Vodafone Terminal Capability Definition

Appendix A Security TCD – Security Assessment Questions

Version: 8.0.0

Owner: **Rob Mitchell**
Authors: Rob Mitchell, Steve Babbage (VF Group R&D)

Security Assessment Questions[1]

1. **Does the phone allow Java MIDP2 applications to be installed after purchase?**
   (a) Yes
   (b) No
   If you answered Yes:
   - 1.1 Does the phone comply with *"The Recommended Security Policy for GSM/UMTS Compliant Devices"*?
     (a) Yes
     (b) No
   - 1.2 Regarding MIDP2 Operator Domain or Manufacturer Domain certificates to be installed on the phone:
     - 1.2.1 Will the Vodafone Operator Domain certificate be installed on the phone?
     - 1.2.2 Will any other Operator Domain or Manufacturer Domain certificates be installed on the phone? If so, which?
   - 1.3 Can the phone read the Vodafone root certificate from the SIM, if present?
     (a) Yes
     (b) No

2. **Does the phone allow unsigned *native code* (e.g. Symbian — *not* Java) applications to be installed after purchase?**
   (a) No — native code applications are not supported at all
   (b) No — only signed native code applications are allowed to be installed
   (c) Yes — but the user is prompted to accept or reject
   (d) Yes — the user is not prompted
   If you answered (b), (c) or (d):
   - 2.1 Which root certificates, that can be used to verify certificates for native code applications, will be installed on the phone?
   - 2.2 Does the phone use the Symbian operating system?
     (a) Yes
     (b) No
     If you answered Yes:
     - 2.2.1 Are you using a version of Symbian that incorporates Symbian Platform Security?

3. **Can the phone send binary SMS messages, of the kind that can change connection settings on the receiving phone (e.g. OMA Client Provisioning messages)?**
   (a) Yes
   (b) No

4. **A phone manufacturer will typically use essentially the same implementation of IMEI in several different phone models — it is typically common to all phones built on a given platform. Which of the following describes the IMEI implementation in this phone?**
   (a) The same implementation has been used in previous phones, for which IMEI reprogramming attacks already exist
   (b) The same implementation has been used in other phones, but only phones which have been on the market for less than six months; no IMEI reprogramming attacks are known. (Which other phones?)
   (c) The same implementation has been used in other phones which have been on the market for at least six months; no IMEI reprogramming attacks are known. (Which other phones?)
   (d) This is a new IMEI implementation, not used in any previous phone models

[1] Contact point for questions: Steve Babbage, Security Technologies Manager, steve.babbage@vodafone.com, tel +44 1635 676209

5. Have you signed up to the GSMA/EICTA IMEI Weakness Reporting and Correction Process[2]?

(a) Yes
(b) No

6. A phone manufacturer will typically use essentially the same implementation of SIMlock in several different phone models — it is typically common to all phones built on a given platform. Which of the following describes the SIMlock implementation in this phone?

(a) The same implementation has been used in previous phones, for which SIMlock unlocking attacks already exist
(b) The same implementation has been used in other phones, but only phones which have been on the market for less than six months; no SIMlock unlocking attacks are known. (Which other phones?)
(c) The same implementation has been used in other phones which have been on the market for at least six months; no SIMlock unlocking attacks are known. (Which other phones?)
(d) This is a new SIMlock implementation, not used in any previous phone models

7. Does the phone allow WAP Push Service Loading service type?

(a) Yes
(b) No

If you answered Yes:

7.1 Does the handset ask for user consent before making a WAP/TCP connection?
(a) Yes
(b) No

If you answered No:

7.1.1 Does the phone implement any type of PPG/SMSC white list to control unauthorised WAP Push of type service loading?
(a) Yes
(b) No

8. Does the phone operate in Bluetooth Security Mode 2?

(a) Yes
(b) No-It operates in Bluetooth Security Mode 3.
(c) No-it operates in Bluetooth Security Mode 1.
(d) No-It changes its behaviour between Mode 3 and 2 based on its “discoverable” status.

If you have answered Yes:

8.1 Please specify the Bluetooth profiles that are considered to be “non-secure”, i.e. do not require Bluetooth authentication. E.g. Object Push Profile, Service Discovery Profile, etc

---

9. Does the phone allow unpaired Bluetooth devices to download or upload data using Bluetooth profiles?

(a) Yes
(b) No

If you answered Yes:

9.1 Does the user need to manually accept (confirm) the download or the upload of data to the phone?
(a) Yes – and this user confirmation cannot be turned off.
(b) Yes – but the user can modify settings so as never to be prompted.
(c) Yes – the user cannot turn off this prompting altogether, but can turn off prompting when the connection is to particular specified Bluetooth devices.
(d) No

[2] EICTA CCIG Doc Ref: Eicta Doc: 04cc101
GSMA Doc Ref: IMEI Weakness and Correction Process 3.0.0
or see GSMA SG Doc 50/08

10. Does the phone allow unpaired Bluetooth devices to make phone calls or send/receive messages (SMS, MMS, etc) via Bluetooth?

(a) Yes – and no user confirmation is required.
(b) Yes – but user confirmation is required.
(c) No

11. Does the phone support Bluetooth SIM Access Profile?

(a) Yes
(b) No

If you answered Yes:

11.1 Does the phone itself generate 16 digit PINs?
(a) Yes
(b) No

11.2 Does the phone update existing link keys at every SAP Connection without PIN entry?
(a) Yes
(b) No
(c)

12. To the best of your knowledge, is the phone vulnerable to any of the publicly described Bluetooth attacks (e.g. Bluesnarfing, Chaos, Denial-of-Service, etc)?

(a) Yes
(b) No

If you answered Yes: Please specify the details below.

---

13. Which versions of the A5 encryption algorithm (A5/1, A5/2, A5/3) does the phone support?

14. Which versions of the GPRS encryption algorithm (GEA1, GEA2, GEA3) does the phone support?