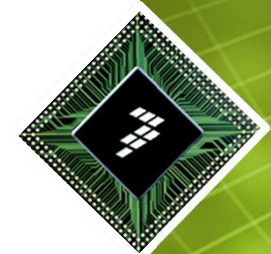




http://www.freescale.com/webapp/ps/site/prod_summary.jsp?code=RDMK30&fsrch=1&sr=1



<http://www.insidesecond.com/eng/Markets/Digital-Security/Smart-metering>

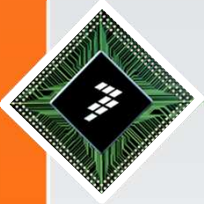


Jan 2012

Freescale, the Freescale logo, AlliVec, C-5, CodeTEST, CodeWarrior, ColdFire, C-Ware, the Energy Efficient Solutions logo, mobileGT, PowerQUICC, QorIQ, StarCore and Symphony are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. Airfast, BeeKit, BeeStack, ColdFire+, CoreNet, Flexis, Kinetis, MagniV, MXC, Platform in a Package, Processor Expert, QorIQ, Qonverge, Qorivva, QUICC Engine, Ready Play, SafeAssure, SMARTMOS, TurboLink, VortiQa and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2012 Freescale Semiconductor, Inc.

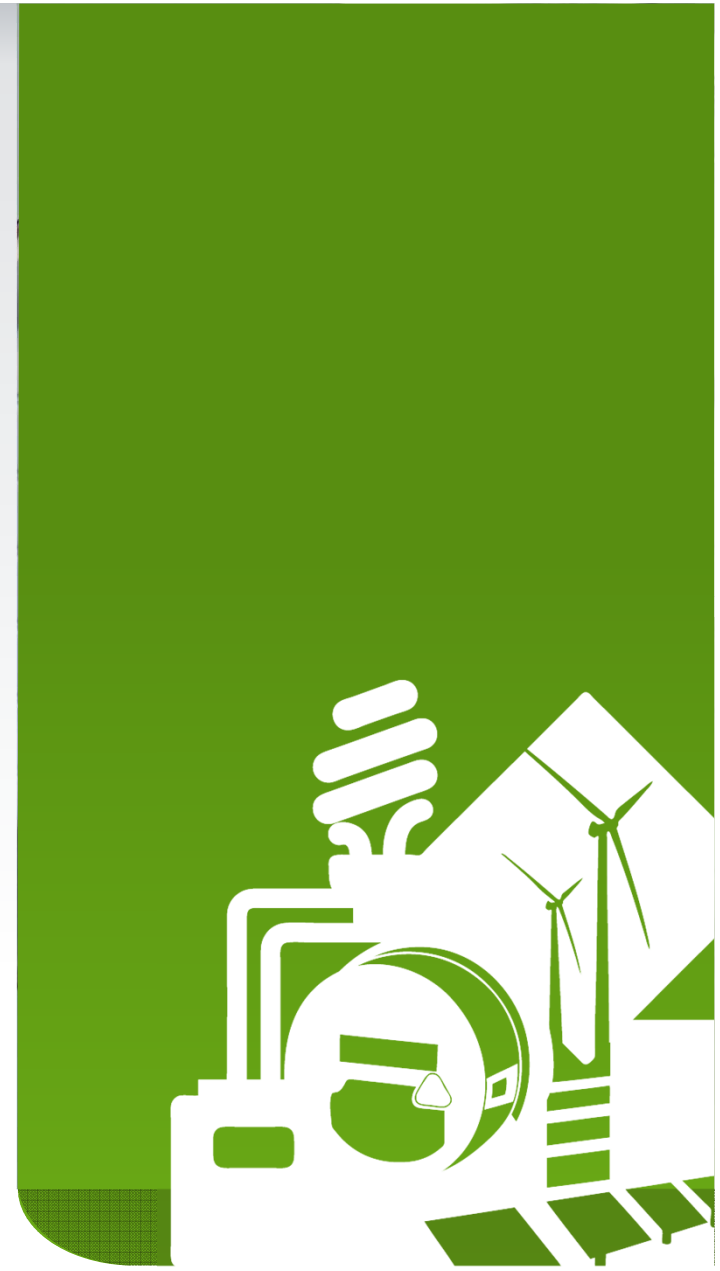
End to End Secure, Prepaid Electricity Meter Reference Design





