



**Understand Electronic-Meter  
Design to  
Better Craft Intelligent and  
Secure Systems**

**driving trust™** **inside**  
SECURE

[www.insideseecure.com](http://www.insideseecure.com)

## AUTHOR, INSIDE SECURE

As more utility companies install smart electric and other types of utility meters to better collect usage data from their customers, the utilities continue to examine approaches to create still better electronic-metering solutions. To do that, organizations are directing the development of an advanced metering infrastructure that will rely on new communications, encryption, and semiconductor solutions that will, in turn, require the development of a new generation of smart meters that are secure, cost-effective, and have high reliability.

Today, there are close to two billion electricity meters installed worldwide, but less than 10% of them are considered “smart” meters with two-way communications. That will change over the next few years as next-generation meters are developed and installed. Add to those numbers the meters used for gas and water, and the number of meters can easily double to four billion or more. One of the major challenges facing the utility companies and the electronic-meter suppliers is the cost of the e-meters and the cost of refitting the infrastructure to support the two-way communications.

Next-generation smart meters will provide a gateway into the home and allow both the utilities and consumers to manage consumption. Utilities can set up dynamic pricing to provide incentives to consumers to shift peak loads, while consumers can better track their usage and decide when not to use appliances that consume large amounts of power to reduce their energy bills. Data regarding usage can initially be accessed over the internet using a PC or smart phone that links to the utility so that consumers can access off-line usage data, but in the future consumers might be able to directly log onto the smart meter to get real-time consumption data. Keeping that data secure is one of the major challenges facing both the utility companies and the e-meter vendors.

Local attackers have physical access to the meter, network gateway, or a connection between these components. They can try to disclose or alter assets that are stored in the meter or gateway or while data is being transmitted between meters in the metropolitan area network and the gateway. This threat model assumes that the local attacker has less motivation than the WAN attacker since a successful attack of a local attacker will only impact one gateway. The local attacker could also be the consumer trying to get services without paying for them.

An attacker located in the WAN (WAN attacker) can try to compromise the confidentiality and/or integrity of the meter data and/or configuration data transmitted via the WAN. Or the attacker can try to conquer a component of the infrastructure (i.e. meter, gateway or controllable local system) via the WAN to cause damage to a component itself or to the corresponding grid (e.g. by sending forged meter data to an external entity). Even though in the concept of Common Criteria the attacker with the highest attack potential (which is the WAN attacker with a high attack potential) determines the level for the vulnerability analysis, the definition of following threats acknowledges that the local attacker has less attack potential than the remote attacker. (Please also refer to chapter 6.11.2 in the Protection Profile for the Gateway of a Smart Metering System published by The German Federal Office for Information Security, v1.01.1 draft)

When designing the e-meters, there are several key concerns – meter power consumption, cost and reliability. Both power consumption and costs have to be as low as possible to ensure the millions of meters don't add any significant power drain to the grid, and at the same time, the meter cost must be low since the utilities must be able to cost-justify replacing the old meters. The reliability requirement is an obvious demand due to the long life time and nature/quality of the service. Additionally, as mentioned earlier, the meters must be secure – data encryption has to be an integral part of the meter design to ensure that hackers can't collect personal data or gain access to the utility's network.

The companies designing the smart meters must account for the different regulatory requirements of each region around the world, as well as for the different services and functions that each market requires. Automated meter reading regulations in the U.S., for example specify the frequency of meter readings, the data transmission scheme, and the amount of data that must be stored locally in the meter at any point in time. The amount of data the system must store to insure against data loss, will affect the amount of local memory needed in the smart meter, and that may have an impact on component selection and cost.

In Germany, the BSI defines a Security Protection Profile for the communication Gateway interfacing with the Wide Area Network and mandates usage of a security module. This gateway is to reach a Common Criteria EAL4+ security level. The VaultIC4xxx Security Module is one of several security solutions in the industry that already offers this security level, reducing to its minimum the certification effort for the gateway manufacturer.

