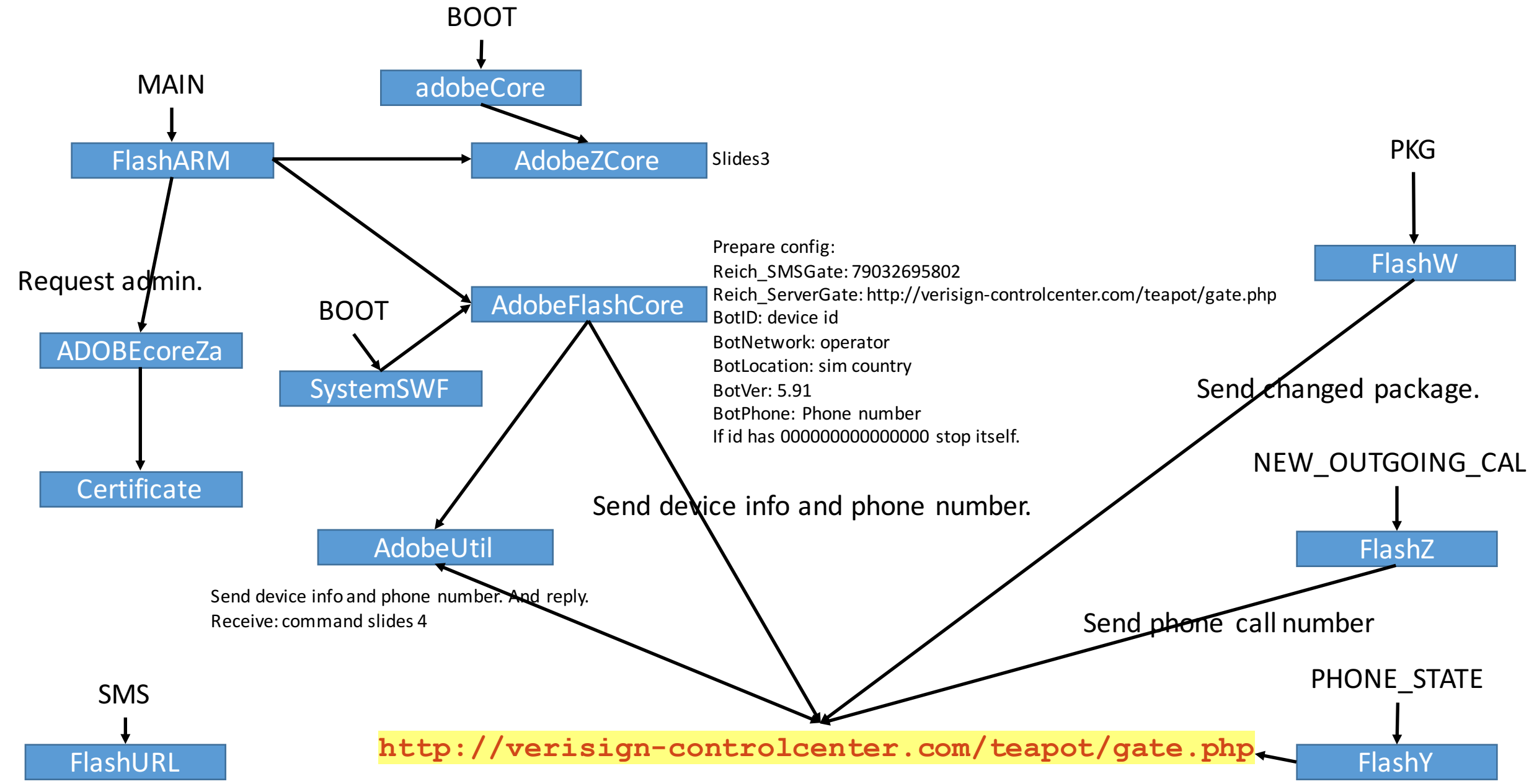
Svpeng Variety1


BOOT
adobeCore
MAIN
FlashARM
AdobeZCore
Slides3
PKG
FlashW
Request admin.
ADOBEcoreZa
BOOT
SystemSWF
AdobeFlashCore
Prepare config:
Reich_SMSGate: 79032695802
Reich_ServerGate: http://verisign-controlcenter.com/teapot/gate.php
BotID: device id
BotNetwork: operator
BotLocation: sim country
BotVer: 5.91
BotPhone: Phone number
If id has 000000000000000 stop itself.
Send changed package.
Certificate
NEW_OUTGOING_CALL
Send device info and phone number.
AdobeUtil
FlashZ
Send device info and phone number. And reply.
Receive: command slides 4
Send phone call number
PHONE_STATE
SMS
http://verisign-controlcenter.com/teapot/gate.php
FlashURL
FlashY
If required Abort sms or reply sms.
Also receive command from sms server.
Send incoming call number

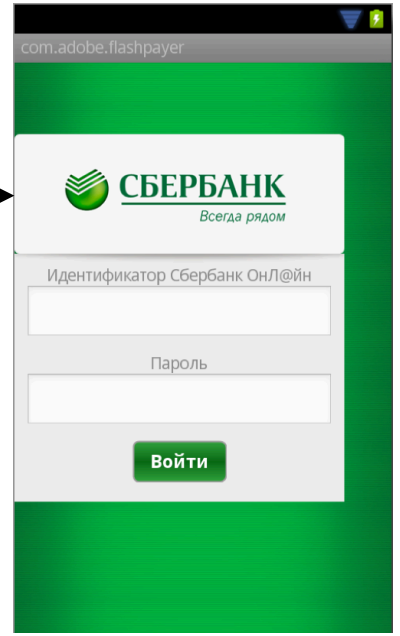
If top activity is:

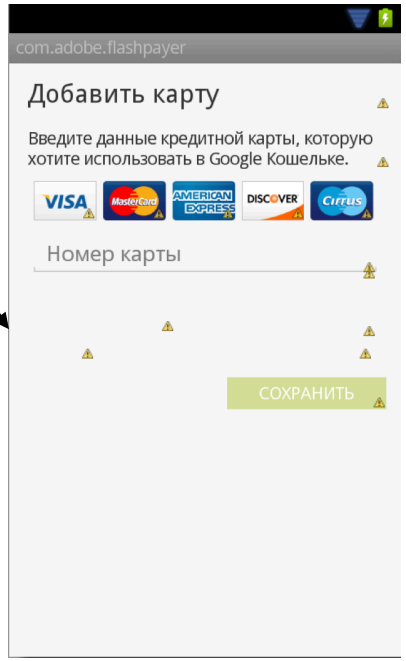
DeviceAdminAdd: jump to setting activity to prevent from delete from admin list

MasterReset: jump to setting activity to prevent from doing master reset

ru.sberbankmobile: show a fake bank loging page, if user type name, pwd, it will be send to the server.

AssetBrowserActivity: show a fake window on top of Google play window, promping the user to enter bank card details.





Newly started activity all with flag:

FLAG_ACTIVITY_LAUNCHED_FROM_HISTORY
FLAG_ACTIVITY_CLEAR_TOP
FLAG_ACTIVITY_NEW_TASK
FLAG_ACTIVITY_NO_HISTORY

command
“setFilter” -> set config “w”
“execMod” -> send “HELP” to 79262000900 (Russia bank number)
“macros” -> send device id to 79194057240 send “HELP” to 79262000900
“forceZ” -> set config “forceZ”
“callBlock” -> set config “c”
”getContacts” -> get contacts and send to server
“loadSpam” -> set config “spam_data”
“sendSpam” -> send each contacts with the spam and reply server with the spam receiver list.
“getMessages” -> get sms inbox and send to server
“keyHttpGate” -> set new server url
“keySmsGate” -> set new sms number
”getCalls” -> get call log and send to server
“getProcesses” -> get running process and send to server
“remoteSD” -> get sdcard mount info and send to server
”Download” -> downlaod file from server
“sendSMS” -> send sms
“browserHistory” -> get browser history and send to server
“faceLock” -> set config “warn”
“forceLock” -> lock the device