T.A.G.
CONSULTATION

Encrypted mobile technology for total security

tag-consultation.net

Table of Contents

04. Take total control

06. Powered by bulletproof operating system

08. Secure Application Suite

14. Built for total security

16. Mobile device management

17. Secure box for complete control

18. Secure SIM card with global connectivity

19. Global coverage

Protect your critical mobile communication and stored data against any cyber-attack

360° DEGREE
PROTECTION

MILITARY-GRADE
ENCRYPTION

SECURE HARDWARE
AND SOFTWARE

GLOBAL
CONNECTIVITY

FREEDOM AND
PROTECTION ALL IN ONE

Take total control

Due to the COVID-19 pandemic, cybercrime went up 600% across the globe.

Statistics look shocking, but also logical. Technologies advance rapidly. We use mobile devices more than ever before to communicate and exchange information. The convenience of fast and effortless connections comes at the cost of excess cybersecurity threats.

In the digital era, your mission-critical data and communications may easily get into the wrong hands. Daily organizations become victims of hacking techniques such as **zero-day exploits, malware attacks, phishing, wiretapping, DDoS, MiTM, and online hacking.** These attacks can potentially turn your device into a spying tool, listening and watching every move you take.

Can you prevent it? Yes. And we, at T.A.G. Consultation, are here to help you. With the right technology, implemented in the right way, you can regain the privacy and security of your data!

Our flagship mobile device, T2 COMUNICATOR, offers 360-degree protection as it integrates five core components:

- custom operating system
- suite of specialized security applications
- own data plan with global connectivity
- management solution for granular control
- self-hosted secure communication solution

T2 COMUNICATOR is the mobile device you need if you truly value your communication privacy and data security.

We protect every vertical

T.A.G. Consultation is a company devoted to helping organizations regain total control over the security of their stored data and critical communications. In order to provide top of the market tailored-made solutions for every vertical we partner with the reputed pioneers in mobile security – Secure Group Lab.

GOVERNMENT AGENCIES

Governments handle information of national security importance, as well as the personal data of citizens. Securing it is an absolute must.

POLITICAL PARTIES

Breaches in political campaigns can lead to meddling in the democratic process. Encrypted communications can hamper such attempts.

SECURITY & DEFENSE

Ensuring the safety of people and property requires secure and reliable communications that rule out an interception by third parties.

ENERGY SECTOR

Data leaks in the energy and drilling sector can affect commodity prices and takedown markets and economies. Securing communications is a must.

PHARMACEUTICALS

R&D data is one of the pharmaceutical industry's most highly valued assets. Ensuring it is transported securely is imperative.

FINANCE & BANKING

Using reliable authentication processes is crucial for preventing financial fraud. Our encrypted communication apps provide just that.

MOBILE SECURITY FOR ANY BUSINESS SIZE

You don't have to be a multinational corporation to need security, as most cyberattacks target small and medium-sized enterprises. Our solutions can secure businesses of any size against cybercrime.

Powered by bulletproof operating system

Android OS and iOS have more than 500% increase in reported distinct vulnerabilities for 2021 compared to what was reported in 2020.

T2 COMUNICATOR runs on Secure OS – a custom operating system. It utilizes multiple defence layers to isolate, encrypt, and secure mobile data against any mobile threat.

ZERO-ATTACK SURFACE

Exploitable entry points such as Google services are entirely removed from the OS. Other entry points, such as GSM and SMS services, Bluetooth, NFC, GPS, and more, can also be blocked on OS level.

VERIFIED BOOT

During first enrollment, the device creates a unique fingerprint. When booting, the system validates the fingerprint against a server-side copy to ensure the integrity and authenticity of the OS.

TRIPLE PASSWORD PROTECTION

Separate passphrases protect the device's storage, OS, and secure applications. If the wrong password has been repeatedly inputted at any level, the system triggers a wipe sequence to ensure data protection.

MULTIPLE LEVELS OF ENCRYPTION

All data stored on the device is secured and encrypted. Incoming and outgoing communication is end-to-end encrypted and transmitted over an encrypted network.

MULTIPLE WIPE OPTIONS

T2 COMUNICATOR provides several ways to wipe all data on the phone in critical emergencies. Wipe is possible in case of physical tampering attempts, lost access to the phone, or if the device is continuously disconnected or turned off.

SECURE KEYSTORE

All encryption keys are generated and stored on a FIPS 140-2 certified cryptographic module. No private keys are ever shared or stored outside the device.

