Autorisation Distribuée

FOUQUES Baptiste

11 octobre 2022

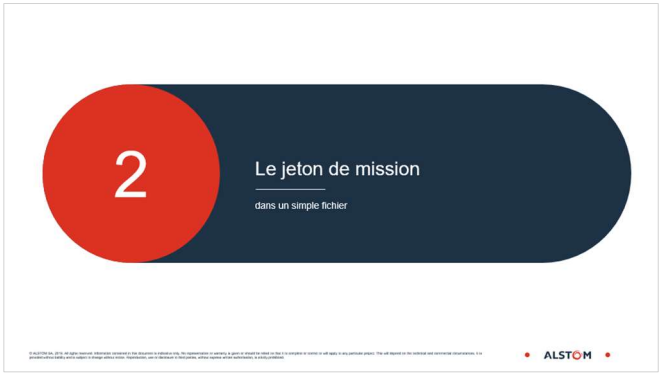
ALSTOM
• mobility by nature •

Autorisation Distribuée

- Identifier les agents
- Authentifier leurs accès
- Autoriser leurs missions

Même sans accès réseau

Programme



1

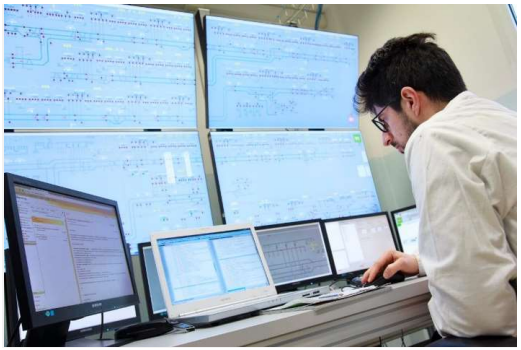
Protéger les missions dans un système industriel

dans un simple fichier

ALSTOM

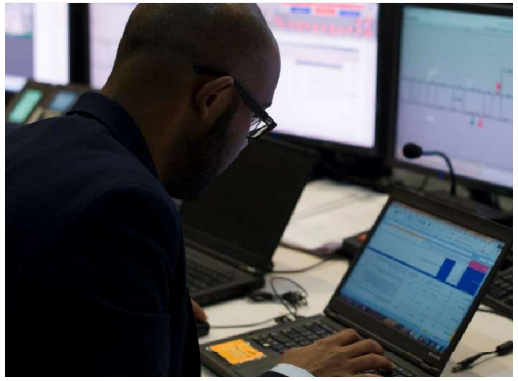
Panne en rase campagne

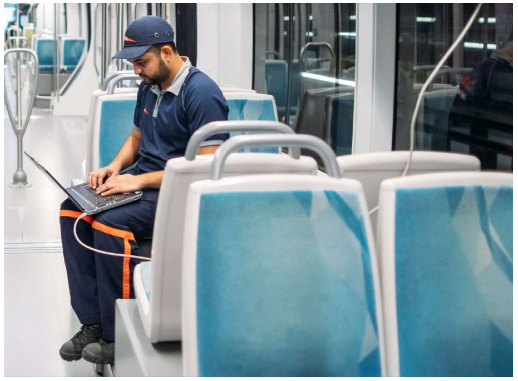
- Le système est bloqué et non communicant.
  Les actions de maintenance standard sont inopérantes. Un spécialiste volant est appelé.
- L'analyse nécessite un accès complet au logiciel du système de contrôle.
- Le responsable informatique crée pour le spécialiste un jeton temporaire.
- Celui-ci le récupère par email.
- Il peut accéder à tout le logiciel du composant et ses traces. Il dépanne le système.



Mise à jour de sécurité sur toute la flotte

- **Mise à jour urgente** d'un composant de sécurité et de ses secrets
- Le responsable sécurité alloue un jeton de mission à tous les agents disponibles.
  Des actions à très forts privilèges, mais la mission est fortement contrôlée (temps, agents, équipement)
- Les agents se déploient sur tous les trains, même sans couverture réseau, et connectent leur jeton de mission sur les équipements cibles.
- Les équipements exécutent les actions du jeton. **Le système est de nouveau sûr.**





2

Le jeton de mission

dans un simple fichier

S’affranchir des contraintes

Gestion des comptes locaux

- **Avantages**
  - Sans couverture réseau

- **Inconvénients**
  - Identification générique
  - Rôles génériques
  - Mise à jour des authentifiants ou droits nécessite une reconfiguration de chaque équipement
  - Révocation d’un utilisateur difficile

Gestion des comptes centralisée
(annuaire, fédération, portail, …)

- **Avantages**
  - Identification individuelle
    - Authentification forte si besoin
  - Gestion des droits fine
  - Mise à jour facile
  - Révocation facile

- **Inconvénients**
  - Forte disponibilité de
    - la couverture réseau
    - du serveur d’authenfication

S’affranchir des contraintes

Objectifs

- **Identification** et authentification, non répudiation
  - Identification individuelle
  - Authentification forte

- **Droits** d’accès
  - Gestion des droits fins
  - Définition et mise à jour facile
  - Révocables

- **Disponible**
  - Pas de contrainte de disponibilité d’infrastructure
    - Réseau
    - Serveur

- **Efficace**
  - En ligne avec les usages des opérateurs

Jeton d’autorisation

De quoi s’agit-il ?

Un fichier

- Facile à transporter et utiliser.
- Ne nécessite pas de couverture réseau, n’est pas *temps réel.*
- Protège les fichiers de mission associés (patchs, confs, …).

Sécurisé

- Sûr, quel que soit le moyen de transport du fichier.
- Protégé contre le vol ou l’usurpation.
- Permet une forte traçabilité de sa création et son usage.

Pour l’opération

- Autorise l’accès aux services de maintenance de l’équipement.
- Met à jour l’équipement et sa configuration.
- Exécute des actions sur l’équipement.
- Récupère les traces de l’équipement.

