THOMSON TECHNICOLOR grass valley RCA THOMSON

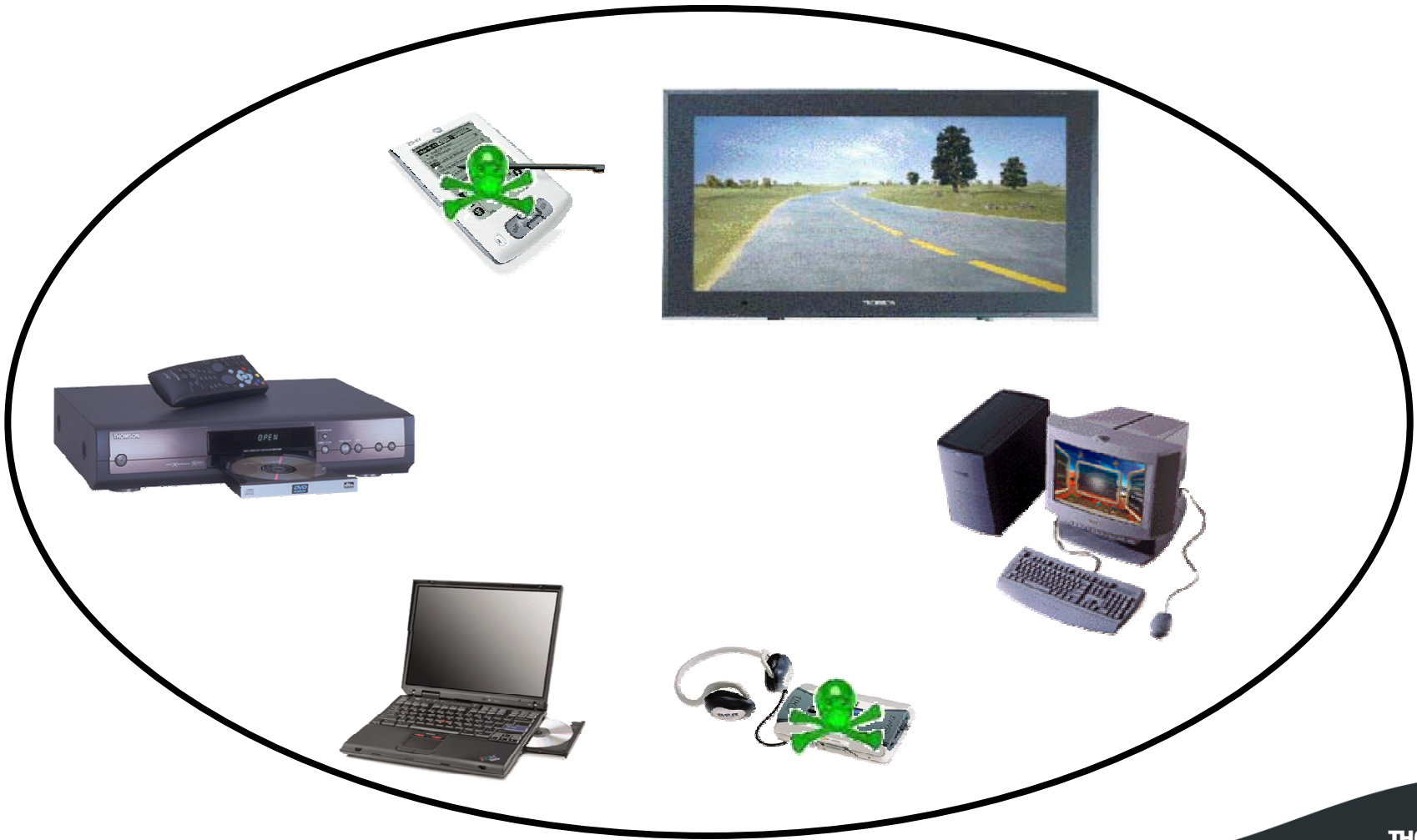
Gestion Sécurisée de Groupes de Dispositifs dans les Réseaux Domestiques

THOMSON Supélec N. Prigent THOMSON SECURITY LABORATORY J.-P. Andreaux THOMSON

Réseaux Domestiques

- Hétérogénéité
- Connectivité erratique
- Pas de point central
- Pas d'administrateur compétent

