**Swedish Certification Body for IT Security**

# Certification Report Sony Xperia X and Sony Xperia X Performance

**Issue: 2.0, 2017-apr-03**

*Authorisation: Imre Juhász, Certifier , CSEC*

*Table of Contents*

# 1 Executive Summary

The Target of Evaluation (TOE) is a mobile device, which is composed of a hardware platform and its system software. The two mobile devices included in the evaluation, Sony Xperia X and Sony Xperia X Performance, use Android version 6.0.1 (Marshmallow MR1) with modification and extensions from Sony Mobile.

- Xperia X: kernel version, 3.10.84 based on Android version 6.0.1, build 34.0.A.1.268, hardware platform 8956 (Snapdragon 650)
- Xperia X Performance: kernel version: 3.18.20 based on Android version 6.0.1, build 35.0.A.1.227, hardware platform 8996 (Snapdragon 820)

The TOE is intended to be used as a mobile device within an enterprise environment where the configuration of the device is managed through a compliant device management solution. The major security functionalities that the TOE offers are; protected storage, mobile device configuration of e.g. policies, protected communication, authentication before accessing protected functionality and data and mobile device integrity e.g. secure boot and self-tests.

The TOE is delivered to retailers in a sealed box. An unbroken seal protects the device from tampering. It also states that Xperia devices are distributed via various distribution channels for e.g. mobile operators, Sony Stores, resellers and retailers.

The Security Target (ST) claims strict conformance to Protection Profile for Mobile Device Fundamentals. Version 2.0 as of 2014-09-17. There is no claim of conformance to an Evaluation Assurance Level package.

There are three assumptions made in the ST regarding the secure usage and environment for the mobile devices. The TOE relies on these assumptions being met in order to counter the eleven threats in the ST. The assumptions and the threats are described in chapter 4 Assumptions and Clarification of scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT security Evaluation, version 3.1, release 4.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for strict conformance to: Protection Profile for Mobile Device Fundamentals, Version 2.0 as of 2014-09-17 [MDFPP2]

# 2 Identification

| Certification Identification | |
|---|---|
| Certification ID | CSEC201003 |
| Name and version of the certified IT product | Sony Xperia X and Sony Xperia X Performance<br><br>Xperia X:<br>Kernel version, 3.10.84 based on Android version 6.0.1, Build 34.0.A.1.268<br>Hardware platform 8956 (Snapdragon 650)<br><br>Xperia X Performance:<br>Kernel version: 3.18.20 based on Android version 6.0.1, Build 35.0.A.1.227<br>Hardware platform 8996 (Snapdragon 820) |
| Security Target Identification | Security Target - Common Criteria Security Target for Sony Xperia |
| EAL | There is no claim of conformance to an Evaluation Assurance Level package |
| Sponsor | Sony Mobile Communications Inc. |
| Developer | Sony Mobile Communications Inc. |
| ITSEF | atsec information security AB |
| Common Criteria version | 3.1, revision 4 |
| CEM version | 3.1, revision 4 |
| Certification date | *2016-12-08* |

# 3 Security Policy

The TOE consists of seven security functions. Below is a short description of each of them. For more information, see Security Target [ST]

### *Cryptographic Support*

Cryptographic support is provided in different ways on different levels by the TOE. On a low level the TOE provides a Trusted Execution Environment (TEE) which is an isolated environment that runs in parallel with the operating system. The TOE is using FIPS 140-2 validated Qualcomm QTI Cryptographic Modules for hardware protection of keys and for cryptographic operations.

Xperia devices offer:

- Full disc encryption with 256-bit AES for all user data in the internal storage, as well as any external SD card.
- Key generation of symmetric and asymmetric keys.
- Import and export for both symmetric keys and asymmetric keys.
- Asymmetric and symmetric encryption and decryption with appropriate modes.
- Asymmetric signing and verification with digesting and appropriate padding modes.
- Generation and verification of symmetric message authentication codes.
- Random number generation used for generation of keys, Initialization Vectors, random padding and other elements of secure protocols that require randomness.

### *User Data Protection*

The Android security model for separation and access control is based in part on the concept of application sandboxes. It also uses the mandatory access control (MAC) provided by Security-Enhanced Linux (SELinux) to further define the boundaries of the Android application sandbox. MAC applies to all processes, even processes running with root/superuser privileges. Access control to devices include access to the following sensitive devices and functions are the following:

- Camera functions (picture and microphone)
- Location data (GPS)
- Bluetooth functions
- Telephony functions
- SMS/MMS functions
- Network/data connections (access and device information)

### *Identification and Authentication*

The TOE provides user authentication and require that users are authenticated before accessing certain protected functionality and data. Authentication is performed during booting of the device as well as during unlocking screen-locking. IT administrators can choose from a wide range of passcode requirements when deploying Xperia devices in a corporate environment.

