White Paper

The Fairhair Alliance: Facilitating the Internet of Things for Commercial Buildings

September 2017

Teresa Zotti and Piotr Polak, Philips Lighting

This White Paper is based on a presentation made at the 2017 LED Professional Symposium (Bregenz, Austria).
Website: www.led-professional-symposium.com/speaker/teresa-zotti

Summary

Fairhair is an alliance of leading companies from the lighting, building automation, and IT industries that aims to facilitate the Internet of Things (IoT) for commercial buildings. It will enable new business opportunities by facilitating the convergence between IT and building automation, as well as by fostering the introduction of wireless control.

The distinguishing way of standardizing in the Fairhair Alliance is firstly to adapt existing Internet Protocols from the Internet Engineering Taskforce (IETF) to the requirements of building control. Secondly, to contribute these adapted protocols to help existing building automation standards (a.o. BACnet, KNX, and zigbee) transition to the IoT.

The specification developed by Fairhair advances interoperability between lighting and other building automation functions. Cyber security is key, and Fairhair adapts existing IT security protocols to the requirements of resource constrained devices and to the installation flows, life cycles and deployment scenarios of lighting systems.

1. Introduction

Today wired and wireless standard protocols allow for IP communication directly to and between end devices over multiple Medium Access Control (MAC) and physical layer interfaces, optimizing power consumption and enabling efficient exchange of control packets even for the most constrained device like sensors, dimmers and luminaires.

IoT applications require standard solutions which can communicate and interwork with each other and where sensor data can be discovered and shared across multiple players in the ecosystem.
However, the need for horizontal integration is confronted with today's highly fragmented market where a plethora of technologies, created to meet the needs of different industries, exists.

Furthermore, in a connected world which envisions data flowing across domains and which relies on multiple underlying networking technologies, security becomes a crucial aspect. The lack of a standard common approach to secure communication between devices, which is independent from the specific networking protocol in use, creates additional barriers.

The fear that thousands of internet-connected devices in close proximity can be compromised by malware created by hackers with unpredictable consequences is becoming more and more a key concern and is unavoidably hampering the adoption of IoT systems in commercial buildings.

As easy as it may appear, it would be naive to think of wiping off the crowded picture of today and start planning the solutions of tomorrow from scratch. Creating yet another IoT standard is not the solution.

Globally successful and established ecosystems such as BACnet, KNX and zigbee already count many millions of field devices deployed in today's buildings and together give a relevant representation of the actual size of the lighting and building automation market. The major asset of these protocols resides in their mature data models, the fruit of years of contributions from many industry leaders. Preserving their models and limiting the impact on existing tooling and their application design paradigms is one of the aspects that needs to be considered while evolving towards IoT.

While the common challenges that these ecosystems are facing in their journey towards IoT are complex obstacles, at the same time they represent an incredible opportunity for the industry: breaking down existing barriers and bringing building domains closer to each other.

This opportunity is the foundation on which Fairhair, an alliance of leading companies from the Lighting, Building Automation, IT, and silicon industry[1] was built. The Fairhair Alliance's mission is to help major lighting and building automation ecosystems such as BACnet, KNX and zigbee in their extensions towards IP-based connected systems, standardizing a common infrastructure and specifying all needed application services, ranging from security, discovery to network management.

Next to the obvious efficiency advantage, the harmonized approach envisioned by Fairhair enables co-existence of devices from different ecosystems on the same IP network and prevents divergent choices, for example in terms of encoding formats, from creating new barriers.

[1] At the time of writing, Fairhair counts six Sponsor Members (Cisco, Lutron, Osram, Philips Lighting, Siemens and Silicon Labs) and five Regular Members (Trilux, KNX Association, NXP, Runtime Inc. and Zumtobel group). More information is available at https://www.fairhair-alliance.org/membership/fairhair-members.

Early in 2017, Fairhair has completed its first draft specification. This paper puts this specification into perspective, describing how the technical solutions specified by Fairhair propose to enhance semantic interoperability and to offer a concrete solution to secure the IoT for smart buildings.

Section 2 describes the generic Fairhair scope, while section 3 describes the core of Fairhair Resource Model and how it enhances interoperability. Finally, section 4 dives into the key building blocks of the Fairhair security solution.

2. Fairhair scope and key technology choices

Although the Fairhair specification does not prescribe any specific physical interface, it is particularly designed to work with resource-constrained interfaces. This becomes obvious when looking at the technology choices and the IP stack shown in Figure 1.