Agenda

- Market Trends
- Technical Security requirements
- Challenges
- Our Solution
- Features and Benefits
- Support and Availability



Market Trends

CLIMATE CHANGE standards and renewable energy mandates are among the key drivers forcing major changes in Power and Energy market



ENERGY COSTS expected to increase in the coming years

REGIONAL DE/REGULATION promotes growth of prepaid meters in several countries across globe



PRE-PAID METER gives customer **greater control** over their expenses

TARGETED REGIONS: UK, Eastern Europe, latin Americas, South Africa, Asia



Smart Grid Security

- **AMR** gains efficiencies for utilities
- **AMI** provides interactive data exchange between the utility company and the consumer equipment.
- As **more intelligence** is installed, there is **more opportunity** for the system to be breached or “hacked”.
- This is even more of an issue where pre-paid meters are involved and customers are in direct control of the funding of their electricity
- **Security** is a key component of any pre-paid meter solution



Smart Grid Requirements



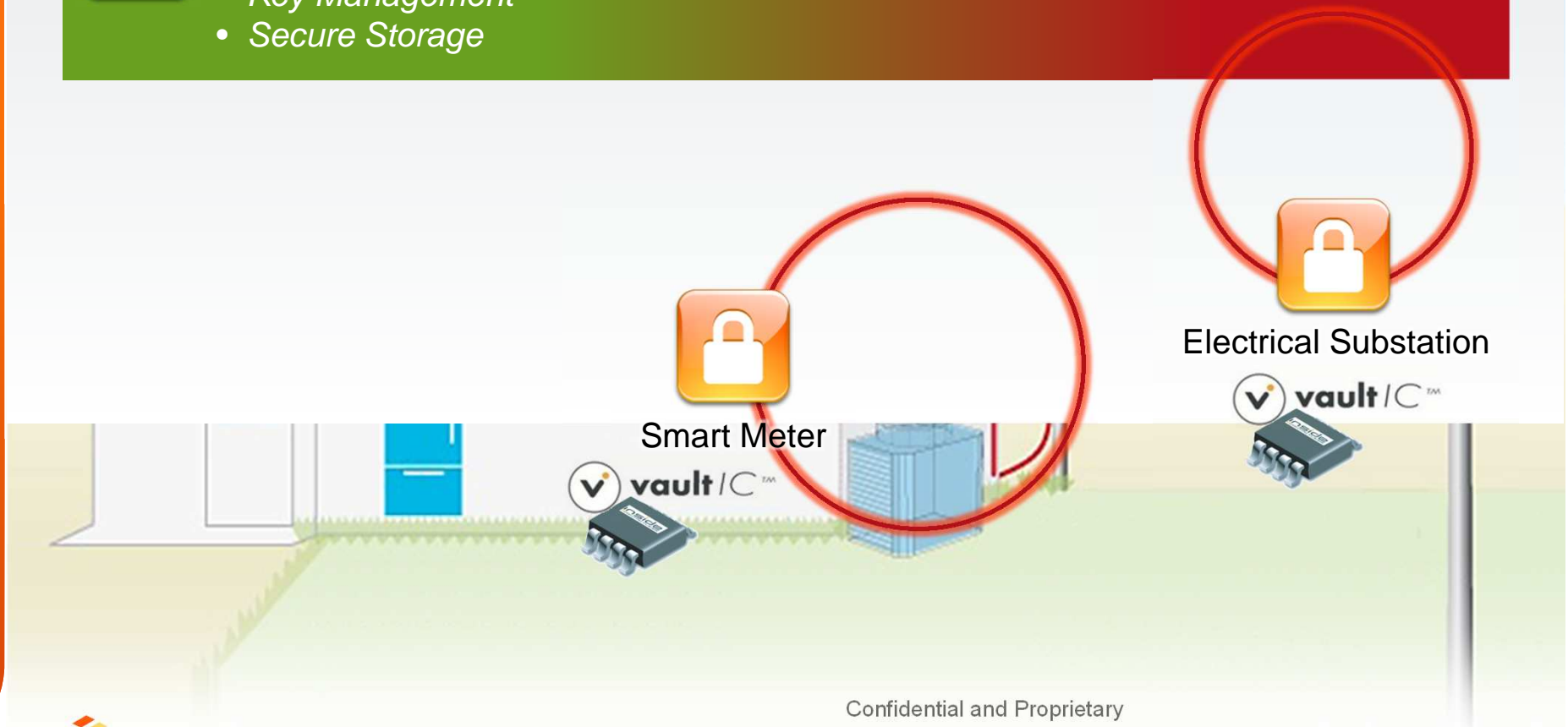
THREATS

Meter Fraud – Privacy – Network Control



VaultIC Security IC brings:

- Authentication
- Key Management
- Secure Storage



Challenges

- **Energy generation** and **distribution assets** needs to be better utilized due to increasing demand for energy
- Growing demand will to lead to **energy price increase**
- Provide customers **greater control over energy usage**
- Energy credits transfer between utility and its distributors and **pre-paid meter is to be secured**
- Pre-paid meter **casing is difficult to seal** because of slot to introduce payment mean (coins, token)
- **Pre-paid meter logs** transferred back to the utilities are **valuable information** for utilities



Our Solution

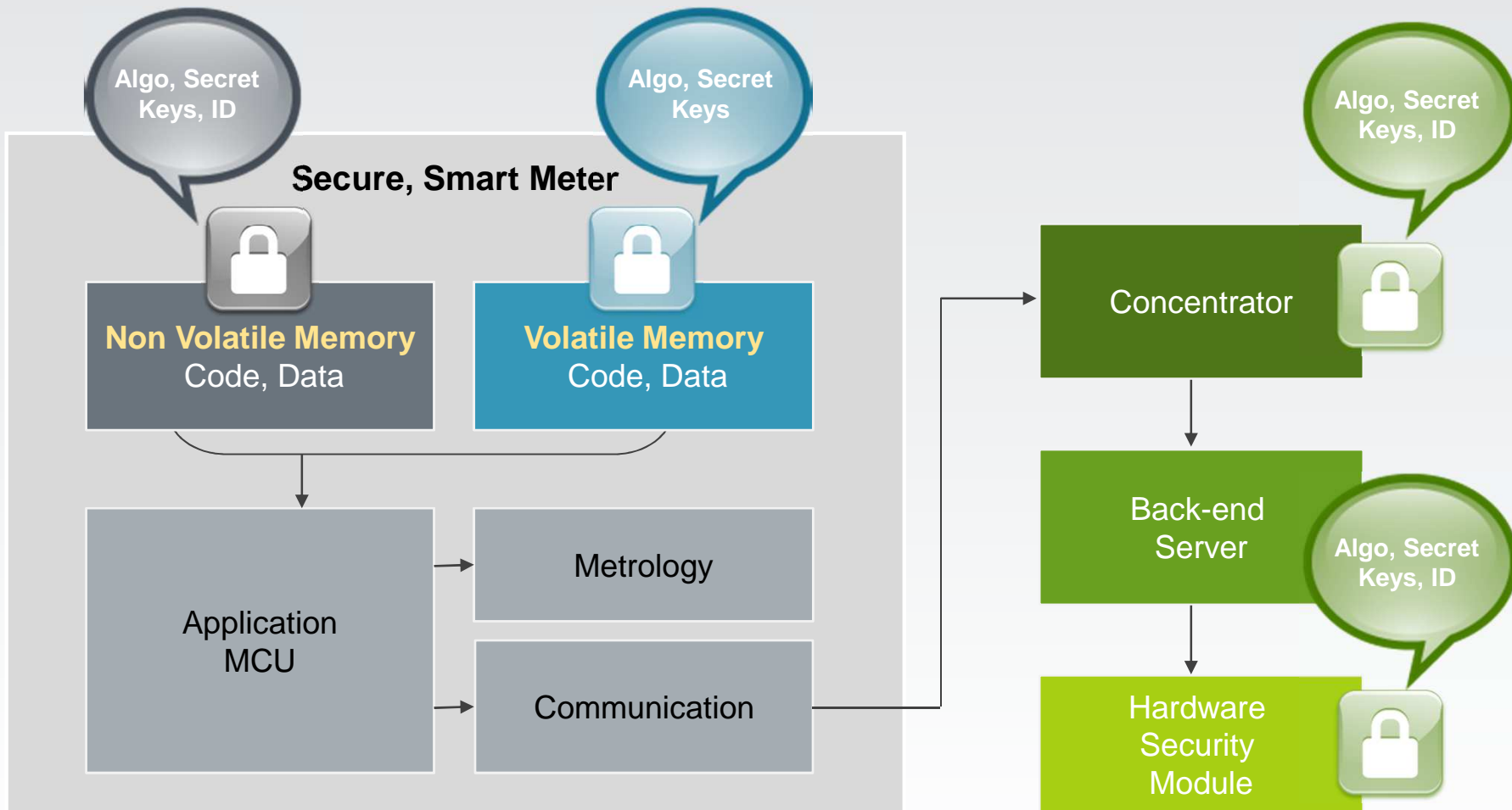
Freescale and Inside Secure have collaborated to develop a reference design supporting a **stand-alone secure, prepaid electricity meter** embedding **Secure Element + NFC reader** with associated **NFC enabled Phone** or **Contactless Smart Card**



