CODENOMICON

**CONFIDENTIAL**

# ROBUSTNESS AND SECURITY ASSESSMENT

## for Mobile Phone Company XYZ!

## CODENAME handset test report for Mobile Phone Company XYZ

Performed: 1. – 30. October 2007
Delivered: 26. November 2007

Version 1.0.6



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## EXECUTIVE SUMMARY

This report documents the implementation and results of the off-site proof of concept robustness testing engagement made using Codenomicon test tools against the Mpbile Phone Company XYZ CODENAME handset equipment. The objective of this assignment was to execute full test runs of all applicable Codenomicon tools, against the handset and report total number of found flaws to be able to quantify the need of adding the robustness testing as integral part of Mobile Phone Company XYZ software development life cycle.

The assessment found over *hundred critical defects* from the tested Mobile phone company CODENAME handset. The defects were verified as real problems, causing denial-of-service and service disruption level problems having the potential of turning into costly *customer identified unique defects* affecting millions of mobile subscribers. These defects are such that they could manifest themselves without being explicitly exploited by for example handset receiving a badly formatted network message as part of normal operation. Furthermore it appears that many of the issues found during this assessment could be remotely triggered by a third party by e.g. sending malicious multimedia messages (MMS) to the victim who could in theory be anyone withing the reach of GSM or CDMA mobile network, anywhere in the world.

All errors reported were repeatable for the client to verify the problem as a valid error.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## SITE INFORMATION AND CONTACT DETAILS

The off-site proof of concept robustness testing engagement was performed at the Codenomicon offices in Boston, Massachusetts. The assessment was performed between 2007-10-01 – 2007-10-30.

The following on and off-site personnel took part in the assessment:

### Codenomicon

- AAA BBBB (nosuch@codenomicon.com), reporting and setup of engagement, execution of engagement
- CCC DDDD (nosuch@codenomicon.com), Sales Manager, North-America, observer

### Mobile Phone Company XYZ

- EEE FFFF (nosuch@example.invalid) - n/a
- GGG HHHH (nosuch@example.invalid) - n/a
- III JJJJ (nosuch@example.invalid), engagement setup and technical support.

Codenomicon wish to express special thanks to EEE FFFF who was instrumental in successful completion of the engagement. By providing Codenomicon with information and access to the tested device in an efficient and timely manner it was possible to carry out the engagement successfully.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## INTRODUCTION

Codenomicon has carried out a off-site proof of concept robustness testing engagement to demonstrate the power and effectiveness of its test suites for testing mobile handsets developed and marketed by Mobile Phone Company XYZ. Codenomicon test tools allow Mobile Phone Company XYZ to preemptively and efficiently harden its implementations against quality and security shortcomings before deploying the products to the marketplace. The objective of this assignment was to execute full test runs of all applicable Codenomicon tools, against the handset and report total number of found flaws. The assignment was carried out by Codenomicon personnel on the premises of Codenomicon Boston support office. Immediate benefits gained from executing the tests include:

- Identified critical defects
- Up-to-date information of real-life actual robustness, quality and implementation level security of tested platform

The results and recommendations are documented inside this document. The test environments, hardware and software versions used and the test configurations are included to this document to guarantee the reproduction of the test results.


Image 1.0 – CODENAME handset and
PANIC failure encountered during test execution.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## TEST VERDICTS

A verdict is assignment used in this report is described here. Possible verdicts are:

- ***Critical Failure***

  *Critical Failure's* are all failures that make the phone automatically
  - reset or restart
  - errors that cause it's operating system or applications to hang so that only way to recover is to remove the batter or push the power button for extended period of time
  - failures where user interaction from the UI is required to restart the subsystem on the phone are considered critical (example is e.g. Bluetooth subsystem which may crash as a result of a tests, and to resume Bluetooth operation, user would need to navigate to Bluetooth menu on handset and turn the service off and on to resume normal operation)

- ***Non-Critical Failure***

  *All other failures such as applications crashes etc. are considered non-critical failures.*

  Failure modes observed here include but are not limited to applications crashing on the handset (allowing restart of the application), sustained and non-sustained slowdowns and performance degradation issues and confusing or suspicious error messages displayed to the user.

  If no single test case can be pointed out, but anomalous behavior is observed from time to time or over a set of test cases, then the verdict is 'non critical *failure*' even though symptoms would alone make the test case a '*critical failure*'.

- ***Passed***

  Those test cases which are neither '*failures*' or '*critical failures'* are consider as passed.

For each found failure or critical-failure, no root cause analysis was performed since objective of this assignment was to "execute full test run against the handset and report total number of found flaws".