## SMART METER BASICS

Although the definitions vary somewhat, a smart meter monitors energy, gas, or water consumption and displays the consumption in real-time, typically on a LCD display. The meter also has a communications interface - in the U.S., many companies have standardized on the ZigBee wireless radio as the link to the utility, while in Europe, many utility groups have agreed to use power-line communications to link the meters to the utility. These communication interfaces also have to be low power even though they spend most of their time in a "sleep" or standby mode.

The electric utility's transition from fixed-rate billing to a time-of-use billing arrangement is driving the creation of second-generation e-meters that are smart enough to handle time-of-use billing and allow for automatic meter reading (AMR). This changeover will require more powerful microcontrollers, wireless radios, information rich LCDs, and real-time-clocks (RTC) to supplement the analog front end (AFE). For the first meters in this generation, multiple chips will be used to provide all the functions. However as the utilities try to drive down the cost, the component/meter suppliers will further integrate the components

At the heart of the smart meter is a low-power microcontroller coupled with an AFE. In an electricity meter, the AFE senses the current and voltage, converts the sensed values into digital form, and then sends the digital values to the microcontroller, which processes the data, stores the reading in local memory, displays the information on a small LCD screen, and on a regular schedule, uploads the data to the utility via a communications interface (Figure 1). For applications in gas or water consumption metering, extremely low power consumption will be an additional requirement since the meters may have to be battery powered and that battery will have to last several years. Or, some type of energy harvesting power source may be used to eliminate the battery.

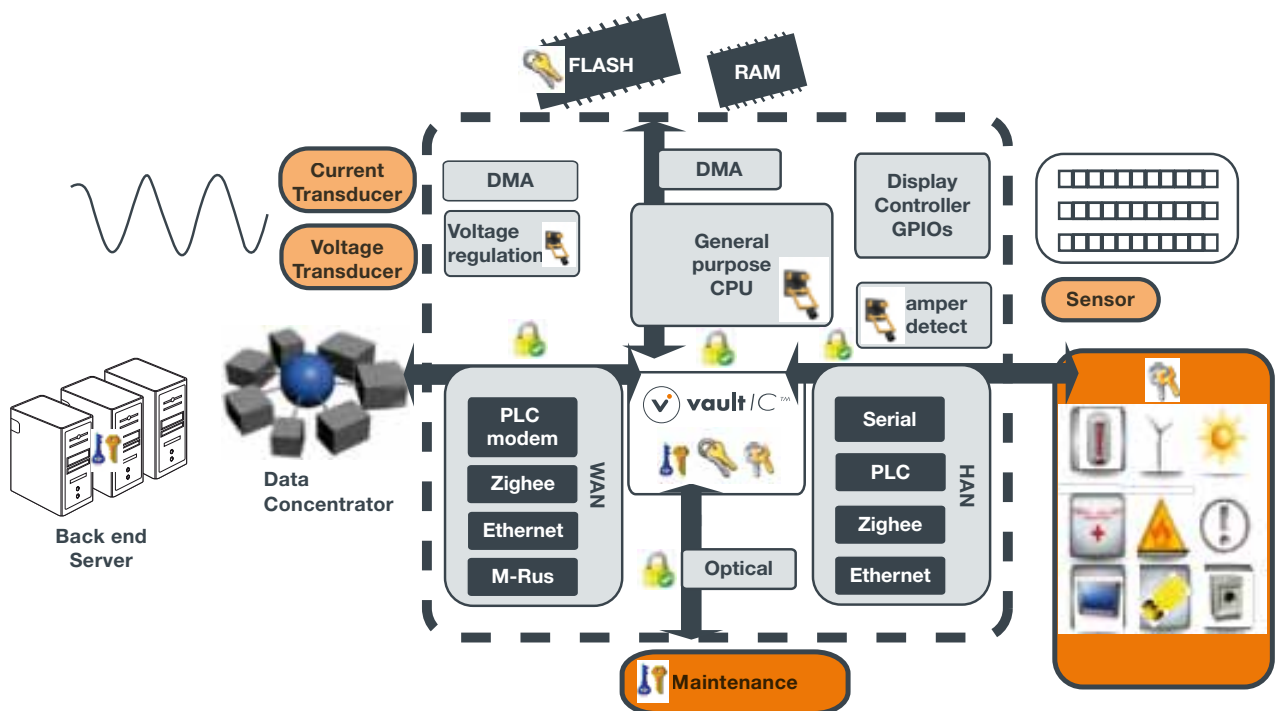


Figure 1: A typical secure smart electricity meter leverages the VaultIC460 from INSIDE Secure to provide data security and tamper protection. The meter also contains an analog front end to sense the power usage, a secure microcontroller to process and display the collected data, and a communications interface to send the data back to the utility company

