SMT-W6100

Upgrade Procedure

Application Terminal Development
Network Division,
SAMSUNG ELECTRONICS CO.
3h Dec, 2005

- General Description
- Memory Map
- Output Package
- Service Network
- Upgrade Test Network
- Upgrade by Message
- Upgrade by MMI
- Upgrade by Console
- Appendix A
- Appendix B
- Appendix C

General Description

- SMT-W6100 is based on Linux platform so its boot area, kernel, root and phone applications partition use several file system types supported by Linux Operating System. Upgrade procedure is downloading a new image from Upgrade Server, erasing appropriate area and writing a downloaded new image to that area.
To do this, SMT-W6100 has an independent upgrade execution program.
This upgrade program first downloads upgrade configuration file which contains upgrade information(model number, date, version, partition/file name,size, checksum). After parsing this information and verifying digital signature if needed, SMT-W6100 starts downloading first image according to the configuration file. If all images to be upgraded are finished, SMT-W6100 reboots with new SW image. If there is network problem, disconnection or no response from Upgrade Server during downloading, SMT-W6100 reboot itself and start upgrade again., SMT-W6100 repeats upgrade procedure until succeeded.

General Description

- SW upgrade of SMT-W6100 can be accomplished by 3 different methods.

First, upgrade by upgrade message from the network.

Second, upgrade by Menu.

Third, upgrade by console CLI command.

Upgrade protocol uses FTP or HTTP.

At first time, upgrade program in r_normal start.

If upgrade by r_normal program finished without failure, phone restart with new sw.

If failed or there are remaining images or files to be upgraded, bootloader jump to upgrade program in r_upgrade instead of normal start.

And upgrade program in r_upgrade continues upgrading failed image or remaining images.

General Description

upgrade configuration file (wifiupgrade_6100.txt)

- Configuration file has some information about partition image blocks and files.

Configuration file is simple text file (block name, block size, checksum, ...)

Phone first request configuration file from Upgrade Server and parse block information.

Next, Phone request first block, check CRC and Flash memory erase and write.

Repeat above process until upgrading finished.

General Description

- upgrade configuration file (wifiupgrade_6100.txt)

  - CHKVER=no : Phone does not check version so upgrade total files in configuration lists.

```
WIFI PHONE UPGRADE CONFIGURATION

[INFORMATION]
MODEL=SMT-W6100
DOMAIN=BellSouth
VER=0.0.1
DATE=2005-12-09 13:02:30
CHKVER=yes

[LIST]
_BLK=k_upgrade
_MNT=none
_FILE=zImage_ug
_AUTH=1
_VER=1.0.0
_SIZE=843584
_CRC=0xe5d4b263

_BLK=r_upgrade
_MNT=none
_FILE=rootfs_ug.cramfs
_AUTH=1
_VER=1.0.0
_SIZE=958464
_CRC=0x9c945fd

_BLK=k_normal
_MNT=none
_FILE=zImage_nm
_AUTH=2
_VER=1.0.0
_SIZE=843584
_CRC=0xe5d4b263….
```

General Description

WiFi Phone check Version Info

- After receiving configuration file first, phone check its current version with version info of configuration file.
- If received version is different from that of current version, Phone start upgrading.

If not, upgrading does not start.

After Upgrading, Phone restart itself automatically without losing customer data.

General Description

Digital Signature

- Digital signing process meets TI requirement.

  - Key : 1024 bits ElGamal (public + private key)
  - Hashing Algorithm : SHA-1
  - Overall signature Algorithm : DSA

- Configuration file(text file) is digitally signed but SW image file(binary file) is not.

That's because Configuration file has information of SW image file, so configuration file encryption is enough for verifying certification.

- Signature file generated from configuration file using Private key is like this;

Public key is hard coded in Phone.

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.4 (Cygwin)

