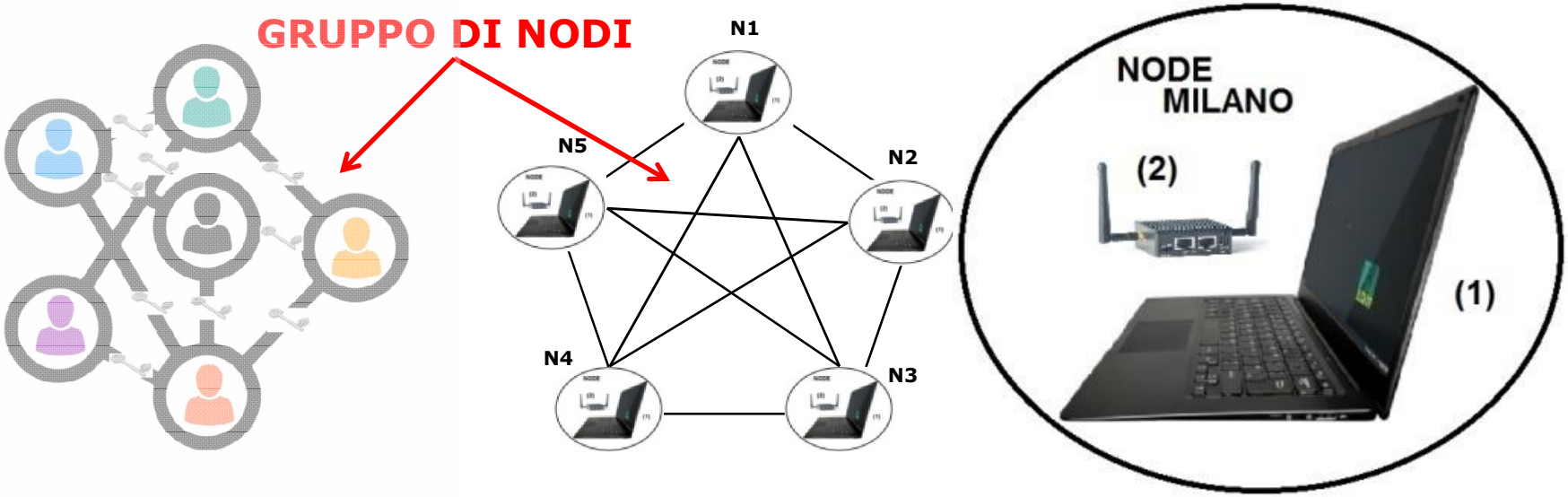
IL GRUPPO

Il **GRUPPO** è un insieme di **NODI** configurati per comunicare solo tra loro.

Il gruppo viene definito inizialmente secondo esigenze cliente.

Il gruppo è composto da un minimo di 2 a un massimo di 250 **NODI.**

I **NODI** creano un network privato di comunicazione crittografata: nessun altro può accedere a tale network e i **NODI** stessi non possono uscirne.



Messaggi crittografati per trasmissioni riservate

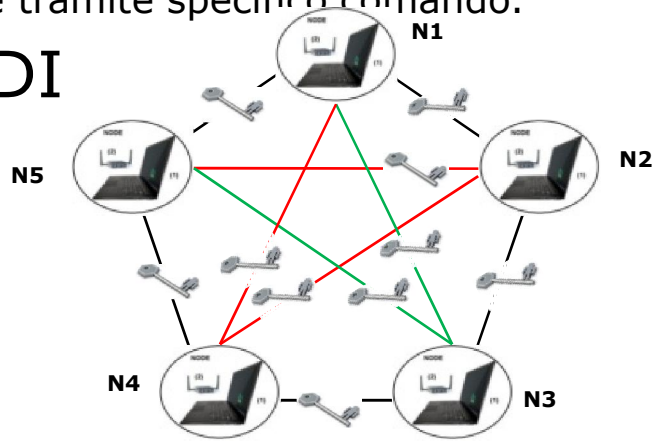
Postazione Fissa

Messaggi tra NODI

Il **NODO** conosce e comunica solo con i **NODI** facenti parte dello stesso **GRUPPO**.
Il **NODO** dopo la trasmissione del messaggio al **NODO** destinazione, rimuove automaticamente il messaggio: nulla resta sul **NODO** mittente *.
Il server del **NODO** si limita a trasmettere o ricevere messaggi criptati, ma non è in grado di decodificarli: tale compito é di esclusiva competenza del client.
Il **NODO** ha il messaggio **solo in memoria RAM**, non salva in nessun dispositivo locale *.
La Chiave è univoca per ogni coppia di **NODI** e per ogni verso della comunicazione.