Basic components of a secure prepaid meter

Secure prepaid, 1-ph electricity Meter

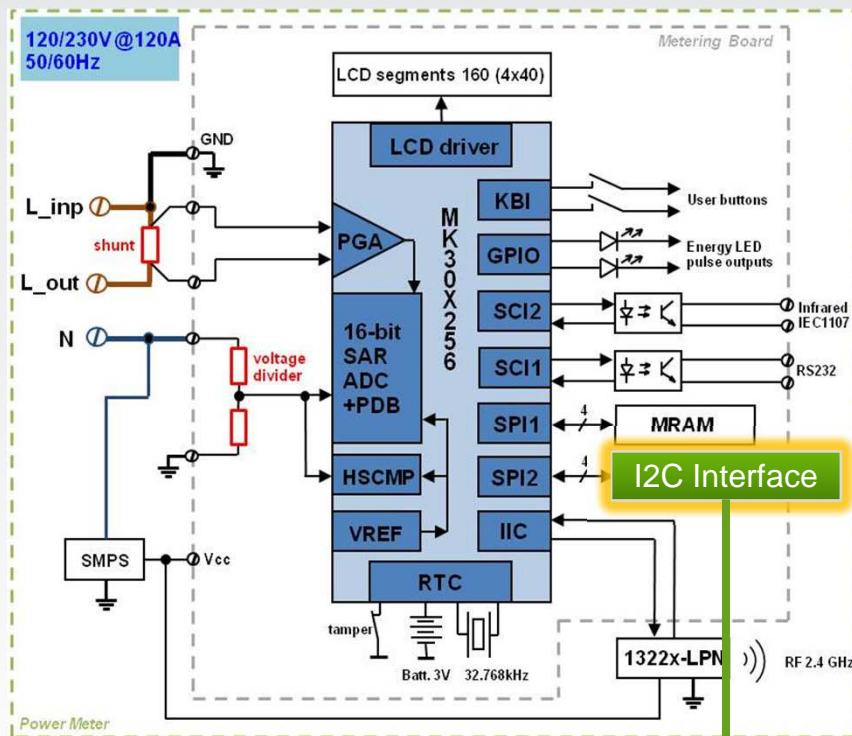
Block Diagram of Secure Smart Meter System