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## RESULTS

The results summarized herein document running the various Codenomicon Test Tools and test modules against following component:

Tested system: **Mobile Phone Company XYZ CODENAME handset**

Test results summary:

**CRITICAL FAILURES FOUND: 185**

**NON-CRITIAL FAILURES FOUND: 64**

See the Appendix A and Appendix B for test setup and test execution time details.

## CODENOMICON TEST TOOLS USED FOR THE TEST

Following Codenomicon test tools were used to carry out the engagement.

- Codenomicon Audio Test Tool 1.0 (11 test suites)
- Codenomicon Bluetooth Test Tool 1.4.1 (21 test suites)
- Codenomicon HTTP Client Test Tool 1.1
- Codenomicon Images Test Tool 1.1.2 (14 test suites)
- Codenomicon MPEG4 Test Tool 1.1 (3 test suites)
- Codenomicon TLS Client Test Tool 3.3.2
- Codenomicon Video Test Tool 1.0 (4 test suites)
- Codenomicon X.509 Test Tool 1.0.4

Following Codenomicon test tools could not be utilized for testing due to test setup limitations (in Mobile Phone Company XYZ development environment it should be straightforward to utilize them):

- Codenomicon IPv4 Test Suite (IP, UDP, TCP, ICMP, IGMP, ARP, IPSEC, MIPv4)
- Codenomicon IPv6 Test Suite (IP, ICMP, MLD, TCP, UDP, IPSEC)
- Codenomicon DNS Client Test Tool
- Codenomicon BOOTPC/DHCP Client Test Tool



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

As a future consideration, specifically in light of achieved results, we recommend the use of following future test suites by Codenomicon which are specifically designed for mobile handset testing:

- Codenomicon DRM test suite
- Codenomicon HTML test suite
- Codenomicon XML test suite
- Codenomicon CSS/CSS2 test suite
- Codenomicon Javascript test suite
- Codenomicon Java/JAR/Jad test suite
- Codenomicon SMS test suite
- Codenomicon MMS/SMIL test suite
- Codenomicon WMLC/WML test suite
- Codenomicon vCard test suite
- Codenomicon iCal/vCal test suite
- Codenomicon SMTP client test suite
- Codenomicon POP3 client test suite
- Codenomicon IMAP4 client test suite
- Codenomicon RFC2822 email + MIME test suite

By using all of the aforementioned test suites the external interfaces of the mobile handset are hardened to the point that attempts to attack the phone are very unlikely to succeed and phone becomes highly resilient to transient network errors and unexpected or malformed traffic and network messages causing robustness failures under normal operating conditions.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## TESTED SOFTWARE PACKAGES AND STACKS

The hardware and software details of the tested systems are documented in section. Any available software and hardware identifications during the evaluation are documented here to guarantee the reproducibility of the test results.

During the engagement the device(s) and hardware were being tested:

- Mobile Phone Company XYZ CODENAME handset

The tested devices ran the following software / operating system:

- Mobile Phone Company SUPPER OS (Menu->Version Information)

During the assessment the handset was updated with a newer OS version to allow tests for more interfaces be executed. The updated CODENAME handset provided following version information:




CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## SOFTWARE SECURITY

Nowadays, security problems plague the software products used to access the vast Internet. Operating systems, WWW-browsers, e-mail programs all have had their share of the reported problems. A significant portion of these vulnerabilities are robustness problems caused by careless or misguided programming. The Internet "underground community" searches for these flaws using non-systematic ad-hoc methods and publishes their results for "fun and profit". The large number of reported problems from some software packages can be explained by the huge attention they have received and, on the other hand, by the clearly the numerous flaws they contain. Although reports of serious damages caused by exploitation of these vulnerabilities are sparse, they pose a threat to the networked society. Security assessment of software by source code auditing is expensive and laborious. Methods for security analysis without access to the source code have been few and usually limited in scope. This may be one reason why many major software vendors have been stuck in the loop of fixing vulnerabilities that have been found in the wild and providing countless patches to their clients to keep the systems protected.

## ROBUSTNESS TESTING

The Codenomicon is developer of robustness testing method and tools. The robustness testing is based on systematic creation of a very large number of protocol messages (tens of thousands) containing exceptional elements simulating malicious attacks. The method provides a low-cost proactive way of assessing software robustness. The security assessment of a software component is based on robustness analysis of the component. Robustness is the ability of software to tolerate exceptional input and stressful environment conditions. A piece of software which is not robust fails when facing such circumstances. A malicious intruder can easily take advantage of robustness shortcomings to compromise the system running the piece of software. In fact, a large portion of information security vulnerabilities reported in the public are caused by robustness weaknesses. All robustness problems can be exploited by causing denial-of-service conditions by feeding the vulnerable component with maliciously formatted input. Often, a buffer overflow type of robustness flaw can be exploited to run externally supplied code in the vulnerable component. This report will only recognize this possibility, but not make judgment calls if any of the found issues could be exploited as such.

