secusmart | BlackBerry Subsidiary

SecuTABLET

SecuTABLET – Secure Mobile Communication

SecuTABLET provides a solution for secure voice and data communication, available on a commercial standard tablet. The product is primarily intended for organizations with high standards for secure mobile communication.

SecuTABLET combines ease of use and security in compliance with the German security classification VS-NfD (Classified – For official use only).

All security features make use of the Secusmart Security Card (SSC) as a hardware based cryptographic anchor. The operating system on the Samsung tablets is a standard version of Android with security enhancements. Each app is secured in an individual container. The following security features are thus implemented:

- storage encryption
- transport encryption
- secure data transfer between apps

The solution features:

- simple and intuitive operation on a typical Android environment
- the parallel use of business and personal apps
- easy commissioning with no need for specific user training
- support for latest off-the-shelf device hardware

1. SecuTABLET Security Architecture

SecuTABLET requires a secure IT-infrastructure. For customers who already own a SecuSUITE solution, the SecuTABLET infrastructure integrates into the existing one. The backend infrastructure comprises the following components:

- VPN Gateway. Cisco ASA and Secunet SINA are supported. The approval for official use by the German Federal Office for Information Security (BSI) is only valid if a Secunet SINA VPN gateway is used in combination with the SecuTABLET.
- EASE server software
- Mobile Device Management system (optional)
- standard IT components

EASE server software

The EASE server software provides the SecuSTORE (app store) function and is used to administer the security features and policies on the devices. The EASE Server is also used to create the app-specific containers for each app based on the provided security policies. This process is known as "app wrapping" and enables the app in question to handle sensitive data securely. More specifically, this means that apps can perform:

- storage encryption (Data at rest)
- transport encryption (Data in transit)
- secure transfer of data between apps (Data in use)

The security features applied during app wrapping are policies defined by the customer. After the wrapping process, the app is signed by the EASE server and made available to the user on the SecuSTORE.

The security architecture on the mobile user device is managed and configured by the EASE server. It comprises the following components:

- Data at rest: Secure persistent storage of business data with an app-specific key. The individual key of the SSC furthermore encrypts the app-specific keys, preventing unauthorized access to the app-specific keys.

- Data in transit: Secure data communication with the backend system is enabled via IPsec-tunnel. The SSC contains and protects the private user keys and certificates required to establish the secure communication.

- Data in use: Ensures that secure data can only be processed by business apps. The master keys required for this mechanism are protected from unauthorized access by the SSC.
  Access rights for each business app are defined in the EASE Server and offer additional protection against the unauthorized inflow and outflow of information.

- Secusmart Security Card (SSC): The Secusmart Security Card is a fully qualified signature card supporting on-board generation of all required cryptographic materials during the personalization phase of the card. This smart card acts as the security barrier by protecting the cryptographic material required to use the SecuTABLET. The SSC is a micro SD form factor smart card with an integrated crypto-controller. The SSC hosts all key material and certificates required to access the local and remote data. The cryptographic functions of the SSC can only be used by unlocking the smart card via a user defined PIN.

- Protection of the operating system: The SecuTABLET protects the integrity of the operating system during both startup and operation of the mobile device. Samsung KNOX features verify that the system is only booted with trustworthy firmware.

The following figure provides an overview of the system components:

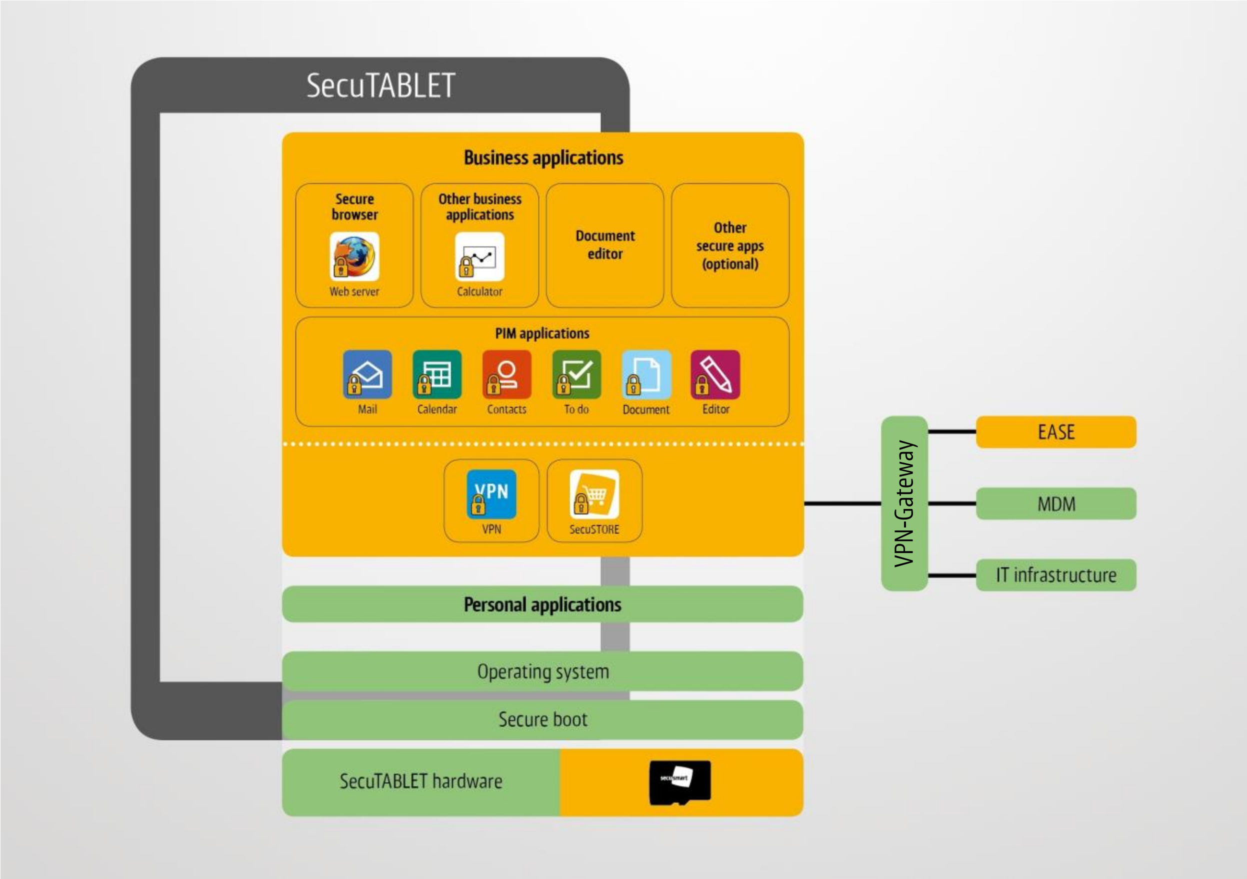

Figure 1: System components of the SecuTABLET solution

2. Business and Personal Apps

The SecuTABLET enables users to access both business and personal apps.

Both types of apps are made available to the mobile user device via the Ease server.

Business apps

Business apps only process sensitive secure data. Only business apps are permitted to use the VPN tunnel, which provides access to the services of the business backend system.

Business apps can be identified by a small padlock on the app icon.

Personal apps

Personal apps are kept strictly separate from business apps. They can neither access sensitive data from business as nor communicate with business apps. They are also not allowed to use the VPN tunnel.

Installing apps

The SecuTABLET is delivered with the SecuSTORE and VPN apps pre-installed. In order to add an additional app, the apps wrapping capability needs to be verified. Once confirmed the following steps must be taken in order to make further apps available for the SecuTABLET:

1. Administrator working for the authority or organization operating the SecuTABLET selects an app for use on the SecuTABLET.
2. The administrator uploads this app to the EASE server. The administrator then individually configures the security features (policies) to be applied to the app and conducts the app wrapping process.
3. The secured app is now available to the user in the SecuSTORE.
4. The user can search the updated SecuSTORE for apps (depending on his/her user profile).
5. The user can now download the app to his/her SecuTABLET from the SecuSTORE and use it securely.