iD8DBQBBJRFZ5LgagZNJJRYRAlzIAKCiIxNWJU15NwhX6eZD/2mQ8CTlgQCfczIz
9nd/9RCF63hwhQw0/6ItwNY=
=Pk13
-----END PGP SIGNATURE-----
```

Memory Map

mtd block	partition name	partition size	image file name	upgradeable
0	bootitcm	16k	bootitcm,img	x
1	bootnand	64k	bootnand.img	x
2	ctrl	32k	ctrl.img	x
3	k_upgrade	1280k	zImage_ug	o
4	k_normal	1280k	zImage_nm	o
5	r_upgrade	1344k	rootfs_ug.cramfs	o
6	r_normal	2048k	rootfs_nm.cramfs	o
7	home	23552k	home.jffs2	o
8	phone	1280k	phone.cramfs	o
9	data	1872k	data.jffs2	x

- SMT-W6100 has 10 partitions.

Some critical partitions are not upgradeable by configuration file in normal case.

Phone main application sw, startbin is located in home partition.

Upgrade program is located in r_upgrade and r_normal partitions.

Upgrade program in both partitions has same functionality.

Pressing ‘u’(console) and power on, bootloader jumps to k_upgrade.

Just power on, bootloader jumps to k_normal.

Output Package

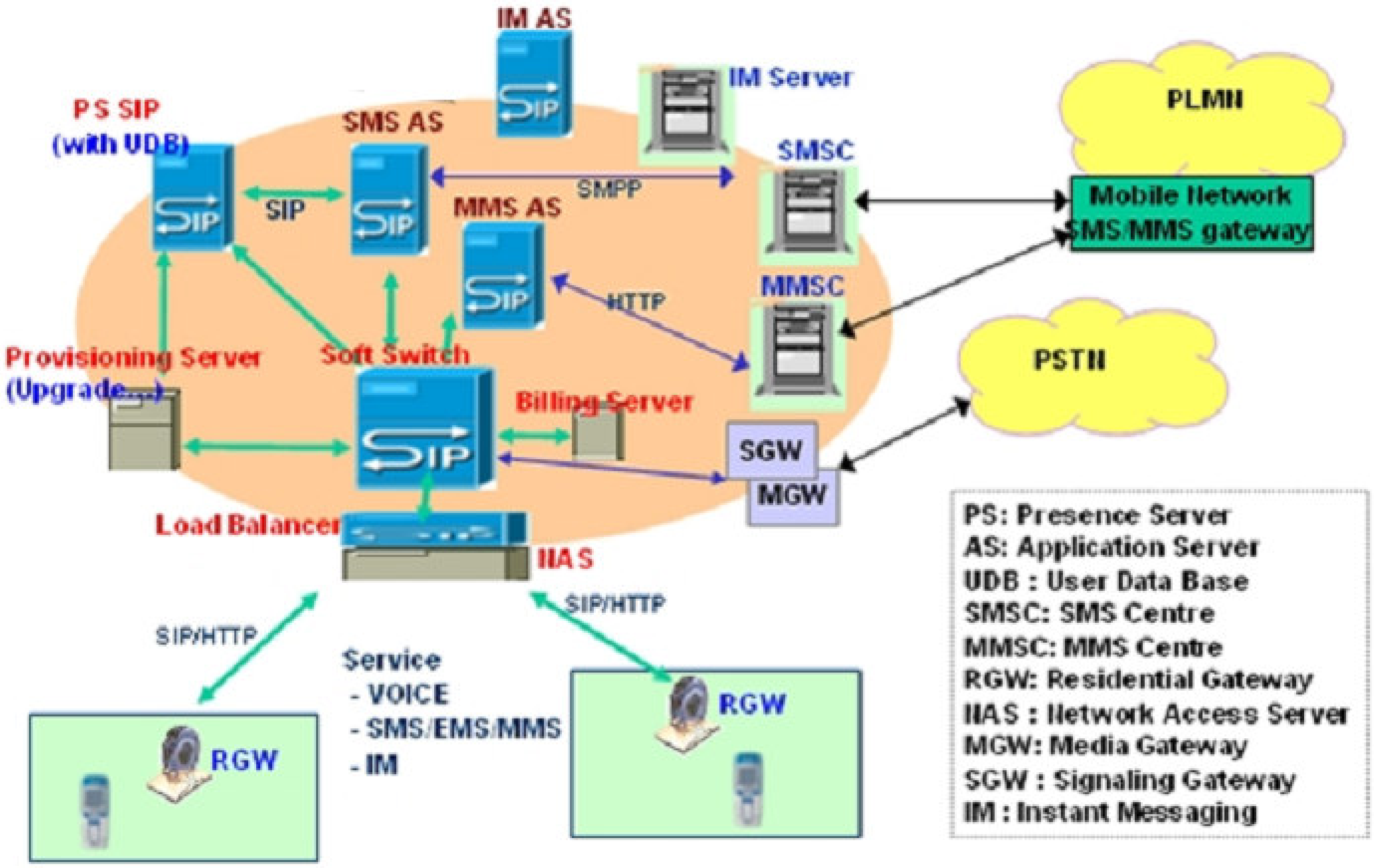
- Package is consists of following lists.

When new package releases, updated image among lists will be uploaded to Upgrade Server and phones will download from the Upgrade server.

```
ls -al /disk4/kubungi/SMT_W6100/pub/../pkg
total 37140
drwxrwxr-x    3 kubungi  kubungi      4096 Dec  6 16:09 .
drwxrwxr-x    9 kubungi  kubungi      4096 Nov 24 14:13 ..
-rw-rw-r--    1 kubungi  kubungi      9940 Dec  6 16:09 bootitcm.img
-rw-rw-r--    1 kubungi  kubungi     12464 Dec  6 16:09 bootnand.img
-rw-r--r--    1 kubungi  kubungi    147456 Dec  6 16:09 data.jffs2
-rw-r--r--    1 kubungi  kubungi  15679488 Dec  6 16:09 home.jffs2
-rw-rw-r--    1 kubungi  kubungi   1200128 Dec  6 16:09 phone.cramfs
-rw-rw-r--    1 kubungi  kubungi   1875968 Dec  6 16:09 rootfs_nm.cramfs
-rw-rw-r--    1 kubungi  kubungi    958464 Dec  6 16:09 rootfs_ug.cramfs
-rw-rw-r--    1 kubungi  kubungi       769 Dec  6 16:09 wifiupgrade_6100.txt
-rwxrwxr-x    1 kubungi  kubungi    843584 Dec  6 16:09 zImage_nm
-rwxrwxr-x    1 kubungi  kubungi    843584 Dec  6 16:09 zImage_ug
```

Service Network

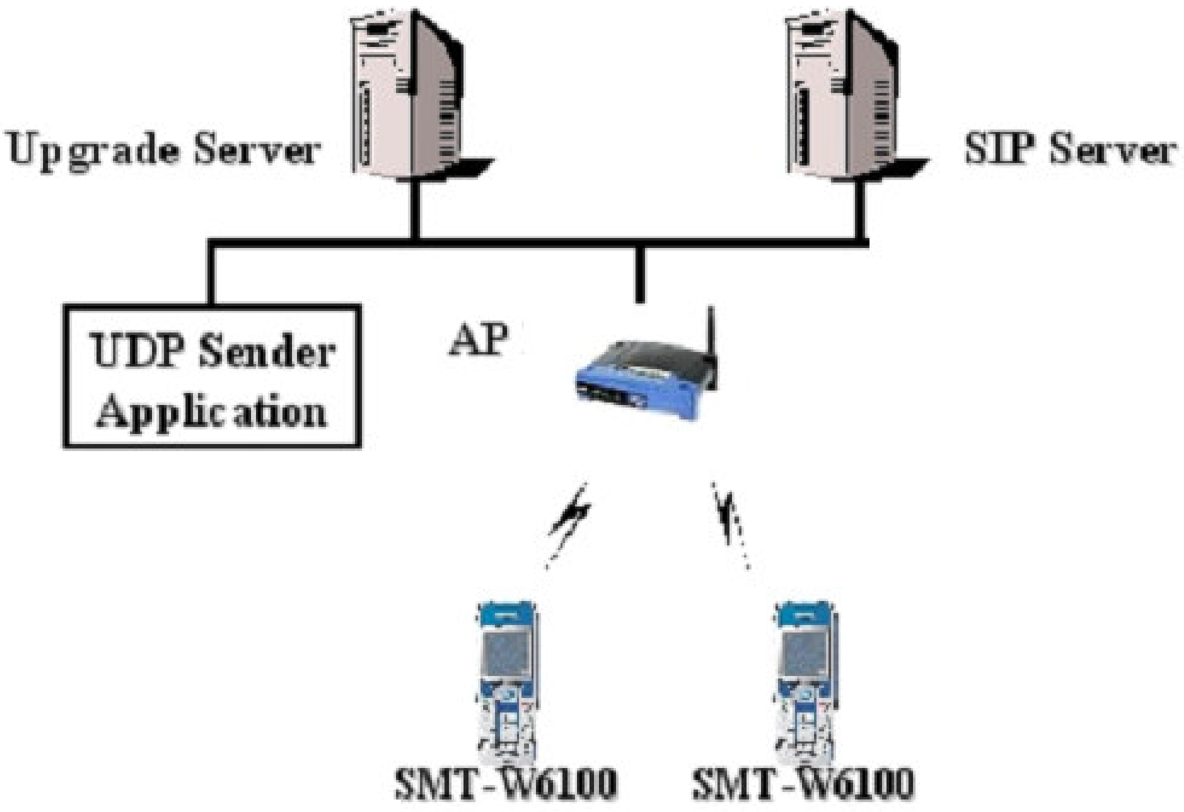
- Service Network



PS: Presence Server
AS: Application Server
UDB : User Data Base
SMSC: SMS Centre
MMSC: MMS Centre
RGW: Residential Gateway
NAS : Network Access Server
MGW: Media Gateway
SGW : Signaling Gateway
IM : Instant Messaging

Upgrade Test Network

- Local Upgrade Network



Upgrade by Message

Not fixed

Upgrade Procedure

- SIP Registration
- SMS to WiFi Phone
- WiFi Phone check Version Info
- Image Configuration file
- Digital Signature
- Download Flow
- Failure during Downloading

Upgrade by Message

Not fixed

SIP Registration

- WiFi Phone send to Network Server Information about its SW, FW release

The detailed format must be: (x is numeric)

User-Agent : Samsung / HW_Vx.x.x / FW_Vx.x.x / SW_Vx.x.x

For example;

