

Traçabilité sécurisée embarquée

Abdourhamane IDRISSE*, Thierry FOURNEL*, Alain AUBERT*

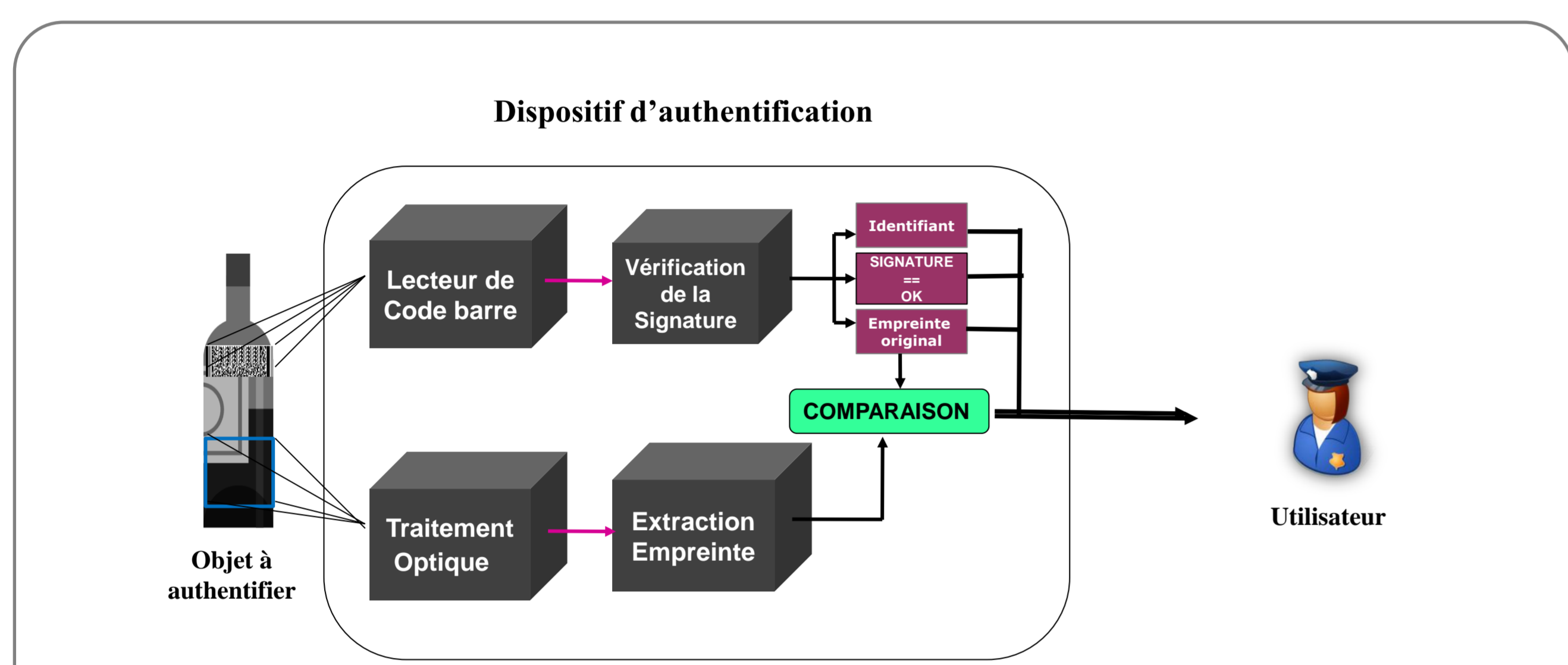
Laboratoire Hubert Curien - Université Jean Monnet de Saint-Etienne

Résumé: L'objectif de nos travaux est de proposer un protocole cryptographique et un système de traçabilité sécurisée basé sur ce protocole permettant de vérifier l'origine d'un produit sans avoir accès à une base données de références. L'empreinte optique de référence et un identifiant qui doivent se trouver sur le produit constituent le code-produit.

POINTS CLÉS

Mots clés: Traçabilité sécurisée, systèmes embarqués, protocole de sécurité, preuve formelle de sécurité, cryptographie, circuit programmable (FPGA).

PROBLEMATIQUE



❑ **Objectif:** sécurisation d'un dispositif de vérification d'authenticité d'objets manufacturés.

❑ **Intérêt:** faire de la traçabilité sécurisée embarquée.

❑ Approches:

✓ Définir un protocole d'authentification d'objets à travers un dispositif sécurisé

✓ Prouver formellement le protocole de sécurisation du dispositif d'authentification

✓ Implanter matériellement (sur FPGA) le dispositif (niveau VHDL)

❑ Contexte de recherche :

✓ Equipe **MorphoSecure*** : Morphometric tools for secured traceability (Pr. Thierry FOURNEL).

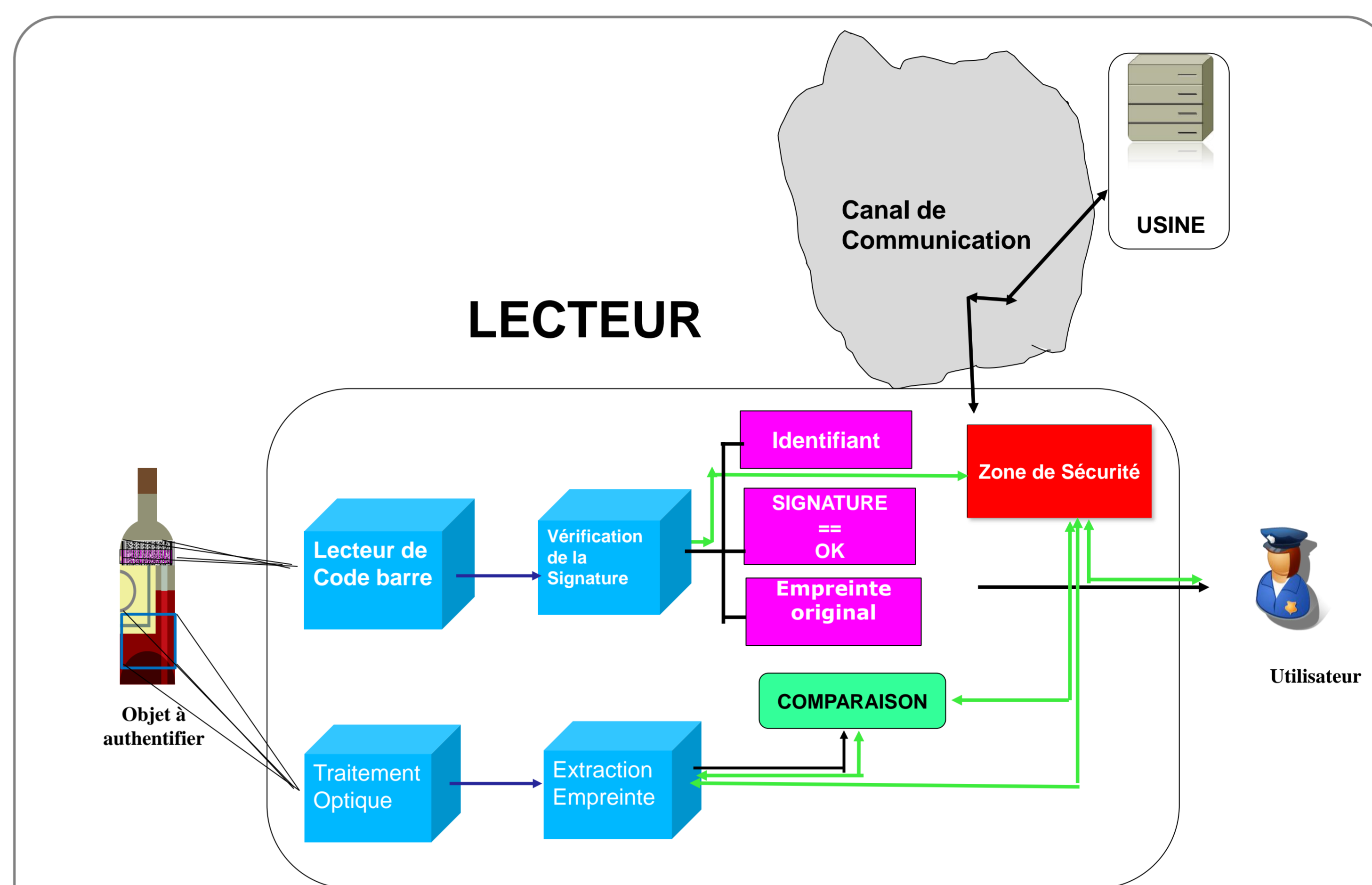
✓ Equipe **SES***: Secure Embedded System (Pr. Victor Fischer et Mc. Alain Aubert)

✓ Opération SISS / TraSecure (UJM-UJF-UCL)

✓ Collaboration avec **Verimag** de Grenoble.

* Equipe (thématique) du Laboratoire Hubert Curien.

TRAVAUX ENGAGES/RESULTATS



Protocole d'authentification

/* Identification du Lecteur */

1. $LECTEUR \rightarrow USINE : id_L, E_{K_L}(id_L, N_L)$
2. $USINE \rightarrow LECTEUR : E_{K_L}(N_U || \text{hash}(N_U || N_L))$
3. $LECTEUR \rightarrow USINE : E_{K_L}(\text{hash}(N_U || id_L))$
4. $USINE \rightarrow LECTEUR : E_{K_L}(K_{\text{session}} || \text{hash}(N_L || id_L))$

/* Vérification de l'intégrité du lecteur */

5. a. $USINE \rightarrow LECTEUR : E_{K_{\text{session}}}(\text{IMG}, R, \text{index}, \text{sign}(R || \text{index}))$
- b. $R' := \text{Empreinte}(\text{IMG})$
 $b_1 := \text{checksign}(R, \text{index}, \text{sign}(R || \text{index})) \in \{0,1\}$
 $b_0 := \text{Macth}(R, R') \in \{0,1\}$
- LECTEUR $\rightarrow USINE : E_{K_L}(\text{hash}(\text{sign}(R || \text{index}) || b_1 || b_0), \text{index})$
- c. $USINE :$
 $\text{SI } \text{hash}(\text{sign}(R || \text{index}) || b_1 || b_0), \text{index) EST CORRECT}$
 ALORS rejouer 5.a
 SINON arrêter le protocol

Travaux en cours :

✓ Preuve du protocole de vérification de l'intégrité du lecteur

Conférence internationale: WIO 2009 Paris 20-24 Juillet 2009.