Samsung Knax

Samsung KNOX TIMA Key Store Guide





Copyright Notice

Copyright © 2014 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trademark of Samsung Electronics Co. Ltd. Specifications and designs are subject to change without notice. Non-metric weights and measurements are approximate. All data were deemed correct at time of creation. Samsung is not liable for errors or omissions. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

About this guide

This guide describes the TIMA Key Store APIs

1 Introduction

TIMA Key Store is implemented as a Key Store Provider for the Java KeyStore Class. This document describes how each of the Java KeyStore class method behaves when TIMA KeyStore is instantiated. Please refer to the Android SDK for the complete description of the KeyStore class. This document's main focus is to describe differences in KeyStore API behavior with respect to the default key store provider in Android.

How TIMA Key Store works

TIMA Key Store provides TrustZone based secure key storage for the symmetric keys. RSA key pairs, and certificates are routed to the default key store provider for storage. However, TIMA Key Store provider modifies the behavior of those functions that are implemented by the default key store provider.

TIMA Key Store controls access to all keys based on the trusted boot measurements. During device boot, measurements of aboot and kernel images are collected and compared against Samsung signed measurements. If there is any difference, device is considered to be booted into a custom kernel. TIMA Key Store only supports signed, official, kernel. In case of custom kernel, TIMA Key Store will refuse to store or retrieve keys.

2 TIMA KeyStore API Specification

TIMA Key Store provider is accessible through standard Java KeyStore Class available on Android. Refer to Android SDK for detailed description of the KeyStore Class. Below, TIMA Key Store specific implementation differences are highlighted

API	TIIMA Key Store Notes
load	InputStream and password arguments must be NULL.
	KeyStore.LoadStoreParameter must be NULL
	Synopsis:
	The load API initializes the TimaKeyStore. Initialization includes license and
	trusted boot measurement checks.
setKeyEntry	Synopsis:
	TIMA Key Store supports symmetric keys, in addition to RSA keys. Keys are not
	stored if the trusted boot measurements do not match to Samsung authorized
4F4	values
setEntry	Synopsis:
	TIMA Key Store supports symmetric keys, in addition to RSA keys and certificates.
	Keys are not stored if the trusted boot measurements do not match to Samsung authorized values
setCertificateEntry	Synopsis:
SelcerinicaleEntry	Certificates are not stored if the trusted boot measurements do not match to
	Samsung authorized values
getKey	Synopsis:
	TIMA Key Store supports symmetric keys, in addition to RSA keys. Keys are not
	retrieved if the trusted boot measurements do not match to Samsung authorized
	values
getEntry	Synopsis:
	TIMA Key Store supports symmetric keys, in addition to RSA keys and certificates.
	Keys are not rertieved if the trusted boot measurements do not match to Samsung
10 110	authorized values
getCertificate	Synopsis:
	Certificates are not retrieved if the trusted boot measurements do not match to
10 (15 1 0)	Samsung authorized values
getCertificateChain	Synopsis:
	Certificates are not retrieved if the trusted boot measurements do not match to
Ctoro	Samsung authorized values
Store	This API is not supported. TIMA Key Store cannot be serialized.

All other KeyStore APIs are supported as documented in Android SDK.