

WIS@print

Security for Printer Cartridges



Counterfeit ink and toner cartridges lead to bad user experience or even potential health issues, damaged printers in addition to a huge loss of revenue for printer manufacturers.

WIS@key offers a complete solution to reduce the risk of fraud and help printer manufacturers to protect their legitimate cartridges. The WIS@print solution includes cryptographic hardware modules and a turnkey high security infrastructure – as used in e-passport applications – as well as services that help deployment from the plant to the field.

Revenue Protection for Printer Manufacturers

- > Unique Digital ID securely stored in tamper resistant VaultIC security module asserting authentic cartridge
- > Digital ID life cycle management using proven Public Key Infrastructure (PKI) suited to high-volume manufacturing
- > Detection of fake or black-listed cartridges in real-time
- > High speed multi-cartridge authentication
- > Refill protection/management
- > Wired or wireless module
- > Solutions for on-line and off-line printers
- > Integration and configuration services

Trusted Identity System

A Digital Certificate reliably asserts the identity of an object, thanks to cryptographic keys used for electronic signature. The certificate is issued and signed by a Certificate Authority (CA) such as WIS@key. A legitimate cartridge, tagged with a combination of certificate and tamper resistant chip, can be authenticated throughout its lifecycle. Counterfeit cartridges cannot replicate the cryptographic keys and can easily be detected and blocked from connecting to the printer. This is made possible by the centralized PKI system.

WIS@key - PKI Expertise

WIS@key is a proven provider of managed Public Key Infrastructure (PKI) services, offering both trusted and vendor-specific Certificate Authority (CA) options tailored to the high volume and reliability requirements of connected objects manufacturers.

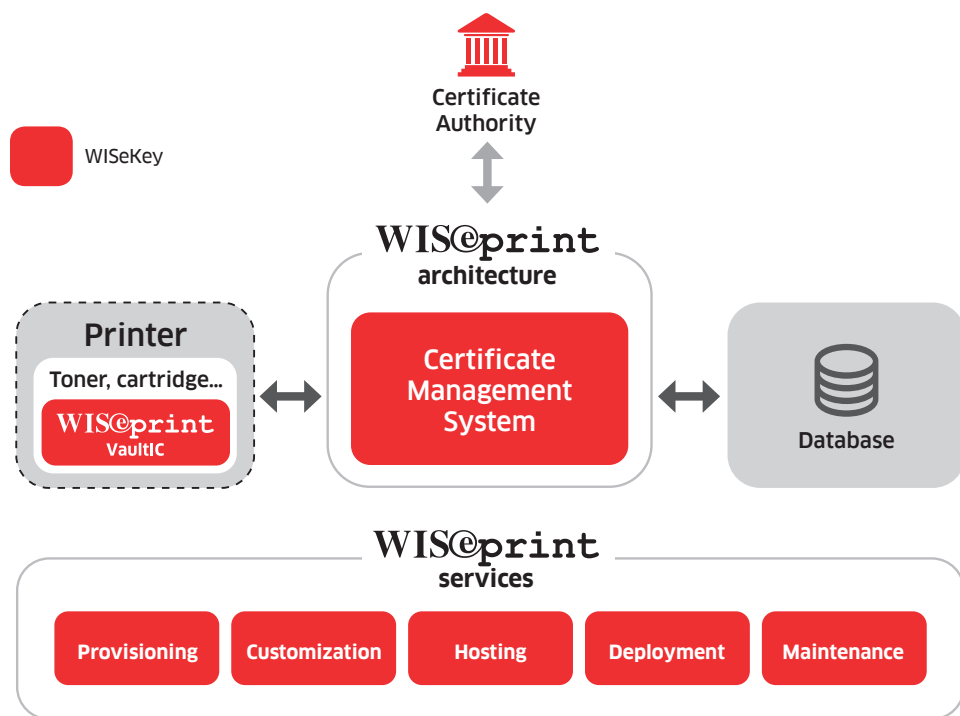
As trusted operator of the International Organization for the Security of Electronic Transaction (OISTE) Global Root, WIS@key combines highly-scalable PKI operations with Swiss neutrality, security and privacy laws.

WIS@key

Architecture

The WISeprint Certificate Management System (CMS) manages the lifecycle of Digital Certificates stored in the tamper resistant VaultIC secure element, providing a cryptographically-protected

cartridge eID. With a user-friendly interface and an easy-to-integrate API, the CMS and its related PKI can be provided as an outsourced service or licensed as a customer dedicated system.



VaultIC secure element

The VaultIC secure element comes with a complete firmware dedicated to IP protection and anti-cloning. This firmware uses a variety of cryptographic mechanisms such as digital signature generation/verification to provide a number of data protection and authentication functions. The specific hardware includes a non-volatile and firewalled data storage space for keys, certificates and customer data. Its large number of security features and a tamper resistant capability offers a full compliance to Common Criteria EAL5+ and FIPS 140-2 Level 3 certifications. Its low-power consumption profile makes it a perfect security companion to a printer host processor. The choice between wired or wireless interface suits any printer configuration.

Services

WISeKey provides all the services needed to efficiently deploy WISeprint within a printer manufacturer's design and manufacturing cycle including provisioning, setup, industrialization,

hosting and consultancy. WISeKey CMS can be installed at customer premises, or outsourced to WISeKey and located in one of our regional secure data centers.



WIS@key

wisekey.com
info@wisekey.com



<https://www.wisekey.com/solutions/digitalbrandprotection/wiseprint>