TRUSTICA

Trustica Mobile - Military Grade Mobile Device Communications with Consumer Simplicity

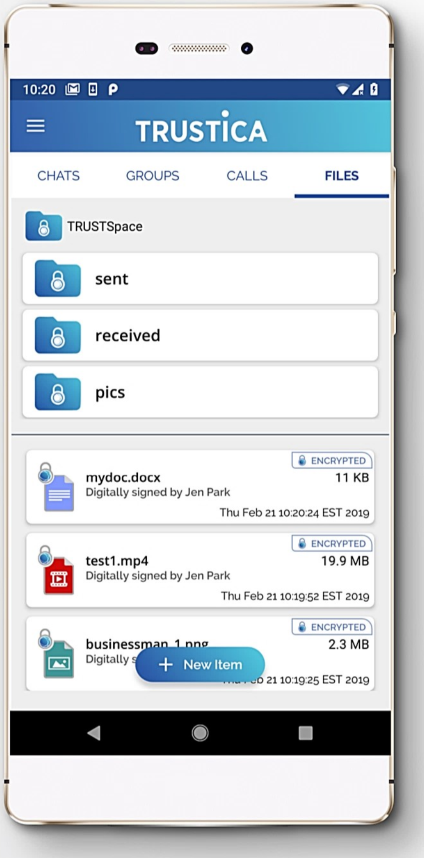
Employee-owned mobile devices are untrustworthy to an enterprise. Yet, they are commonly used for storing sensitive information and communications. Assuming administrative control over such devices with questionable cyber hygiene, and improper configurations is burdensome for the enterprise and intrusive to employees.

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

Trustica Mobile installed on their devices, enterprise personnel can securely:

- Store Files
- Transfer Files
- Send Individual Group Chat or voice messages
    - Each message encrypted with a unique key

Available for Android & iOS



TRUSTSpace

sent

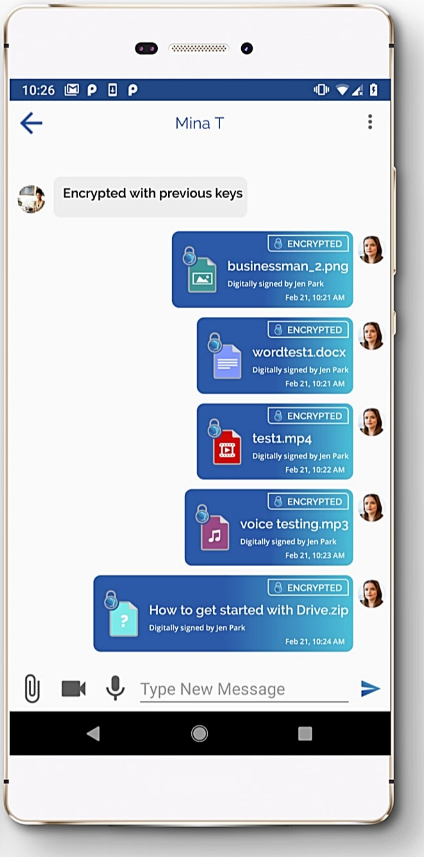
received

pics

ENCRYPTED
mydoc.docx 11 KB
Digitally signed by Jen Park
Thu Feb 21 10:20:24 EST 2019

ENCRYPTED
test1.mp4 19.9 MB
Digitally signed by Jen Park
Thu Feb 21 10:19:52 EST 2019

ENCRYPTED
businessman_1.png 2.3 MB
Digitally s
...b 21 10:19:25 EST 2019



Encrypted with previous keys

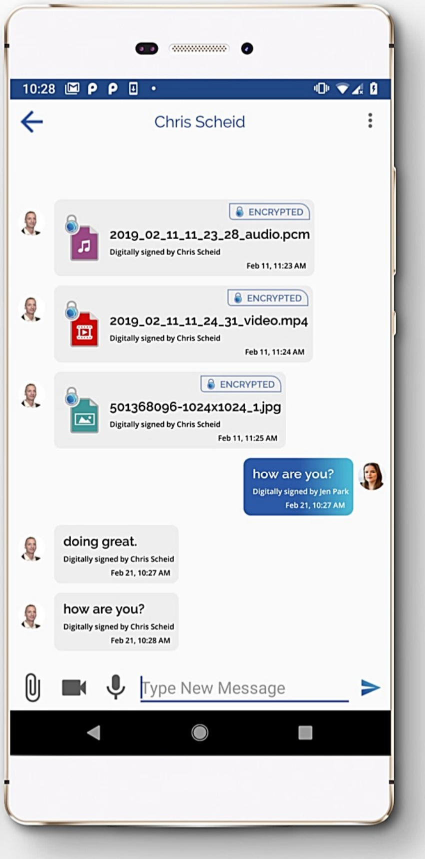
ENCRYPTED
businessman_2.png
Digitally signed by Jen Park
Feb 21, 10:21 AM

ENCRYPTED
wordtest1.docx
Digitally signed by Jen Park
Feb 21, 10:21 AM

ENCRYPTED
test1.mp4
Digitally signed by Jen Park
Feb 21, 10:22 AM

ENCRYPTED
voice testing.mp3
Digitally signed by Jen Park
Feb 21, 10:23 AM

ENCRYPTED
How to get started with Drive.zip
Digitally signed by Jen Park
Feb 21, 10:24 AM



ENCRYPTED
2019_02_11_11_23_28_audio.pcm
Digitally signed by Chris Scheid
Feb 11, 11:23 AM

ENCRYPTED
2019_02_11_11_24_31_video.mp4
Digitally signed by Chris Scheid
Feb 11, 11:24 AM

ENCRYPTED
501368096-1024x1024_1.jpg
Digitally signed by Chris Scheid
Feb 11, 11:25 AM

how are you?
Digitally signed by Jen Park
Feb 21, 10:27 AM

doing great.
Digitally signed by Chris Scheid
Feb 21, 10:27 AM

how are you?
Digitally signed by Chris Scheid
Feb 21, 10:28 AM

Contact Us: 703.786.8884 | sales@appguard.us | www.appguard.us

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 storage 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
Accidently sharing restricted files with third party	TM sharing is 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 (1H2019)