Whitepaper: A Solution for Successful Interoperability with DLMS/COSEM and LoRaWAN®

Abstract: This whitepaper explains the results of the engineering work that has taken place over the last few months to build a high-performance, standards-based, interoperable communications profile exploiting the best elements of both technologies to link to the new SCHC internet technology.

The reader will learn that the two organizations have proved the concept and expended significant efforts to design a scalable, secure communications profile, and will understand the key features of the profile and benefits of adopting this solution.

Executive Summary

This whitepaper provides the reader with information about technology being developed that aims to solving significant challenges related to addressing new applications, security, scalability, and efficiency faced by utilities and other organizations rolling out large scale IoT applications making use of DLMS application with LoRaWAN® networks.

The combination of DLMS application model and IP capable messaging with LoRaWAN transport, leveraging on the upcoming SCHC Static Context Header Compression technology delivers an interoperable, secure and scalable solution for data exchange with utility meters and other IoT devices.

The paper describes the application and use cases targeted, the process of developing the new technology and it outlines the DLMS LoRaWAN profile being developed with a view of international standardization.

Table of Contents

Preamble. How to get the best out of this document.

This whitepaper contains information about the background and process to develop this technology in the earlier pages. Page 9 and onward contain an outline description of the communications profile. Pages 16 and onwards contain reference information.

Introduction: Utilities and cities are facing challenges that new communication technologies can help to tackle

With the global population growing at a rate of approximately 80 million people a year, by 2030 it is estimated that the world will need 30% more water, 50% more energy and 50% more food compared to 2019. The utilities responsible for the supply of water and energy are faced with the direct challenges of the population growth, the increased demand of industry due to the socio-economic development, and the changing consumption patterns. As reported by United Nations Organization 68% of the world population will live in cities by 2050, which is stressing even more the need of sustainable solution to augment supply with existing infrastructure and resources in urban areas. Energy and water supply management have become then a direct challenge for the cities.

The European Council agreed in 2014 on the 2030 climate and energy framework for the EU and endorsed several important targets including ambition for:

- A 40% cut in greenhouse gas emissions compared to 1990 levels
- At least a 32% share of renewable energy consumption, with an upward revision clause for 2023
- Indicative target for an improvement in energy efficiency at EU level of at least 32.5%, following on from the existing 20% target for 2020
- Support the completion of the internal energy market by achieving the existing electricity interconnection target of 10% by 2020, with a view to reaching 15% by 2030.

In this global context, the pressure from public policies and regulators are pushing utilities for changes that translate into efforts for a greater overall efficiency. All utility industries are in the midst of a great transformation with existing infrastructure to introduce more and better integration with more of the renewable energies.

Many examples are proving the benefits of new technologies adopted by utilities for optimizing consumption and efficiency. As reported in various examples, the smart metering for energy and water are helping utilities to improve the overall efficiency.

Smart metering is a good illustration of how the utilities are benefiting from the internet and communication technologies (ICT) to tackle these global challenges. In the past decade, with progress of electronics and the spread of internet-based applications, utilities have digitized their infrastructure and transformed their business models.

The electric utility industry has been first to adopt smart metering early in the 1990s and driven by public incentives such as:

- North America — The American Recovery and Reinvestment Act (ARRA) passed in 2009 injected billions of dollars into the metering market. Whilst the program has ended the market momentum remained and much of the original communicating installed base is now entering a replacement phase
- Europe — The Third Energy Package in the EU required member states to assess the cost and benefits for smart metering. Many European countries therefore have started roll out plans peaking around the early 2020s
- India — The Indian Government' Ministry of Power has announced an initiative to introduce smart prepayment metering built around the IEC standards in a three year program with planned completion in 2022
- Chinese manufacturers have delivered many millions of meters both within China and around the rest of the world
- Asia — Many countries have sustained long standing rollouts like the recent roll outs announced in Japan

The efforts of utilities continue in parallel with the rolling outs of the smart meters and new applications to digitize further their grid infrastructure and unleash more benefits of new technologies.

The core values of DLMS/COSEM

There are a number of aspects that are critical for successful large-scale rollouts of systems, like smart metering systems that contain a large number of end-devices:

- **Interoperability:** Multi-sourcing is important to keep purchasing costs down. Ease of system integration is important to keep the time and the costs of deploying the system under control. These aspects call for a solution that provides standards-based interoperability. On the other hand, the standard shall allow freedom to accommodate project-specific requirements
- **Long-term stability:** As a large smart metering system is rolled out over several years and kept in operation for many (15-20) years, long term stability of the underlying technologies is crucial
- **Separation of application and transport technologies:** Whereas the requirements for the functions and the use cases that the system has to fulfil are relatively stable over time, the communication technologies used to carry the messages change rapidly. For this reason, the application shall be media agnostic so that it can be used over any transport technologies emerging
- **Application level, end-to-end security:** Messages between the end devices / meters may need to be transported to the applications of utilities, energy service providers and similar organizations through a number of devices and the communication links between them. Therefore, the solution has to provide application level, end-to-end security that provides confidentiality, authenticity, and proof of origin between the end points
- **Efficiency:** Due to the large number of devices, the need for a large amount of data, and in order to reduce power consumption especially of battery-operated devices, the solution has to be highly efficient minimizing the number of bytes transferred and the number of round trips;
- **Remote maintenance:** During the lifetime of the system the firmware in the devices may need to be updated for various reasons e.g. to add functionality or to correct any bugs. Therefore, the solution shall provide standardized and secure firmware upgrade mechanisms — taking also into account legal metrology requirements — to update the firmware of a large number of devices in an efficient and secure manner

- **Remote diagnostics:** The operation of the system has to be monitored without the need of any physical interaction. Therefore, the solution shall provide a wide range of diagnostic information on the operation of the devices, including the core functionality, communication performance, and discovery of any fraudulent attempts

These were the main design goals of leading utilities and manufacturers that created the DLMS User Association two decades ago to develop the Device Language Specification, DLMS. It defines the semantics and the syntax of the language for interoperable data exchange with smart utility meters and similar devices.

International standardization is a key element of the strategy of the DLMS UA. The DLMS specification developed by the DLMS UA the “DLMS UA Books” are brought to international standardization for electricity metering via the International Electrical Commission (IEC) for electricity metering and via the European Committee for Standardization (CEN) for metering other than electricity.

IEC 62056 has been adopted by regional standardization bodies like CENELEC, the European Committee for Electrotechnical Standardization, BIS, the Bureau of India Standards, ANSI, the American National Standards Institute, SABS, and the South African Bureau of Standards.

The disruption of LoRaWAN for the IoT adoption by the utilities

Utilities have deployed huge efforts in enabling communications to connect their new smart meters and many other assets.

For water and gas meters, powered with batteries, the critical factor is always the power consumption. With the recent rise of LPWAN technologies enabling Low-power sensors to be connected on wide area networks, utilities have been able to wirelessly connect these devices in a cost-effective manner with very long life term.

Beyond the smart metering, utilities can benefit from the LPWAN technologies to enable connectivity for other assets and create new applications leveraging on the numerous and affordable IoT sensors, enabling therefore new business models.

The LoRa Alliance was created in 2015 as the sole association in charge of the LoRaWAN network protocol specification and rules of certification. This ecosystem keeps on increasing with many LoRaWAN network operators (>120 operators in September 2019), new devices (>150 certified devices) and numerous members (>500 members in January 2019).

The key benefits of LoRa® technology and LoRaWAN protocol for the utilities are:

- A network communication technology very appropriate for low power consumption devices (enabling very long battery life) and for long range communications with an automated mechanism to adapt the data rates to the best channel conditions
- An embedded two-layer security based on AES 128 bit encryption keys
- A choice between three different communication classes depending on the trade-off between communications latency and power consumption
- A large flexibility in the network model between public; private or hybrid networks; in different scales, from small to large, with roaming capability, enabling utilities to associate with partners and create new business models of share revenues from connectivity
- Interoperability of devices ensured by unique certification defined by the LoRa Alliance
- A large availability of different devices and large adoption with millions of LoRa®-based meters for water, gas, and electricity having been deployed

The liaison between the LoRa Alliance and DLMS User Association

Overview

The Liaison was created to address markets world-wide which are interested in using efficient narrow-band communications to operate meters and other IoT devices in a secure way. The concept of a highly standardised approach was attractive to both organisations, and it was clear that there is an opportunity for both technologies to leverage each other to provide users with an optimised technical solution.

Applications identified for DLMS/COSEM over LoRaWAN

The first application that will benefit from the development of the DLMS LoRaWAN profile is smart metering rolled out by utilities.

In addition, it will bring advantages to other domains and uses like facility management, electromobility, smart buildings, and smart cities. For example, the electrical mobility with use case of EV charging is at stake for a city and the submetering matters very much in the smart building vertical market.

Here is a non-exhaustive list of applications identified:

- Utility revenue metering (electricity, gas, water, thermal energy)
- Submetering
- Sensors on medium and low voltage electrical networks
- Public lighting
- Electromobility / vehicle charging
- Management of Distributed Energy Resources
- Demand Response
- Renewable energy
- Smart city

As presented by EURIDIS association, here is a view of the different types of information required per application. (Euridis is an international technical association based in France that has strong relationships with both the LoRa Asalliance and the DLMS User Association).