TRUSTED UPDATES

Updates are issued and digitally signed exclusively through the Secure Administration System (SAS). Devices apply updates only after verifying the authenticity of the digital signature.

Secure Application Suite

83% of consumer-grade mobile applications have at least one security flaw.

Choosing suitable mobile applications is essential for any organization. It's vital to have seamless integration of different apps supporting data in transition, data at rest, and other functionalities to ensure no gap and no chance for a data leak.

T2 COMUNICATOR provides a secure application suite to assist you in day-to-day communication and data flow. With the secure application suite, you don't need to rely on conventional third-party applications anymore.

The Secure Communication Suite consists of **Secure Chat, Secure Vault, and Secure Calendar.** Even if an attacker intercepts apps' traffic, the communication can't be decrypted and read.

Integration of Trusted Enterprise Apps can be offered as an option.

SECURE CHAT

Secure Chat is an end-to-end encrypted secure messaging app that allows users to:

- Send peer-to-peer messages;
- Join group chats;
- Make unlimited voice and video calls.

Serverless P2P chat characteristics and protocols:

- OTR cryptographic protocol;
- Messages encrypted with 256-bit AES cipher;
- 4096-bit Diffie-Hellman key exchange;
- SHA-2 hashing used for authentication;
- Different keys for every chat session.

Secure group chat characteristics and protocols:

- OMEMO cryptographic protocol;
- Double Ratchet Algorithm for multi-end to multi-end encryption;
- Elliptic curve (ECC) Curve25519/Ed25519;
- Elliptic curve Diffie–Hellman (ECDH) key agreement scheme;
- SHA-256 hash function.

P2P voice and video call characteristics and protocols:

- ZRTP cryptographic protocol;
- Diffie-Hellman key exchange;
- Secure Real-time Transport Protocol (SRTP);
- Short authentication string (SAS) against MiTM;
- Keys discarded after every call.

PGP chat characteristics and protocols:

- 4096-bit RSA key pair used for encryption and decryption;
- Content encrypted with IDEA cipher;
- User managed encryption keys;
- Private keys are never stored server-side.

SECURE VAULT

Secure Vault is an encrypted file storage app. You can store information as encrypted notes, rich file formats, conversations and create secure backups of your settings, contacts, and data.

Secure vault characteristics and protocols:

- XTS encryption with state-of-the-art SHA-512 hashing;
- Additional password protection;
- Compatible with multiple file formats;
- Encrypted notes;
- Encrypted backups.

SECURE CALENDAR

Secure Calendar is a private calendar app to organize your work schedule, create meetings and events, set reminders, and securely share them with your peers through Secure Chat.

Secure calendar characteristics and protocols:

- SQLCipher 256-bit AES full database encryption;
- Additional password protection.

SERVERLESS PEER-TO-PEER CHAT

Our Serverless Peer-to-Peer Chat uses our infrastructure only to establish a secure connection between the two parties. All data is end-to-end encrypted and transmitted directly between the communicating devices, without it passing through our servers.

T.A.G. CONSULTATION

Competitors

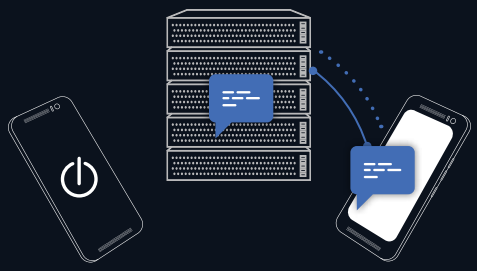
Sender is online; recipient is offline

When you tap send, the app connects to the server, which checks if the recipient's device is online. If it isn't, the message doesn't get sent. It never leaves your device.

When you tap send, the app sends the message to the server, which checks if the recipient's device is online. If it isn't, the message stays on the server and waits for the recipient to come online.

Sender is offline; recipient is online

When the recipient comes online, they do not receive the message you tried to send while they were offline – it never left your phone.



When the recipient comes online, they receive your message which was waiting for them on the server, regardless if you are now online or not.

Both parties are online

The server checks if the recipient is online. If they are, your phone sends the message directly to them.

The messages get sent to the server and then from the server to the recipient.

