GISFI TR IOT.107 V1.0.0 (2013-09)

Technical Report

Global ICT Standardisation Forum for India;

Technical Working Group IOT;

IoT Device Specific Protocols and Security Aspects

(Draft)

 

The present document has been developed within GISFI and may be further elaborated for the purposes of GISFI.

Keywords

IoT, IoT Protocol, IoT Security.

***GISFI***

Postal address

GISFI office address

Address

Tel.: +91 xxxxxxx Fax: +91 xxxxxx

Internet

http://www.gisfi.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2013, GISFI

All rights reserved.

Contents

Foreword 4

Introduction 4

1 Scope 5

2 References 5

3 Definitions, symbols and abbreviations 6

3.1 Definitions 6

3.2 Symbols 6

3.3 Abbreviations 7

4 IoT Device Specific protocol 8

4.1 Universal Plug and Play (UPnP) 8

4.2 Devices Profile for Web Services (DPWS) 8

4.3 IETF Constrained Application Protocol (CoAP) 8

5. Communication Security in IoT protocols 9

5.1 Communication Security in UPnP 9

5.2 Communication Security in DPWS 9

5.3 Communication Security in CoAP 9

6. GISFI Lightweight IoT security requirements 11

6.1 Device Security 11

6.2 IoT service platform 11

6.3 Application 11

7. Comparison of IoT Device Specific Protocols 13

8 Proposal 15

Annex <A>: <Annex title> 16

A.1 Heading levels in an annex 16

# Foreword

This Technical Report has been produced by GISFI.

The contents of the present document are subject to continuing work within the Technical Working Group (TWG) and may change following formal TWG approval. Should the TWG modify the contents of the present document, it will be re-released by the TWG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TWG for information;

2 presented to TWG for approval;

3 or greater indicates TWG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

# 1 Scope

The scope of this document is to survey the existing device communication protocols which are implementable under resource constraint environments such as UDP, DPWS, CoAP. Our study mainly focuses on the protocol stack requirements, security aspects and suitability for constraint devices. In the end this document has a comparison section which compares all the protocol on the above mentioned aspects.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

 [1] Open Mobile Alliance OMA-TS-DM\_Security V1.3: "Device Management Security ". URL: <http://www.openmobilealliance.org/>

[2] Securing the IP-based Internet of Things with DTLS (<http://tools.ietf.org/html/draft-keoh-lwig-dtls-iot-02>)

[3]. Security Considerations in the IP-based Internet of Things, <http://tools.ietf.org/html/draft-garcia-core-security-05#section-5>

[4] CoAP Security Architecture ( [http://tools.ietf.org/html/draft-arkko-core-security-arch-00#section-3](http://tools.ietf.org/html/draft-arkko-core-security-arch-00%22%20%5Cl%20%22section-3) )

[5] 3GPP MTC Lightweight M2M Security requirements [3GPP TR 33.868 V0.13.0 (2013-04)]

[6] OMA Lightweight M2M Security requirements [OMA-RD-LightweightM2M-V1\_0-20121002-C and OMA-TS-LightweightM2M-V1\_0-20130904-D]

[7] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000

[8] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol (updated by RFC5282)", RFC 4306, Aug 2008.

[9] Universal Plug and Play Forum (UPnP): http://upnp.org/

[10] Devices Profile for Web Services (DPWS) : http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01

[11] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, “Constrained Application Protocol (CoAP).” IETF Internet Draft, http://www.ietf.org/id/draft-ietf-core-coap-07.txt , July 2011.

