**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Annex C Rewrite |
| Date Submitted | 26 March, 2015 |
| Source | Robert MoskowitzHTT ConsultingOak Park, MI 48237 USA | Voice: +1 248 968-9809Fax: +1 248 968-2824E-mail: rgm@labs.htt-consult.com |
| Re: | Rewrite of Annex C |
| Abstract | This document contains the rewrite of Annex C |
| Purpose | CID 45 solution |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

# 1.0 Editing instructions for the D1.0\_P802-15-9\_Draft\_Standard.pdf

*Replace the text of Annex C as follows:*

C.1 Description

The Host Identity Protocol (HIP), “Host Identity Protocol Version 2 (HIPv2)”, RFC 7401 is an IETF standard that provides a Key Management Protocol. Although primarily used to establish Security Associations between hosts at the IP layer, it is truly layer independent and can as readily establish SAs at the MAC layer. HIP has a Base Exchange (BEX) protocol and a simpler Diet Exchange (DEX) protocol (draft-moskowitz-hip-dex). Highly constrained systems will benefit from the minimal architecture of DEX. A less constrained system like a coordinator can easily support BEX and DEX peers, as DEX is largely a subset of BEX.

A central concept in HIP is a cryptographic Host Identifier (Host Identity or HI) namespace. The self-asserting nature of HIs make for simple to implement and deploy models for small enclaves of constrained devices. As the Host Identity format is determined by the underlying cryptographic algorithm, a Host Identity Tag (HIT) is used as a normalized identity format. HITs are valid IPv6 addresses (2001:20::/28 prefix) and can be used in applications to provide mobility or where there is no real IP layer supported. HITs are also used in Access Control Lists (ACLs) for simple authentication control. Third party assertion authorities are optional with HIP. HIP does support both PKI and RADIUS based assertion authorities.

HIP is a four packet peer exchange protocol. These packets can be very small (particularly DEX), thus requiring very little fragmentation support. Either party may initiate an exchange and a responder can force itself to be the initiator.

C.2 Use Cases

HIP's lightweight nature works well with highly constrained devices and scenarios with no back end authentication services. It can use an asymmetric defense against man-in-the-middle attacks for initial deployments; that is if a sensor's HI (actually HIT) is registered to a coordinator, the coordinator can control permitted connections. Sensors are still exposed to connecting to rogue controllers, but this is detectable as the sensor would not be working in the desired network.

C.2.1 Isolated Enclave

HIP works well in an isolated enclave where there is no apparent Authentication Server. It can work strictly ad hoc. There can be no authentication, that is the mode where “I don't know who you are, but we will communicate securely”. There can be at authentication validation of the HITs on devices with screens that can display HITs. Finally HITs could be preloaded into devices that can read QR codes where HITs can be encoded for devices.

C.2.2 Home net

Home nets may use the isolated enclave approach, e.g. for a lighting system, or could use a RADIUS approach where the RADIUS server resides in a home gateway/server. HITs can be readily added to the RADIUS server either by a UI for entry, or more simply (for the user) by scanning QR codes on sensors that would contain encoded HITs.

C.2.3 City net

City nets will be have a mix of rich-function devices that have higher layer requirements for digital certificate based identities and highly constrained sensors that would benefit from the small footprint HIP DEX and HIT-based authentication. HIP BEX with certificate-based (RFC 6253) and HIP DEX with HIT-based authentication can readily coexist; the initial packet, I1, identifies which exchange is called for. As DEX is basically a subset of BEX (with the switch to ECDH identities), coordinators can readily support both exchanges.

C.2.4 RFID networks

Although there are no known Transmit only RFID devices that can support any KMP, many RFID devices used supporting 802.15.4 have a Receive mode for initial PAN joining. This can be used to provide the KMP support. The nature of RFID PANs of 3 receivers visible to any device, tends to produce deployments where most devices use the same key for data protection. In this scenario, the KMP is used to register devices to the PAN and distribute the group keys.

C.2.5 Infrastructure sensor nets

Highly constrained, low energy, critical infrastructure sensors are well matched with HIP DEX for a small memory/CPU/power footprint. The typical large infrastructure deployments in LECIM would work well with a RADIUS-styled device registration and authentication solution.

C.3 802.15 specifics

C.3.1 Message Framing

HIP payloads are directly supported within KMP payload. There is no IP or TCP/UDP content within Base or Diet Exchanges.

As the cipher algorithm supported by IEEE 802.15.4 is AES-CCM\*, only this and related authentication (AES-CMAC) are needed.

C.3.2 Key Derivation and Security PIB interaction

IEEE 802.15.4 supports complex security models through the Security PIB. As such, the higher-layer may use the ESP\_TRANSFORM (RFC 7402), the ENCRYPTED\_DATA or the ENCRYPTED\_KEY parameters as is appropriate. These can support unicast or group key distributions.

C.3.3 Deployment recommendations

Host Identities (HI) and HITs can be preinstalled in devices to avoid the processing cost of generation. The HIT can be provided externally as in a QR code for loading into an authentication service.

C.3.4 HIT authentication

C.3.4.1 ACL-based

The PAN coordinator can maintain a HIT ACL that it distributes to sub-coordinators. This ACL can be built manually or via a QR reading application. Only devices in this ACL will be permitted to join the PAN.

C.3.4.2 RADIUS-based

Here the HITs are loaded into a RADIUS server. Many RADIUS servers do not specify a MACaddr size limit, so storing HITs as 'MACaddrs' have been shown to work. Each coordinator then operates as a RADIUS client to validate that the HIT and thus the device is allowed to join the PAN.

C.3.4.3 Certificate-based

HIP does support X.509 authorization (RFC 6253). Thus each device’s HIT can be the altSubjectName and the coordinator can use standard X.509 methods to validate the certificate.