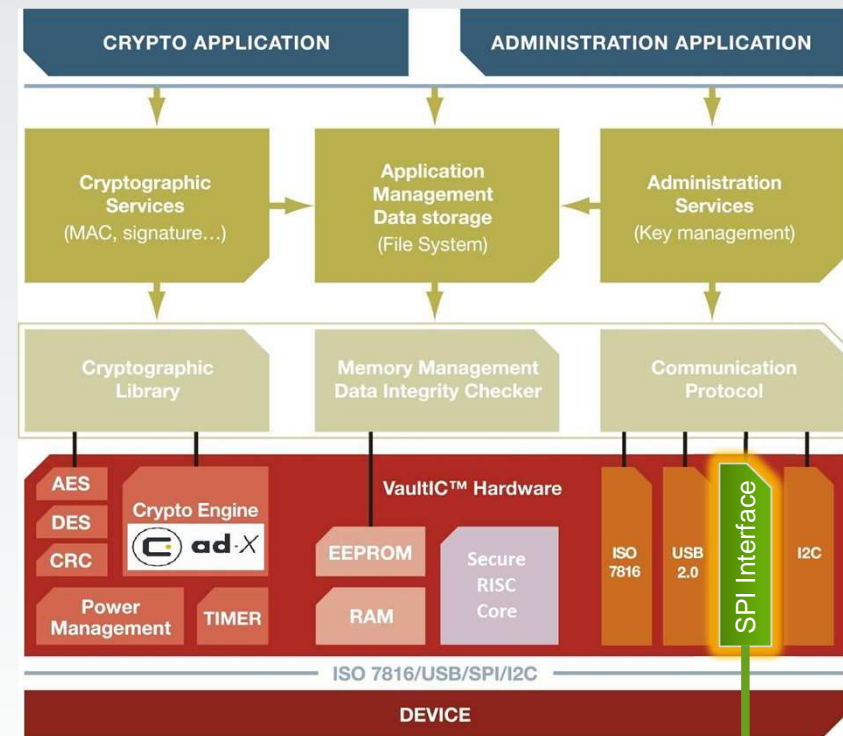
Security is achieved through Cryptography
 Crypto uses strong & proven algorithms (i.e. AES, ECC)

End to End Secure, Prepaid eMeter Reference Design From Inside Secure & Freescale

Freescale K30 ARM Cortex M4 1-ph Reference Design



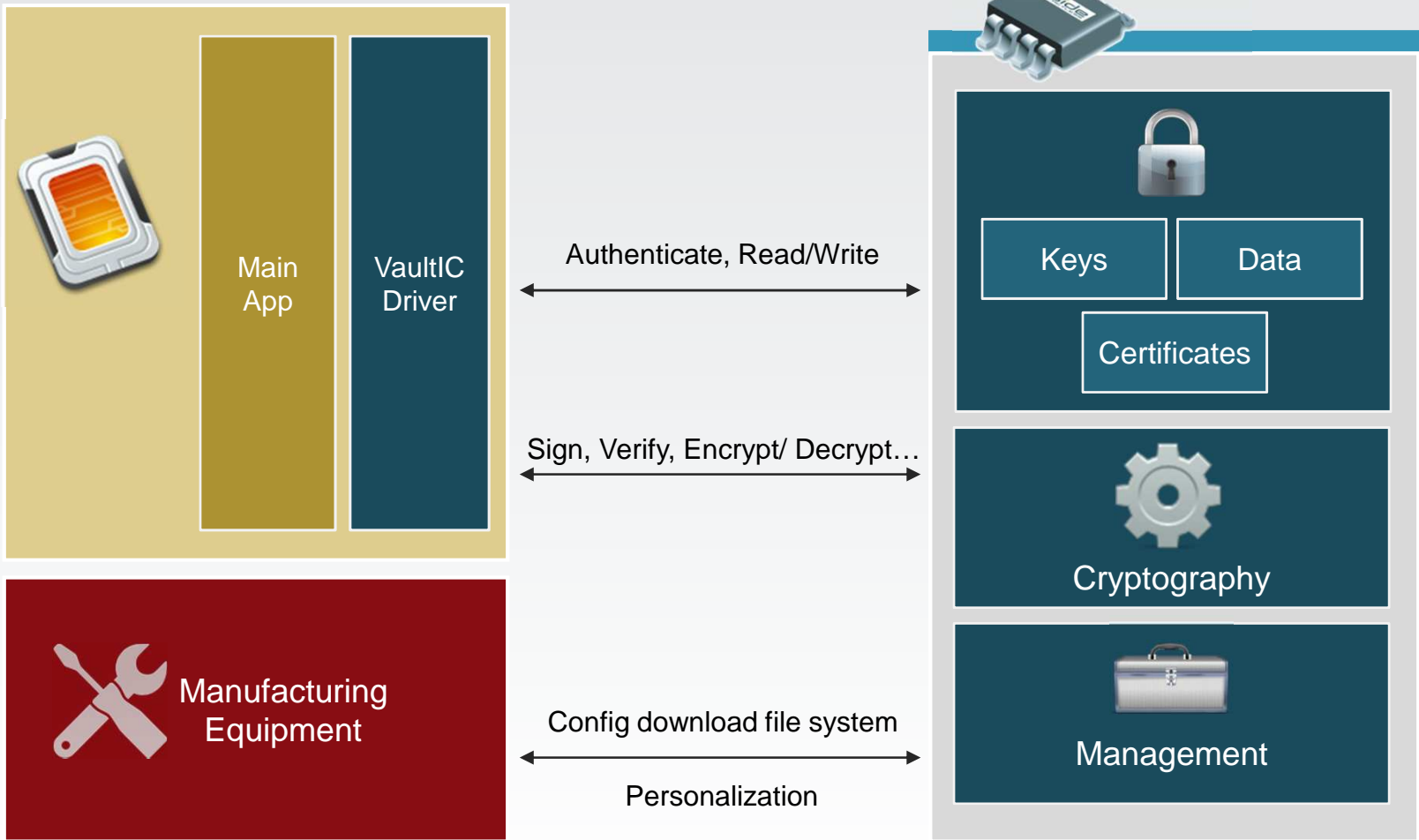
Inside Secure VaultIC Security IC



End to End Security
Secure Storage, Authenticate,
Sign/Verify, Encrypt/Decrypt



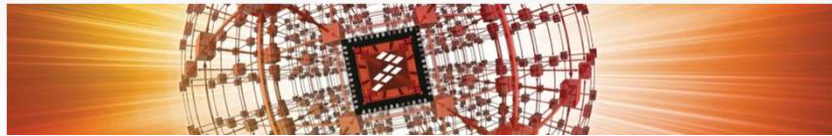
VaultIC™ Integration



VaultIC™ Secure Element Features

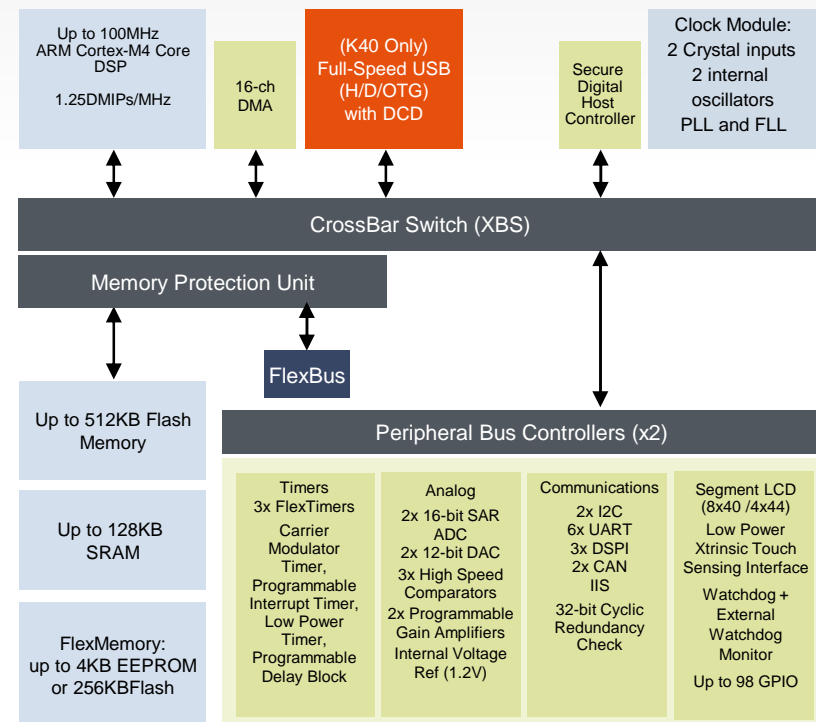
- Tamper resistance
- Secure Secret keys and certificates storage
- On board Keys generation
- Secure implementation of standards algorithms (i.e. AES, ECC)
- Security functions: Mutual Authentication, Verify / Generate certificate, Encryption / Decryption
- True Random Number generation
- Security level evaluation by 3rd party, FIPS140-2 Level 3 ready, EAL4+ ready

