MAX32550 Secure ROM FAQ

Contents

v1.0, 1-jul-2014

1. what is ANGELA ?
   A secure loader and a secure boot, for MAX32550. It is stored in the chip internal ROM.
2. How is the boot secure ?
   The boot is secure as ANGELA can not be circumvented and ANGELA checks the signature of the application to be run, before running it
3. How is the loader secure ?
   The loader is secure as ANGELA checks the signature of the downloaded data before using them.
4. Which kind of signature does ANGELA use ?
   ANGELA uses a P256 ECDSA digital signature scheme.
5. Which key is used ?
   ANGELA uses a customer key, named CRK, for digital signatures control on boot and load.
6. How is the CRK made available ?
   The CRK is downloaded with a digital signature, using Maxim Root Key, MRK, hard-coded in the ROM.
7. which links can I use for secure loader ?
   The loader communicates with a Host, using a protocol named SCP, through USB connection or a serial connection.
8. which kind of boot can Secure ROM support ?
   From the internal flash
9. How to run an application ?
   a. program the CRK in the OTP,
   b. sign the application with the CRK,
   c. program the signed application in the internal flash,
   d. power up the chip !
10. How to easily start with ANGELA ?
    A ANGELA package is available, explaining how to start a simple application on a EvKit,
11. Is there a life-cycle for the chips ?
    Yes
12. What is the life-cycle description ?
    a. before phase 3, the chip is owned by Maxim
    b. chips are shipped in phase 3; they contain no CRK in the OTP
    c. in phase 3, the customer shall and can not do anything else than programming the CRK in the OTP
    d. by programming the CRK, the chip moves automatically to phase 4
    e. in phase 4, the chip can perform secure load and secure boot: this is normal operation
    f. by programming a magic value in the OTP, the chip can be moved to phase 5
    g. in phase 5, the chip is not working any more.
13. How are shipped the chips ?
    The chips are delivered in phase 3, with 2 different P/Ns:
    a. production chips having ICE JTAG disabled
    b. development chips having ICE JTAG enabled.
14. Is there a JTAG on MAX32550 ?
    There is always a JTAG on MAX32550.
    What is disabled is the ARM core ICE,i.e. the in-circuit emulation (ARM TAP controller), helping for debug.

a. development parts have the ICE enabled
b. production parts have the ICE disabled.
This disable/enable function is controlled by OTP configuration. Dev parts have specific OTP lines not initialized, while production parts have these lines initialized. It means a dev part can become a production part but not the opposite.
c. A third situation is, for RMA, to bring the ICE back. This is possible by full erasure of the specific OTP lines. This enables the ICE back but the battery-backed key is erased at each reset.

15. How to bring the ICE back on production parts ?
As the ICE is not available any more, it is typically an applet or an application that performs that operation in the embedded OTP, so fully controlled by a CRK digital signature check.

16. What kind of controls does ANGELA perform ?
ANGELA performs self-checks on ROM code, AES, ECDSA, Unique Serial Number and TRNG

17. What action does ANGELA take in case of self-check failure ?
ANGELA provokes what is called a shutdown

18. What is a shutdown ?
A shutdown is erasure of battery-backed AES-256 key and reset of the platform.

19. Does ANGELA update any security register in case of shutdown ?
No

20. Does ANGELA configure any security or sensor register ?
No, it is up to customer application to set up the security, like secret key loading, sensors lock, ...

21. which kind of actions does the loader support ?
The loader, via SCP protocol, supports CRK programming, OTP programming, memory erasure/programming/verification and applets loading and execution

22. What is an applet ?
An applet is a small application, loaded by the SCP into internal RAM. This application provides special actions for the three commands, memory erasure/programming/verification. This is invoked depending on the data address range. The applet can be seen as an extension of the default functioning of these three commands, provided by the ROM. An applet can be developed by anybody.

23. What is the OTP made of ?
The OTP is made of two parts: a Maxim area and a user area

24. Which area can the SCP OTP programming command address ?
The OTP programming command addresses only the user area.

25. How to program the Maxim area ?
Except for the two very very specific situations of JTAG re-activation or move to phase 5, there is no need for the customer to program the Maxim area.

26. How to tune the SCP window duration ?
This is done using the write-timeout command in the SCP protocol. It has to be done for each SCP connection link, the USB and the serial. Note this command can be used only once per link.

27. Can we disable a SCP connection link, USB or serial ?
Yes, by writing the value 0xFFFF for this link, through the write-timeout command.

28. Is my sample delivered in phase 3 ?
Yes,

29. If there is a new revision: will it work with the current ANGELA package ?
No, you have to ask for the ANGELA package supporting this version.
New revisions mean SLA shall be re-signed with the new revision number and the applets shall be re-built with the new revision number.

30. What is the typical flow for a customer regarding ANGELA ?
    a. The customer securely generates his CRK, i.e. by using a HSM,
    b. The customer sends the CRK public value to Maxim for endorsement,
    c. Maxim sends backs a certificate to the customer,
    d. The customer programs the chip with this certificate (which includes the CRK public key),
    e. The customer prepares the data/code to be programmed on the device,
    f. The customer signs the data/code using his CRK private key, securely thanks to his HSM,
    g. The customer provides the signed data/code to the manufacturer plant,
    h. The manufacturer performs the programming, securely thanks to ANGELA.
    i. The device is ready for in-the-field use.

31. Could you give me some references for further reading ?
    The following documents are available from IDM:
    a. UG25H04: Secure ROM Code User Guide
    b. UG25T01: Secure ROM Package README
    c. SPEC22T02: SCP specifications