Table 1 - Euridis mapping of possible applications

Applications/Uses Cases	Energy Registering				Diagnostic & Alarm		Control	Firmware Upgrade	Power Supply			Time of use	Security
	Reading Register	Load Profile	Tariff	DR	Logbook	Alarm			Battery Powered	Network Powered	PV Powered	Date	
Water	**X**	**X**	**X**	x	**X**	x		x	x			x	x
Gas	**X**	**X**	**X**	x	**X**	x	x	x	x			x	x
Thermal Energy	x	x	x	x	x	x		x	x			x	x
Electricity Revenue	**X**	**X**	**X**	x	**X**	x	x	x		x		x	x
Electricity Sub-Metering	x				x	x		x		x	x		x
Sensor LV-MV Network					x	x		x	x		x		x
Public Lighting					x	x	x	x	x	x	x		x
EV	x				x	x				x			x
ENR	x				x	x		x	x	x	x		x

First "Proof of Concept" in 2018

One key result from the feasibility study was to demonstrate a first "proof of concept" assembled by Euridis association in cooperation with the LoRa Alliance and DLMS Members. This proof of concept was delivered at the EUW show in 2018 on the booth of Semtech and was received warmly by both parties and the wider industry.

This "proof of concept" demonstrated the feasibility to move DLMS/COSEM messages over a LoRaWAN network, in preparation for an interoperable, standardised, scalable solution. To build the solution that would deliver a formal response there needs to be a formal relationship, and this relationship, the Liaison, was put in place with a liaison agreement and workplan. The Liaison was announced publicly in April 2019.

Technical Development

Engineering work then formally started, in July 2018. The initial work explored the key use cases to be delivered by the resulting technical development, and a Core Team was formed, chaired by a director of the DLMS User Association.

As DLMS can be based on Internet Protocol (IP) and LoRaWAN by default does not transport IP-packets, a strong decision in the work has been the choice of a new technology for the Internet and especially developed for the IoT over LPWAN technology. This new technology called SCHC — static context header compression — makes the use of Internet Protocol practical over low power wide area network technologies by reducing the overhead due to the static header with reduction of the redundancy when sending every message with same header. The Internet Engineering Task Force (IETF) standard organization for the use of Internet protocols is finishing the review of draft proposal submitted by members of the LoRa Alliance and the IETF LPWAN working group.

The expectation is to have publication of two IETF Requests for Comments (RFCs). The first RFC, that documents the SCHC technology generically for LPWAN, is with the IETF and scheduled for publication. The second, that documents the options selected from SCHC for LoRaWAN, called a profile, is in draft version and scheduled to follow in 2020.

An international specification, IEC-TS 62056-1-1 is being applied to document the design. This specification is used to generate communications “Profiles” that cover all aspects of building a successful protocol.

The Liaison stipulates the use of the processes within the DLMS User Association to manage the document outputs, and therefore a document classified as a “Contribution”. A Contribution is an interim document that can output to one or more of: an international standard, inclusion in the DLMS “Books”, application notes or other technical outputs.

At the time of writing, the final approach to standardisation of the Profile is to be agreed, but DLMS User Association members and LoRa Alliance members will have unfettered access to the documented solution, via the DLMS Blue and Green Books, and the LoRa Alliance.

When the RFCs are published, then the publication process within the Liaison can be completed, and the remaining public standardisations can be delivered.

Now and the future

This paper is published to align with the European Utility Week show in 2019, where a live demo of the technical solution takes place. Detail of the demo is in a paper prepared by the LoRa Alliance.

There are many applications where this development will add a sound technical base to real world implementations, and these will generate some technical support request requirements. Contact information for assistance is provided at the end of this document.

Inevitably, there will be the opportunities to refine the technical description of the technology. The DLMS User Association and LoRa Alliance will maintain a relationship to ensure that updates to either of the core technologies are applicable into the future.

Key concepts of the DLMS profile over LPWAN

Introduction to DLMS/COSEM

To define data exchange with smart devices DLMS uses a three-step approach:

- **Modelling** is defined with COSEM objects
- **Messaging** is defined with DLMS services
- **Transport** is defined with communication profiles

Modelling

DLMS uses the client-server model, where the devices play the role of the servers and Head End Systems play the role of the client.

A Physical Device may host one or more Logical Devices, each providing a specific set of functions. A Head End System may host one or more client applications, each having a specific role that allows them to use the functions of the server.

In addition, applications of third parties may also access the servers using a client as an agent.

The functions of the devices are modelled with COSEM objects. A COSEM object defines the attributes of a data element and the methods that define operations that can be performed on those attributes. COSEM objects are used by reading or writing their attributes and invoking their methods.

COSEM objects are named by the OBIS codes.

Servers provide a specific view of their resources to the clients – depending on their role – within AAs, as these can be seen through the interfaces. This includes the list of objects visible, the access rights to their attributes and methods including the required cryptographic protection on requests and responses.

The COSEM objects provide several mechanisms, like selective access, compact data types, and compact encoding to ensure high efficiency.