Frontière Floue

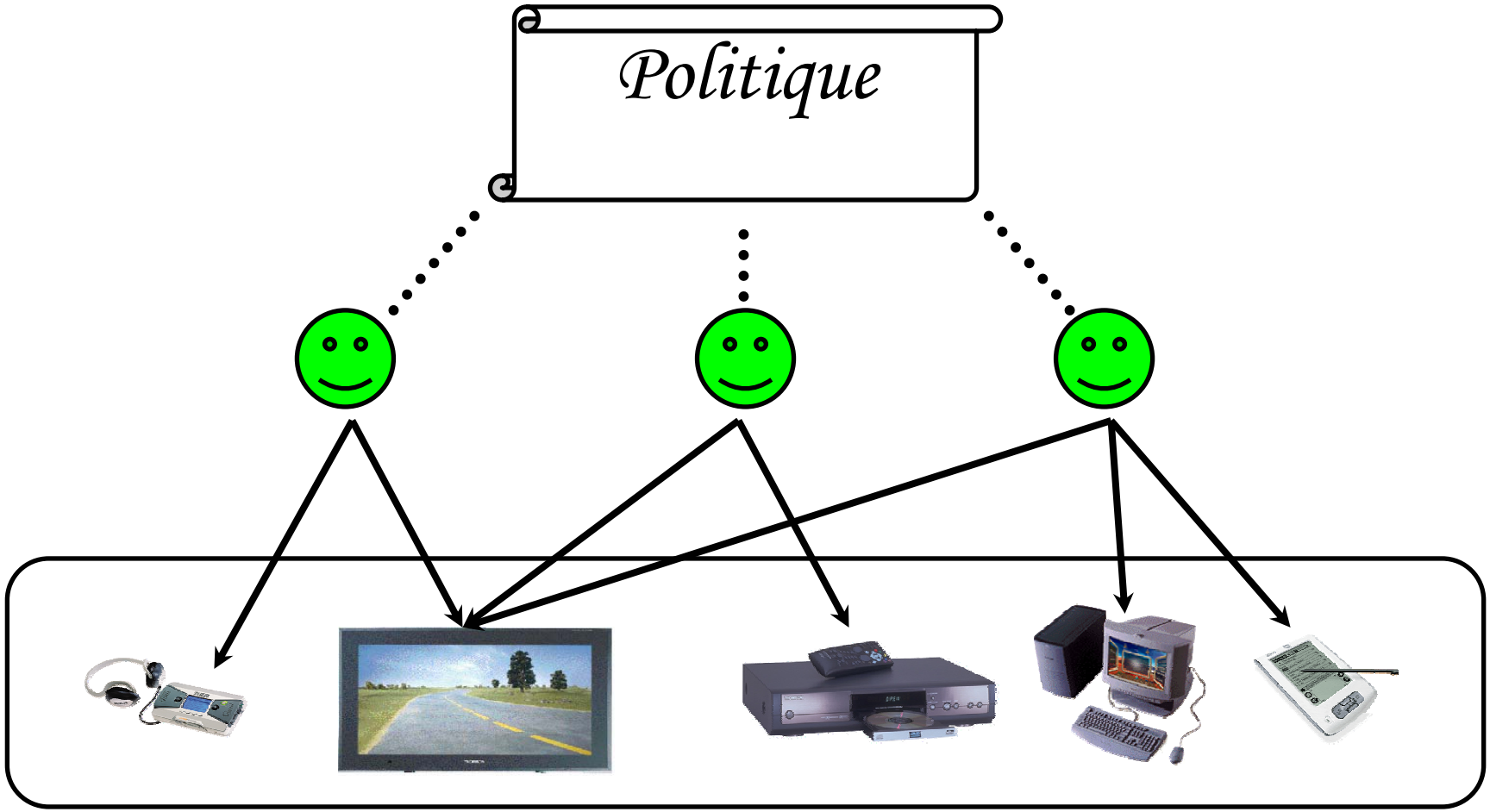


THOMSON TECHNICOLOR grass valley RCA THOMSON

Communautés Durables Sécurisées

THOMSON SECURITY LABORATORY

Communautés Durables Sécurisées 5

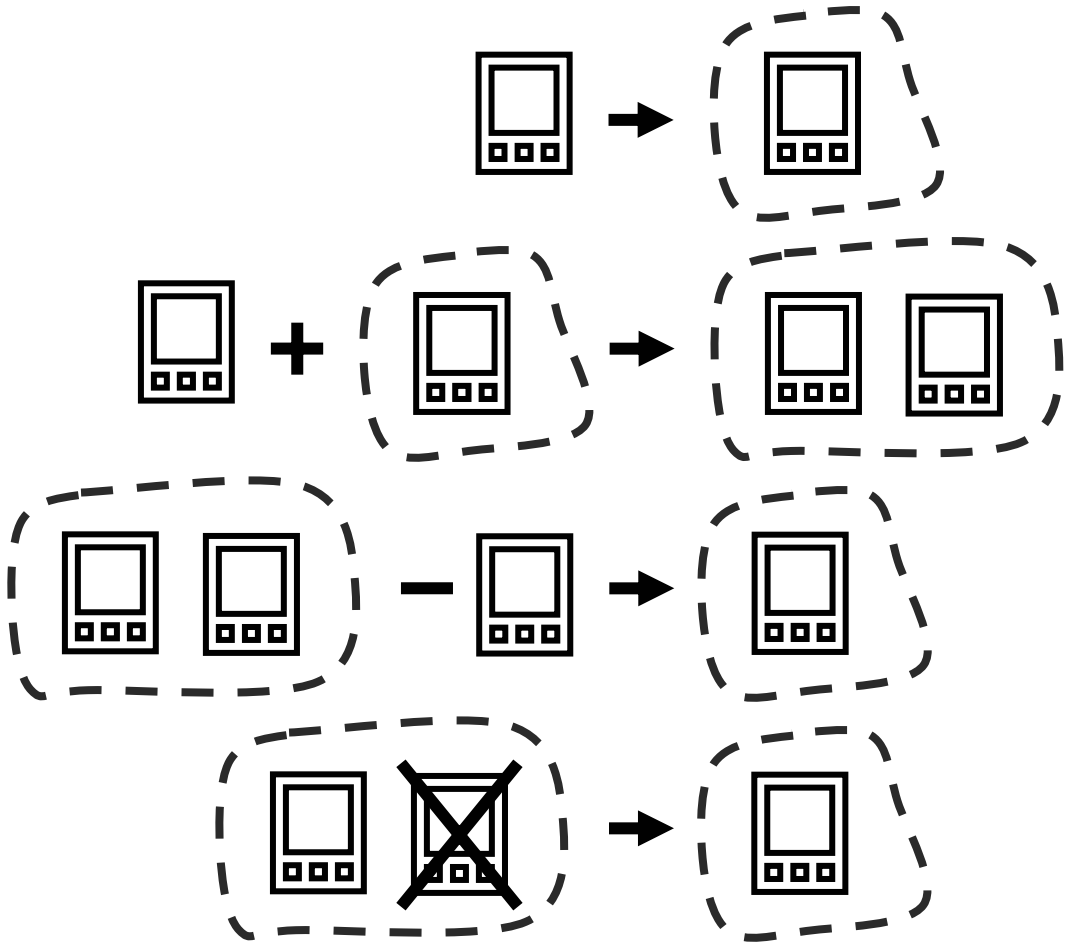


Services de Sécurité

- **Authentification des dispositifs**
- **Confidentialité des communications**
- **Authenticité des communications**
- **Évolution sécurisée de la communauté**

Opérations d'évolution

- **Initialisation**
- **Insertion**
- **Retrait**
- **Bannissement**



Contraintes Particulières

- **Aucun dispositif spécifique pour sécuriser les communications**
- **Aucun dispositif spécifique pour gérer l'évolution**
- **Cohérence des connaissances locales**

