

ORIDAO

**Traçabilité Terrain
& Authentification**



23-26 mars 2010
Paris Nord Villepinte – Hall 6

Traçabilité Sécurisée

Authentification Terrain

RFID Passive LF, HF/NFC, UHF...

RFID Active, Réseaux de Capteurs

- Cession de Licences des protocoles sécurisés
- Assistance Implémentation Logicielle/Matérielle
- Conseil



LASEC / LSM / RFIC



INTEL Labs
WISP



Salon RFID – 23-26 mars 2010





- **Exploitation/Distribution – Environnement peu/pas accessible**
 - Acteurs multiples...
 - Couverture géographique large...
 - Connexion intermittente/non-existante...
- **Nécessité d'une preuve d'origine**
 - Raisons de sécurité...
 - Accès à des informations authentiques...
- **Nécessité d'une preuve de bon déroulement du processus**
 - Contrôle des circuits de distribution...
 - Opérations de maintenance, Acteurs autorisés & qualifiés...
 - Suivi de paramètres: Contrôles, Durée, Température, Chocs....

Authentification terrain de l'origine et du cheminement !

1) Protocole de Traçabilité Sécurisée Pathchecker

- Sécurité démontrée (Path forgery, Tag manipulation, Tag impersonation, DOS)
- Possibilité de développement multi-plateformes
- Publication [Vaudenay, Ouafi, RFID Sec 2009]



Pathchecker: an RFID Application for Tracing Products in Supply-Chains*

Khaled Ouafi** and Serge Vaudenay
EPFL
CH-1015 Lausanne, Switzerland
<http://laocsw.epfl.ch>

Abstract. In this paper, we present an application of RFIDs for supply-chain management. In our application, we consider two types of readers. On one part, we have readers that will mark tags at given points. After that, these tags can be checked by another type of readers to tell whether a tag has followed the correct path in the chain. We formalize this notion and define adequate adversaries. However, we derive requirements in order to meet security against counterfeiting, cloning, impersonation and denial of service attacks.

1 Introduction

Radio Frequency Identification (RFID) tags are being massively deployed in several applications and business in order to ensure integrity and security. The deployment of this technology is mainly motivated by the gain in terms of time and cost due to the automation of previously labor-intensive control processes such as access control, authentication, shipment tracking, inventory and logistics, payment... In addition, RFID tags are extensively used to track and identify goods, supplies and equipment. Some of these deployments, like in the biometric identity cards and passports, are used to identify people or keep track of animals. In other applications, these tags are used as a countermeasure to cloning and counterfeiting (especially in the luxury and pharmaceutical industries) as it allows to authenticate the object they are associated with. Large companies are increasingly using RFIDs to extract intelligence from operations that can contribute to their competitiveness and efficiency. Finally, RFIDs are increasingly being considered for convenience and added-value applications for users like in access control where the automation of the process reduces waiting and processing time.

While much attention by researchers has focused on the efficiency, authentication, and privacy aspects (all fundamental concerns), the context in which

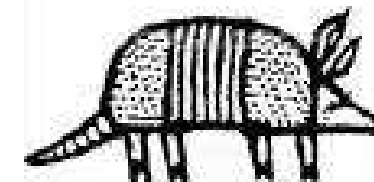
* The content of this paper is subject to a pending patent by ORIDAO. This work was partially funded by the European Commission through the ICT programme under Contract ICT-2007-216646 ECRYPT II.

