Federal Office
for Information Security

Requirements for OEM regarding Smartphone Security

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 95820
E-Mail: referat-tk12@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Preliminary Note

This catalogue of requirements is aimed to original equipment manufacturer (OEM) of smartphones. It describes the required basic equipment of devices from the IT security perspective and implementations for a secure operation.

The requirements must be implemented as state of the art and additionally have to respect the referred BSI Technical Guideline (BSI-TR)[1].

1 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

2 Catalogue of Requirements

2.1 EU law compliance

New devices, preinstalled apps and connected services have to be conform to the General Data Protection Regulation (GDPR) of the European Union and the German national requirements for data protection. Manufacturer must give a statement respectively.

This important requirement will be repeated in some subsequent chapter.

2.2 Actuality of data

2.2.1 Actuality of the OS version

For every kind of devices OEM have to make a statement about the maintenance with OS updates (main version). This statement must contain the duration in years post to the release and the minimum number of main versions planned. (For this, we assume that there is one main OS version released per year.)

New devices must be provided with the latest OS available at release time. If there is a newer OS version available at the time of activation, this OS version must be provided for download and installation.

2.2.2 Support for security updates

Devices must be provided with security updates for five years after release. The devices description must specify the time the support for security updates will end for that device.

Security Updates must close all publicly known security vulnerabilities of all software component (that is driver, operating system, customized software layer and preinstalled apps). A detailed bulletin with comprehensive and transparent information about the security update must exist.

2.2.3 Duration of rollout

Security updates must be provided for download and installation within one month after public release.

2.3 Unauthorized Access Protection

2.3.1 Lock Mechanisms

At least one of the following unlock mechanisms must be present and securely implemented

- Alphanumeric password
- Fingerprint
- Face recognition / 3D face recognition
- High secure biometric scan

2.3.2 Device Encryption

Internal Memory must have full disk encryption. The key generation must be a combination of the user password and an individual, device specific property. The keys must be saved in secure environments (refer chapter Secure Executable Environment and HSE).

2.3.3 Encryption of external memory

For external memory (e.g. SD cards) secure encryption must be possible.

2.3.4 Secure Executable Environment and HSE

Devices must provide a secure executable environment isolated form the normal OS based on a hardware secure element (HSE). Additionally the HSE must be used to store critical user data. Additionally refer to chapter “Dedicated Hardware for cryptographic Functions”.

2.3.5 Secure Boot

Devices must provide secure boot. With this characteristic every stage in the boot process ensures the integrity and authenticity for the next stage before it transfers execution control to it. Furthermore the first stage – the bootloader – is responsible for checking updates for integrity and authenticity. Mismatches must be recorded and the whole boot process has to be cancelled if a mismatch is detected. A recovery option that restores the initial operating system must be offered. Additionally an option to shut down the device must be presented.

2.3.6 Bootloader Unlock

For every device a process to unlock the bootloader must be provided from OEM. It must be a transparent process with a software tool or an easy to use guide.

In case of bootloader unlock, all user data must be deleted in a safe way.

Furthermore, users must be informed clearly about the unlock and potential risks of the unlocked bootloader.

2.3.7 Cyphering

From the network perspective the use of the newest Radio Canal Cyphering Algorithms has very high priority. Devices supporting these algorithms are better protected.

New devices must be equipped with state of the art technology to support the newest Radio Canal Cyphering Algorithms. For more information refer to BSI TR-02102 Chap. 4.7 “Cypering”.

2.4 Data Privacy Protection

2.4.1 Pre-installed Apps in system partition

In the system partition only apps with the need for system permissions are allowed (e.g. signature permission on Android). Apps with normal permission requirements must not be installed in this partition (e.g. OEM owned browser app, other third-party apps).

2.4.2 App Permission for (pre-installed) Apps

Apps are only allowed to request permissions that are absolutely necessary for fulfilling their tasks. Critical[2] runtime permissions must be opt-in permissions and must be switched off after app installation. If a user opts-in a runtime permission he/she must be able to opt-out at any time and vice versa. Declined and/or rejected permissions could lead to functional limitations but not to app crashes. Any permission (internal and public) must be presented to the user in an appropriate settings item. Permissions must be documented in a complete and comprehensible way.

This requirement generally stands for all apps. In this catalogue pre-installed apps are in focus.

2.4.3 Secure Software Development Process

In the scope of a secure software development process all specifications of the platform manufacturer must be respected. In case of Android these are the “Google Best Practices”. Furthermore additional guidelines should be taken in account, e.g. “Mobile AppSec Verification Standard” of OWASP.ORG.