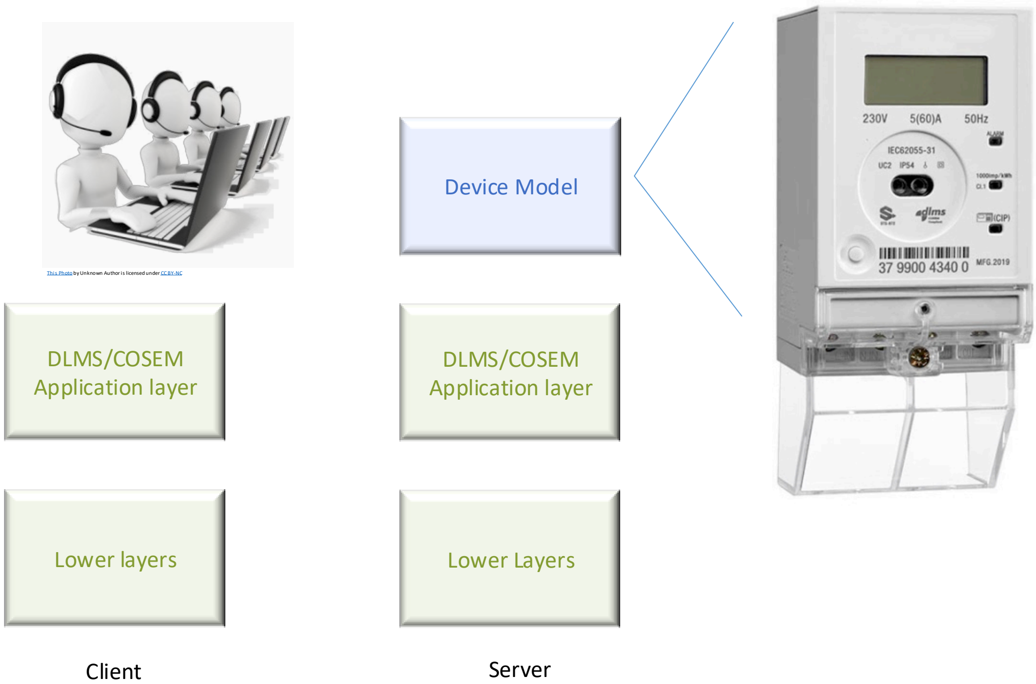

Figure 1 – DLMS Architecture

Messaging

Messaging is defined by DLMS application layer services.

Data exchange takes place with Application Associations (AAs) that allow negotiating the contexts of the exchange i.e. the DLMS services and capabilities to be used. This allows tailoring the parameters of the data exchange to the actual requirements and the properties of the communication media.

AAs are established and released using the services of the Association Control Service Element, ACSE. AAs may also be pre-established, meaning that the parties use a pre-agreed set of rules and capabilities.

Once an AA is (pre-)established COSEM objects are accessed by the xDLMS services provided by the xDLMS ASE. Services may be of request / response type or may be unsolicited to support push operation and notification of events / alarms.

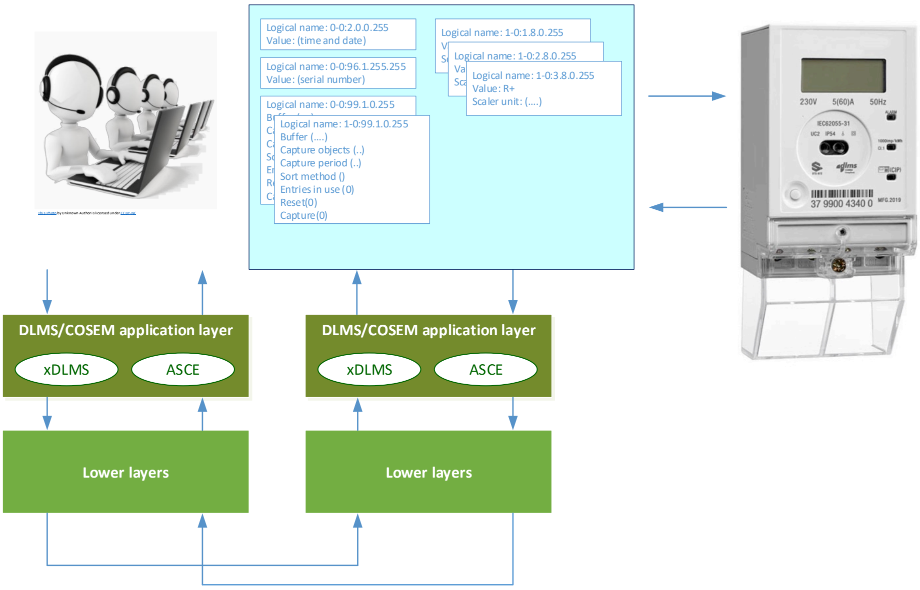

Figure 2- message construction

Each AA defines also the security context, i.e. the cryptographic algorithms available and the security policy that stipulates the protection on each message.

