



Architecture des Systèmes d'Information

Département  
ASI



# Rapport de stage ingénieur Carte Acoustique



# **Remerciements**

Je souhaiterais tout d'abord remercier Philippe BLOT et Jean-Charles RENAUD, tous deux coordinateurs de la société UNT, pour m'avoir accueilli chaleureusement au sein de leur équipe.

Je voudrais ensuite remercier mon tuteur de stage, Jean-Philippe AUTHIER, pour toute l'aide qu'il m'a apporté et tout le temps qu'il m'a consacré pour mener à bien mon stage d'ingénieur. De plus, je souhaiterais remercier les autres membres de l'équipe technique UNT, Thomas LE OUËDEC et Didier MOBETIE entre autres, pour avoir pris de leur temps pour répondre à mes questions et Guy LANGLOIS, pour ses explications sur le contexte de travail.

# Table des matières

<b>Remerciements</b>	<b>3</b>
<b>Glossaire</b>	<b>5</b>
<b>1 Introduction</b>	<b>6</b>
<b>2 Présentation de l'entreprise</b>	<b>7</b>
2.1 Activité . . . . .	7
2.2 Stratégie . . . . .	9
2.3 Ressources humaines . . . . .	9
2.4 Ressources technologiques . . . . .	10
<b>3 Présentation du sujet du stage</b>	<b>11</b>
3.1 Plate-forme de tests . . . . .	11
3.2 Plate-forme de démonstration . . . . .	12
<b>4 Le travail effectué</b>	<b>13</b>
4.1 Contexte de travail . . . . .	13
4.2 Plate-forme de tests . . . . .	28
4.3 Plate-forme de démonstration . . . . .	35
<b>5 Conclusion</b>	<b>51</b>
5.1 Les réalisations . . . . .	51
5.2 Bilan personnel . . . . .	51
<b>Bibliographie</b>	<b>53</b>
<b>A Procédure SVI dans l'application Web</b>	<b>54</b>
<b>B Documentation d'une signature acoustique</b>	<b>57</b>

# Glossaire

**ASI** *Architecture des Systèmes d'Information*

**HTTP** *HyperText Transfert Protocol.* Protocole de transfert de fichiers HTML à travers un réseau TCP/IP

**INSA** *Institut National des Sciences Appliquées*

**ISP** *Internet Service Provider.* Fournisseur d'accès à internet (FAI), est un organisme (généralement une entreprise mais parfois aussi une association) offrant une connexion à Internet, un réseau informatique mondial.

**IVR** *Interactive Voice Response.* Un serveur vocal interactif est un système informatique permettant aux utilisateurs d'accéder à la base de données d'une société et d'émettre diverses demandes de service, au moyen d'un téléphone fixe, mobile ou logiciel. Les serveurs vocaux interactifs entrent plus généralement dans la catégorie des systèmes de dialogue.

**OTP** *One-time password.* Un Mot de passe unique ou OTP est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaque par rejeu(replay attack).

**PCI/DSS** *Payment Card Industry Data Security Standard.* Standard de sécurité des données pour l'industrie des cartes de paiement.

**PHP** *Hypertext Preprocessor,* est un langage de scripts libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP

**SAS** *Strong Authentication Server*

**XML** *eXtend Markup Language.* Langage extensible de balisage de documents, élaboré par le groupe de travail ERB (Editorial Review Board) du W3C (World Wide Web Consortium)

# **Chapitre 1**

## **Introduction**

Dans le cadre de ma scolarité au sein du département Architecture des Systèmes d'Information de l'Institut National des Sciences Appliquées de Rouen, il me fallait suivre une formation qui est consolidée par deux stages obligatoires. Ce rapport constitue une synthèse du travail effectué lors de mon stage ingénieur réalisé au sein de la société UNT entre le 25 Mars et le 31 Août 2013 qui dure 22 semaines .

Le stage ingénieur permet d'approfondir d'une part mon savoir-faire au sein de l'entreprise et permet de mettre en pratique d'autre part les connaissances acquises au cours de ma formation au sens du département ASI.

Ce rapport se divisera en 3 parties. Dans un premier temps, je donnerai une description de la société UNT, de ses objectifs et de quelques uns de ses produits. S'en suivra une présentation du travail effectué lors de ce stage de vingt-deux semaines. Enfin, je concluerai sur ce qui a été réalisé et sur le bilan personnel.

# Chapitre 2

## Présentation de l'entreprise

### 2.1 Activité

La société UNT développe et commercialise des circuits électroniques fins, souples et autonomes embarqués dans les cartes à puces. Les docteurs et ingénieurs au service d'UINT déploient leur forte expérience dans la recherche et le développement de l'électronique, de la sécurité des transactions et de la fabrication des cartes à puces, en maîtrisant tous les processus et cycles de vie des produits allant de la conception à la fabrication.

UINT a pour ambition d'être le leader mondial sur le marché des cartes à puces ISO dites actives (qui embarquent leur propre source d'énergie). En créant de la valeur ajoutée sur le support carte notamment via l'intégration de ses électroniques flexibles autonomes, UNT permet l'interactivité du porteur avec la carte et vice versa, offrant de nouveaux services disponibles 24h/24h qui vont révolutionner l'utilisation des cartes à puces avec leur environnement.

UINT a développé ses propres produits :

- *U-GIFT* est une carte au format bancaire, embarquant une pile, un haut parleur et des diodes. Cette carte peut jouer de la musique et avoir des lumières qui scintillent. Cette carte est destinée au marché de l'affinitaire et de la carte cadeaux. Par exemple, une carte prépayée « joyeux anniversaire » qui peut jouer de la musique en plus de toutes les autres fonctions d'une carte cadeau « traditionnelle ».
- *SPI* (Solution numérique d'impression sécurisée) est une solution logicielle et matérielle permettant de s'assurer que la personne qui imprime un document est la même que celle qui va récupérer les documents sur l'imprimante. Pour simplifier, pour récupérer les documents sur l'imprimante, la personne va devoir s'authentifier via un badge et un code pin.
- *uSecure* est une carte au format bancaire qui permet de contrôler l'émission d'une trame RF en appuyant sur un bouton. Il s'agit de la première carte RF contrôlée par l'utilisateur.

#### 2.1.1 Circuits flexibles

UINT conçoit et développe ses circuits flexibles qui s'insèrent notamment dans des cartes au format bancaire ISO 7810. L'électronique utilisée dans les produits est choisie en fonction

de ce critère de flexibilité ainsi que de leur faible consommation.



### 2.1.2 Sécurité / Identification

Que ce soit pour l'identification, l'authentification, le contrôle d'accès, le paiement ou tout autre service lié à la sécurité, l'expertise dans le domaine de la sécurité de notre équipe vous garantit une compréhension totale de votre projet.



Voici quelques exemples de produits phares et voies de développement envisagées :

- Jeu : carte de jeu prépayée
- Santé : auto contrôle de paramètres physiologiques (pouls, température...)
- Sécurité : affichage de mot de passe dynamique ; contrôle de l'émission de signature RF, acoustique, biométrie
- Marketing : carte musicale, à lumière, à écran...
- Logistique : traçabilité, surveillance de température, capteurs...

Concernant les modèles de revenus de la société, ces derniers sont variables suivant les projets. Lorsqu'UINT réalise de la R&D pour ses clients en vue de la fabrication de leurs produits, la société se rémunère sur cette R&D et bénéficie de royalties ou licences sur les produits. Lorsqu'il s'agit de ses propres produits, par exemple la U-GIFT Card, UINT démarche les grands noms des distributeurs ou émetteurs de cartes cadeaux / fidélité pour mettre la U-GIFT Card dans leur catalogue. Dans ce cas, UINT personnalise la carte (visuel, musique) à la demande du client qui, lui, vendra la carte en «boutique».

### 2.2 Stratégie

La R&D est au cœur de l'activité de la société. Sur les 8 salariés, 7 ont une formation de type technique (électronique ou informatique) dont 3 docteurs et 2 ingénieurs. Il est à noter que deux des produits conçus par UIINT ont reçu une certification Mastercard.

Sur le territoire national, UIINT n'a aucune concurrence. Au plan international, bien qu'il y ait des sociétés proposant des produits «cartes» avec de l'électronique flexible, aucune ne se positionne comme UIINT avec un portfolio de produits aussi variés. Hormis UIINT, à notre connaissance, la concurrence ne conçoit et ne produit que des cartes avec un afficheur dans le domaine de la sécurité.

Come abordé précédemment, UIINT maîtrise la conception de circuits flexibles ainsi que la gestion de la faible consommation des composants électroniques.

La société UIINT a reçu «L'Électron d'Or de la meilleure Start-Up 2010» lors de la cérémonie qui s'est tenue au siège parisien de la FIEEC (Fédération des Industries Électriques, Electroniques et de Communication), le 16 juin 2010. Ce prix est remis par le magazine ElectroniqueS et le sponsor RS parmi les 12 lauréats de cette 13ème édition. Les nominés sont des entreprises et des grands groupes nationaux et internationaux (France, Etats-Unis, Allemagne, Royaume-Uni, Norvège, Japon...) repérés par la rédaction du journal à travers l'actualité de leur activité ou de leurs projets. Un jury expert comptant des professionnels du secteur, des consultants et des membres de la rédaction du journal ElectroniqueS est chargé de l'attribution des prix.

La société UIINT a reçu le prix «de l'innovation à l'internationale 2010» lors du 5ème forum de l'international à Evry le 9 décembre 2010. Ce prix a été décerné par la CGPME 91 et la CCI Essonne.

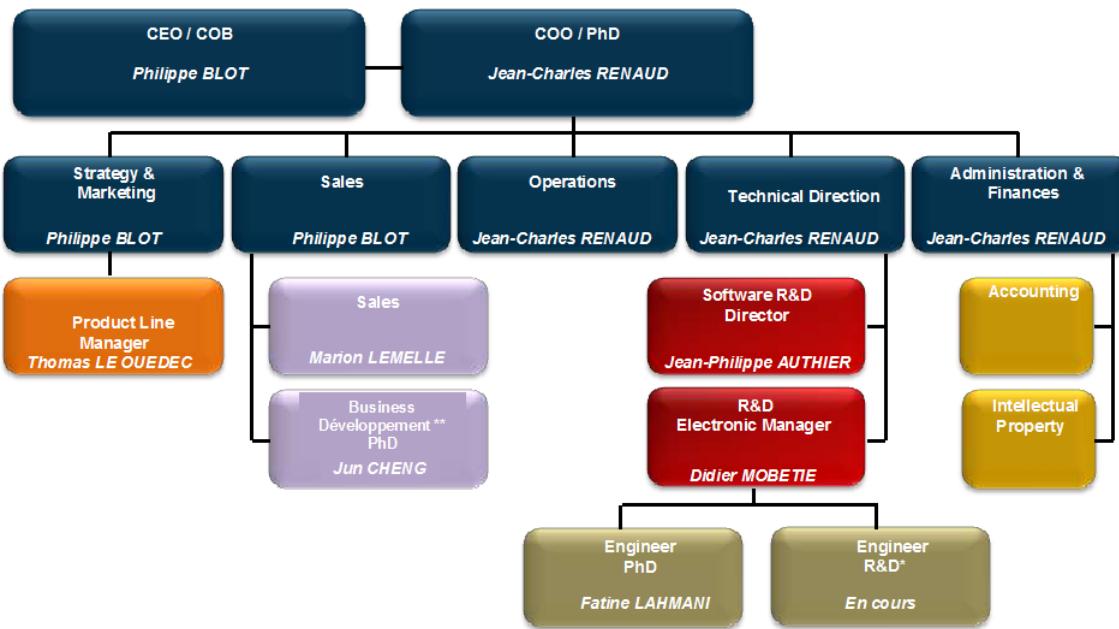
Enfin, la société s'est tournée ces derniers mois vers la Chine en vue d'établir des partenariats technologiques, commerciaux et avec des distributeurs. Depuis le 4 janvier 2011, elle a signé deux contrats avec un partenaire technologique (fabrication de carte) et un distributeur.

UIINT vient de créer sa propre usine d'hybridation (soudage des composants électroniques au circuit flexible), afin de réduire les coûts de fabrication et augmenter ainsi sa marge. UIINT souhaite également agrandir son équipe d'ingénieurs en électronique afin de toujours concevoir de nouveaux produits innovants.

### 2.3 Ressources humaines

A ce jour, UIINT est composée de 8 salariés. UIINT fait principalement de la R&D. Sur les 8 salariés, 7 ont une formation de type technique (électronique ou informatique) dont 2 docteurs et 5 ingénieurs.

Ce bilan est antérieur à l'ouverture des Laboratoires sur le site de Limoges et qui doit conduire à l'ouverture d'une vingtaine de postes d'ici fin 2014.



## 2.4 Ressources technologiques

### 2.4.1 Savoir faire et technologies maitrisées

- UNT maîtrise la conception de circuits fins et flexibles ainsi que la gestion de la faible consommation des composants électroniques.
- UNT maîtrise l'hybridation des composants électroniques sur circuit flexible
- UNT invente, conçoit, développe et distribue des solutions de cartes multifonctions avec des microprocesseurs sécurisés et autonomes.
- UNT conçoit et développe des solutions pour authentifier des utilisateurs lors d'échanges sécurisés.

### 2.4.2 En termes de protection industrielle, elle possède des brevets

- WO2011067543 : activation et indication d'un champ RF sur un dispositif comprenant une puce
- PCT / FR 2010 / 052767 : carte à puce multi-applicatifs avec validation biométrique
- FR 2953619 : dispositif électronique (jeton) téléphonique

### 2.4.3 Certifications acquises

A l'heure actuelle, la société UNT ne possède pas de certification, néanmoins deux de ses produits ont reçu une certification Mastercard.

# Chapitre 3

## Présentation du sujet du stage

J'ai intégré l'équipe *Carte acoustique* pendant mon stage d'ingénieur.

Le stage proposé s'inscrit dans le cadre de l'optimisation d'un système d'authentification forte dont le mot de passe dynamique est généré en acoustique.

Le format du système d'authentification sera préférentiellement celui d'une carte bancaire mais pourra également revêtir celui d'une mini calculette. L'un des objectifs du stage est de fiabiliser la signature acoustique : celle-ci devra prendre en compte les requis des systèmes de télécommunications, les contraintes des formats proposés et les spécifications électroniques. Les informations incluses dans le message acoustique devront pouvoir être déconvolées puis traitées avec un pourcentage de succès important, celui-ci sera notamment déterminé en fonction de conditions opératoires variables.

### 3.1 Plate-forme de tests

Maintenant la carte est en version 4G (V4G : quatrième génération de smartcard), qui est fonctionnelle et attend les tests. Les tests ont pour objectif d'évaluer la performance de carte en différents aspects, par exemple :

- Taux de récupération avec différents périphériques et conditions
- Fiabilité de l'encryptage
- Durée de vie
- etc...

C'est le stagiaire qui est le responsable de concevoir le plan de test et de l'implémenter.

## 3.2 Plate-forme de démonstration

Maintenant UINT possède une plate-forme de démonstration, un site pour montrer l'utilisation de la carte acoustique figuré ci-dessous, mais les fonctionnalités sont très limites. Un nouveau site de démonstration, plus complet et abondant est nécessaire.

Plug-In	IVR	OneClick
	<p>Please call <b>+33 (0)9 70 75 19 28</b> and follow instructions for authentication.</p> <p><b>UINT</b> The Acoustic Authentication module currently supports only Microsoft Internet Explorer.</p>	
	<p>You want to be called back? Call <b>+33 (0)9 70 75 19 29</b> then hang up when ringing. You will be called back immediatly.</p> <p>You can also make a Skype call: <a href="http://uinttechno">uinttechno</a></p>	<input type="text"/> <input type="button" value="Call me"/>
	<b>Session Number: 451727</b>	
<hr/>		
<p>RAW</p> <input type="text"/>	<input type="button" value="Submit RAW"/>	
<input type="button" value="v Transcode v"/>		
<p>Serial Number</p> <input type="text"/>	OTPa <input type="text"/>	OTPb <input type="text"/>
		<input type="button" value="Submit SN+OTPa"/>

FIGURE 3.1 – Site de démonstration acoustictechno

Le nouveau site (par exemple un site d'achat en ligne) doit contenir au moins les fonctionnalités suivantes :

- Utiliser la carte acoustique comme un moyen d'authentification par un utilisateur déjà inscrit
- Utiliser la carte acoustique comme un moyen de paiement avec les différents possibilités
  - avec navigateur Web
  - avec téléphone ou mobile
  - Autres à définir

# Chapitre 4

## Le travail effectué

### 4.1 Contexte de travail

#### 4.1.1 Caractéristiques générales de la carte acoustique

##### Caractéristiques physiques de la carte acoustique

Les caractéristiques physiques de la carte acoustique respectent les standards suivants :

- **ISO 7810** : la carte a été certifiée conforme. Ce format est celui de la carte bancaire (85.60 x 53.98 mm)
- **ISO 7811** : ce standard est une extension de l'ISO 7810. Il décrit les techniques d'enregistrement d'identité sur la carte : embossage et piste magnétique.
- **ISO 7816** : la carte est compatible avec cet ISO si l'on souhaite y apposer une puce de type EMV
- **ISO 14443** : la carte peut être équipée d'une puce et d'une antenne RFID (13.56 MHz)



FIGURE 4.1 – Face avant d'une carte acoustique

##### Fonctionnalités générales

La carte acoustique émet une séquence acoustique unique à chaque pression du bouton. La carte utilise un microprocesseur pour calculer les deux OTP (One Time Password). L'énergie utilisée provient d'une batterie fine et flexible.

### Schéma d'une carte acoustique

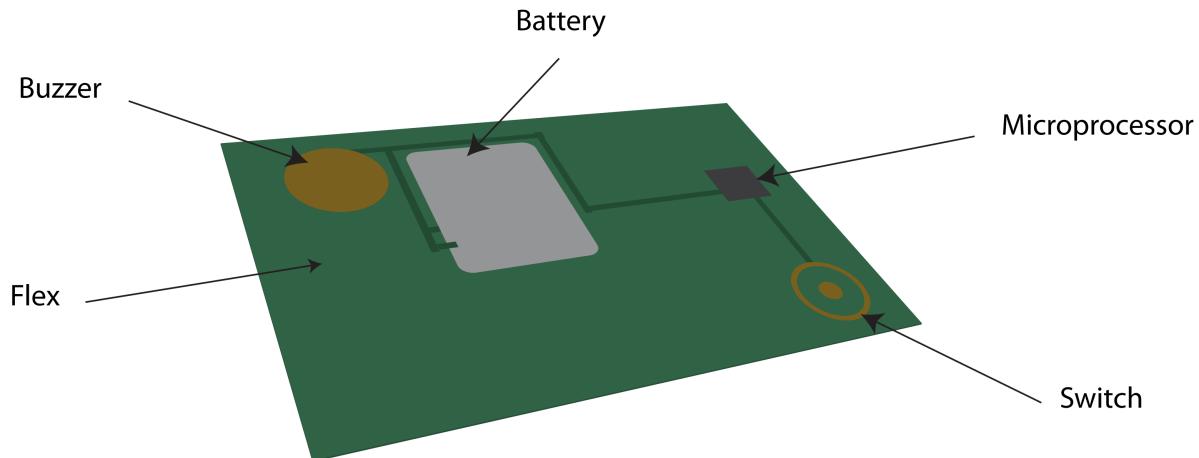


FIGURE 4.2 – Schéma d'une carte acoustique

L'électronique embarquée est composée des éléments suivants :

- Un microcontrôleur
- Une pile flexible de 3V – 10 mAh
- Un buzzer
- Un « bouton » qui déclenche la séquence acoustique.

Tous ces éléments ont été intégrés sur un circuit imprimé flexible, ou « flex ». L'ensemble des composants électroniques (microcontrôleur, buzzer et pile) sont directement soudés au « flex » par un processus de capillarité. Cet ensemble (Flex composants) est appelé Inlay et est intégré à l'intérieur de la carte PVC.

#### 4.1.2 Introduction à l'authentification forte

Cette section a pour objectif de présenter le domaine de l'authentification forte, c'est-à-dire la problématique à laquelle il répond ainsi que les solutions qu'il propose.

##### Définition de l'authentification

S'authentifier, c'est prouver son identité (« je suis bien celui que je prétends être »).

##### A quoi sert l'authentification

Les nouvelles technologies de l'information et de la communication conduisent à une véritable explosion des échanges d'information sur les réseaux de télécommunication, tant dans l'univers professionnel que dans la vie quotidienne. Dans le même temps, les tentatives de fraude se multiplient, notamment par usurpation d'identité. L'authentification a pour objectif de renforcer la sécurité de ces échanges.

### Les principaux moyens d'authentification

L'utilisateur apporte la preuve de son identité en fournissant un élément :

- Que l'utilisateur est le seul à savoir (un mot de passe ou un secret par exemple) ;
- Que l'utilisateur est le seul à détenir (un authentificateur : une carte, une clé, ...) ;
- Qui caractérise l'utilisateur (empreinte digitale, image rétinienne, ...).

Chaque élément s'appelle « facteur d'authentification ». On parle d'authentification forte dès que le processus d'authentification fait appel à la combinaison d'au moins deux facteurs, par exemple un objet détenu par l'utilisateur et un mot de passe (code PIN) qu'il est le seul à connaître. Le processus d'authentification forte fait appel à un serveur d'authentification capable de comparer les éléments présentés par l'utilisateur avec les informations qu'il détient afin de délivrer – ou non – les droits d'accès.



FIGURE 4.3 – Représentation schématique de l'authentification forte

### Le mot de passe dynamique

Il constitue une solution de plus en plus utilisée, notamment parce qu'il permet de conjurer simplicité d'utilisation et robustesse en termes de sécurité. L'objet détenu par l'utilisateur (authentificateur ou « Token ») affiche, ou envoie directement, à intervalles réguliers ou à la demande, un mot de passe imprévisible et non réutilisable.

Au même instant, le serveur a calculé le même code pour cet utilisateur. Ceci est possible car l'authentificateur et le serveur disposent des mêmes éléments pour calculer le code. Il suffit alors au serveur de comparer le code calculé avec celui qui lui a été transmis. Le deuxième facteur associé à la solution, permettant de renforcer la sécurité en évitant le vol de l'authentificateur par un fraudeur lui donnant ainsi accès à l'information, est constitué d'un code personnel d'accès.

### Le marché de l'authentification

Il connaît actuellement une très forte croissance, avec une prise de conscience de la nécessité de renforcer la sécurité de l'accès aux services en ligne et aux applications sensibles des entreprises. Dans le monde bancaire, le Federal Financial Institutions Examination Council (FDIC) a récemment publié un rapport incitant les banques à mettre en œuvre des solutions d'authentification forte à la mesure des risques encourus. Une étude récente de Frost & Sullivan prévoit que le marché des authentificateurs, évalué à 248,1 millions de dollars en 2004, devrait bondir à 1,171 milliards de dollars en 2011.

### OATH

OATH (Open AuTHentication) est une initiative d'un ensemble d'acteurs leaders du marché IT, travaillant ensemble afin de fournir une architecture de référence pour l'authentification forte. Basé sur des standards ouverts, OATH propose une interopérabilité entre les plateformes de validation (hardware et software) et tokens de fournisseurs différents afin d'offrir aux entreprises la possibilité de choisir et d'intégrer les meilleures offres du marché, afin de faciliter le déploiement et d'optimiser les coûts.

#### 4.1.3 Mécanismes de la séquence acoustique

##### Les constantes et variables essentielles

L'algorithme permettant la génération de la trame acoustique est constitué de différentes fonctions cryptographiques qui vont calculer les cryptogrammes nécessaires à la génération du message. Il existe plusieurs valeurs importantes à traiter lors du calcul d'un cryptogramme. Ces valeurs sont de différentes natures, constantes ou variables, secrètes ou non, mais sont toutes enregistrées dans l'EEPROM lors de la personnalisation, c'est-à-dire lors de l'ultime étape de programmation du microcontrôleur. Ces différentes valeurs sont présentées dans le chapitre qui suit.

*Les clés cryptographiques (HOTP KeyA & HOTP KeyB) :* Les clés cryptographiques sont des clés de quelques octets chacune. Ces clés sont générées par un logiciel développé par la société UINT. Ce logiciel fournit un couple de clés complètement aléatoires.

Ces deux clés sont des constantes et ne sont jamais modifiées par le programme sous peine de rendre le token inutilisable. Ces clés représentent un secret à protéger absolument car elles sont à la base du calcul du cryptogramme.

*Le compteur d'événements (Event Counter) :* Le compteur d'événements, comme son nom l'indique, comptabilise le nombre de pressions du bouton effectuées depuis la mise en route du token. Il est important de noter que ce compteur est chargé, lors de la personnalisation, avec une valeur aléatoire. Ce compteur représente le second secret à conserver car, tout comme les clés, il est utilisé dans le calcul du cryptogramme. Ce compteur a une taille de 8 octets.

*Le numéro de série (Id) :* Le numéro de série du token est codé sur 29 bits. Cette valeur permet de répertorier les tokens et de les associer avec leurs clés et leur compteur d'événements. Le numéro de série n'est pas un secret, il est d'ailleurs transmis dans la trame acoustique. Maintenant que sont connues les quelques valeurs importantes utilisées lors de

l'exécution du programme, il est possible de s'intéresser à la manière dont elles sont utilisées par l'algorithme de génération de la trame acoustique.

### 4.1.4 Génération du cryptogramme acoustique

Une fois les étapes préliminaires effectuées, il s'agit de calculer le cryptogramme à l'aide de fonctions spécifiques normalisées par des standards. Le chapitre qui suit explique la méthode adoptée afin de calculer ces données qui constituent le cœur du futur message à émettre.

#### La génération d'un HOTP

Les informations qui suivent sont issues de la rfc4226, HOTP : An HMAC-Based One Time Password Algorithm. Ce document décrit un algorithme basé sur HMAC pour générer un mot de passe unique (One Time Password). Ce document est le fruit d'un effort conjoint des membres de la communauté OATH pour spécifier un algorithme d'authentification qui est proposé librement à toute organisation.

#### La génération du cryptogramme

Les différentes opérations nécessaires à la génération d'un HOTP définies, il s'agit maintenant de présenter l'utilisation qui est faite de ce HOTP. Afin de créer un cryptogramme qui va par la suite être encodé, le programme va générer deux HOTP, HOTPa et HOTPb, respectivement de 31 octets et 20 octets, à partir de deux clés distinctes, HOTP\_Keya et HOTP\_Keyb. Le programme va ensuite concaténer ces HOTP en leur ajoutant l'identifiant (Id) du token, et l'on obtient un cryptogramme représenté schématiquement ci-dessous :

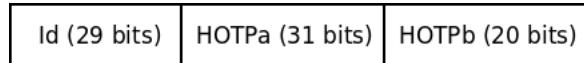


FIGURE 4.4 – Représentation schématique du cryptogramme

Le cryptogramme est ainsi fabriqué. Cette étape constitue la dernière étape du processus de chiffrement des informations. Le cryptogramme peut maintenant être encodé afin de le rendre plus robuste au canal de transmission.

#### L'encodage du cryptogramme

L'encodage du cryptogramme est une étape qui consiste à mettre en forme et à ajouter de l'information au cryptogramme afin de le rendre plus robuste aux perturbations engendrées par le canal de transmission. L'encodage est composé de trois opérations distinctes :

- Le mélange du cryptogramme,
- L'ajout d'un code de redondance cyclique au cryptogramme,
- L'encodage convolutif du cryptogramme

#### Le cryptogramme et les symboles

Comme étudié précédemment le cryptogramme générer est constitué de 20 octets. Introduisons maintenant la notion de symbole. Un symbole est un quartet, mot de quatre bits. Le cryptogramme est donc constitué de 40 symboles. Chaque symbole appartient donc à

l'ensemble de valeurs hexadécimales [0-F], et la représentation du message peut être la représentation hexadécimale. Ces symboles vont être transmis un à un par l'émetteur au destinataire afin que ce dernier puisse reconstituer le message dans son intégralité.

### Le mélangeur

Comme vu précédemment, la séquence à encoder comporte un numéro de série fixe suivi de deux champs variables. Le but du mélangeur est d'éviter qu'une partie de la séquence soit stable d'une émission à l'autre, et donc que l'on retrouve les mêmes symboles aux mêmes emplacements dans la séquence. De plus si l'on imagine un canal de transmission qui détruit ou déforme systématiquement certains symboles, cet outil permet de disperser dans le temps les séquences difficilement décodables.

### L'ajout du CRC16 au message

Les informations relatées dans ce paragraphe sont tirées d'un document intitulé A Painless Guide To CRC Error Detection Algorithms. Ce document explique en détail l'implémentation des différents Code de Redondance Cyclique (CRC).

Le but des techniques de détection d'erreurs est de permettre au destinataire d'un message transmis à travers un canal bruité de déterminer si le message a été corrompu. Pour ce faire, l'émetteur construit un code de contrôle, appelé somme de contrôle (checksum) par abus de langage, qui est fonction du message et le rajoute à la fin du message. À la réception, il suffit d'effectuer la même opération sur le message reçu, avec la même fonction et par comparaison des deux codes de contrôle on peut tester la validité du message. L'exemple qui suit est une illustration du fonctionnement d'un code de contrôle très simple. Il s'agit en fait d'additionner la valeur de chaque octet.

Message	6 23 4
Message avec code de contrôle	6 23 4 33
Message reçu	6 27 4 33

À la réception on s'aperçoit aisément qu'il y a une erreur de transmission. Dès lors on peut redemander l'envoi des données ou bien ignorer le message en fonction de l'application. L'exemple présenté ci-dessus n'est pas utilisé en télécommunication, domaine dans lequel on lui préfère des codes de contrôle plus complexes permettant de détecter des erreurs mais aussi d'en corriger certaines.

L'idée de base des algorithmes CRC est de traiter le message comme un grand nombre binaire, de le diviser par un second nombre binaire constant (le polynôme), et de considérer le reste de la division comme le code de contrôle à ajouter à la fin du message. Les différents algorithmes diffèrent par la valeur du polynôme utilisé, la taille du code de contrôle calculé et la valeur initiale du registre de calcul.

### Le codage convolutif

En plus du calcul et de l'ajout du CRC à la séquence, un codage convolutif est appliqué à cette séquence afin de la renforcer et de compléter le code de contrôle.

Un codeur suivant une loi de codage convolutif associe N bits « codés » à K bits d'information. Chaque bloc de N éléments binaires transmis dépend non seulement du bloc de

K éléments présents à son entrée mais aussi des m blocs précédents. Le codeur est constitué de m registres à décalage de K éléments binaires. Une logique combinatoire constituée de N générateurs linéaires de fonctions algébriques génère les blocs de N éléments binaires fournis par le codeur.

### La modulation acoustique

La modulation acoustique des symboles est l'ultime étape de la chaîne de traitement du signal. Elle consiste à traduire un symbole par un son au travers d'un buzzer. Cette opération permet d'adapter le message électronique au canal de transmission utilisé qui est celui de la voix téléphonique. Il a donc fallu prendre en considération la bande passante de ce canal qui est [300 Hz ; 3400 Hz]. Les sonorités produites par le buzzer devront donc être des fréquences comprises dans cette bande passante.

#### Principe

Lorsque l'on excite le buzzer avec un signal, le buzzer oscille à la fréquence propre du signal et émet un son à cette fréquence. Donc pour résumer, si on arrive à générer un signal sinusoïdal pur à partir du microcontrôleur l'on peut représenter aisément un symbole par une fréquence et donc une sonorité. Malheureusement il est plutôt complexe de réaliser cette opération et l'on préfère générer un signal créneau (état bas = 0, état haut = 1) dont la fréquence est celle du symbole à émettre. En effet un signal carré peut être considéré comme une somme de sinusoïdes, dont la principale, appelée aussi fondamentale, oscille à la fréquence du signal. Enfin en choisissant judicieusement les fréquences pour chaque symbole on s'affranchit de tout risque de « débordement » d'une harmonique sur la plage d'un autre symbole. Une fois les sonorités émises, c'est au microphone du téléphone ou de l'ordinateur de transcrire les vibrations acoustiques au système de traitement qui les numérise et les transmet au destinataire.

### Organigramme de fonctionnement de la carte acoustique

L'organigramme ci-après présente les différentes étapes de l'algorithme de la carte acoustique. Les variables y sont représentées en jaune, les constantes secrètes en rouge, les algorithmes en bleu et la restitution des données en vert. Les flèches indiquent le sens de déroulement de l'algorithme général.

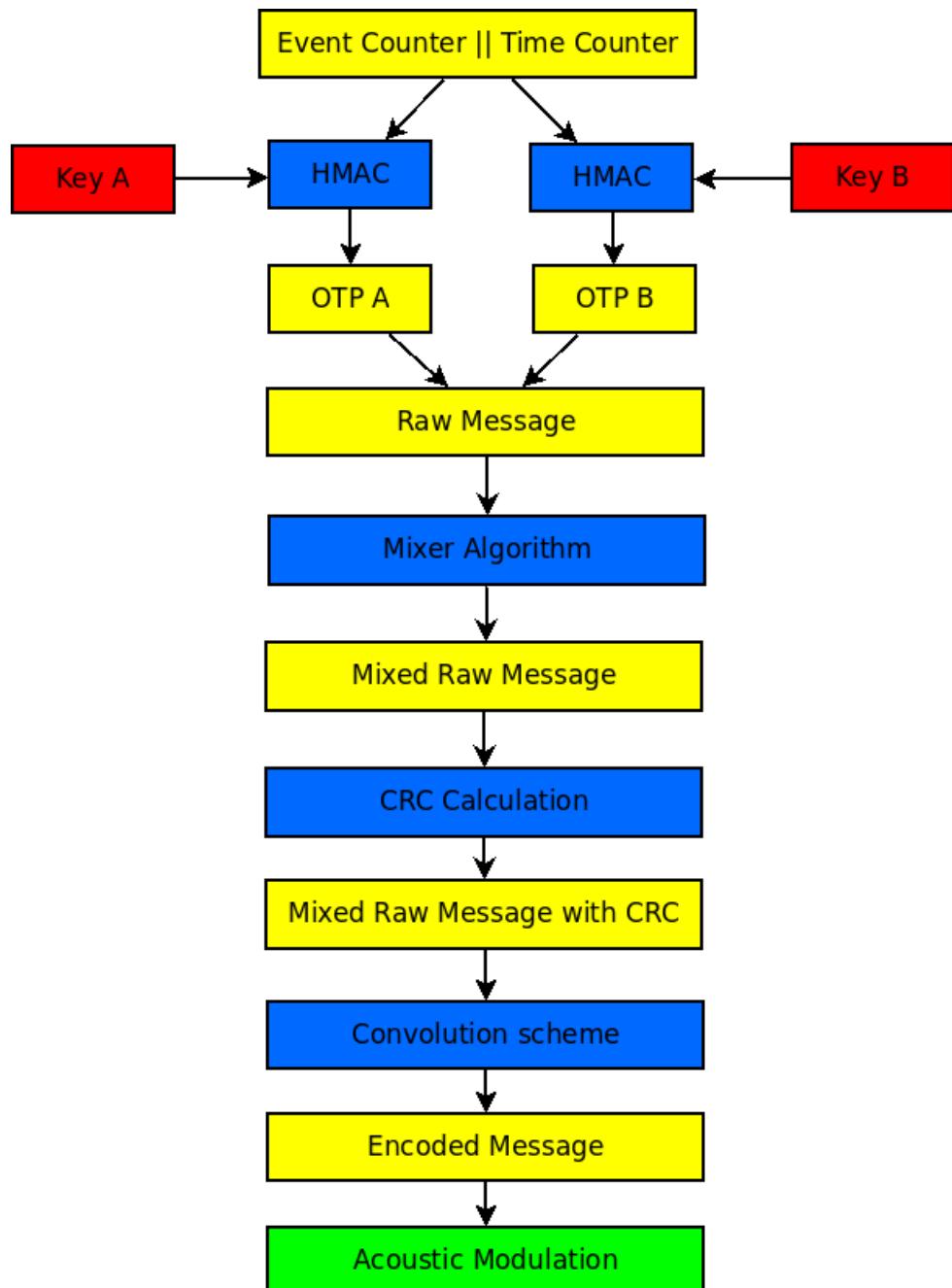


FIGURE 4.5 – Fonctionnement de la carte acoustique

#### 4.1.5 Évolution de carte acoustique

Il y a trois versions de carte acoustique. Les cartes de version 4G (V4G) sont déjà en fabrication, la version 0 (V0) est en cours de développement, et la version 1 (V1) est en cours de conception.

Voici un schéma pour présenter l'évolution de carte acoustique développée par UNT :

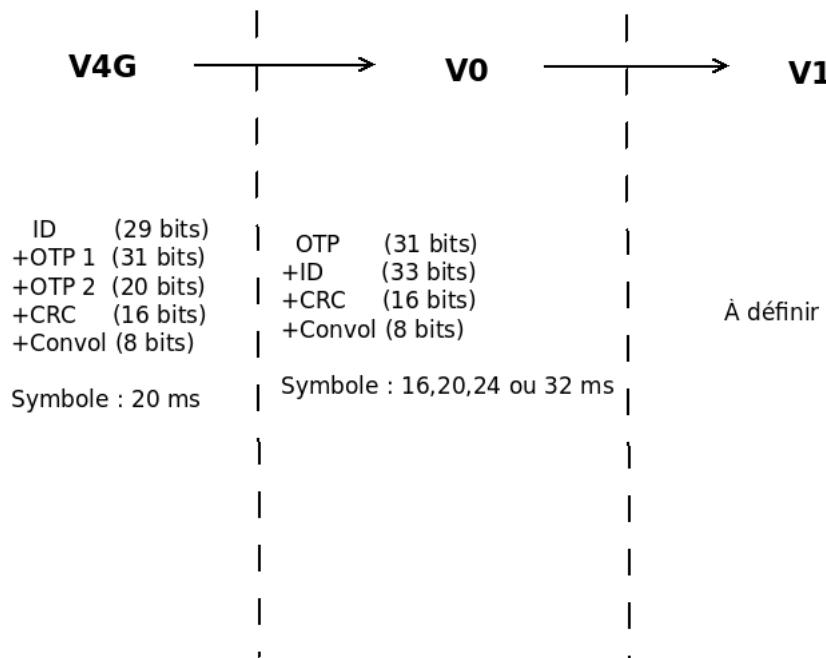


FIGURE 4.6 – Évolution de carte acoustique

#### 4.1.6 Cahier des charges

Comme indiqué dans chapitre 3 :Présentation du sujet du stage , mon travail est divisé en deux parties :

- Concevoir les tests pour la version 4G (V4G)
  - Développer d'un site de démonstration pour l'utilisation la carte acoustique

### 4.1.7 Outils

Les outils pour réaliser les tâches :

#### Offline

L'utilitaire ListenAcousticMessage\_V1.2.1.35.exe, développé par UINT, permet de voir le message acoustique produit par la carte pour les systèmes sous Windows.

#### Online

La page de test pour Internet Explorer (IE), disponible sous l'url suivante, permet de voir le message acoustique produit par la carte :

<http://solution.uint.info/AcousticMessage>

#### Transcodage

Le transcodage est l'opération de conversion du message acoustique physique, le bruit de la carte, en un message numérique informatique

#### Décodage

Le décodage est l'opération de conversion du message transcodé en une structure plus simple présentant les informations individuelles ici le numéro de série et les OTPs. Dans la version 4G de carte les informations sont simplement concaténées.

#### Authentification

Un serveur d'authentification est accessible en ligne. Une description est détaillée dans la section 4.3.5.

#### 4.1.8 Architecture globale du système de démonstration

Voici une architecture globale d'un système que l'utilisateur peut s'authentifier avec sa carte acoustique :

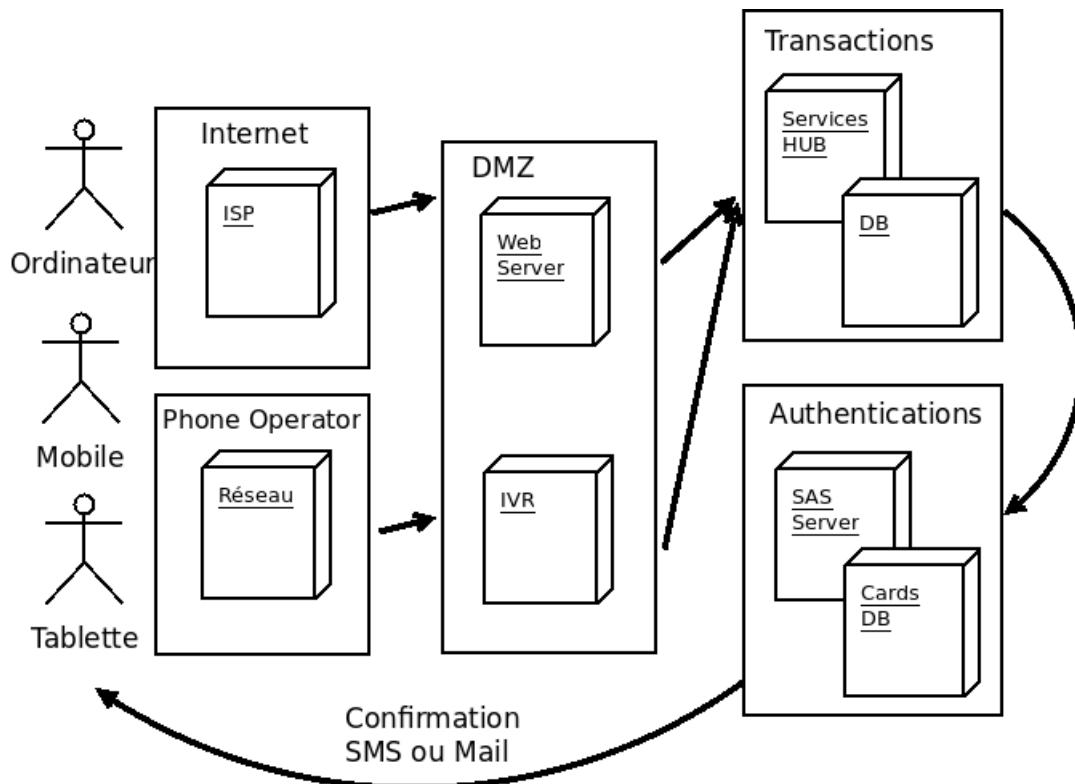


FIGURE 4.7 – Schéma d'architecture globale

Le système est divisé en 6 parties :

- ISP
- Opérateur téléphonique
- IVR
- Serveur Web
- Base de données
- Serveur d'authentification

Comme nous avons besoin d'utiliser la carte acoustique dans l'environnement téléphonique, on a besoin d'un opérateur téléphonique, et aussi, un SVI.

#### 4.1.9 SVI (Serveur vocal interactif)

«Un serveur vocal interactif (en anglais Interactive Voice Response) est un système informatique permettant aux utilisateurs d'accéder à la base de données d'une société et d'émettre diverses demandes de service, au moyen d'un téléphone fixe, mobile ou logiciel. Les serveurs vocaux interactifs entrent plus généralement dans la catégorie des systèmes de dialogue.

«La nouvelle génération de serveurs vocaux interactifs permet de traiter et de publier tous types de médias (sons, images, vidéos) et de données (base de données, fichiers textes, xml, pages web). Le VoiceXML, langage reconnu par le W3C, standardise les développements et redonne une forte impulsion à ces systèmes.»

– Wikipédia

#### Paiement par SVI

Le paiement par le SVI permet le déroulement de la cinématique de paiement classique, mais sur le canal vocal. Avec autant de garanties de sécurité pour le commerçant. Tous les paiements à distance devant respecter la norme PCI/DSS, l'interface vocale permet donc de proposer un paiement sécurisé sur ce canal.

Les principaux objectifs de l'application pour le commerçant :

- Réduire les coûts de traitement des paiements
- Sécuriser les paiements
- Proposer un nouveau canal de paiement et élargir la clientèle

Avec deux cas d'utilisation possibles :<sup>1</sup>

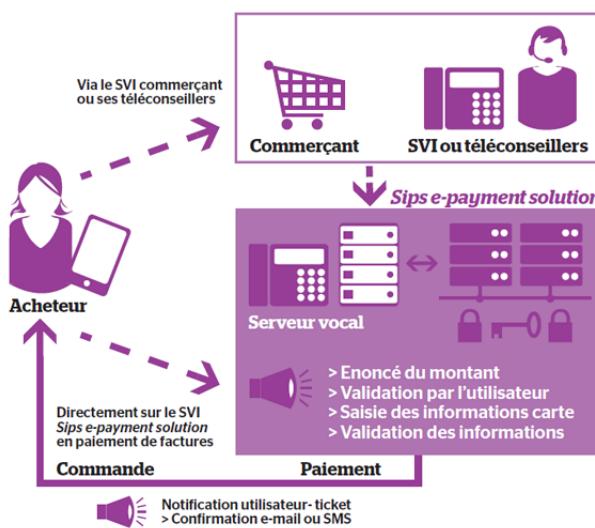


FIGURE 4.8 – cas d'utilisation de SVI

1. <http://www.sips-atos.com/fr/63/L-offre-en-detail/Multicanal/Serveur-vocal-interactif.html>

### Le SVI de paiement de factures

La solution de paiement de factures via le SVI permet à un commerçant d'émettre des factures qui seront payables, entre autres, via un téléphone sur un SVI sécurisé. Ce qui peut représenter un canal complémentaire de paiement pour un commerçant, et éviter le traitement de chèques par exemple.

Cette offre permet à des fournisseurs de services d'offrir à leurs clients finaux un nouveau moyen de paiement à distance de leurs factures grâce à un SVI de paiement sécurisé. L'interconnexion avec les fournisseurs de services permet d'identifier la facture à régler et le client final est invité à effectuer le paiement de celle-ci en saisissant, en parfaite autonomie, les informations de sa carte de paiement.

### Le routage par le centre d'appels

Le SVI permet à un téléconseiller marchand de transférer son client vers le SVI au moment de la finalisation de la transaction en cours. Le client, transféré sur ce SVI, est informé de la transaction pour laquelle le paiement va être réalisé et est ensuite invité à finaliser cette transaction en saisissant les informations de sa carte de paiement. La saisie de ces informations est réalisée par le possesseur de la carte lui-même, elles ne sont donc pas divulguées à une tierce personne.

Et ainsi :

- Gagner du temps d'occupation des téléopérateurs et donc de réduire les coûts de traitement des appels
- Sécuriser le processus et éviter aux téléopérateurs d'avoir connaissance des informations carte du client
- Proposer de nouveaux services qui feront l'objet d'un paiement via ce canal

Le paiement via le SVI permet donc d'élargir le champ d'action commercial, de proposer du paiement en toute sérénité, et surtout de diminuer les coûts de traitement des appels ou d'encaissement.

### SVI d'UINT

Pour l'utilisation du système SVI d'UINT, nous avons conçu trois modes d'utilisations à choisir par les utilisateurs :

#### Mode 1 : Utilisation classique

L'utilisateur utilise sa carte acoustique et le code PIN avec son téléphone, le statut est visualisé sur la page Web.

## CHAPITRE 4. LE TRAVAIL EFFECTUÉ

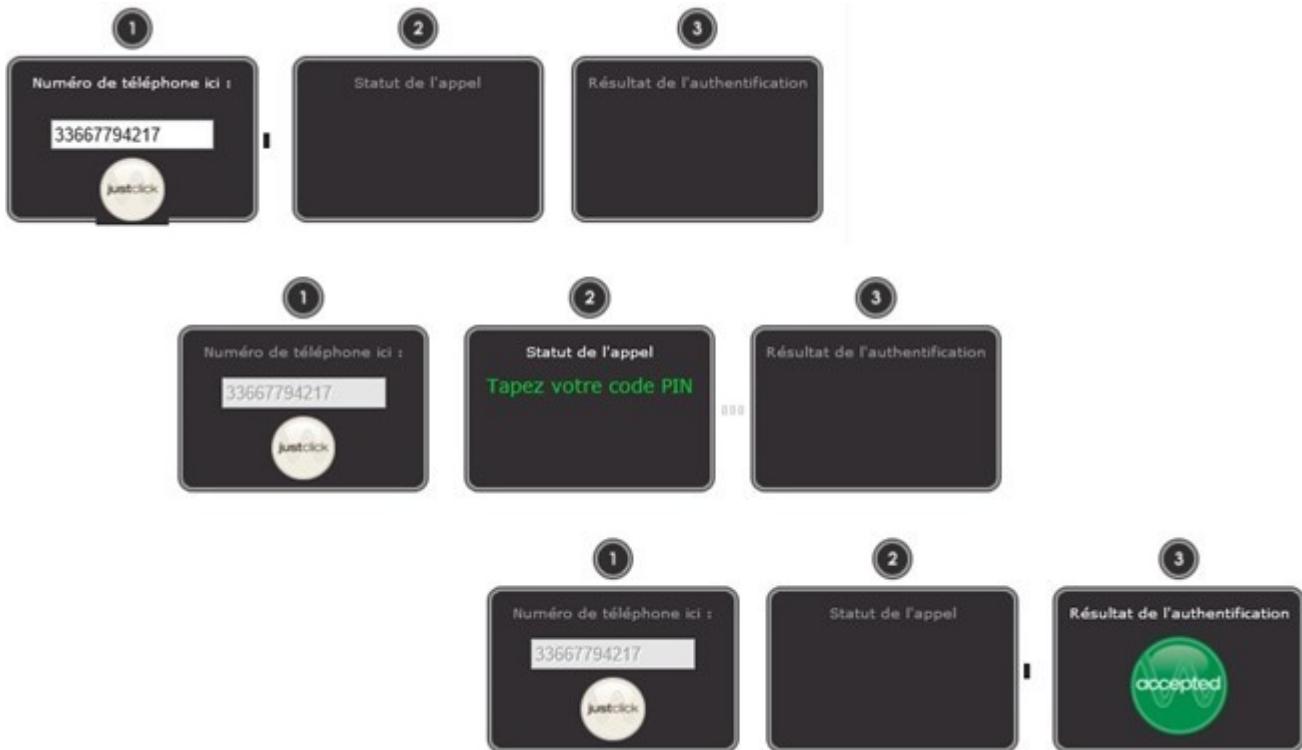


FIGURE 4.9 – Mode 1 de cas d'utilisation de SVI

### Mode 2 : Utilisation classique + Code dynamique

Le deuxième mode est similaire au premier, mais il ajoute une étape de vérification par un mot de passe dynamique envoyé par SMS à l'utilisateur.



FIGURE 4.10 – Mode 2 de cas d'utilisation de SVI

### Mode 3 : Code dynamique

Le troisième mode est destiné aux ceux qui ne peuvent pas utiliser la carte acoustique, l'authentification est réalisée par un code dynamique seulement, qui est envoyé par SMS à l'utilisateur.



## Identification

Pour vous protéger contre l'utilisation frauduleuse de votre carte bancaire, nous vous demandons de vous identifier en saisissant le code que vous avez reçu sur votre téléphone portable.

Marchand : XL

Montant : 440,00 EUR

Date : 05/30/13 08:20:03

N° de carte : 1000000000000000

Mot de passe reçu par SMS :

Cette identification est obligatoire pour conclure votre transaction. Si vous refusez de vous identifier, votre achat sera annulé.

[Ne pas m'identifier et annuler mon achat](#)

Copyright WEGA 2011

FIGURE 4.11 – Mode 3 de cas d'utilisation de SVI

Un schéma figurant la procédure d'utilisation du SVI et son principe est disponible en Annexe A.

## 4.2 Plate-forme de tests

Pour évaluer la performance de carte acoustique Version 4G, j'ai conçu une procédure de test qui est divisé en trois phases :

**Phase 1 :** Plan du test

**Phase 2 :** Démarrage du test

**Phase 3 :** Analyse des résultats

### 4.2.1 Phase 1 : Plan du test

#### TEST 1 : Fiabilité de l'encryptage

Objectifs du test : Valider les éléments constituants d'une trame acoustique et le taux de récupération.

#### TEST 2 : Fiabilité émission sonore

Objectifs du test : Observer la génération de signaux harmoniques lors de l'émission de la trame acoustique et vérifier que ceux-ci sont identiques avec les signaux harmoniques générés par la trame de référence.

#### TEST 3 : Consommation

Objectifs du test : S'assurer que la consommation par le prototype est conforme à la consommation attendue.

#### TEST 4 : Durée de vie

Objectifs du test : Obtenir, dans le plus mauvais des cas (utilisation continue, sans endormissement), le nombre d'utilisations possibles pour une pile SoliCore 10mAh.

#### TEST 5 : Récupération via IPad

Objectifs du test : Observer les taux de récupération des trames sur un équipement de type IPad.

#### TEST 6 : Récupération via iPhone

Objectifs du test : Observer les taux de récupération des trames sur un équipement de type iPhone.

#### TEST 7 : Récupération via Windows

Objectifs du test : Observer les taux de récupération des trames sur un équipement de type ordinateur portable.

Pour certain test, il y a des facteurs à considérer (Pour obtenir le pourcentage de récupération par exemple) :

#### Distances

Pour chaque test, il y a 4 conditions de distance, marqué par C, N, B, S. qui sont respectivement les acronymes de Contact, Near, Beside, Speakerphone :

## CHAPITRE 4. LE TRAVAIL EFFECTUÉ

- **Contact** : La carte doit être utilisée collée, plaquée ou appliquée contre le combiné, téléphone portable en contact physique avec le terminal.
- **Near** : La carte doit être utilisée proche du combiné du téléphone entre trois et quatre centimètres, assez proche du microphone. Cette distance correspondant approximativement à l'épaisseur de deux doigts.
- **Beside** : La carte doit être utilisée à dix centimètres du combiné du téléphone. Cette distance correspondant approximativement à la largeur d'une main.
- **Speakerphone** : Le mode haut-parleur ou main libre doit être activé en début de communication. La carte doit être utilisée à quelques centimètres du combiné du téléphone. Cette distance peut être très variable en fonction de votre configuration. Vous pouvez indiquer des détails dans le champ Phone Brand Model.

### Importance

Le niveau d'importance de chaque test :

- **1** : Pas importante
- **2** : Importante
- **3** : Critique
- **4** : Vital pour la mesure de reconnaissance

### Périphériques

Liste de périphériques :

- Mobile iPhone4
- Mobile iPhone4s
- Mobile iPhone5
- Tablette iPad2
- Tablette iPad3
- Tablette iPad4
- PC desktop avec microphone externe
- PC laptop avec microphone interne
- PC laptop avec microphone externe
- SVI
- Casque GN Netcom 2000 Stereo USB
- Webcam Logitech Pro 9000, utilisation en mode webcam fixe
- Téléphone Microsoft 1106 Catalina, utilisation en combiné ou haut-parleur

### Environnements

Liste des environnements à tester :

- Calme,
- Bruyant à définir probablement Radio source musicale, ou Radio source Vocale,
- Bruit blanc ou Bruit Rose.

### Versions

Il pourra être considéré plusieurs versions pour les périphériques, notamment version de système d'exploitation et de périphérique iPad 3 vs. iPad 4 et Windows 7 vs. Windows 8.

### Phases

Pour le test de performance, il y a 2 phases :

**Mode Prototype** : les tests seront faits avec un montage prototype. Le prototype génère une séquence de 100 messages acoustiques dans la version à tester : 4G, version 0 ou version 1. Le prototype de ce test produit une séquence continue de 100 messages acoustiques séparé entre eux d'une durée intervalle d'une ou trois fois la durée utile du message acoustique. Pour la 4G, l'intervalle sera donc d'environ 1 ou 3 secondes, pour la V0 l'intervalle sera d'environ 880 ms ou 2,64 secondes. Une documentation de signature de la carte est disponible en Annexe B.

Il faut donc trois prototypes par version de message acoustique :

- intervalle = 1d = 1,25s
- intervalle = 3d = 3.75s
- intervalle = 1d = 1,25s avec buzzer de 20 mm avec la résonnance de 4KHz

**Mode Carte** : les tests seront effectués avec une carte physique vraie. Le testeur utilisera une seule carte pour tous ses tests. Par contre, il sera nécessaire de fournir une carte par version de message acoustique. Il y aura donc au moins trois cartes acoustiques s'il n'y a qu'une seule version pour la V1.

### Nombre de tests

*Phase Prototype* : 100 signatures \* 20 fois le test

*Phase Carte* : 10 signatures \* 4 fois le test

### Logiciel utilisé

**LAMW** : LAMW est l'acronyme du logiciel ListenAcousticMessage sous Windows proposé par UINT, il a pour objectif de décoder le message acoustique généré par le prototype ou la carte.

**LAMI** : LAMI est l'application qui est utilisée dans l'environnement IOS, avec les mêmes fonctionnalités que LAMW.

### Numérotation des tests

On utilise un tableau Excel pour lister tous les tests à faire avec leurs niveaux d'importance.

### 4.2.2 Phase 2 : Démarrage du test

#### TEST 1 : Fiabilité de l'encryptage

**Description du test** : Génération de 100 signatures acoustiques. Les trames sont enregistrées via le programme ListenAcousticMessage v.1.2.1.71. On analyse les résultats du premier fichier (sur les 10), en comparant les OTP (a et b) récupérés avec ceux générés par le programme Display HOTP v.1.02. Une fois le premier fichier validé, on réalise une comparaison 1 à 1 (avec le premier fichier comme référence) avec le programme WinMerge v.2.14.

### TEST 2 : Fiabilité émission sonore

**Description du test :** Génération d'une trame acoustique. Enregistrement de la trame sur WaveSurfer (fréquence échantillonnage 48 KHz) et comparaison avec une trame de référence (en utilisant la version V.40 Assembleur).

### TEST 3 : Consommation

**Description du test :** Analyse de la consommation lors des différentes étapes de l'émission d'une trame acoustique. On s'assure que la consommation n'est de l'ordre du 10mA que lorsque l'on calcule, émet la trame acoustique et que l'on trouve une consommation de l'ordre de 0,1 uA lorsque le microcontrôleur est en mode «sleep». On branche le multimètre en série, entre l'alimentation (3V) et la pin Vdd du microcontrôleur.

### TEST 4 : Durée de vie

**Description du test :** Exécution continue l'émission de la trame acoustique (environ toutes les 2 secondes) jusqu'à épuisement de la pile. L'endormissement du microprocesseur et son réveil suite à l'appui sur bouton ont été tronqué. Une pile SoliCore 10mAh a été montée sur le prototype à la place des piles plates usuelles.

### TEST 5 : Récupération via Ipad

**Description du test :** Génération de 100 signaturess acoustiques. On utilise l'application smarphone UINT pour enregistrer les trames. A la fin du test, on récupère directement via l'application le nombre de trames enregistrées. On ne vérifie pas la validité des OTPs, ni de l'ID.

**Le scénario de test** Vous disposez un prototype du montage, avec des programmes qui fabrique un certain nombress de signaturess pour ces mesuress.  
 Par exemple, on définit 100 signaturess émis à la fois par le prototype de montage, et on enregistre les trames récupérés, puis on note le pourcentage de récupération. On répète la même opération 20 fois.

Il a été défini quatre positions ou distances différentes d'utilisation de la carte acoustique. vous devez suivre le déroulement pour chacune des quatre positions ou distances différentes.

Vous devez suivre le déroulement en gardant toujours la même distance pour une position ou distance choisie au début d'un déroulement. Il n'est pas nécessaire de faire les séries de déroulements en chaîne, vous pouvez les faire quand cela vous convient et dans l'ordre qu'il vous convient.

### TEST 6 : Récupération via Iphone

**Description du test :** Génération de 100 signaturess acoustiques. On utilise l'application smarphone UINT pour enregistrer les trames. A la fin du test, on récupère directement via l'application le nombre de trames enregistrées. On ne vérifie pas la validité des OTPs, ni de l'ID.

### TEST 7 : Récupération via Windows

**Description du test :** Génération de 100 signatures acoustiques. On utilise l'application smarphone UNT pour enregistrer les trames. A la fin du test, on récupère directement via l'application le nombre de trames enregistrées. On ne vérifie pas la validité des OTPs, ni de l'ID.

### 4.2.3 Phase 3 : Analyse des résultats

#### TEST 1 : Fiabilité de l'encryptage

Cette série de tests a permis de découvrir la non-détection d'un dépassement de taille de l'ID. En effet, l'ID est actuellement codé sous la forme de 4 octets (soit 32 bits) en mémoire Flash, mais uniquement 29 bits sont utilisés lors de la transmission du message. Si l'ID écrit en mémoire Flash à une valeur supérieure à la valeur maximale qu'il est possible de coder sur 29 bits, cela génère des erreurs lors de la génération des OTPs.

Pour parer à ce type d'erreur, un masque a été ajouté lors de la récupération du byte de poids fort de l'ID, pour tronquer sa valeur et bien avoir uniquement un ID sur 29 bits.

#### TEST 2 : Fiabilité émission sonore

A l'observation sur WaveSurfer, les trames semblent similaires. On remarque que les fréquences et leurs harmoniques sont sensiblement identiques entre la trame de référence et celle étudiée. Néanmoins, en l'absence d'un outil adapté et de par le procédé d'acquisition et d'enregistrement des trames, il est difficile de faire une interprétation précise des résultats. Il convient donc de modérer le résultat de ce test. En effet, si rien ne semble «aberrant» lors de la comparaison des trames, on ne peut affirmer catégoriquement que les fréquences et harmoniques émises sont identiques.

#### TEST 3 : Consommation

On observe bien une chute du courant consommé par le microcontrôleur lors de son entrée dans le mode «sleep». On a vérifié que le code «disassembly» de la version C est identique à la version Assembleur pour l'entrée en mode «sleep» (set GIE, set INTE, sleep).

Les causes de cette décroissance plus lente demandent à être investiguées plus en profondeur :

- Utiliser un appareil de mesure plus précis pour s'assurer qu'en mode «sleep», le microcontrôleur à la même consommation avec la V.4G en C et la V.4G en Assembleur
- Obtenir des courbes de courant selon l'utilisation du microcontrôleur

#### Traitemenstatistique des résultats

Dès qu'on reçoit les pourcentages de Trames récupérées, on fait le traitement statistiques des résultats, par exemple :

- Moyenne du taux de recouvrement : $M$
- Variance : $V$
- Écart type des taux de recouvrement : $v$

On pourra également supposer que les valeurs soient normalement distribuées, cela nécessite de calculer

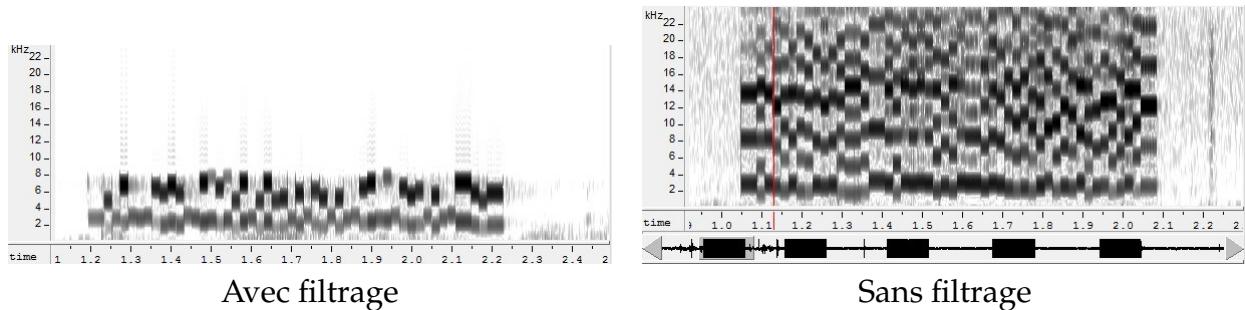
- 68% des tests auront entre  $M-v$  et  $M+v$  de trames récupérées.
- 95% des tests auront entre  $M-2*v$  et  $M+2*v$  de trames récupérées.
- 99% des tests auront entre  $M-3*v$  et  $M+3*v$  de trames récupérées.

On pourrait alors affirmer que dans le pire des cas, le pourcentage de récupération par un périphérique dans un environnement.

### Analyse de l'effet filtrage sous PC

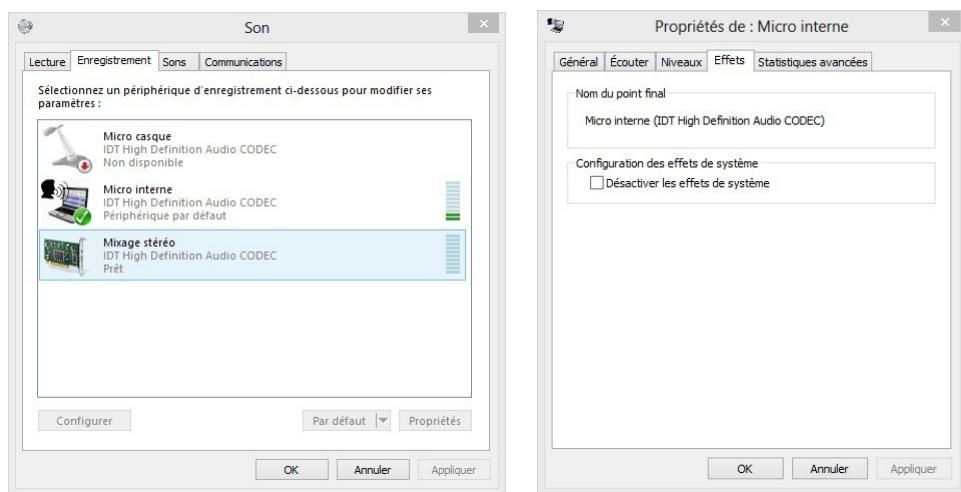
On a fait une comparaison pour voir l'effet de filtrage sous PC. Nous avons constaté que la configuration du périphérique d'enregistrement est très importante. En effet les résultats pouvaient être très variable pour une même configuration PC. On a fait donc une analyse spectrale des trames enregistrées pour chercher la raison.

D'abord, en Windows 8, on récupère les messages dans différentes configurations avec logiciel wavesurfer<sup>2</sup>, comme figuré ci-dessous :



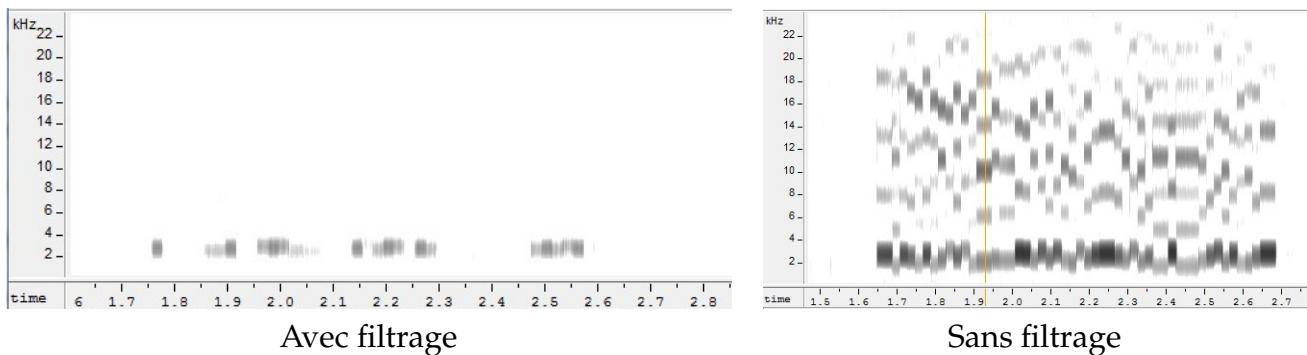
On peut voir que le filtrage coupe les fréquences qui sont supérieur à 8kHz, c'est pourquoi le résultat est trop mauvais si on utilise le filtrage du périphérique.

Plus précisément, la configuration est celui "Déactiver les effets de système" :

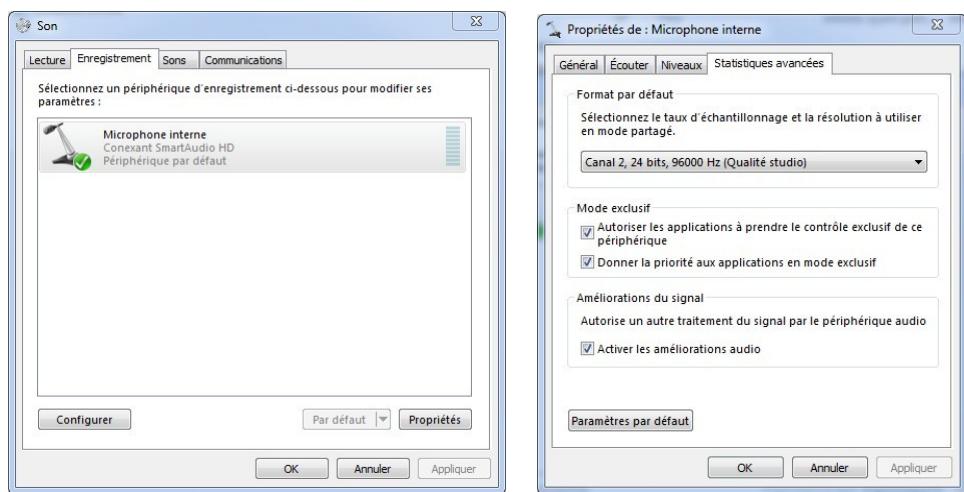


Pour Windows7, on fait le même test, le résultat est figuré ci-dessous :

2. Site officiel :<http://www.speech.kth.se/wavesurfer/>



Avec les configurations suivantes :



On peut voir que ce filtrage coupe les fréquences à partir de 4kHz environs.

### Les autres analyses

J'ai aussi fait les autres analyses suivantes qui ne sont pas détaillés dans ce rapport :

- Analyse de volume de son par sonomètre
- Différences entre les prototypes et les cartes
- Analyse de l'effet environnement
- etc...

## 4.3 Plate-forme de démonstration

Cette section décrit l'utilisation de la carte acoustique dans le contexte d'un achat en ligne. L'intégration des différents composants technologiques permettant sa réalisation est également détaillée.

### 4.3.1 Guide d'utilisation

#### Etape 1 : page d'accueil

L'utilisateur arrive sur la page d'accueil d'un site de commerce électronique. Il souhaite acheter cette télévision en promotion. Il clique sur «Add to cart»



FIGURE 4.12 – Etape 1 : page d'accueil

#### Etape 2 : identification

Dans la page suivante, les informations des achats sont visualisés, pour continuer, l'utilisateur est invité à s'identifier.

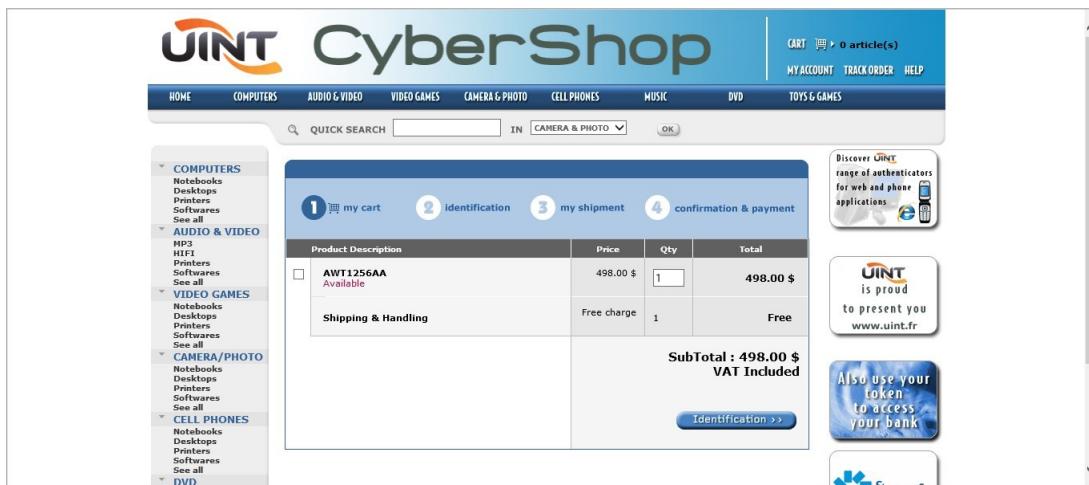


FIGURE 4.13 – Etape 2 : identification

### Etape 3 : choix du mode d'identification

Choix du mode d'identification. L'utilisateur peut choisir d'utiliser sa carte directement dans le navigateur (via l'activex, étape 4) ou via le serveur vocal.



FIGURE 4.14 – Etape 3 : choix du mode d'identification

### Etape 4 : activX

En arrivant sur la page d'identification, l'utilisateur s'il arrive pour la première fois sur cette page doit installer un ActiveX. Cet ActiveX, une fois installé, invite l'utilisateur à placer sa carte Wega près du microphone de son ordinateur et à appuyer sur le bouton de sa carte.



FIGURE 4.15 – Etape 4 : activX

### Etape 5 : livraison

Une fois la carte décodée, le serveur web dialogue avec le serveur d'authentification pour vérifier la validité de la carte. Si la trame acoustique est valide, le serveur d'authentification va alors renvoyer les informations de l'utilisateur qui vont s'afficher dans le navigateur : Nom, prénom, adresse,...

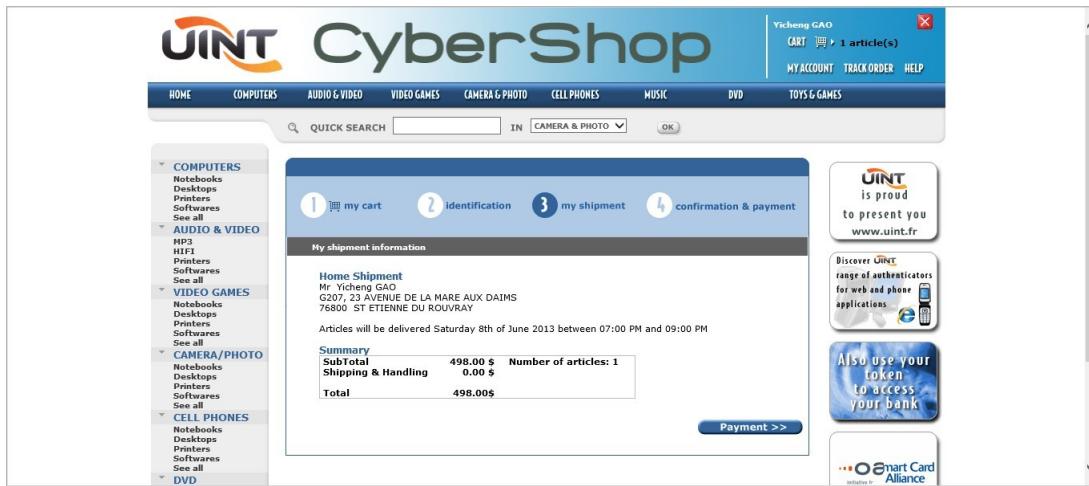


FIGURE 4.16 – Etape 5 : livraison

### Etape 6 : choix du type de paiement

La prochaine étape est celle du paiement. L'utilisateur est invité à choisir le type de paiement.



FIGURE 4.17 – Etape 6 : choix du type de paiement

## CHAPITRE 4. LE TRAVAIL EFFECTUÉ

### Etape 7 : activeX paiement

Si l'utilisateur choisi de payer via l'active X, la procédure est identique qu'à l'étape 3 mais il lui sera demandé un code PIN (voir étape 8) pour s'assurer qu'il est bien le porteur de la carte.



FIGURE 4.18 – Etape 7 : activeX paiement

### Etape 8 : demande du code pin

Pour s'assurer que le porteur de la carte est bien celui qu'il prétend être, il lui est demandé un code PIN qu'il doit saisir à la souris ou au clavier. La signature acoustique ainsi que le code pin sont envoyés de manière sécurisée au serveur d'authentification. Si les 2 informations sont correctes, l'utilisateur est alors redirigé vers la page lui confirmant son achat (étape 10)



FIGURE 4.19 – Etape 8 : demande du code pin

### Etape 9 : authentification par le serveur vocal

Dans le cas où lors de la demande du type de paiement, l'utilisateur choisi l'option «serveur vocal», une fenêtre s'ouvre lui demandant d'appeler un numéro de téléphone pour se faire rappeler ou s'identifier directement. Un numéro de session s'affiche dans la pop-up, il devra être retapé à l'aide du clavier de son téléphone. L'utilisateur devra ensuite utiliser sa carte contre le combiné de son téléphone, puis saisir son code PIN. Les informations sont ensuite vérifiées par le serveur d'authentification. Si celles-ci sont correctes, l'utilisateur est automatiquement redirigé vers la page confirmant son achat (étape 10).



FIGURE 4.20 – Etape 9 : authentification par le serveur vocal

### Etape 10 : finalisation de l'achat

Cette dernière étape est la confirmation de l'achat. Un mail ainsi qu'un SMS sont envoyés à l'utilisateur lui indiquant les informations de son achat.



FIGURE 4.21 – Etape 10 : finalisation de l'achat

### 4.3.2 Principe de fonctionnement

Cette démo d'un magasin de vente en ligne, repose sur 4 acteurs :

- L'utilisateur et sa carte
- Le serveur Web
- Le serveur d'authentification
- Le serveur vocal

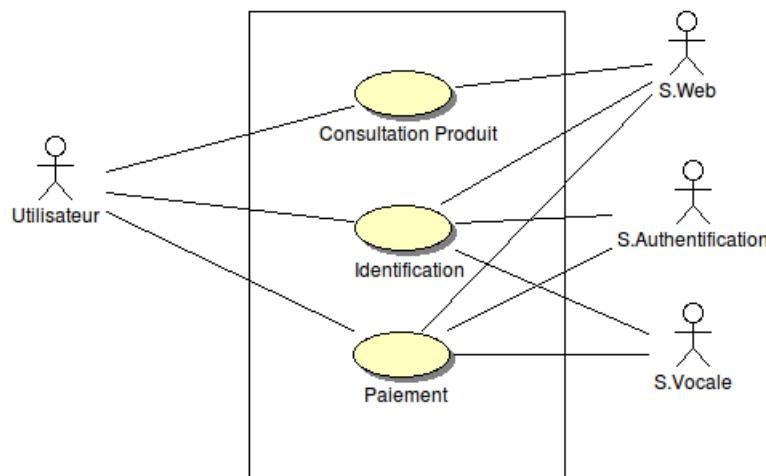


FIGURE 4.22 – Diagramme des cas d'utilisation

Voici un diagramme de séquence décrivant la procédure en utilisant le serveur vocale :

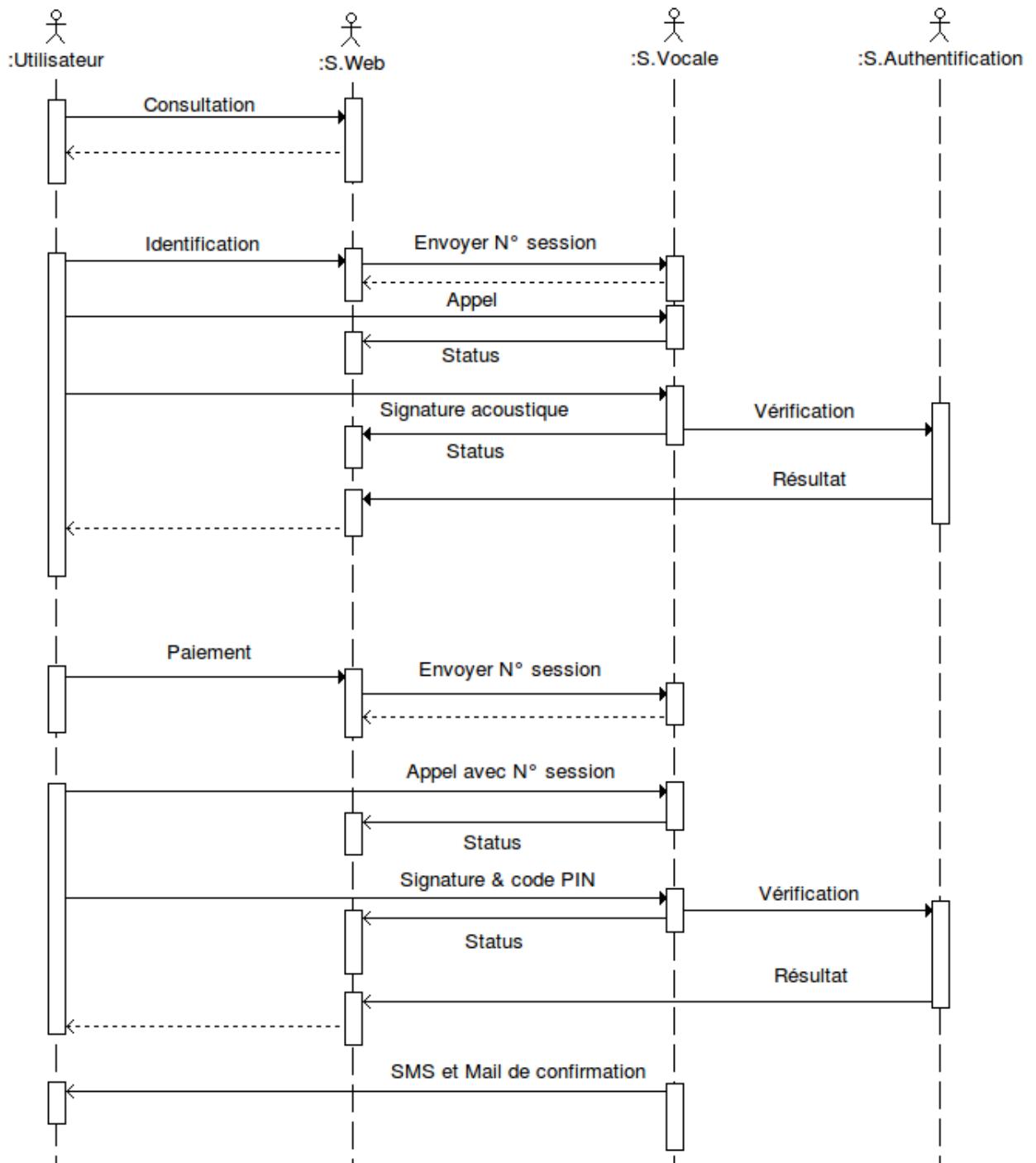


FIGURE 4.23 – Diagramme de séquence

### 4.3.3 Fonctionnement ActiveX

#### Présentation de l'ActiveX

Dimension : 237px × 96 px

Couleur : le fond est blanc et ne peut être changé

Textes : les textes sont modifiables directement dans la source de la page



FIGURE 4.24 – L'affichage de l'ActiveX

#### Initialisation de l'ActiveX

L'ActiveX fonctionne dans 2 modes (tag nC\_vMode) :

**HTTP** : l'ActiveX transcode la signature acoustique reçue et forge un fichier xml codé contenant des informations relatives à la capture acoustique ainsi que son environnement

**JAVASCRIPT** : l'ActiveX transcode la signature et la met à disposition d'une fonction javascript. Seul le message acoustique est transmis.

Suivant le contexte de l'intégration, on s'orientera vers l'un ou l'autre des 2 modes.

Dans le mode HTTP, l'ActiveX récupère le message acoustique émis par la carte, le formatte dans un fichier xml et l'envoie en POST à l'url indiquée par la valeur de l'input «nC\_vURL».

Dans le mode JAVASCRIPT, à l'issu du transcodage, la signature acoustique est transmise à la fonction Javascript «nC\_Authenticate».

L'avantage du mode JAVASCRIPT est de permettre facilement la manipulation du numéro de série pour faire des traitements avant l'envoi au serveur d'authentification.

La présence de tous ces tags HTML dans le code d'une page permet l'affichage de l'ActiveX.

L'utilisateur doit cliquer dans l'ActiveX pour initialiser la capture acoustique.

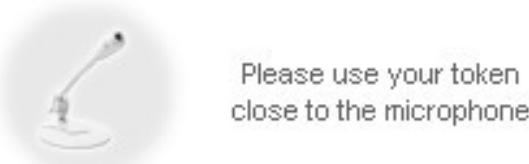


FIGURE 4.25 – L'affichage si activée

Une fois la capture réalisée, l'ActiveX envoi les informations à la page spécifiée dans le tag HTML «nC\_vURL»

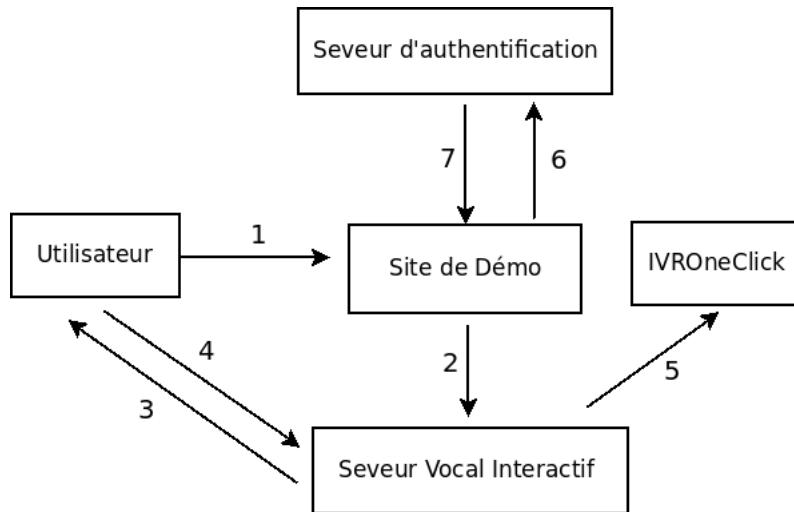
### Envoi des informations récupérées par l'activeX au serveur d'authentification

Le traitement des fichiers XML et l'envoi d'une requête WEB peuvent être réalisés par n'importe quel framework.

Le serveur PHP va récupérer les informations envoyées par l'ActiveX et les soumettre au serveur d'authentification via les WebServices.

#### 4.3.4 Fonctionnement serveur vocal

##### Scénario



1. Après l'authentification. Le numéro de téléphone d'utilisateur est enregistré en base de données
2. Le serveur Web envoie une requête au serveur vocal interactif avec comme paramètres (numéro de session + numéro de téléphone + demande de code pin)
3. Le serveur vocal interactif rappelle l'utilisateur sur le numéro de téléphone renseigné
4. L'utilisateur utilise sa carte et son code pin (L'utilisateur peut aussi être demandé un code envoyé par SMS selon le mode de carte WEGA)
5. Le serveur vocal interactif envoie ces informations au serveur web. Le serveur web lui renvoie une réponse indiquant si les informations en base de données ont été mises à jour
6. Le serveur web réalise l'authentification avec les informations fournies et indique à l'utilisateur le résultat de l'authentification

##### Principe

Le dialogue entre le SVI et le serveur web se fait à l'aide de 2 pages Web. Ces 2 pages Web doivent donc être accessibles de l'extérieur (via un VPN par exemple) ou alors en local si les 2 serveurs sont sur le même réseau.

- Une première page permet au SVI de savoir si une session est valide ou pas et s'il doit demander un code Pin à l'utilisateur
- La deuxième page permet au SVI d'envoyer au serveur web la signature acoustique de la carte et le code pin

##### Numéro de session

Lorsque l'utilisateur désire s'identifier via le serveur vocal, le serveur web doit créer un numéro de session de 6 chiffres, qu'il va mettre en base de données. S'il s'agit d'une authentification, le serveur web doit également indiquer dans la base de données qu'un code pin

sera demandé.

### Exemple de présentation



### Exemple de la structure de la Base de Données

Nom du champ	Type
Session	varchar
DtStampInit	varchar
Status	int
RAW	varchar
PINRequired	int
PINCode	varchar
DtStampSend	varchar
Demo_Name	varchar

### GET\_Session

Ce fichier est appelé par le SVI pour savoir si le numéro de session saisie par l'utilisateur sur son téléphone est valide ou pas. Un fichier XML est généré en retour à destination du SVI. Le serveur Web doit chercher dans sa base de données si le numéro de session reçu est valide ou pas.

#### Input :Session

Le SVI effectue via un POST à l'URL `http://<URL serveur web>/GET_Session.php` avec comme paramètre «Session». Cette session contient les chiffres saisis par l'utilisateur sur le SVI.

#### Output :

Si une session a été trouvée dans la base de données, le fichier XML est alors retourné par le serveur web.

L'attribut <ExitCode> est à 0 si la session a été trouvée, sinon il est à 1

L'attribut <ExitMessage> est la description du code erreur

L'attribut <PinRequired> est à 0 si le code Pin n'est pas requis, sinon il est à 1

### POST\_RAW

Ce fichier permet au SVI de poster la signature acoustique de la carte ainsi que du code pin. Un fichier XML est généré pour indiquer au SVI si l'opération s'est bien déroulée.

Le serveur web reçoit plusieurs informations provenant du SVI via un POST à une URL précise du type `http://<URL serveur web>/POST_RAW.php`, la session, le RAW (signature acoustique) et le code pin.

Le serveur doit mettre à jour sa base de données avec ces informations et retourner au SVI si l'opération s'est correctement déroulée.

#### **Input :**

- Session
- RAW
- PINCODE

#### **Output :** Fichier XML

```

1  <?xml version="1.0" encoding="ASCII" ?>;
2  <result>
3  <ExitCode>0</ExitCode>
4  <ExitMessage>Session is OK</ExitMessage>
5  </result>
```

### Les paramètres

Pour communiquer avec le serveur SVI, quelques paramètres sont nécessaires d'envoyer par POST ou GET selon le besoin. Il faut au moins le paramètre `PhoneNumberToCall` pour émettre un appel (et `SessionId` pour que le backoffice s'y retrouve après).

Les paramètres utilisés pour envoyer au SVI :

**PhoneNumberToCall** : est le numéro qui doit être appelé. Ce numéro doit être préférablement au format international sans le prefix

**DemoID** : permet d'identifier le serveur émetteur de la demande

**InternalPINCardRange1**, **InternalPINCardRange2** : sont des plages de numéros de série devant être gérée de façon particulière par le SVI

**SessionID** : est l'identifiant de session pour identifier de façon unique les demandes d'appels

**AskPIN** : valeur 0 ou 1 par défaut 0 indique au SVI s'il doit demander un code PIN après un détection carte

## CHAPITRE 4. LE TRAVAIL EFFECTUÉ

Dans la vitrine présentée dans le guide le SVI renvoi les résultat vers un serveur Web vitrine sous la forme d'un POST où sont les données précédentes ajoutées avec les information de carte PIN et les codes de statut de l'appel.

Il y a plusieurs status de l'appel :

Status Code	CONSTANT	Description
0	INIT	Initialisation
1	RAW_RECEIVED	Signature acoustique transmise
2	CALL_NOT_ACCESSIBLE	Numéro inaccessible
4	INVALID_PHONE_NUMBER	Numéro invalide
8	CALL_OCCUPIED	Ligne occupée
16	CALL_NO_ANSWERED	Pas de réponse
32	CALL_REQUESTED	La demande de callback est reçue et prise en compte
33	CALL_ANSWERED	L'appel est décroché
34	IVR_CLOSE_CALL	L'appel est raccroché
64	IVR_ASK_SEQ	L'IVR attend la séquence de la carte
65	IVR_CARD_NOT_RECOGNIZED	Carte non reconnue
66	IVR_ASK_PIN	Attente saisie du code PIN
128	IVR_CHECK_RESULT	L'IVR envoie les informations de la séquence et attend la réponse du serveur
256	INTERNAL_ERROR	Erreur interne

### Authentification

Le serveur web doit donc vérifier si pour une session donnée, les informations de la capture acoustique et du code Pin sont présentes dans la base de données.

Le serveur web peut maintenant extraire ces informations de la base de données et réaliser une authentification ayant à sa disposition les informations de la carte et du code pin en utilisant les Web Services fournit par UINT.

### 4.3.5 SAS Web Services

#### Présentation générale

Dans une première étape de tests et de validations UINT met à disposition un accès au SAS (Strong Authentication Server) pour valider des identités porteuses de cartes.

SAS fournit un certain nombre de services disponibles par Internet ou Intranet qui sera permettre aux clients de :

- Vérifiez la disponibilité des serveurs
- Récupérer des informations à partir de SAS
- S'authentifier à l'aide d'un Token
- Lister les informations d'identification des utilisateurs
- Ajouter/Modifier les informations d'identification de l'utilisateur
- Supprimer les informations d'identification d'un utilisateur
- Récupérer les informations d'identification d'un utilisateur

Ces services Web peuvent être accessibles à partir de n'importe quel endroit à travers le protocole HTTP ou HTTPS.

#### Modèle opération simple

Les Webservices fournissent le modèle question-réponse d'une action ou demande d'information. Les échanges entre SAS et demandeur de Webservices génère un identifiant de session qui peut être jeté s'il n'est pas utilisé.

#### Modèle Session

Afin de manipuler des transactions complexes entre les Webservices et demandeur de services Web, identification de session doit être géré sur les deux côtés offrent des fonctionnalités transactionnelles en particulier des opérations de gestion.

#### Formats

La requête et les réponses peuvent être du texte, HTML ou XML.

#### Demandes

Une requête de Webservices peut être envoyée à SAS en utilisant la syntaxe de texte, de données ou en forme de chiffrement.

#### Réponses

Le SAS répond aux requêtes de Webservices avec le format requis définis dans la requête.

#### Sessions

Les requêtes et les réponses sont effectuées en utilisant la gestion des sessions SAS et fournissent caractéristiques transactionnels.

#### Syntaxe

Une requête WebServices doit suivre la syntaxe suivante :

HTTP [S] ://SASAddress [:Port] /WEBSERVICES?

OP=[OPERATION] [&PARAMETERVALUE=[Parameter Data]]

Les paramètres optionnels :

```
&INFORMAT=[Input Format]  
&OUTFORMAT=[Output Format]  
&SKEY=[Session Key]  
&DATA=[XMLData]
```

### SASAddress

C'est l'adresse SAS au format numérique comme 192.168.2.204 ou au format canonique comme Authentication.UnipaysINTelligence.com

### Port

Indique le port TCP que SAS écoute. La valeur par défaut, lorsqu'il n'est pas défini, est de 80 en utilisant le préfixe http et le port 443 en utilisant https.

### /WEBSERVICES ?OP=

Indique quelle requêtes de WebServices sera traitée par le SAS.

### OPERATION

Le type d'opération que SAS à effectuer.

Pour simplifier avec les Web Services, il y a trois commandes à considérer :

- *ISALIVE* pour vérifier que le serveur est online, pourrait être ignorée mais signifie de gérer un timeout sur la commande suivante.
- *AUTHTOKEN* pour tester le message d'authentification
- *LOGOUT* pour fermer la session avec le serveur.

Les codes retour à considérer sont :

- Pas de communication avec le serveur suite à la command *ISALIVE*
- Echec authentification suite à la commande *AUTHTOKEN*
- Réussite authentification suite à la commande *AUTHTOKEN*

### Exemples d'utilisation

### Exemple 1 : Exemple de service Web simple renvoyant une sortie type XML

Cet exemple permet de récupérer les informations générales SAS et le statut avec la sortie type XML :

#### REQUEST

```
http://Authentication.UnipaysINTelligence.com/WEBSERVICES?OP=
ISALIVE&OUTFORMAT=512
```

#### RESULTAT

```

1  <?xml version="1.0" encoding="ASCII"?>
2  <Data>
3  <ServerInfo>
4    <Session>
5      <SessionID>8157e499-7766-4d9c-9013-9880c8280b72</SessionID>
6    </Session>
7    <Identity>
8      <Version>3.0.278</Version>
9      <ServerName>SSPRO</ServerName>
10     <SID>AA</SID>
11     <PublicKey>0602000000a40000525341310002000001000100f5c51d9cc8
12       a78a9b7e221128a70eb7110016a8b7d4f7842c2998dc9b36f3f654c9b48aa
13       4bdb56bd406640dae89782bd7bdf25cd45da6cc162c5233605e2634a8</PublicKey>
14   </Identity>
15   <Localization>
16     <TimeZone>2</TimeZone>
17     <LocalTime>20040803195315</LocalTime>
18     <UTCTime>20040803175315</UTCTime>
19     <Country>France</Country>
20     <CountryIndex>64</CountryIndex>
21   </Localization>
22   </ServerInfo>
23   <result>
24     <ExitCode>0</ExitCode>
25     <ExitMessage/>
26   </result>
27 </Data>
```

### Exemple 2 : Exemple de service Web simple renvoyant une sortie type HTML

#### REQUEST

```
http://Authentication.UnipaysINTelligence.com/WEBSERVICES?OP=
ISALIVE&OUTFORMAT=256
```

#### RESULTAT

OK

# **Chapitre 5**

## **Conclusion**

La conclusion sera scindée en deux parties. Dans un premier temps, je présenterai ce qui a été réalisé vis à vis du cahier des charges. Dans un second temps, je tirerai un bilan personnel vis à vis de ce stage.

### **5.1 Les réalisations**

Nous avions un cahier des charges détaillé des fonctionnalités à implanter (cf 4.1.6). Le cahier des charges était divisé en deux parties et ce stage nous a permis de réaliser entièrement les deux, qui concernait la plate-forme de tests, et l'application de démonstration.

En ce moment, l'application web est entièrement fonctionnelle et est maintenant en test pour être mise en ligne. Les performances sont beaucoup plus puissantes par rapport aux précédents.

Par ailleurs, nous avons maintenu la documentation et l'avons adaptée aux changements que nous avons apportés. Cependant, nous avons manqué de temps pour la rendre plus complète.

### **5.2 Bilan personnel**

Ce stage a eu pour moi une signification particulière en comparaison avec les précédents stages que j'ai pu effectués.

A l'issue de ces 5 mois de stage je peux dire que cette expérience a été très bénéfique pour moi. Tout d'abord, sa durée de 22 semaines, deux fois plus longue que mes précédents stages, m'a permis une véritable intégration au sein d'une équipe. Pendant le stage, J'ai pu mettre en oeuvre mes compétences acquises lors de ma formation dans le département ASI autour des trois filières (Acquisition de l'information, Traitement de l'information, et Informatique) et en acquérir de nouvelles.

Ensuite, le fait que ce stage se soit déroulé dans une société du secteur privé, m'a fait me rendre compte concrètement des différences qui existent entre le secteur privé et le secteur public. De plus, le fonctionnement d'UINT en start-up m'a permis de jouer des rôles

## CHAPITRE 5. CONCLUSION

multiples en dehors du projet de stage, avec plus ou moins de responsabilité, et d'utiliser ainsi bon nombre des connaissances que j'ai pu acquérir au cours de mes études. Le fait d'avoir intégré une équipe de travail, d'avoir participé à des réunions d'avancement ou de réflexions mais aussi d'avoir dû respecter des contraintes temporelles pour certaines livraisons ont été à mes yeux très enrichissant pour mon expérience professionnelle.

Sur le plan technique, ce stage m'a permis de me rendre compte de la difficulté de reprise d'une application web lorsque peu de documentation est disponible. Construire un site web commercial s'avère être néanmoins une très bonne expérience pour comprendre les mécanismes d'une application malgré son coût énorme en temps. Je me suis également rendu compte que les technologies Web sont certes intéressantes mais assez répétitives.

Sur le plan personnel, bien que je travaille depuis quelques années assez fréquemment avec PHP, ce stage m'a permis encore une fois d'expérimenter la dynamique et le travail en équipe. Ceci est un réel plus et je ne pense pas que ce stage aurait été aussi bien réussi sans cela.

# Bibliographie

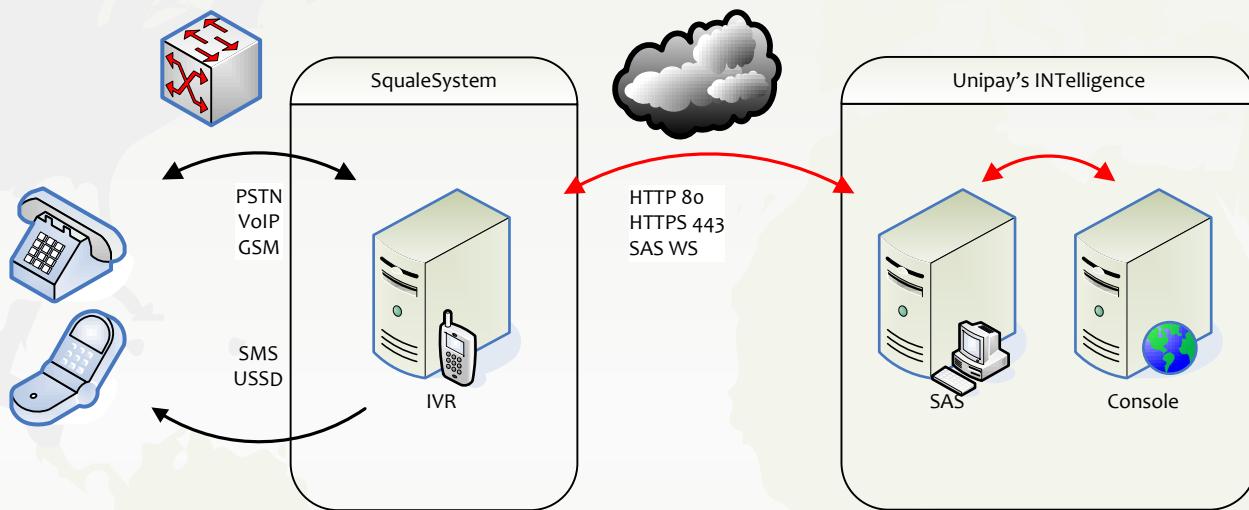
- [1] La société UINT :  
<http://www.uint.fr>
- [2] HOTP : An HMAC-Based One-Time Password Algorithm :  
<http://www.ietf.org/rfc/rfc4226.txt>
- [3] HMAC : Keyed-Hashing for Message Authentication :  
<http://www.ietf.org/rfc/rfc2104.txt>
- [4] Secure Hash Algorithm :  
<http://csrc.nist.gov/fips/fip180-1.txt>
- [5] Attacks on SHA1 :  
<http://www.openauthentication.org/pdfs/Attacks%20on%20SHA-1.pdf>
- [6] SVI :  
[http://fr.wikipedia.org/wiki/Serveur\\_vocal\\_interactif](http://fr.wikipedia.org/wiki/Serveur_vocal_interactif)
- [7] Sips Serveur Vocal :  
<http://www.sips-atos.com/fr/63/L-offre-en-detail/Multicanal/Serveur-vocal-interactif.html>

## **Annexe A**

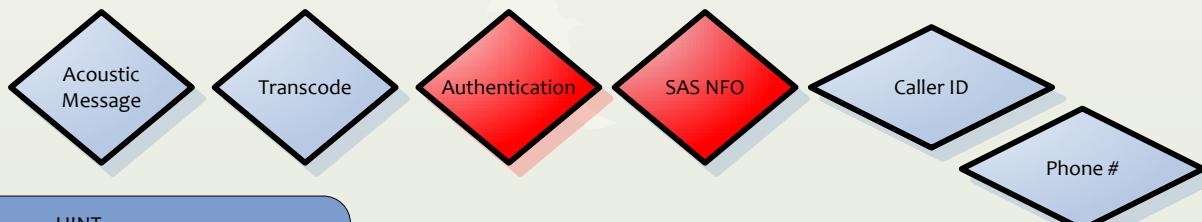
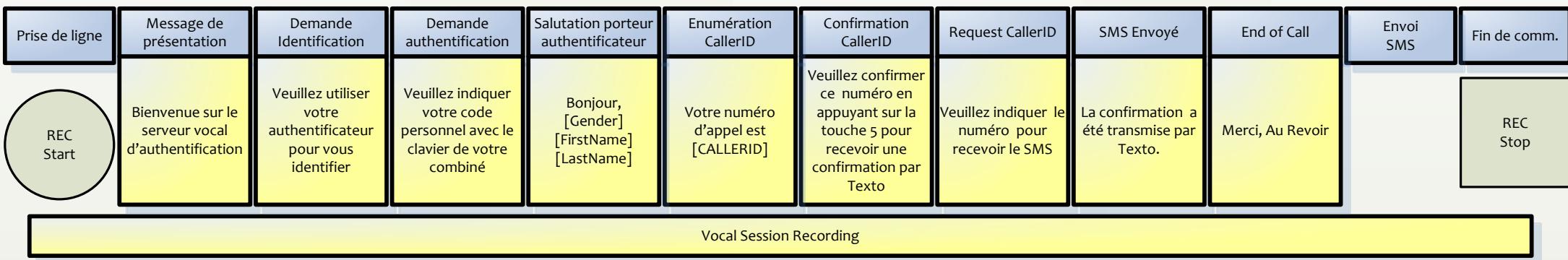
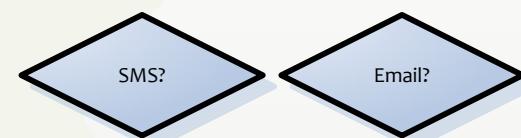
### **Procédure SVI dans l'application Web**

## IVR Test Bed

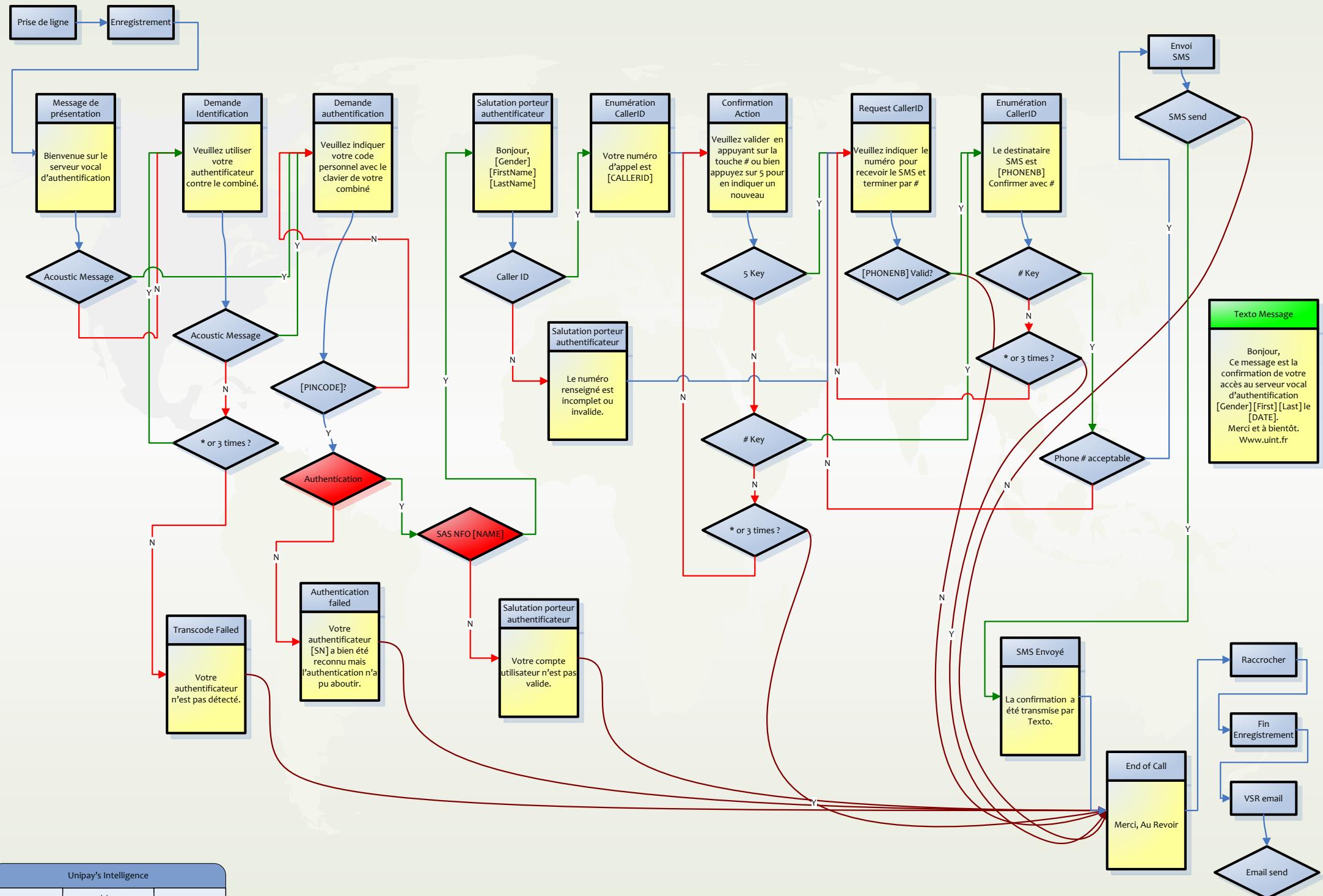
oA01 Update uint  
8924 Detailed Scenario  
8918 ConfCall Squale  
8821 Initial Draft



IVR		
TestBed		
Symbol	Count	Description
	1	SAS
	1	Telephone
	1	IVR
	1	Web server
	1	Cell phone
	1	Internet
	1	Phone Network



UINT



## Annexe B

# Documentation d'une signature acoustique

**Title :** Acoustic\_Card - Mode 16ms

**Creator :** Yicheng GAO

**Date :** 21/05/2013

### Development Tools :

- IDE : MPLAB V8.88
- Compiler : XC8 V.1.12
- OS : Windows 7 version 6.1 running on amd64
- uC : PIC16F648A

### Signature details :

- "bip" at 6.6 KHz for 50 ms, silence for 50 ms, "bip" at 3.3 KHz for 50 ms, silence for 200 ms
- 44 symbols (176 bits) : (31 bits of OPT + 33 bits of ID + 16 bits of CRC + 8 bits Convolution Constraint) \* (1 / Convolution Yield)
- Convolution Yield : 1/2
- Duration of symbols about 16 ms
- Silence for 200 ms, "bip" at 3.3 KHz for 50 ms, silence for 50 ms, "bip" at 6.6 KHz for 50 ms
- ID = 0000000001h
- Initial Counter = 0123456789ABCDEFh
- Key HOTP = 3132333435363738393031323334353637383930h

### Behaviour :

- Initialize the device and the parameters
- Infinite Loop :
  - If no Signature has been calculated yet, do a calculation
  - Else, wait for button pushed, play signature, calculate new frame

**Table of Symbols :**

Symbols (hexa)	Frequency (Hz)	Nb_period (hexa, dec)	Duration (ms)
0x00	1602,56	0x1A, 26	16,224
0x01	1706,49	0x1B, 27	15,822
0x02	1908,40	0x1F, 31	16,244
0x03	1805,05	0x1D, 29	16,066
0x04	2304,15	0x25, 37	16,058
0x05	2202,64	0x23, 35	15,890
0x06	2000,00	0x20, 32	16,000
0x07	2100,84	0x22, 34	16,184
0x08	3105,59	0x32, 50	16,100
0x09	2994,01	0x30, 48	16,032
0x0A	2793,30	0x2D, 45	16,110
0x0B	2906,98	0x2F, 47	16,168
0x0C	2403,85	0x26, 38	15,808
0x0D	2500,00	0x28, 40	16,000
0x0E	2702,70	0x2B, 43	15,910
0x0F	2604,17	0x2A, 42	16,128

**Functions implemented :**

- SHA1 functions in Assembly
- HOTP functions in Assembly / void HOTP(void) can be called in C
- Decimal Truncation function in Assembly / void DecimalTrunc(void) can be called in C
  - DecimalTrunc has been modified to follow the requirements of the new signature, namely the HOTP result is before the ID in the frame to be sent
- Generate Acoustic Frame in C, composed of :
  - Decimal Truncation
  - Mixing Frame
  - CRC16 Calculation
  - Convolution
- Play Acoustic Frame in C, composed of :
  - PIC16F648A\_RingTone
  - PIC16F648A\_RingSilence
  - SetupFreq
  - PIC16F648A\_Isr\_Hnd (Interrupt)
- Driver for EEPROM in C :
  - Init\_EEPROM\_Variables
  - Read Counter (only the writing of Counter from Flash into RAM is in Assembly - void CopyFlashCounter(void) can be called in C)
  - Increment Counter
- Driver for PIC16F648A in C :
  - PIC16F648A\_Init

## Résumé :

Le stage présenté dans ce rapport a été réalisé par Yicheng GAO dans la société UINT situé à SAINT AUBIN (91) entre le 25 mars et le 31 Août 2013. La société UINT développe et commercialise des circuits électroniques fins, souples et autonomes embarqués dans les cartes à puces, dans les domaines de la recherche et le développement de l'électronique, de la sécurité des transactions et de la fabrication des cartes, en maîtrisant tous les processus et cycles de vie des produits allant de la conception à la fabrication.

Au cours de mon stage, je suis principalement intervenu sur la maîtrise d'ouvrage d'un projet carte acoustique. En temps que maîtrise d'ouvrage, j'ai du spécifier les besoins des clients internes, établir la recette du application développée, et la conception d'une plate-forme de tests permettant d'évaluer la performance du produit. A l'issue de ces 22 semaines de stage je peux dire que cette expérience a été très bénéfique pour moi. J'ai pu mettre en oeuvre mes compétences acquises lors de ma formation dans le département ASI et en acquérir de nouvelles.

## Abstract :

The internship described in this report was conducted by Yicheng GAO in the society UINT located in SAINT AUBIN (91) between March 25th and August 31st, 2013. The society UINT develops and markets electronic equipments, flexible electronic board solutions that fit in a credit card format card and are autonomous, in the areas of research and development of electronics, security transactions and manufacturing of smart cards, mastering all the processes and life cycles of products from conception to manufacturing.

During my internship, I'm mainly occurred on the developpement of acoustic card project. During the developpement of this project, I have specified the needs of internal customers, established the recipe of developed application, and designed a test platform for evaluating the performance of the product. At the end of the 22-week course I can say that this experience has been very beneficial for me. I could implement my skills acquired during my training in the ASI department and acquire new ones.

INSA de Rouen  
Avenue de l'Université - BP 08  
76801 Saint-Etienne-du-Rouvray Cedex  
Tél : 02 32 95 97 79  
Fax : 02 32 95 97 08  
[https://asi.insa-rouen.fr](http://asi.insa-rouen.fr)



À taille humaine,  
à l'échelle du monde