### *Security Management*

The TOE supports several types of users:

- Primary – The first user added to a device which cannot be removed except by factory reset.
- Secondary – Any user added to the device other than the primary user.
- Guest – A guest user is a temporary secondary user with an explicit option to quick delete the guest user when its usefulness is over.
- Administrator – The administrator is acting remotely using a Mobile Device Management (MDM) system acting through an MDM-agent on the TOE. Neither the MDM nor the MDM-agent are parts of the TOE.

Device management functions include, installing and deletion of apps, changing the device settings, setting passwords, activating and deactivating Wi-Fi and Bluetooth, etc. Device management can be performed either locally on the mobile device or remotely using a MDM.

The TOE also supports the possibility to add policies restricting the use of certain features on a device, or to determine which features should be disabled or enabled. Security policies include e.g. encryption of the external SD card, disabling the camera and application blacklists and whitelists.

### *Protection of the TSF*

The TOE implements several different means for protection of the TSF:

- The TOE provides Address Space Layout Randomizer.
- Kernel-level application sandbox, enforcing security between applications and the system at the process level.
- Hardware protection of the Keystore.
- Full disk encryption which is a kernel feature that works at the block device layer.
- Secure boot and self-test.
- Possibility for the user to check software and firmware versions.
- Trusted update, which is performed by using Firmware Over the Air. The updates are secured by digital signatures which are validated via the Sony Security library.

### *TOE Access*

An unlocked TOE will transit into a locked state after a certain time of user inactivity. The time interval is configurable by the user and administrator. In a locked state the TOE will be able to display time and date, notifications, missed calls, text messages, signal strength and battery life. The level of information shown on the locked device is configurable by the user and the administrator.

The TOE can connect to wireless networks (WiFi), but is restricted only to connect to those networks that selected by the user or administrator. It is also possible to disable USB mass storage mode.

### *Trusted Path/Channels*

The TOE provide mutually authenticated and encrypted channels using 802.11-2012, 802.1X, EAPTLS, TLS to provide a communication channel between itself and another trusted IT product.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage Assumptions

The following assumptions about the usage are made:

A.CONFIG: It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

A.NOTIFY: It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.

A.PRECAUTION: It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

## 4.2 Clarification of Scope

The threats against the TOE defined in the Security Target are listed below:

T.EAVESDROP:

Network Eavesdropping

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints

T.NETWORK:

Network Attack

An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software update of any applications or system software on the device. These attacks also include malicious web pages or email attachments which are usually delivered to devices over the network.

T.PHYSICAL:

Physical Access

The loss or theft of the Mobile Device may give rise to loss of confidentiality of user data including credentials. These physical access threats may involve attacks which attempt to access the device through external hardware ports, through its user interface, and also through direct and possibly destructive access to its storage media. The goal of such attacks is to access data from a lost or stolen device which is not expected to return to its user. Note: Defending against device re-use after physical compromise is out of scope for this protection profile.

T.FLAWAPP:

Malicious or Flawed Application

Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally by its developer or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access. They may also conduct attacks against the platform's system software which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.

T.PERSISTENT:

Persistent Presence

Persistent presence on a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat in itself. In this case the device and its data may be controlled by an adversary at least as well as by its legitimate owner.

No Organisational Security Policies are defined in the Security Target:

# 5 Architectural Information

## 5.1 TOE Design

The TOE are the two smartphones Sony Xperia X and Sony Xperia X Performance. They both use Android version 6.0.1 (Marshmallow MR1). The kernel version is 3.18.20 in Xperia X Performance and the kernel version is 3.10.84 in Xperia X.

Xperia devices from Sony provide a multi-layer security architecture:

- System security - Xperia devices offer Linux kernel-level security from Android with Sony Mobile enhancements like Runtime integrity, HW and SW integrity and Secure Boot Chain.
- Secure storage - Devices are protected by passwords and data on the devices is encrypted.
- Network security - Transmissions are encrypted and Xperia devices have built-in support for industry-standard VPN protocols.
- Device security - Administrators can control the use of certain features or apps on devices, e.g. data from lost devices can be wiped.
- Digital certificates - Xperia devices support digital certificates to enable authentication and authorization of users connecting to corporate networks.

# 6 Documentation

The physical scope of the TOE also includes the following guidance documentation:

1. User guide Xperia™ X, F5122, [XperiaXGUIDE]
2. User guide Xperia™ X Performance, F8131, [XperiaXPerformanceGUIDE]
3. Common Criteria Guide for Xperia™ devices, [CCGUIDE]

# 7 IT Product Testing

The main part of the testing effort was performed at the atsec office in Stockholm, Sweden. The evaluators also traveled to the developers site in Lund, Sweden to perform some of the tests there.

## 7.1 Developer Tests

Not applicable.

## 7.2 Independent Evaluator Tests

Testing approach:

The test results from the independent testing are documented in the Assurance Activities Report (AAR).

The ST lists two different TOE devices:

- Sony Xperia X running on the Qualcomm platform: Snapdragon 650
- Sony Xperia X Performance running on the Qualcomm platform: Snapdragon 820

Configuration:

The evaluator configured the TOE and set up the test environment. The evaluator verified that the configured TOE and environment is consistent with the requirements of the ST. The evaluator used the following documentation during the installation and configuration of the TOE:

- Common Criteria Guide for Xperia devices: [CCGUIDE]
- User guide Xperia X F5121: [XperiaXGUIDE]
- User guide Xperia X Performance F8131: [XperiaXPerformanceGUIDE]

Coverage:

The evaluator has tested all SFR:s to ensure that the TOE behaves as specified in the ST and the guidance documentation as well as to perform tests described in the Protection Profile for Mobile Device Fundamentals.

Results

All evaluator test cases were completed successfully and recorded in the Assurance Activity Report. [AAR]

## 7.3 Penetration Tests

The evaluator performed a search of public domain sources to identify potential vulnerabilities in the TOE. The evaluator also provided an analysis of all applicable vulnerabilities and concluded that some vulnerabilities are applicable to the TOE. These applicable vulnerabilities are considered as residual.

The developer confirmed that the identified potential vulnerabilities are indeed applicable; therefore, penetration testing activities were not necessary. However these vulnerabilities are residual, i.e. not applicable to attackers possessing basic attack level.

# 8 Evaluated Configuration

The TOE is the mobile device delivered in an unbroken seal. In order to use the product in evaluated configuration, the product must be configured as specified in the manual Common Criteria Guide for Xperia devices document version 1.0, October 10 2016 [CCGUIDE].

## 8.1 Dependencies to Other Hardware, Firmware and Software

No additional hardware and software are needed for the TOE to reach its security goals. However, for being able to use the TOE in its intended way, the TOE will need SIM card and a subscription with a mobile operator, as well as access to a Google play account, most enterprise users will likely also use some sort of MDM system for the configuring and management of the TOE

# 9 Results of the Evaluation

The verdicts for the assurance classes and components are summarized in the following table:

| Assurance Class Name / Assurance Family Name | Short name (including component identifier for assurance families) | Verdict |
|---|---|---|
| Security Target Evaluation | ASE | Pass |
| ST Introduction | ASE_INT.1 | Pass |
| Conformance claims | ASE_CCL.1 | Pass |
| Security Problem Definition | ASE_SPD.1 | Pass |
| Security objectives for the operational environment | ASE_OBJ.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| Stated security requirements | ASE_REQ1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |
| Life-cycle support | ALC | Pass |
| Assurance activities for MDFPP | ALC_MDFPP.1 | Pass |
| Labeling of the TOE | ALC_CMC.1 | Pass |
| TOE CM coverage | ALC_CMS.1 | Pass |
| Timely Security Updates | ALC_TSU_EXT.1 | Pass |
| Development | ADV | Pass |
| Basic function specification | ADV_FSP.1 | Pass |
| Guidance documents | AGD | Pass |
| Assurance activities for MDFPP | AGD_MDFPP.1 | Pass |
| Operational user guidance | AGD_OPE.1 | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |
| Tests | ATE | Pass |
| Assurance activities for MDFPP | ATE_MDFPP.1 | Pass |
| Independent testing - conformance | ATE_IND.1 | Pass |
| Vulnerability assessment | AVA | Pass |
| Assurance activities for MDFPP | AVA_MDFPP.1 | Pass |
| Vulnerability assessment | AVA_VAN.1 | Pass |

# 10 Evaluator Comments and Recommendations

The developer identified a number of applicable vulnerabilities during the public domain search, however these vulnerabilities are considered as residual, i.e. not applicable to attackers possessing basic attack level.