The xDLMS services provide a number of mechanisms like the unified ACCESS service, composable messages, compression and block transfer with streaming to ensure high efficiency.

Data Transport

Transport of DLMS messages is defined by communication profiles.

A communication profile defines the set of protocol layers, the binding between the media-specific lower layers (e.g. PHY, MAC, Link) to the upper network and transport layers and the methods to set up, monitor, and diagnose the communication.

The binding is often specified in an adaptation layer that may specify routing and compression.

DLMS was founded as a request/response language, but has evolved to provide efficiency, and this evolution features:

- PUSH notification – where the device sends data to the client according to a schedule or in response to an event
- Access services, which group several commands like GET, SET or ACTION in one server request: this is to avoid too many roundtrips and reduces power consumption by limiting cryptographic calculations

LoRaWAN Standard

The LoRaWAN MAC layer supports 3 devices classes, where user can select network latency versus power consumption: all devices implement the Class A, some end-devices may implement Class B or Class C.

Class A: The simplest class of end-devices. It is allowed to transmit at any time. The network may reply immediately following the uplinks. Therefore, the network cannot initiate a downlink, it has to wait for the next uplink from the end-device to get a downlink opportunity. The Class A is the lowest power end-device class.

Class B: Class B end-devices implement all the functionalities of Class A devices, but also schedule configurable periodic listen windows. This allows the network to send downlinks on these windows and not only following an uplink. There is a trade-off between the periodicity of those scheduled Class B listen windows and the power consumption of the end-device. The lower the downlink latency, the higher the power consumption.

Class C: Class C end-devices implement all the functionalities of Class A devices but keep their receiver open whenever they are not transmitting. Class C end-devices can receive downlinks at any time at the expense of a higher power consumption. Battery-powered end-devices can only operate in Class C for a limited amount of time (for example for a firmware upgrade over-the-air).

Most of the Class C end-devices are grid powered (for example electricity meters).

SCHC: Static Context Header Compression

The document specifying SCHC profile applied to LoRaWAN is called *Static Context Header Compression (SCHC) over LoRaWAN*.

This document specifies how to apply a static context compression and fragmentation of payload for LPWAN technologies. It is used in this context to compress IPv6 and xDLMS header to minimise overhead and to optimise fragmentation on DLMS/COSEM payloads to be transported by the LoRaWAN.

The main concepts are:

- Uplink: Recommended SCHC overhead is only 1 byte. Acknowledgments are reduced to the minimum in order to reduce downlinks, selected mode is called *Ack-on-error* in SCHC terminology
- Downlink: All downlinks are acknowledged to have fast error detection and recovery; it also helps LoRaWAN class A devices to open Rx windows.
- Multicast is handled but without any ACK, fragmentation or variable MTU, and in the DLMS use case, DLMS/COSEM mechanisms are used to ensure complete file uploads over a group of devices

Description of the Communications Profile

This profile consists of a stack, message flows, message construction, and management considerations.

Stack

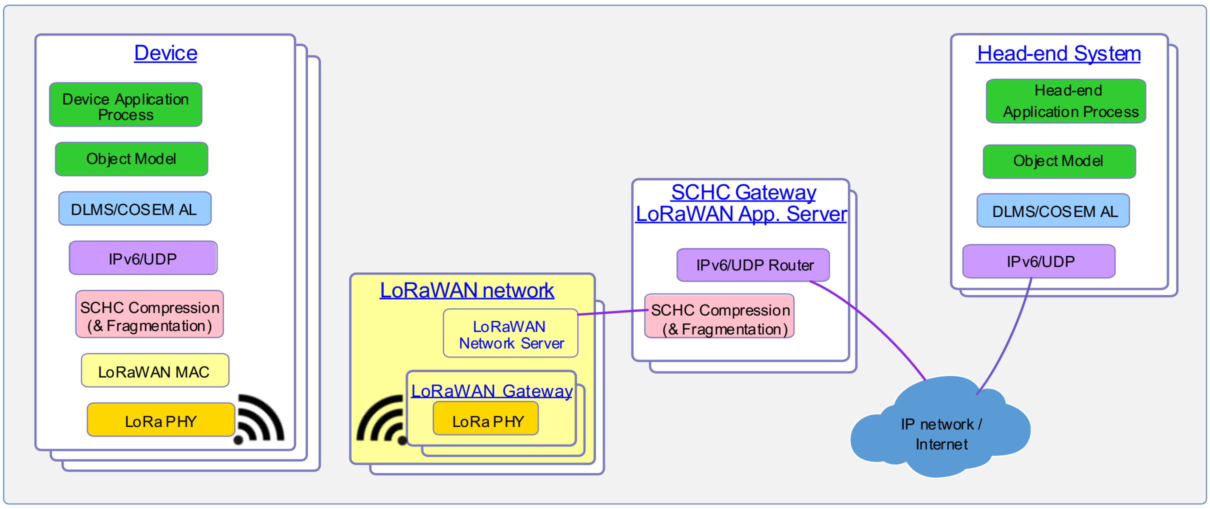

Figure 3 - Architecture description for DLMS over LoRaWAN

Efficiency is driven by the correct choices within the DLMS elements of the stack and correct parameterisation of the SCHC compression. Examples of these choices include:

- Pre-established Application Associations with managed security, removing the need for handshaking as a precursor to data exchange while retaining message security
- Efficient data types and use of compact data formats
- V.44 compression in the Application Layer, a leading technology to compress data
- Confirmed data push services, under development in parallel, reducing the need for head-end system outbound communications
- Block transfer and fragmentation strategy, careful selections are made to ensure that efficient use is made of the LoRaWAN packets across the range of packet sizes

Message Flows

LoRaWAN operates in 3 classes. Metering devices are expected generally to use the classes A and B.

Messages are usually unicast in both directions, that is, messages are from a single sender to a single recipient, but multicast is being exploited for specific situations, for example firmware update.

Below is a flow chart of DLMS get request from HES directed to a LoRaWAN class A device. LoRaWAN network server has to wait for device uplink to send the request to the device; in this example it uses RX opportunity given by a data notification from the device (DLMS server push)

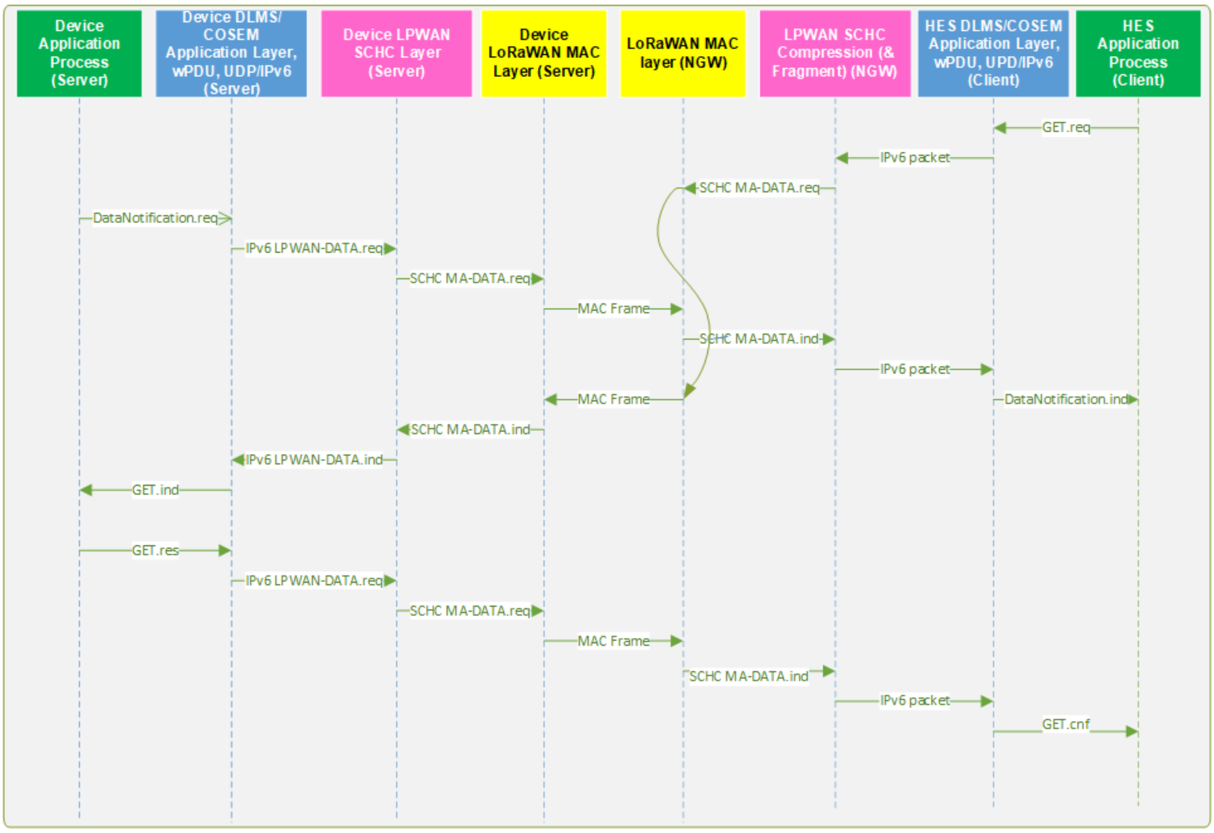

Figure 4 - Full end to end message flow

In the diagram above, routine data is

1) Assembled in the Application Process, and encoded into the COSEM format
2) Packed and secured in the DLMS step, to ensure that Confidentiality, Privacy, and Authentication (or even non-repudiation) is assured
3) Prepared into a packet suitable for use over the Internet in IPv6/UDP
4) Processed by SCHC to strip the routine parts from the start of the message, and replace it with a context header, and fragments it as required
5) Moved the packet (or packets) over air via the LoRaWAN layer

The LoRaWAN network layer then employs some power saving strategies to ensure that the response from the gateway to the device is suitably timed. If the head-end system has provided a message that is buffered on the LoRaWAN network (downlink), then this will be sent in return.

Once the integrity is checked, the LoRaWAN network passes the message to allow SCHC reassembly, if any, and decompression. When this SCHC packet reconstruction is complete, the message is in standard internet format, for transfer to the head-end system thanks to internet.

Management Considerations

LoRaWAN network management is highly automated with little interaction needed at device installation, where many network parameters are known before the device is placed into service. This can be coupled with the DLMS abilities for pre-configuration and pre-establishment to allow a high level of automation when the device is installed.

Security concerns are ever-present and growing, and the combination of the DLMS/COSEM security suites and contexts with the inherent strengths of the LoRaWAN will provide users with both confidence in the approach, and the ability to monitor, the messaging security across the communications system. DLMS User Association is developing and publishing a whitepaper on the DLMS/COSEM security features and benefits.

DLMS/COSEM, though has documented several Interface Classes to allow on-site configuration and diagnostics, and it is expected that, along with LoRaWAN management technologies, will allow highly dependable communications to be supported and optimised for efficiency. The Interface Classes will provide facilities as needed to move a device from one network to another.

Conclusion: Publication Approach

As the liaison aims for having one specification of how to use DLMS over LoRaWAN, both associations, LoRa Alliance and DLMS User Association continue the technical effort with a progressive publication approach. The main direction followed is LoRaWAN and DLMS/COSEM are leveraging on SCHC to ensure the momentum of both technologies in the rapidly evolving world of the Internet of Things. SCHC delivers substantial efficiency gains without impact on the established strengths in the security of both the DLMS and the LoRaWAN technologies, and the combination is optimised through this technical work.

There will be a number of documents that define the detail of the interworking of the core components.

1. SCHC and fragmentation for LPWAN, application to UDP/IPv6 (IETF)
2. SCHC over LoRaWAN (IETF)
3. Contribution containing the specifics of the communications Profile (DLMS UA & LoRa Alliance)
4. Updates to and additions to International standards to describe the communications profile (IEC)

Glossary

Abbrev	Description
AA	Application Association – DLMS mechanism for Role Based Access Control
ACSE	Association Control Service Element
AL	Application Layer
ASE	Application Service Element
Blue Book	DLMS document that contains the Object model used to model devices
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
Contribution	A document used to contain technical information as a precursor to internal publication and/or standardisation
COSEM	Companion Specification for Energy Metering
DLMS	Device Language Message Specification
EN	European Norm – a standard published by CEN or CENELEC
EU	European Union
EV	Electric vehicle
Green Book	DLMS Application Layer specification
ICT	Internet & Communication Technologies

Abbrev	Description
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv6	Version 6 of the Internet Protocol
FUOTA	Firmware upgrade over the air
LoRa	Long Range (Radio)
LPWAN	Low-power wide-area network. Note a special group within IETF is referred to as LPWAN
MAC	Media Access Control
OBIS	Object Identification system
Profile	A formal description of a communications stack, describing features needed to build interoperable network components
PHY	Physical Layer
PUSH	A data service where the Server sends a pre-determined dataset at a routine interval or in response to an event
RFC	Request for Comment – a standard published by the IETF
SCHC	Static Context Header Compression
TS	Technical Specification
UDP	User Datagram Protocol
V.44	Compression algorithm standardised by ITU
xDLMS	Application layer services

FAQ

What is profile of DLMS over LoRaWAN?

It is a document that specifies how DLMS application messages can be transported over a LoRaWAN IP capable network. It specifies the set of protocol layers, the binding between the LoRaWAN lower layers, and the IPv6/UDP network and transport layers, as well as specific COSEM objects needed to set up, monitor, and diagnose the traffic. See the paragraph “Technical Development”.

What is profile of DLMS over SCHC?

It is a document that specifies how DLMS application messages carried by UDP/IPV6 packets can be transported over any LPWA networks, independently of the lower layer technologies. It makes use of the IETF RFC Static Context Header Compression (SCHC) that brings internet connectivity to LPWA networks.

How can I get the profile specification document?

For the time being, the profile is available to the development team members, and it will be made available when complete initially to members of the LoRa Alliance and the DLMS User Association.

What is DLMS over IP over SCHC over LoRaWAN?

It’s an architecture model with different layers approved by both associations, (Figure 3).

What is DLMS?

DLMS stands for *Device Language Message Specification.* It defines the semantics and the syntax of a language used to exchange data with smart devices in an interoperable, efficient, and secure manner. Currently, it is mainly used for utility metering, but it is evolving to other IoT applications.

