

# Table des matières

<b>Préface . . . . .</b>	1
Delphine BECHEVET et Ana LOIZEAU	
<b>Remerciements . . . . .</b>	3
<b>Présentation des auteurs . . . . .</b>	5
<b>Avant-propos . . . . .</b>	7
<b>Partie 1. Introduction et contexte technique . . . . .</b>	13
<b>    Introduction de la partie 1 . . . . .</b>	15
<b>    Chapitre 1. Généralités . . . . .</b>	17
1.1. De l'IFF au transpondeur. . . . .	17
1.2. La genèse de la RFID . . . . .	19
1.3. La carte à puce et le besoin de sécurité. . . . .	20
1.4. Convergence carte à puce et RFID en HF . . . . .	21
1.5. RFID en UHF, EPC, Rain . . . . .	23

---

<b>Chapitre 2. Généralités techniques de la RF . . . . .</b>	<b>25</b>
2.1. Propagations et rayonnements des ondes RF . . . . .	25
2.1.1. Comportement du champ rayonné en fonction de la distance . . . . .	25
2.1.2. Quelques appellations contrôlées. . . . .	27
2.1.3. Remarques concernant les applications RFID et NFC . . . . .	28
2.2. Communications RF en bandes étroite, large et ultra large : notion de bande passante fractionnaire. . . . .	29
2.2.1. <i>Narrow Band</i> (NB) : bande étroite . . . . .	30
2.2.2. <i>Wide Band</i> (WB) : bande large . . . . .	31
2.2.3. <i>Ultra Wide Band</i> (UWB) : bande ultra-large . . . . .	32
2.3. Contraintes réglementaires . . . . .	35
2.4. Normes et standards. . . . .	35
2.4.1. Normes . . . . .	35
2.4.2. Standards . . . . .	36
<b>Partie 2. Identification radiofréquences RFID en LF et en HF . . . . .</b>	<b>37</b>
<b>Introduction de la partie 2 . . . . .</b>	<b>39</b>
<b>Chapitre 3. Radio-identification en LF et HF . . . . .</b>	<b>41</b>
3.1. Généralités . . . . .	41
3.1.1. RFID en LF (125/134,2 kHz) et en HF (13,56 MHz) . . . . .	41
3.1.2. RFID en UHF (autour de 900 MHz) et en SHF (entre 3 et 30 GHz) . . . . .	42
3.1.3. Lecteur, interrogateur, <i>base station</i> , PCD, tag, <i>target</i> , PICC, etc. . . . .	43
3.1.4. Énergie fournie et modes d'alimentations du tag . . . . .	43
3.1.5. Liaison descendante ( <i>downlink</i> ) du tag vers le lecteur . . . . .	45
3.1.6. Communication descendante passive : modulation de charge . . . . .	46
3.2. RFID LF à 125 et 134,2 kHz : identification générale et animale . . . . .	48
3.3. RFID HF à 13,56 MHz : introduction et éléments communs. . . . .	48
3.3.1. Genèse et essaimages. . . . .	48
3.3.2. Un petit peu de physique. . . . .	49
3.3.3. Rappel des contraintes réglementaires à 13,56 MHz . . . . .	51
3.3.4. Facteurs limitant les distances en RFID HF . . . . .	52

