**Title :** Input document on different device specific protocol

**Company :** NEC

**Purpose :** Discussion and approval

**Doc number :** GISFI\_IoT\_201306409

**Meeting :** GISFI#13, New Mumbai, India, 10 – 13 June, 2013

# Abstract

Scope of this document is to study the different device specific protocol (like UPnP, DPWS and IETF CoAP) and its security aspect. We compared all these protocol with respect to release, protocol stack requirements, security aspects and also suitability for constraint device. This document end with a proposal section where discuss scope of standardisation in this protocol while using in IoT application.

# Introduction

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. We have provided an comparison section which compare all the protocol on the above mentioned aspects. Section 2 discusses the salient features of the protocols. Communication security aspects discussed in section 3. Section 4 provides a compassion table of the different protocols.

# Device Specific Protocol

## Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a standard that uses Internet and Web [protocol](http://searchnetworking.techtarget.com/definition/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.

## 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.

## 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)

# Communication Security

## 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.

## 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.

## 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.

# Comparison of different protocols

|  |  |  |  |
| --- | --- | --- | --- |
| 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 or  DTLS channel establishment can be mutually authenticated |
| Encryption / Privacy | If required actions and responses can be authenticated | Encrypted by default | In DTLS and IPsec/ESP encryption  is 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 Device  Security | Yes if platform offers Transport Layer Security | Yes if DTLS or IPsec is supported by the  device |
| 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.

# Proposal

The following standardisation aspects need to be considered before finalization of protocol for light weight IoT architecture

* IoT Application for which the Light weight architecture need to used
* Type of device which need to be used for that IoT application (Refer above section for the device type )
* Decision on the security level implementation
* Decision on the Gateway and higher layer network architecture
* Standardisation of the device to device interface
* Standardisation of device to Gateway interface
* Modification of Gateway based on the device protocol section

# References

1. Universal Plug and Play Forum (UPnP): <http://upnp.org/>
2. Devices Profile for Web Services (DPWS) : <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>
3. 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.
4. White paper on “Security Flaws in Universal Plug and Play Unplug. Don’t Play : Jan 2013 , <https://community.rapid7.com/docs/DOC-2150>
5. CoAP recent draft release : draft-ietf-core-coap-16 (1st May 2013)