```
REGISTER sip:168.219.148.225 SIP/2.0
From: <sip:3003@168.219.148.225>;tag=a8db91f9-13c4-174-5b874-3e2
To: <sip:3003@168.219.148.225>
Call-ID: a8db91f9-13c4-174-5b865-60d7
CSeq: 5 REGISTER
Via: SIP/2.0/UDP 168.219.145.249:5060;branch=z9hG4bK-2aa-a744f-1deb
Max-Forwards: 70
User-Agent: Samsung / HW_V0.3.0 / FW_V0.1.2 / SW_V0.2.0
Contact: <sip:3003@168.219.145.249:5060>
Expires: 60
Content-Length: 0
```

Upgrade by Message

Not fixed

SMS to WiFi Phone

- Network Server send SMS with the XML format:

XML format:

```
<sdc>
        <firmware-download url="http://[A]:[B]/[C]">
</sdc>
<tag-name>
        <version info = FW_Vx.x.x / SW_Vx.x.x>
</tag-name>
```

http : In case of using ftp, replace http to ftp.

***[A] : Upgrade Server IP Address or URL**

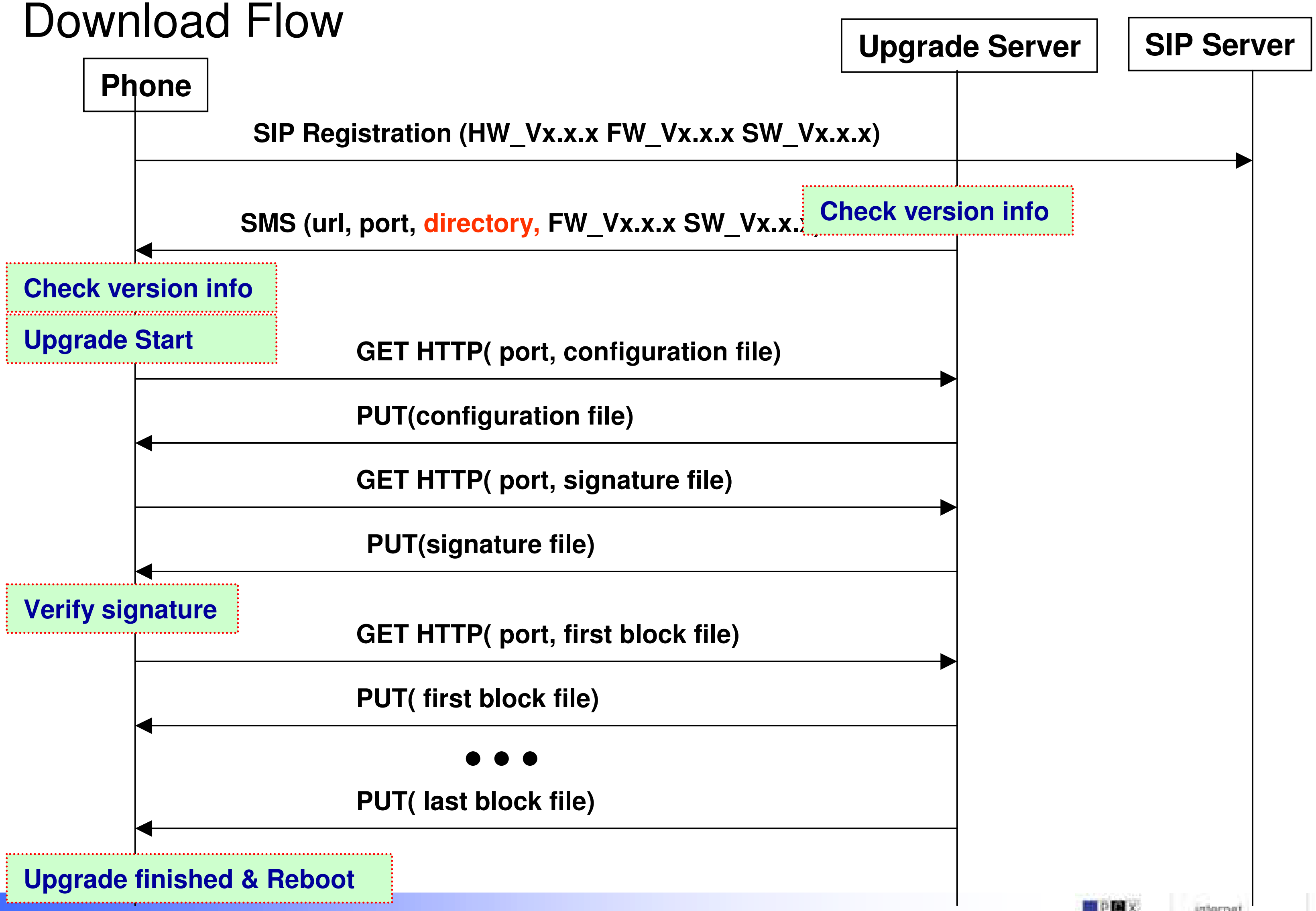
***[B] : Option : HTTP Port Number (if omitted, well known port(80) will be used by Phone)**
In case of ftp, port number is 21 and login by anonymous.

***[C] : upgrade directory**

Upgrade by Message

Not fixed

- Download Flow



Phone

Upgrade Server

SIP Server

SIP Registration (HW_Vx.x.x FW_Vx.x.x SW_Vx.x.x)

Check version info

SMS (url, port, directory, FW_Vx.x.x SW_Vx.x.x)

Check version info

Upgrade Start

GET HTTP(port, configuration file)

PUT(configuration file)

GET HTTP(port, signature file)

PUT(signature file)

Verify signature

GET HTTP(port, first block file)

PUT(first block file)

● ● ●

PUT(last block file)

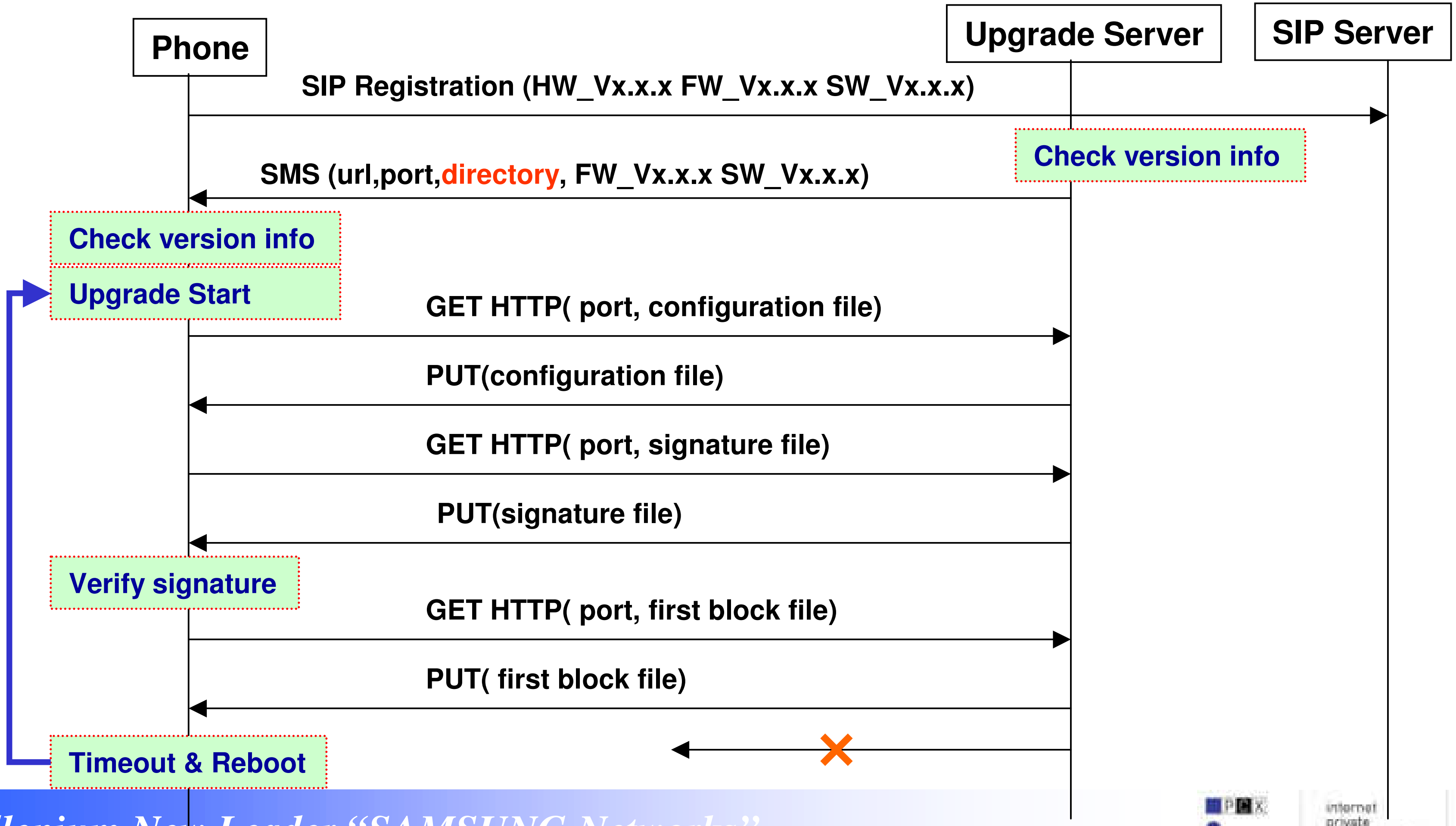
Upgrade finished & Reboot

Upgrade by Message

Not fixed

Failure during downloading (1/2)

- If there is network problem, disconnection or no response from Upgrade Server during downloading, Phone reboot itself and start upgrading again.



Phone

Upgrade Server

SIP Server

SIP Registration (HW_Vx.x.x FW_Vx.x.x SW_Vx.x.x)

Check version info

SMS (url,port,directory, FW_Vx.x.x SW_Vx.x.x)

Check version info

Upgrade Start

GET HTTP(port, configuration file)

PUT(configuration file)

GET HTTP(port, signature file)

PUT(signature file)

Verify signature

GET HTTP(port, first block file)

PUT(first block file)

Timeout & Reboot

Upgrade by Message

Failure during downloading (2/2)

- Does the phone need the service message from the Network Server to start upgrading again or does it do it by itself? If the upgrade server is unavailable for some hours after the failure during downloading, does the phone work?

There are two cases

1. If Phone receive first Image block, and occur problem without erasing first flash memory area → The Phone display failure on LCD and reboot as normal process.
   : The Phone works.
2. If Phone receive first image block and erase flash memory area, after then occur problem → The Phone's one of SW image already been erased so jump to upgrade program again until upgrading is finished. : The Phone repeat upgrading process never to return until upgrading succeed.