The semantics is defined by the COSEM objects.

The syntactics is defined by the DLMS application layer services.

The two elements are also known together as DLMS/COSEM

What is COSEM?

COSEM stands for *Companion Specification for Energy Metering.* It defines an object-oriented data model, the semantic element of DLMS. COSEM objects are used to model the functions of smart devices, as these are seen through its interfaces. Data elements are modelled by attributes that can be read and written and by methods that can perform operation on those attributes. COSEM objects can work together to model the various use cases. The model covers utility metering, monitoring, managing consumption, and demand and controlling of any physical quantity. It can be readily extended to IoT applications beyond utility metering.

The naming of the COSEM objects is defined by OBIS.

What is OBIS?

OBIS stands for Object Identification System. It defines the naming system for COSEM object. Each OBIS code identifies the application domain, the physical or abstract quantity and the way the quantity is processed, classified and stored.

What is SCHC?

SCHC stands for Static Context Header Compression. The principle is that, where repeated communications between the same parties are identified or anticipated, a Rule is prepared that reduces the repeated data in the header to less than 8 bits. SCHC also manages fragmentation where this is needed.

How can I certify a DLMS device for LoRaWAN network?

Both the DLMS User Association and the LoRa Alliance offer certification schemes. Devices that carry both certifications will be appropriate.

What are the important points and benefit of DLMS over LoRaWAN?

For detailed information, please refer to the paragraphs “The disruption of LoRaWAN for the IoT adoption by the utilities” and “The core values of DLMS/COSEM”

Where can I find information and a guide to implement my DLMS device on an existing LoRaWAN network?

Contact the technical experts in the LoRa Alliance or the DLMS User Association for the latest publications available.

Where can I find network equipment, devices, and solution providers for enabling LoRaWAN network? Where Can I find DLMS certified devices?

LoRa Alliance web portal provides information on the available network equipment manufacturers and network server providers, plus a list of LoRaWAN Certified^CM products. DLMS User Association also has a page listing DLMS/COSEM certified devices.

How security is performed with DLMS over LoRaWAN?

LoRaWAN provides encrypted transport of packets, and DLMS/COSEM has an extensive security suite. Both LoRa Alliance and DLMS/COSEM have published whitepapers on the security that is available. The combination of LoRaWAN and DLMS/COSEM can provide a comprehensive, multi-layered approach to messaging security.

What are the limits of using DLMS over LoRaWAN?

The limitations of DLMS over LoRaWAN are dependent on many factors, but it is anticipated that, if correctly implemented, DLMS over LoRaWAN will be capable of delivering any use case related to metering, including firmware update.

Links and contacts for more information

- LoRa Alliance: https://lora-alliance.org
- DLMS User Association: https://www.dlms.com/
- EURIDIS Association: http://www.euridis.org/

Technical References

- Whitepaper from Acklio on SCHC - https://www.ackl.io/downloads/schc-whitepaper
- IETF RFCs:
  - SCHC for LPWAN - https://datatracker.ietf.org/doc/draft-ietf-lpwan-ipv6-static-context-hc/
  - SCHC for LoRaWAN - https://datatracker.ietf.org/doc/draft-ietf-lpwan-schc-over-lorawan/
  - IEC standards for DLMS - https://webstore.iec.ch/searchform&q=62056
  - Description of the demonstration at EUW 2019 – Available at EUW

Market Info

- The global challenge of utilities to improve resource efficiency for satisfying the demand growth: https://www.water-energy-food.org/
- EU third energy package:
  - https://ec.europa.eu/energy/en/topics/markets-and-consumers/market-legislation/third-energy-package
  - https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/2030-energy-strategy
  - India press information - https://mercomindia.com/government-electricity-meters-smart-prepaid/

Contacts

- DLMS/COSEM technical questions, contact technical@dlms.com
- DLMS User Association membership enquiries, https://www.dlms.com/the-association/who-we-are
- LoRa Alliance technical questions about LoRaWAN, contact https://lora-alliance.org/contact
- LoRa Alliance membership enquiries, https://lora-alliance.org/membership-benefits

Undertakings and Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the DLMS User Association and LoRa Alliance®, (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the DLMS User Association and LoRa Alliance, (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors makes any representation or offer to license any of their intellectual property rights to the other, or to any third party. Any recipient shall rely on nothing in this information or communication.

The DLMS User Association and LoRa Alliance also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The DLMS User Association and LoRa Alliance takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the DLMS User Association or LoRa Alliance nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect, or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

Copyrights and Trademarks

LoRa Alliance®, LoRaWAN® and LoRaWAN Certified℠ and associated Logos are registered trademarks.

The DLMS Logo is a registered trademark of the DLMS User Association.

LoRa Alliance 5177 Brandlin Court, Fremont CA 94538 USA	DLMS User Association Bahnhofstrasse 28 CH-6302 Zug Switzerland