Description technique du jeton

Qui

L'agent autorisé à effectuer la mission

Où

Sur quels sous-systèmes ou équipements

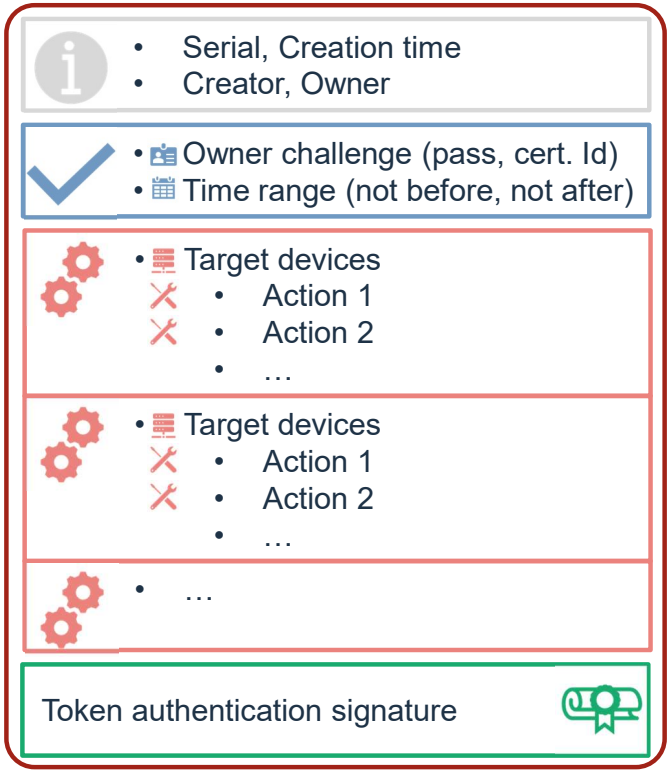
Quand

Durée de la mission

Optional : one shot

Quoi

Quelles actions



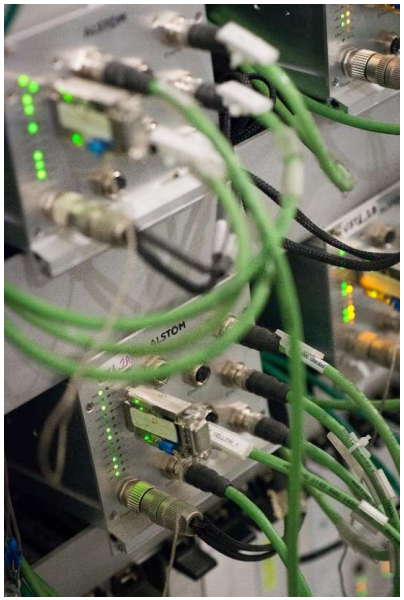
ALSTOM

La journée d’un agent

```
[etroche@windows-156]$
ssh sectoken@comet1.coradia26

Executing token mission ...
[X] Downloading file from ftp://windows-156/srv/mission/conf-evc-com1.tar.gz
[X] checking checksum: sha256:13d1b96c7582bb13b4011b29eb50beee1bc2e8b87f2b3a0d8e7f434f4d67acfc
[X] Checking file authenticity against authority certificate – Öskjuhlíð Root 1
[X] Executing script: /tmp/conf-evc-com1/hard-fix-comet1-2022-11-06-v22.sh
[X] Sending file: /tmp/conf-evc-com1/exec.logs to ftp://windows-156/srv/mission-log/com1-cor26/
[X] Opening maintainer level bash

[etroche – maint@comet1.coradia26]$
```

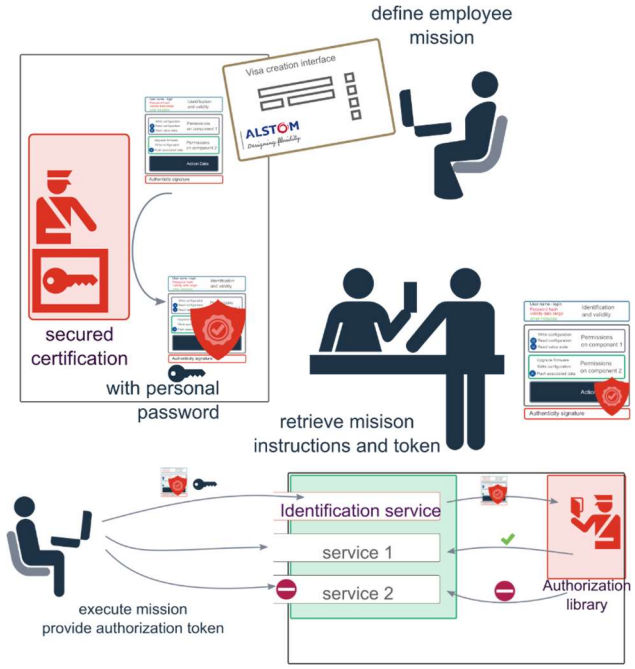
Öskjuhlíð Railway Compagny -- EVC v.2.3.0

```
[etroche@windows-156]$ ssh sectoken@comet1.coradia26
etroche’s token path [file://usb/et.token]:
ftp://windows-156/srv/mission/conf-evc-com1.tar.gz
[X] checking checksum: sha256:13d1b96c7582bb13b4011b29eb50beee1bc2e8b87f2b3a0d8e7f434f4d67acfc
[X] Checking file authenticity against authority certificate – Öskjuhlíð Root 1
[X] Executing script: /tmp/conf-evc-com1/hard-fix-comet1-2022-11-06-v22.sh
[X] Sending file: /tmp/conf-evc-com1/exec.logs to ftp://windows-156/srv/mission-log/com1-cor26/
[X] Opening maintainer level bash

[etroche – maint@comet1.coradia26]$
```



L’infrastructure d’autorisation

- Un serveur de certification
  - Interface de définition des missions
  - Un serveur de sécurité pour la génération et signature du jeton.
- Pour chaque agent
  un moyen de transport du jeton (usb, 4g, réseau, …)
- Dans chaque équipement,
  une bibliothèque d’autorisation
  - Lié à une interface standard (pam pour Linux)
  - Associé à un moteur d’exécution
- À chaque application d’administration
  module d’interface ↔ api d’autorisation.