Upgrade by MMI

Upgrade by Menu

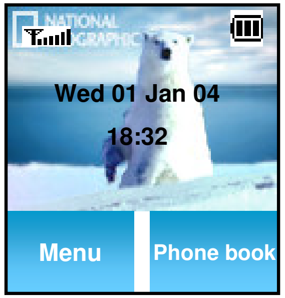
- Upgrade by MMI works almost same with Message upgrade.

But MMI upgrade has more choice of selecting upgrade target.

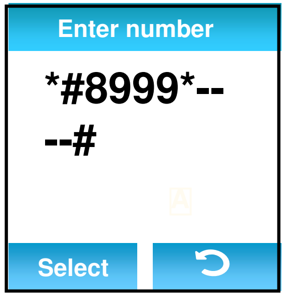
It is possible to upgrade Total package as well as one partition or one file

Upgrade by MMI

Upgrade by TestMenu : Env Settings



Main Window



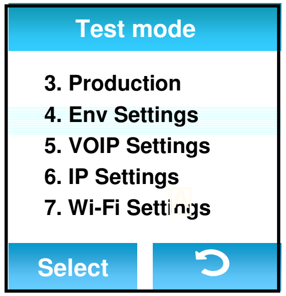
Enter " *#8999* 8378# " (Test mode key sequence)

Last four digits will be encrypted (displaying symbol "-")

Or

Enter ""*#8999*2585#"(Env Settings menu key sequence)

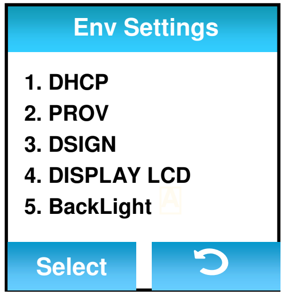
for direct access to the Env Settings menu



Among Test mode items, Env Settings

Upgrade by MMI

Upgrade by TestMenu : Env Settings



[Env Settings menu]

1. DHCP : DHCP enable flag
2. PROV : PROVISIONING enable flag

- DISGN : DIGITAL SIGNATURE enable flag

- DHCP

If [DHCP] flag is on, All IP network parameters will be received from DHCP Server.

If Your Network does not support DHCP, set [IP Addr], [Gateway Addr], [Netmask], [DNS IP] manually at IP Settings menu.

- PROV

Provisioning will received OutBoundProxy IP, SIPKey, and CLI from Residential GateWay according to the provisioning flow.

If your Network does not support Provisioning, turn off [PROV] flag, set [Proxy IP Addr] manually at VOIP Settings menu.

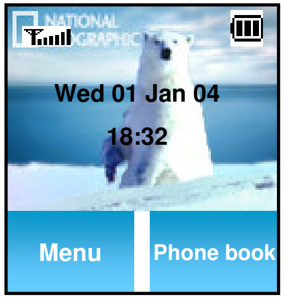
- DSIGN

Digital Signature is used for verification that the received upgrade files from Upgrade Server is trusted by TI.

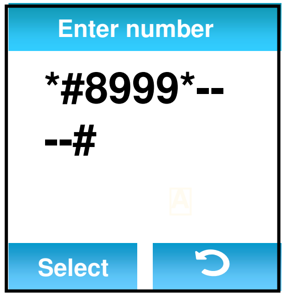
If your Network does not support Digital Signature, turn off [DSIGN] flag.

Upgrade by MMI

Upgrade by TestMenu : IP Settings



Main Window



#8999--
--#

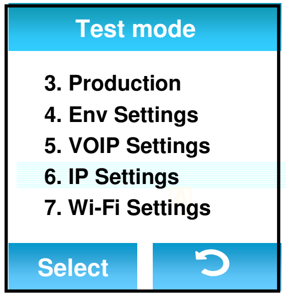
Enter “ *#8999* 8378# “ (Test mode key sequence)

Last four digits will be encrypted (displaying symbol “-”)

Or

Enter “*#8999*2581#”(IP Settings menu key sequence)

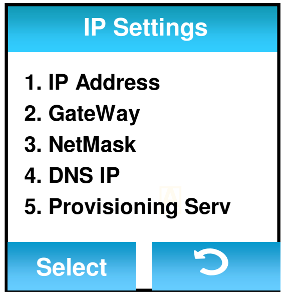
for direct access to the IP Settings menu



Among Test mode items, IP Settings

Upgrade by MMI

- Upgrade by TestMenu : IP Settings

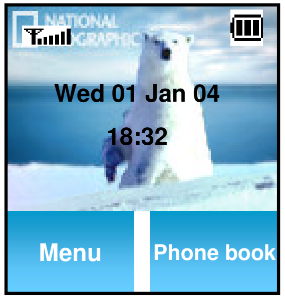


[IP Settings menu consists of 6 items]

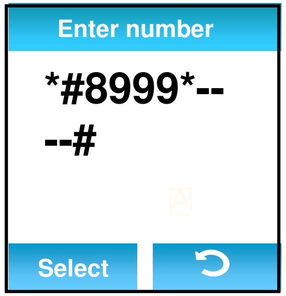
1. IP Address : WiFi Phone IP Address
2. GateWay : WiFi Phone Gateway IP Address
3. Netmask : WiFi Phone NetMasks
4. DNS IP : Domain Name Server for URL Query
5. Provisioning Server IP : Residential GateWay IP Address
6. Upgrade Server IP :Upgrade Server IP Address or URL

Upgrade by MMI

Upgrade by TestMenu : Upgrade Settings



Main Window



#8999----#

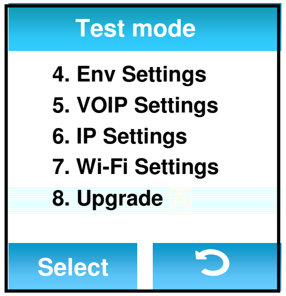
Enter “ *#8999* 8378# “ (Test mode key sequence)

Last four digits will be encrypted (displaying symbol “-”)

Or

Enter ““*#8999*2582#”(Upgrade menu key sequence)

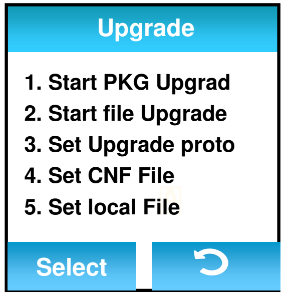
