Certifications sécuritaires : genèse et fonctionnement

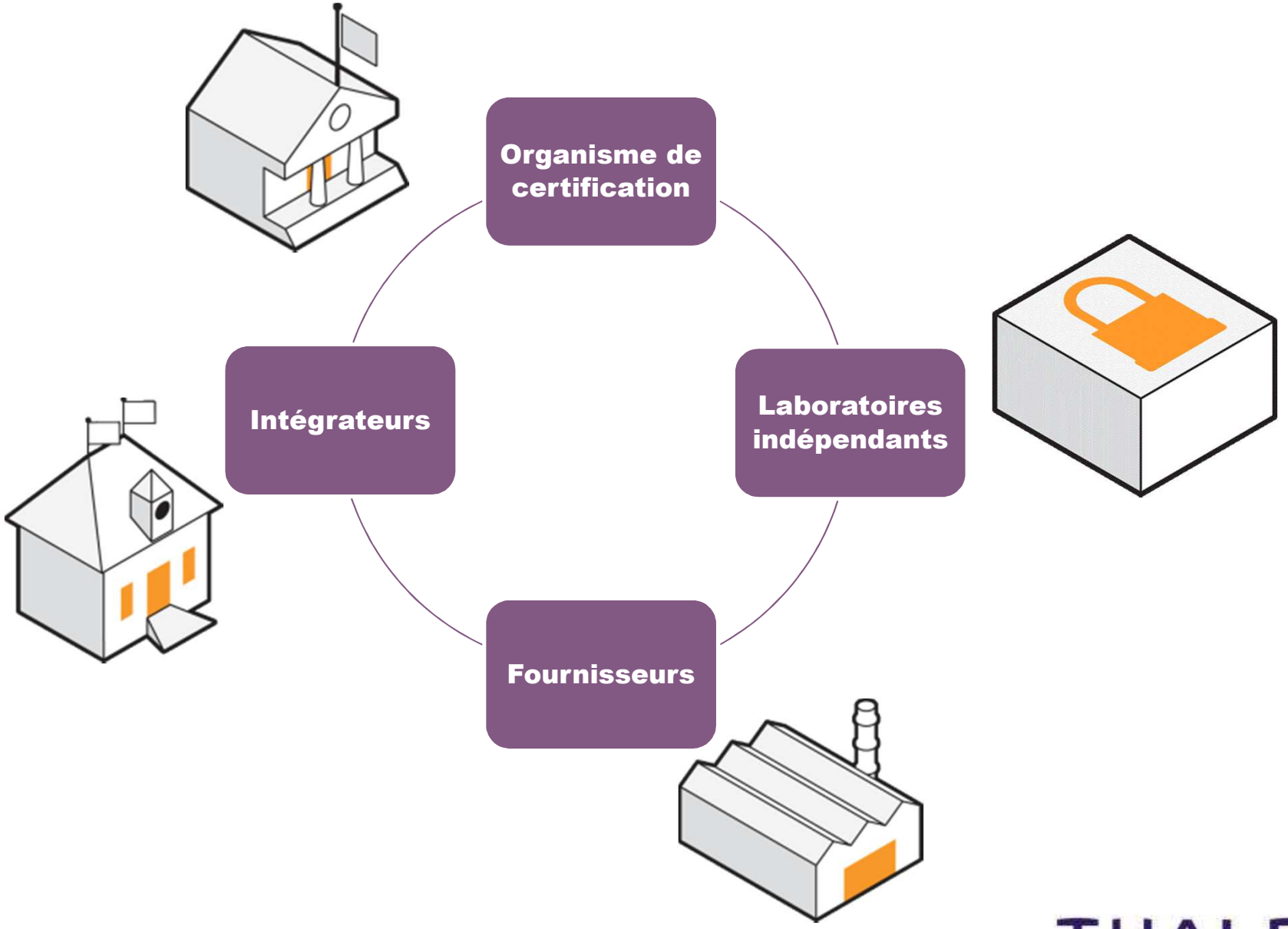
Nathalie FEYT / Thales Communication & Security

THALES

Bénéfices des certifications sécuritaires

- ✓**Assurance pour les utilisateurs du produit**
- ✓ **Mesure et Maîtrise du risque**
- ✓ **Comparaison possible des produits**
- ✓ **Partage des responsabilités**

Acteurs d'un schéma de certification



Une réponse à un besoin étatique

Etre en mesure de qualifier le niveau de sécurité des produits qui peuvent être utilisés et approvisionnés par les administrations ou instances gouvernementales (préoccupation d'achat « procurement »)

Deux standards émergent dans les années 80

- ✓ **FIPS poussés par les Etats Unis, uniquement pour les modules crypto (FIPS140-2), standardisé par le NIST**
- ✓ **CC (Common Criteria) poussés en Europe et standardisés à l'ISO sur la base d'une CEM: « Common Evaluation Methodology »**