** Supported by a grant of the Swiss National Science Foundation, 200021-119847/1.

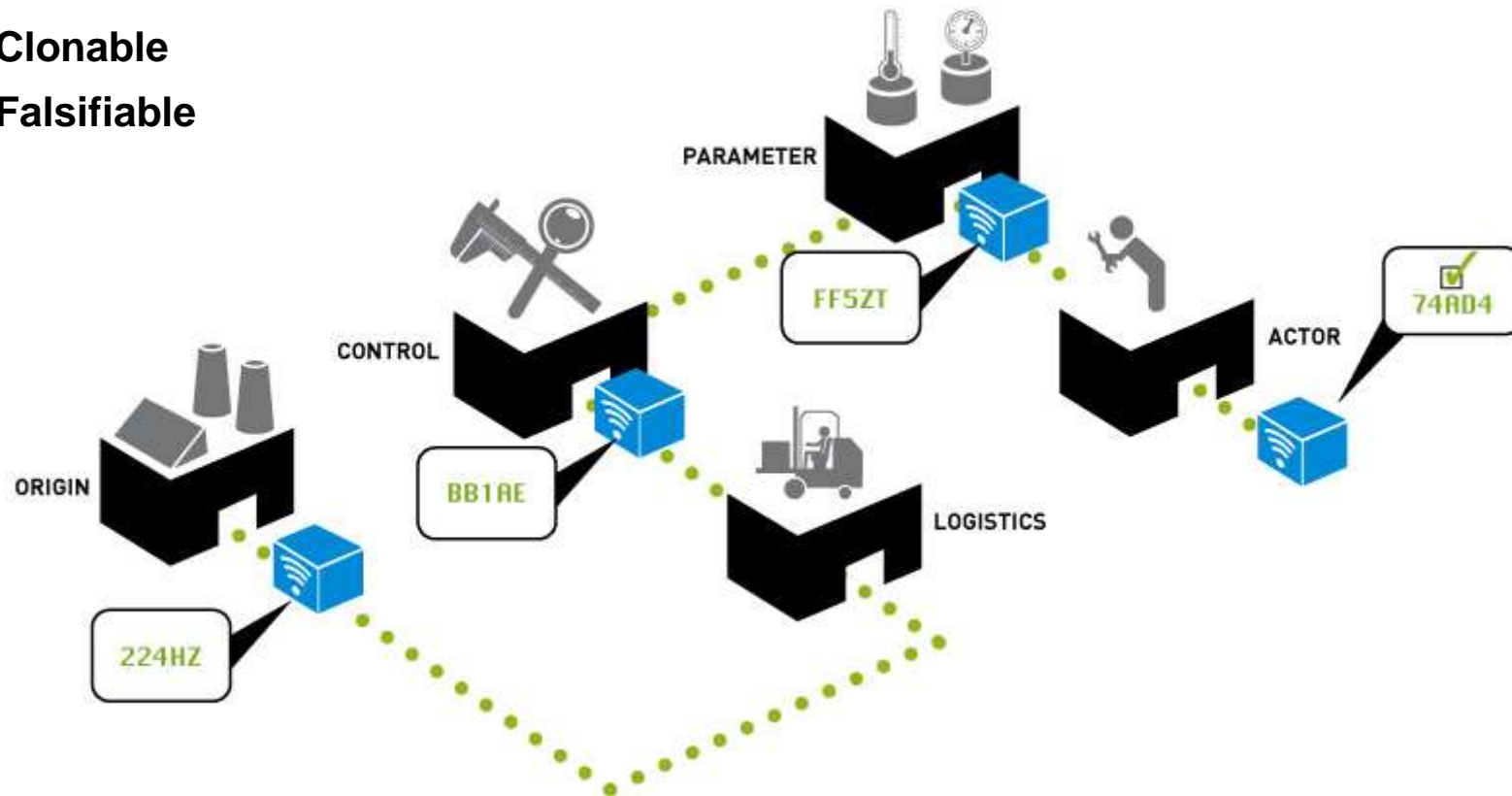
2) Algorithme de Hachage basses-ressources ARMADILLO

Orientation matérielle (RFID, Capteurs autonomes....)