for direct access to the Upgrade menu



Among Test mode items, Upgrade

Upgrade by MMI

Upgrade by TestMenu : Upgrade Settings



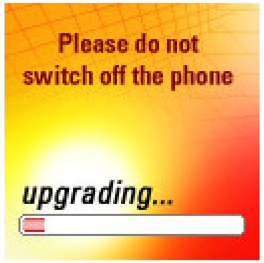
Upgrade

1. Start PKG Upgrad
2. Start file Upgrade
3. Set Upgrade proto
4. Set CNF File
5. Set local File

Select

[Upgrade menu]

1. Start PKG Upgrade : PKG Upgrade Start
2. Start file Upgrade : file Upgrade Start
3. Set Upgrade protocol : HTTP or FTP
4. Set CNF File : Upgrade Configuration File name(ex,wifiupgrade_6100.txt)
5. Set local File : upgrade local File name(ex, startbin)
6. Server Login ID : Upgrade Server Login ID
7. Server Login Passwd : Upgrade Server Login Password
8. Directory Path : Upgrade File Directory path of Upgrade Server



Please do not switch off the phone

upgrading...

1. Start PKG Upgrade

If you need to upgrade partition area,
select this menu(you should set 4. Set CNF File)

2. Start file Upgrade

If you need to upgrade file only(for example startbin),
select this menu(you should set 5. Set local File)

Upgrade by MMI

Upgrade by HTTP Summary

- **Using HTTP**

1. **Check All Settings(env settings, IP settings, Upgrade menu) are correct.**
2. **If your Network does not support DNS, set [Upgrade Server Addr] as IP not URL.**
3. **Set [Set Upgrade Protocol] as HTTP.**
4. **In case of PKG Upgrade, set [Set CNF File] name.**
5. **In case of file Upgrade, set [Set local File] name.**
6. **No need to set [Server Login ID] and [Server Login Passwd].**
7. **Set [Directory Path].**
8. **In case of Main Upgrade, select [Start PKG Upgrade].**
9. **In case of Sub Upgrade, select [Start file Upgrade].**

Upgrade by MMI

Upgrade by FTP Summary

- **Using FTP**

1. **Check All Settings(env settings, IP settings, Upgrade menu) are correct.**
2. **set [Upgrade Server Addr] as IP(FTP does not use DNS).**
3. **Set [Set Upgrade Protocol] as FTP.**
4. **In case of PKG Upgrade, set [Set CNF File] name.**
5. **In case of file Upgrade, set [Set local File] name.**
6. **Set [Server Login ID] and [Server Login Passwd].**
7. **Set [Directory Path].**
8. **In case of PKG Upgrade, select [Start PKG Upgrade].**
9. **In case of file Upgrade, select [Start file Upgrade].**

Upgrade by Console

Execute Upgrade program

- Upgrade program located in r_upgrade and r_normal partitions but having almost the same functionality.

Upgrade program in r_upgrade partition is “upgrade” and in r_normal partition is “upgrade2”.

“Upgrade” can’t upgrade itself(k_upgrade, r_upgrade partition).

“Upgrade2” can’t upgrade k_normal and r_normal partitions.

Just writing file name will show help.

If you want to upgrade partition first check that the wifiparam , upgradeparam and networkparam are configured correctly.(see Appendix.A)

Third argument must be one of partition name or file name you want to upgrade.

(k_upgrade, r_upgrade, k_normal, r_normal, home, phone, startbin)

For example;