[12] White paper on “Security Flaws in Universal Plug and Play Unplug. Don’t Play : Jan 2013 , https://community.rapid7.com/docs/DOC-2150

[13] CoAP recent draft release : draft-ietf-core-coap-16 (1st May 2013)

# 3 Definitions, symbols and abbreviations

##

## 3.1 Definitions

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

COAP Constrained Application Protocol

CoRE IETF Constrained RESTful environments

DPWS Devices Profile for Web Services

DTLS Datagram Transport Layer Security

ETSI European Telecommunications Standards Institute

H2T Human to Things

IETF Internet Engineering Task Force

ITU International Telecommunication Union

LWM2M Lightweight M2M

MAC Medium Access Control

M2M Machine to Machine

OMA Open Mobile Alliance

T2T Things to Things

UPnP Universal Plug and Play

# 4 IoT Device Specific protocol

We study three different device specific protocols in this document like Universal Plug and Play (UPnP), Devices Profile for Web Services (DPWS), and Constrained Application Protocol (CoAP) which are mostly used for sensor network, and Machine to Machine (M2M) application. Our study mainly focuses on the protocol stack requirements, security aspects and suitability for constraint devices.

## 4.1 Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a standard that uses Internet and Web protocol s to enable devices such as PCs, peripherals, intelligent appliances, and wireless devices to be plugged into a network and automatically know about each other. With UPnP, when a user plugs a device into the network, the device will configure itself, acquire a TCP/IP address, and use a discovery protocol based on the Internet's Hypertext Transfer Protocol (HTTP) to announce its presence on the network to other devices.

The salient features of UPnP are:

* Media and Device independent,
* Platform independent,
* Based on widely used Internet protocols and technologies like HTTP, DHCP, XML, SSDP, SOAP, GENA
* Offers both user interface based and programmatic control
* Provides mechanisms for the implementation of extensions.

## 4.2 Devices Profile for Web Services (DPWS)

The Devices Profile for Web Services (DPWS) defines a minimal set of implementation constraints to enable secure Web Service messaging, discovery, description, and eventing on resource constrained devices. The first specification of DPWS was published in 2004, submitted for standardization 2008 and approved as an OASIS standard in 2009. DPWS mainly uses web service technology (SOAP, WSAddressing, WSDL and XML Schema) and the focus on enterprise-wide applications.

DPWS specifies a set of predefined services:

* Discovery services: advertise and discover devices.
* Metadata exchange services: provide dynamic access to the services metadata.
* Eventing services: subscribe to asynchronous event messages from a given service.

## 4.3 IETF Constrained Application Protocol (CoAP)

IETF Constrained Application Protocol (CoAP) is being designed and standardized by IETF having in mind the extension of Internet communication to constrained devices, with particular focus on constrained and wireless networking.

CoAP has the following main features:

* Constrained web protocol fulfilling M2M requirements.
* UDP [RFC0768] binding with optional reliability supporting unicast and multicast requests.
* Asynchronous message exchanges.
* Low header overhead and parsing complexity.
* URI and Content-type support.
* Simple proxy and caching capabilities.
* A stateless HTTP mapping, allowing proxies to be built providing access to CoAP resources via HTTP in a uniform way or for HTTP simple interfaces to be realized alternatively over CoAP.
* Security binding to Datagram Transport Layer Security (DTLS)

# 5. Communication Security in IoT protocols

## 5.1 Communication Security in UPnP

UPnP Security Working Committee developed standards enabling strong cryptographic authentication, authorization (access control), replay prevention, and privacy of UPnP control operations, including a Security Console administrative function. Device Security service that has been specified by the UPnP Security Working Committee regards the SOAP control actions as a means to cater for security issues in non isolated network where more than one Control Points (CPs) might be able to discover and gain access to devices.

* UPnP Security defines mechanisms to be applied by UPnP devices when operating in networks that are not isolated and thus foreign Control Points might be able to acquire access to these devices. The Device Security service aims at securing the control actions and does not cover discovery and description functions.
* Trust establishment that regards acquisition of the ownership of a device by a Control Point is achieved by use of a password known by the device and presented by the CP in order to initialize ownership. Thereafter, the signature key of the Control Point is maintained by the device in the list of owners.
* Since the security mechanism is embedded into the body of SOAP messages, in order to allow for policy enforcement with respect to access control, end to end security can be verified by the validity of the signatures.
* The authentication mechanism is based on signing of messages with keys known to devices either as owner keys or as more restricted CPs.

