

Certificates and Loaders

Description

Certificates and Loaders

Description

© Ericsson Mobile Platforms AB, 2002. All rights reserved.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Ericsson shall have no liability for any error or damages of any kind resulting from the use of this document.

Confidentiality

Confidential under bilateral non-disclosure agreement.

Abstract

Certificates stored in flash memory can be modified by either recovery loaders or loading application software. In this document, the allowed transitions and properties of the platforms and the loaders are described.

Contents

| | | |
|------------|--|-----------|
| 1 | About this Document | 5 |
| 1.1 | Purpose | 5 |
| 1.2 | Audience | 5 |
| 1.3 | Assumed Knowledge | 5 |
| 1.4 | Revision History | 5 |
| | | |
| 2 | Certificates | 6 |
| | | |
| 3 | Characteristics of Loaders | 7 |
| 3.1 | Recovery Loader | 7 |
| 3.2 | Flash Loader | 7 |
| 3.3 | Explorer Loader | 7 |
| 3.4 | Production Loader A | 8 |
| 3.5 | Production Repair Loader | 8 |
| 3.6 | JTAG Loader | 9 |
| | | |
| 4 | Set of Tools for the Different Colored Certificates | 10 |
| | | |
| 5 | Differences Between the Platforms with Colored Certificates | 11 |
| | | |
| | Terminology and Abbreviations | 12 |

1 About this Document

1.1 Purpose

This document covers A1 hardware platforms based on Ericsson DB 2000 (Marita) versions P1A and P2A.

The document describes the different certificates for loading software, the corresponding properties of the phones, and the existing loaders for the different certificates in the phone for the standard Ericsson Mobile Platforms security setup.

1.2 Audience

The document is aimed for persons responsible for loading software into the phones at the R&D and the factory. Furthermore it is useful for people responsible for the release of phone software and the planning of the factory processes.

1.3 Assumed Knowledge

The document assumes that the reader knows how to load software into the phone and is familiar with the Platform Assistant Tool.

1.4 Revision History

Table 1.1 Revision history.

| Date | Rev. | Comment |
|------------|------|-------------------------------|
| 2002-11-xx | R1A | First version of the document |

2 Certificates

The A1 hardware based platforms contain two certificates: an EMP root certificate in the ROM and a customer certificate in the flash memory.

The customer certificate is signed by Ericsson Mobile Platforms and is used to verify

- 1) The loader.
- 2) The loaded software.

The customer owns the customer certificate.

Tools (loaders) used in R&D and in the factory should not be used, or be usable, in a product. Therefore, the tools, as well as the customer certificates, are distinguished by three different colors:

- Blue certificate indicates factory use.
- Brown certificate indicates R&D use.
- Red certificate indicates product use.

There is only one instant where certificates change color: at the end of the factory process, the factory certificate is changed to either R&D or the product certificate. This determines; which tools can be used for the corresponding platform after production, that is, tools for R&D or for the product.

This means that the only allowed transition is from a blue certificate to either a brown or a red certificate.

3 Characteristics of Loaders

3.1 Recovery Loader

Recovery loaders are used to reinstall the customer certificate in case it has not been loaded or has been destroyed. Therefore they are signed with the EMP root key. To distinguish the color of the platform, the OTP is used. See differences between the platforms described in the previous section.

3.2 Flash Loader

The Flash Loader, used to flash software into the platform, is signed with the customer key. Software written with the flash loaders contains a customer certificate with a certain color.

To prevent the customer certificate in the platform from being changed when software with another customer certificate is loaded, the Flash Loader only accepts software that does not change the customer certificate.

3.3 Explorer Loader

The Explorer Loader is used to load or extract data from the file system or GDFS. It is signed with the customer key.

3.4 Production Loader A

The Production Loader A has the following capabilities:

- Flash software into the platform.
- Generate Test signature to enable the radio transmission of the platform.
- Write to GDFS. Read parameters from GDFS.
- Write IMEI, PAF and CID into the OTP memory.
- Change factory certificate (blue) to product (red) or R&D (brown) certificate.
- Set dynamic and static CRCs.

The production loader A is signed with customer key.