```
>./upgrade2 start r_upgrade  noreboot
```

Upgrade by Console

- Execute Upgrade program

```
# ./upgrade2 start r_upgrade noreboot
Jan  1 00:38:11 UPGRADE2: UPGRADE START :
2291.51 2262.60
>>> openLcd()
mmap returned pointer: 0x40093000
Start  draw_Image!!
Jan  1 00:38:11 UPGRADE2: /usr/bin/killall -9 startbin
killall: startbin: no process killed
Jan  1 00:38:11 UPGRADE2:  FIXME!!!!
wlconfigapi (47): lo found
wlconfigapi (47): eth0 found
wlconfigapi (47): Wireless interface found: 'eth0'(2).
wlconfigapi (47): Wireless interface MAC: 00:02:00:16:A1:07.
...
...
...
Jan  1 00:38:17 UPGRADE2: UPGRADE>FIXME!!! ComposeDns
Jan  1 00:38:17 UPGRADE2: >>> BuildUrl : download
url=ftp://down:down@165.213.109.142/down/smt/
Connecting to 165.213.109.142[165.213.109.142]:21
rootfs_ug.cramfs     100% |*****************************|   936 KB    --:-- ETA
Erasing 16 Kibyte @ 14c000 -- 98 % complete.
1872+0 records in
1872+0 records out
```

Appendix A

Setup Parameters

- Before execute upgrade program by console command, check wifiparam, upgradeparam and networkparam.

>./upgrade2 changewifi