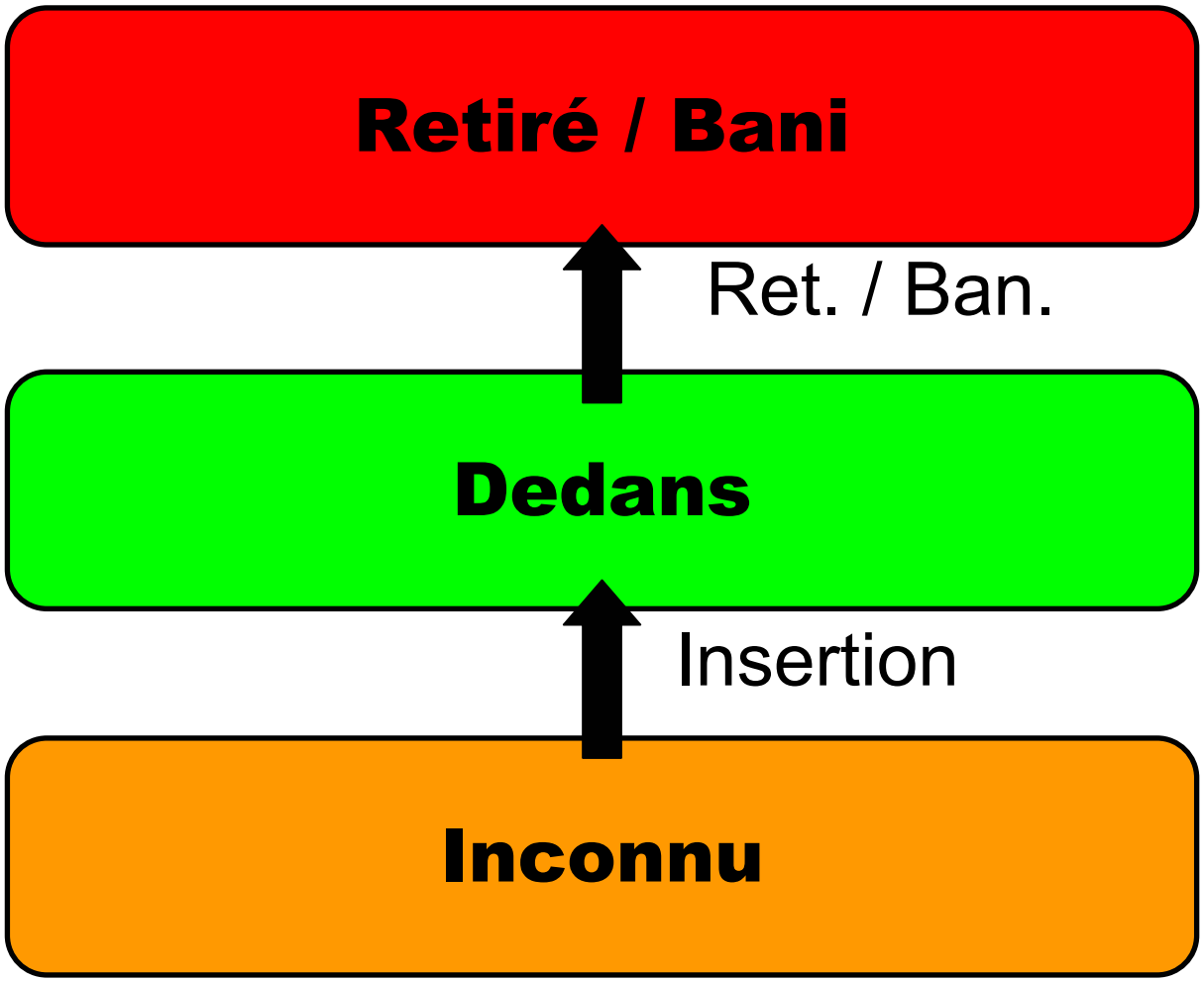
Notre mécanisme distribué

THOMSON SECURITY LABORATORY

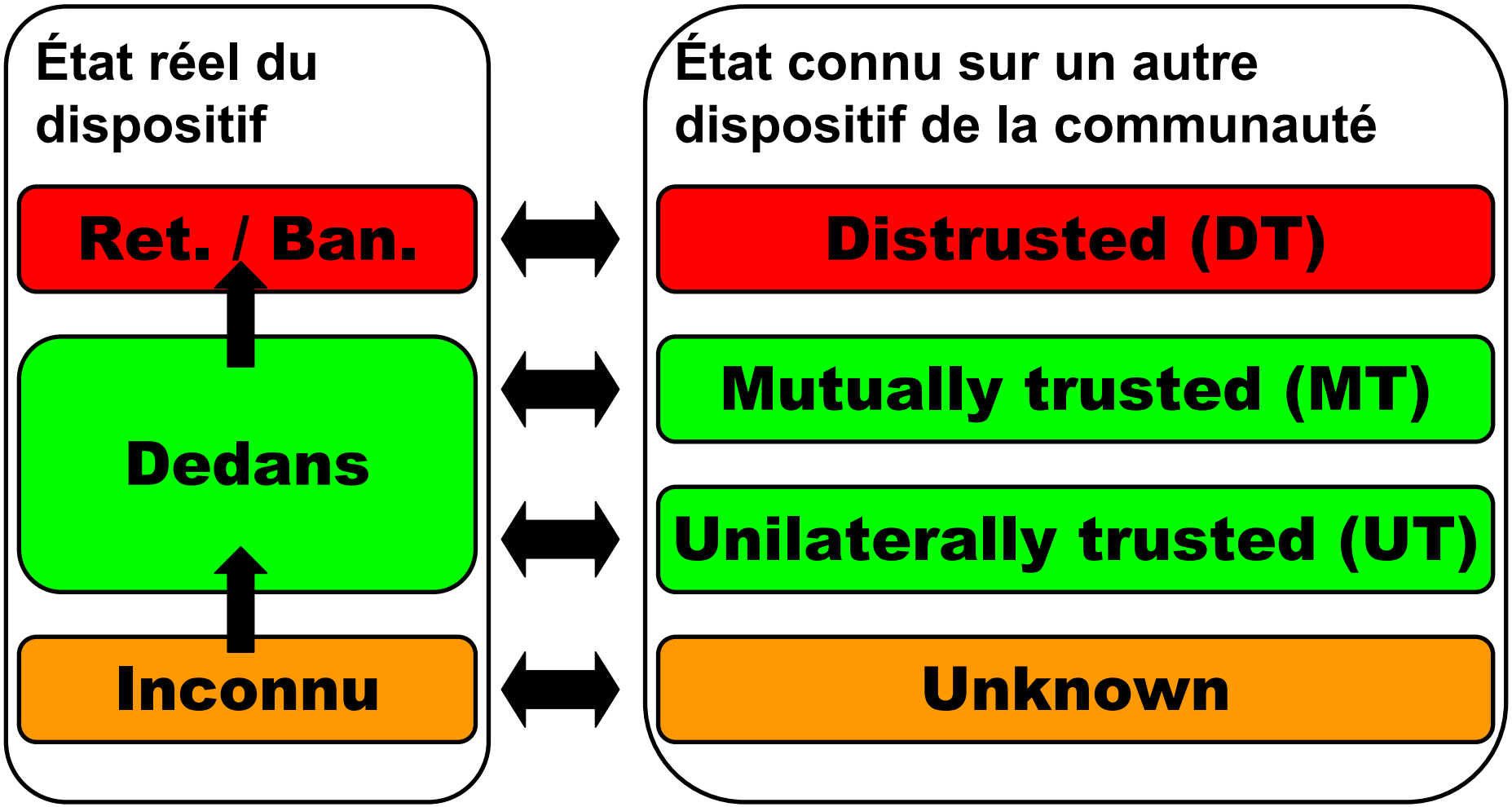
Notre mécanisme distribué

- **Chaque dispositif gère localement sa connaissance de la communauté**
- **L'autorité initie localement les évolutions**
- **L'échange d'informations entre dispositifs maintient la cohérence des connaissances locales**

État possible d'un dispositif



Connaissance locale

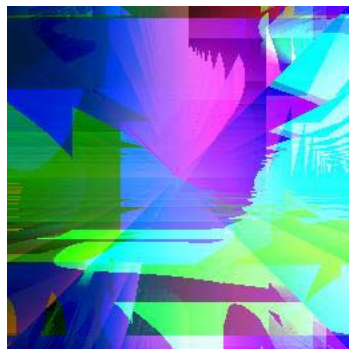


Identité Prouvable

- **Difficile à usurper**

```
4E203CBC67
4B96F6B02B
D33F316DA5
3F06631F86
```

- **Simple à vérifier**



- **Permet de chiffrer et de signer**

Sources du Random Art : http://gs2.sp.cs.cmu.edu/art/random/

THOMSON TECHNICOLOR grass valley RCA THOMSON

Opérations d'évolution

THOMSON SECURITY LABORATORY

Initialisation d'un dispositif

Identité Prouvable

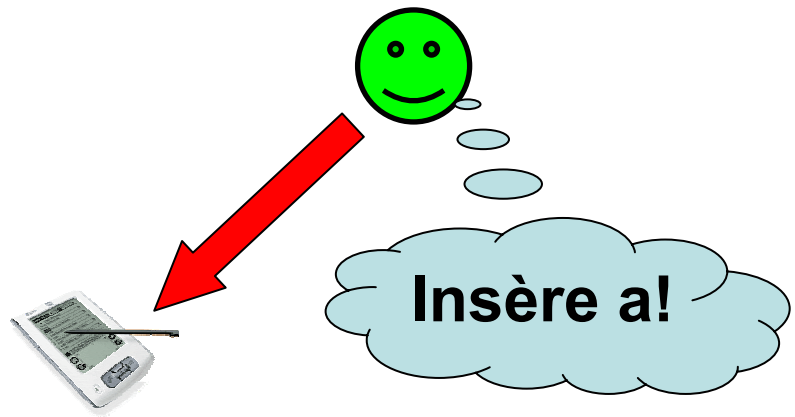
Pub.

Priv.

Dispos.

As MT

Insertion d'un Dispositif



b is in com(a)

$\mathcal{A}$

Prov. ID a

a a

Devices

a As MT

b As MT

Prov. ID b

b b

Devices

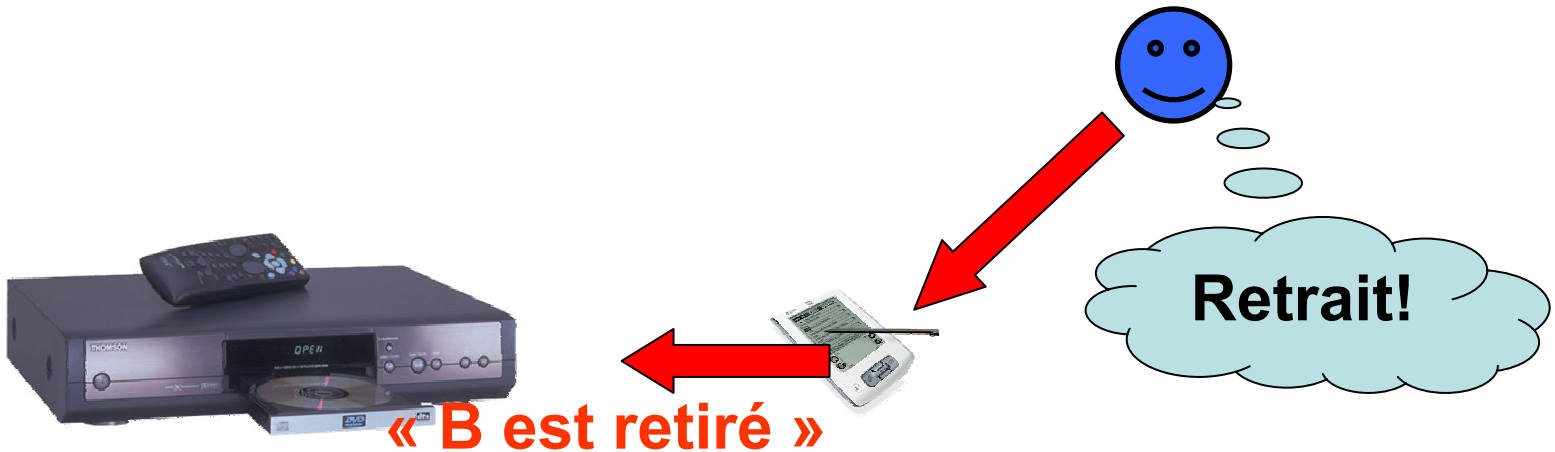
b As MT

a As MT

a is in com(b)

$\mathcal{B}$

Retrait d'un Dispositif



Bannissement d'un Dispositif

Prov. ID a

Devices

As MT

As DT

Synchronisation entre Dispositifs

Prov. ID a

a a

Devices

a As MT

c As MT

b As DT

d As MT

e As UT

Prov. ID c

c c

Devices

c As MT

a As MT

b As DT

d As UT

e As UT

c is in com(a) $\mathcal{A}$

a is in com(d) $\mathcal{D}$

d is in com(e) $\mathcal{E}$

Synchronisation entre Dispositifs

c is in com(a) $\mathcal{A}$

a is in com(d) $\mathcal{D}$

d is in com(e) $\mathcal{E}$

Prov. ID c

c c

Devices

c As MT

a As MT

b As DT

d As UT

e As MT

c is in com(a) $\mathcal{A}$

a is in com(d) $\mathcal{D}$

d is in com(e) $\mathcal{E}$

Prov. ID e

Devices

e As MT

d As MT

c As MT

Supélec

THOMSON

Conclusion

- **Mécanisme distribué de gestion de groupes**
- **Compatible avec les réseaux domestiques**
- **Utilisateur limité à l'expression de l'autorité**

Travaux Futurs

- **Interactions trans-frontalières**

- **Autorités aux politiques divergentes**