In addition to increased information security, software robustness promotes software quality in general. A robust piece of software has less bugs which increases user satisfaction and provides more undisturbed uptime. Robustness analysis provides



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

tools for assessing software quality as a complementary method with traditional process based quality systems and code audits. Robustness weaknesses are introduced during programming implementation) of the vulnerable software component. These kind of errors easily slip through ordinary code auditing and testing since robustness problems generally do not manifest themselves during normal operations. They become visible only when someone or something presents the implementation with a carefully constructed "malicious piece of input", or corrupted data.

The security assessment practiced by the Codenomicon is based on the systematic creation of a large set of exceptional input data fed into the tested component. The number of input data units causing problems provides a quantitative figure about the robustness, quality and information security of the component. As a short-term benefit for the customer, the assessment provides information to estimate the maturity of the tested software component. In the long-term, the assessment promotes awareness on the importance of solid programming practices among involved development units and subcontractors of the customer.

Also, the test tool is likely to find out various vulnerabilities that would be found by the "underground community" searching for vulnerabilities for "fun and profit". All this results in less information security problems to be found and reported after shipment of the assessed system.

See http://www.codenomicon.com/ for more information of robustness testing, and its applications.

## LIMITATIONS

The usual limitations for black-box testing and testing in general also apply to robustness analysis. Passing the analysis is in no way a certificate for a vulnerability free system. A complete security audit of a system requires many actions besides robustness analysis and must cover design of the system in general, usability, and other aspects. Robustness analysis can be used as a part of the complete audit or as a standalone method to provide an insight into the security and quality of the tested software component. In a typical case, the test cases are created for a specific subset of the chosen protocol and for specific types of errors. This means that only a portion of the system under test is exercised. Any available tools for code coverage metrics would provide information about the proportion of the software statements covered by the tests.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## EXPECTED RESULTS

Codenomicon Ltd. uses in-house tools and methods for producing the test cases used in the assessment. The software vulnerabilities that are found by the assessment are likely to be robustness problems caused by implementation-time mistakes (i.e. mistakes made during programming). Many of these mistakes are vulnerabilities from a security point of view. During testing these mistakes manifests their existence is various ways:

1. Crashing of the component, followed by possible restart.
2. Hanging of the component in a busy-loop where most CPU-time is wasted leading to a denial-of-service situation.
3. Failure of the component to provide useful services leading to a denial-of-service (e.g. network connections are refused).

In the programming language level the possible types of mistakes leading to robustness problems are numerous: missing length checks, pointer failures, index handing failures, memory allocation problems, threading problems, etc. Not all problems found have a direct security impact, but in any case their removal promotes reliability of the assessed software component.

## NOTES

Multimedia test tools (Audio, Video, Images) were executed only against the media player component. We however believe that if same image should be received over either HTTP or MMS bearer, the same outcome would occur due to use of lbrary decoding routines. Should e.g. MMS or web browser component use their own media decoding routines it is recommended to specifically run the multimedia test cases against the web browser and similar components on the mobile handset.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## CONCLUSIONS

The results of this engagement left no doubt about the usefulness and efficiency of Codenomicon testing technology in the Mobile Phone Company XYZ's testing environment. Furthermore, the ability to run the tests easily from any standard PC proves an advantage of our software-only solution over more fixed protocol testing solutions.

It is our recommendation that the Mobile Phone Company XYZ deploy the full Codenomicon Robustness Testing solution for the protocols specific to their environment, listed in the "Codenomicon test tools used for tests" section of this document. This will enable the Mobile Phone Company XYZ to take full advantage of our complete solution. Thus minimizing the risk of critical user identified defects or other similar field errors and improving the reliability and secure operation of future Mobile Phone Company XYZ mobile handsets.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## APPENDIX A – TEST SETUPS

Test setup and configuration details used during the engagement are presented in more detail below. The actual configurations ran inside the handset are not available for the purpose of writing this report.

### TEST SETUP #1 – Multimedia files

Test setup described by the figure 1.0 was used to execute the following tests:

- Codenomicon Audio Test Tool
- Codenomicon Images Test Tool
- Codenomicon Video Test Tool
- Codenomicon MPEG4 Test Tool

The media file format test materials were executed by extracting the files from the test tool into test workstations file system and uploading the contents to the handsets microSD card through USB cable. Supported audio and picture files could be tested using media player component automatically or semi-automatically (using next button) playing them. The media finder feature of the handset seemed to filter out some test cases. In development environment the test cases should be fed directly to the decoder stack bypassing the media finder functionality. Also any possible user interface automation tools should be deployed for automatizing the media file format test runs on target platform.