```
# ./upgrade2 changewifi
        SSID                [Alice-SEC.www.com   ] : Alice-SEC.www.com
UPGRADE> Upgrade Info Right ? (y/n) => y
#
```

Appendix A

Setup Parameters

>./upgrade2 changeupgrade

```
# ./upgrade2 changeupgrade
Upgrade Protocol(ftp:f, http:h)=>f
use FTP.
        Server IP          [                ] : 165.213.109.142
        Port                0                 : 21
        Config File        [                ] : wifiupgrade_6100.txt
        Login              [                ] : down
        Passwd             [                ] : down
        Directory Path     [                ] : /down/smt
Use digital signature(y/n)=>n
Digital Signature Verification Skip.
===== UPGRADE INFORMATION ================
UPGRADE> Protocol FTP
UPGRADE> Server IP      : 165.213.109.142
UPGRADE> Port    : 21
UPGRADE> Config File     : wifiupgrade_6100.txt
UPGRADE> Login          : down
UPGRADE> Passwd          : down
UPGRADE> DirPath        : /down/smt
UPGRADE> DGSIGN  : OFF
==========================================
UPGRADE> Upgrade Info Right ? (y/n) => y
#
```

Appendix A

Setup Parameters

>./upgrade2 changenetwork

```
# ./upgrade2 changenetwork
        IP Addr          [165.213.109.21     ] : 165.213.109.21
        Netmask            [255.255.255.0      ] : 255.255.255.0
        Gateway            [165.213.109.1      ] : 165.213.109.1
Use DHCP(y/n)=>n
DHCP Skip.
Use DNS1(y/n)=>n
DNS1 Skip.
Use DNS2(y/n)=>n
DNS2 Skip.
Use DNS3(y/n)=>n
DNS3 Skip.
Network Info Right ? (y/n) => y
[NCC] ifAddrSet
[NCC] ifMaskSet
SIOCSIFADDR: Invalid argument
[NCC] routec
>>>route add default gw 165.213.109.1
route: SIOC[ADD|DEL]RT: File exists
#
```

Appendix B

- SW Local Download Simulation

It is possible to simulate upgrade message reception and upgrade procedures.

1. Use [UDP send program] to generate SMS and send to WiFi Phone.

2. Receiving sms, WiFi Phone display message whether upgrade SW or not.

3. User select Ok soft key, then upgrade start.

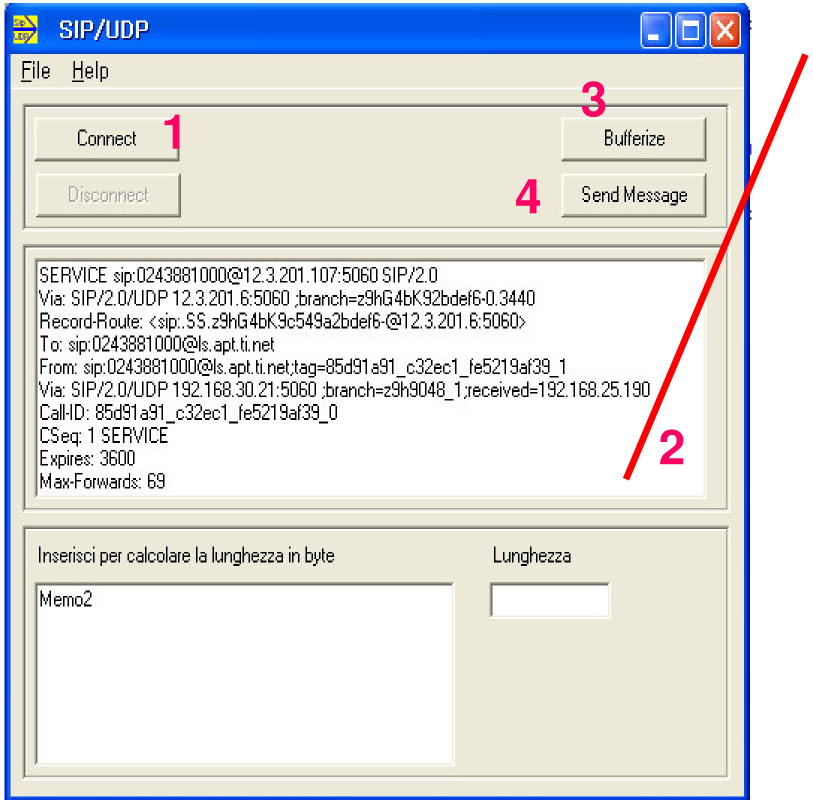
4. Upgrade time is varied according to network speed.

   About 5 minutes enough for upgrade in case of 300kbps download speed of Main SW. (16Mbytes)

5. If upgrade fails during upgrading, WiFi Phone retry upgrade procedure until success.

Appendix B

[UDP send program]



```
SERVICE sip:0243881000@12.3.201.107:5060 SIP/2.0
Via: SIP/2.0/UDP 12.3.201.6:5060 ;branch=z9hG4bK92bdef6-0.3440
Record-Route: <sip:.SS.z9hG4bK9c549a2bdef6-@12.3.201.6:5060>
To: sip:0243881000@ls.apt.ti.net
From: sip:0243881000@ls.apt.ti.net;tag=85d91a91_c32ec1_fe5219af39_1
Via: SIP/2.0/UDP 192.168.30.21:5060 ;branch=z9h9048_1;received=192.168.25.190
Call-ID: 85d91a91_c32ec1_fe5219af39_0
CSeq: 1 SERVICE
Expires: 3600
Max-Forwards: 69
```

[SIP/UDP Message]

```
SERVICE sip:0243881000@12.3.201.107:5060 SIP/2.0
Via: SIP/2.0/UDP 12.3.201.6:5060 ;branch=z9hG4bK92bdef6-0.3440
Record-Route: <sip:.SS.z9hG4bK9c549a2bdef6-@12.3.201.6:5060>
To: sip:0243881000@ls.apt.ti.net
From:
sip:0243881000@ls.apt.ti.net;tag=85d91a91_c32ec1_fe5219af39_1
Via: SIP/2.0/UDP
192.168.30.21:5060 ;branch=z9h9048_1;received=192.168.25.190
Call-ID: 85d91a91_c32ec1_fe5219af39_0
CSeq: 1 SERVICE
Expires: 3600
Max-Forwards: 69
Content-Transfer-Encoding: xml
Content-Type: application/x-ti-sdc+xml
Content-Length: 44

<?xml version="1.0" encoding="ISO-8859-1"?>
<xml >
                <sdc>
        <firmware-download url="http://192.168.1.9/down">
    </sdc>
•</xml >
```

Execute "message.exe" program

1. Connect to WiFi Phone(IP address and port:5060)
2. Copy SIP message(change upgrade server IP and configuration file name)
3. Buffering message
4. Send message to WiFi Phone

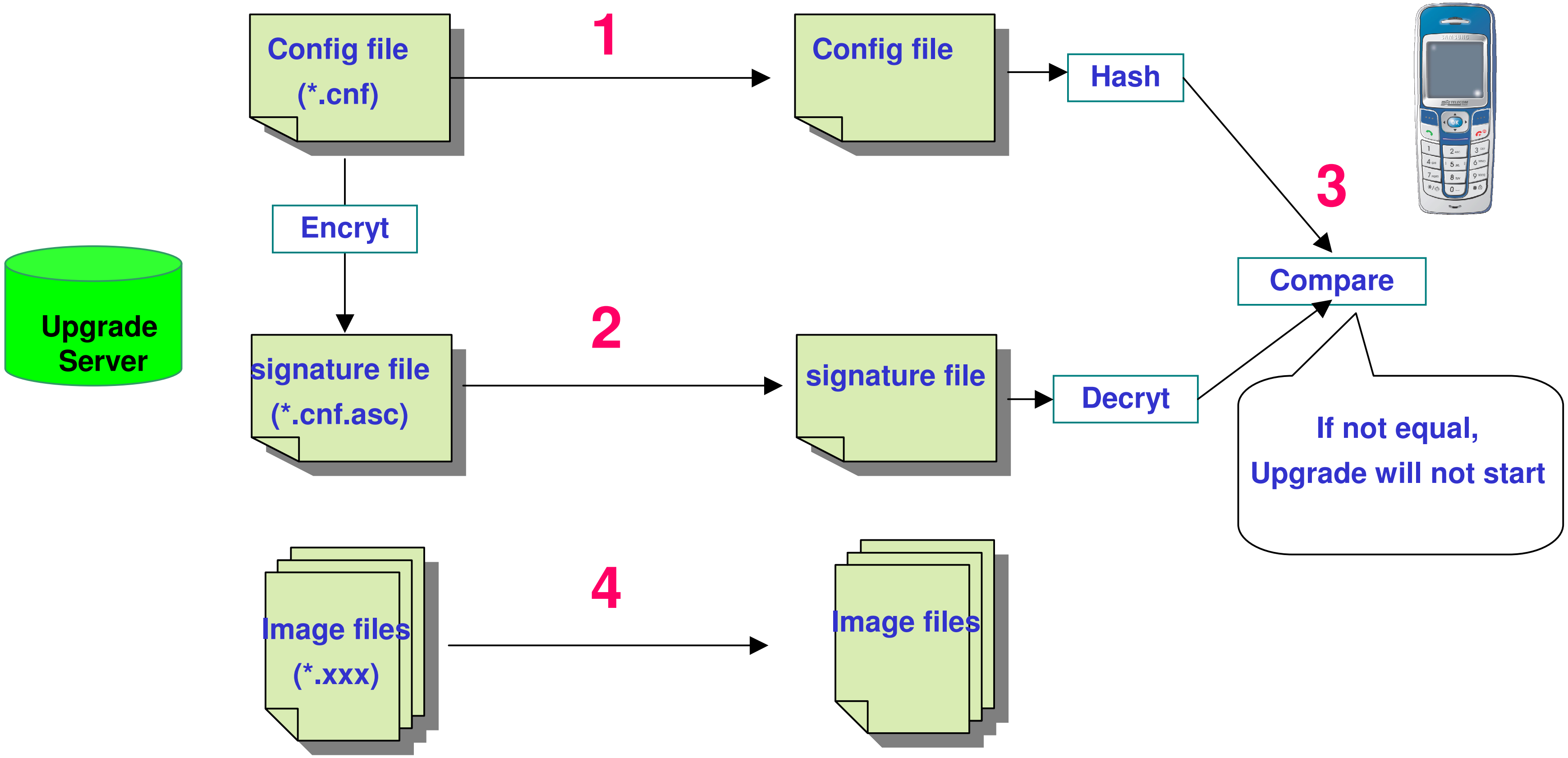
Appendix C

- **Digital Signature**

Key : 1024 bits ElGamal(public + private key)

Hashing algorithm : SHA-1

Overall signature algorithm : DSA


Upgrade Server
Config file (*.cnf)
1
Config file
Hash
3
Encryt
Compare
signature file (*.cnf.asc)
2
signature file
Decryt
If not equal,
Upgrade will not start
Image files (*.xxx)
4
Image files