Kinetis Family Overview



- Flexible, low power LCD Interface**
 - Segment LCD Blink mode lowers average power
 - Segment fail detect prevents erroneous readouts and reduces LCD test cost
 - Front/back plane reassignment provides pin-out flexibility and allows configuration changes in firmware
- Diverse communications suite**
 - A multitude of serial interfaces, with UART support for ISO7816 SIM/Smart Cards and IrDA interfaces
 - Dual CAN for industrial network bridging
- System reliability & safety**
 - Hardware Cyclic Redundancy Check safeguards memory contents and communication data
 - Memory Protection Unit increases software reliability
 - Independently-clocked watchdog prevents code runaway for fail-safe applications e.g. IEC60730
- Hardware and software compatibility**
 - Common packages & peripherals across families enable rapid feature growth with minimal hardware and software disruption
- Built-in voltage regulator (K40)**
 - 5V regulator input with 3.3V regulated output
 - 3.3V regulated output can power MCU and also external components (source current up to 120 mA)

K30/K40 Family Block Diagram



- Enablement Bundle
- TOWER development system
- Complementary MQX RTOS with USB Stack
- Eclipse-Based CodeWarrior 10.0 IDE
- Processor Expert Rapid Application Development Tool
- IAR, Keil and Full ARM Ecosystem Support

Family	USB OTG + DCD	Segment LCD
K30	-	X
K40	X	X

Confidential and Proprietary

Features & Benefits of the Reference Design

Feature	Benefits
Secure VaultIC™	Provides End to End security between the meter and utility and its energy credit distributors. This is possible through Strong authentication, Secure Storage, Secure Channel (Authentication, Confidentiality) of Secure VaultIC
NFC Microread®	Enables physical security of meter through hermetic sealing Energy balance reload through near field communications Enhancements for remote secure interfacing (through smart phone) – ability to reload the meter’s balance and anti-counterfeiting check Meter logs Secure transfer from NFC enabled smart phone to utilities sever
MK30 metering MCU	Integrated Metrology Solution based on popular ARM Cortex™–M4 Core
Hardware schematics	Readily available schematics reduce design time
Software	Complete Security software stack available Advanced metering algorithms (Fast Fourier Transform) source code provided
MQX RTOS	MQX™ RTOS based design is suitable for advanced markets
Cost-effect BoM	Results in competitively priced end product

Support and Availability

The Secure, Prepaid 1-ph electricity Meter units are available on loan. Please contact your local Freescale Sales person or Freescale Distributor.

Following Collateral available at: freescale.com/metering

- Press Release of Freescale and Inside Secure
- Secure prepaid meter Fact Sheet
- Presentation on Secure Prepaid meter solution
- You-Tube Video of Secure, pre-paid ref. design

Smart Grid and Smart Metering

Freescale solutions for smart metering and smart grid address the challenge of efficient energy management and distribution. Understanding that embedded control and integrated connectivity will be at the heart of future smart grids, Freescale delivers intelligent controllers for smart electricity, water, gas and heat meters in addition to home energy management systems, communication solutions, including robust power line modems and low-power radios, enabling automated meter reading.

Smart Grid and Smart Metering Applications

- Home Energy Management Systems
 - Metering Data Concentrator
 - Substation Automation **NEW**
 - Solar Power Inverters
 - Residential Solar Power Inverters
 - Commercial Solar Power Inverters
 - Off-Grid Solar Power Inverters
 - Electricity Meters
 - Polyphase Electricity Meter
 - Low-End Mechanical Type with AMR Add-on Meter
 - Low-End Electronic Type Meter

Design Resources

- Getting Started
 - Low-Power Micro
 - Motor Control
 - Single Board Com
 - Smart Energy Bro
- Reference Designs
 - MPC8308 Network
 - i.MX28/MC13224V Reference Platform
 - MK30X Single-Ph
 - MCF51EM Polyph
 - Single Phase Digi
 - 9S08LL Thermost
- Technologies, Stand
 - IEEE 802.15.4
 - ZigBee
- Design Partners
 - All Freescale Alliat



Industrial, Connectivity

Secure Pre-Paid eMeter Reference Design

Overview

This reference design provides a secure pre-paid eMeter with the ability to securely reload an energy balance. The secure element from Inside Secure allows for implementation of end-to-end security between the pre-paid meter and the utility companies and distributors who sell energy credits. Integrated NFC connectivity allows users to upload energy credits using contactless smart card technology or an NFC phone. Firmware for this reference design is based on the MQX™ real-time operating system. All standard metering values are displayed on the built-in LCD and selectable via the built-in push button. A variety of communication interfaces are available for remote data collecting, making this an idea solution for residential metering.