The following vulnerabilities were found to be applicable for both models of the TOE:

CVE-2016-3863, CVE-2016-3861, CVE-2016-3821, CVE-2016-3820, CVE-2016-3819, CVE-2016-3862 and CVE-2016-0834-

The following vulnerabilities were found to be applicable for the Xperia X model:

CVE-2016-3840, CVE-2016-3822, CVE-2016-3743, CVE-2016-3742, CVE-2016-3763, CVE-2016-3741, CVE-2016-2508, CVE-2016-2507, CVE-2016-2506, CVE-2016-2505, CVE-2016-2464, CVE-2016-2463, CVE-2016-0841, CVE-2016-0839, CVE-2016-2428 and CVE-2016-2429

The TOE was evaluated and tested in the versions stated by the [ST]. Modification of TOE firmware/software/hardware will technically result in the operation of a non-certified product. This is due to the fact that the evaluation of the TOE cannot foresee whether such changes might affect the behavior of the evaluated security functionality. It is therefore the responsibility of the individual organization to determine their potential risks and benefits associated with installing newer product versions or modify TOE firmware/software/hardware that was not subject to this evaluation, and by doing so to deviate from the evaluated configuration that has been certified.

The evaluator notes that there are residual vulnerabilities in the TOE and that these vulnerabilities will be fixed by the developer according to the timely security update process described in the [ST] and the [AAR]. Sony Mobile deploys available patches as soon as possible and updates Xperia smartphones both directly to open-market devices and via carrier partners, so timings can vary by region and/or operator. Trusted updates are performed using Firmware Over the Air (FOTA). The developer signs the update package, uploads it to a distribution server and notifies the client that an update is available. The TOE user downloads the update and initiates the installation. After this step the TOE verifies the signature, checks that the version is newer than what is currently installed, verifies that the update supports the device model, and installs the update. If any of the steps before installation fails then the installation is aborted. The evaluator determined that the provided information in [ST] 10.5.6 "Software Firmware Control and Updates" fulfills the requirement in [MDFPP2] for ALC_TSU_EXT.1.

# 11 Certifier Comments and Recommendations

The certifier is aware of the occurrence of residual vulnerabilities in the TOE. The Security Functional Requirement (SFR) ALC_TSU_EXT.1 mandated in [MDFPP2] puts requirements on the TOE to securely manage software/firmware updates. The assurance activates for this SFR shows that Sony has implemented a firmware update program that will provide monthly security updates for the evaluated mobile devices.

As the threat landscape is shifting at a high pace, the current security level of the mobile devices can swiftly change, as new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. The certifier notes that for many scenarios a reasonable policy would be to keep products up to date with the latest version of the firmware/software. However, the benefit of installing firmware/software updates must be balanced with the potential risks that such changes might have unexpected effect on the behavior of the evaluated security functionality.

# 12 Glossary

| | |
|---|---|
| AAR | Assurance Activities Report |
| CAVS | Cryptographic Algorithm Validation Program |
| CC | Common Criteria |
| ITSEC | Information Technology Security Evaluation Criteria |
| EAL | Evaluation Assurance Level |
| MAC | Mandatory Access Control |
| MDM | Mobile Device Management |
| OSP | Organisational Security Policies |
| PP | Protection Profile |
| SELinux | Security-Enhanced Linux |
| SFR | Security Functional Requirements |
| ST | Security Target |
| TEE | Trusted Execution Environment |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSFI | TOE Security Functions Interface |
| WiFi | Wireless networks |

# 13 Bibliography


| | |
|---|---|
| [CCp1] | Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001 |
| [CCp2] | Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002 |
| [CCp3] | Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003 |
| [CEM] | Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004 |
| [ST] | ST Common Criteria Security Target for Sony Xperia, Sony Mobile Communications Inc., 2017-01-25, version 1.2 |
| [AAR] | Assurance Activity Report, atsec information security AB, 2016-10-26, version 1.0 |
| [CCGUIDE] | Common Criteria Guide for Xperia devices, Sony Mobile Communications Inc., 2016-10-01, version 1.0 |
| [MDFPP2] | Protection Profile for Mobile Device Fundamentals, NIAP, 2014-09-17, version 2.0 |
| [XperiaXGUIDE] | User guide Xperia X F5121, Sony Mobile Communications Inc., 2016-07-07 |
| [XperiaXPerformanceGUIDE] | User guide Xperia X Performance F8131, Sony Mobile Communications Inc., 2016-07-07 |

# Appendix A QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2016-01-26:

QMS 1.19.3 valid from 2016-05-30

QMS 1.20 valid from 2016-10-06

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.19.3” and “Ändringslista QMS 1.20”.

The certifier concluded that, from QMS 1.19.3 to the current QMS 1.20, there are no changes with impact on the result of the certification.