ZERO-SERVER TRACE GROUP CHAT

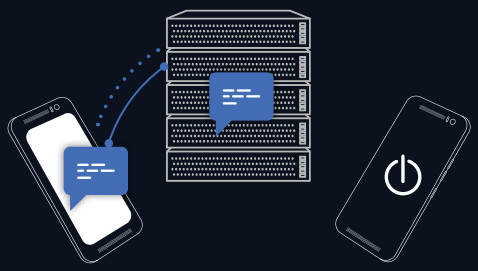
To facilitate a private, secure, and feature-rich group chat experience, our servers store the encrypted messages until they are delivered to all peers or for a maximum of seven days. The messages can be decrypted only by the participating devices.

T.A.G. CONSULTATION

When you tap send in a group chat room, the app connects to the server and sends the encrypted message.

Sending a message

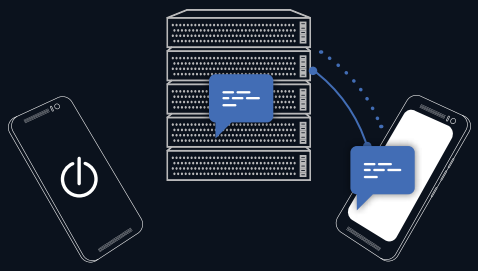
Competitors



When you tap send, the app sends the message to the server, which checks if the recipient's device is online. If it isn't, the message stays on the server and waits for the recipient to come online.

If one or more recipient is offline, the encrypted message remains on the server for a maximum of seven days. It gets deleted after it is delivered to all recipients or after this period.

One or more recipient is offline



When the recipient comes online, they receive your message which was waiting for them on the server, regardless if you are now online or not.

If all recipients are online, the encrypted message is delivered and instantly deleted from the server.

All recipients are online

The messages get sent to the server and then from the server to the recipient.

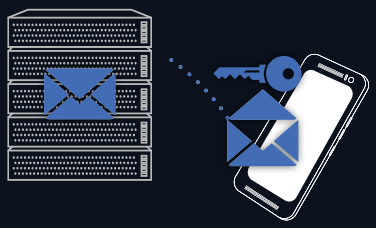
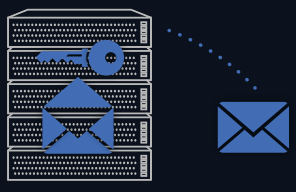
PEER-TO-PEER VOICE & VIDEO CALLS

With T.A.G. Consultation you can make unlimited encrypted VoIP calls. Our devices use our server only to establish a connection between peers, but not to facilitate communication. The flow of data allows us to create a true peer-to-peer connection with zero data retention, ensuring unmatched privacy

T.A.G. CONSULTATION		Competitors
	**Key pair generation**	
Both devices generate ephemeral key pairs.		The ephemeral key pairs are generated on the server and then distributed to the peers' devices.
	**VoIP calls**	
When making a call, the phone uses the server to check if the recipient is online. Communication then takes place directly between devices in a true peer to peer environment		When making a call, the phone connects to the server and uses it to facilitate the connection with the other device. The communication is interceptable on a server level.
	**Call fees**	
Users can make unlimited calls without any additional fees.		Both users are charged for each call.

PGP CHAT WITH USER MANAGED KEYS

Messages sent through the PGP Chat are encrypted with 4096-bit keys, unbreakable even for modern supercomputers. All private keys are generated and stored directly on the device, not allowing any party, including T.A.G. Consultation, to decrypt the transferred information.

T.A.G. CONSULTATION		Competitors
	**Key pair generation**	
The key pair is generated by the app on your device.		The key pair is generated on the server and then sent to the device.
	**Private key storage**	
No private keys are ever stored on our servers, and there is no way for us to replicate them.		The server stores copies of the private keys or can generate identical ones.
	**Message exchange**	
Your messages pass through the servers but cannot be decrypted by anyone but you - with the private key stored only on your device.		Your messages pass through the server and can be decrypted with copies of the private keys.

Built for total security

The common practice of BYOD (bring your own device) has exposed numerous organizations to the risk of security breaches. Although MDM systems centrally control devices, employees still tend to:

- Connect to the internet through insecure networks;
- Download malicious files;
- Keep sensitive information unprotected.

50% of companies that allowed BYOD experienced a data breach through a personal device.

T2 COMUNICATOR solves the challenge by introducing a complete security-hardened solution. The implementation of numerous quality assurance methods guarantees the integrity of the hardware you're receiving. By blocking out easily compromisable sensors, the device significantly reduces the attack surface.

You can store everything on the handset's encrypted databases behind additional password. Multiple password mismatches trigger a device wipe mechanism. You can also easily wipe all the data remotely.