Another important aspect of smart meter design is protecting the meter from tampering – there are many markets around the world where utility theft accounts for a significant portion of total usage. By incorporating various sensing schemes that detect if the meter case is opened, or a probe inserted, or a strong magnet brought nearby, or some other tampering approach, the meter can send a message back to the utility or even lock out the customer until a service technician comes out to determine the actual event that triggered the tamper warning. Such an approach can help the utilities to exert better control and reduce unmetered losses.

To design a meter, the best way to start would be to define a common platform that can be used across multiple applications and regions with just a few minor variations. Then, determine the amount of computational horsepower the internal microcontroller (MCU) will need to perform all the tasks. There are many off-the-shelf highly-integrated MCUs that can handle the task, but when the low-power-consumption constraint and data-encryption requirements are added to the mix, the choice narrows considerably. Of course there is always the option of crafting a dedicated system-on-a-chip (SoC) that is tuned for the electronic-meter application, but the cost and development time may be an issue for that approach. However, the final solution could lower overall system cost by eliminating many of the discrete components.

Combining cryptographic services and a 8/16 bits RISC processor, the VaultIC4xx family delivers a secure control solution for metering and many other applications (Figure 2). Included on the chip is a true random number generator as well as a hardware triple-DES crypto accelerator (112-bit keys), a hardware AES crypto accelerator, and a hardware 32-bit public-key crypto accelerator.

The AdX accelerator consists of an N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secure processor core which uses the AdX accelerator during encryption/decryption. AdX is based on a 32-bit technology, thus enabling fast computation and low power operation. AdX supports standard finite fields arithmetic functions (including RSA, DSA, DH and EC) and GF(2<sup>N</sup>) arithmetic functions (including ECC). Additional security features include power, frequency and temperature protection logic, logical scrambling on program data and addresses, power analysis countermeasures, and memory accesses controlled by a supervisor mode.

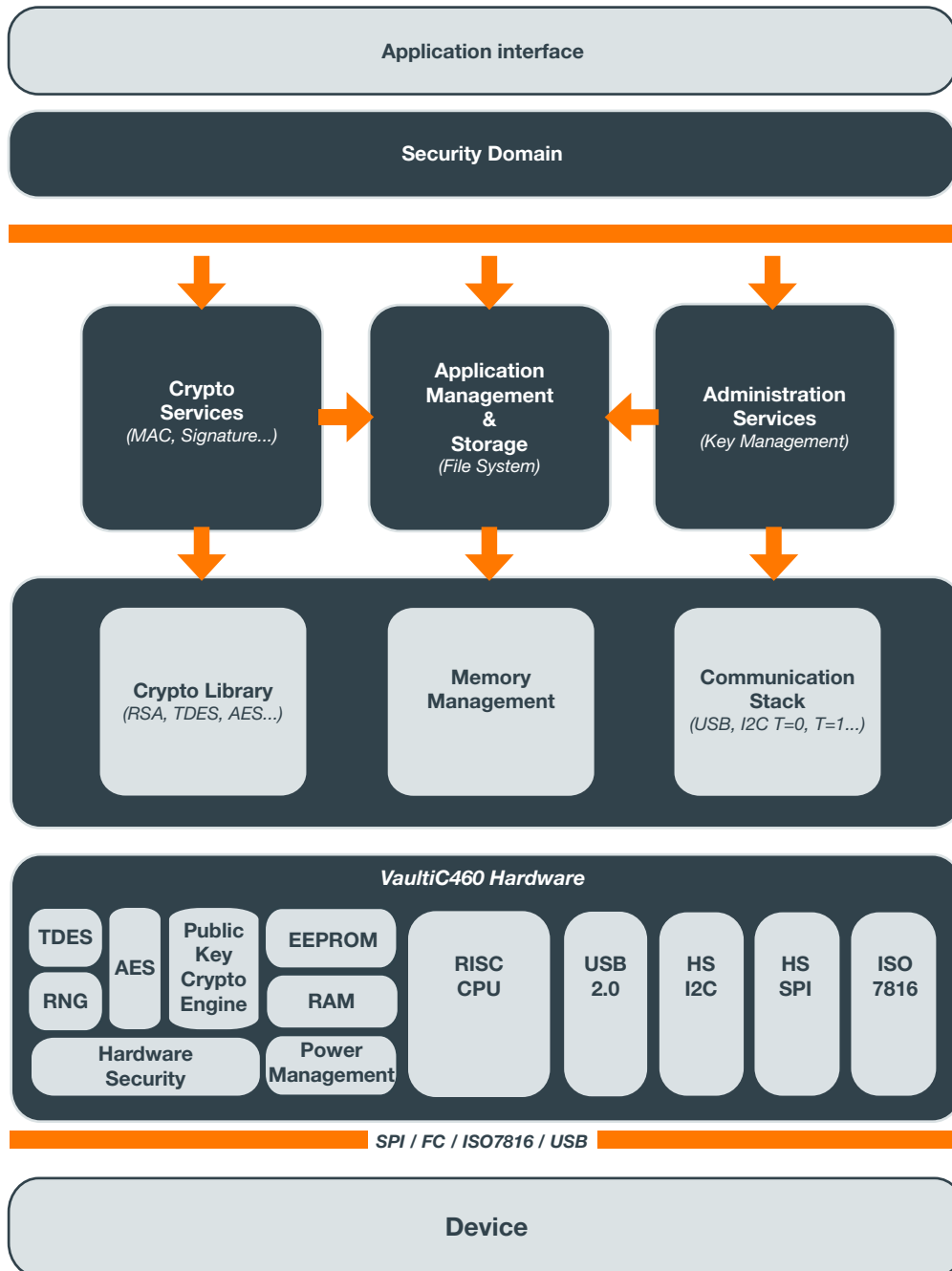


Figure 2: A highly-integrated system-on-a-chip, the VaultIC4xx solution includes many acceleration engines for multiple crypto algorithms as well as an 8/16-bit RISC processor core and lots of on-chip storage – up to 128kbytes of reprogrammable EEPROM.

With these on-chip hardware acceleration engines the VaultIC4xx series can handle DES/3DES algorithms as well as AES 128/192/256-bit algorithms, RSA algorithms up to 4096 bits, DSA algorithms up to 2048 bits, and Elliptic Curve algorithms up to 384 bits. The security features allow the controllers to provide FIPS 140-2 identity-based authentication using password, Secure Channel Protocol (SCP02/SCP03) or Microsoft's minicard driver strong authentication. Additionally, the controllers are EAL4+ ready and can also support FIPS 140-2 level 3, Microsoft CSP minidriver, SSL, PKCS#11 and other certifications and standards. A typical secure communications channel can be implemented with the VaultIC4xx on a network adapter card that can be used in an electronic meter is shown in Figure 3.

Designed to keep its memory contents secure and avoid leaking information during code execution, the VaultIC4xx controllers include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised.

Tampering can take many forms, and it is not always a hacker – even service personnel can access the meter and compromise the data. In fact, about 25% of all reported data security breaches are the result of malicious insider activity. For example, during meter maintenance when diagnostic tools are connected to the meter to log, fix, or update the meter software, the service person can access the secure data. To prevent that, human intervention must be locked out via the security engine to eliminate the possibility of data manipulation or the installation of malicious modifications.

Strong Authentication capability, secure storage and flexibility thanks to its various interfaces (USB, SPI, I2C, ISO7816), low pin count and low power consumption, the ATVaultIC4xx series provides all the control hardware the meter needs. Additionally, the embedded firmware stored on the chip provides advanced functions such as Identity-based authentication, a large cryptographic command set, various public-domain cryptographic algorithms, cryptographic protocols, secure channel protocols, and robust communication protocols.

A VaultIC evaluation kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC security products. In the kit is the VaultIC460 with 1 dedicated test socket, a VaultIC460 USB dongle, or 1 generic USB to SPI /I<sup>2</sup>C adapter, a CD-ROM containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the VaultIC features, the “VaultIC Manager” tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code.

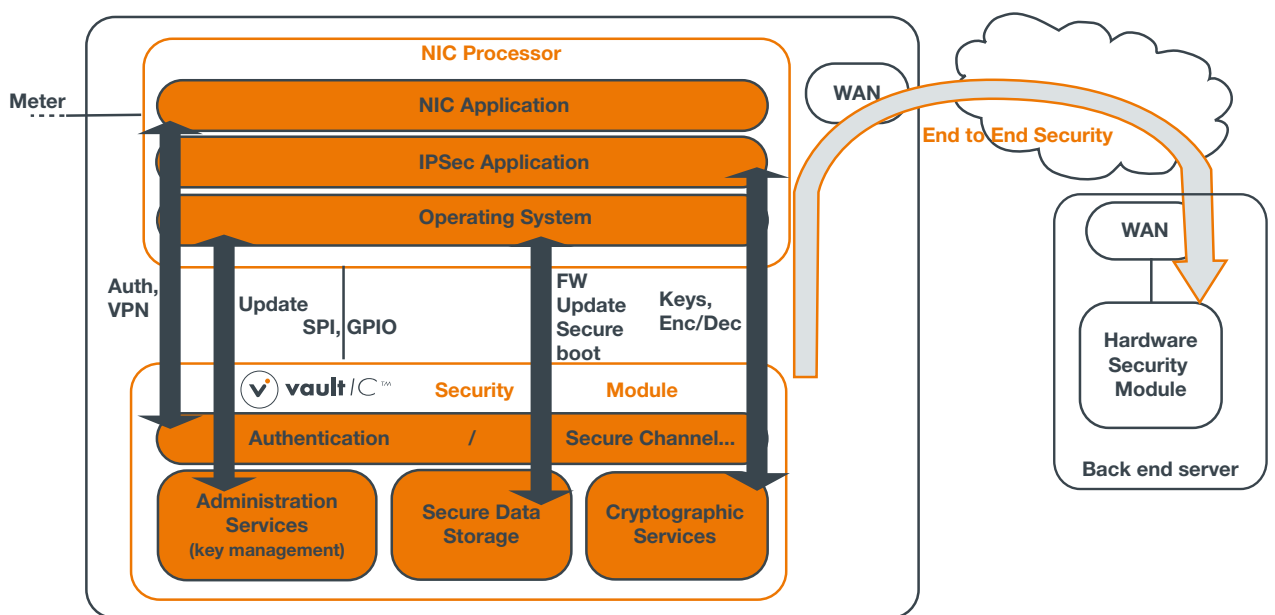


Figure 3: Security Module inserted into a Network Interface Card.

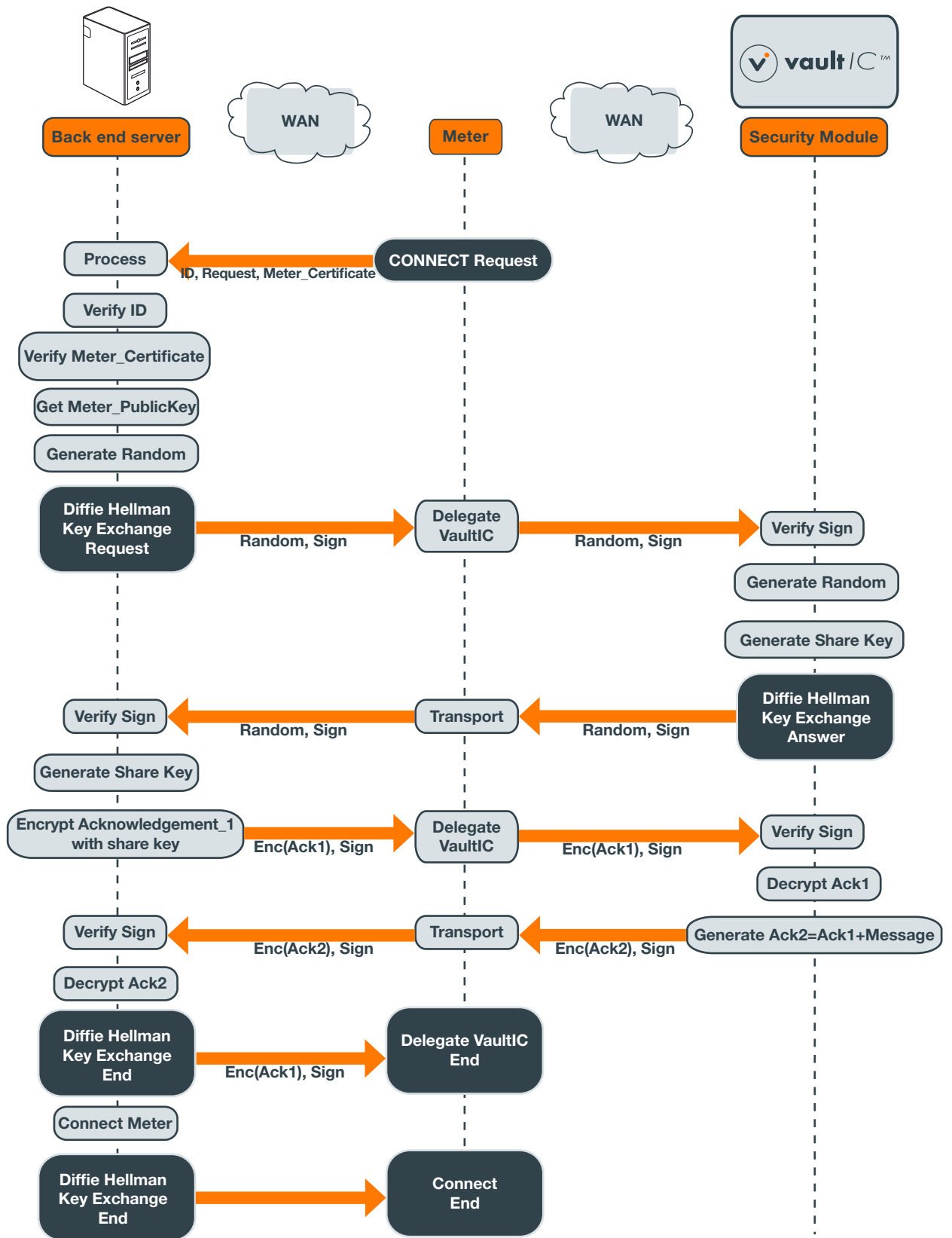


Figure 4: Authentication Sequence diagram to secure a channel using VaultIC, Diffie-Hellman based.

VaultIC460 is able to setup and establish secure communication between a smart meter and remote server. Here upper example is based on Diffie Hellman key exchange method with message signing to avoid a “man in the middle” attack. This method is generating a secret key between VaultIC and Remote server without exchanging/disclosing any secret. This key is then used to encrypt all communication frames during a session. It could be initiated from the smart meter or from the server.

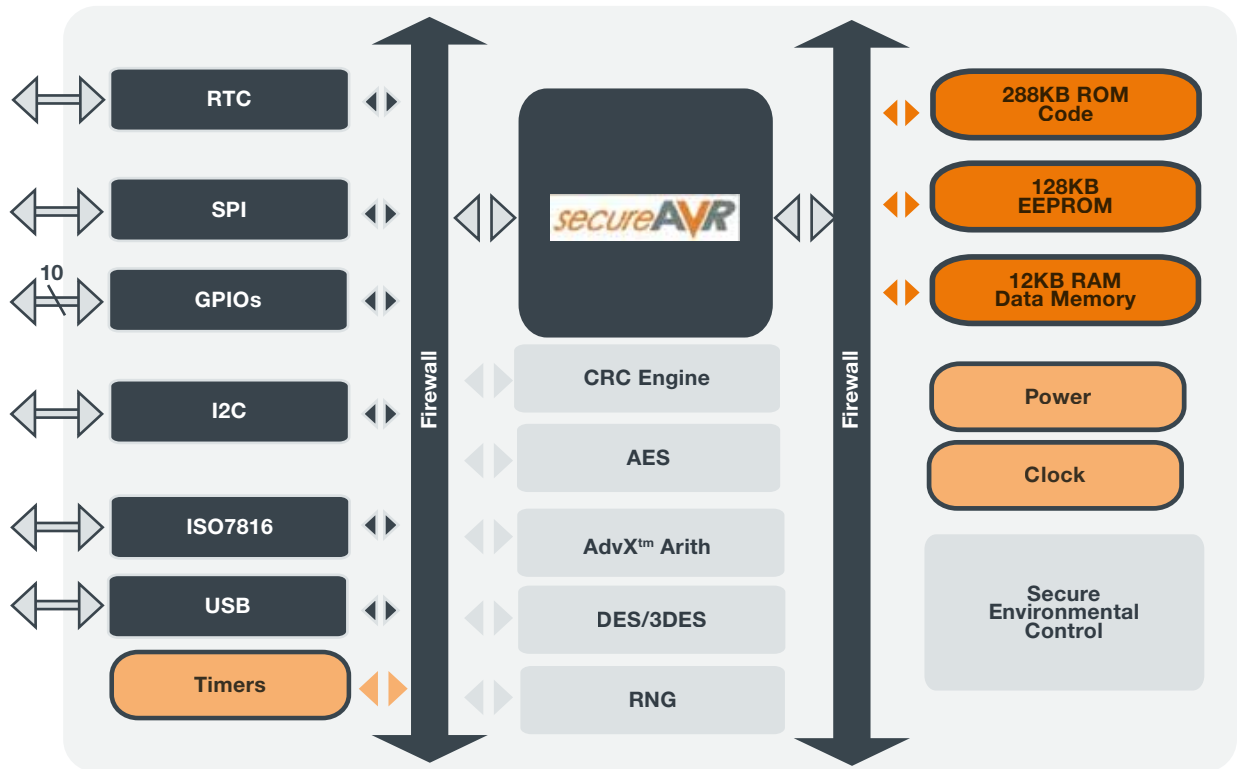


Figure 5: Based on a 8/16 bit RISC advanced secure processor core, the VaultIC4xx solution from INSIDE Secure allows a real hardware firewall to be used to increase the overall security level of the application, thus reducing the software overhead.

Although various microcontroller vendors have MCUs that include on-chip analog-to-digital converters (ADCs), the signal capture and conversion requirements often lead to the use of a separate analog-front-end chip. Such chips are designed to sense the usage (electricity flow, gas flow, water flow, and convert the sensor output into digital form so that the consumption data can be analyzed. For instance, in an electric meter, a single-phase or polyphase front end can incorporate many advanced power-monitoring features such as power factors, vector sum, and harmonic components. Metering accuracy and electric fast transient (EFT) response are critical requirements for electric meter designs.

Depending on the region of the world where the meter will be installed, designers may end up selecting a different communications interface. For instance, in most of Europe, many of the utilities have standardized on power-line communications (PLC) for transferring meter data to the utility. In the U.S. many utilities have standardized on the wireless ZigBee radio and protocol for use in the meters. The ZigBee transceiver can be set up to work in a mesh type network that offers high levels of connectivity and very low power consumption since the ZigBee transmitters are typically powered-up for only a few milliseconds during each cycle, thus keeping the average power consumption very low. These developments and many others in the communications market make it difficult to predict which communication technology, if any, will dominate in the future.

As mentioned earlier, the utility networks require security and higher-layer interoperability as defined in ANSI C12.19 to ensure the various Smart Grid subsystems function as a secure network of networks. There are additional technologies in development to help ensure communications between networks will be reliable and secure. Currently many systems employ established algorithms such as AES and Elliptic Curve. In the future, the 128-bit encryption will probably be replaced by 256-bit schemes for a higher level of security in the utilities' networks. Standards such as ZigBee Smart Energy 2 and 802.16 WiMAX call for that level of security. For a list of standards being developed for the U.S. Smart Grid, go to

**<http://smartgrid.ieee.org/standards/ieee-smartgrid-standards-in-development>**