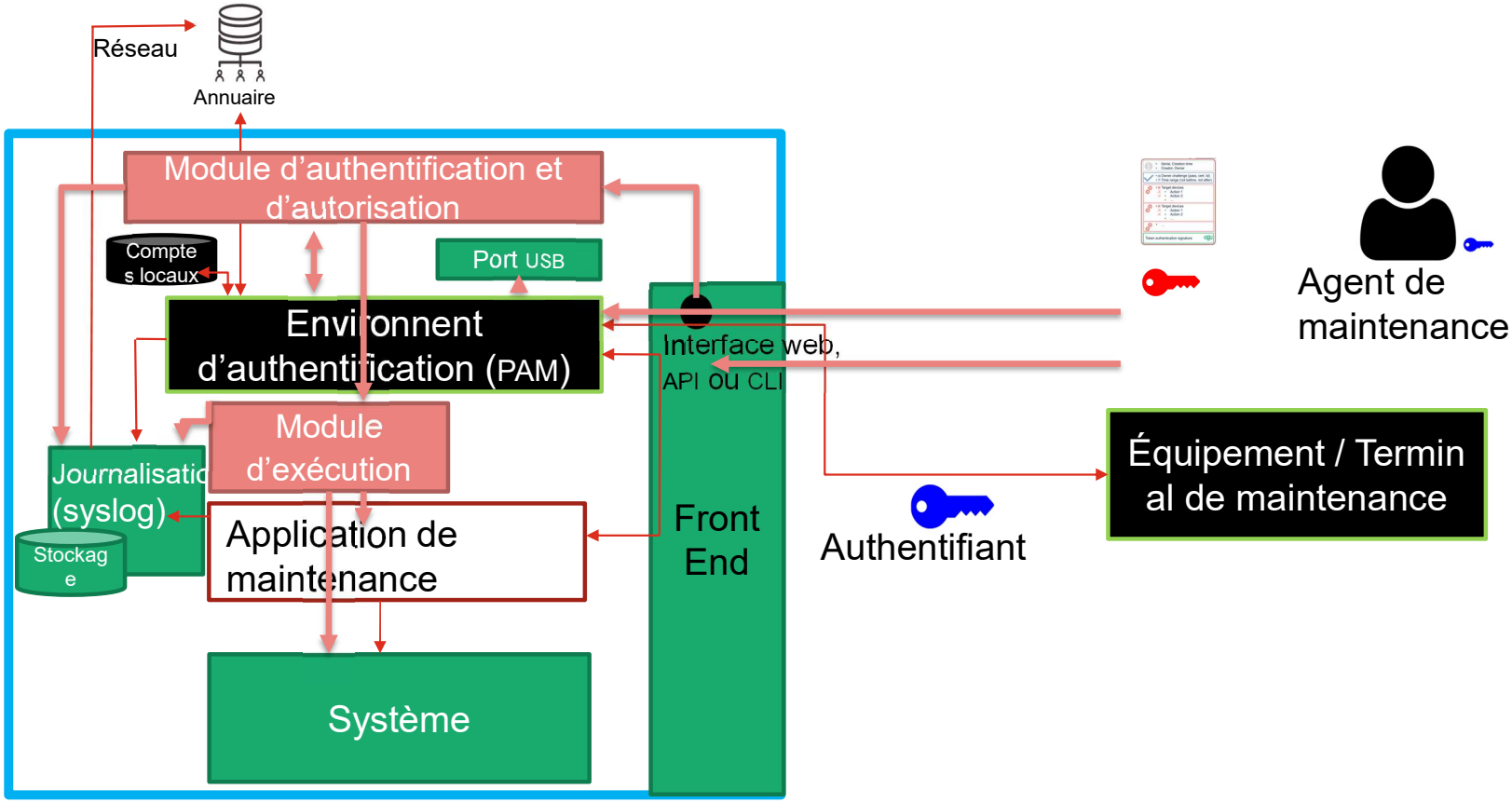


La couverture réseau n’est pas nécessaire.

3

Développements chez Alstom

Prototype — Architecture



Prototype — Format du jeton

- **Description métier**
  - Lisible
  - Mature
  - Limite la surface aux vulnérabilités
- ⟶ Description Json

- **Certification du jeton**
  - Standard et éprouvé
  - Facilitant la gestion de vulnérabilités
- ⟶ Certification pkcs 7

Format hybride Json encapsulé dans un PKCS 7.

Prototype — Format du jeton

Data:

```
basicData:
  missionID: UUID
  tokenID: UUID
  creator: userID
  creationTime: utcTime
  description: String
ownerData:
  owner: userID
  credentials: List(
```

combinaison of different ways of authentification, like Password + Certificate number

```
    type: String,
    value: String   )
 validityDate:
  notBefore: utcTime
  notAfter: utcTime

mission: List(
  device: String,
```

DNF of device attributes

```
  actions: List(
   ACTION   ) )
```

```
{
"basicData": {
  "missionID": "123e4567-e89b-12d3-a456-426652340043",
  "tokenID": "123e4347-e29b-54d7-a378-781901340000",
  "creator": "john.doe@mail.com",
  "creationTime": "2021-04-24T15:20+01:00",
  "description" : "…"},
"ownerData": {
  "owner": "isabelle.michu@mail.com",
  "credentials": [{
  "type": "argon2dHashedPassword",
  "value": "$argon2i$v=19$m=80,t=10,p=10$ZmVya2Z…"}]},
"validityDate": {
  "notBefore": "2021-03-24T16:00+01:00",
  "notAfter": "2021-09-30T20:00+01:00"},
"mission": [{
  "device": "CC_42 + CC_56 + train_22 * CC",
  "actions": [{
    "actionType": "Download&Execute",
    "executionFileLocation": "file://…/download_and_execute_test.sh",
    "executionFileFinalLocation": "/run/…/",
    "executionUser": "net_maintainer",
    "executionLocation": "/home/vagrant/cc/",
…
  }]}
```


ALSTOM

Jeton — Choix clés

Authentification du propriétaire

S'assurer que l'utilisateur est le propriétaire

- **Difficulté :** ne pas créer de contrainte de **confidentialité** sur le jeton.
- **Proposition :** séquence de **défis d'authentification** portés par le jeton :
  - un mot de passe fortement haché ; *(quelque chose que tu connais)*
  - un certificat épinglé, une clé publique ; *(quelque chose que tu possèdes)*
  - une donnée biométrique (!?) ; *(quelque chose que tu es)*
  - …?

```
"ownerData": {
  "owner": "isabelle.michu@mail.com",
  "credentials": [{
  "type": "argon2dHashedPassword",
  "value": "$argon2i$v=19$m=80,t=10,p=10$ZmVya2Z…"}]},
```

Jeton — Choix clés

Identification des équipements cibles

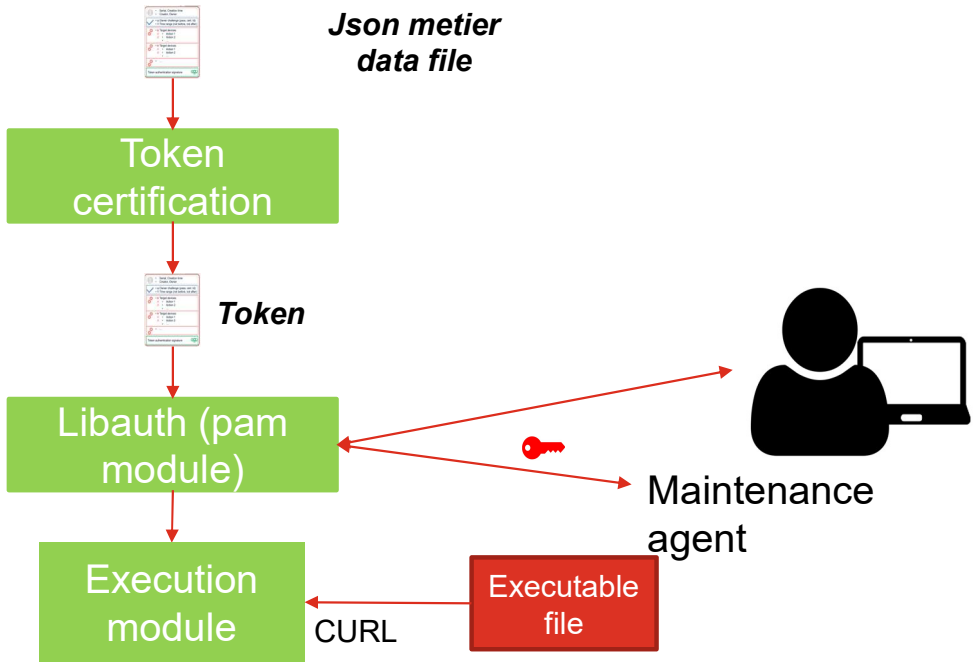
Identifier l'ensemble des équipements pour une séquence d'actions.

- **Difficulté :** Identifier les équipements **unitaires** et des **groupes** d'équipements.
- **Proposition :** Liste disjonctive **DNF** (liste de « ou » de « et ») d'**attributs** d'équipement.
  - Les équipements portent des attributs d'identification (identifiant unique, localisation, projet,…)
    CC_58, *CC*, *Cab_1*, *Train_22*, *Projet_Rx*, *Sys_Sacem*
  - DNF dans le jeton
    CC_42 ∨ *CC_56* ∨ *(Train_22* ∧ *CC)*

```
"mission": [{
  "device": "CC_42 + CC_56 + train_22 * CC",
  "actions": [{
```

Prototype — Développement

- 3 modules en Rust
- Certification du jeton (serveur)
- Libauth (embarqué, pam) authentification et autorisation
- Daemon d'exécution (embarqué) exécute les actions



l’Autorisation Distribuée ne fournit pas …

- **Un protocole d’administration**
- La distribution du jeton
  - Le jeton (un fichier) doit être amené sur l’équipement cible
    via un élément physique (clé usb) ou un serveur local (réseau point à point avec l’équipement de maintenance par exemple)
- La révocation
  - Les contrôles (utilisateur, validité temporelle et spatiale) limite le recours à la révocation
  - Nécessite une distribution d’une règle de révocation, donc une distribution (réseau, apport manuel etc.)
  - Pourrait être mis en œuvre au cas par cas
    chaque jeton possédant un identifiant unique

4

Les prochaines étapes de l’ Autorisation Distribuée

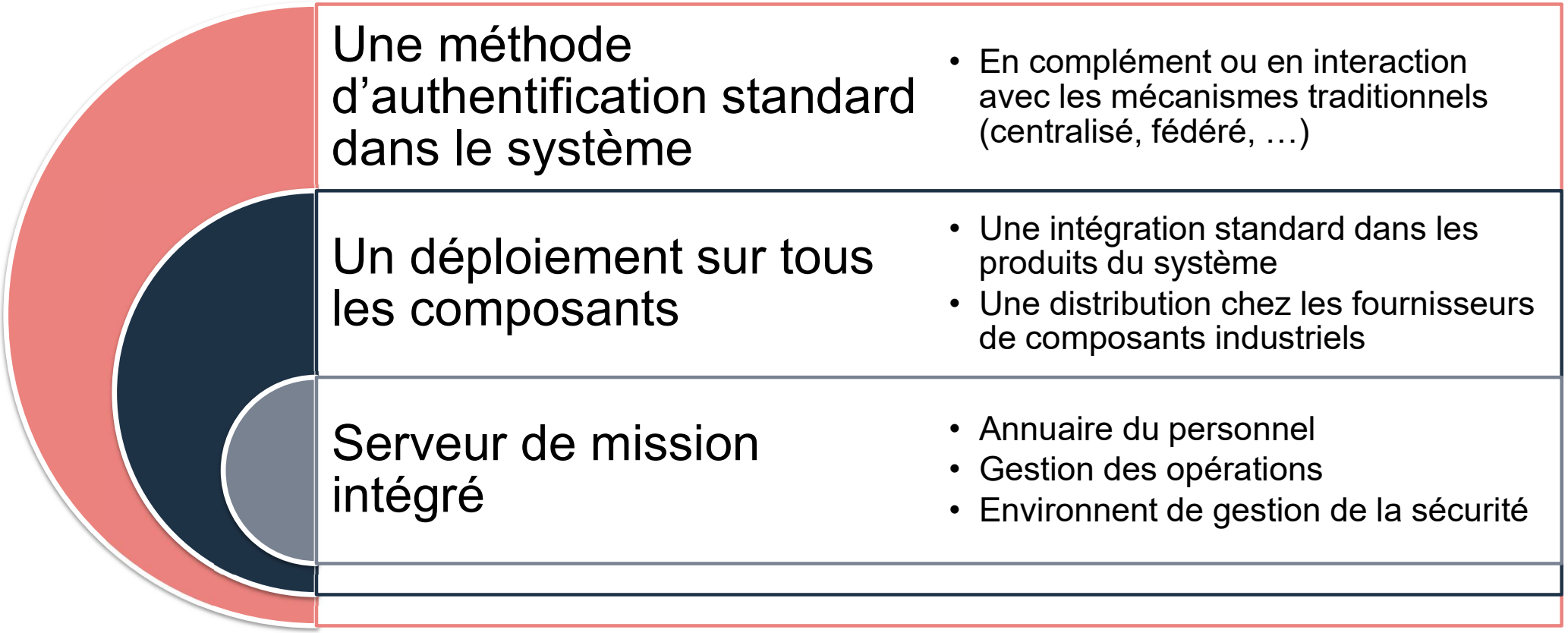
Aujourd’hui, Un développement

- Axé vers fonctions et rôles spécifiques

  - Procédures « bris de glace »
  - Retour en configuration « d’usine » d’un produit en service
  - Rôles et interfaces non fonctionnelles du produit
    - Activation des interfaces de mise au point
    - Ouverture de ports normalement restreints (usb, lien série, etc.)
    - Interface cli administrateur produit (compte « product engineer »)

- En co-définition avec des fournisseurs

Une intégration dans le système



ALSTOM

Solution ouverte

Mécanisme libre
-Concept publié
-Intérêt partagé

Publications et Brevet ouvert

Spécification ouverte
-Format du jeton ouvert et évolutif
-Interfaces et actions

Travaux *open source*

Mise en œuvre de référence
-Pour l'embarqué
-Tourné vers la sécurité

Disponible pour intégration

Finalement, quels avantages ?

Sécurité en l'absence de réseau :

– fournit une authentification forte ;

– contrôle des actions ;

– assure la non répudiation.

Flexibilité pour toutes les industries :

– adapté aux missions ;

– adaptable aux transmissions disponibles ;

– contrôlant les actions à fort privilège.

Une développement qui nécessite des partenaires : utilisateurs, intégrateurs, fournisseurs.

Autorisation Distribuée

Pour contribuer

développeur, fournisseur, intégrateur, utilisateur

cas d'usages, spécification, développement, intégration.

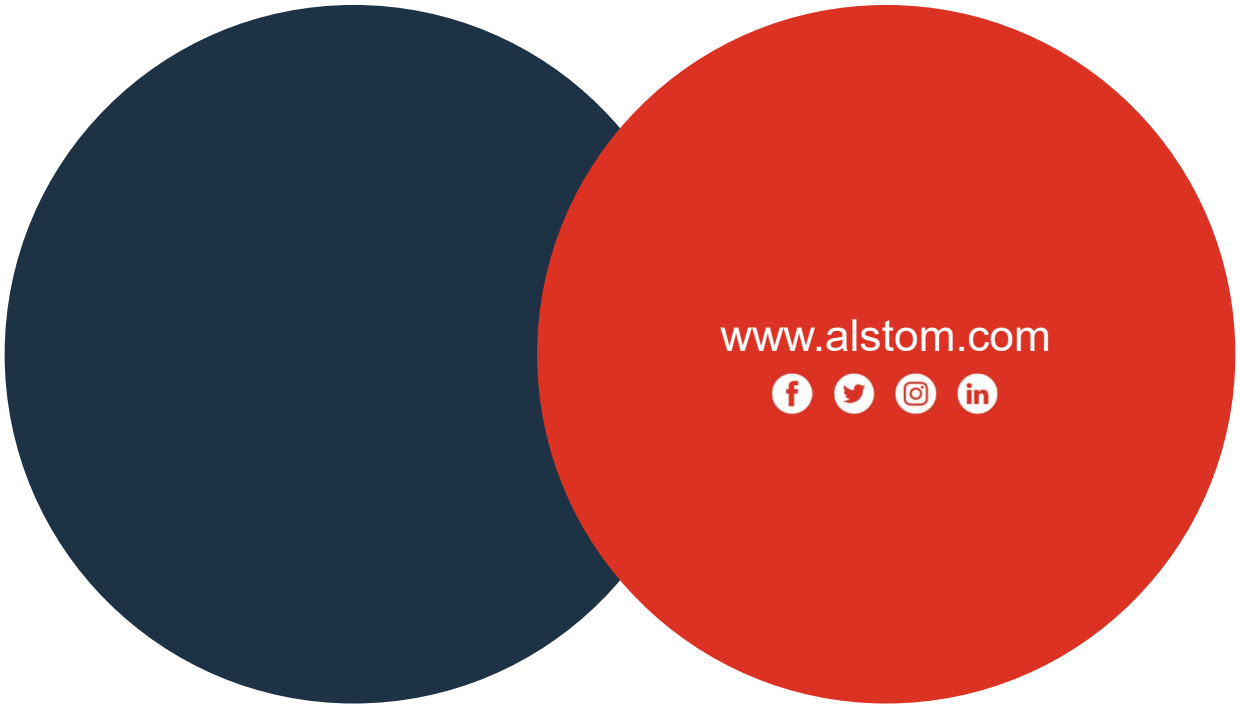
Contacter Baptiste Fouques :

baptiste.fouques@alstomgroup.com
+33 4 81 65 71 62

Inventeurs :
Baptiste Fouques,
Xavier Degenève.

Contributeurs Alstom :
Jean-François Gillot,
Thibaut Avenin,
Florent Bernard.

ALSTOM



ALSTOM

• mobility by nature •

Référence des Brevets

- Référence : EP3477517B1, FR3073058B1, US11048806B2, …
- Titre : Procédé de contrôle d'accès à une zone sécurisée d'un équipement, programme d'ordinateur, support informatique et équipement associés
- Title: Method for controlling access to a secure area of a device, associated computer program, computer medium and device
- Inventeurs : Xavier Degenève, Baptiste Fouques

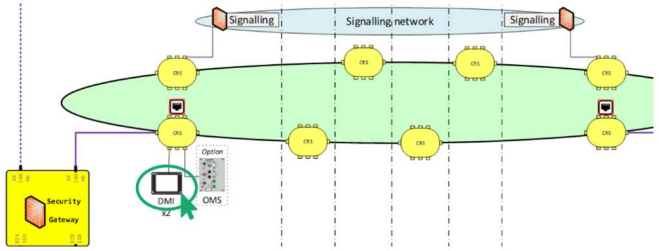
Travaux semblables

- Iec 62351-8 Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance
  - « Jetons d’accès » rbac, quatres profils x.509 extensions, x.509 attributs, jwt et radius.
- Biscuits
  - Jetons d’autorisation définis sur série de « faits » spécifiés en datalog.
  - Conçu à destination des architecture web micro-services
- Mise en œuvre ad-hoc chez divers industriels

Token usage

Interface de gestion de missions

On train :
- any
- 2 7 16



To agent :
- any security maintainer
-
  - QUIRINO Teodor
  - ZAHIDE Fermín
  - ETHELDREDA Melant

Selected targets :
- dmi1.train2.prj_mla
- dmi2.train2.prj_mla
- dmi1.train7.prj_mla
- dmi2.train7.prj_mla
- dmi1.train16.prj_mla

Validity :
- From : Today
- To : 2020-12-24
- (duration : 2 months)

Mission actions :
1. Download & install
   - from : https://oms/repo/file1.tar.gz
   - hash : 32a1d3e088d241d8-af77-05fe5ef8ce15
2. Download & exec
   - from : https://oms/repo/file_to_exec.sh
   - hash : 2fe6e567718546cfa1e08f20224abad2
3. Login to web
   - role : security administrator

Detailled Options **Add Mission** **Generate Token**

Mission actions

- Download and install
- Download a file from a specified url
  - file://media/usb/file_dmi_v2.tar.gz
  - https://oms.unit1/repo/file_dmi_v2.tar.gz
  - sftp://192.168.1.1/srv/file_dmi_v2.tar.gz
- Control file authenticity and integrity
- Place the file at expected location
- Install the file
  - extract archive and update file attributes

Action configuration

- File location
  - Certificate or public key of file server
- File integrity
- File final location
- File final attributes
  ownership, access rigths, security attributs

Mission actions

- Download and execute
- Download a file from a specified url
  - file://media/usb/exe_dmi_v2.sh
  - https://oms.unit1/repo/exe_dmi_v2.sh
  - sftp://192.168.1.1/srv/exe_dmi_v2.sh
- Control file authenticity and integrity
- Place the file at expected location
- Execute file

Action configuration

- File location
  - Certificate or public key of file server
- File integrity
- File execution context
  - Execution location
  - Execution system user
  - Execution execution output location

Mission actions

- Open maintenance interface
- Identify the agent
- Grant access
  to the maintenance service
- Grant actions rights or role
  in the maintenance service

Action configuration

- Maintenance service
  - Web interface, file transfert, command line
- Role to be used in the service

Mission actions

- Retrieve data
- Upload files from the device
  - /var/log/system.log.*
- to a specified url
  - file://media/usb/logs/dmi/
  - https://oms.unit1/repo/log/dmi/
  - sftp://192.168.1.1/srv/log/dmi/

Action configuration

- Files to upload
- Upload location
  - Certificate or public key of file server
- System user to be used to read the files