Réalisation de l'Interopérabilité au sein du Gouvernement Haitien

08.09.2015 Haiti, Port-au-Prince

Oliver Väärtnõu, CEO
Tarmo Oja, UXP product manager

For a more secure and safe world.

CYBERNETICA

Sujets de la Présentation

- Cybernetica AS, Contexte
- Interopérabilité du Gouvernement
- UXP ™ Présentation du produit et déploiement
- Haiti,Vue d’ensemble du projet

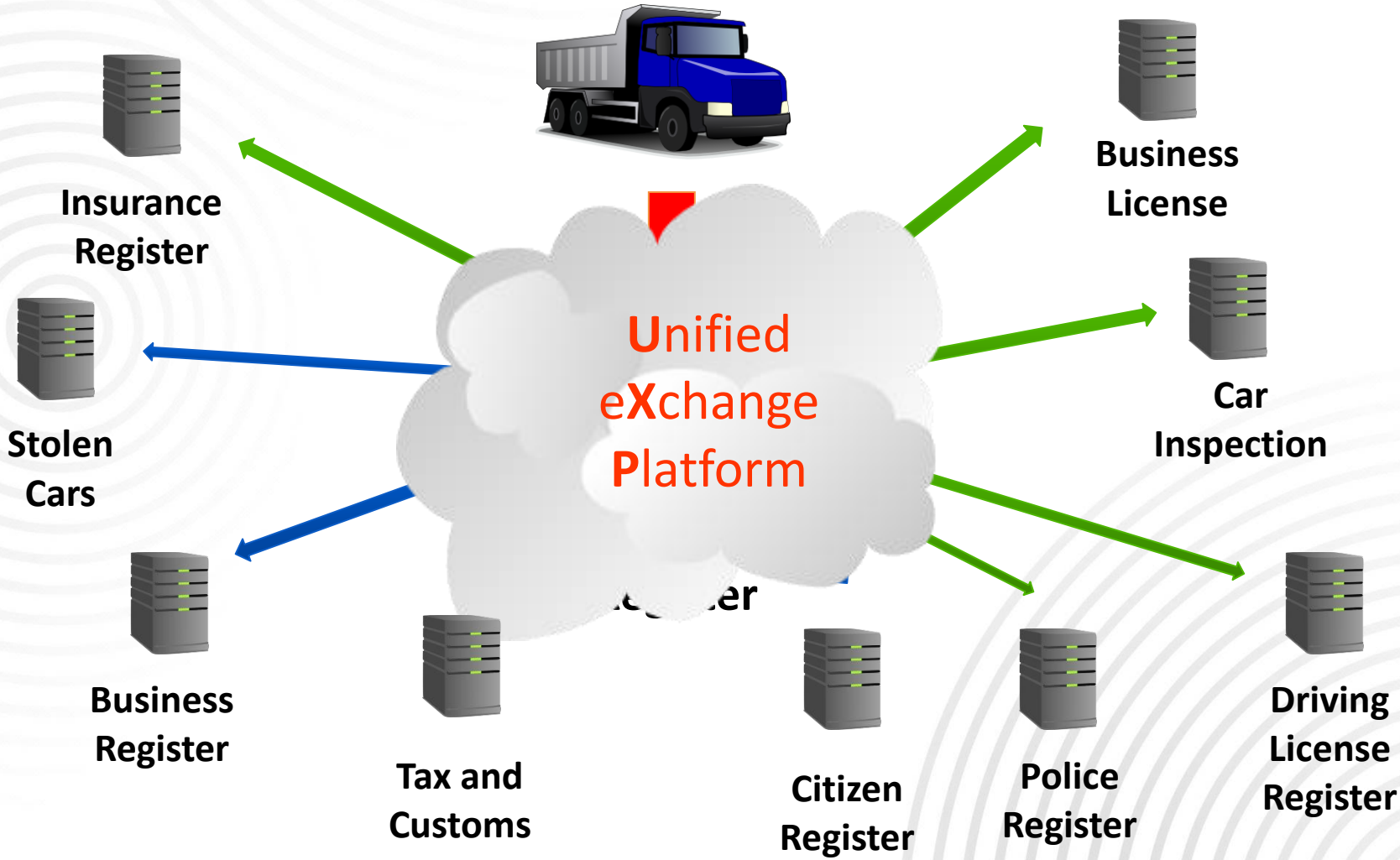
Cybernetica AS, Faits Principaux:

- Créé en 1997, formé sur la base de l'Institut de Cybernétique (Estonian Academy of Sciences)
- Status: Société privée à responsabilité limitée
- Personnel en 2015: 110, plus de 80 en R&D
- Revenu en 2015: 9 millions d'euros (10 MUSD), 30% des exportations
- Certifié en ISO 9001 et ISO 14001
- Evaluation Internationale (UE) positive pour la recherche de la sécurité de l'information et le développement de logiciels
- Recompense: Prix nationaux et internationaux.

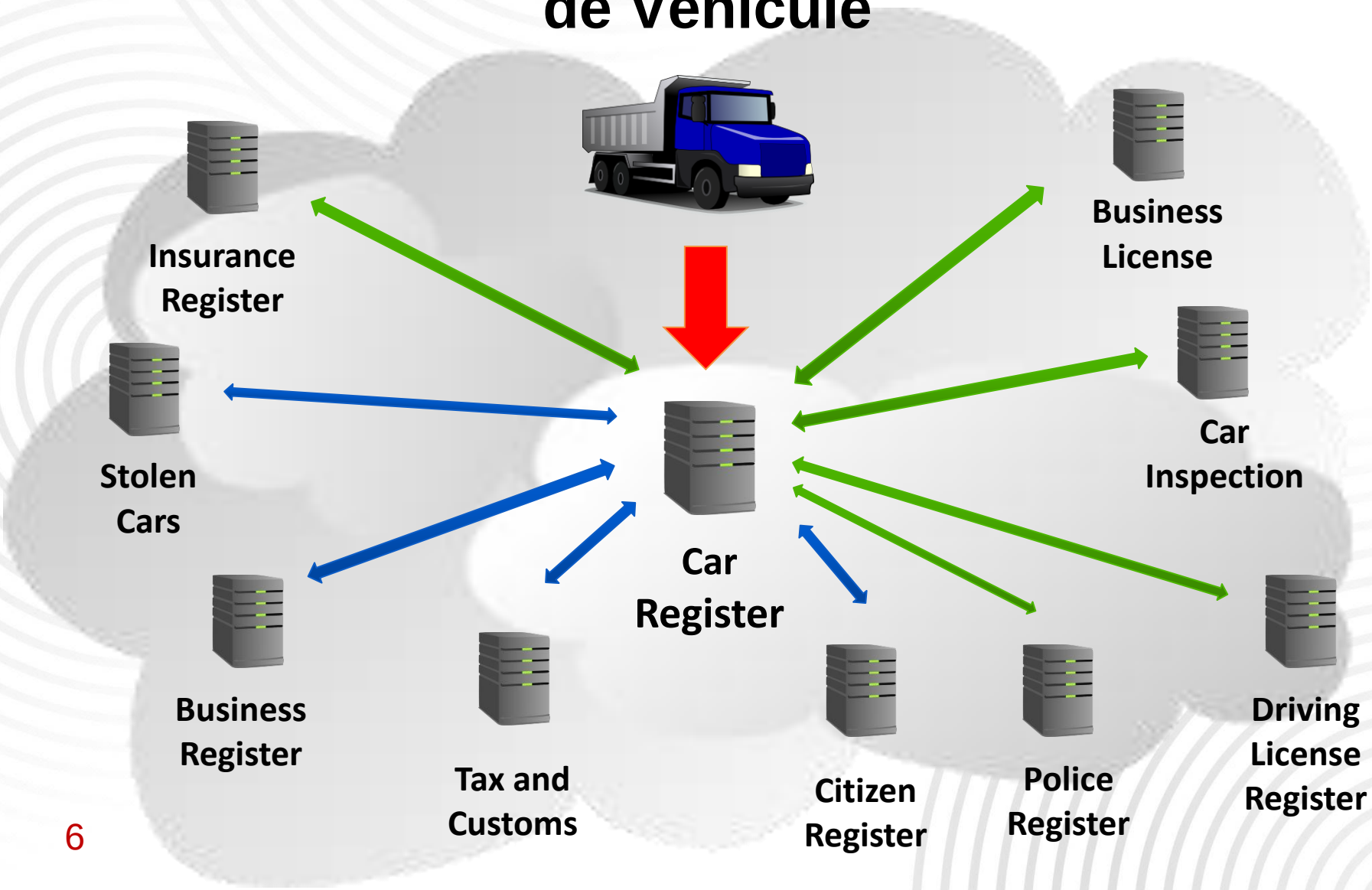
Cybernetica AS, operations:

- **eGovernment Software Solutions**:
  - Plateforme d'interopérabilité sécurisée : UXP™
  - Plateforme de l'identité numérique : Mobile-ID
  - Systèmes basés sur le Web pour les autorités fiscales et douanières
  - Système de vote par Internet
  - Traitement de données sécurisées : Sharemind™
- **Marine Systems**:
  - signalisation lumineuse et de la télématique de produits visuels
  - systèmes de surveillance côtière
  - les systèmes de radio communication
  - **Research in Information Security:** Problèmes théoriques et applications

Cas d'utilisation : Enregistrement et contrôle de Véhicule



Cas d'utilisation: Enregistrement et contrôle de Véhicule



Histoire et Contexte de UXP

- Initiée par le programme **X-road en** 2000 en Estonia
- Système actif dépuis **2001**, aucun temps d’arrêt
- Plus de 2000 services publics et privés
- Plus de 600 millions de transactions l'année dernière 2014
- 2014 marque la naissance de la technologie UXP (v6)
- Gouvernement de la Finlande adopte la technologie
- Gouvernement de la Namibie adopte la technologie

Valeurs clés

UXP fournit un accès sécurisé, le protocole de transport unifié pour les services Web :

- **Distribué**, pas de base de données unique ni super base de données
  - L'accès au service contrôlé par le Data Owner
  - Prise en charge des systèmes hétérogènes
  - Les structures organisationnelles et fonctionnelles existantes doivent être maintenues
- Canal sécurisé avec authentification forte
- Tous les messages sont signés avec des signatures numériques légales.
- Le système est évolutif et élastique.

Eléments Clés

◎ **Security Server** – Passerelle entre le système local et les services UXP.

◎ **Central Server/System** – Serveur de gestion. Utilisé pour la gestion UXP et de recueillir des statistiques sur l'utilisation.

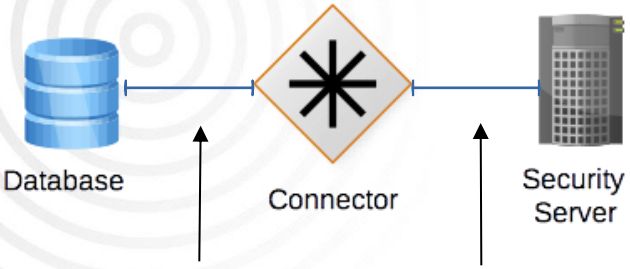
Configuration globale distribuée

◎ **Governing Authority** – gère le système central, traite les demandes

◎ **Trust Services** – Certificate Authority, Time-Stamping Authority

Construisons la connectivité!

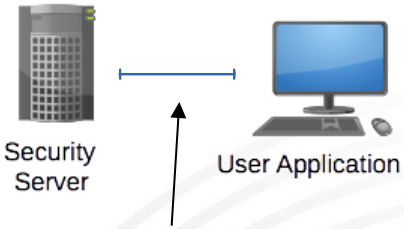
Organisation I
Data Owner



SQL
JSON
....

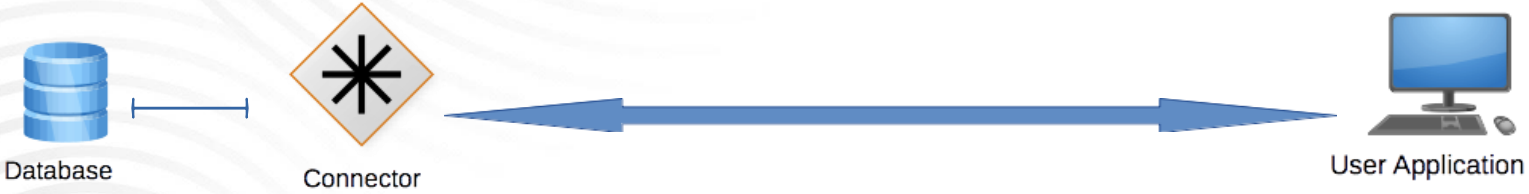
SOAP

organisation II
Service customer



SOAP

Comment Data owner et Customer service se mettent d’accord ?



Pour décrire le service nous avons besoin:

WSDL - Web Services Description Language

- ✓ La description de l'interface lisible à partir XML-based
- ✓ Définit les paramètres d'entrée et de sortie
- ✓ Développeur de service va construire WSDL et le fournir au développeur de côté des consommateurs

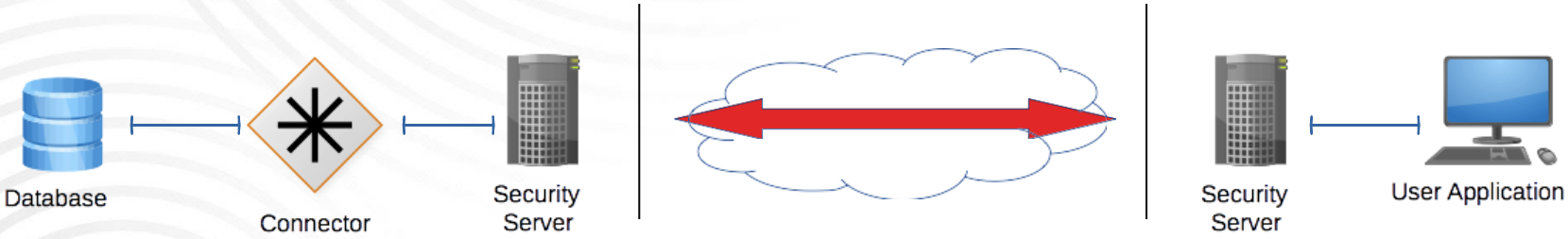
Communication entre Data Owner et Service Customer?

Pour échanger des données nous avons besoin:

◎ **SOAP** - Simple Object Access Protocol

- ✓ XML-based **protocole d'échange de message**
- ✓ SOAP les messages sont contruits en utilisant les informations de **WSDL-file**

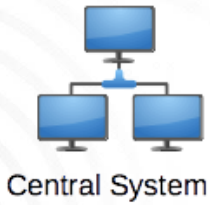
Comment établir la confiance?



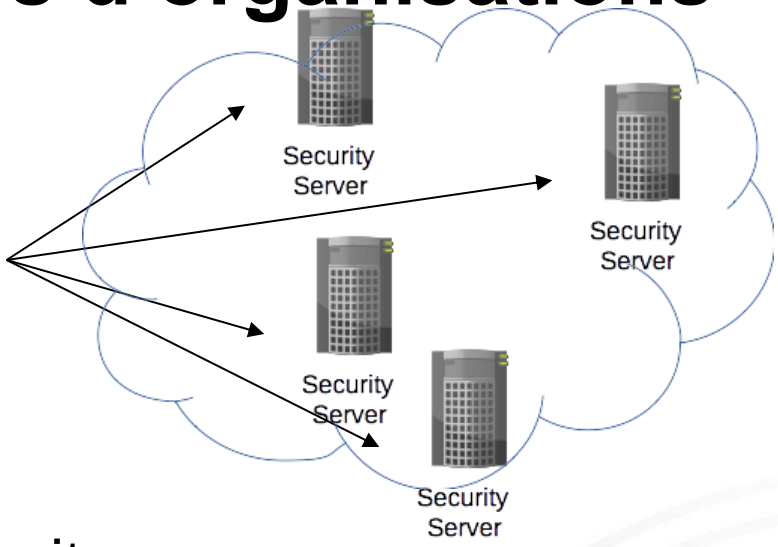
Les messages doivent être sécurisés contre l'interception et modification :

- Encryptage fort.
- Les serveurs de sécurité sont mutuellement authentifiés.
- Tous les messages sont signés avec signature numérique.
- Les signatures sont vérifiées par le serveur de réception de sécurité.
- Les messages sont classés par heure/date et connexion.

Communication entre les serveurs de sécurité et les serveurs d'organisations /services?



Global Configuration



Configuration comprend :

- Identificateur de membre inscrit
- Serveur de sécurité enregistre adresse publique et de l'information du certificat
- Liste des services d'affectation spéciale approuvée :
  - Information sur **Certificate Authority and OCSP**
  - **Informations de service sur Date /Heure**

Déploiement, propriétaire de service

- Choisir systèmes d'information / bases de données / registres
- Appliquer les politiques d'accès aux données.
- **Interfaçage** des systèmes d'information
- Définition des services, WSDL
  - ✓ **Développer** des interfaces SOAP
  - ✓ Placement de **serveur de sécurité** dans le réseau
  - ✓ Serveur physique ou virtuel distinct
  - ✓ **Les interfaces réseau** doivent être sécurisés, un pare-feu
  - ✓ **L'échange d'informations** de service
  - ✓ **Accord** entre producteur et client

Déploiement, Client

- **Trouver un service**
- Accord de conditions de service et les détails avec l‘émetteur.
- Élaborer une politique d'accès au service.
- Placement de serveur de sécurité dans le réseau
  - ✓ Serveur physique ou virtuel distinct
  - ✓ Les interfaces réseau doivent être sécurisés, un pare-feu
  - ✓ **Interfaçage des systèmes d'information**
  - ✓ Développer SOAP pour les récepteurs

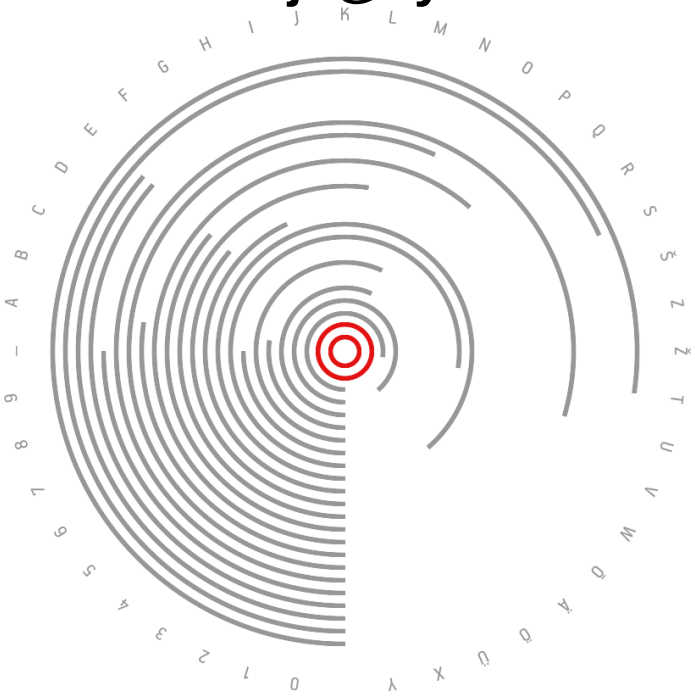
Vue d’ensemble du Projet

- Financé par l'USAID, exécuté par Chemonics International Inc.
- l’implémentation du Integrated Financial Management System se fera avec 12 premières institutions publiques choisies.
- Trois ans de support et de maintenance avec la collaboration d’un partenaire local.

Delivery	Delivery Name	Delivery Date
1	Detailed Project Plan	25 September 2015
2	Software and Licenses	30 September 2015
3	Workshop in Estonia	3 – 9 October 2015
4	System Installation and Documentation	27 November 2015
5	Trainings in Haiti	18 December 2015
6	Final Report	12 February 2016

MERCI!
Questions?

oliver.vaartnou@cyber.ee
tarmo.oja@cyber.ee



CYBERNETICA