The T2 COMUNICATOR package includes additional privacy protection accessories such as **a faraday bag** and **a privacy screen protector.**

HARDWARE MODEL SPECS:

Octa-Core processor	4500mAh battery
128GB encrypted storage	25MP front camera
4GB RAM	48MP + 8MP + 5MP back cameras
6.53'' Full HD	

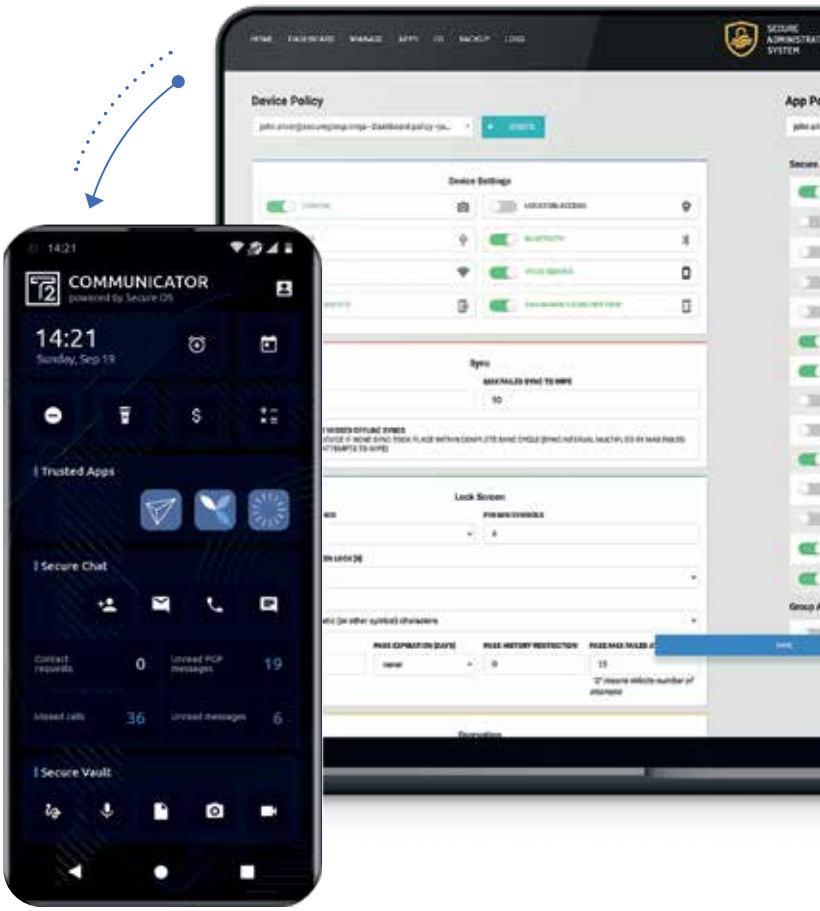
Mobile device management

Nearly half of all organizations have at least one employee who downloads a malicious mobile application that threatens their organization's networks and data.

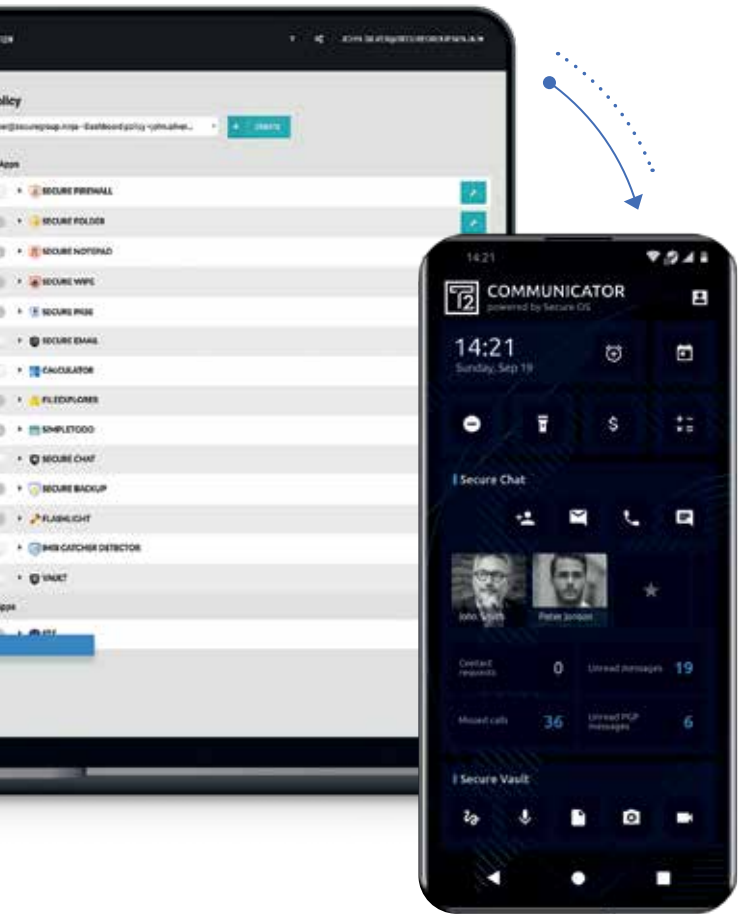
The **Secure Administration System (SAS)** is a mobile device management (MDM) solution that provides comprehensive and intuitive tools for Secure OS-powered devices. It gives you the ability to granularly control, monitor and configure your user devices.