2.4.4 Telemetry

All data collection (device data and user data) with the purpose of product development are “Telemetry”. OEMs must ask the user for an explicit agreement of usage and/or a transfer of these data to partners. OEMs must provide detailed information about the kind and amount of telemetry data. Collection and transfer of telemetry data must be reduced to an absolute minimum.

In parallel OEMs must sign a GDPR agreement for devices consisting of operation system, manufacturer branding, pre-installed apps and pre-installed third-party apps. If the user opts out of this regulation, telemetry data must not be collected, processed or transferred in any kind.

2.4.5 Secure Software Platform

Software downloads and updates must be provided via a secure platform. Collection and transfer of device and user data must be reduced to a minimum to fulfil the service. These data must only be used for this service and must not be transferred to partners. OEMs must sign a GDPR agreement.

2 Critical Permission: Permission that enables access to private or private-related data (e.g. Contacts, messages, geo-location), manipulation of security-related functions (e.g. overlay of system dialogue or settings) or permissions that cause costs.

2.4.6 Network Gateways

Data interchange between a device and the internet must be routed via the provider suggested gateway or via a user configurable gateway. Hard coded fall-backs to other servers are not allowed.

Same applies for DNS configurations.

2.5 Reduction of Attack Surface

2.5.1 Cloud Services

Prior any use of cloud services users must be informed. Any usage of cloud services must be conform to the GDPR. Any usage must be listed in a clear and understandable way. New devices must be free of pre-configured cloud services (e.g. Google account, OEM apps). This also includes local services with activated cloud connection. Cloud services must be opt-in services with the possibility of opting out. In that case all user data in the cloud must be deleted.

2.5.2 Basic Settings

For new devices security related settings must be configured safe instead comfortable for users. Warnings for weak settings must be presented to users (e.g. screen lock and disk encryption).

2.5.3 Communication Ports

Wi-Fi: an opt-out option must exist for automatic connection to known Wi-Fi access points. The internal list of known Wi-Fi access points must be readable and editable. Wi-Fi probe requests must not contain SSIDs and MAC addresses must be changeable/randomized.

Bluetooth: Users must be able to configure these interfaces (e.g. switch off). Turning those interfaces off must be an option at any time.

NFC: The NFC interface must be certified for NFC Handset Test Books[3] from GSM Association (TS 27). The interface must be configurable for users. The interface should be switched off by default. Users must legitimate data exchange through the NFC interface – e.g. for payment services – prior to the transfer. The interface must be separated from the system in an appropriate manner. Protection against not allowed communication attempts must be implemented and the transfer of not-signed code is forbidden. In particular only trustworthy connection and certified app should be accepted.

2.5.4 Dedicated Hardware for cryptographic functions

Main cryptographic functions of the operating system must be supported by dedicated hardware. Especially all cryptographic keys have to be managed in secure hardware by a certified Cryptographic Service Provider. Private and secret keys must exported in a secured way.

The security functions Full-Disk-Encryption, Secure Boot and FIDO2 must be supported by secure hardware which must also be provided to applications. Security critical applications must be performed by hardware supported applets.

3 https://www.gsma.com/newsroom/wp-content/uploads//TS27-v15-0.pdf

The hardware element must be certified with Protection Profiles „Cryptographic Service Provider“ (BSI-CC-PP-0104-2019)[4] or „Cryptographic Service Provider Light“ (BSI-CC-PP-0111-2019 Commen-Criteria.

Furthermore the hardware element must be able to process eID-Applets corresponding to section 2.2.4 of BSI-TR 03159-2 „Mobile Identities Part 2: EAC and FIDO based mobile identities“[5].

2.5.5 Processor security features

The processor must support hardware based security functions for attack defence. This includes mechanisms for ROP/JOP mitigation, attacks to speculative execution and memory encryption, and separation mechanisms (TEE).

2.6 Advanced Requirements

2.6.1 Migration of PIM Data

Exporting of PIM data from a given devices and importing to another device must be possible. The export must be made into a standardized data format. PIM data consist of contacts, appointments, tasks and notices and additionally local mails.

2.6.2 Central Services

Operating system services and services of os integrated apps must be hosted and processed in German data centers. Such services are (e.g.) update server and external telemetry data processing.

2.6.3 FIDO2 authentication

The device must support authentication mechanisms following the FIDO2 standard for easy to use web service authentication. The FIDO2 authentication must at least be certified with FIDO Level 2.

4 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0104.html
5 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-2.pd