* A meno che l'utente non forzi questa questa opzione tramite specifico comando.

Schema di esempio a 5 NODI

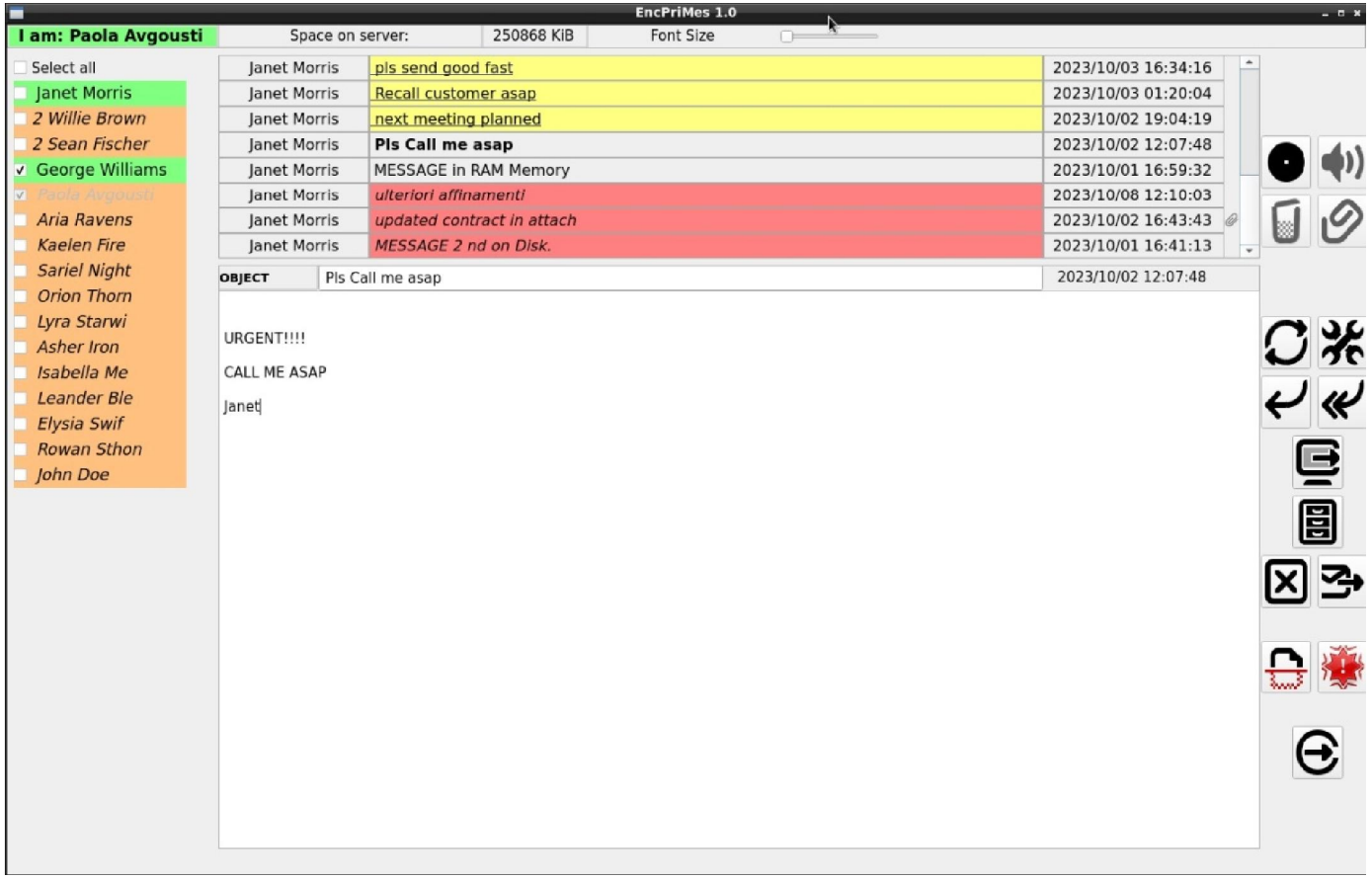


Messaggi crittografati per trasmissioni riservate