It allows IT teams to manage single or multiple mission-critical devices from a centralized command center.

- Deploy apps and installer packages;
- Set up and manage fleets of secure devices;
- Configure device settings and features;
- Create policies for a group of devices;
- Push mass actions;
- Erase devices remotely;
- Backup and restore devices;
- Monitor network security and detect IMSI Catchers;
- Disable and enable apps;
- Control device's functions;
- Keep devices secure and disable vulnerabilities.



Secure box for complete control



Almost 70% of all organizations leave back doors open to attackers through misconfigured cloud services with a low-security score.

Secure Box is a self-hosted solution for end-to-end encrypted communications designed for organizations that control their sensitive data entirely. It's a pre-configured turnkey solution that allows your IT teams to quickly and easily deploy single or multiple servers.

Unlike cloud-based hosting solutions, Secure Box is a dedicated server that you can move from point A to point B or store in a secured data center. Thus reducing the risk of security breaches, credential stealing, data loss, unauthorized access, reduced visibility, and control.

Advantages of Secure Box:

- **Complete control** - own your data for mission-critical communication across your organization.
- **Zero-knowledge architecture** - no storing of sensitive information, confidential data, or private encryption keys on the server.
- **Decentralization and security** - harder to attack with the ability to stay intact and operational if a single server is compromised.
- **Always on communication** - stay connected at all times.
- **Infinitely scalable** - allows for limitless and rapid scalability.
- **Turnkey deployment** - quickly and easily deploy single or multiple servers.

Secure SIM card with global connectivity

No matter what device you're using, your data and communications security are interrelated to your mobile service provider or network carrier. Anyone who owns or has access to the mobile network can access the data that pass through it.

Our mobile solutions have the option to add **Secure SIM - a Multi-IMSI SIM card that gives you total freedom from third-party service providers.** The card stores multiple IMSI numbers and can switch between them to connect to multiple operators, ensuring the best signal in any region worldwide.

- **SS7 firewall**
  reliable protection against unauthorized access, malware distribution, physical tracking, and DoS attacks;
- **Built-in VPN**
  always-on VPN protection
  when connected to 3G, or 4G network.

GLOBAL COVERAGE

The SIM stores multiple IMSI numbers and can switch between them to always connect to the local operator with the best coverage, ensuring smooth connectivity in more than 120 countries across the globe.

AFRICA

Algeria, Burkina Faso, Congo, Egypt, Ghana, Kenya, Mali, Mauritius, Morocco, Nigeria, Rwanda, Senegal, South Africa, Tanzania, Tunisia, Uganda, Zambia

ASIA

Bahrain, Bangladesh, Brunei Darussalam, Cambodia, China, Hong Kong, India, Indonesia, Iran, Israel, Japan, Jordan, Kazakhstan, Republic of Korea, Kuwait, Kyrgyzstan, Macau, Malaysia, Myanmar, Pakistan, Philippines, Qatar, Russian Federation, Saudi Arabia, Singapore, Sri Lanka, Taiwan, Tajikistan, Thailand, Turkey, United Arab Emirates, Uzbekistan, Vietnam

EUROPE

Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom

NORTH AMERICA

Anguilla, British Virgin Islands, Canada, Costa Rica, Dominican Republic, El Salvador, Haiti, Mexico, Nicaragua, Panama, Trinidad and Tobago

OCEANIA

New Zealand

SOUTH AMERICA

Argentina, Aruba, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Netherlands Antilles, Paraguay, Peru, Suriname, Uruguay, Venezuela

T.A.G.
CONSULTATION

DSE International

Authorized Reseller

dseinternational.com