Following chart describes the multimedia formats used and target directories at the microSD card they were copied for letting the handset media finder to locate them:

| SDCard | Phone | Formats |
|---|---|---|
| \mobile\music | mediafinder\ringtones\sounds | MID, WAV |
| \mobile\audio | mediafinder\audio | MP3, AU, M4A |
| | mediafinder\voicenotes | AMR |
| | mediafinder\ringtones\sounds | IMY,MID,WAV |
| | mediafinder\ringtones\music | MP3, AU, M4A |
| | mediafinder\ringtones\voicenotes | AMR |
| \mobile\graphics | mediafinder\pictures | JPG |
| \mobile\picture | mediafinder\pictures | JPG, PNG, BMP,WBMP. GIF |
| | mediafinder\wallpaper\graphics | JPG |
| \mobile\video | mediafinder\videos | 3GP5, 3GP6 |

Chart A.1 – media file locations on handset mini SD card



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## TEST SETUP #2 – Tests over 2.5/3G

Test setup described by the figure A.2 was used to execute the following tests:

- Codenomicon HTTP Client Test Tool
- Codenomicon TLS/SSL Client Test Tool
- Codenomicon X.509 Test Tool

For these tests the test tools were executed at gw1.codenomicon.com. The web browser on the handset was configured to access this address via the 2.5/3G connection through AT&T / Cingular mobile network (proxy APN). Due to uncertainity over actual components in access and core networks, the running of e.g. IP test suites was not performed to avoid causing possible disturbances to AT&T mobile network. Should the handset had e.g. WiFi (IEEE 802.11a/b/g/n) connectivity, running these tests would had been significantly more straightforward.

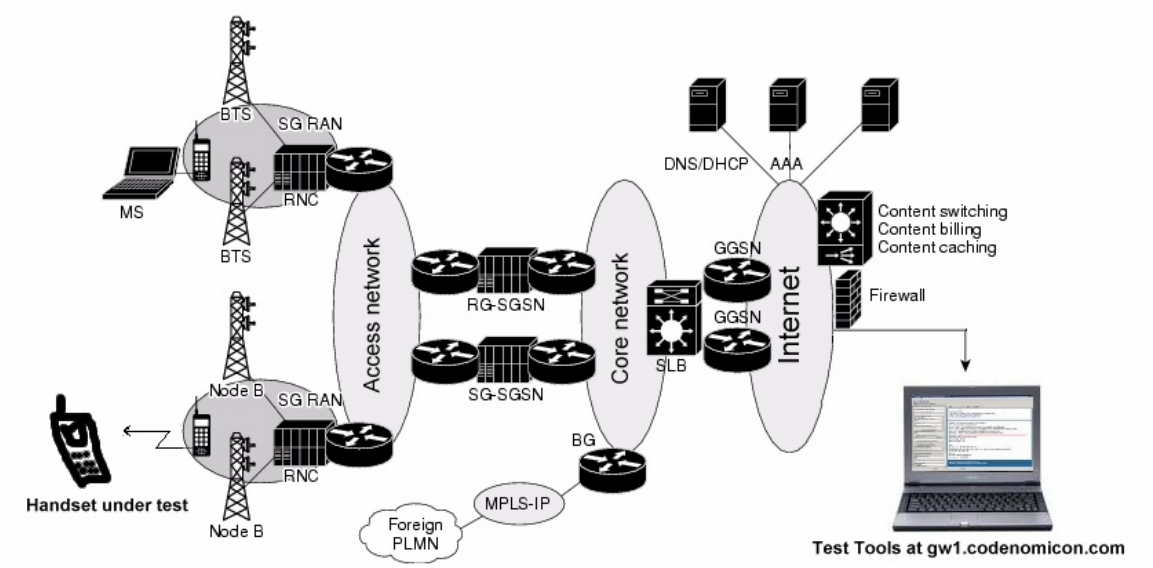


Figure A.2 – Test setup for 2.5G/3G tests



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

### TEST SETUP #3 – Bluetooth test suites

Test setup described by the figure A.3 was used to execute the following tests:

- L2CAP (Bluetooth Logical Link Control and Adaption Protocol)
- SDP (Bluetooth Service Discovery Protocol)
- RFCOMM (Bluetooth RFCOMM)
- DUN (Bluetooth Dial-up networking profile)
- HFP (Bluetooth Handsfree Audio Gateway Profile)
- HSP (Bluetooth Headset Profile)
- OPP (Bluetooth Object Push Profile)
- BIP (Bluetooth Imaging Profile)
- FTP (Bluetooth File Transfer Profile)
- AVRCP (Bluetooth AV-Remote Control profile)
- A2DP (Bluetooth Advanced Audio Distribution Profile)

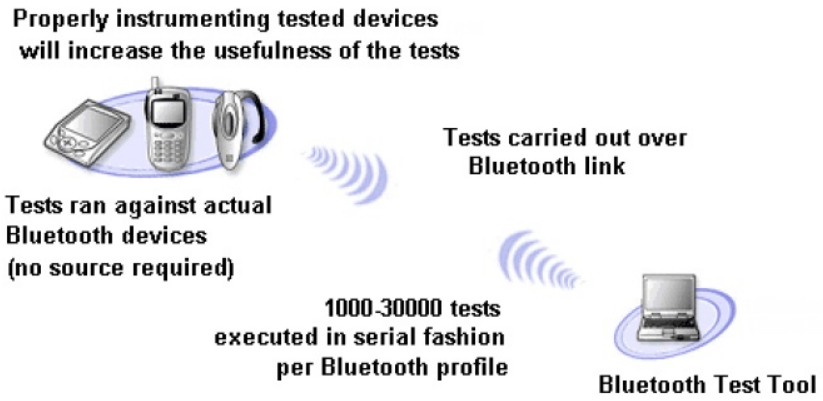


Figure A.3 - Test setup for Bluetooth tests

For running the Bluetooth test tools the handset was made discoverable and paired with the test tool. After pairing operation the automatic connection to the device without further verification was set to true on the handsets. This allowed automated and easy execution of the Bluetooth test suites against the tested devices.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## APPENDIX B – TEST EXECUTION TIMES

Test execution times for test materials vary greatly depending on the test material, amount of test cases included and means of automation capability of executing test cases at the DUT. Generally speaking more UI and other test automation capability there is, more the speed and regression reliability of the tests may be enhanced. To give idea as of how long executing various test suites will take, some example times for some test materials are given below. Note also that execution times are likely to be reduced when found flaws (if any) are fixed, and test execution does not pause for waiting the application or whole test subject to be restarted.

| Test suite | Test cases | Execution time | Notes |
|---|---|---|---|
| Bluetooth/SDP | 5935 | 21 min | Bluetooth test suites are quick and easy to setup and execute. |
| Bluetooth/FTP | 22932 | 255 min | (see above) |
| TLS/SSL Client | 13241 | 748 min | Due to lack of UI automation at DUT each test case has to be manually loaded via bookmark to the web browser component.´In development environment these tests could be sped up significantly |
| HTTP Client | 45801 | 1493 min | (see above) |
| Images/JPEG | 4827 | 116 min | With mediaplayer set to autoplay (options->picturesetup->slideinterval:1) |
| Audio/WAV | 4315 | 109 min | (see above) |

Chart B.1 – Sample test execution times against CODENAME handset

Chart B.1 reflects the time spent in running the test suites. On top of what is presented in chart B.1 the test setup and analysis on found issues will take significant time. Some estimates for test setup times are presented below:

- Multimedia test suites: 30minutes to 1 hour / test suite

  Includes time spent in extracting the test cases from test suite and copying them to the handset using SD card.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

- 3G/2.5G test suites: 30 minutes

  Includes time spent in setting up handset GPRS connectivity and creating bookmarks for phone to making testing easier.

- Bluetooth test suites: 30 minutes

  Includes time spent e.g. in installing Codenomicon Bluetooth hardware, installing drivers, pairing the phone with the test suite and otherwise setting the parameters such that testing may commence.

Fault/root cause analysis for each found flaw or suspicious behavior observed during test runs involved re-running a specific test case to verify if the bug may be reproduced using single test case only or if it requires multiple test cases to trigger. Time spent for verifying each bug as a real problem was around 2-5 minutes per found bug. Bluetooth and 2.5/3G test suites were in this regard slightly easier compared to multimedia test suites which were generally at the higher end of the margin due to way how they were fed to the multimedia browser in the handset.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com

## APPENDIX C – OTHER OBSERVATIONS

See Notes section. No other observations in regard to the test runs were made.



CODENOMICON Ltd.

Tutkijantie 4E
FIN-90570 OULU
FINLAND
+358 424 7431

101 Metro Drive, Suite 660
San Jose, CA 95110
UNITED STATES
+1 650 714 5460

info@codenomicon.com
www.codenomicon.com