## 5.2 Communication Security in DPWS

DPWS uses WS-Security mechanisms to secure the authentication of devices, the integrity of message exchanges between devices and the confidentiality of message exchanges between them. This set of recommended default security mechanisms allows a minimalistic security between devices. Beside the recommend security feature, DPWS devices are free to use additional mechanisms, specified through policies. The devices security requirements were distributed during the discovery process with authentication and secured discovery.

* Secured discovery: All multicast and uni-cast discovery messages are protected by using message-level signatures in secured discovery, while the discovery messages themselves are not encrypted.
* Authentication mechanisms: The devices may use self-signed certificates or trusted root certificates for authentication.
* Key negotiation phase: The devices negotiate the key establishment protocols to be used between each other and generate a session key
* End-to-end communication: Based on the session key the default mechanism recommended by DPWS is to set up a TLS (SSL) session, which is sufficient as long as the communication is without gateways. Based on this the HTTPS protocol is used for exchanging messages.

## 5.3 Communication Security in CoAP

CoAP does not define a specific security mechanism but CoAP based communications can be either based on Datagram Transport Layer Security (DTLS) or IPsec. Use of DTLS assumes a provisioning phase during which a CoAP device is provided with the security information that it needs, including keying materials and access control lists. Depending on the type of information provided four security modes are identified

* No protocol level security (DTLS disabled).
* Pre-shared Key: DTLS is enabled and there is a list of pre-shared keys with each key including a list of nodes with which is valid to be used for communication.
* Raw Public Key: DTLS is enabled and the device has an asymmetric key pair, but without an X.509 certificate. The device also has an identity calculated from the public key and a list of identities of the nodes it can communicate with.
* Certificate: DTLS is enabled and the device has an asymmetric key pair with an X.509 certificate that binds it to its Authority Name and is signed by some common trust root. The device also has a list of root trust anchors that can be used for validating a certificate.
* IPsec Encapsulating Security Payload (ESP) can be alternatively used to secure CoAP in constrained environments.

The following feasibility of realizing secure deployments with existing CoAP protocols and the practicality of creating comprehensive security architectures based on this protocol:

* DTLS has been defined as the basic building block for protecting CoAP
* (D)TLS was designed for traditional computer networks and, thus, some of its features may not be optimal for resource constrained networks
* Raw public-key in DTLS has been defined as mandatory
* Performance of DTLS from a system perspective should be evaluated involving not just the cryptographic constructs and protocols, but should also include implementation benchmarks for security policies, since these may impact overall system performance and network traffic.
* Protection of lower protocol layers is a must in networks of any size to guarantee resistance against routing attacks such as flooding or wormhole attacks. The wireless medium that is used by things to communicate is broadcast in nature and allows anybody on the right frequency to overhear and even inject packets at will. Hence, IP-only security solutions may not suffice in many IoT scenarios.

# 6. GISFI Lightweight IoT security requirements

The present LWIoT baseline architecture address the high level security requirement of IOT system blocks and their interface. A detailed study technical report on IoT protocol aspect was submitted during GSSM#13. This document discusses only the security requirement of present GISFI Baseline Lightweight IoT architecture.

High level security requirement of baseline LWIOT architecture were grouped under three different categories via i. device security ii. IoT platform and iii. Application. To avoid the unexpected peak load as well as bandwidth requirements, the IoT platform requires the advanced device management techniques which include lightweight secured communication with reduced encryption and reliability mechanisms, addressing the scalability. The details on the specific mandatory and desirable security requirements are given below:

## 6.1 Device Security

* Devices should be authenticated M
* Support for decoding encrypted data from sensor devices D
* Support for low complexity management of security infrastructure D

## 6.2 IoT service platform

* Authenticate the application developer while installing the application or new services. M
* Support secure channel establishment with IoT gateways as well as application D

## 6.3 Application

* Follow a secured channel while communicating with service platform D
* Support preserving of privacy of the data while fetching from service platform O

# 7. Comparison of IoT Device Specific Protocols

In this section, we compare the three device specific protocols mentioned in the section 4 such as UPnP, DPWS and CoAP in terms of protocol stack requirement, suitability for constraint devices, and the security aspects like authentications/ authorisations, encryptions, network layer security, transport layer security and applicability.