Key Features

- End-to-end security between the meter, the utility company and energy credit distributors
- Physically secure: Hermetically sealed meter casing via NFC technology
- NFC energy balance reload
- 5–60 amp current range
- 85–264-volt range
- 47–63 Hz frequency range
- Four-quadrant measurement (lead/lag energy)
- Active and reactive energy accuracy: IEC50470-3 Class B, one percent
- Meter constants (imp/kWh, imp/kVAh): 500, 1000, 2000, 5000, 10000



Secure pre-paid meter using MK30 MCU



- Line frequency measurement
- Cost-effective shunt resistor sensing circuit implementation
- Cost-effective bill of materials
- Effective implementation of low-power modes, including use of the built-in real-time clock
- LCD display with charge pump
- Values displayed on the LCD: V, A, W, VAR, VA, kWh, kVAh, cos φ, Hz, time, date
- OBIS identifier on the LCD
- Tamper detection via two tamper buttons or magnetometer (event is stored in memory)
- Built-in push button
- LED pulse outputs (kWh, kVAh)
- Optically isolated open collector output
- IEC1107 infrared hardware interface
- Optically isolated RS232 interface
- MQX-based for advanced markets
- Advanced metering algorithm based on the Fast Fourier Transform (FFT)
- Optional ZigBee communication

Related Documentation

- Readily available application firmware for balance reloading scheme and related security functions
- Design reference manual: DRM122
- Application note: AN4255
- Quick start guide for MK30 secure meter
- MQX reference manual and user guide
- Device development tools/demo kits
- Device documentation: MK30X256, VaultIC™460, NFC (Microread® 3.4)



MK30X256 Microcontroller

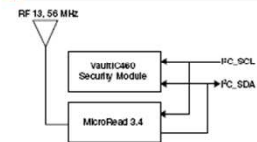
- Up to 100 MHz frequency with 1.25 DMIPS/MHz
- ARM® Cortex™-M4 Core
- 256 KB of program flash memory
- 256 KB of FlexNVM and 4 KB FlexRAM
- 64 KB of SRAM
- 16 independently selectable DMA channels
- Integrated 16-bit SAR ADCs with PGAs
- Two integrated 12-bit DACs
- Programmable 1.2-volt voltage reference
- High-speed analog comparator with 6-bit DAC
- WDOG + external watchdog monitor
- Hardware CRC generator circuit (16/32-bit)
- External bus interface (FlexBus) for external memory, gate-array logic or LCD
- Communications: CAN, PC, IIS, SDHC, SPI, UART
- Timers: FlexTimers, programmable delay block, programmable interrupt timer, low-power timer, carrier modulator timer, RTC
- Human-machine interface: Touch-sensing, segment LCD

- 10 low-power operating modes
- 144-pin LQFP or MAPBGA packages
- -40°C to +105°C operating temperature range

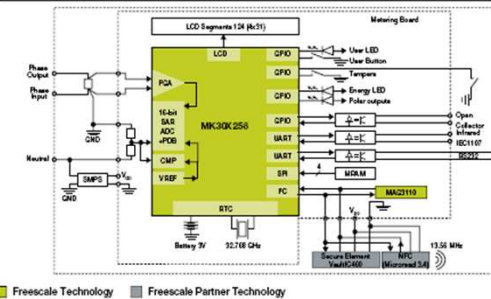
VaultIC™ Secure Element Features

- Tamper resistance
- Secure secret keys and certificates storage
- On-board key generation
- Secure implementation of standards algorithms (i.e. AES, ECC)
- Security functions: Mutual authentication, verify/generate certificate, encryption/decryption
- True random number generation
- Security level evaluation by third party
- FIPS 140-2 Level 3 certified, EAL4+ ready

VaultIC—NFC Connectivity



MK30X Single Phase Secure Meter Block Diagram



For more information, visit freescale.com/metering

Freescale and the Freescale logo are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. ARM is a registered trademark of ARM Limited. Cortex-M4 is a trademark of ARM Limited. All other product or service names are the property of their respective owners. © 2011 Freescale Semiconductor, Inc.
Document Number: SECPEMTRFS REV 0