Postazione Fissa

TIPO DI MESSAGGIO

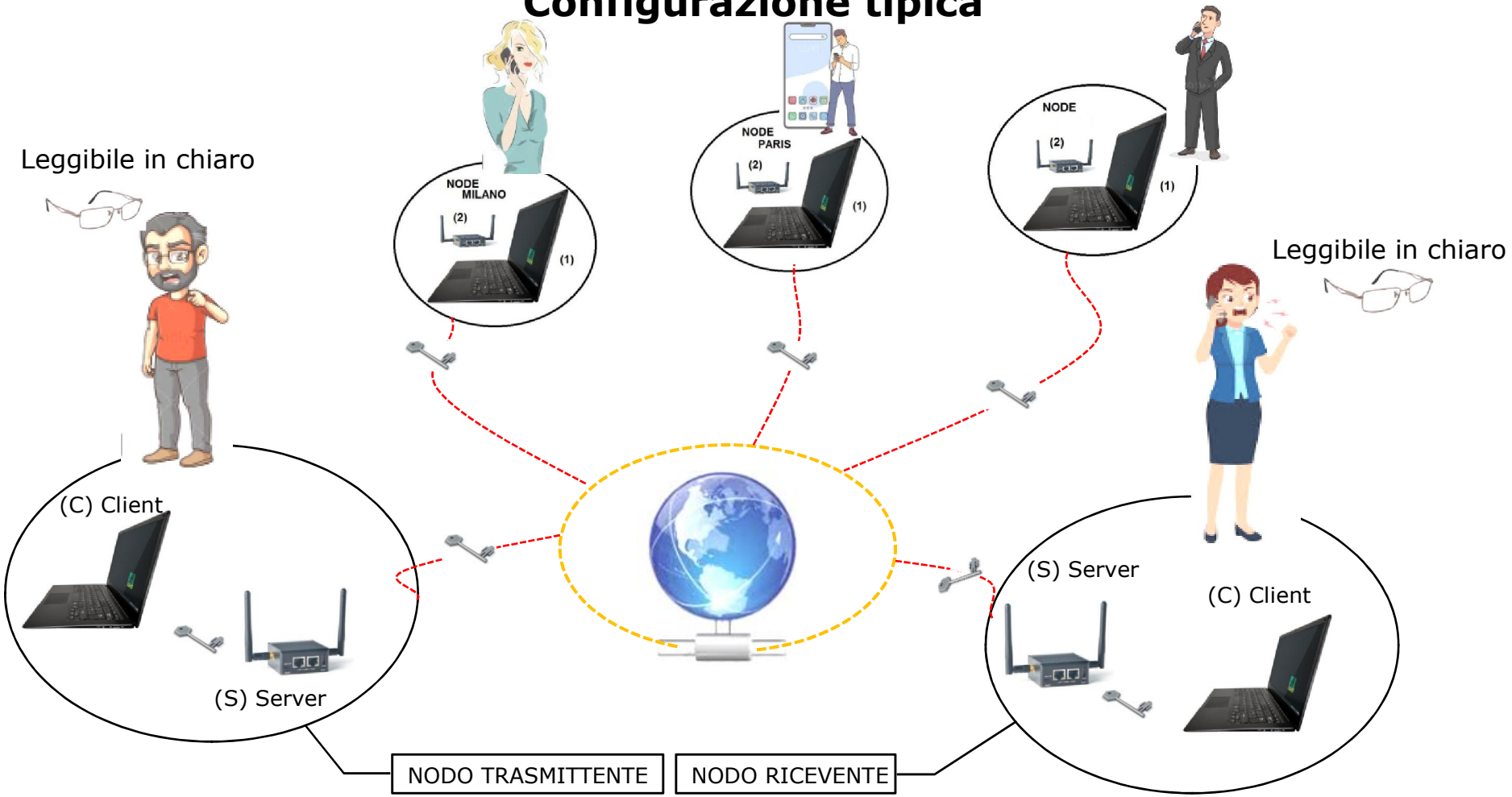
- **E-Mail** con Messaggio di testo ed eventuali **allegati (documeti, foto, audiovisivi)**