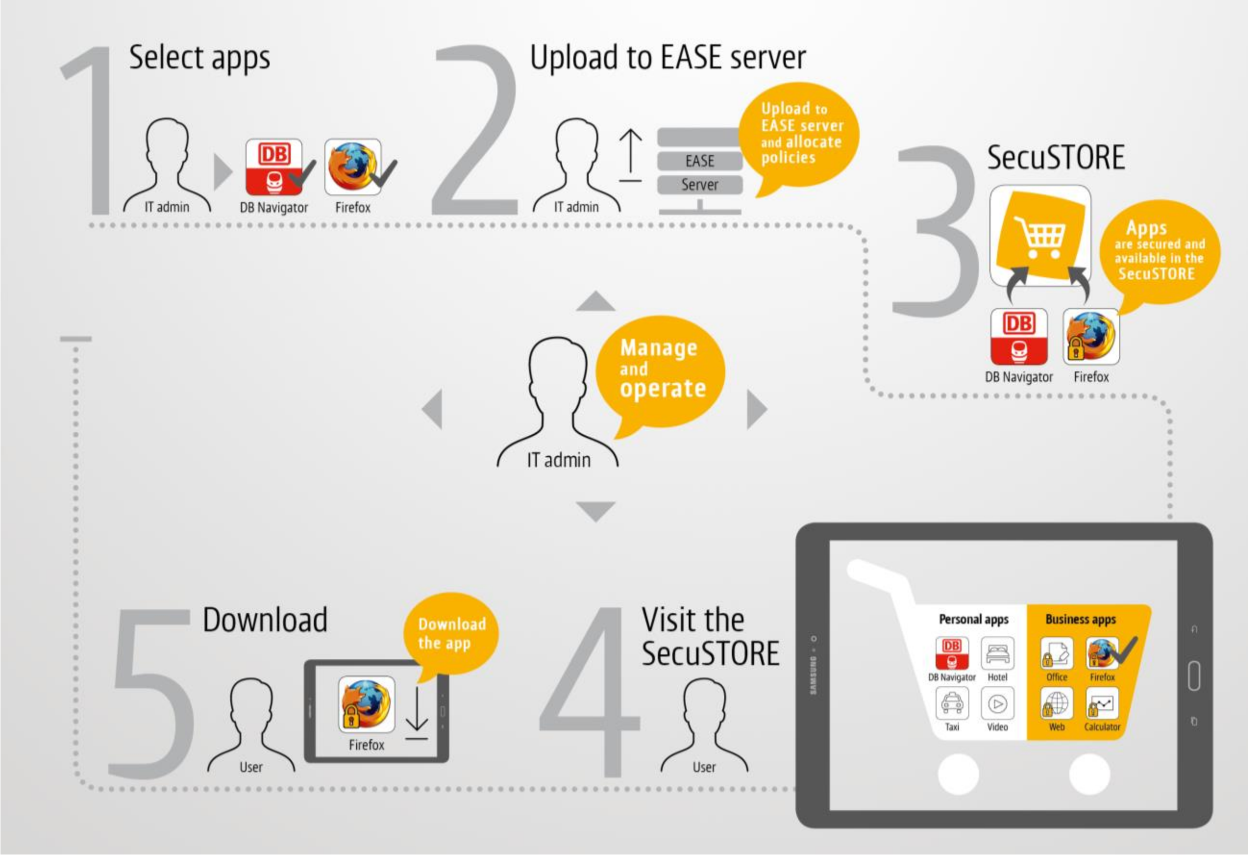

Figure 2: End-to-end process

Initially available business apps

An initial group of business apps for personal information management (PIM), mobile office and search purposes are available for the SecuTABLET.

The SecuSTORE and VPN apps are pre-installed on the SecuTABLET and are essential for its operation.

SecuSTORE

The SecuSTORE is the secure resource centre from which business and personal apps can be installed and updated. It enables apps to be distributed to their assigned user groups and implements the security policies.

VPN app

The VPN app is responsible for the IPsec-based connection of the SecuTABLET to the VPN gateway. It implements an app-level VPN and ensures that only business apps can access the business background system.

Secure browser

Firefox is the secure browser available on the SecuTABLET. All the data traffic from this secure browser passes through the VPN gateway. The app supports HTTP and HTTPS proxies, enabling the intranet and internet to be accessed via the business background system.

Document editor and viewer

WPS Office enable documents to be fully displayed and are able to edit a variety of file formats, such as Adobe PDF, Word, Text, PowerPoint and Excel.

E-Mail, Contacts & Calendar

The SecuTABLET provides users access to their email, contacts, calendar & notes in a personal information management (PIM) client. Lotus Notes, BlackBerry Hub Plus & standard POP/IMAP servers are supported. All the data traffic from the PIM client passes through the VPN gateway.

Image viewer

The image viewer supports all current and relevant image formats, such as JPG, PNG, GIF and BMP. The app was developed to display individual image files and does not store any information when business files are opened.

File manager

The secure file manager app is used to manage secure files and provides standard functions such as the ability to copy and paste, move, delete and open files.

3. Facts and Figures

3.1 Mobile User Device

The Samsung Galaxy Tab S2 9.7 (SM-T815) is currently used for the SecuTABLET solution. A summary of its specifications can be found below:

- Display size: 9.7”/resolution: 2048 x 1536
- Main camera: 8 MP/front camera: 2.1 MP
- RAM: 3 GB/storage: 32 GB
- WiFi, GSM (2G), UMTS (3G), 4G FDD LTE
- Dimensions: 237.3 mm x 169 mm x 5.6 mm
- Weight: 392 g
- Nano SIM
- USB 2.0

Figure 3: Samsung Galaxy Tab S2 9.7