Critères communs: reconnaissance internationale EAL2

Evaluation assurance level

EAL7: Formally Verified Design and Tested

EAL6: Semiformally Verified Design and Tested

EAL5: Semiformally Designed and Tested

EAL4: Methodically Designed, Tested, and Reviewed

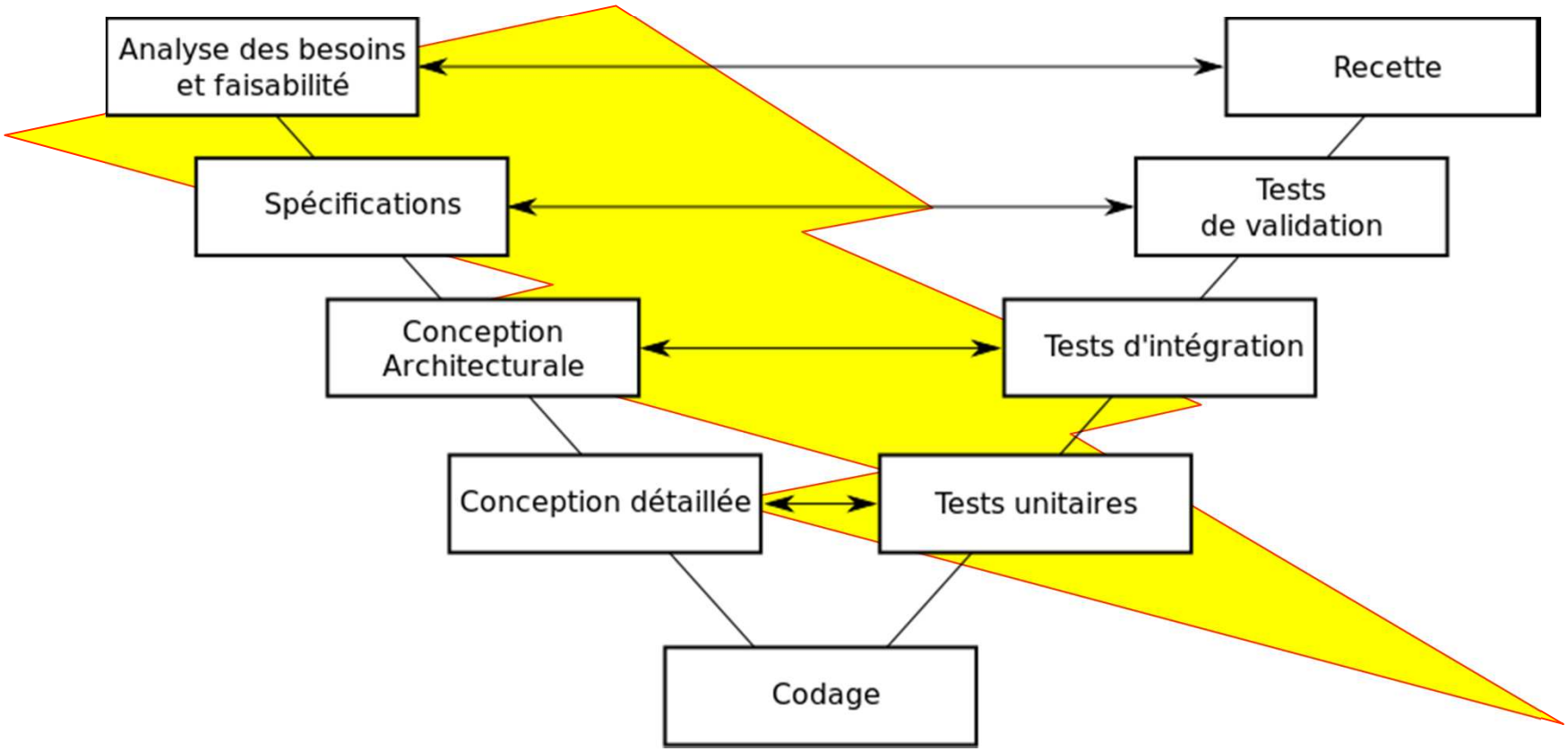
EAL3: Methodically Tested and Checked

EAL2: Structurally Tested

EAL1: Functionally Tested

Common Criteria

Activités d'évaluation Critères Communs



Reconnaissance européenne EAL4

Le SOGIS, senior official group information systems security, créé en réponse de la décision de l'EU Council en 1992 (92/242/EEC) de coordonner la déclinaison de directives européennes comportant des aspects liés à la sécurité des technologies de l'information.

Allemagne, BSI - Bundesamt für Sicherheit in der Informationstechnik (Office fédéral pour la sécurité des technologies de l'information)

Autriche, Bundeskanzleramt (Chancellerie fédérale)

Espagne, CCN - Organismo de Certificación de la Seguridad de las Tecnologías de la Información Centro Criptológico Nacional (Centre national de cryptologie / Organisme de certification de la sécurité des technologies de l'information)

Finlande, FICORA - Viestintävirasto (Autorité de régulation des communications)

France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information

Italie, OCSI - Organismo di Certificazione della Sicurezza Informatica (Organisme de certification de la sécurité informatique)

Norvège, SERTIT - Sertifiseringsmyndigheten for IT-sikkerhet i produkter og systemer (Autorité nationale de certification de la sécurité des technologies de l'information)

Pays bas, NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations (Agence nationale de la sécurité des communications)

Royaume uni, CESG - Communications-Electronics Security Group (Groupe sur la sécurité des communications électroniques)

Suède, FMV - Försvarets Materielverk (Administration des matériels de défense)

THALES

Fonctionnement du schéma public français

En France, les CC sont utilisés et prescrits par Décret pour les qualifications de produits:

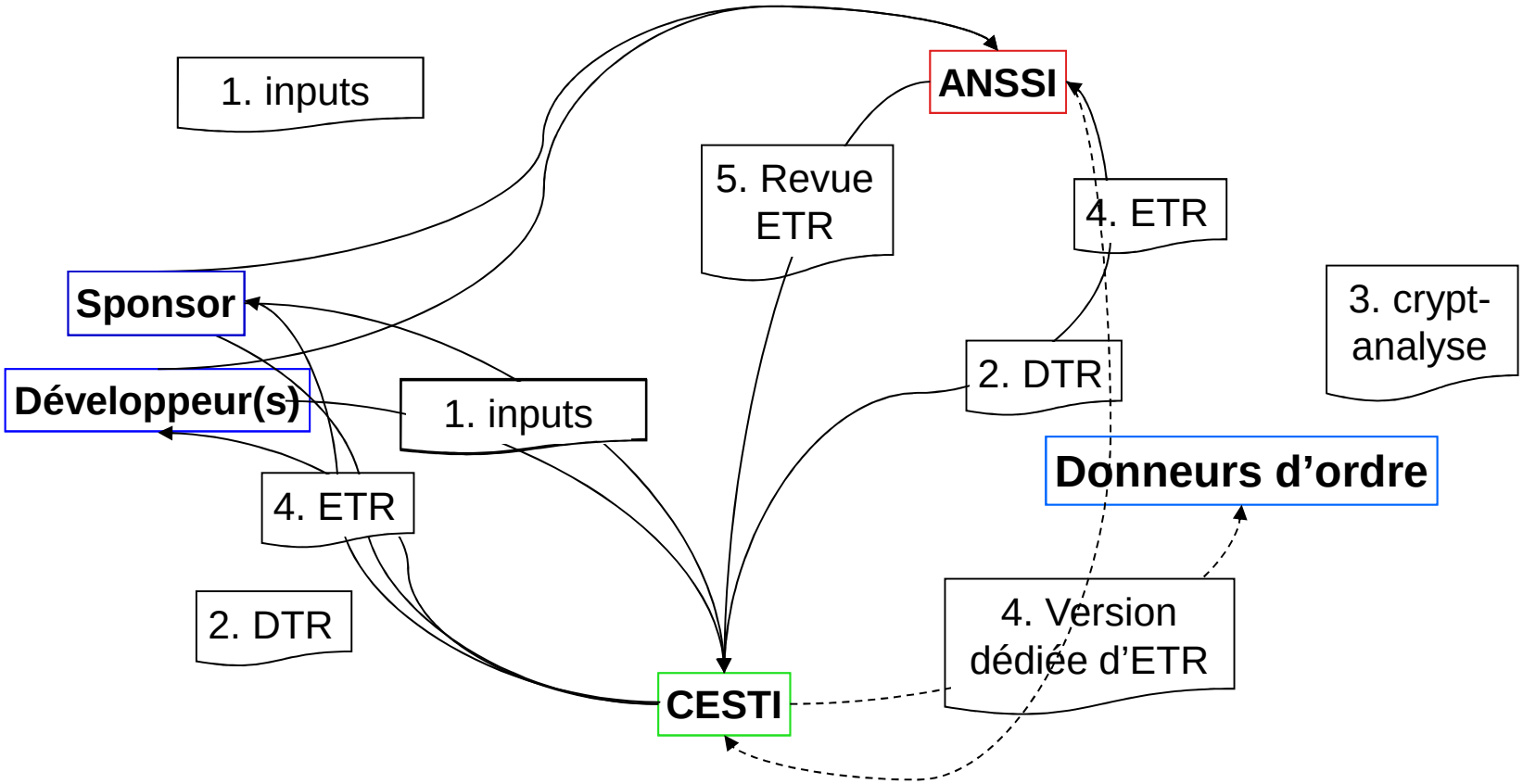
- Elémentaire: **certification de sécurité de premier niveau (CSPN dédié à la France et non reconnu à l'international)**
- Standard: **CC EAL3+ , le + signifiant des augmentations d'assurance notamment sur la gestion des bugs après déploiement**
- Elevée: **CC EAL4 à EAL5+**

C'est l'ANSSI qui gère ce schéma:

- ✓ **Relation avec les donneurs d'ordre**
- ✓ **Agrément des laboratoires**
- ✓ **Certification**
- ✓ **Relation avec les développeurs de produits**

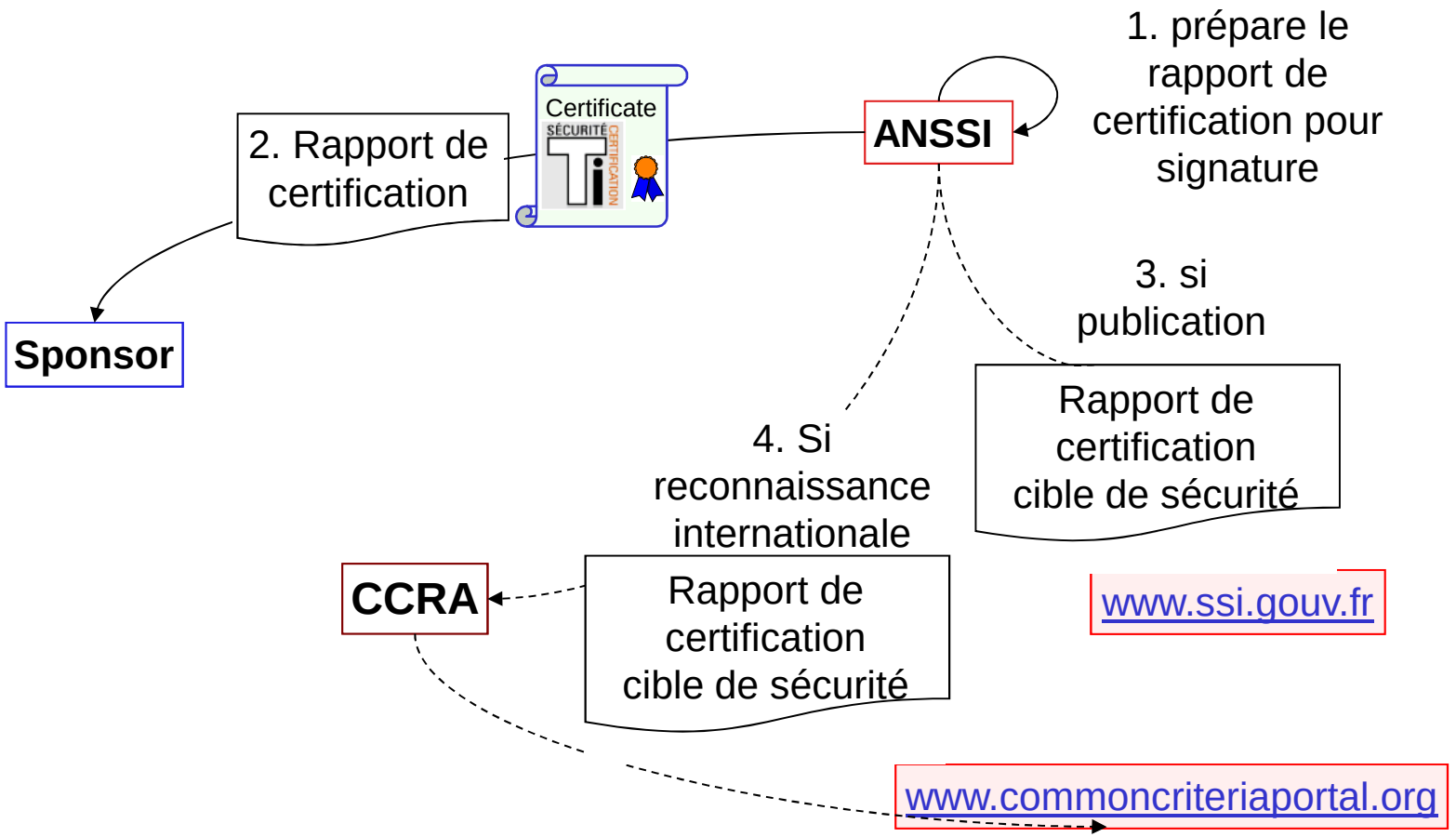
Fonctionnement du schéma: requête d'évaluation

- ETR/DTR: "evaluation technical report" & "detailed technical report"
- Voir www.ssi.gouv.fr
- CESTI: laboratoires indépendants aggréés par l'ANSSI



Fonctionnement du schéma: certification

- **L'ANSSI certifie**



Les secteurs industriels actuellement concernés

Corporate

Paiement

Communication

E-Gouvernement

Transport

Contrôle d'accès

Exemples de produits certifiés CC

Cartes Bancaires et composants de sécurité avec GIE carte bancaire comme donneur d'ordre

Terminaux bancaires avec l'EPC (European Payment Council comme donneur d'ordre)

Galileo avec l'ESA comme donneur d'ordre

A400M avec les nations comme donneur d'ordre

Passeport (standards internationaux)

Cartes SIM de Paiement Mobile (opérateurs et banques)

Produits réseaux (administrations)

Certifications privées: quelques exemples

- **Plateforme de Paiement Mobile et Cartes bancaires**

http://www.emvco.com/approvals.aspx?id=179

GLOBALPLATFORM

- **Application de Paiement Mobile et TEE (Trusted Execution Engine)**

http://www.globalplatform.org/specificationscard.asp

Zoom sur un schéma privé: certification de cartes bancaires

- ✓ **Un standard international fonctionnel, les normes EMV®**

- ✓ **Comportant 6 membres:**
  - ✓ American Express,
  - ✓ Discover,
  - ✓ JCB,
  - ✓ MasterCard,
  - ✓ UnionPay,
  - ✓ Visa

- ✓ **S'appuyant sur des labos agréés EMVCo, la plupart du temps déjà CESTIs (8 dans le monde)**

Comparaison certification privée ou public

	☺	😐
Schéma Privé	Peut être adapté aux besoins d'une industrie Peut proposer différents niveaux d'assurance	L'autorité de certification doit être indépendante
Critères Communs	Pas spécifique d'une industrie Reconnaissance internationale (EAL2)	Durée plus longue

Comment monter son schéma privé ?

Il peut être envisagé de créer son schéma privé:

- **Définir une base fonctionnelle de produit**
  - Un type de produits
  - Un standard industriel
- **Définir les outils du schéma**
  - Une méthodologie d'évaluation
  - Un périmètre d'évaluation
  - Un niveau d'évaluation
- **Déterminer les différents rôles**
  - Les fournisseurs de produits/systèmes
  - Les entités d'évaluation
  - L'entité de certification

THALES

Niveau d'évaluation sécuritaire et périmètre de sécurité

Niveau d'évaluation

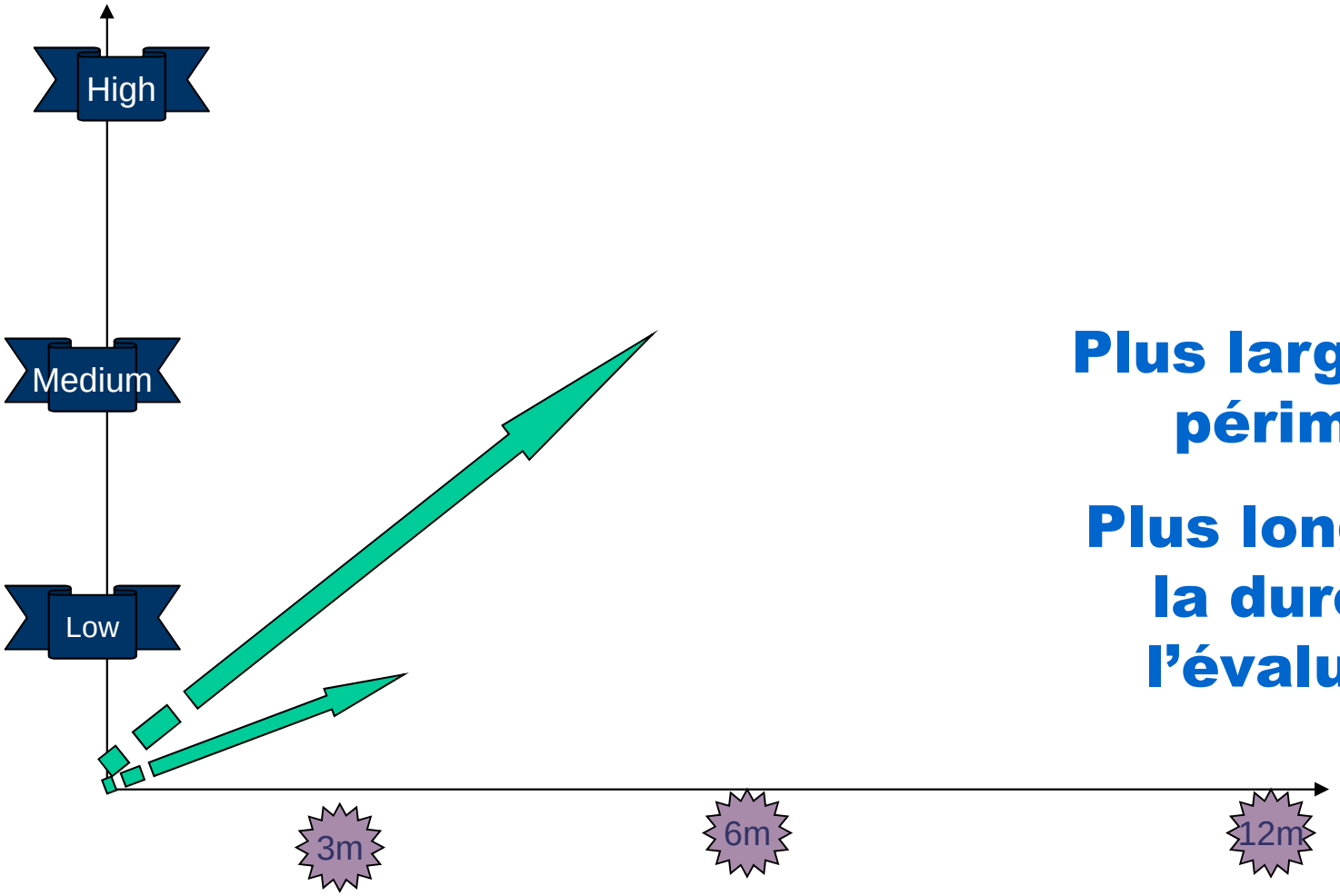
- Dépend du niveau d'attaquant
- Peut-être élévé ou faible
- Démontre la résistance du produit et sa conformité à sa spécification

Périmètre

- « TOE: Target Of Evaluation »
- Doit être définie avant l'évaluation
- Donne la valeur à la certification

Niveau de risque

Temps /Assurance/Périmètre



Plus large est le périmètre

Plus longue est la durée de l'évaluation

De l'importance de s'appuyer sur des laboratoires déjà aggréés

Les agréments

- Un contrôle continu par les schémas sur la qualités des essais et des rapports (assurance de qualité)
- Une comparabilité des niveaux d'évaluation (assurance d' homogénéité)
- Des méthodes connues et auditées (possibilité de comparaison des essais et de mesure de « couverture »)
- Des équipes d' ethical hackers à l'état de l'art et reconnus
  - Contrôlés par des experts étatiques et internationaux

Une compréhension des enjeux industriels

- Capacité à évaluer et accompagner
- Stratégie d'évaluation pérenne

Thales Lab: défaillance et malveillance, nos services d'évaluation

Notre objectif : être le partenaire de confiance de nos clients en apportant des solutions à leurs besoins en fiabilité et sécurité du composant à l'équipement

- Thales CESTI (Centre d'Evaluation de la Sécurité des Technologies de l'Information) agréé par l'ANSSI & par les principaux schémas bancaires
- Tests d'intrusion Hardware et Software
- Agrément de savoir-faire par 3 agences spatiales
- Expertise composants critiques
- Audit de systèmes et conseil IT

Thales produit, expertise et évalue chaque brique technologique constituant un système critique

Partenariats

Un PARTENARIAT avec le CNES depuis 1994

Partenariat CNES et THALES:

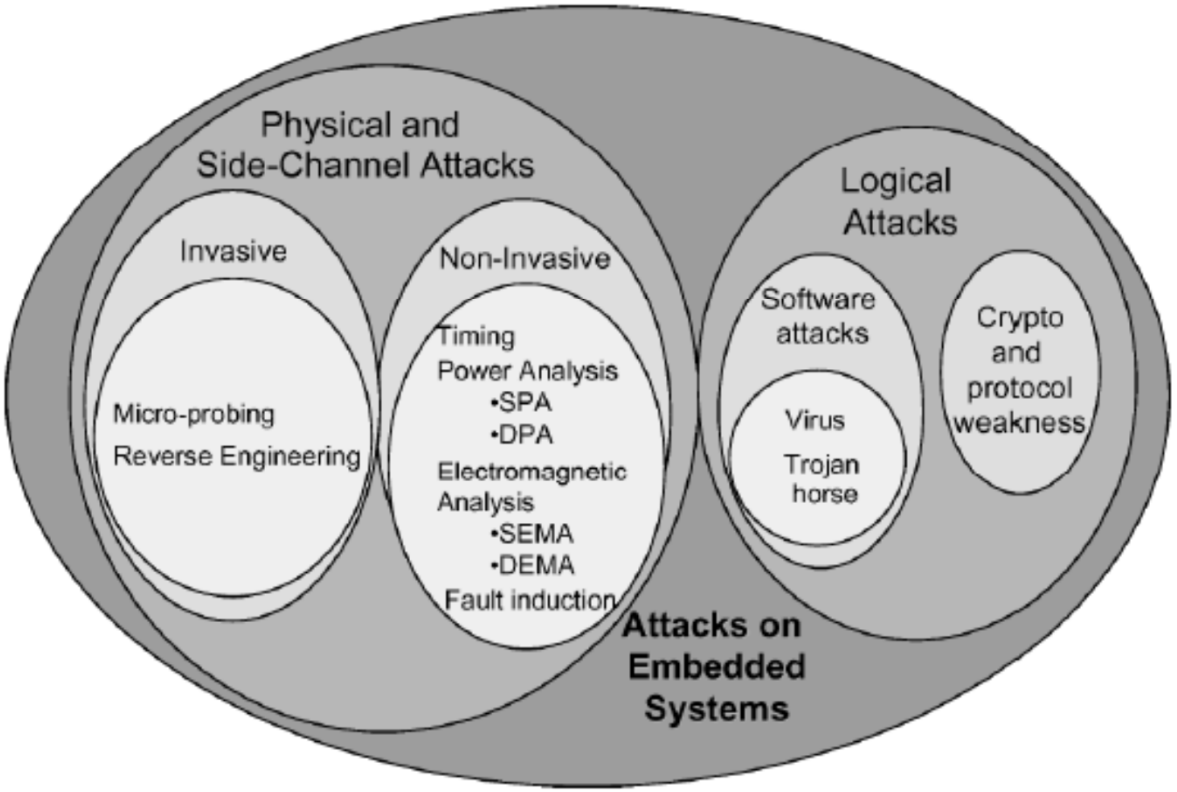
- **Moyens:**
  - 1 000 m² de laboratoire
  - 10 M€ de materiel de haute technologie
  - 500 K€ d'investissements annuels
- **Recherche:**
  - R&T commune
  - Feuille de route technique
- **Un réseau d'experts**

cnes
CENTRE NATIONAL D'ETUDES SPATIALES

Un des plus grands centres technologiques en Europe

Les attaques considérées sur les évaluations

Secure Embedded Systems, S.Ravi, 2004

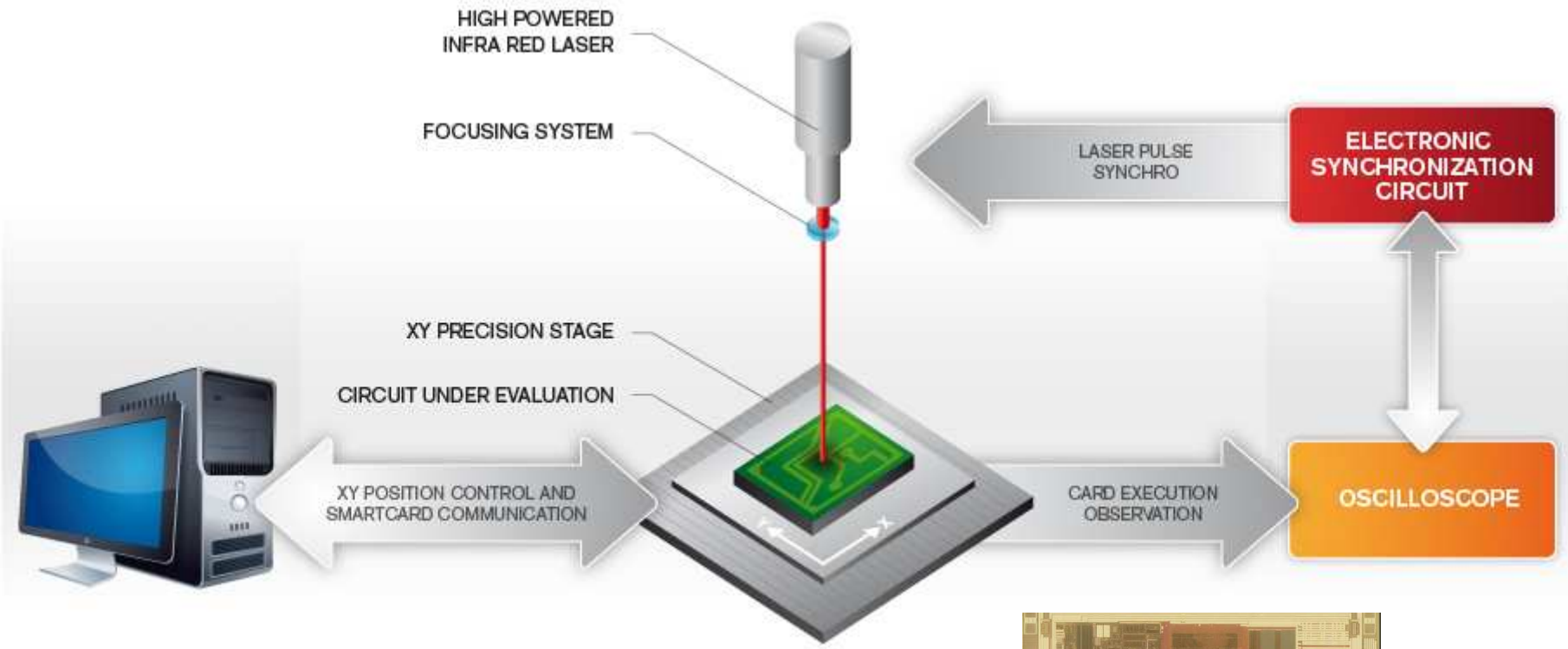


Examples of attack threats faced by embedded systems.

