TRUSTICA

Trustica Mobile - Military Grade Mobile Device Communications with Consumer Simplicity
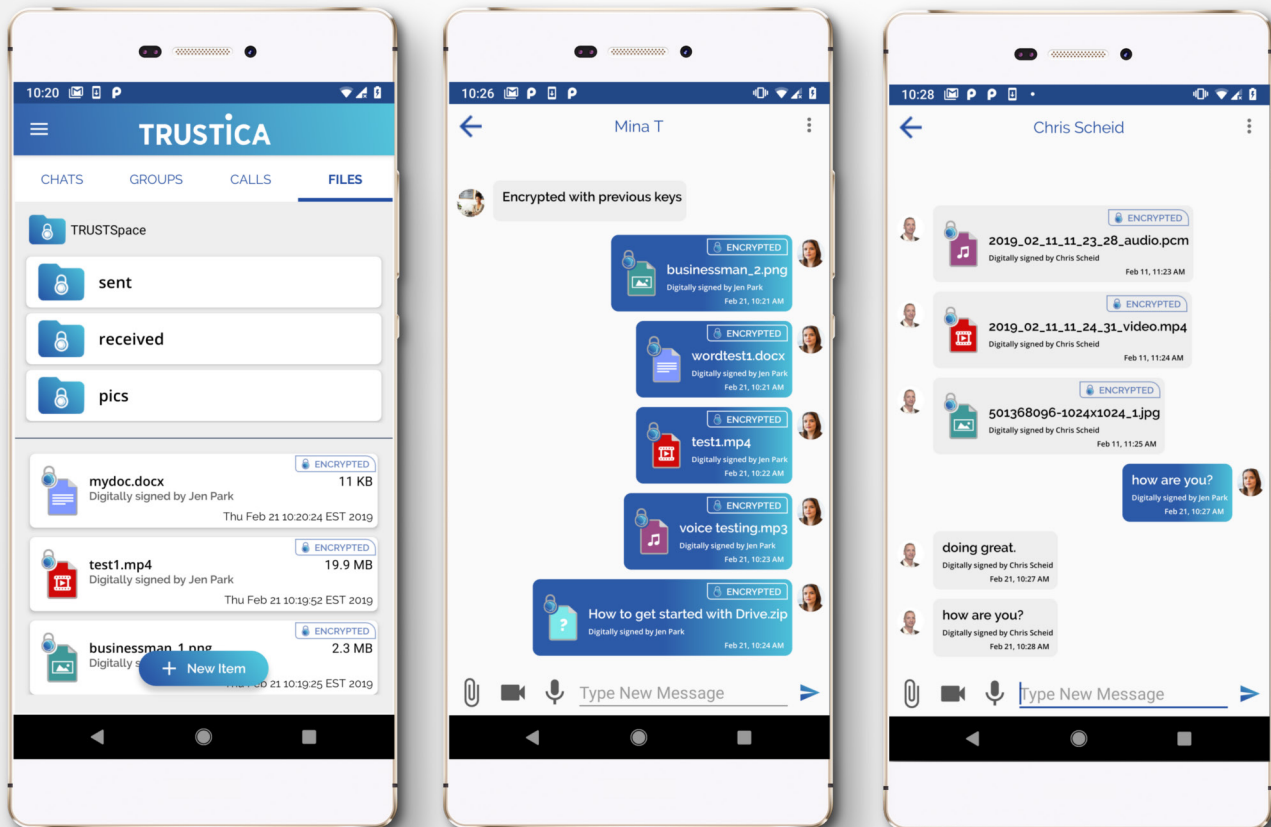
Employee-owned mobile devices are untrustworthy to an enterprise. Yet, they are commonly used for storing sensitive information and communications. Assuming administrative control over devices with questionable cyber hygiene, improper configurations are burdensome for the enterprise and intrusive to employees.

With Trustica installed, enterprises can enforce a secure environment for communication and information storage without compromising employee privacy.

With Trustica Mobile (TM), enterprise personnel can securely:

- Make Encrypted Voice Calls
- Send Encrypted Text Messages (one to one or group texts)
- Transfer and Store Encrypted Files

Available for Android & iOS

TRUSTICA

See How We Mitigate The Risks Expressed by Enterprise CISOs

Risk	Mitigation
Confidentiality attack on data in motion	Encrypted; key changes for each message, file transfer, voice/video session; end-to-end device and user authentication; keys secured in hardware KeyStore
Manipulation of data in motion	Digital signature validations for all data exchanges; keys secured in hardware KeyStore
Data exposure or loss due to malware or malicious app	Files are crypto-isolated in a secure application space; message and file data store in cloud; device integrity checks and harmful apps warnings
Data loss due to lost/stolen device	All TM data is encrypted; device screen lock is enforced (supports all available authentication factors); failed password entry timeouts stymie brute force; user-session timeout suspends TM data access until next cloud login; and more
Other apps eavesdropping on user communications	Users warned of other apps accessing microphone or camera while TM in use
Accidentally sharing restricted files with third party	TM sharing restricted to authorized groups only
Viewing TM content creates temporary copies that can be stolen	Secure, in-memory handover to viewer applications prevents generation of temporary files
Phishing or social engineering attack	TM only accepts communications from other TM sources following device AND user authentication
Confidential information exposed via screen capture or mirroring	Screen captures and mirroring are blocked on all app pages
App reverse engineering exposes vulnerabilities	Advanced application package hardening prevents reverse engineering attacks
Compromised smartphones (outdated OS/apps, risky apps/settings) may simplify attacks	Device integrity is validated continuously; device settings are verified by remote security policies; Data at rest is crypto-isolated, data in motion is encrypted

Supported Platforms

- Android X.Y
- iOS AA.B