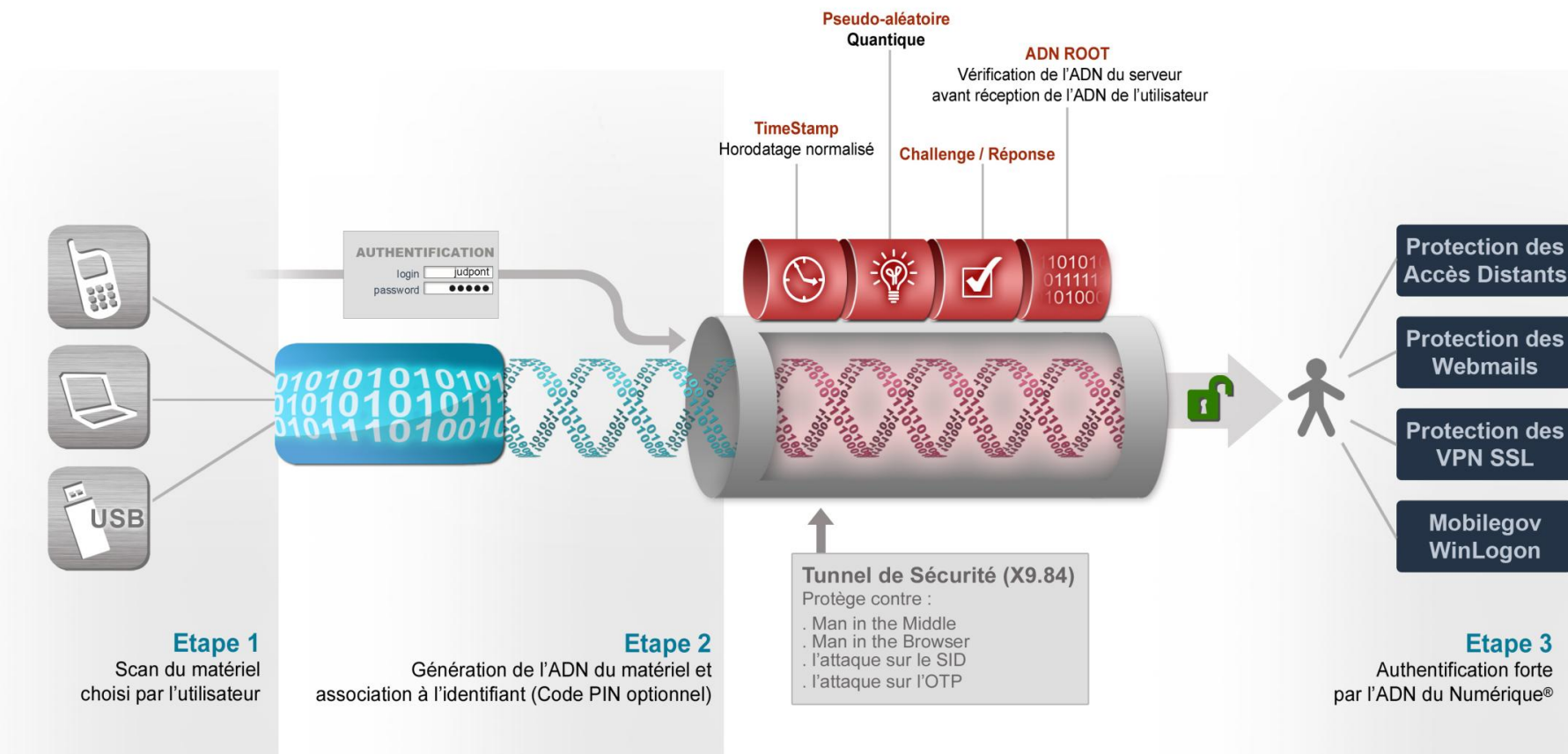


Savoir faire Mobilegov



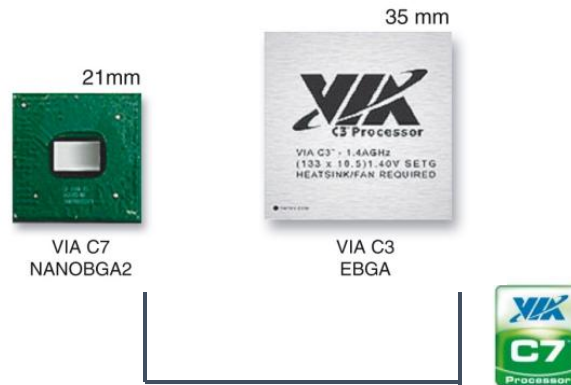
- Identifier des infos spécifiques qui se trouvent sur les composants numériques
- Extraire ces informations
- Transporter et archiver ces informations, de façon sûre et respectueuse de la « vie privée » (comme s'il s'agissait d'infos biométriques)
- Intégrer ces informations dans les principaux standards et outils de sécurité: annuaires (LDAP...), contrôle d'accès (VPN, SSO, accès distants), sécurité du poste de travail (Winlogon, sécurité des endpoints)

Au Coeur de l'ADN du Numérique





Serveur AAA¹ innovant et chiffré en cours de certification CSPN



L'ID-BOX contient une CARTE QUANTIQUE pour toutes les opérations de générations aléatoires.

La force et la sécurité d'un OTP² reposent principalement sur le caractère aléatoire du challenge; les attaques sur SID³ et sur le challenge OTP deviennent quasiment impossibles.

L'ID-BOX intègre le processeur VIA C7, avec le moteur de sécurité VIA PadLock Security Engine, le moteur de sécurité x86 le plus rapide du monde, disposant de la panoplie d'outils la plus complète pour les opérations de cryptographie. Il offre le brouillage SHA-1 et SHA-256 et un multiplicateur Montgomery supportant des clés allant jusqu'à 32K de longueur pour accélérer la cryptographie à clé publique.

Toutes les opérations de chiffrement et d'échanges à l'intérieur de la technologie ID BOX sont donc tous chiffrées de manière hardware.

¹ Authentication Administration Audit
² One time Password = Mot de passe valable une fois
³ Session identifier



L'ADN du Numérique est utilisé dans les produits:

- Device Control: sécurité des Endpoints, intégrité du poste de travail
- Winlogon: OEM Sohos
- SSOX et VPN SSL: OEM Avencis
- Authentification forte ID4YOO: application web, remplace le « login-passeoire » par la reconnaissance d'un équipement que l'utilisateur possède, et non pas d'un équipement spécifique d'authentification
- Question: quels sont les besoins des fontainiers que nous pouvons contribuer à satisfaire?



Tâche	H/M
Tâche 0: Coordination et dissémination scientifique, pédagogique et industrielle	3
Tâche 1: Identification du cadre socio-économique et de ses contraintes	3
Tâche 5: Intégration et validation en environnement équipé et contrôlé	6

Principale activité innovante



- Sous-tâche T5.5 : Gemalto, l'entreprise leader au niveau mondial dans le domaine des cartes à puces et des applications embarquées, propose de réaliser un équipement personnel mobile de sécurité. Ce dispositif s'intégrera et fournira des services à la plate-forme. **Mobilegov, jeune entreprise innovante dans les domaines de la sécurité informatique, maîtrise une technologie d'identification basée sur l'ADN du Numérique (composants d'un périphérique). Elle renforce la sécurité des systèmes tout en rendant la sécurité plus transparente aux utilisateurs finaux. Cette technologie s'intégrera à la plate-forme.**



- D 5.1 : Prototype du dispositif (T0+24)
- D 5.2 : Adaptation et Développement de Web Services sur les Web Services métiers existants (T0+27)
- D 5.3 : Prototype fonctionnel intégrant l'ensemble des développements des partenaires (T0+12, T0+30)
- Dans ces livrables, Mobilegov souhaite apporter sa compétence relative aux contextes associés à l'identité de devices (composants ou ensembles de composants numériques) pertinents.

Pourquoi tout ça?



CONTINUUM

Pour déployer la technologie de l'ADN du Numérique dans de nouvelles applications en informatique ambiante.

En effet, Continuum étudie l'interopérabilité des composants matériels et logiciels dans un environnement où explose la densité des réseaux sans fils et le nombre de composants communicants.

Alors que la tendance est à la généralisation des communications incontrôlées entre objets hétérogènes, *Mobilegov* apporte une solution pour limiter ces communications entre les seuls objets réputés sûrs, en s'appuyant sur son savoir faire à identifier tout objet communicant de manière unique.

Mobilegov est convaincu que sa technologie d'ADN du Numérique a un rôle important à jouer, en complément des étiquettes RFID et des cartes à puces de haute sécurité. Continuum doit permettre:

- 1. de convaincre les partenaires industriels du projet d'adopter la technologie *Mobilegov* pour renforcer leur propre sécurité**
- 2. d'aborder, notamment au cours des manifestations auxquelles le Projet participera, d'autres industriels pour les sensibiliser à la sécurité bâtie sur la reconnaissance des objets numériques**
- 3. grâce aux échanges avec les industriels et les chercheurs du Projet, identifier de nouvelles applications de l'ADN du Numérique, étudier leur potentiel économique et s'il est favorable lancer leur développement soit en interne, soit en collaboration.**

Travail réalisé à ce jour



- Vincent Hourdin, thésard CIFRE partagé entre I3S et Mobilegov, a travaillé à plein temps depuis le début du projet jusqu'à mai 2010 sur la
 - **PRISE EN COMPTE DU CONTEXTE DANS LE CONTRÔLE DES INTERACTIONS ENTRE LES ENTITÉS D'INFORMATIQUE AMBIANTE**
- Ce travail est repris dans sa thèse de Docteur es Sciences Informatique présentée ces jours-ci
- C'est un travail plutôt théorique, que Mobilegov souhaite poursuivre maintenant par les applications pratiques prévues dans le projet.

Thèse V. Hourdin: table des matières



CONTINUUM

- Introduction à l'informatique sensible au contexte
- I État de l'art et analyse des problématiques
 1. L'informatique sensible au contexte
 2. La sécurité en informatique ambiante
 3. Sécurité dans la prise en compte du contexte ou prise en compte du contexte dans la sécurité
- II Contribution
 1. Modèle de prise en compte réactive du contexte dans les interactions
 2. Notre plate-forme expérimentale WComp et le modèle de composition dynamique de services pour dispositifs SLCA/AA
 3. Prise en compte du contexte dans les interactions sur la plate-forme expérimentale WComp
- III Conclusion et perspectives



- **Merci!**
- Plus d'info:
 - www.mobilegov.com
 - Michel.frenkiel@mobilegov .com
 - Tel 06 62 01 28 51