Messaggi crittografati per trasmissioni riservate

Postazione Fissa

Configurazione tipica



Messaggio leggibile in chiaro solo dal mittente e destinatario

Messaggi crittografati per trasmissioni riservate

Postazione Fissa

SINTESI

1) **UTENTE AUTONOMO!** Totale indipendenza da server di terze parti (ad esempio protonmail) che, essendo fuori dal controllo dell'utente finale, per definizione non è sicuro.
2) **SCIENTIFICA GARANZIA DI INDECIFRABILITÀ** del messaggio grazie al metodo crittografico utilizzato.
3) **IMPOSSIBILITÀ DI DECIFRAZIONE** anche da parte del fornitore, quindi totale sicurezza della privacy dell'utente. Non potremmo intervenire per decifrare il messaggio nemmeno se obbligati per legge, in quanto non disponiamo di copia delle chiavi.
4) **I NODI** fanno parte di un network privato di comunicazione crittografata, nessun altro può accedere al tale network e i nodi stessi non possono uscirne.
5) **IL CLIENT NON ACCEDE A INTERNET**, in questo modo non può essere vittima di attacchi remoti.

Messaggi crittografati per trasmissioni riservate

Postazione Mobile

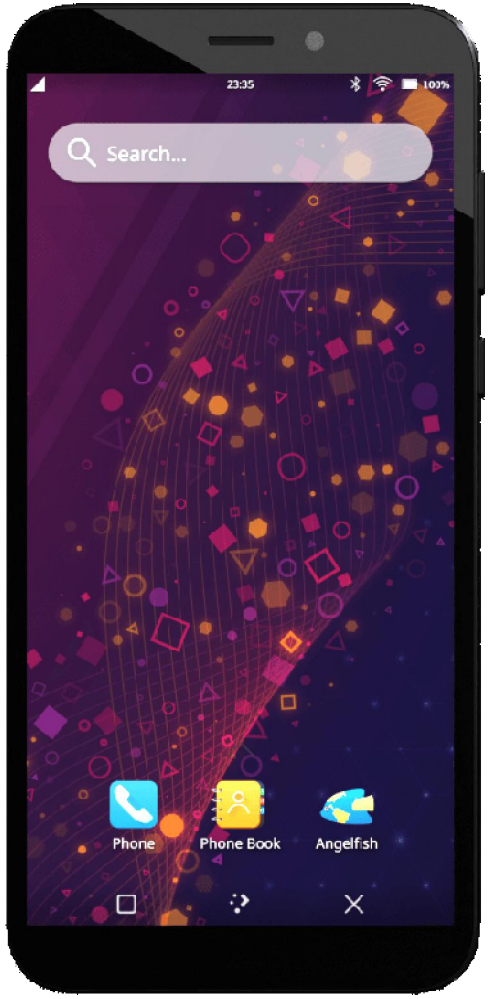
SmartPhone

Open Source Smartphone: **Linux Phone**

Dotato di **hardware privacy switches**

SMS Criptati localmente mediante chiavi **OTP** precaricate sul dispostivo

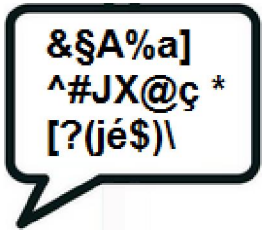
Anche in questa configurazione il numero dei telefoni abilitati alla trasmissione criptata è predefinita in fase di configurazione e **NON espandibile** successivamente.
E' possibile utilizzare sim telefoniche di qualunque provider purchè abilitate alla trasmissione di **SMS**.
Mediante interfaccia guidata è possibile associare la SIM al telefono criptato predefinto.
Gruppo Min **2** Max **250** partecipanti.



Messaggi crittografati per trasmissioni riservate

Postazione Mobile

Caratteristiche



Messaggi scambiati in modalità **E2EE** (**E**nd **2** **E**nd **E**ncription).

Chiave **OTP** disponibile per ogni coppia di telefoni del gruppo e per ogni flusso (andata/ritorno).

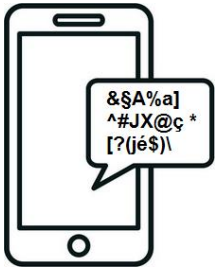
Chiave **OTP** a **lunghezza variabile** pari alla lunghezza del messaggio trasmesso/ricevuto.

Gestione dei **messaggi solo in memoria** RAM, mai salvati su disco (effimeri).

E’ possibile gestire messaggi NON crittografati con persone esterne al gruppo.

Limite di utilizzo da minimo **6 mesi** a **3 anni** su richiesta in fase di fornitura.

Notifica di avvenuta ricezione sempre attiva.



Grazie per l'attenzione

Riferimenti e CONTATTO

PRODEV SRL
Via Cavour, 88
20030 SENAGO MI Italy
Mobile +39 348 2720240
m.gherbin@gmail.com
Massimo Gherbin