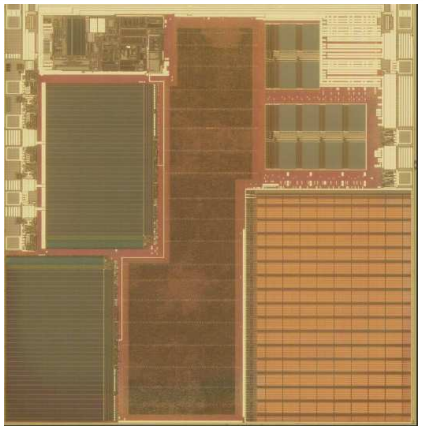
Les attaques semi-invasives

THALES

Les attaques semi-invasives

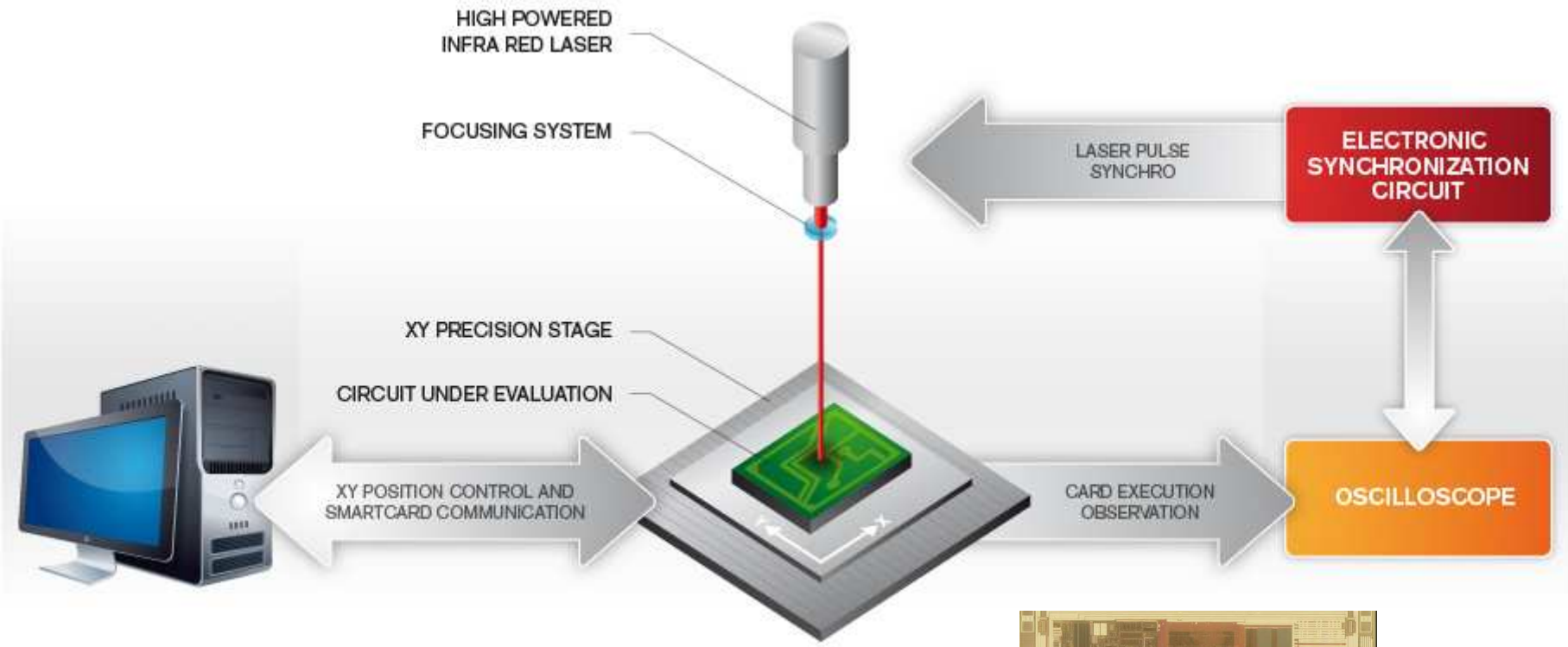



```
if (memcmp(value, ref_password, 16) == 0)
{
     // success
}
else
{
     // bad password, try again
}
```

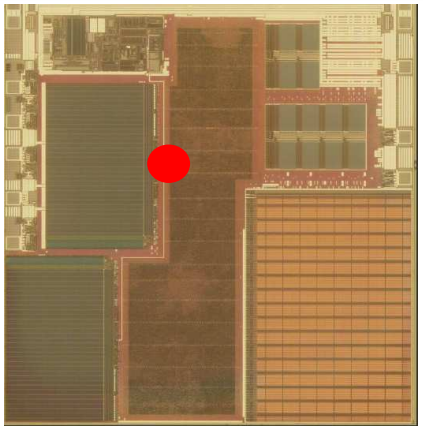


Source : BlackHat 2010

Les attaques semi-invasives




```
if (memcmp(value, ref_password, 16) == 0)
{
     // success
}
else
{
     // bad password, try again
}
```