---

3.3.5. Actualisations, enrichissements et nouveautés des normes ISO . . . . .	54
3.4. RFID HF à 13,56 MHz – Norme ISO/IEC 14 443 – Cartes de proximité . . . . .	56
3.4.1. Optimisation de la liaison entre PCD et les « PICC's...ss » . . . . .	56
3.4.2. <i>Active Load Modulation</i> en ISO/IEC 14 443 . . . . .	57
3.4.3. Classes d'antennes . . . . .	61
3.4.4. Débits numériques HBR et VHBR. . . . .	65
3.4.5. <i>Loading effect, detuning et multichips</i> dans le champ. . . . .	68
3.4.6. Enrichissements techniques propriétaires . . . . .	72
3.5. RFID HF à 13,56 MHz – Norme ISO/IEC 15 693 – Cartes de voisinage . . . . .	74
3.5.1. Distance maximale en « main libre » . . . . .	75
3.5.2. <i>Electronic Article Surveillance</i> en ISO 15693 . . . . .	79
3.5.3. <i>Active Load Modulation</i> en ISO/IEC 15693 . . . . .	80
3.5.4. Enrichissements propriétaires et évolutions de la norme . . . . .	80
3.6. RFID HF à 13,56 MHz – Norme ISO/IEC 18 000-3 : <i>item management</i> . . . . .	81
3.6.1. ISO/IEC 18 000-3M 1 (ou 18 000-31). . . . .	82
3.6.2. ISO/IEC 18 000-3M 2 (ou 18 000-32). . . . .	82
3.6.3. ISO/IEC 18 000-3M 3 (ou 18 000-33). . . . .	82
 <b>Chapitre 4. Du protocole à l'application . . . . .</b>	 <b>85</b>
4.1. Introduction . . . . .	85
4.1.1. Un lecteur sachant faire bien autre chose que lire . . . . .	85
4.1.2. Deux niveaux de lecture . . . . .	86
4.2. Modèle OSI et normes de la RFID en HF . . . . .	86
4.2.1. Partie analogique . . . . .	87
4.2.2. Partie digitale . . . . .	87
4.2.3. Couches hautes . . . . .	88
4.3. Détection du tag par le lecteur : boucle de <i>polling</i> et anticollision . . . . .	89
4.3.1. TTF versus RTF. . . . .	89
4.3.2. Boucle de <i>polling</i> . . . . .	90
4.3.3. Gestion des collisions et multi-activation . . . . .	91
4.3.4. Multi-activation, possibilités et limites pratiques . . . . .	93
4.3.5. Stratégie à adopter face à plusieurs tags ? . . . . .	93
4.4. Mission de la couche de transport : assurer la qualité de service sur un médium peu fiable . . . . .	94
4.4.1. Détection et classification des erreurs . . . . .	95
4.4.2. <i>Card tracking, timeout</i> et réactivité . . . . .	97

4.4.3. Plans de certification des lecteurs . . . . .	98
4.5. Développer une application utilisant les tags . . . . .	101
4.5.1. Cas de tag étant une (vraie) carte à puce (sans contact). . . . .	101
4.5.2. Cas des cartes à logique câblée . . . . .	103
<b>Chapitre 5. Transactions sans contact sécurisées . . . . .</b>	<b>107</b>
5.1. Introduction . . . . .	107
5.1.1. RFID, NFC ou « carte à puce sans contact » ? . . . . .	107
5.1.2. Sécurité de la carte et sécurité du système . . . . .	108
5.1.3. Les acteurs de l'écosystème carte et l'évaluation de la sécurité. . . . .	110
5.1.4. Le cycle de vie de la carte . . . . .	111
5.2. Notion de transaction sécurisée . . . . .	114
5.2.1. Le concept d'une transaction . . . . .	114
5.2.2. <i>Anti-tearing</i> et atomicité de la transaction . . . . .	114
5.2.3. Le besoin de sécurité . . . . .	116
5.2.4. Des transactions sécurisées « légères » . . . . .	118
5.3. Mécanismes d'authentification . . . . .	118
5.3.1. Authentifier la carte ou authentifier les données ? . . . . .	118
5.3.2. Authentification mutuelle symétrique . . . . .	121
5.3.3. Authentification mutuelle asymétrique . . . . .	123
5.4. Communication sécurisée . . . . .	127
5.5. Attaques et défense . . . . .	128
5.5.1. Les différents angles d'attaques mis en jeu . . . . .	128
5.5.2. L'importance de la sécurité de bout en bout . . . . .	130
5.5.3. Petite panoplie du <i>hacker</i> . . . . .	131
5.5.4. Les attaques classiques (et quelques idées pour les parer) . . . . .	131
<b>Partie 3. Near Field Communication en HF (NFC) . . . . .</b>	<b>137</b>
<b>Introduction de la partie 3 . . . . .</b>	<b>139</b>
<b>Chapitre 6. La communication en champ proche . . . . .</b>	<b>141</b>
6.1. Présentation et concepts généraux . . . . .	141
6.1.1. De la RFID HF à la NFC . . . . .	141
6.1.2. Les promesses du marketing . . . . .	142
6.1.3. La normalisation . . . . .	143

---

6.2. Rôles et modes de fonctionnement des appareils NFC . . . . .	144
6.2.1. Un peu de vocabulaire . . . . .	144
6.2.2. Rôles d'un <i>NFC Device</i> . . . . .	146
6.2.3. Modes de communication entre deux <i>NFC Devices</i> . . . . .	147
6.2.4. Croiser les modes et les rôles . . . . .	149
6.3. Champs d'applications de la communication en champ proche . . . . .	149
<b>Chapitre 7. Le monde du <i>NFC Forum</i> . . . . .</b>	<b>151</b>
7.1. Introduction . . . . .	151
7.1.1. Création et évolution du <i>NFC Forum</i> . . . . .	151
7.1.2. Extension du domaine de la NFC . . . . .	151
7.1.3. <i>NFC Forum</i> face aux normes ISO . . . . .	152
7.1.4. Comparaison des deux corpus . . . . .	153
7.1.5. Contraintes nées de la dualité ISO/ <i>NFC Forum</i> . . . . .	153
7.2. Les modes d'un <i>NFC Forum Device</i> . . . . .	154
7.2.1. Sens 1 : quel appareil pour générer la porteuse ? . . . . .	154
7.2.2. Sens 2 : le fonctionnement de l'appareil . . . . .	155
7.2.3. Tentative de synthèse. . . . .	156
7.3. Les tags du <i>NFC Forum</i> . . . . .	157
7.3.1. Sous-jacents techniques du <i>tag NFC Forum</i> . . . . .	158
7.3.2. <i>NFC Forum</i> T2T et T5T, les tags basés sur de la logique câblée . . . . .	159
7.3.3. <i>NFC Forum</i> T4T, la carte à puce utilisée comme tag . . . . .	160
7.3.4. Quel tag pour quelle application ? . . . . .	161
7.3.5. Géométrie, performances et ergonomie . . . . .	161
7.4. Messages NDEF et enregistrements RTD . . . . .	162
7.4.1. Le RTD URI . . . . .	162
7.4.2. Le RTD type externe (MIME) . . . . .	163
7.4.3. <i>Handshaking</i> et <i>handover</i> . . . . .	164
7.5. Vie et mort du <i>peer-to-peer</i> . . . . .	164
7.5.1. NFC-DEP, LLCP et SNEP . . . . .	164
7.5.2. Abandon du P2P . . . . .	165
7.5.3. Forme de réincarnation. . . . .	166
7.6. L'émulation de carte . . . . .	166
7.7. Chargement par induction avec NFC . . . . .	167
<b>Chapitre 8. Le <i>smartphone</i> NFC . . . . .</b>	<b>169</b>
8.1. Le <i>smartphone</i> , l'appareil NFC à (presque) tout faire . . . . .	169
8.2. La gestion des tags <i>NFC Forum</i> par le <i>smartphone</i> . . . . .	171

8.2.1. Le tag comme déclencheur d'actions . . . . .	171
8.2.2. Manipulation d'un tag au sein d'une application . . . . .	172
8.3. Le <i>smartphone</i> en mode lecteur . . . . .	173
8.3.1. Principes . . . . .	173
8.3.2. Mise en œuvre Android . . . . .	174
8.3.3. Mise en œuvre iOS . . . . .	176
8.4. Le <i>smartphone</i> en mode émulation de carte . . . . .	179
8.4.1. Une petite histoire du père Castor . . . . .	179
8.4.2. Aspects physiques et protocolaires . . . . .	180
8.4.3. Émulation de carte par un <i>Secure Element</i> ou la SIM . . . . .	182
8.4.4. Émulation de carte dans le processeur principal . . . . .	183
8.5. Les passes NFC et les applications « Wallet » . . . . .	187
8.5.1. Les passes <i>NFC Google Smart Tap</i> . . . . .	188
8.5.2. Les passes <i>NFC Apple VAS</i> . . . . .	190
8.5.3. Vers le « multi purpose tap » . . . . .	192
8.6. Prenons un peu de distance . . . . .	193
8.6.1. Le cas doublement idéal du tag idéal face au lecteur idéal . . . . .	193
8.6.2. Lecteur conventionnel et tag conventionnel . . . . .	194
8.6.3. <i>Smartphone</i> en mode lecteur ou initiateur NFC . . . . .	194
8.6.4. <i>Smartphone</i> en mode émulation de carte . . . . .	195
8.6.5. Deux <i>smartphones</i> en face à face . . . . .	196
8.6.6. Les pistes d'améliorations : le <i>NFC Forum Release 15</i> . . . . .	196
 <b>Chapitre 9. Objets connectés NFC . . . . .</b>	 199
9.1. Objets « lecteurs » . . . . .	199
9.1.1. Principes . . . . .	199
9.1.2. Détails de mise en œuvre . . . . .	200
9.2. Objets « tags » . . . . .	202
9.2.1. Principes . . . . .	202
9.2.2. Détails de mise en œuvre . . . . .	203
9.2.3. Capteurs minimalistes . . . . .	204
9.3. Objets « tags » avec échanges dynamiques . . . . .	205
 <b>Chapitre 10. Applications NFC en boucle ouverte . . . . .</b>	 207
10.1. NFC, RFID HF et RFID UHF . . . . .	207
10.1.1. Un besoin de convergence poussé par la vente au détail . . . . .	208
10.1.2. Les premiers pas vers une fusion NFC et RFID UHF . . . . .	209

---

10.2. NFC et paiement, NFC et transport . . . . .	211
10.2.1. Le transport public . . . . .	211
10.2.2. Le paiement . . . . .	212
10.3. NFC et eID . . . . .	213
10.3.1. Du passeport aux cartes d'identité électroniques . . . . .	213
10.3.2. Les limites du MRTD et la création du mDL . . . . .	215
10.3.3. Vers un portefeuille numérique unique ? . . . . .	216
10.4. NFC et automobile. . . . .	217
10.4.1. <i>Car Connectivity Consortium</i> (CCC) et la clé virtualisée. . . . .	219
10.4.2. CCC et <i>NFC Forum</i> . . . . .	219
10.5. NFC et contrôle d'accès physique. . . . .	220
10.5.1. Vers une solution contrôle d'accès « universelle » ? . . . . .	221
10.5.2. Convergence contrôles d'accès physique, accès logique et gestions des identités . . . . .	222
10.6. <i>Digital Product Passport</i> : DPP et le NFC. . . . .	222
10.6.1. Généralités . . . . .	222
10.6.2. Le DPP et le NFC en HF . . . . .	223
<b>Partie 4. Identification en UHF et SHF localisation en UWB . . . . .</b>	<b>225</b>
<b>Introduction de la partie 4 . . . . .</b>	<b>227</b>
<b>Chapitre 11. Radio-identification en UHF . . . . .</b>	<b>229</b>
11.1. Introduction et rapide historique de la RFID en UHF . . . . .	229
11.2. Rappels techniques nécessaires . . . . .	232
11.2.1. Surface effective de l'antenne d'un tag en UHF . . . . .	232
11.2.2. Équation de Friis. . . . .	232
11.2.3. Principe de fonctionnement en RFID UHF . . . . .	234
11.3. Nouveautés et compléments à la norme originale ISO 18 000-6 . . . . .	235
11.3.1. Populations d' <i>interrogators</i> denses et multiples . . . . .	235
11.3.2. « Traceable » et « Untraceable » . . . . .	240
11.3.3. « Visibilité » et « invisibilité » du tag . . . . .	245
11.3.4. Exemples usuels en UHF. . . . .	247
11.4. Mode <i>Untraceable</i> et $P_{max}$ admissible des circuits intégrés . . . . .	247
11.4.1. Champs forts en UHF. . . . .	247
11.4.2. Premières conclusions . . . . .	248
11.4.3. Exemples : champ UHF, tag sur métal, puissance maximale du circuit intégré . . . . .	251

11.5. Conclusions générales <i>Traceable</i> et <i>Untraceable</i> . . . . .	252
11.6. Compléments/améliorations propriétaires . . . . .	254
11.7. UHF RFID et RAIN RFID <i>Technology</i> . . . . .	254
11.7.1. RAIN . . . . .	254
11.7.2. RAIN RFID . . . . .	254
11.8. <i>Digital Product Passport</i> (DPP) et la RFID UHF . . . . .	255
11.8.1. Informations requises par le DPP . . . . .	256
11.8.2. Calendrier de l'introduction des DPP . . . . .	256
11.8.3. Le DPP, la RFID UHF et RAIN RFID . . . . .	257
 <b>Chapitre 12. De l'identification RFID à la localisation en UWB . . . . .</b>	 259
12.1. Bref historique du concept UWB ( <i>Ultra Wide Band</i> ) . . . . .	261
12.2. Réglementations concernant les émissions UWB. . . . .	266
12.2.1. Introduction. . . . .	266
12.2.2. Exemple aux États-Unis . . . . .	270
12.2.3. Exemple en France . . . . .	271
12.3. Organismes gravitant autour de l'UWB . . . . .	272
12.3.1. OSI . . . . .	272
12.3.2. IEEE . . . . .	273
12.3.3. ETSI . . . . .	273
12.3.4. Apple . . . . .	273
12.3.5. FiRa . . . . .	274
12.3.6. <i>Car Connectivity Consortium</i> (CCC). . . . .	275
12.3.7. Collaborations entre ces organismes . . . . .	276
12.4. Fonctionnalités de l'UWB . . . . .	278
12.5. Distance maximale de fonctionnement . . . . .	278
12.6. Fonctionnement en usage de télématrice . . . . .	279
12.7. Stabilité de fonctionnement en présence de multiples éléments . . . . .	280
12.8. Compréhension de mouvements et de positions relatives . . . . .	280
12.9. Qualité accrue de sécurité. . . . .	280
12.10. Techniques de fusion d'informations de localisations . . . . .	281
12.11. Conclusion. . . . .	281
 <b>Chapitre 13. Génération de signaux UWB . . . . .</b>	 283
13.1. Signal, codage et modulation. . . . .	285
13.1.1. Format de l'impulsion . . . . .	285
13.1.2. Mise en œuvre d'un signal UWB . . . . .	291

---

13.2. Communication avec des impulsions . . . . .	294
13.2.1. Fréquence de répétition des impulsions (PRF) . . . . .	294
13.2.2. Séquence de codes. . . . .	298
13.2.3. Portée maximale de communication . . . . .	299
13.3. Propriétés de la technologie UWB . . . . .	302
13.4. Architectures et technologies des émetteurs-récepteurs UWB . . . . .	306
13.4.1. Émetteurs UWB . . . . .	306
13.4.2. Récepteurs UWB . . . . .	307
13.4.3. Implémentation des émetteurs-récepteurs UWB . . . . .	312
13.4.4. Résumé émission-réception et synthèse UWB . . . . .	313
<b>Chapitre 14. Introduction et méthodes de localisation . . . . .</b>	<b>315</b>
14.1. Zoner, zonage. . . . .	315
14.2. Localiser. . . . .	316
14.3. Localisation . . . . .	316
14.4. Méthodes de (géo)localisation . . . . .	317
14.5. Solutions de localisation et UWB . . . . .	317
14.6. Méthodes de localisation en UWB . . . . .	318
14.6.1. Principe de la trilateration en 2D . . . . .	319
14.6.2. Performances d'une localisation . . . . .	322
14.6.3. Précision requise pour juger d'un système de localisation . . . . .	322
14.6.4. RADAR et <i>Ranging</i> . . . . .	323
14.6.5. <i>Ranging</i> et télémétrie . . . . .	324
14.6.6. RADAR et applications UWB. . . . .	337
14.7. Concurrence à/de l'UWB . . . . .	340
14.7.1. Bluetooth LE . . . . .	340
14.7.2. Bluetooth 6.0 : concurrent à <i>Ultra Wide Band</i> ? . . . . .	342
<b>Chapitre 15. Champs des applications UWB . . . . .</b>	<b>347</b>
15.1. Domaine de la santé et du médical . . . . .	348
15.2. Domaine de l'identification RFID. . . . .	349
15.3. Domaine grand public . . . . .	351
15.4. Domaine industriel. . . . .	352
15.5. Domaine des transports en commun . . . . .	353
15.5.1. Billetterie UWB – Exemple . . . . .	354
15.6. Domaine de l'automobile . . . . .	355
15.6.1. UWB en automobile, localisation, contrôle d'accès . . . . .	355
15.6.2. <i>Standard Digital Key</i> du CCC. . . . .	361

15.6.3. <i>Digital Key</i> UWB dans le marché automobile . . . . .	369
15.6.4. Usages UWB à d'autres commodités dans le véhicule . . . . .	370
15.6.5. Le problème des alimentations des modules UWB . . . . .	371
<b>Chapitre 16. Exemples de composants pour applications UWB . . . . .</b>	<b>375</b>
16.1. NXP : famille Trimension® . . . . .	375
16.1.1. Pour applications automobiles. . . . .	376
16.1.2. Pour applications domestiques et industrielles . . . . .	379
16.2. Qorvo . . . . .	380
16.2.1. Pour applications industrielles et <i>consumer</i> . . . . .	380
16.3. <i>Ultra Wide Band</i> : conclusions actuelles . . . . .	382
16.4. La suite de l'aventure de l' <i>Ultra Wide Band</i> . . . . .	384
<b>Conclusion . . . . .</b>	<b>387</b>
<b>Bibliographie . . . . .</b>	<b>389</b>
<b>Index . . . . .</b>	<b>391</b>