

*“Secure mobile communication based on Tutus Färist”*

**Färist Mobile is a complete solution for secure mobile communication based on the certified and EU-approved Tutus Färist product family.**

**Today’s use of mobile devices requires increased security**  
Smartphones and tablets have become our most important tools in voice and data communication, access to information, and local storage. This creates new demands for security.

#### **Secure mobile communication**

Färist Mobile has been developed to satisfy the needs of an organisation to be able to use smartphones and tablets in a secure way for all its mobile communication.

- Encrypted voice calls and messaging
- Browsing the Internet securely and anonymously
- Secure access to internal resources

#### **Latest models of smartphones and tablets**

Färist Mobile supports the most recent models from leading suppliers, with all of the functions that are now available for efficient and mobile work, implemented in Tutus's own high-security systems.

#### **Ease of use**

Färist Mobile is available both for smartphones and tablets in various sizes and designs. They all have in common that they are based on Tutus’s secure mobile platform, which is fully Android-compatible.

- End users do not need to learn a new interface
- All Android apps can be installed and will be automatically protected by Färist Mobile

#### **Based on Tutus's approved products**

The solution consists of a central node that is based on Tutus’s certified and approved Färist VPN product, and secure Android-compatible smartphones and tablets.



#### **Key features**

- Encrypted messaging and voice calls
- Secure always-on VPN over 3G/4G/Wi-Fi
- Application whitelisting
- Disk encryption with strong keys
- Central firewall
- Can be used as secure 3G/4G/Wi-Fi modem
- Remote and local secure wipe
- Can be used as a secure USB-memory
- Integrity control of key components
- Secure updates over-the-air
- Seamless roaming between Wi-Fi and 3G/4G
- No hidden applications added by any third party
- Central management
- Easy and straightforward provisioning
- No vendor account needed for activation or updating

#### **Färist Mobile protects against all security challenges**

- Malware
- Hacking
- Eavesdropping
- Loss or theft
- Misconfiguration
- Lack of integrity

### Encrypted voice calls

Färist Mobile is equipped with an IP-based function for encrypted voice calls. All the user has to do to activate an encrypted voice call is to use a prefix. An easy-to-use contact list and catalogue service are also provided. Encrypted voice calls can be held with other users of Färist Mobile either individually or in groups.

### Encrypted messaging

It is as easy to send an encrypted SMS with Färist Mobile to a receiver who has Färist Mobile as it is to send a normal SMS.

### Connect laptops

Färist Mobile can be used as an encrypting 3G/4G or Wi-Fi modem for a laptop. Connecting Färist Mobile to a laptop through a USB port makes it possible to communicate and access a corporate office in a secure manner over open networks.

### Encrypted storage

Färist Mobile encrypts all locally stored user information using strong external keys, which guarantees that sensitive information remains protected, even from advanced attackers with physical access to the device.

### Apps from a dedicated marketplace

Färist Mobile uses whitelisting based on certificates to determine which apps are to be allowed to be installed on the device. An organisation can easily sign apps and make them available on its own marketplace.

### Secure updating

Färist Mobile can be updated over-the-air using secure methods. This ensures in an efficient and continuous manner that all Färist Mobile devices always have the most recent version.

### Integrity control of key components

A control is carried out at regular intervals that security-critical components of Färist Mobile have not been modified.

### Encrypted voice calls with Färist Mobile



### Secure Internet browsing and secure access to internal resources with Färist Mobile



### Management and security policies

Färist Mobile includes a centralised management system. Organisations can, at a moment's notice, change internal communication policy, disconnect, upgrade or remotely wipe any device at any time.

### IP traffic is secured with Tutus's approved products

All IP traffic from the device is protected by an encrypted VPN tunnel. The traffic in the tunnel arrives at a central Färist VPN node, where it is decrypted. Internet access will always go through a central firewall.

### Färist Mobile has security built in

Tutus designs and develops security products based on modular concepts combined with a comprehensive approach. The strategy has been very successful, and we have developed several certified and approved products. We have used the strategy to combine our secure platform, Färist, with market-leaders among hardware platforms in a secure and cost-effective manner, while retaining control over the complete solution.

Färist Mobile is produced in a highly controlled process in which all existing software in the device, including the operating system, is removed and replaced by Tutus's secure platform, Färist. The device is then equipped with a transparent and secure operating system. This enables us to ensure in a unique manner the integrity and security of all functions in the device, and to equip it with robust protection, with full control.

### Security and assurance

Färist Mobile is based on the Färist security core, identical to all other products within the Färist product family. Färist products have been evaluated and certified according to Common Criteria with assurance packet EAL4+ and are approved to protect classified information at the level of Restricted in Sweden and in the EU.

Our policy of continuous development may cause the information and specifications contained herein to change without notice.