- Faible GE, consommation
- Publication en cours

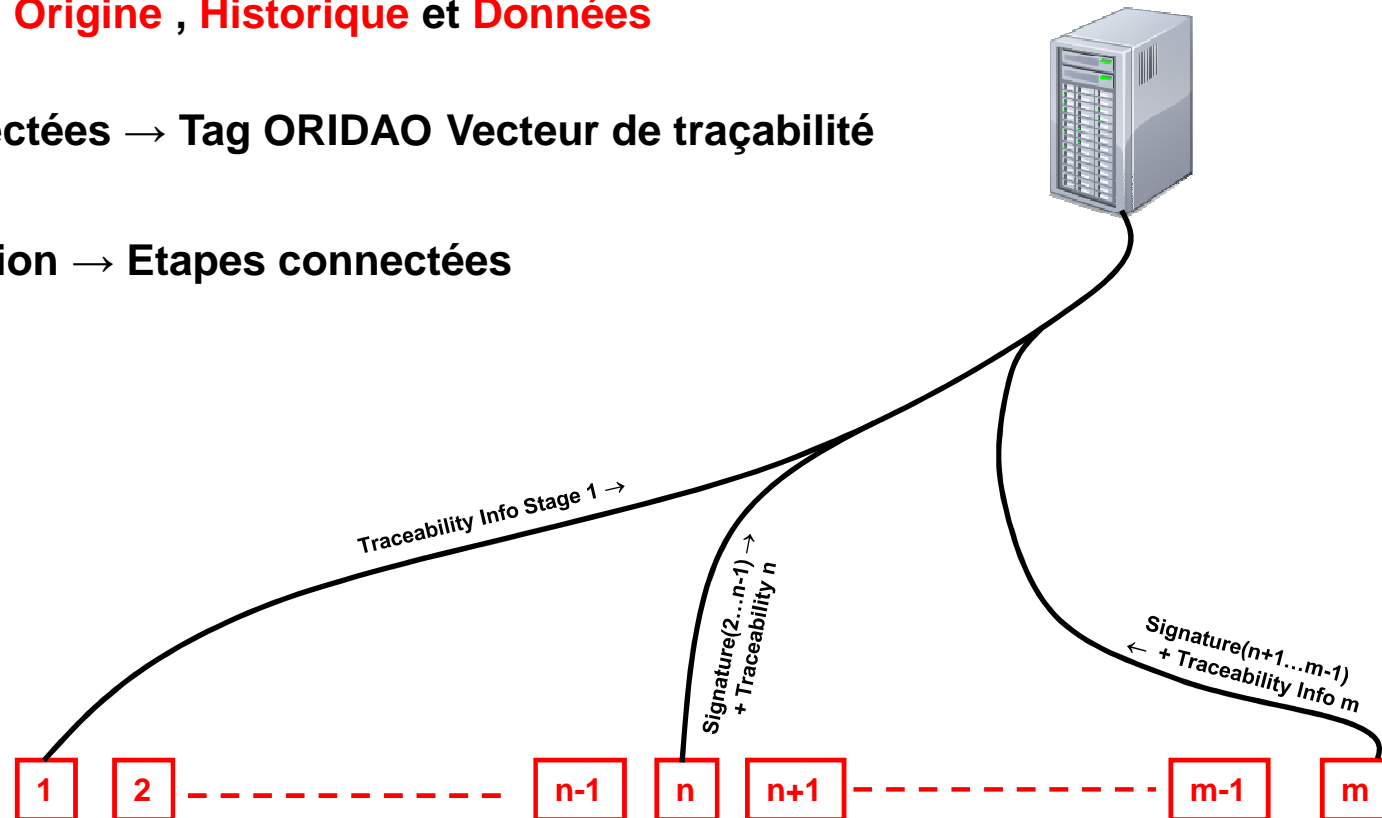


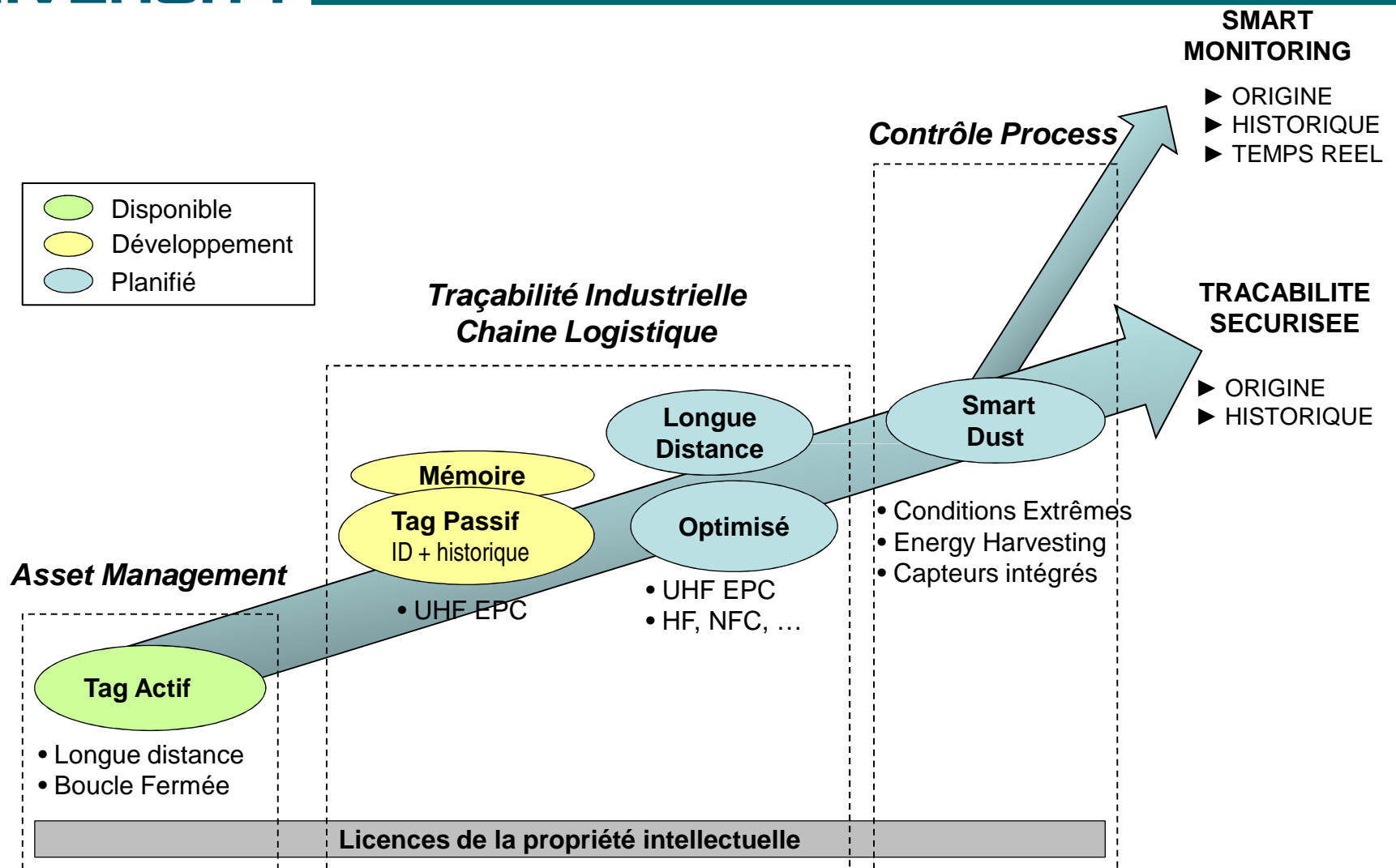
- Logique câblée (RFID passive) ou μ -processeur (RFID Active, Chipset...)
- Faibles ressources de calcul/ ~20 bytes mémoire non volatile
- Non Clonable
- Non Falsifiable

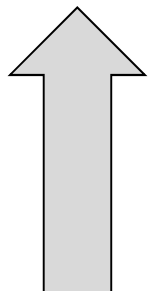


Répartition de l'intelligence applicative : Réseau / Tag

- Authentification **Origine** , **Historique** et **Données**
- Etapes déconnectées → Tag ORIDAO Vecteur de traçabilité
- Resynchronisation → Etapes connectées







Transmission GPRS de Données Sécurisées et Authentiées

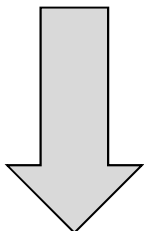
Télésurveillance

Camion
Train
Bateau
Container
...

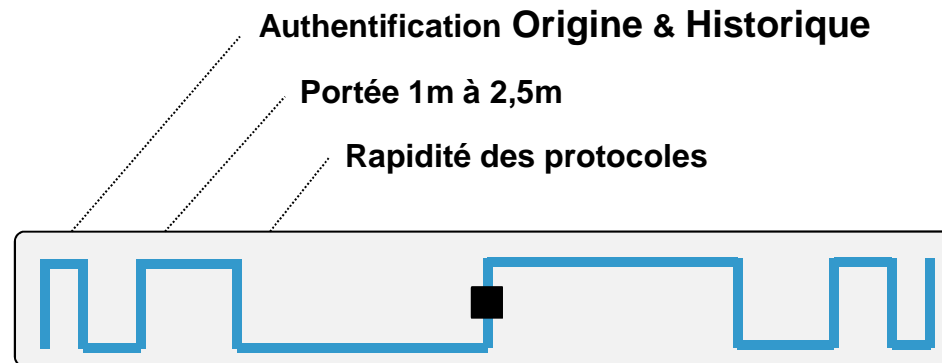
**Plateforme
Communication
RFID/GPRS/GPRS**
+
Active RFID &
Sensors
+
ORIDAO
Passive RFID

Géolocalisation Unité de Transport : GPS
Supervision sécurisée des objets/colis
Supervision paramètres : T, Chocs....

Chargements / Déchargements



**Generation de rapports de transports certifiés
(autorité de confiance)**



UHF EPC GEN 2

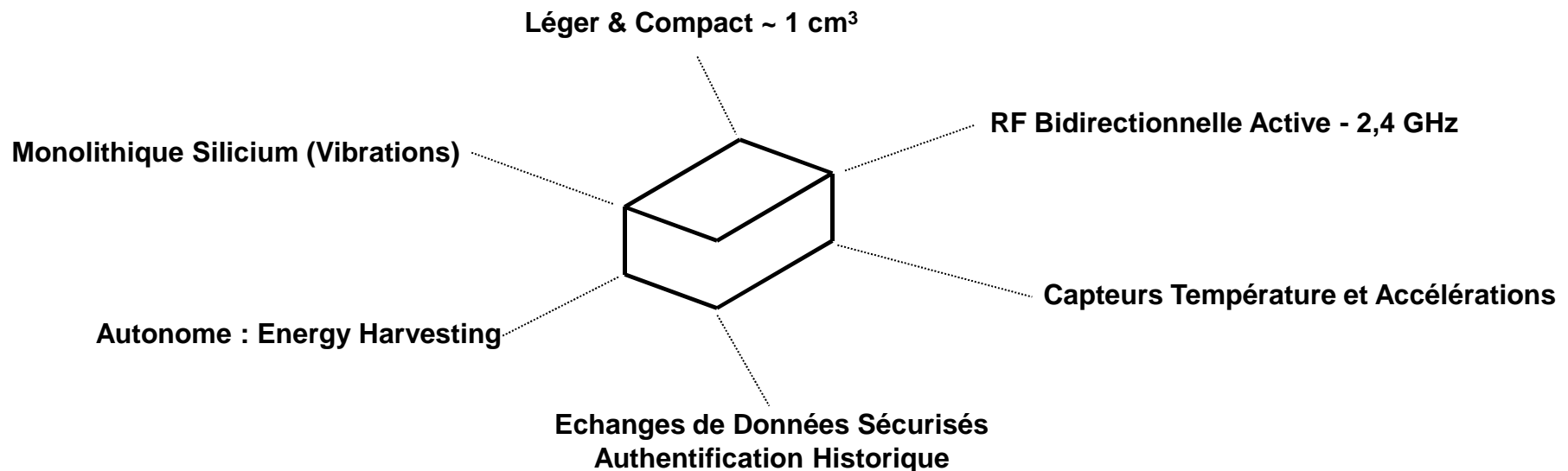
- Tag non-clonable/Signature non-falsifiable
- Authentification mutuelle Tag/Lecteur
- Compatible avec les infrastructures existantes
- Mise à jour Firmware lecteur ou Middleware

Disponibilité 3ème trimestre 2010

Mémoire:

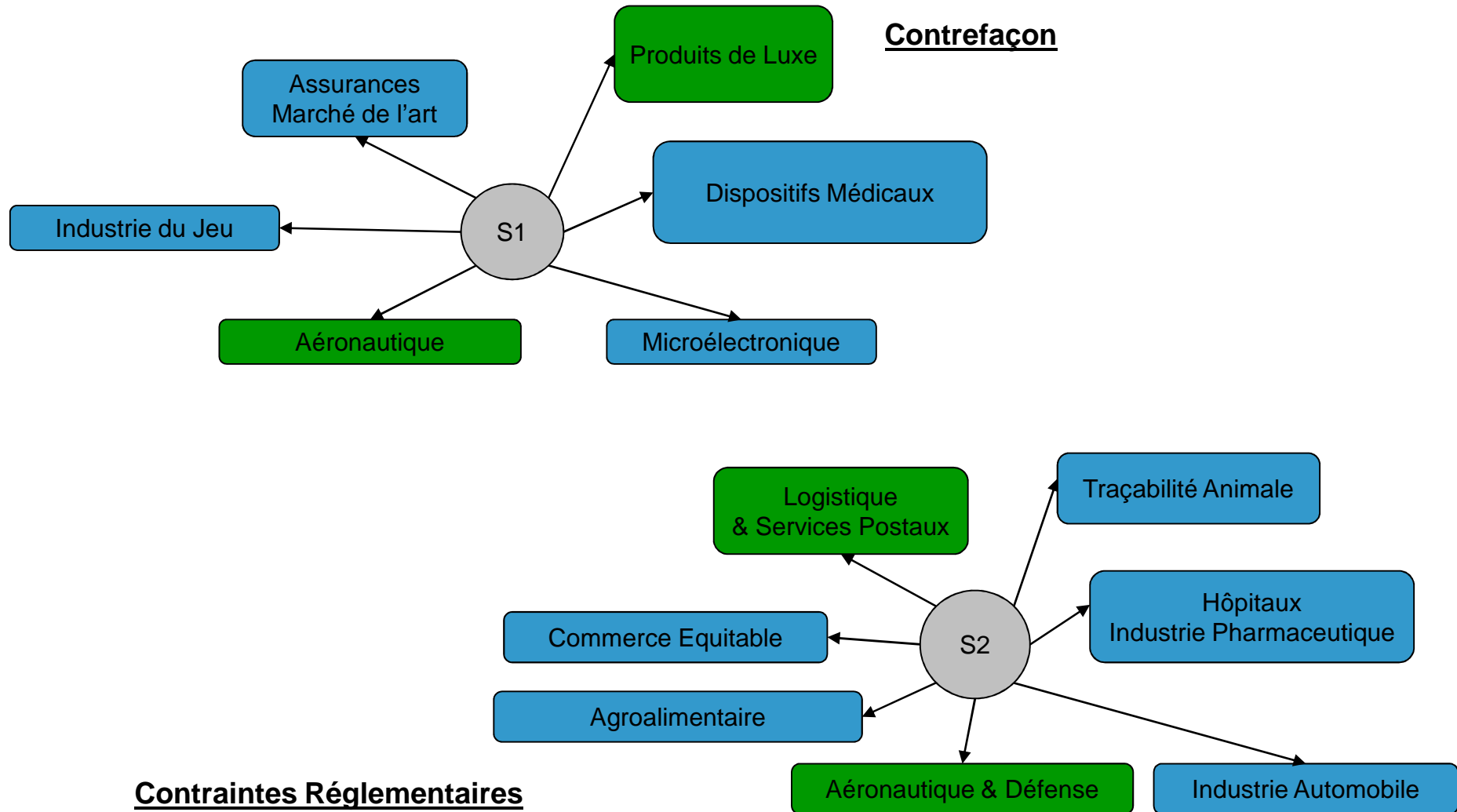
- Contenu Clair ou Chiffré
- Droits d'accès conditionnels
- ATA Spec 2000 Chap 9.5

IP transférable : LF, HF/NFC, SHF...



Applications Aéronautiques et Industrielles....

- Supervision et Anticipation Failles - Machines tournantes critiques...
- Monitoring Conditions d'Utilisation - Pneumatiques...
- Asservissements Eléments Hautement Mobiles...Partenaire Industriel



Merci pour votre attention

nicolas.reffe@oridao.com
+33 4 67 13 00 65

Salon RFID – 23-26 mars 2010