Table 1: Comparison of the different device specific protocol

|  |  |  |  |
| --- | --- | --- | --- |
| Properties | UPnP | DPWS | CoAP |
| Released | * UPnP Industries forum Initiative.
* As ISO/IEC 29341 in December 2008
 | * DPWS specification was initially published in May 2004
* DPWS 1.1 was approved by OASIS in June 30 2009
 | * IETF Constrained RESTful environments (CoRE) Working Group has done the major standardization
* draft-ietf-core-coap-16 is published in 1st May 2013 (work under progress)
 |
| Protocol stack requirement | * Requires TCP, UDP and IP networking support.
* Other operations of the UPnP entities depend on SSDP, HTTP, SOAP, XML and HTML processing.
 | * Requires IP (v4/v6) in combination with UDP (SOAP-over-UDP) or TCP and HTTP (SOAP-over-HTTP) support.
 | * Requires UDP and IP support
* Communication using CoAP doesn’t required translation otherwise HTTP/CoAP translation required
 |
| Authentication/Authorization | Signature keys are used to verify signed action requests | SSL/TLS sessions can be mutually authenticated | Either IPsec security associations orDTLS channel establishment can be mutually authenticated |
| Encryption / Privacy | If required actions and responses can be authenticated | Encrypted by default | In DTLS and IPsec/ESP encryptionis by default |
| Transport Layer Security | No | Yes | Yes (if DTLS is used) |
| Network Layer Security | No | No | Yes (If IPsec-ESP is used) |
| Easily Applicable | No, there is need for supporting DeviceSecurity | Yes if platform offers Transport Layer Security | Yes if DTLS or IPsec is supported by thedevice |
| Suitability for constrained terminals | * Not suitable for energy efficient design consideration.
* UPnP functionalities need to be implemented in a Gateway node
 | * The usage of web services generates communication (XML-based message format) and computing (XML parsing) leads to increase in over head.
* Not suitable for energy efficient design consideration.
* Functionalities need to be implemented in a Gateway node
 | * Requires UDP and IP support
* Not suitable for Type 3 device
* Gateway node need to implement HTTP/CoAP functionalities to interact with constraint device Type 3.
* Direct implementation of typical CoAP ready protocol stacks shall be feasible for Type2 devices
 |

**Note: Device Types**

**Type1:** Unconstrained terminals have sufficient computational power and energy reserve to implement complex tasks

**Type2:** Constrained terminals have: 1) reduced transmission capabilities (< 1 Mbit/s), 2) Energy reserve (battery operated or co-powered through energy saving circuitry), 3) memory storage (RAM < 10 Kbytes, ROM < 100 Kbytes), 4) computational capabilities (typically their micro-controllers have clock speeds smaller than 100 MHz).

**Type3:** These device typically not able to participate in an end-2-end IP communication due to their extreme limitations in computing power, memory storage and limited energy storage.

# 8 Proposal

CoAP meets most of the device specific security requirement defined in GISFI LWIOT architecture. With help of IKEv2 and HIP, TLS and DTLS provide end-to-end security services including peer entity authentication, end-to-end encryption and integrity protection above the network layer and the transport layer respectively.

We propose GISFI members, to discuss and approve this study report as an input document for IoT architecture document..

Annexes are only to be used where appropriate:

Annex <A>:
<Annex title>

Annexes are labelled A, B, C, etc. and are "informative"(3G TRs are informative documents by nature).

# A.1 Heading levels in an annex

Annex <1>:
Change history

It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:

|  |
| --- |
| **Change history** |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2013-07 |  |  |  |  | Input document on IOT device specific protocol. |  | 0.0.0 |
| 2013-09 |  |  |  |  | Content updated with security aspect |  | 0.0.1 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |