Ecole Nationale des
Sciences Géographiques

Ecole Nationale des
Sciences Géographiques

Stage de fin d'études

Cycle des Ingénieurs diplômés de l'ENSG 3ème année

Feuille de style LaTeX de l'Ensg
Documentation plus que rapide
Version provisoire du 15 septembre 2015 à 14:49

Mohamed-Amjad LASRI

Septembre 2015

☒ Non confidentiel ☐ Confidentiel IGN ☐ Confidentiel Industrie ☐ Jusqu'au ...

Ecole Nationale des Sciences Géographiques
6-8 Avenue Blaise Pascal - Cité Descartes - 77420 Champs-sur-Marne
Téléphone 01 64 15 31 00 Télécopie 01 64 15 31 07

Jury

Président de jury :

Le président de jury

Commanditaire :

le commanditaire

Encadrement de stage :

qui a encadré ?

Responsable pédagogique du cycle Ingénieur :

Serge Botton, IGN/ENSG/DE/DPTS

Tuteur du stage pluridisciplinaire :

Patricia Parisi, IGN/ENSG/DE/DSHI

Stage de fin d'étude du xxx au xxx

Diffusion web : ☒ Internet ☒ Intranet Polytechnicum ☒ Intranet ENSG

Situation du document :

Rapport de stage de fin d'études présenté en fin de 3ème année du cycle des Ingénieurs

Nombres de pages : 23 pages dont 3 d'annexes

Système hôte : LaTeX

Modifications :

EDITION	REVISION	DATE	PAGES MODIFIEES
1	0	09/2012	Création

Remerciements

Je tiens à remercier toutes les personnes qui ont participé de différentes façons à la réussite de mon stage et plus particulièrement les personnes que je cite ci-dessous.

Olivier MARTIN, Frederic VERLUISE, Christian THOM et Christophe MEYNARD qui m'ont encadré, conseillé et ont répondu régulièrement à mes questions tout au long de mon stage.

Emmanuel BARDIERE, mon référent de stage ENSG, qui a suivi l'évolution de mon stage tout au long de ces cinq mois.

Tout le personnel du Laboratoire d'Opto-Électronique et de la société KYLIA.

Résumé

Ceci est mon résumé

Mots clés : clés, clés, clés

Abstract

This is my abstract

Key words: key, key, key

Table des matières

Table des figures

Liste des tableaux

Glossaire et sigles utiles

ENSG École Nationale des Sciences Géographiques
FIFO First In First Out
G3OS Geocube Operating System
GNSS Global Navigation Satellite Systems
GPS Global Positionning System
IEC The International Electrotechnical Commission
IHM Interface Homme Machine
ISO The International Organization for Standardization
NFC Near Field Communication
PCD Proximity Coupling Device
PICC Proximity Inductive Coupling Card
RTOS Real Time Operating System
TCP/IP Transmission Control Protocol/Internet Protocol

Introduction

La communication en champ proche (NFC) est une méthode de communication utilisée pour l'identification des personnes et des objets

Chapitre 1 Concepts clés et problématiques

Ce chapitre a pour but d'introduire le lecteur aux concepts clés nécessaires pour comprendre le travail effectué lors de ce stage. Le lecteur est prié de prêter une attention particulière au tableau des sigles lors de la lecture du présent document. Les protocoles qu'on présente utilisent un certain nombre d'abréviations conventionnelles pour désigner Les opérations d'échanges entre.

1.1 Les Géocubes

La miniaturisation des capteurs ainsi que la baisse des coûts de fabrication et de la consommation électrique des puces GNSS sont des facteurs qui peuvent laisser à envisager d'abandonner sur le terrain un réseau de capteurs opérant en permanence. Certains de ces capteurs GNSS permettent d'effectuer des mesures sur la phase donnant la possibilité de remonter à des précisions millimétriques, d'où l'idée d'un réseau de Géocubes. Le système Géocube est un réseau de capteurs GPS conçu et développé par le Laboratoire d'Opto-Éléctronique de Mesure et d'Instrumentation de l'Institut Géographique et Forestière Nationale. Il a comme objectif de mesurer les déformations avec une précision millimétrique. Ce réseau de capteurs a la particularité d'être très peu gourmand en énergie. On peut envisager de l'abandonner dans un milieu difficilement accessible sans qu'on ait à se soucier de son alimentation continue en électricité. En plus d'un module radio, un Géocube peut supporter plusieurs couches de capteurs lui permettant de collecter un certain nombre d'informations sur son environnement.

Dans les premières versions du Géocube initiés par LOEMI, Un opérateur humain peut communiquer directement avec un géocube en utilisant une de ces méthodes :

— Liaison série filaire, qui permet d'envoyer des commandes à travers l'interface en lignes de commandes de G3OS.
— Radio : Un protocol propriétaire particulier (DigiMesh©) est utilisé pour communiquer avec un Géocube.

Dans la version industrielle du Géocube maintenue par la société Kylia, une attention particulière est prêtée à l'étanchéité du boîtier qui le contient et à la robustesse du produit final. Ce choix crucial se justifie principalement par le fait qu'un réseau de Géocube peut être destiné à la surveillance environnementale en temps de crise et doit, par conséquence, être résistant aux conditions extremes que peut présenter un tel contexte.

Un réseau de Géocubes communique à travers le protocol radio DigiMesh©et l'utilise aussi pour centraliser les mesures acquises par les Géocubes vers un ordinateur, appelé coordinateur. Le coordinateur est le composant central du réseau, il encapsule toute la logique liée au traitement et au stockage des données. Il permet aussi à l'utilisateur de lancer des séries de calculs, récupérer les résultats ou de communiquer avec un Géocube en lançant des commandes qui seront transmises par radio. La Figure1.1 résume ce schéma de fonctionnement.

1.2 Les systèmes embarqués et les noyaux temps-réel dur :

Un système embarqué est par définition : Un système éléctronique et informatique autonome, souvent temps-réel, spécialisé dans une tâche bien précise []. De cette définition on peut ressortir

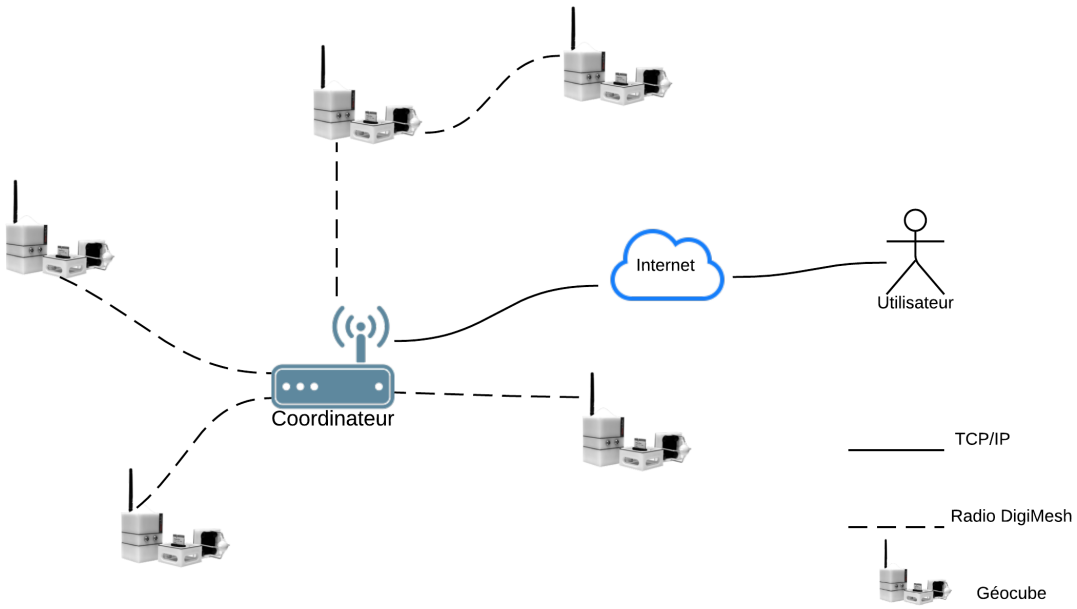

FIGURE 1.1 – Un réseau de Géocubes

deux éléments clés :

— Un système embarqué nécessite un développement matériel (électronique) mais aussi logiciel.
— Un système embarqué a la particularité d'opérer en temps-réel.

Le lecteur peut se poser la question légitime : Pourquoi on insiste sur le "temps-réel" dans cette définition ? Nos ordinateurs personnels n'opèrent-ils pas en "temps-réel" ?. Pour répondre à ces questions et introduire l'importance de ... dans le cas du système Géocube Il faut comprendre que le concept de temps réel en informatique est très relatif et varie d'un métier à un autre : Le temps-réel pour un développeur web est de pouvoir fournir à l'internaute de l'information sous forme de flux, en tolérant les temps de latence qui peuvent résulter parfois des temps d'accès à une base de données ou à la bande passante d'internet. Pour un développeur qui fait de l'informatique pour automobiles et doit, par exemple, développer les couches logicielles relatives à un système d'airbag, Le temps-réel dans ce cas est très strict et la quantification de ce temps latence est primordiale, sinon la vie des gens serait en danger.

1.2.1 Les tâches

Une tâche est le composant principal d'un RTOS. Lorsque vous effectuez plusieurs tâches simultanées sur un ordinateur avec une mémoire vive limitée, vous pouvez remarquer à partir d'un certain ... que vos tâches auront du mal à tourner ... Pour les systèmes d'exploitation en temps-réel, communément connus sous le nom de RTOS (Real Time Operating Systems) La quantification de ce temps de latence est primordiale.

Dans cette perspective, une équipe de chercheurs du LOEMI ont mis au point un RTOS adapté aux tâches qui sont effectuées par un Géocube.

Une liste non exhaustive de ces tâches serait alors :

— Une tâche GPS qui gère toutes les opérations en relation avec l'acquisition des données GPS :
— Une tâche Radio qui gère toutes les orpérations relatives à l'envoi et à la réception des

données et des commandes par radio ;
— Une tâche accéléromètre qui gère l'acquisition des données de l'accéleromètre...

On note ici qu'à chaque tâche on affecte une priorité. On revient à notre exemple d'airbag pour mieux appréhender cette notion. Imaginons maintenant que dans un RTOS destiné à l'industrie automobile on ne donne pas à la tâche qui gère l'airbag la plus haute priorité. Cela reviendrait à dire qu'à

1.2.2 La communication entre les tâches

Dans un RTOS généralement, et dans G3OS plus particulièrement, une tâche peut communiquer avec ses semblables ou répondre à des signaux provenant des capteurs, qu'on appelle interruption.

Un signal d'interruption permet à un composant du système embarqué de notifier le microcontrôleur central de l'arrivée d'un événement qui mérite son attention. Le choix de ces événements se fait souvent en programmant les registres des composants du système. Conventionnellement, le registre qui permet de choisir les événements déclencheurs d'interruptions s'appelle le registre principal des interruptions (Main Interrupt Register).

La communication entre les tâches s'effectue par plusieurs méthodes. La principale connue est la queue de messages. Ce mécanisme permet à une tâche de communiquer avec les autres en envoyant des messages. Un exemple typique serait alors : une tâche qui s'occupe de l'acquisition des données d'une puce GPS. Dès qu'une nouvelle trame de données est disponible, Cette tâche envoie et une autre du traitement de ces données, Dans ce cas la première tâche envoie à la deuxième les données acquises à travers la que

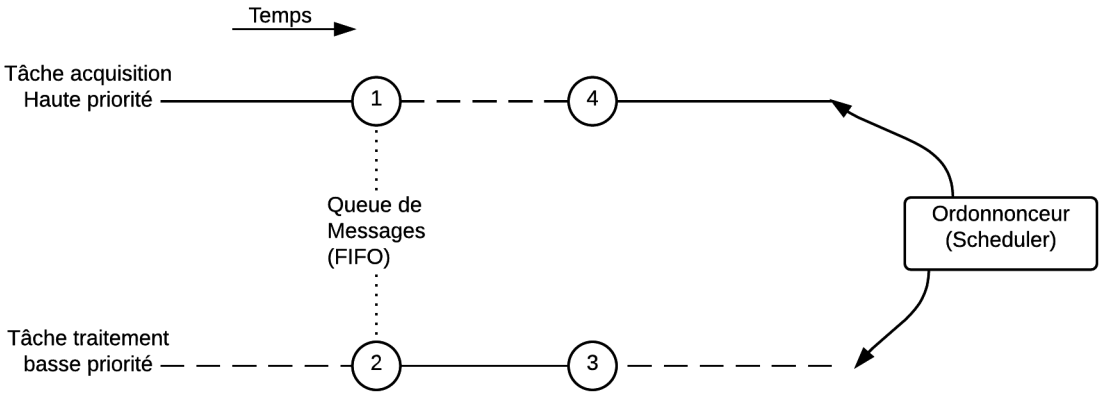

FIGURE 1.2 – Exemple multi tâches

1.3 La communication en champs proche (NFC)

La communication en champs proche est un ensemble de protocoles permettant d'établir une connexion radio entre deux dispositifs avec une distance ne dépassant pas 4cm. Aujourd'hui, on compte des millions d'objets connectés contenant la technologie NFC(cartes bancaires, smartphone, arrêts de bus, smartwatch...). L'interopérabilité entre les différentes puces équipant ces objets a poussé les constructeurs à mettre en place un certain nombre de normes régissant la fabrication, la programmation et l'utilisation de cette technologie.

La guerre des normes a fait converger les constructeurs vers l'ISO/IEC 14443. Cette norme encapsule en elle même quatre sous normes :

— ISO/IEC 14443-1 : Description des couches physiques
— ISO/IEC 14443-2 :
— ISO/IEC 14443-3 :
— ISO/IEC 14443-4 :

1.3.1 couches matérielles :

La conception des couches matérielles d'un circuit NFC doit respecter les recommandations de l'ISO/IEC 14443-1 et une partie de l'ISO/IEC 14443-2 pour garantir l'interopérabilité avec les autres dispositifs disponibles sur le marché. Un circuit NFC typique est composé de 3 parties principales :

— Une antenne : Selon les spécifications de la dite norme les dimensions de l'antenne ne doivent pas excéder 86mm x 54mm x 3mm.
— Une capacité adaptée pour garantir une raisonnance du circuit sur la fréquence 13.56Mhz ;
— Le PICC

1.3.2 couches logicielles :

1.4 Les infrastructures de production des logiciels

La conception et le développement des solutions logiciels dans un milieu industriel nécessite des infrastructures permettant d'automatiser un certain nombre de tâches qui, ensemble, forment ce qui est communément connu sous le nom de pipeline de production logicielle.

Cette chaîne de production est itérative, Elle favorise les cycles courts pour délivrer au client un produit évolutif et s'adaptant à ses besoins. Dans la Figure... on présente les principales étapes de cette chaîne.

Comme montré dans la Figure.... Une pipeline de production logicielle a un certain nombre d'acteurs externes humains qui garantissent son alimentation en versions(1) et en tickets(2). On définit alors ces acteurs comme suit :

— Développeur : s'occupe de la conception et le développement des solutions informatiques en réponse aux besoins des clients exp.. dans le gestionnaire des bugs. Son travail permet d'alimenter le gestionnaire de versions.
— Product owner : terme emprunté à la méthode Scrum. Il est l'interlocuteur unique des clients et permet de traduire leurs besoins en tickets(Gestionnaire de tickets)
— Testeur :

En plus de ces acteurs humains une infrastructure de production logicielle contient des composants logiciels pour automatiser un certain nombre de tâches :

— Gestionnaire de bugs : Comme son nom l'indique ce composant est un outil de communication et de traçabilité permettant de suivre l'évolution de la réponse du développeur au besoin du client et à la correction des bugs.
— Gestionnaire de versions : Cet outil est un classique de la gestion des projets informatiques, il permet, entre autres, aux développeurs de collaborer sur le même code source sans que cela n'affecte d'archiver tous les changements effectués sur un code source. Par souci de traçabilité, un gestionnaire de version est indispensable dans un projet informatique même s'il n y a qu'un développeur.
— Intégration continue

Chapitre 2

Conception, développement et déploiement d'un système de mise à jour automatique destinée au système Géocube :

Dans ce chapitre plusieurs diagrammes UML(Unified Modelling Language) sont utilisés pour simplifier la conception du système de mise à jour au lecteur. Pour plus d'informations sur le langage voir []. Le système de mise à jour développé fut baptisé Sharokey

2.1 Étude du besoin :

Le besoin se fait ressentir de plus en plus au sein de la société Kylia de disposer d'un système permettant aux clients qui ont acheté un système Géocube d'eefectuer des mises à jour automatiques et de profiter ainsi des améliorations éventuelles qui seront amenées aux couches logicielles des produit sans pour autant procéder à un rappel de celui ci.

En plus du de la gestion des mises à jour, ce système doit être au coeur de plusieurs métiers, permettant de coordonner le travail entre le développeur, l'administrateur système, l'opérateur commercial et les clients désirant profiter des dernières améliorations portées sur les couches logicielles.

De la Figure2.1 on définit les acteurs suivants :

— Opérateur commercial : Personne qui procède à la vente des systèmes Géocubes et des licences de mise à jour. Une licence a un date de début et une date de fin. Elle détermine la période ((pour laquelle)) le client à le droit de profiter du support logiciel à travers la mise à jour de son dispositif.
— Développeur : Personne responsable de l'alimentation continue du système en versions.
— Administrateur : Personne responsable de l'administration et la supervision du système de mise à jour.
— Coordinateur : Dispositif client destiné à être mis à jour.

Ce système doit en plus présenter les particularités suivantes :

— La supervision et l'administration du système doit être simplifiée à travers des interfaces homme-machine.
—
— Les logs du système doivent être expressifs et facilement accessible par l'administrateur.
— Les requêtes du client et les réponses du serveur doivent être sécurisées.

2.2 Conception statique

La Figure2.2 résume les cas d'utilisation de Sharokey.

La modélisation de la base de donnée est présentée dans la Figure2.2. On définit alors les entités suivantes :

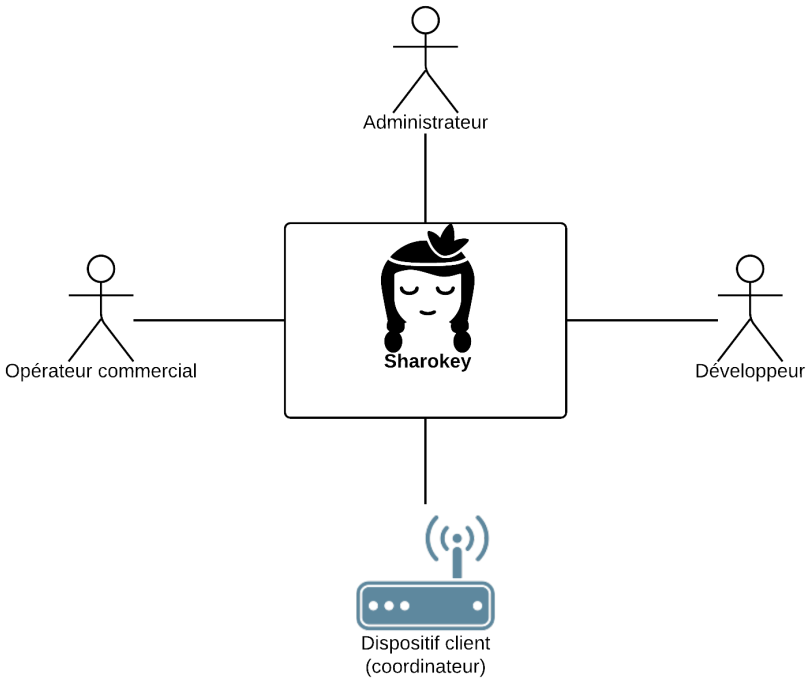

FIGURE 2.1 – Diagramme de contexte statique

— client : Personne physique qui effectue la commande d'un produit, elle est identifiée par IDC (clef primaire ID Client). Cette personne peut appartenir à une institution (entreprise ou organisme étatique), Les autres champs de la table servent à identifier les informations nécessaires au contact : Nom, Prénom, Téléphone, E-mail et un commentaire qui est laissé au soins de l'opérateur commercial.
— product : C'est le coordinateur qui est destiné à recevoir les mises à jour. Il est identifié par son Part-Number (IDP). On lui attribue en plus un nom qui est généralement celui de la marque du fabriquant.
— license : Entité qui établie la relation entre la table product et la table client, en utilisant des clés étrangères vers leurs identifiants. Elle attribue à chaque client une licence de mises à jour sur un produit pour une durée comprise entre une date de début (start date) et une date de fin (end date).
— software : C'est la table qui contient toutes les mises avec les numéros de versions correspondants. Elle contient une clef étrangère vers la table product, puisque chaque mise à jour est destinée à un produit particulier. chaque mise à jour est identifiée par une version majeure, une version mineure et une version de patchs. La version 1.0.5 correspond alors à la version majeure 1, la version mineure 0 et la version de patchs 5. En plus, chaque mise à jour a un type qui peut être soit V (pour version), ou P pour (patch). La différence réside dans la pertinence des améliorations portées.
— Les triggers : Deux triggers pour écouter les événements des tables : client et product.

2.2.1 Format des mises à jour

Une mise à jour est un script auto-extractible fabriqué en utilisant le programme Makeself. Un format de paquets a été conçu pour simplifier et automatiser la création des scripts de mise à jour. Ce format a un point d'entrée qu'on nomme "go.sh" et un répertoire de scripts et de données baptisé "installerScripts". go.sh est un script shell qui execute les scripts contenus

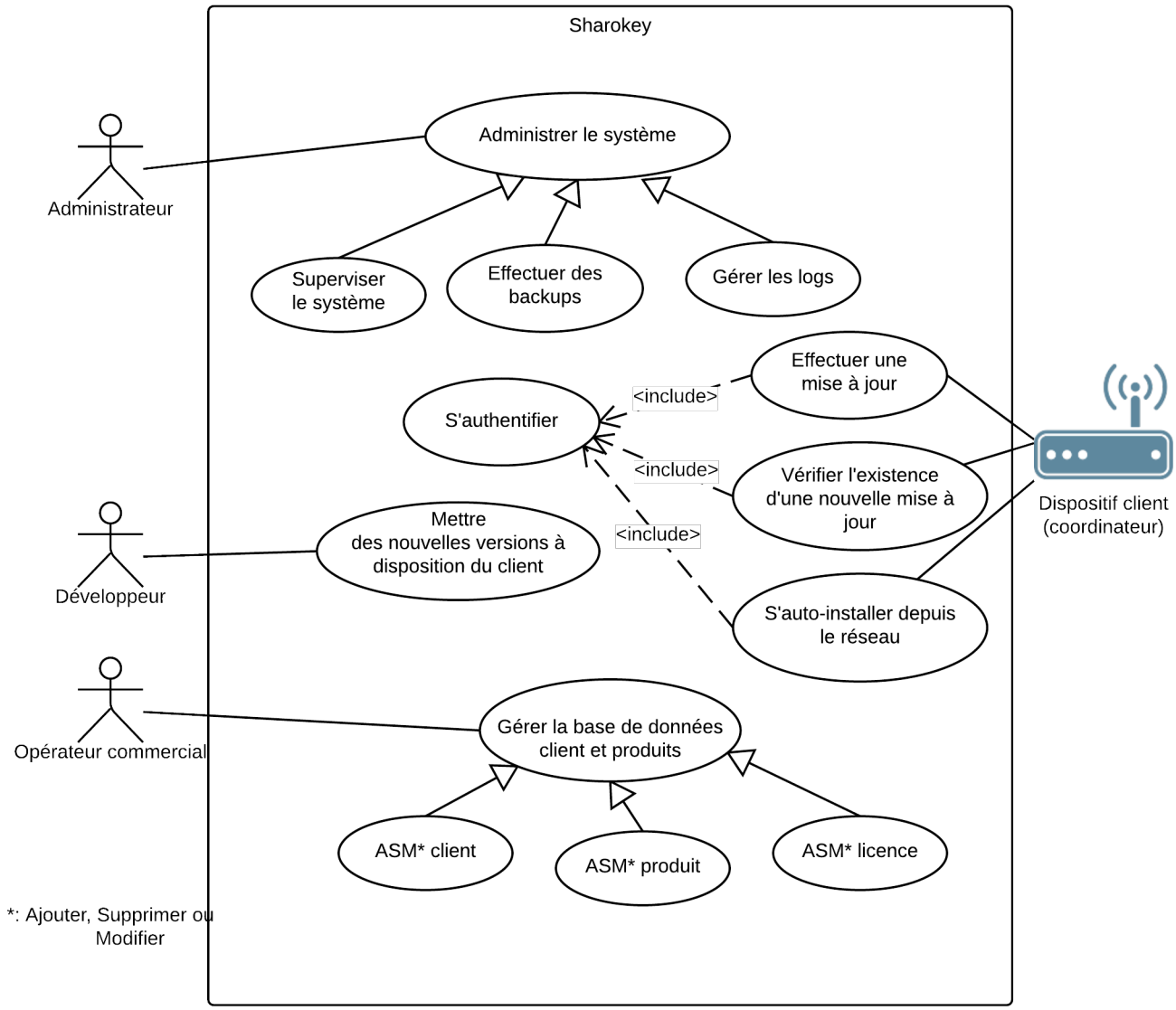

FIGURE 2.2 – Diagramme UML des cas d'utilisation de Sharokey

dans installerScripts. la fabrication d'un éxecutable auto-extractible à partir de ces éléments en utilisant Makeself permet d'ajouter un mécanisme de vérification de l'intégrité du paquet de mise à jour avec une somme MD5.

2.2.2 Architecture logicielle

Sharokey est une solution informatique légère de mise à jour automatique pour les solutions informatiques propriétaires basés sur un système d'exploitation GNU/Linux et nécessitant une licence ou une autorisation pour faire les mises à jour. Il est basé sur une architecture client-serveur. Le client est codé entièrement en Shell pour garantir une portabilité sur toutes les distributions GNU/Linux et sur une grande panoplie d'architectures matérielles : Intel, ARM, MIPS, ... Le serveur est écrit en NodeJS. Ce choix garantie se portabilité sur les serveurs utilisant des OS type Windows ou GNU/Linux. Toute fois, il est fortement conseillé d'utiliser GNU/Linux. Les tests effectués jusqu'à ce jour n'ont porté que sur ce type d'OS.

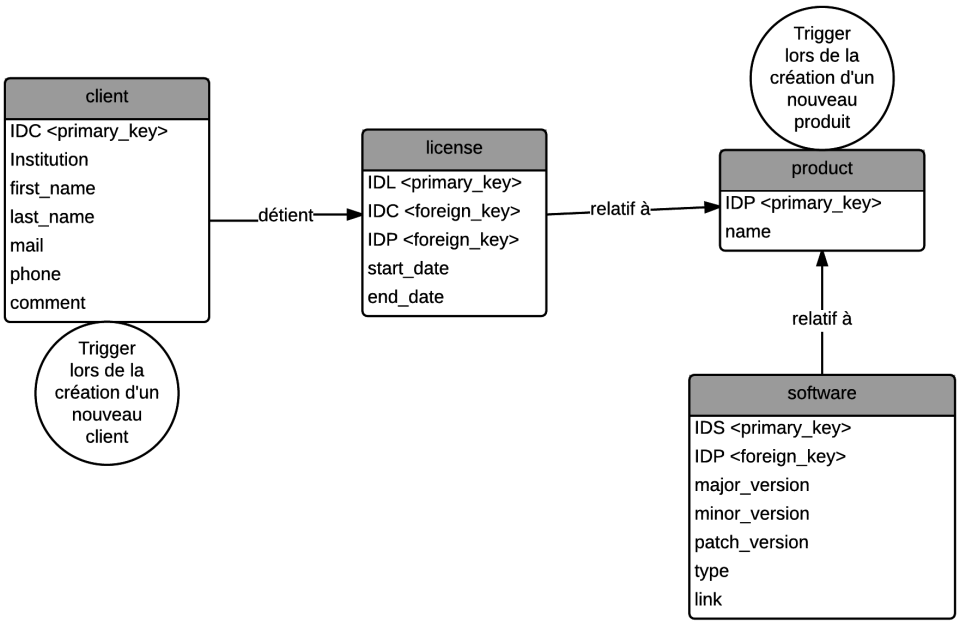

FIGURE 2.3 – MDP (Modèle Physique des Données) de la base de données Sharokey

Client :

Comme schématisé dans la Figure, La partie client est contituée d'un ensemble de paquets Kylia dont nous présentons les fonctionnalités ci-dessous :

— checker.kyl : Ce paquet renvoie trois codes possibles 0, 1 ou 2. 0 si le dispositif client arrive à se connecter au serveur mais aucune nouvelle mise à jour n'est disponible. 1 si le dispositif client arrive à se connecter au serveur et il y a une nouvelle mise à jour a effectué. 2 si le dispositif client n'arrive pas à se connecter à internet [1].

2.3 conception dynamique

Dans la conception dynamique on définit un certain nombre de scénarios typiques que le système ...

2.3.1 Sécurité du système

La stratégie de sécurité instaurée pour Sharokey doit respecter les trois points suivants :

— S'assurer de l'identité du dispositif qui effectue la mise à jour
— Les requêtes des clients et les réponses du serveur doivent être cryptés pour assurer la protection des paquets binaires lors de leur transition via le réseau.
— S'assurer de l'intégrité des paquets envoyés par le serveur.

Dans cette perspective un système d'authentification par vérification de signature numérique sur la clef publique du client a été implémenté dans Sharokey. Une autorité de certification (KyliaCA) a été créée [2]. Son but est de signer la clef publique des clients pour garantir que leur dispositif a bien été vendu par Kylia. La génération des clés (privé et publique) des clients

1. Le code retour 2 est important pour le coordinateur des Géocubes, puisque ce dernier est dépendant d'internet. Ce code retour permet d'informer le client d'un souci de réseau
2. Système cryptographique asymétrique en utilisant le standard RSA

s'effectue d'une manière automatique dans Sharokey dès la création d'un nouveau client dans la base de données, d'ou le trigger Pl/PGSQL sur la table client(Figure2.2).

Pour créer une pair de clés (privé et publique signée) pour un client. Sharokey effectue trois opérations en utilisant les fonctions de la librairie OpenSSL :

— Créer une pair de clés aléatoires en utilisant le standard RSA et avec une longueur de 2048 octets [3]
— À partir de la clef publique, créer un CSR (Certificate Signature Request).
— Signer le fichier CSR avec KyliaCA et générer ainsi une clef publique signée par l'autorité de certification de l'entreprise [4].

Un tel mécanisme d'authentification assure que le dispositif qui veut effectuer la mise à jour provient de la société Kylia, et répond donc au premier point de sécurité précédemment énoncé.

Concernant le deuxième point relatif au cryptage des requêtes clients et des réponses du serveur. Sharokey oblige toutes les requêtes à passer par le protocole HTTPS pour garantir le cryptage des informations échangés entre le client et le serveur, et ceci en utilisant une cryptographie asymétrique basée sur l'échange mutuel des clés publiques.

Enfin, le troisième point relatif à l'intégrité des données transitant par le réseau est garantit par un mécanisme de checksum-MD5 implémenté par défaut dans le générateur de scripts auto-extractibles Makeself.

2.4 Commandes personnalisées

— `\newevenpage` : identique à `\newpage` mais en insère une page blanche de façon à débuter la nouvelle page sur un numéro de page impaire.
— `\evenchapter{titre}` : démarre un nouveau chapitre sur une page impaire, `\evenchapter[titre sommaire]{titre}` fonctionne aussi mais pas `\evenchapter*{titre}`
— idem pour `\evenpart{titre}`

2.5 Fichier source de cette doc

Ce fichier `tex` contient toute la structure d'un rapport mais une bonne partie est désactivée car commentée par l'environnement `\begin{comment} ... \end{comment}`

3. À ce jour, aucune faille n'est connue dans RSA pour les clés de longueur 2048 octets
4. Une autorité de certification est aussi une pair de clés publique-privé sauf qu'elle n'a été signée par aucune autre CA. Elle est auto-signée par elle même

Conclusion

Il est l'heure de conclure : bonne nuit !

Annexes

Filtre de Kalman

Annexe A

Annexe 1