

Internet of Things architectures et technologies

Chapitre #4 Enjeux et perspectives



Enjeu #1: Inter-opérabilité

L'enjeu de la Normalisation

Actuellement, très forte hétérogénéité des équipements, protocoles, modèle de données, etc.

Conséquences:

un travail d' « intégration » systématique qui augmentent les coût de « build » de toute solution IoT

Objectif:

faire adopter un standard permettant le développement d'un écosystème riche et ouvert, comprenant équipements « plug and play » et modules applicatifs compatibles.



Organismes de normalisation

ETSI

European Telecommunications Standards Institute

Indépendant, but non lucratif Fondé en 1988, basé à Sophia Antipolis (FR).

Membres: 800, 64 pays, organismes de recherce, entreprise (groupes, PME).

Standards techniques communication/information (fixe, mobile, radio, internet...).

>2k standards par an Ex: GSM, DECT, Smart Cards



http://www.etsi.org/

3GPP

3rd Generation Partnership Project



Fondé 2000, avec pour objectif la normalisation mondiale de la « 3G ».

Publie régulièrement des « release » (préparées pendant 1-2 ans) qui intègrent de nouvelles normes ou études (actuellement: #13)

Ex: 2G (reprise), 3G, LTE, 5G?

IETF

Internet Engineering Task Force

Depuis 1986, USA

Publie les « RFC » (= Request For Comments)

Ex: IP, ICMP, TCP, FTP, SMTP, domain names, NTP, POP...



http://ietf.org/

OMA

Open Mobile Alliance



www.openmobilealliance.org

Créé en 2002, pour unifier les « forums » portant sur des standards applicatifs ouverts en lien avec la téléphonie mobile.

Membres:

fabricants (Ericson, Thomson, Huawei,...), opérateurs (Vodafone, Orange, T-Mobile...), dévelopment software (Microsoft, Sun, IBM...)

IEEE



Institute of Electrical and Electronics Engineers

https://www.ieee.org

Créée en 1963 (fusion d'anciennes organisations), Association professionnelle des « ingénieurs électriciens et électroniciens ».

Organise conférence et réalise publications techniques.

Différents comités:

802=LAN (802.11=Wifi, 802.15=bluetooth/zigbee..., 1003=POSIX, P1901=CPL, etc.)

W₃C

World Wide Web Consortium

Fondé en 1994, organisme de standardisation chargé de promouvoir la compatibilité des technologies WWW:

HTML/CSS, XML, SOAP, SVG, RDF...



https://www.w3.org/

Créé en 2012, regroupe de grands organismes (ETSI et équivalents chinois, américains, japonais, etc.)



Objectif:

interopérabilité M2M, via une couche de service standardisée qui permette l'émergence de hardware et logiciel compatible, et le développement de service sur les domaines des transports, de la santé, de l'industrie, du smart home,

Standards M2M/IoT



TR-069

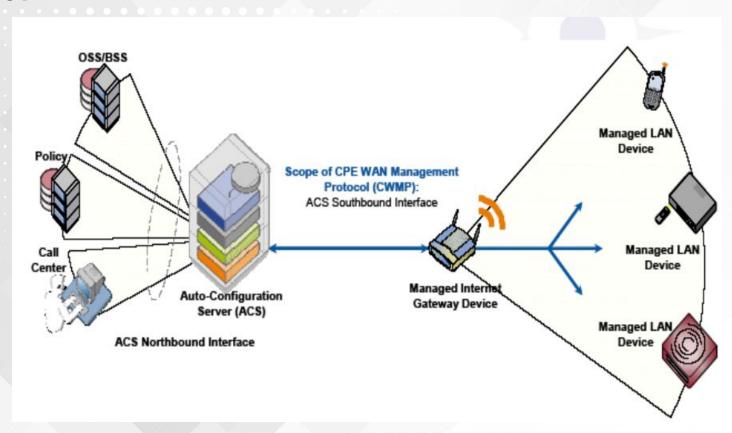
Communication entre équipement (« CPE »: box internet, NAS, etc.) et serveur d'auto-configuration (ACS), défini par « BroadBand Forum » (DSL forum)

Sorte de SNMP sécurisé et standardisé, basé sur des appels « RPC » SOAP (XML/HTTP)

Fonctions:

auto-configuration / gestion software / gestion firmware / supervision / diagnostic /

TR-069



TR-069

Très utilisé par les opérateurs telco pour gestion de « box », mais peu répandu au-delà: inadapté pour équipements contraints.

- Protocole verbeux: peu adapté quand bande passante limitée,
- Data modèle spécialisé gestion box internet / ligne fixe...

OMA-DM (« Device management »)

Fonctions:

- Provisioning,
- Device Configuration,
- Software Upgrades,
- Fault Management.

Transport:

- Lien série (USB, RS232), sans-fil (GSM, CDMA, IrDA, BT)
- WSP (WAP), HTTP, OBEX

LWM2M (ETSI) - overview

- Protocole basé sur CoAP / DTLS (ou SMS)
- Fonctions: échanges sécurisés, Device
 Management et collecte de donnée,
- Conçu pour équipements <u>très contraints</u>.
- Bonne dynamique d'adoption côté plateforme et opérateurs.

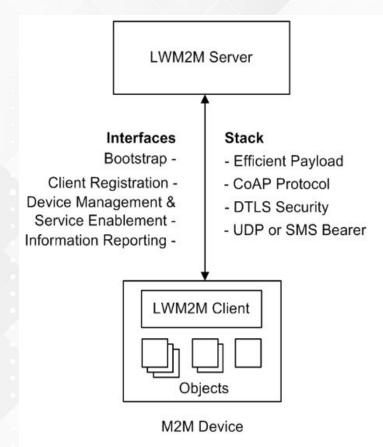


Figure 1: The overall architecture of the LWM2M Enabler.

LWM2M (ETSI) - overview

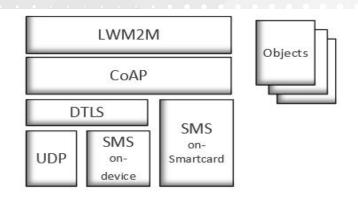


Figure 2: The protocol stack of the LWM2M Enabler.

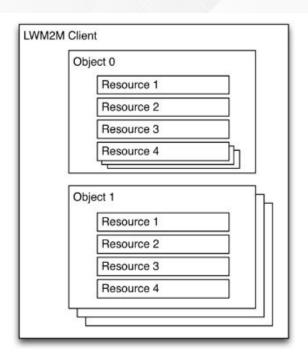
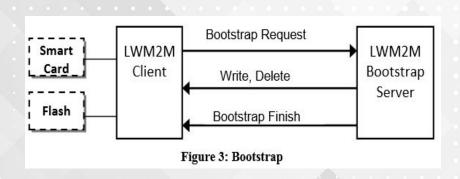
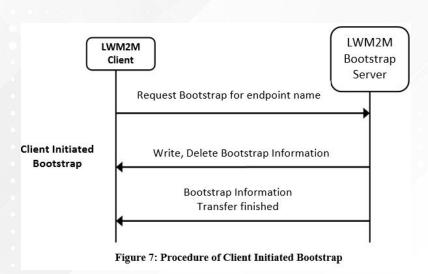


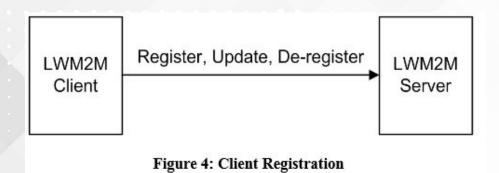
Figure 13: Relationship between LWM2M Client, Object, and Resources

LWM2M (ETSI) - bootstrap





LWM2M (ETSI) - registration



LWM2M (ETSI) - DM

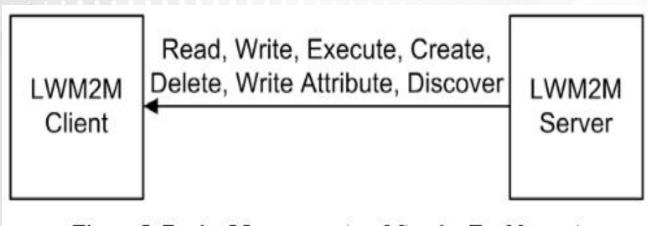
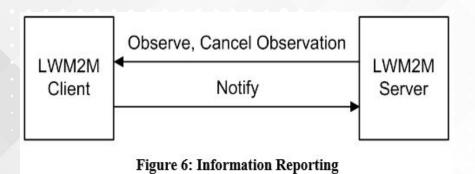


Figure 5: Device Management and Service Enablement

LWM2M (ETSI) - reporting (data)



LWM2M (ETSI) - reporting (data)

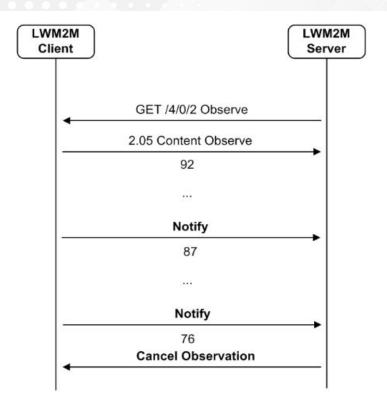


Figure 11: Example flow for Information Reporting Interface for the RSSI Resource of the Connectivity Monitoring Object of the example client (Appendix E).

LWM2M (ETSI)

Technical Ref. [PDF]

http://technical.openmobilealliance.org/Technical/Release Program/docs/LightweightM2M/V1 0-2 0151201-C/OMA-TS-LightweightM2M-V1 0-20151201-C.pdf

Organisme dédié à un standard « chapeau » pour l'IoT:



http://www.onem2m.org/

s'appuie sur les autres standards (ex: LWM2M) pour normaliser à plus haut niveau les interactions plateforme à plateformes.

Tente de traiter tous les cas: équipements intelligents, gateways portant une partie de l'applicatif, fédérations de plateformes, équipements nativement compatibles ou non avec One M2M...

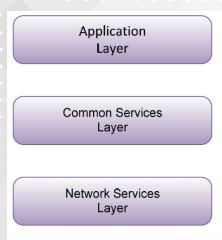
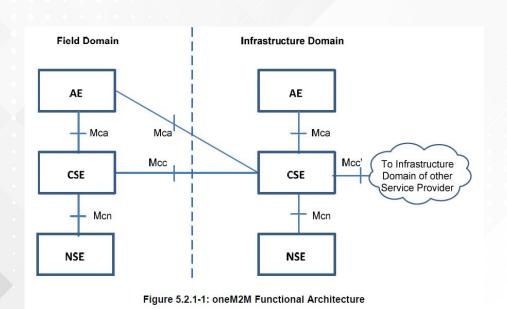


Figure 5.1-1: oneM2M Layered Model



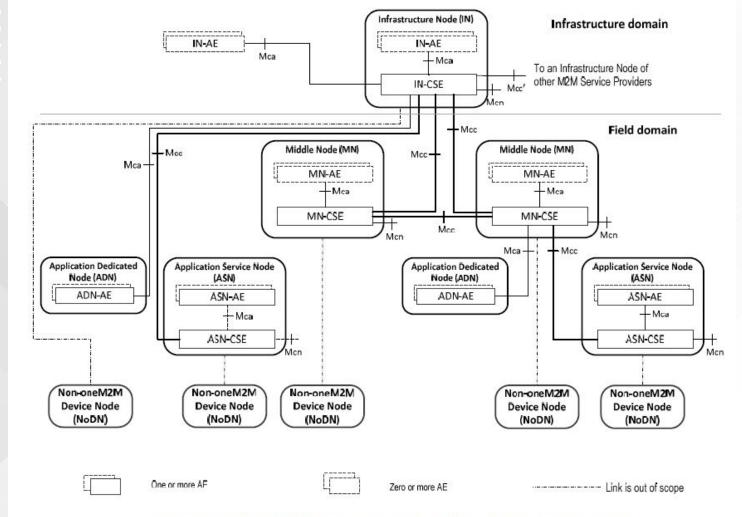
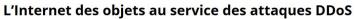


Figure 6.1-1: Configurations supported by oneM2M Architecture

Enjeu #2: Sécurité



e site, vous acceptez l'utilisation de cookies à des fins de mesure d'audience



En septembre dernier, le leader européen de l'hébergement, OVH, a fait l'objet d'une attaque informatique sans précédent. Les pirates ont détourné près de 145 000 caméras connectées

La revue

« numérique

systèmes d'information (ANSSI) a traité près de bersécurité, soit 50 % de plus qu'en 2014 : 61 ts de sites web ; 12 %, des « compromissions aient liés à des courriels malveillants ; 6 %

lundi 12 decembre 2016

UN TRIMESTRE EN EUROPE V

étaient des « infections » virales ainsi que des ialiciels (logiciels malveillants développés dans le le consentement de l'utilisateur « infecté »).

urer de connexions un serveur ou le centre de ors les plus grandes difficultés pour « trier » les ırs. Parmi les attaques par déni de service, celle eny of Service - consiste à engorger le serveur

La revue V Les auteurs Oui sommes-nous / V S'abonner



Choisir l'auteur

f 151 Fans

SE2 Suivenire



Une Jeep piratée et stoppée à distance sur une autoroute

♠ > TECH & WEB > TECH & WEB

Par Jules Darmanin | Publié le 21/07/2015 à 19:51



Sécurité - familles de risques

- Vol de données sensibles (données personnelles)
- Usurpation d'identité: collecte de fausse informations
- Détournement d'objets
- Déni de Service (DDoS)



Sécurité - solutions

Pas de risque zéro, les mesures doivent être en adéquation avec la menace.

Besoin de traiter le risque en cohérence bout en bout:

- Stockage sécurisé de secrets dans l'objet
- Authentification forte / chiffrement des échanges
- Signatures des contenus exécutables (firmware, applications, etc.)
- Cloisonnement des échanges (réseau privés, ex: APN GSM)
- Sécurisation de la plateforme (accès dédiés à l'administration, suivi des mises à jour de sécurité, respect des normes de développement OWASP, pen-testing, etc.)
- Processus humains: le risque vient aussi de l'intérieur (ex: renouvellement des crédentials après départ d'un membre d'équipe)



Enjeu #3: Autonomie

Autonomie énergétique

- Hardware basse consommation (tous les composants),
- Protocoles adéquats (ex: LPWAN)
- Comportement optimisé: fréquence de collecte et de communication, déclencher les échanges/traitement couteux que au besoin (ex: wake-up SMS)



Enjeu #4: Normalisation Applicative

Normalisation applicative

- Développement de « meta-languages » permettant d'attendre les promesses du « web sémantique »:
- o Tentatives de standardisation de dictionnaires « métier » (cf. IPSO)
- O Surcouche de références croisées / sémantique: JSON-LD, schema.org
- Programmes de développement de bibliothèques de modules applicatifs libre d'utilisation: ex: Fondation Eclipse, (Europe) programme Fiware

