

Features

- Builds and manages security credentials
- Support for manufacturing processes for signed code loads
- Highly flexible and scalable solution
- Supports multiple independent or interacting supply chains
- Based on X.509 certificates
- Supports industry standards and protocols
- Support for hardware acceleration
- Linux and ANSI-C based
- Builds on generic ARM, PPC, X86 platforms

Applications

- Anti-cloning and anti-counterfeiting
- Key injection
- DRM schemes (CPRM, HDCP)

Ellipsys Trust Framework

- ESS-04: Ellipsys-SB
- ESS-06: Ellipsys-CA
- ESS-07: Ellipsys-VSM

ESS-06 is a member of the Ellipsys Trust Framework, designed to provide credential management and allow the distribution of inherited trust through manufacturing and OEM production lines. Customers can use Ellipsys-CA to quickly and efficiently deploy the secure deployment of anti-tampering, anti-cloning and secure boot technologies.

General Description

Ellipsys-CA is a server based set of applications that provide the ability to generate and manage security credentials to support anti-tampering, anti-cloning and secure boot technologies.

The solution provides a trusted, managed environment to generate, inject, transport, archive and revoke certificates and private keys.

Through an SQL-based backend storage, credentials are stored into an auditable database with logging information that provides accountability for all Certificate Authority (CA) operations.

The cryptographic components of Ellipsys-CA comply with industry standards such as PKCS #1, PKCS #5, PKCS #8, ANSI X9.62, X.509, NIST FIPS 197, NIST FIPS 180-2, and IETF RFC 1312 to ensure security and interoperability with third party vendors.

Ellipsys-CA shares a common API and code base with the other products of the Ellipsys Trust Framework, like Ellipsys-SB and Ellipsys-VSM. Any or all of these products may be used, depending on the needs of a particular project.

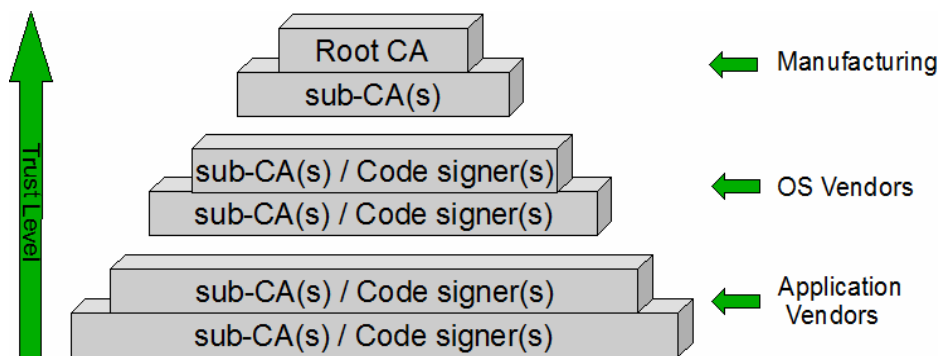
The solution is built to support hardware acceleration for cryptographic operations and/or offload for the main CPU(s).

Ellipsys-CA provides an interface to the user specifically tuned for the operations required to deploy secure boot systems, removing the need for crafting in-house tools to prepare boot images, hence reducing development time and risk.

At the start of any chain of trust is the root credential, often called the root CA. All credentials signed by the root CA are called sub-CAs. These credentials are designated as being able to sign other credentials themselves. Below the sub-CAs can be further sub-CAs and/or code/data signers.

Ellipsys-CA is a flexible and scalable solution for designating and delegating signing authority to different departments, vendors, developers, and others, because the levels of trust and breadth of nesting are not limited.

The diagram below shows how a typical trust hierarchy may be built.



Ellipsys Trust

The Ellipsys Trust Framework offers manufacturers the ability to implement cost-effective cryptographic protection of high value assets. Using the framework it is now possible for:

- Manufacturers to protect against counterfeiting, cloning, overbuilding of products produced by ODMs;
- IP designers to protect Design IP through all phases of product life cycle;
- Content Distributors to protect high value content such as High Definition video;
- Device manufacturers to enable the commissioning of products at the point of sale;
- Network operators and administrators to manage the identity and approved features of network elements in mobile and wired networks

In each of these situations, cryptographic credentials such as keys or certificates must be managed and inserted into the target device. The Ellipsys Trust Framework is designed to be very flexible in the format of keys and certificates to allow it to be adapted to the use model required for the target application.

For example, if a manufacturer wishes to protect against anti-cloning when using an ODM, it can securely inject credentials from a secure server administered by the manufacturer. Only those products that receive these credentials will function correctly. Similarly, a designer of DSP algorithms for example could decrypt and enable the code only for authenticated use through the secure injection of credentials during manufacturing by customers. This will ensure that only authorized (and paid) copies are enabled.

All product offerings from the Ellipsys Trust Framework share a common API and code base and any or all components may be used depending on the needs of a particular project.

The framework is built to optionally support hardware acceleration for cryptographic operations and offload for embedded processors.

Ordering Information

- Offered in either portable source code or binary formats
- As the solution is highly configurable, it will support many options. Further technical details on the options available to developers can be provided under NDA.

Ellipsys Trust Framework

