iMX COM Boards
Security Considerations

Embedded Artists

Embedded Artists AB
Davidshallsgatan 16
SE-211 45 Malmö
Sweden

http://www.EmbeddedArtists.com

Disclaimer

Embedded Artists AB makes no representation or warranties with respect to the contents hereof and specifically disclaim any implied warranties or merchantability or fitness for any particular purpose. Information in this publication is subject to change without notice and does not represent a commitment on the part of Embedded Artists AB.

Feedback

We appreciate any feedback you may have for improvements on this document. Send your comments by using the contact form: www.embeddedartists.com/contact.

Trademarks

All brand and product names mentioned herein are trademarks, services marks, registered trademarks, or registered service marks of their respective owners and should be treated as such.

Table of Contents

1 Document Revision History 4

2 Introduction 5

2.1 Security concepts 5
2.1.1 Authentication 5
2.1.2 Authorization 5
2.1.3 Integrity 5
2.1.4 Confidentiality 5
2.2 Security techniques 5
2.2.1 Symmetric encryption 5
2.2.2 Asymmetric (public key) encryption 6
2.2.3 Message digest 6
2.2.4 Message Authentication Code (MAC) 7
2.2.5 Digital signature 8
2.2.6 Certificates 8
2.3 Conventions in the document 8

3 Secure Boot 10

3.1 Introduction 10
3.1.1 Overview of procedure 10
3.1.2 Image layout 10
3.1.3 Additional Documentation 12
3.2 Instructions: Generate keys 12
3.3 Instructions: Enable secure boot 12
3.4 Instructions: Sign images 13
3.5 Instructions: Burn fuses 14
3.6 Instructions: Verify signature 14
3.7 Instructions: Put HAB into closed state 15
3.8 Instructions: Manufacturing tool images 15
3.8.1 DCD size and offset 16

4 Troubleshooting 17

4.1 iMX6 UltraLite Linux kernel not starting 17

1 Document Revision History

Revision	*Date*	*Description*
A	2015-12-21	First release
B	2015-01-15	- Added the Troubleshooting chapter.

The full version of this document is available at the support page for the i.MX Developer's Kit you are using.

NOTE: You need to register the serial number that comes with the kit to get access

http://www.embeddedartists.com/support/overview