

• software

- Javacard® 3.0.4 Classic Edition with OTA patching support
- GlobalPlatform 2.2.1 with Amendments A, C, D
- Compliant with GlobalPlatform embedded Secure Element configuration
- GSMA UICC Event notification API support
- GlobalPlatform Event API notification support
- Native Mifare Classic Card 1k/4K emulation

• hardware

- INSIDE AVR 8/16-Bit RISC secure microcontroller core
- 352 KB of ROM
- 208 KB EEPROM
- External interfaces include ISO7816 & single-wire protocol (SWP)

• cryptographic support

- DPA resistant cryptographic support
 - Hardware DES, 3DES & AES
 - Hardware PKI accelerator (Ad-X2) for RSA, ECC
 - CRC16 & 32 engine

• operations

- Temperature -25°C to +85°C
- Typically 500,000 write/erase cycles at 25°C
- 10 years data retention

• certification

- EMVco Platform Security (v1.2)
- CUP IC Security (v1.3)
- CUP/UPCard/PBOC/qPBOC applet
- Global Platform compliance

• packaging

- WL-CSP 36B 3.16x3.16*0.576mm format
- 8L DFN8 4.2*4mm format

Mobility is changing the ways in which businesses, consumers, and service providers purchase, use, and deliver services. Mobile devices such as notebooks, laptops, tablets, and phones are smarter and more capable than ever. What have been missing are trusted mobile security solutions that protect users' identities, enterprise information, and digital content. For example, businesses are implementing Bring Your Own Device (BYOD) strategies to give employees greater convenience and increase enterprise responsiveness. Yet, it is difficult to secure and manage security for a wide range of mobile devices. Content providers want to ensure that their media is protected from piracy. And consumers want the convenience of making everyday purchases with their smartphones without fear of identity theft and fraud.

The WIS@key® vaultSEcure™ secure element is an innovative mobile security solution that allows multiple trusted third parties to independently install and control their applets in the same secure element. vaultSEcure 1.3 can be easily implemented into mobile phones, tablets, laptops, desktop computers, and other consumer equipment for fast time to market and simplified provisioning.

A comprehensive security solution

The embedded vaultSEcure 1.3 secure element enables WIS@key customers to deploy out-of-the-box trusted platforms and offer secure services universally. Semiconductor manufacturers easily can add value to their chipsets with secure element functionality. Mobile device manufacturers can build security into mobile devices and systems with applets that support payment, access control, fare collection, and content protection. vaultSEcure 1.3 includes fully certified embedded secure element hardware based on the WIS@key AVR 8/16-Bit RISC secure microcontroller core; the vaultSEcure 1.3 operating system; and a full set of applets that support many mobile services:

- Data, device, and network access security solutions for enterprises
- Personal data security solutions for consumers
- Premium content protection solutions for entertainment providers
- Secure payment solutions
- NFC applications for access control, transit, and other use cases



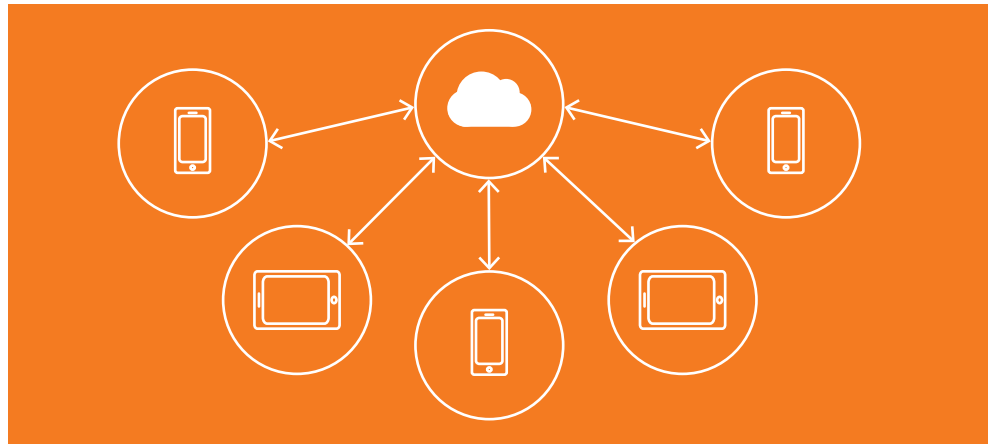
Certified applets reduce development time

WISeKey **vaultSEcure** 1.3 offers a comprehensive suite of certified mobile payment, transit, loyalty, access control, and identity applets. For the first time, device manufacturers, mobile network operators, content providers, and other trusted third parties can install, personalize, and administer their own applets on the same secure element. WISeKey also provides a flexible licensing agreement to meet the specific needs of its customers. Available applets include:

- WISeKey Mobile Security Applet Suite
- Support for mobile payment with leading brands:
 - v1.3: PBoC/China UnionPay with CUP, UPCard, PBOC and qPBOC
 - v1.2: Visa, MasterCard and Amex
- Closed-loop and private-label payment
- Transit fare collection

Accelerate time to market

WISeKey **vaultSEcure** 1.3 accelerates time to market. Multiple connectivity interfaces enable customers to quickly integrate **vaultSEcure** 1.3 with a range of hardware, operating system, and application environments. Applet support for leading payment brands and white label flexibility enable manufacturers, mobile operators, and content providers to take advantage of globally installed payment systems.



Simplify deployment and management

Each trusted party can implement and manage its own applets without users having to replace chips or devices. Over-the-air patching and support simplify updates. GlobalPlatform 2.2 features, such as Authorized Management and Contactless Registry Services, enable activation and deactivation of individual applets on a device. These advanced capabilities offer the greatest flexibility in tailoring and differentiating services for end customers.

Virtually unlimited memory space

vaultSEcure 1.3 features Secure Memory Swap technology, which provides virtually unlimited storage for applet libraries at almost no cost. Using advanced cryptographic techniques, Secure Memory Swap allows infrequently used applets to be securely stored in available host memory and moved back into the secure element memory for execution as needed. Applets can be “activated” back in secure element memory based on any number of contextual factors, such as location, date, time, first tap and more.

WISEKEY® SERVICES

WISeKey® provides “one-stop-shop” support to accompany customers from initial designs until full product certification.

- **Accelerate Deployment with WISeKey Services**
With its staff of technical specialists, WISeKey can help developer organizations accelerate the integration and adoption of **vaultSEcure** with reference designs and a wide range of professional services.
- **Global Reach**
WISeKey teams and expertise centers are located worldwide to deliver Level 2 support from our centralized sites or close to customers’ development sites.
- **Lifecycle Support**
WISeKey works with you from project kick-off to certification, providing assistance with hardware, software, certification, training, and other requirements.

For further details on all of WISeKey’s security solutions, visit www.wisekey.com

WIS@key

Information in this document is not intended to be legally binding. WISeKey products are sold subject to WISeKey Terms & Conditions of Sale or the provisions of any agreements entered into and executed by WISeKey and the customer. ©WISeKey 2013. All Rights Reserved. WISeKey, WISeKey logo and combinations thereof, and others are registered ® trademarks or tradenames of WISeKey or its subsidiaries. Other terms and product names may be trademarks of others. The products described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.