The Fairhair application framework sits on top of a generic User Datagram Protocol [2] (UDP)/IPv6 stack that provides a medium-independent means of data transport over wired or wireless physical interfaces.

At the transport layer, UDP is a natural choice for network applications such as lighting control applications in which latency is critical, guaranteeing a lower bandwidth overhead when compared for example to the Transmission Control Protocol (TCP).

To interface to the UDP/IPv6 stack, Fairhair uses services provided by the Constrained Application Protocol (CoAP) [3], designed by IETF for use with low-power and constrained networks.

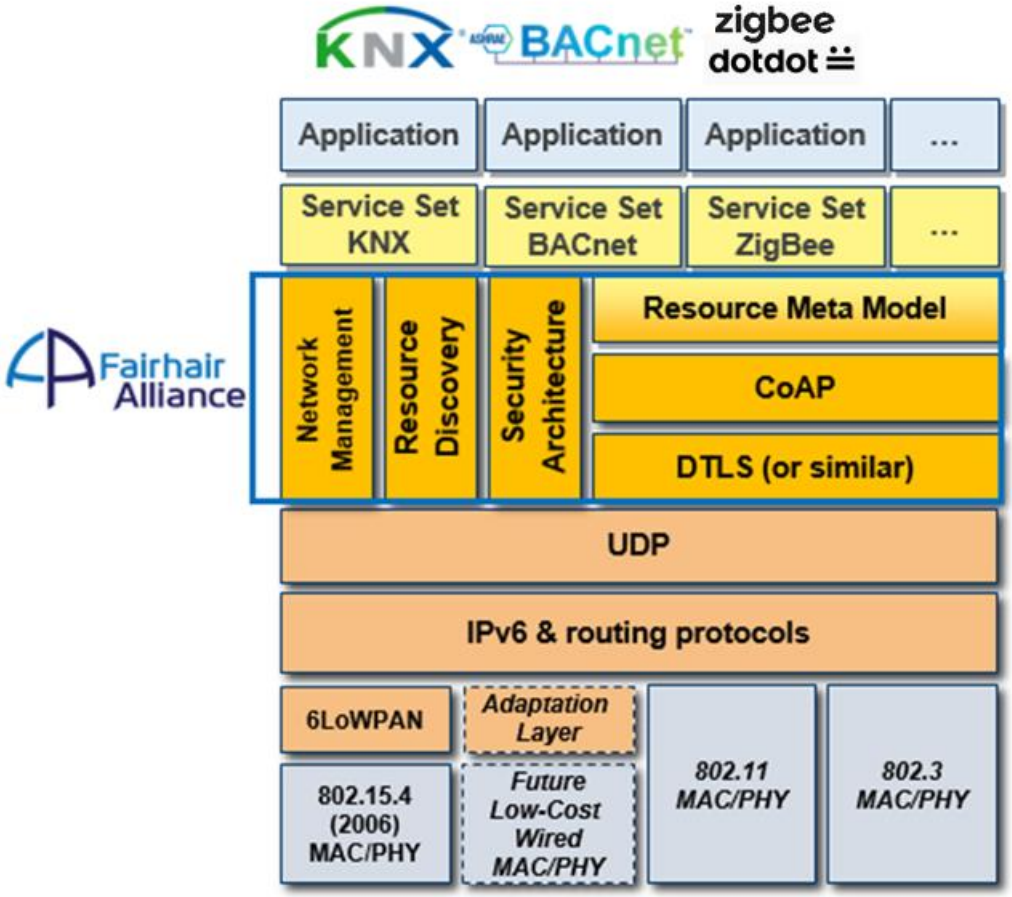

Figure 1- Fairhair technology stack

In general, the work carried out in Fairhair builds upon specifications coming out of the IETF, restricting existing RFCs as dictated by the requirements of the building automation industry, or driving new RFCs.

The core of Fairhair is represented by a set of mechanisms, such as network management, service discovery and security which are independent from the specific application layer protocol in use. These services all operate on resources that are described according to common rules and interfaces defined by the Fairhair resource model.

A Representational State Transfer (REST) architectural style is used as interaction model for creating, reading, setting, and deleting data by means of standard CoAP methods (i.e., GET, PUT, POST, DELETE) [3].

The format chosen to encode the messages exchanged between devices is the Concise Binary Object Representation (CBOR) [4] which is based on the widely successful JSON (JavaScript Object Notation) format [5], specified in IETF. The usage of CBOR aims to reduce both code and message size thereby enabling faster processing of data.

