

### Features

- Management and protection of sensitive information like keys and certificates
- Secure generation, storage, archiving, cloning and migration of key material
- Highly configurable and flexible architecture
- Supports industry standards and protocols
- Support for hardware acceleration and CPU offload
- Linux and ANSI-C based
- Builds on generic ARM, PPC, X86 platforms

### Applications

- Anti-cloning and anti-counterfeiting
- Anti-tampering
- **Key exchange applications (IPsec IKE)**

### Ellipsys Trust Framework

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

*ESS-07 is a member of the Ellipsys Trust Framework, designed to provide a software system that manages and protects highly sensitive information such as keys and certificates, in embedded system environments. Ellipsys-VSM (Virtual Security Module) implements many of the features of a Hardware Security Module (HSM) with the goal of greatly enhancing the security of software solutions when HSMs are either too costly or not feasible.*

### General Description

Software developers dealing with keys and other secrets often rely on basic protection of these values through simplistic mechanisms such as folder or file permissions. This leaves these credentials open to an easy compromise. In some cases, secrets may have enough value (such as an RSA or ECC private key for e-commerce) that an expensive Hardware Security Module (HSM) needs to be used. For many applications however, a well constructed software system designed to hide keys and secrets can be a cost-effective solution.

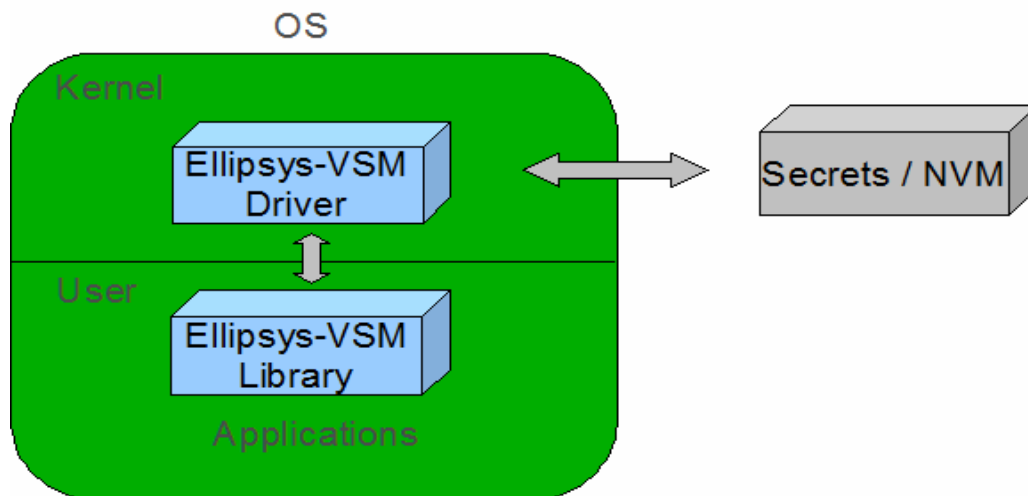
Elliptic offers this capability through the Ellipsys-VSM, which is a Virtual Security Module (VSM) that offers software based cryptographic services, similar to a Hardware Security Module (HSM), to support a range of solutions for digital identity and transactional security applications.

Ellipsys-VSM is a “software smart card” used to secure embedded secrets in software systems and has the capability to manage and protect sensitive information such as keys and credentials for system applications executing on embedded platforms. The solution supports a wide range of protected key management services such as secure generation, storage, archiving, cloning, and migration of key material.

Ellipsys-VSM shares a common API and code base with the other products of the Ellipsys Trust Framework, like Ellipsys-SB and Ellipsys-CA. 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).

The diagram below shows how Ellipsys-VSM is integrated into an operating system.



### 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.