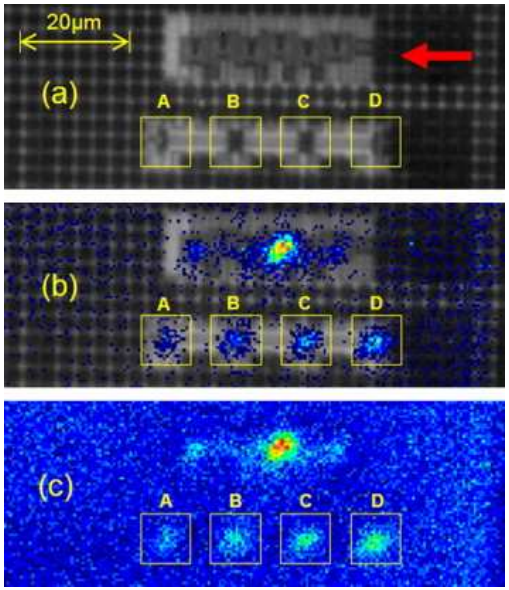
Source : BlackHat 2010

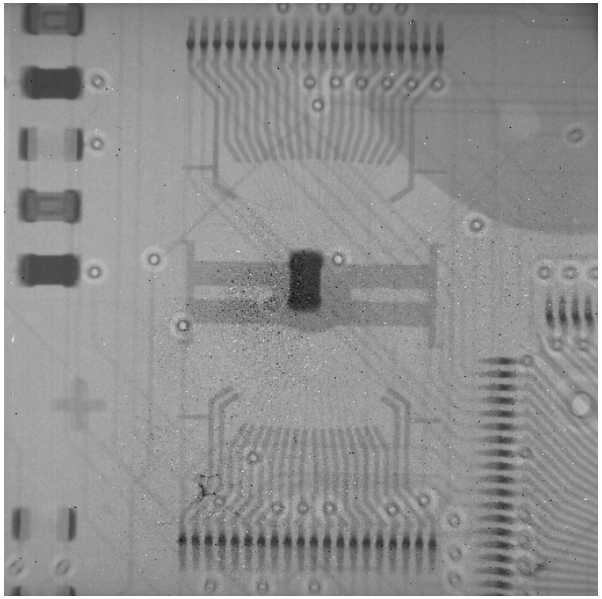
Les attaques invasives

Source : iFixIt

Les attaques invasives

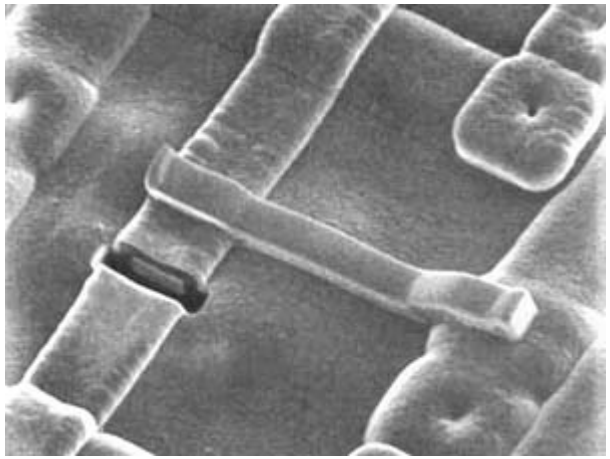
Localisation par émission photonique

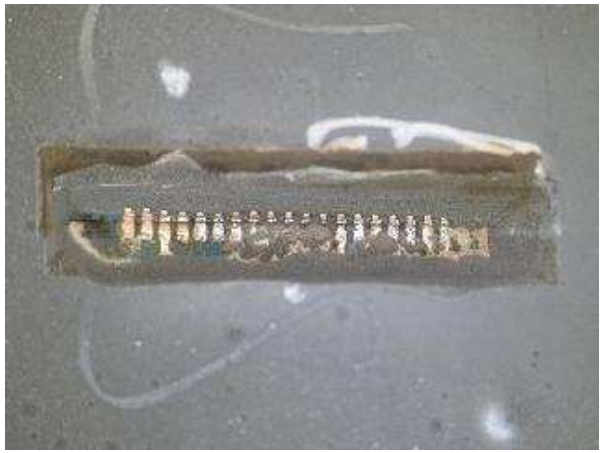




Analyse RX

Edition de circuit au FIB





Depackaging

Les attaques logiques

- Tests d'intrusion logiciel: une équipe dédiée sur Toulouse reconnue par l'ANSSI
- (Certification de sécurité CSPN= 25 à 45 jours)

Missions sur systèmes avioniques embarqués et sols, Mission sur systèmes de communication , Mission sur produits grand public (téléphones mobiles-Android,IOS, applications-, smartTv, box)

Thales Lab: les clients qui nous font confiance

Aeronautique Defense

Energie

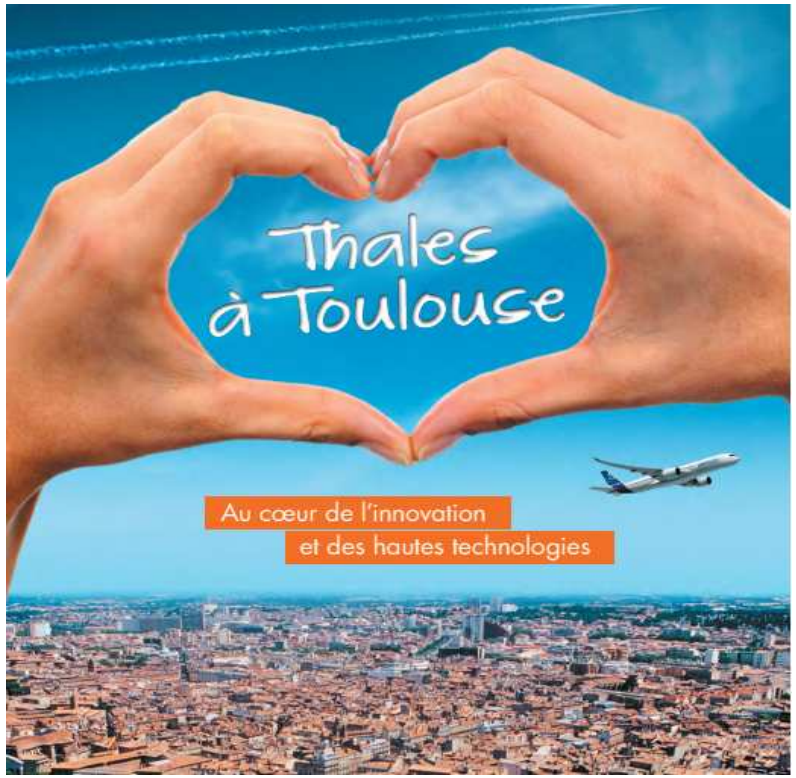
Semiconducteur

Smartcard Banking

Communication Mobile

Référence / date

THALES



MERCI DE VOTRE ATTENTION

Nathalie.feyt@thalesgroup.com

0680358624