Solution Brief

eperi Integration with Entrust nShield HSM

Eperi GmbH

Version 26.8, July 2026

Table of Contents

Introduction

This document provides a functional overview of integrating Entrust's nShield HSM with the eperi solution via the industry-standard PKCS#11 interface. The nShield HSM serves as the master key source, keeping cryptographic key material within a FIPS-validated hardware boundary at all times.

Hardware Security Modules (HSMs)

A Hardware Security Module (HSM) is a purpose-built cryptographic device that generates, stores, and uses keys within a tamper-resistant hardware boundary. HSMs enforce strict access controls and key-usage policies that software-only solutions cannot match.

Entrust nShield

Entrust nShield is a family of both FIPS 140-2 and 140-3 validated hardware security modules designed to protect cryptographic keys and perform sensitive operations in a trusted hardware environment.

FIPS Validated

Entrust nShield is validated against the highest US Federal NIST cryptographic security standards, providing tamper-evident and tamper-resistant physical protection.

Network-attached or embedded

nShield HSMs are available as network appliances (Entrust nShield or nShield 5s).

Security World architecture

A trust domain shared between nShield modules and authorized clients, enabling centralized key management across multiple devices.

PKCS#11 standard

The industry-standard API for cryptographic operations, ensuring interoperability with a wide range of applications and security solutions.

eperi sEcure

With eperi sEcure, sensitive business data and PII (Personally Identifiable Information) data reaches the cloud only in encrypted form. For admins and attackers it's invisible, for users it works seamlessly. Data stays protected and unreadable—'at rest', 'in use', and 'in transit'.

Only the data owner possesses the cryptographic keys necessary for encryption and decryption, allowing eperi sEcure-enabled organizations to manage the entire encryption process with a single point of control.

This ensures compliance with data protection regulations and makes any data accessed by attackers or cloud providers worthless.

The eperi Master Key Concept

eperi sEcure differentiates between **Master Keys**, **System Keys**, and **Data Encryption Keys**:

- The **Master Key** is used to encrypt and decrypt the **System Keys**, shown as **Encryption** under **System Keys** in the diagram below.

- **System Keys** are used to encrypt and decrypt the **Data Encryption Keys**.

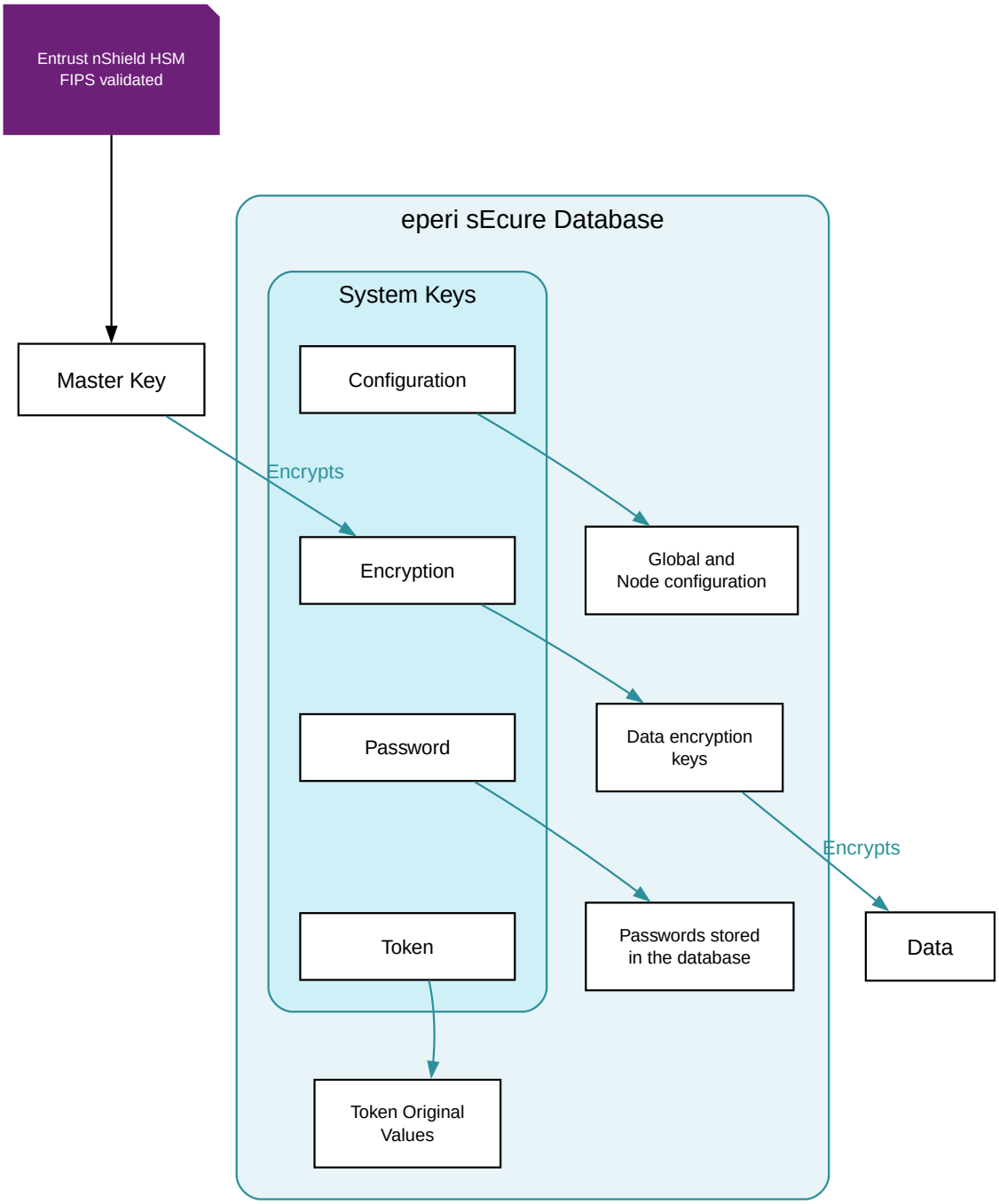

Figure 1. Integrating an Entrust nShield HSM with eperi sEcure Cryptographic Key Architecture

To use generic cryptographic key terminology, the eperi Master Key functions like a Master Key Encryption Key (MKEK). eperi System Keys serve the same role as KEKs. They encrypt and decrypt Data Encryption Keys (DEKs). When using nShield with eperi sEcure, the nShield HSM can function as an MKEK, i.e., to serve the role of the eperi Master Key for encrypting and decrypting the eperi System Keys.

Integrating with eperi sEcure

1. Deploy the nShield HSM:
    - Establish the Security World and enroll the nShield module following Entrust's deployment guidelines.
2. Create the `database.conf` file:

Create the appropriate `database.conf` file by following the instructions specific to Entrust nShield in sEcure Platform: Performing the initial configuration. This file will point to the nShield HSM for the Master Key.

3. Configure the PKCS#11 client:
    - Configure the nShield PKCS#11 client library and key access policy to allow eperi sEcure to communicate with the HSM.
    - Ensure that the eperi sEcure service user has the necessary permissions to access the HSM key assets.
4. Start eperi sEcure:

    eperi sEcure will then encrypt the system keys with the keys from the nShield HSM using the PKCS#11 interface.