Secure Information Exchange and CRK Certification Guide

ABSTRACT

This security guide contains detailed information about the procedure of the customer root key (CRK) certification.

OVERVIEW

Devices that support the secure communication protocol bootloader (SCPBL) require the creation of a signed public key that is unique to each customer, referred to as the customer root key (CRK) certificate. The CRK certificate is issued by ADI and must be loaded into the device by the customer before it can operate.

The CRK certificate is part of a public key infrastructure (PKI), utilizing a manufacturer root key (MRK) and a CRK to ensure secure boot trust and security. The parts of this PKI are:

- MRK (public): This portion is hard-coded in the device in immutable ROM.
- MRK (private): This is used to sign the customer CRK public key to create the CRK certificate.
- CRK (public): This key is securely submitted to Analog Devices by the customer and is signed with the MRK private key to create the CRK certificate.
- CRK (private): This key is used by the secure boot tools utility to sign packets that will be sent to the SCPBL.
- CRK Certificate: This is the customer CRK public key signed with the MRK private key. It is returned to the customer in the form of prebuilt SCP packets. The CRK certificate is automatically loaded into the device's OTP when the packet is executed.

The MRK key pair (public key plus private key) is securely stored at the factory using a high-grade-security hardware security module (HSM). The customer must use similar methods to protect their own key pair—the chain of trust is compromised if the customer's key pair is discovered.

Individuals are assigned specific roles to help maintain the security of the CRK and preserve the root of trust:

- Customer Key Security Officer (CKSO): This is the customer project manager, security manager, or other administrator who will generate the CRK key pair and conduct the CRK certificate generation process. The CKSO is the customer point of contact for all secure communications.
- Manufacturer Secure Communication Contact (MSCC): This is an Analog Devices representative who interfaces with the CKSO. The MSCC receives the CRK public key from the CKSO and return the SCPBL packets to the CKSO that loads the CRK certificate into the device.
- Manufacturer Key Security Officer (MKSO): This is the internal Analog Devices individual responsible for generating the CRK certificate by signing the CRK public key using the HSM.

The steps required to generate a CRK certificate are:

1. Establish a secure communication channel using pretty good privacy (PGP) encryption between Analog Devices and the customer.
2. The customer generates their own CRK key pair. The key is either a 256-bit ECC key pair using the curve NIST P-256 or an RSA key pair, depending on the device design.
3. Customer sends the CRK public key to Analog Devices using the secure communication channel.
4. Analog Devices returns a series of secure copy protocol (SCP) packets to the customer. These are used to load the CRK certificate using the SCPBL.

One Analog Way, Wilmington, MA 01887-2356, U.S.A. | Tel: 781.329.4700

Devices are delivered to customers without CRK certificates programmed into them. The only exception is those devices preassembled in evaluation (EV) kits—these devices are preloaded with a test root key certificate to allow a quick start with the EV kit. They do not require the creation of a unique CRK certificate as described in this document.

After the CRK certificate has been loaded into a device, it is now configured and can perform trusted firmware updates and execute application software from internal memory. Although outside of the scope of this document, the remaining steps are:

1. The customer compiles the firmware image to be programmed on the device.
2. The customer signs firmware image using his CRK private key.
3. The customer converts the signed firmware image to a series of packets used for transmission over the SCP.
4. The customer (or contract manufacturer) securely programs the packets using the SCPBL.

The device is now fully programmed and ready for use.

ESTABLISHING A SECURE COMMUNICATION CHANNEL

Unencrypted email is used for initial contact between CKSO and MSCC. PGP-encrypted email is to ensure security when transferring information about the CRK.

Note that the keys used for secure PGP email communication with the customer are different than the CRK keys used for the generation of the CRK certificate.

The procedure is:

1. The customer designates a CKSO to generate their CRK key pair and conduct the CRK certificate generation process.
2. The CKSO initiates a conversation with the MSCC through the email address *processors.support@analog.com*. Be sure to state that the issue concerns the creation of a secure CRK certificate and the specific part number of interest.
3. The CKSO emails their PGP key to the MSCC and confirms the CKSO's PGP fingerprint through another channel such as a voice call or a non-email messaging application.
4. The MSCC emails their PGP key to the CKSO and confirms the MSCC's PGP fingerprint through another channel such as a voice call or a non-email messaging application.

*Customers have found it extremely helpful to have some kind of unique identifier to distinguish the keys that can be associated with multiple projects. The customer can use any convention they find useful.

CUSTOMER SENDS THE CRK PUBLIC KEY TO ANALOG DEVICES

After establishing a secure communication channel, the customer must send their CRK public key to Analog Devices for processing. This example is for ECDSA keys.

1. The CKSO creates a text file with the CRK public key. The file must be in unformatted ASCII hexadecimal format. The format differs depending on whether the requested CRK certificate is for the first write of a key (WRITE_CRK) or the second write of a key (REWRITE_CRK). Most users will only require one (first) key.

- For WRITE_CRK, the text file will have two lines, each consisting of 64 hexadecimal characters:
  - First line: Qx coordinate
  - Second line: Qy coordinate
- For REWRITE_CRK, the text file will have four lines, each consisting of 64 hexadecimal characters:
  - First line: Previous key Qx coordinate
  - Second line: Previous key Qy coordinate
  - Third line: New key Qx coordinate
  - Fourth line: New key Qy coordinate

2. The CKSO signs the text file using their PGP tool.
3. The CKSO emails the signed text file, with PGP encryption, to the MSCC using this format:
   - Subject line: CRK certificate request – *company_name*
   - Body text:
     - Company name
     - CKSO name
     - CKSO contact phone
     - CKSO contact email
     - Customer project name or identifier*
     - Full ordering part number for the device as found on the device data sheet
     - CRK certificate type: *SCP write CRK script* or *SCP rewrite CRK script*
   - Attachment: Signed text file

ANALOG DEVICES GENERATES THE CRK INSTALLATION PACKETS FOR THE CUSTOMER

The last step of the process is for Analog Devices to create the CRK certificate and return it to the customer in the form of SCP packets, which is how the certificate is loaded into the device.

1. After verifying the customer's signature, the MSCC internally transfers the CRK public key text file to the MKSO.
2. The MKSO creates the CRK certificate by signing the CRK public key with the MRK private key using the manufacturer HSM.
3. The MKSO converts the CRK certificate to a series of SCP packets to execute the WRITE_CRK or REWRITE_CRK command, which will load the CRK certificate into the device's OTP memory.
4. The MKSO transfers the CRK certificate to the MSCC.

5. Using PGP encryption, the MSCC emails the SCP packet to the CKSO.
6. The customer verifies the signature of the received file and decrypts the generated packets.
7. The customer executes the packets through the SCPBL.

REVISION HISTORY

REVSION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	8/21	Initial release	-
1	9/25	Significant edits, removal of Kleopatra application tutorial, update of secure information exchange and CRK signing procedures	All