```
          +=======================================================+
          +     i.MX Secure and Encrypted Boot using HABv4        +
          +=======================================================+
```

1. Introduction

The i.MX family of applications processors provides the High Assurance Boot (HAB) feature in the on-chip ROM. The ROM is responsible for loading the initial program image (U-Boot) from the boot media and HAB enables the ROM to authenticate and/or decrypt the program image by using cryptography operations.

This feature is supported in i.MX 50, i.MX 53, i.MX 6, i.MX 7 series and i.MX 8M family (i.MX 8M, i.MX 8MM, i.MX 8MN, i.MX 8MP devices).

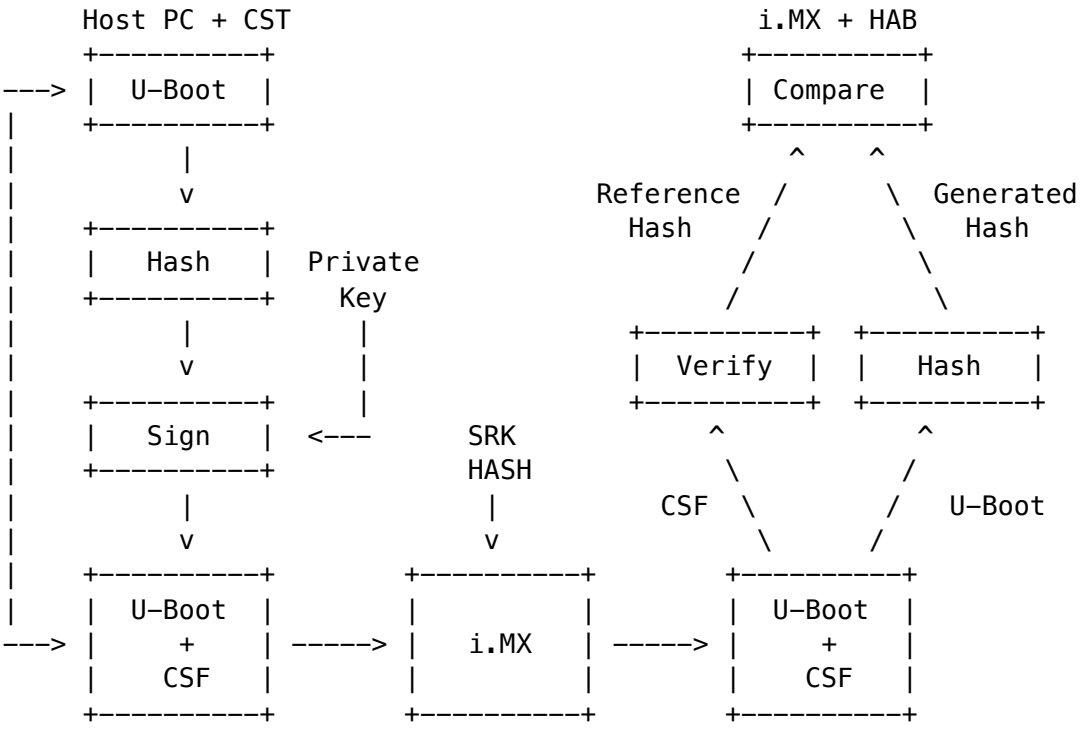
Step-by-step guides are available under doc/imx/habv4/guides/ directory, users familiar with HAB and CST PKI tree generation should refer to these documents instead.

1.1 The HABv4 Secure Boot Architecture

The HABv4 secure boot feature uses digital signatures to prevent unauthorized software execution during the device boot sequence. In case a malware takes control of the boot sequence, sensitive data, services and network can be impacted.

The HAB authentication is based on public key cryptography using the RSA algorithm in which image data is signed offline using a series of private keys. The resulting signed image data is then verified on the i.MX processor using the corresponding public keys. The public keys are included in the CSF binary and the SRK Hash is programmed in the SoC fuses for establishing the root of trust.

The diagram below illustrate the secure boot process overview:



The U-Boot image to be programmed into the boot media needs to be properly constructed i.e. it must contain a proper Command Sequence File (CSF).

The CSF is a binary data structure interpreted by the HAB to guide authentication process, this is generated by the Code Signing Tool[1]. The CSF structure contains the commands, SRK table, signatures and certificates.

Details about the Secure Boot and Code Signing Tool (CST) can be found in the application note AN4581[2] and in the secure boot guides. Syntax and details about CSF can be found in the CST User Guide which is packaged with the CST tool and located in the doc directory.

1.2 The HABv4 Encrypted Boot Architecture

The HAB Encrypted Boot feature available in CAAM supported devices adds an extra security operation to the bootloading sequence. It uses cryptographic techniques (AES-CCM) to obscure the U-Boot data, so it cannot be seen or used by unauthorized users. This mechanism protects the U-Boot code residing on flash or external memory and also ensures that the final image is unique per device.

The process can be divided into two protection mechanisms. The first mechanism is the bootloader code encryption which provides data confidentiality and the second mechanism is the digital signature, which authenticates the encrypted image.

Keep in mind that the encrypted boot makes use of both mechanisms whatever the order is (sign and then encrypt, or encrypt and then sign), both operations can be applied on the same region with exception of the U-Boot Header (IVT, boot data and DCD) which can only be signed, not encrypted.

The diagram below illustrate the encrypted boot process overview: