

# UMI – THE USB FOR SMART METERING



By Alistair Morfey

**The Universal Metering Interface (UMI) is a set of three free specifications to help develop smart metering, smart energy and smart appliance products. These specifications define a module interface based on SPI, an optical interface based on EN62056-21 (FLAG port), and a security interface based on ECC-256 and AES-128. The specifications can be downloaded freely and do not involve a licence fee.**

So why do we need another interface definition? This article explains the arguments. They apply to all smart energy systems around the world, but the examples focus primarily on Europe and the UK.

UMI helps you to develop ultra low power secure modular products that protect your R&D investments. By reducing obsolescence, UMI products can support more functional variations, enabling them to be sold across more regions for more years.

UMI enables you to use existing communication modules in your product development. These could be HAN modules for a meter or WAN modules for a communications hub. UMI peripherals have already been developed for ZigBee, Wireless M-Bus, GSM, DECT and WiFi.

UMI has been adopted by Elster Gas in Europe. Their domestic gas meter uses UMI-spi and UMI-opto in its electronic index.

The IET recognized these benefits by picking UMI as the winner of their 2010 Innovation Award for Information Technology.

## SMARTER ENERGY

A major goal for smart metering systems is to enable homes and industry to make smarter energy decisions leading to reduced carbon emissions (as required by the EU 2020 energy targets). We think this is most likely to happen if the smart metering systems (white boxes on the metering HAN in Figure 1) stimulate the adoption of smart appliances and micro-generation (green boxes on the consumer HAN).

The communications architecture in Figure 1 is one way to achieve this goal, but there will be several others. Even within this architecture there are many different technologies that could be used for the

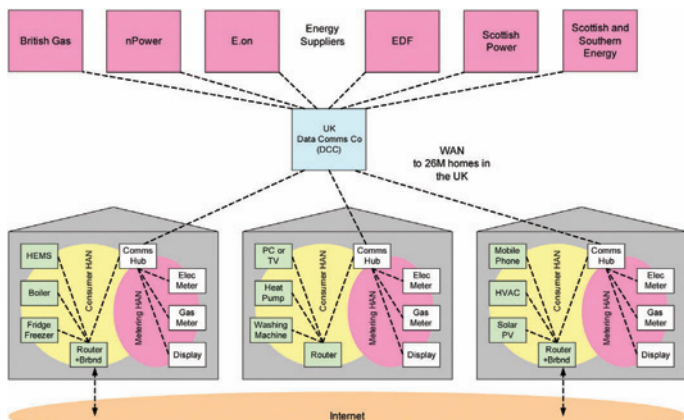


Figure 1 – Communications architecture for smart metering and smart energy in the UK

WAN, the metering HAN, the consumer HAN, the network layer, the transport layer, the security and the application layer data objects.

## UNCERTAINTY

Smart metering standardization is not happening as fast as everyone had hoped. Some programmes in Europe have been delayed and there has been a general acceptance that the level of security and personal data privacy required for smart metering products is actually much higher than previously thought necessary. The commercial ownership of meters varies greatly from one country to another, which has led to different preferred communications solutions with a variety of wireless and wired technologies being considered. The functionality required in a smart meter also varies from one country to another, with different views on prepayment, time-of-use pricing, remote disconnect and many other functions. Within a given country, the functional requirements often vary considerably from one month to another! So we can see that in most countries there is still a high degree of uncertainty.

By contrast, the metrological parts of a meter are stable. In Europe all meters must comply with the MID (Measuring Instruments Directive). This can enable substantial parts of a “dumb” meter to be standardized across Europe, enabling larger economies of scale and lower unit costs.

## MODULAR vs MONOLITHIC

This has encouraged some manufacturers to adopt a modular architecture for their equipment, separating the certain (dumb) functions from the uncertain (smart). The certain functions can be standardized across Europe and the uncertain can vary from region to region and from year to year (if necessary).

There are some advantages to a monolithic meter that combines the dumb and smart functionality in a fixed manner. But with so much uncertainty and regional variation, we feel that at present these are outweighed by the benefits of a modular architecture where different parts of the meter are joined with internal wired connectors and an associated protocol. It is much easier to achieve very long periods (decades) of backward compatibility and good performance from a simple wired interface, than it is from an RF interface where new interference sources can appear each year. This separation of functionality means that R&D investments are less likely to be wasted.

It is also interesting to note that once a meter is modular, it is possible for the different modules to be supplied by different manufacturers. Of course it is still important to be clear as to who is responsible for the overall product and its correct operation. It is also important that manufacturers can choose which organizations they do and do not want to partner with. Module A manufacturer might be happy to operate with module B, but not with an unknown module, so wants a module technology to enforce this.

This way of doing business is already used for gas meters in the USA where the meter body and index can often be from different manufacturers. This leaves the utility free to choose its favourite

meter body and favourite index, which frequently come from different manufacturers.

### UMI-spi

It would be good if the internal wired interface for modular smart meters could be based on an existing standard such as USB, Ethernet, SD card, RS232 or M-Bus. Unfortunately none of these have the required features for secure, low power, outdoor, damp, long life operation that is required for a meter, especially when battery powered.

UMI-spi is an internal wired interface that has been specifically designed for ultra low power smart metering products. It includes definitions for mechanical, electrical and protocol interfaces. It has a software protocol based on SPI that can be implemented in any small microcontroller.

Like USB, UMI is physically a star network with one host and up to fifteen peripherals. A typical meter might allocate functions so that the host is inside the metrological seal and the peripherals are outside. With this architecture, an MID-approved host can be standardized across Europe and the peripherals can be varied (to support different wireless or wired communications standards, data objects and application processing) as required from one region to another. In this case the host is fixed early and new peripherals are developed and changed for years afterwards. It also enables a “smart ready” meter to be installed without a peripheral. The peripheral can be fitted later when the “smart” requirements are known.

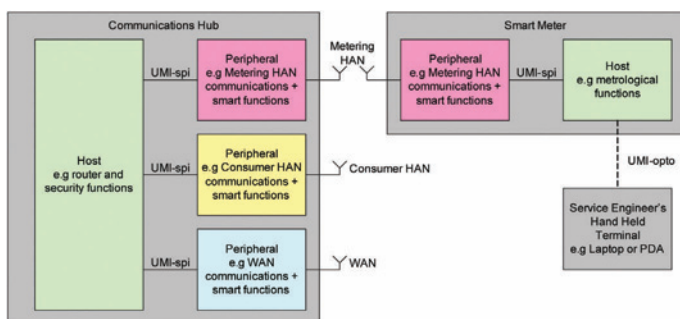


Figure 2 – Smart meter and communications hub based on a UMI modular architecture

Figure 2 shows how a smart meter or communications hub could be based on a UMI modular architecture.

A UMI host is the master of power and time within the product. It must always be powered and contain a UTC real time clock (usually synchronized to a central network time periodically). The host can turn the power to each UMI peripheral on and off individually. This is essential as a connector cannot be conformally coated and 3 V across a 50 kΩ water droplet would allow 60 μA to flow. This is four times the total current budget for a modern electronic gas meter!

The mechanical form factor can vary from one host to another, but is the same for all peripherals. A host can be fitted with different peripherals (see Figure 3) to support different communications



Figure 3 – Smart gas meter and ZigBee UMI Peripheral

standards, because they are all the same physical size and shape. There are no software drivers in the host, so a change of peripheral does not require any software to be changed in the host. This is essential if the host is a certified device (e.g. metrology in a meter or security in a communications hub).

The host contains up to fifteen ports, one for each peripheral (UMI-spi or UMI-opto). The peripheral connector is always a male 10-IDC (2.54 mm pitch). The host connectors can be female (for board to board connection) or male (for ribbon connection). The connector contains two ground, two power and six signal pins. The host is the SPI master and the peripherals are SPI slaves.

Like USB, each UMI port is either low power or high power. The low power port can supply up to 50 mA at 3 V<sub>nom</sub> making it ideal for battery powered products. The high power port can in addition supply up to 1 A at 12 V<sub>nom</sub>, meaning that it is normally within a mains powered product. The peripherals all have the same mechanical form factor and connector, but can be low power (e.g. for HANs), high power (e.g. for WANs) or self powered (e.g. for wired interfaces or peripherals with their own battery). Any peripheral can be plugged into a high power port. Only the low power and self powered peripherals can be plugged into a low power port.

Although UMI is physically master-slave (like most SPI networks), it has link and application layers that allow it to be logically peer-peer. All transactions consist of a command followed by a response. However, the command can be initiated by either the host or the peripheral (so long as it is powered). This enables very powerful systems to be developed. Indeed the transaction can even be between two peripherals, with the host providing link layer forwarding.

Link layer frames can be up to 256 bytes, but fragmentation enables application layer packets to be larger. The maximum packet size is device specific, determined by the RAM available in the device. UMI supports packets up to 64 kB.

Every UMI device has a unique 64-bit identifier. The UMI ID is actually an IEEE EUI-64 number. This is used for routing and security purposes. Manufacturers wanting to use EUI-64 numbers should apply to the IEEE for their unique OUI-24 prefix number. UMI IDs and other fields are included in the UMI packet header, making every UMI packet unique. When signed, this helps prevent security attacks.

UMI defines C-like data types, but not specific data objects. Manufacturers are allocated their own bank of 64 k UMI codes. They can then develop their own devices that contain their own UMI data objects identified by their own 32-bit UMI codes, knowing that that they will not overlap with the UMI codes from any other manufacturers. Manufacturers create a confidential UMI datasheet for their device that defines all the UMI data objects in it. This allows products from different manufacturers to differentiate themselves and means they can express new functionality even if it does not exist in the standard data profiles (e.g. DLMS, ZigBee Smart Energy, ANSI C12).

The peripheral is normally used as a translator from UMI-spi to a particular wireless or wired communication standard (e.g. ZigBee, Wireless M-Bus, WiFi, GPRS or PLC). It also translates most of the device specific host data objects to the chosen data profile (e.g. DLMS or ZSE). Objects which cannot be translated can be tunnelled through the communications channels to a UMI virtual device at the other end of the communication.

The UMI application layer provides powerful services for power, events, objects, images, tunnelling and security. Most smart metering installations require remote software upgrade because the requirements for future years are too uncertain to freeze the functionality of devices in the field at the time of installation. However, this introduces a huge security risk as it provides a potential mechanism for attackers to establish control of devices in the field. So the remote software upgrades must be done in a very secure manner. The UMI image service provides the features required to make such remote software upgrades secure, with end-to-end security from the software publisher to devices in the field.

### INSTALLATION AND SERVICE

All the national smart metering rollouts present huge logistical problems. The UK alone plans to install three or four networked boxes (communications hub, in-home display, electricity meter and normally a gas meter) to 26 million homes between 2014 and 2019. Successfully setting up the HAN and WAN networks and securely pairing so many devices will be difficult.

Installations will be done by different utilities using equipment from different manufacturers. The installations will be eased if there is a standard local port that is used in all devices. The local port could be a wired interface (as used in most mobile phones and LAN routers) but most utilities prefer an optical interface as it is harder to vandalise.

### UMI-opto

The FLAG opto port (Ferranti, Landis And Gyr) has been used in electricity meters for years and is now being used in many smart gas meters. The low layers of this interface are standardized in EN62056-21. However the high layers have been implemented with different proprietary protocols from one manufacturer to another.

Standard FLAG port cables for PCs and PDAs are readily available with RS232, USB or Bluetooth interfaces. These are not only used by service engineers at meter installation. They are also used by manufacturers for configuration and calibration in the factory.

UMI-opto enables a standard open protocol to be used for the high layers above EN62056-21, instead of the proprietary protocols used to date. The UMI link layer, application layer, application services, data types and security described for UMI-spi are all available in UMI-opto running over EN62056-21.

The advanced security functions of UMI ensure that only certified users are able to use the UMI-opto port.

### UMI-security

Smart metering systems must exchange large amounts of data. The utilities and national standards authorities have recognised that this information must be kept secure and private. Information exchanges must ensure confidentiality, integrity, availability, authenticity and non-repudiation.

The UMI security specification defines a leading edge security system that can even be implemented in battery powered metering devices. It is a public key infrastructure (PKI) scheme based on National Institute of Standards and Technology (NIST) approved cryptography. Asymmetric ECC-256 primes (as used in European ePassports) are used for ECDSA signatures and for establishing session keys with ECDH. Symmetric AES-128/GCM is used for session encryption. Having a unique identifier for every actor enables traceability across the system. The end-to-end exchange is secure even if the intermediate channels are not, thus reducing audit requirements and cost. UMI security includes many powerful features, including a few described here.

UMI has 16 security roles. Unauthenticated devices have Role 0. UMI devices are designed to defend themselves. DeviceA will grant only minimal rights to deviceB until it authenticates itself to one of roles 1-F (granting different permissions to each role). To do this, deviceB must supply a certificate signed by a certificate authority (CA) that deviceA trusts. The certificate indicates that deviceB has a certain UMI ID and public key and should be granted a certain role (1-F). When deviceB wants to start a session, deviceA issues a challenge (to confirm that deviceB has the correct private key), then grants deviceB the certificate role (for a time period) and generates a session key (using ECDH Diffie-Hellman key exchange).

UMI defines data structures for certificates and certificate signing requests (CSRs) based on the card verifiable certificate (CVC) format and ISO7816.

UMI security operates at the UMI application layer. Every command and response packet can be signed (with the private key) and encrypted (with the session key). Signatures and encryption can also be used for remote software upgrade images and critical commands such as remote -disconnect and tariff -update.

In practice, a battery-powered device can only use the ECC functions (ECDSA, ECDH) occasionally as they use a lot of energy. However, it can afford to encrypt all transactions with the current session key (changed each day or each week). This could be between two modules inside the product, or between the meter and an external HEC (acting as a UMI virtual device).

UMI security is end-to-end. It is not enough to secure data transactions separately by region (e.g. HAN then WAN). UMI's security enables a complete smart metering system to be highly secure and private for data transactions between modules in a meter, from meter to utility and from utility to meter.

### UMI ALLIANCE

The UMI specifications are currently owned by Cambridge Consultants and are made freely available to organizations to use. The ownership of the UMI specifications will be transferred to the UMI Alliance when the members want to form it.

### UMI SOFTWARE PRODUCTS

There is enough information in the UMI specifications for manufacturers to develop their own software stacks. However, if they prefer, they can licence the UMI stack and coordinator that Cambridge Consultants has developed in C.

The UMI specifications are available at [www.CambridgeConsultants.com/umi](http://www.CambridgeConsultants.com/umi).

*UMI and the UMI logo are trademarks of Cambridge Consultants Ltd, registered in the UK.*



#### ABOUT THE AUTHOR:

Alistair Morfey is a Technology Director at Cambridge Consultants where he leads the smart metering practice and the UMI programme. He is a member of the UK DECC STEG (Security Technical Experts Group). He has degrees in engineering and microelectronics from Cambridge and Edinburgh universities and specialized in ultra low power electronic systems, ASICs and embedded processors. [alistair.morfey@cambridgeconsultants.com](mailto:alistair.morfey@cambridgeconsultants.com).

#### ABOUT THE COMPANY:

Cambridge Consultants is a multi-disciplinary engineering design consultancy with 300 staff in Cambridge, UK and 40 in Boston, USA. It has developed products for companies in many markets for over 50 years, including gas, water, heat and electricity meters. Its strengths in system design, RF, sensors, security and ultra low power electronics are all being used in new smart metering developments.

[www.CambridgeConsultants.com/umi](http://www.CambridgeConsultants.com/umi)