In smart buildings, where thousands of devices are deployed and installed, a mechanism which enables the discovery of devices and the resources they host is an essential step during commissioning as well as at run-time.

The need for seamless scalability from small, for example ten devices, to large (1000+ devices) networks and the ability to support battery-powered devices, are driving requirements for the Fairhair Resource Discovery.

The solution proposed is based on IETF CoAP discovery using Link Format [6] resource descriptions. Fairhair supports both a distributed discovery, usually via multicast queries to the "/.well-known/core" resource of devices, as well as unicast queries and registrations to a central resource directory [7].

The security architecture is based on state-of-the-art IT technology, appropriating the technology for wireless mesh networks. It builds on public key cryptography (IEEE 802.1ar) [8] supporting strong device identities. The protocol flow to bring devices automatically onto the network is based on the Autonomic Networking Integrated Model and Approach (ANIMA) [9]. Application layer security is based on DTLS [10] and adapts the well-known Transport Layer Security (TLS). Additional extensions are developed to secure group communication for example, as in COSE (CBOR Object Signing and Encryption) [11].

On top of the common application services defined by Fairhair, we find the ecosystem specific "service-set". It is here where the ecosystems like KNX, BACnet and ZigBee position their core asset: their application layer protocol specifications with their specific commands and device representations. A concrete example of "service-set" is the ZigBee Cluster Library (ZCL), a mature and very fine-grained specification of control functions and properties for luminaires, sensors, switches, etc.

3. Towards semantic interoperability: Fairhair standard metadata.

Smart devices can potentially generate a vast quantity of data, however the semantic of this data is often implicit or exposed in eco-system specific formats. This leads to a labor-intensive process of interpretation of data before value creation can start.

To make interpretation of data easier, some protocols nowadays already define ways of adding a notation to the data, the so-called metadata. Literally "data about data", metadata can be extremely useful to understand things such as the data types of a value for example binary, string, or integer, its resolution or even the engineering units used to represent it such as degrees Celsius or Fahrenheit for temperature data.

However, there will still be limited value in defining metadata if each application protocol chooses different formats and mechanisms to retrieve it.

As a first step to enhance semantic interoperability, Fairhair defines a standard list of metadata and promote its adoption by the relevant ecosystems.

Table 3-1 shows a subset of Fairhair metadata, with their standardized description and mnemonic.

Metadata	Description	Mnemonic
Base	The base data type of the data item (e.g. Boolean, unsigned integer)	**$base**
Unit	The engineering unit of the data item (e.g. meter, Celsius, Fahrenheit)	**$unit**
Min	The minimum value allowed for the data item.	**$min**
Max	The maximum value allowed for the data item.	**$max**
Access	The allowed methods of accessing the data item (i.e. readability, writability, etc.)	**$acc**

Table 3-1- Subset of Fairhair standard metadata

Metadata is accessible by means of the same CoAP methods and RESTful interfaces used for data. The list of standardized metadata is the result of a careful evaluation of common information that each protocol needs to expose. At the same time, to address those use cases not common to all applicable protocols, Fairhair provides guidelines which allow for ecosystem-specific metadata definitions, avoiding clashes with those ones proposed by Fairhair.

Fairhair achieves the next step towards semantic interoperability by standardizing primitive data types (e.g., boolean, string, integer), complex data types (e.g., array, list) and restrictions of values (e.g., range for numeric values, length for strings), their definition and a consistent encoding format of this information in CBOR.

In this way, each application protocol could annotate an ecosystem specific data value with additional information that is commonly interpreted.

For example, an ecosystem specific resource is enriched with a Fairhair metadata “$base” equal to “uint”. Because of the use of the same agreed notation and format value, every protocol will properly parse and interpret “uint” as an unsigned integer without possibility of misinterpretation.

Table 3-2 shows the Fairhair primitive datatypes and their corresponding CBOR representations.

Fairhair Data Type	**Description**	**Standard mnemonics** ($base=)	**CBOR Representation**
Null	No value. The data item has no value set.	null	CBOR null (major type 7, additional information 22)
Boolean	Boolean value (true/false)	bool	CBOR true (major type 7, additional information 21) CBOR false (major type 7, additional information 20)
Unsigned Integer	Represents unsigned integer values of different sizes.	uint	CBOR unsigned integer (major type 0)
Signed Integer	Represents signed integer values of different sizes.	int	CBOR unsigned integer (major type 0) or CBOR signed integer (major type 1), depending on the actual value
Half Float	Half precision floating point	float16	major type 7, additional information 25
Float	Single precision floating point	float32	major type 7, additional information 26
Double	Double precision floating point	float64	major type 7, additional information 27
String	Unicode character string	string	CBOR text string data item (major type 3)
Enumeration	Value from a set of assigned names	enum	CBOR unsigned integer data item (major type 0)
Bits	Set of flags identified by position	bits	CBOR byte string data item (major type 2)
Binary	Binary data, i.e. a sequence of octets	binary	CBOR byte string data item (major type 2)

Table 3-2- Fairhair primitive data types

The continuous and open dialogue with the involved ecosystems highlighted how the work done so far in Fairhair could become even more useful if standard metadata along with their definitions and format would be described in a machine-readable format. The creation of this machine-readable description represents work in progress in Fairhair. By accomplishing this task, it will be possible to discover the semantic of data in real-time and make the solution future-proof. Changes in the definition of the metadata across different software versions will be in fact reflected in their online descriptions, easing maintenance.

4. Fairhair security solution

As enterprises consider how they will deploy new and advanced lighting, HVAC and other building automation systems, they will need to take into account whatever new security risks those systems entail. Similarly lighting and HVAC systems have to operate in a more open, IP protocol stack based environment, directly exposed to public internet unlike the siloed proprietary networks of the past. This makes them more vulnerable as they are a part of an enterprise network, requiring them to protect themselves with multiple layers of security.

While no system is impervious to attack, Fairhair specification is intended to make clear how such systems can be secured against many forms of attack. The goals of the specified approach are as follows:

- The device can be made reasonably safe from attackers on the network
- The network will be resilient against a device being operated by an attacker, thus restricting the value of the attack to the smallest scope
- The system will provide economical, yet reasonably secure, auto-configuration capabilities, such that the device need only be pulled out of a box by an installer and plugged in for it to find any relevant controllers, perform any relevant discovery, and then operate

One key aspect that the Fairhair security specification brings forward is the need to strengthen the trust relationship between the manufacturer and the operator. Fairhair brings together a number of technologies to accomplish this. Examples include:

- Manufacturer Usage Descriptions are a means for manufacturers to communicate what sort of access a device needs, such that basic access controls can be deployed
- ANIMA Bootstrapping Key Infrastructure provides a means for the manufacturer to introduce the device and the local deployment to one another

In addition, a security zone concept is used to bridge between diversely administered systems. Conduit Controllers mediate trust between different zones, thus simplifying the design of individual components within a zone, and ease the operation of federated and multi-tenant deployments.

On top of that, the application level authorizations of resource model limit the scope of what a particular device is entitled to do within a single security zone.

4.1. Security Layers

The Fairhair security model takes a layered approach based on network segmentation, federated security zones, and the application level authorizations, leveraging multiple networking technologies, including Ethernet, WiFi, and THREAD-based IEEE 802.15.4 networks.

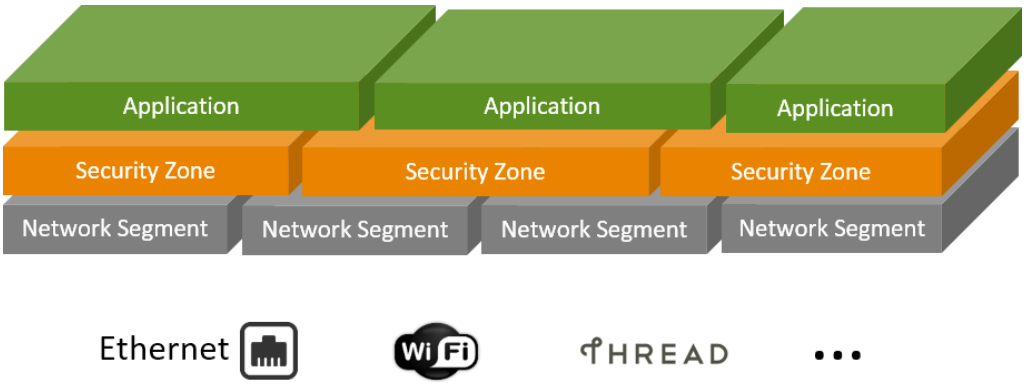

Figure 2: Fairhair security layers

This multilayer approach enables enterprises to establish their own independent security zones, control what devices are authorized to do within a zone but also establish secure communication channels between the zones if required.

These capabilities address special requirements of professional building automation applications typically handled by multiple operators addressing different application domains like lighting, safety or HVAC. The approach taken by Fairhair security specification provides elegant, simple and open standard based solution allowing to:

- Establish multiple secure operational zones
- Facilitate secure interactions between the zones via conduits and between devices within the constraints of a particular zone

All done independently from the underlying networking technologies.

4.1.1. Security Zones and Conduits

The security zones may span multiple network segments and are established by grouping devices based on function, location and responsible organization. Each of the devices belonging to a security zone are provisioned with a device certificate that enables secure communication over DTLS. This way every device belonging to a zone gets unique operational identity issued by Certificate Authority controlled by the operator of the zone.

If required, a security zone may incorporate controller devices that are responsible to communicate with other zones over secure channels called conduits. The conduits are established by authorizing the pair of controllers belonging to two different security zones to communicate with each other. The conduits are established during device enrolment process by issuing two operational identity certificates for both controllers linked by the conduit. On top of that application level authorizations are set to limit the scope of what type of the requests can be exchange between the controllers.

The conduit controller is responsible to "police" the data exchanged between zones and act on behalf of devices belonging to the security zone the controller originates from. The conduit controller can also provide application level protocol translation to bridge different protocols.

By means of a conduit, two operational organizations may easily set up secure communication channel between their security zones, but also define and control the scope of communications.

4.1.2. Application level authorizations

The operational identities issued to all devices participating in a single security zone are used to establish secure DTLS channels between the devices. That means only devices participating in a single security zone can communicate with each other.

However, if one of the devices belonging to a security zone gets compromised, an attacker can issue any request to other devices with no restrictions. To address this issue, application level authorizations are used to limit the scope of what a particular device belonging to a security zone can do. This is done by means of tokens that are linked to operational identities and define what type of request can be issued by client devices towards resource server devices.

The tokens are issued during device enrolment process towards the client devices or directly injected into the resource servers. A resource server device can verify any incoming request based on the identity of the client and the token scope linked to the identity. This way any unauthorized request will be rejected. This mechanism will significantly limit of what a malicious device can do lowering incentive for an attacker to compromise a device.

4.2. Device Enrolment

The device enrolment process described by Fairhair specification provides means for the manufacturer to introduce the device and local deployment to one another. This is done to automate and secure the process of device enrolment allowing seamless provisioning of the certificates and tokens required to establish the described above security layers.

The autonomous enrolment specified by Fairhair uses the ANIMA bootstrapping process as defined in [9].

The process involves three main steps as depicted in the Figure 3:

1. Device authentication based on strong identity (device certificate) provisioned by the manufacturer
2. Security zone Certificate Authority root certificate provisioning
3. Security zone device operational certificate enrolment

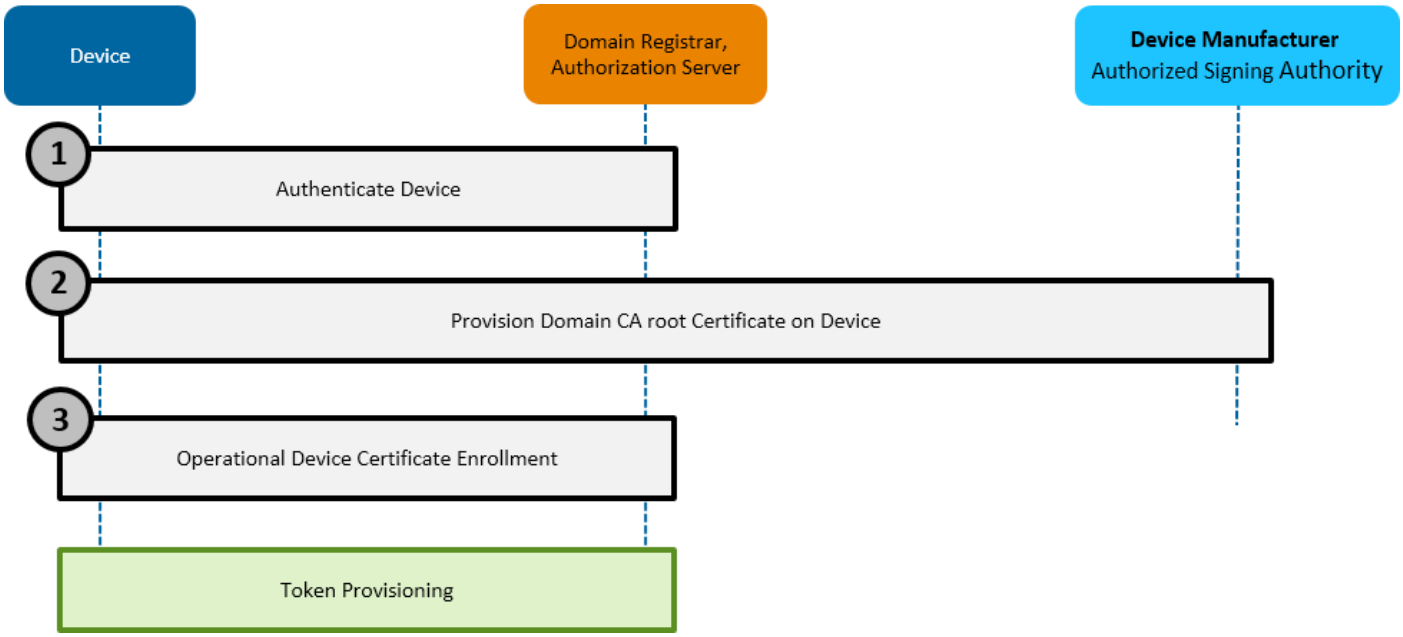

Figure 3: Device enrolment process

Once the device identity is set as the result of the process, the token provisioning can be performed. The required tokens defining the scope of interaction with other devices are injected into the device.

The process described here can be fully automated when network infrastructure allows direct connectivity to the Domain Registrar and Deviance Manufacturer servers as defined in [9]. It is however also possible to utilize out of band communication and provision the device manually if required.

The trust relation between the device manufacturer and the network operator are the key in establishing the trust between the devices operating within the zone.

5. Conclusions

The technical work carried out in Fairhair facilitates the realization of a common, infrastructure for building control, enables integration with IT, brings building domains closer to each other and breaks down existing barriers to more advanced building and lighting control.

Enhancing semantic interoperability and offering standard solutions to secure connected systems for commercial buildings are the main drivers of the draft specification produced by Fairhair which represents work in progress.

The Fairhair Alliance is an open, global consortium, and welcomes all potential new members. Companies, associations and universities can benefit from joining Fairhair by:

- Receiving recognition as one of the leaders that are making the Internet of Things in smart buildings a reality.
- Breaking down the traditional silos of independent building-automation and lighting-control systems in buildings.

- Co-creating specifications for a common network infrastructure.
- Defining requirements and validating related specifications to create an aligned, unified, IP-based solution.
- Co-creating draft specifications for the application protocol layer, for adoption by the respective ecosystems such as BACnet, KNX and zigbee.
- Getting access to specifications • Participating in interoperability testing with other members.

Interested to join and contribute to Fairhair? Please contact the secretary general of Fairhair Alliance Ruud van Bokhorst, secretary-general@fairhair-alliance.org.

6. References

[1] Deering, Hinden, " Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998, https://tools.ietf.org/html/rfc2460

[2] Postel, "User Datagram Protocol", RFC 768, 28th August 1980, https://tools.ietf.org/html/rfc768

[3] Shelby, Hartke, Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014, https://tools.ietf.org/html/rfc7252

[4] Bormann, Hoffman, Concise Binary Object Representation (CBOR), RFC 7049, October 2013, https://tools.ietf.org/html/rfc7049

[5] Bray, The JavaScript Object Notation (JSON) Data Interchange Format, RFC 7159, March 2014, https://tools.ietf.org/html/rfc7159

[6] Shelby, Constrained RESTful Environments (CoRE) Link Format, RFC 6690, August 2012, https://tools.ietf.org/html/rfc6690

[7] Shelby, Koster, Bormann, van der Stok, CoRE Resource Directory, https://tools.ietf.org/html/draft-ietf-core-resource-directory-10

[8] 802.1AR-2009 - IEEE Standard for Local and metropolitan area networks - Secure Device Identity, https://standards.ieee.org/findstds/standard/802.1AR-2009.html

[9] Pritikin, Richardson, Behringer, Bjarnason, Watsen, Bootstrapping Remote Secure Key Infrastructures (BRSKI)", May 20177, https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-06

[10] Rescorla, Modadugu, Datagram Transport Layer Security Version 1.2, RFC 6347, https://tools.ietf.org/html/rfc6347

[11] Schaad, Cellars, CBOR Object Signing and Encryption (COSE), May 2017, https://tools.ietf.org/html/draft-ietf-cose-msg-24