

Ecole nationale Supérieure d'Informatique (ESI)

**ECOLE DOCTORALE NATIONALE EN SCIENCES ET
TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
STIC**

**Mémoire de Magister Option : Ingénierie des
Systèmes Informatiques (ISI)**

**Contrôle d'accès et authentification
fédérés à base de revendications
dans les réseaux véhiculaires.**

Réalisé par Ramzi Debab

Composition du jury :

Mr. Mouloud Koudil	Professeur, ESI	Président
Mr. Walid-Khaled Hidouci	Maître de Conférences, ESI	Examineur
Mr. Mahfoud Benchaiba	Maître de Conférences, USTHB	Examineur
Mr. Djamel Djenouri	Maître de Recherche, CERIST	Examineur
Mr. Yacine Challal	Maître de Conférences, UTC	Directeur de Mémoire

Année 2009/2010

Table des matières

Liste des figures :	VII
Liste des tables :	IX
Liste des abréviations :	X
Dédicaces :	XII
Dédicaces spéciales :	XIV
Remerciements :	XV
Résumé:.....	1
Abstract:.....	2
Introduction Générale :	3
Partie I : Etat de l'art des communications véhiculaires.	7
Chapitre 1 : Les Communications Véhiculaires :	8
Introduction :	8
1. Définition :	9
2. Motivation :	9
3. Types des VC :	10
4. Architecture :	12
5. Les VANETs :	13
6. Applications des Communications Véhiculaires :	14
6.1. Sécurité routière :	14
6.2. Confort :	15
Conclusion :	16
Chapitre 2 : La sécurité des communications véhiculaires :	17
Introduction :	17
1. Pourquoi penser à la sécurité des Communications Véhiculaires?	18
2. Activités de recherche :	18
3. Les défis de la sécurité des communications véhiculaires :	18
4. Adversaires:	19
5. Les attaques:	19
6. Mécanismes d'authentification dans les réseaux véhiculaires :	20
6.1. Solutions à base de certificats X.509 :	20
6.2. Solution à base de tickets Kerberos :	23
6.3. Solution à base des Mots de passe:.....	24
Conclusion :	26
Partie II : La technologie des Web Services.	27
Chapitre 3 : SOA & Web Services	28
Introduction :	28
1. SOA & Services:	29
1.1. Architecture logicielle contemporaine : la couche service.....	29
1.2. Le Service :	30
1.3. Définitions du SOA :	31
1.4. Modèle conceptuel du SOA :	31
2. Web Services WS-* :	32
2.1. Définitions :	33
2.2. Pile protocolaire des Web Services :	34
2.2.1. La couche transport :	35

2.2.2. La couche Messaging :	35
2.2.3. La couche Description:.....	38
2.2.4. La couche découverte :.....	39
2.2.5. La couche QoS :.....	39
2.2.6. La couche composition des services:.....	40
3. Les Web Services et les réseaux véhiculaires :.....	40
Conclusion :	41
Chapitre 4 : Le SODA (Service Oriented Devices Architecture)	42
<i>Introduction</i> :	42
1. Du SOA vers le SODA :	43
2. Le profil DPWS :	44
2.1. Définition :	44
2.2. <i>Architecture</i> :	45
2.3. Performances :	47
3. <i>DPWS et les réseaux véhiculaires</i> :	48
Conclusion :	48
Chapitre 5 : Sécurité des Web Services :	49
<i>Introduction</i> :	49
1. Niveaux de sécurité :	50
2. Pourquoi le niveau échange ?	50
3. Principes de la sécurité des applications XML :	51
3.1. <i>Signature XML (XML DSig)</i> :	52
3.2. <i>XML encryption (XML Enc)</i> :.....	52
3.3. <i>SAML (Security Assertion Markup Language)</i> :.....	52
3.4. <i>Extensible Access Control Markup Language (XACML)</i> :.....	52
3.5. <i>Extensible Rights Markup Language (XrML)</i> :.....	52
3.6. <i>XML Key Management Specification (XKMS)</i> :.....	52
4. Architecture des spécifications de sécurité des Web Services :	53
4.1. <i>Couche Sécurité de base</i> :.....	53
4.2. <i>Couche Stratégies et Relations</i> :	53
4.3. <i>Couche Interopérabilité et Autorisation</i> :.....	54
5. Sécurité des Web services et sécurité des réseaux véhiculaires :	54
Conclusion :	56
Chapitre 6 : La fédération de l'accès à base des jetons de sécurité :.....	57
<i>Introduction</i> :	57
1. Définition par la problématique :.....	58
2. L'identité digitale :.....	59
2.1. Définition :.....	59
2.2. Les lois de la fédération :	60
3. Architecture d'un méta système d'identité à base de jetons de sécurité :	60
3.1. Rôles :	60
3.2. Composants :	61
4. Profils de la fédération :	63
4.1. WS-Federation Active Requestor Profile :	63
4.2. WS-Federation Passive Requestor Profile :	63
5. La mobilité et la fédération d'identité :	64
Conclusion :	66
Partie III : Solution : Vers VPWS et VSB.....	67
Chapitre 7 Conception de l'architecture communicationnelle.....	68
<i>Introduction</i> :	68
1. Vers un Vehicular Service Bus (VSB) :	69

1.1. Challenges :	69
2. L'ESB et le SOA :	70
2.1. Définition:	70
2.2. Architecture d'un ESB :	71
3. Vers un VSB :	72
3.1. La technologie WCF :	72
3.1.1. Présentation de WCF :	72
3.1.2. Création d'un service WCF :	73
3.1.3. Architecture de WCF :	75
3.1.4. Pourquoi penser à WCF ?	75
3.1.5. Adaptation des applications LOB :	76
3.2. Architecture de VSB :	77
3.2.1. Modèle décentralisé du VSB :	77
3.2.2. Les composants du VSB :	79
3.2.3. Architecture de VSB :	80
3.2.4. Scénarios d'échanges de messages :	81
Chapitre 8 : Conception de la sécurité fédérée	83
Introduction :	83
1. Principes de la sécurité dans WCF :	84
2. Spécifications supportées :	85
3. Contrôle d'accès aux ressources avec WCF :	85
3.1. Authentification :	85
3.1.1. <i>Modes d'authentification</i> :	85
3.1.2. Types de jetons supportés :	86
3.2. Autorisation :	86
3.2.1. Autorisation orientée ressources :	86
3.2.2. Autorisation orientée rôles :	86
3.2.3. Autorisation orientée jetons :	86
4. Architecture de la sécurité fédérée :	87
4.1. Importance de la fédération :	87
4.2. Architecture du contrôle d'accès fédéré :	88
5. Vers un nouveau profil :	92
Conclusion :	94
Chapitre 9 : Analyse et développement d'une application sécurisée de gestion des intersections à base de VSB	95
Introduction :	95
1. Définitions des besoins :	96
1.1. Besoins fonctionnels :	96
1.2. Besoins techniques :	97
1.2.1. Besoins matériels :	97
1.2.2. Besoins logiciels :	98
2. Architecture de l'application (vue logicielle) :	99
2.1. Le pattern Pub/Sub :	99
2.2. Architecture :	99
3. Architecture de la fédération :	101
3.1. Scénario de la fédération :	101
3.2. Configurations :	102
3.2.1. Définition des assertions :	103
3.2.2. Configuration du service d'assistance :	104
3.2.3. Configuration du service de délivrance des jetons de sécurité (STS) :	105

3.3. Etapes de la fédération :.....	106
4. Test et résultats :.....	108
4.1. Environnement de développement et tests :.....	108
4.2. Tests du scénario de la fédération :.....	108
4.3. Tests des performances :.....	112
4.3.1. Temps consommés :.....	112
4.3.2. Mesure des flux de transmission:.....	113
4.4. Analyses et discussions :.....	114
4.4.1. Flexibilité et agilité :.....	114
4.4.2. Vie privée :.....	115
4.4.3. Temps Réel :.....	115
4.4.4. La taille des messages :.....	115
4.4.5. Le débit de transfert:.....	115
4.4.6. La Mobilité :.....	116
Conclusion :.....	117
Conclusion & perspectives :.....	118
Démarche :.....	118
Résultats :.....	119
Perspectives :.....	119
Bibliographie.....	121
Annexe A.....	125
Annexe B.....	127