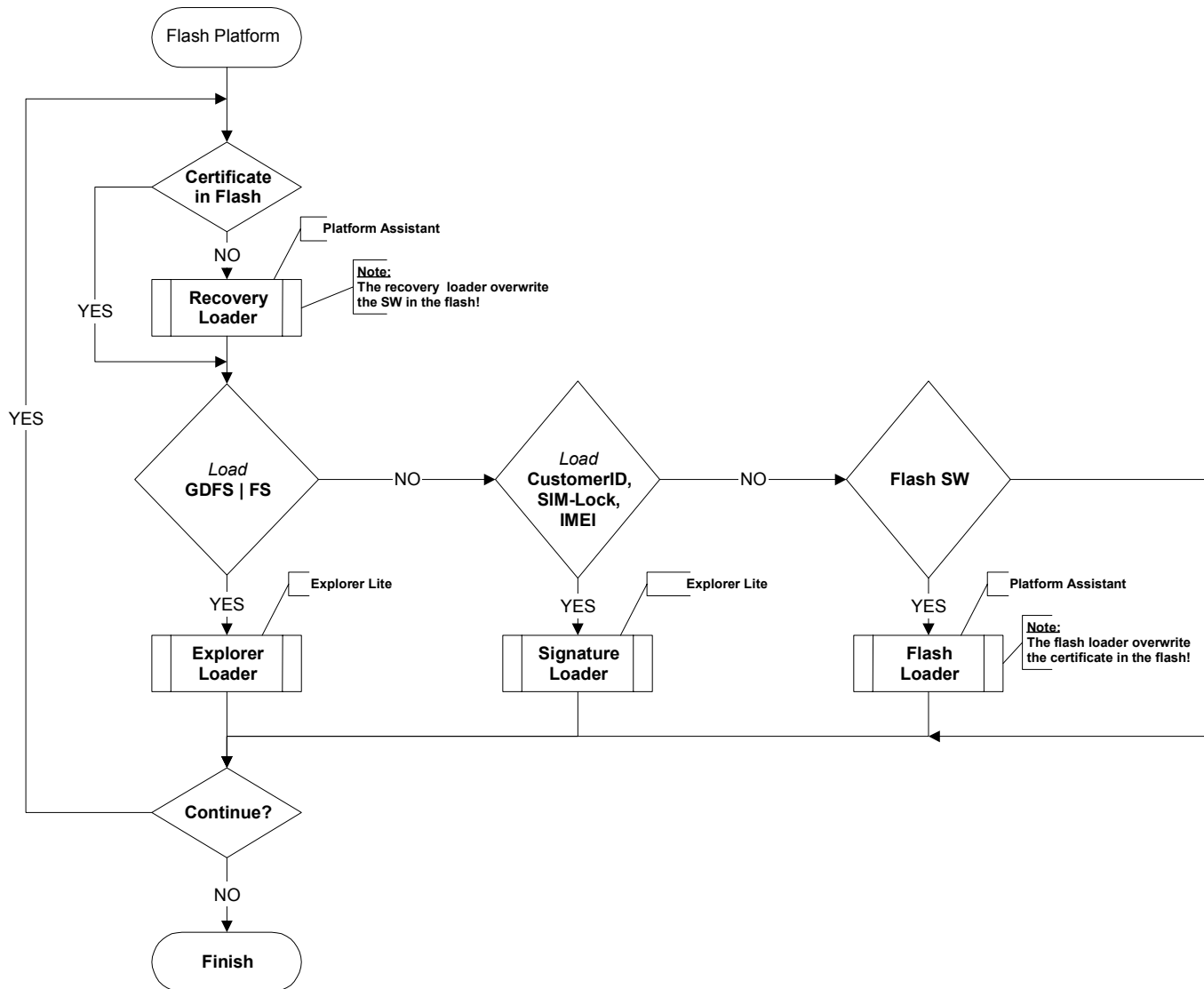
3.5 Production Repair Loader

Sometimes the customization of the platforms has to be changed in production. If the platform is already a product platform, the common tools, such as Explorer Loader and Production Loader, do not work.

The Production Repair Loader is a tool, with which you can set customization parameters in dynamic data, GDFS, and the file system. To prevent this tool from working without restriction on product (red) platforms, it requires the SIMlock codes to work.

3.6 JTAG Loader

The JTAG Loader enables the JTAG interface for debug purposes. This tool works only with unlocked OTP or OTP=000000.



4 Set of Tools for the Different Colored Certificates

Table 4.1 Tools for different certificates.

| Tool | Certificate / Platform | Domain |
|--------------------------|------------------------|--|
| Flash Loader | Brown, red | R&D and product. |
| Explorer Loader | Blue, brown | Factory and R&D. |
| Recovery Loader | Blue, brown, red | Factory, R&D, and product. |
| Production Loader | Blue | Factory |
| Production Repair Loader | Red | For factory use, but works on product platforms. |
| JTAG Loader | Brown | Works only on platforms with unlocked OTP or OTP=000000. |

5 Differences Between the Platforms with Colored Certificates

Since the Recovery Loader needs to recognize the color of a certificate of a platform, even if the certificate cannot be recognized, the produced platform has to have certain properties, which have to be guaranteed by the production process.

Table 5.1 Differences between platforms.

| Certificate / Platform | OTP | Domain |
|------------------------|--|--|
| BLUE | Unlocked. | Production |
| | All zero. | R&D and Factory. (Cannot be converted to product domain.) |
| Brown | All zero. | R&D and Factory. (Cannot be converted to product domain.) |
| | Locked: test IMEI, PAF=0, CID = customer | R&D platform. |
| Red | Locked: IMEI , PAF=1, CID = customer | Product platform. |

The loaders that may change certificates are:

- The Recovery Loader: reinstalls the customer certificate in a platform with a certain color.
- The Flash Loader: loads software into a platform. If the software contains a certificate, the Flash Loader must not change the certificate in the platform.

Terminology and Abbreviations

Certificate

The certificate consists of a public key with some additional data. Additionally a hash encrypted with a private key is added, which allows verification of the certificate.

CID

Customer ID: unique number, which identifies an Ericsson Mobile Platforms customer. It is stored in the OTP.

Customer key

The customer gets a key pair consisting of a private key which is used to sign loaders and a public key which is stored in the flash of the phone and is used to verify the loaders and the software.

Dynamic and static CRC

Areas in the platform protected by a cryptographic checksum (CRC).

EMP root certificate

A root certificate issued by Ericsson Mobile Platforms and stored in the ROM code of the platform.

EMP root key

A key associated with a root certificate issued by Ericsson Mobile Platforms and used to sign customer certificates and the recovery loaders.

File system

Logical part of the platform, where software can be stored.

Flash

Physical data storage in the platform.

GDFS

Global Data File System - Non-volatile memory area for parameters in the phone.

IMEI

International Mobile Equipment Identity

Test IMEI

Special IMEI value reserved for test products.

JTAG

Debug interface for ARM processors.

OTP

One Time Programming Memory: Area in the flash, which can be locked permanently.

PAF

Product Activation Flag: Is one for a product and zero for a factory or R&D prototype.

Platform Assistant

Tool for loading software into the platform.