Démarches de Sécurité & Certification : Atouts, Limitations et Avenir

Orange Business Services
Silicomp-AQL
1 rue de la Chataigneraie
CS 51766
35517 CESSON-SEVIGNE Cedex
France

SGDN-DCSSI

Certificat
N°1994-/2759h

Accréditation N° 1-1528
Section Laboratoires
Portée sur www.cofrac.fr

Christian Damour – Responsable Activité Sécurité et Protection de l'Information

christian.damour@aql.fr

1er juin 2007

Sommaire

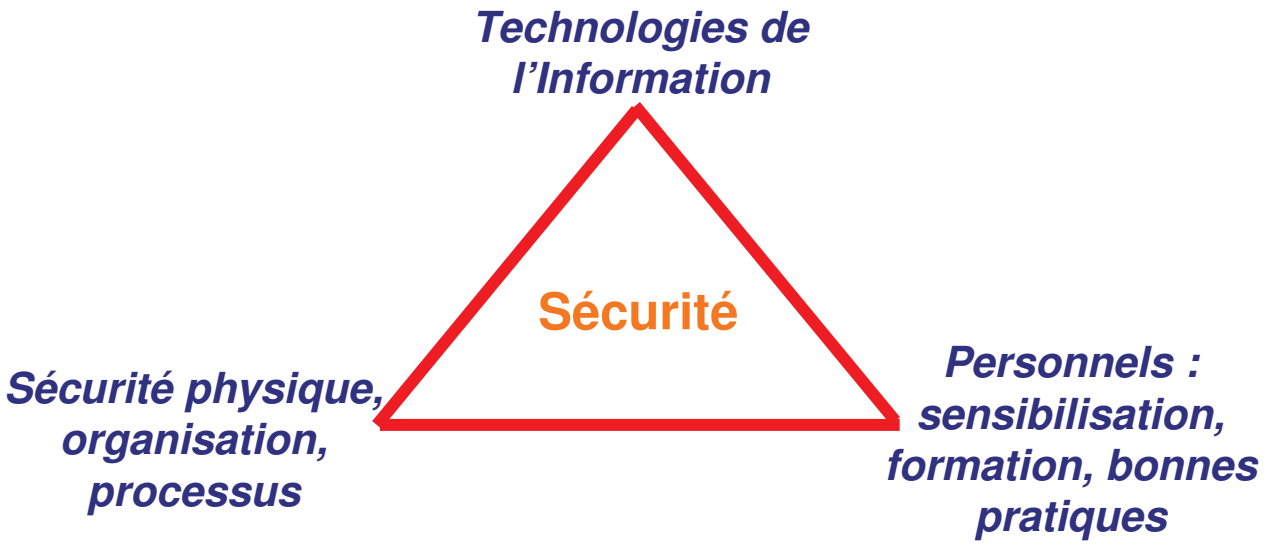
- Introduction – la problématique de la confiance
- La sécurité : un effort permanent
- Les démarches de sécurité
- Quelques référentiels de certification
- Les Critères Communs : référentiel de certification
- Le Schéma Français d'évaluation et de certification et les accords de reconnaissance mutuelle des certificats : qu'est-ce qu'un CESTI ?
- Limitations de la certification : les pièges à éviter, conseils et solutions
- Conclusion

Introduction – la problématique de la confiance

FONDAMENTAUX DE LA SECURITE

> Une démarche de progrès permanente :
  - Veille technologique / mise à niveau
  - Communication
  - Sensibilisation / formation

> Selon 3 axes :



La sécurité : un effort permanent

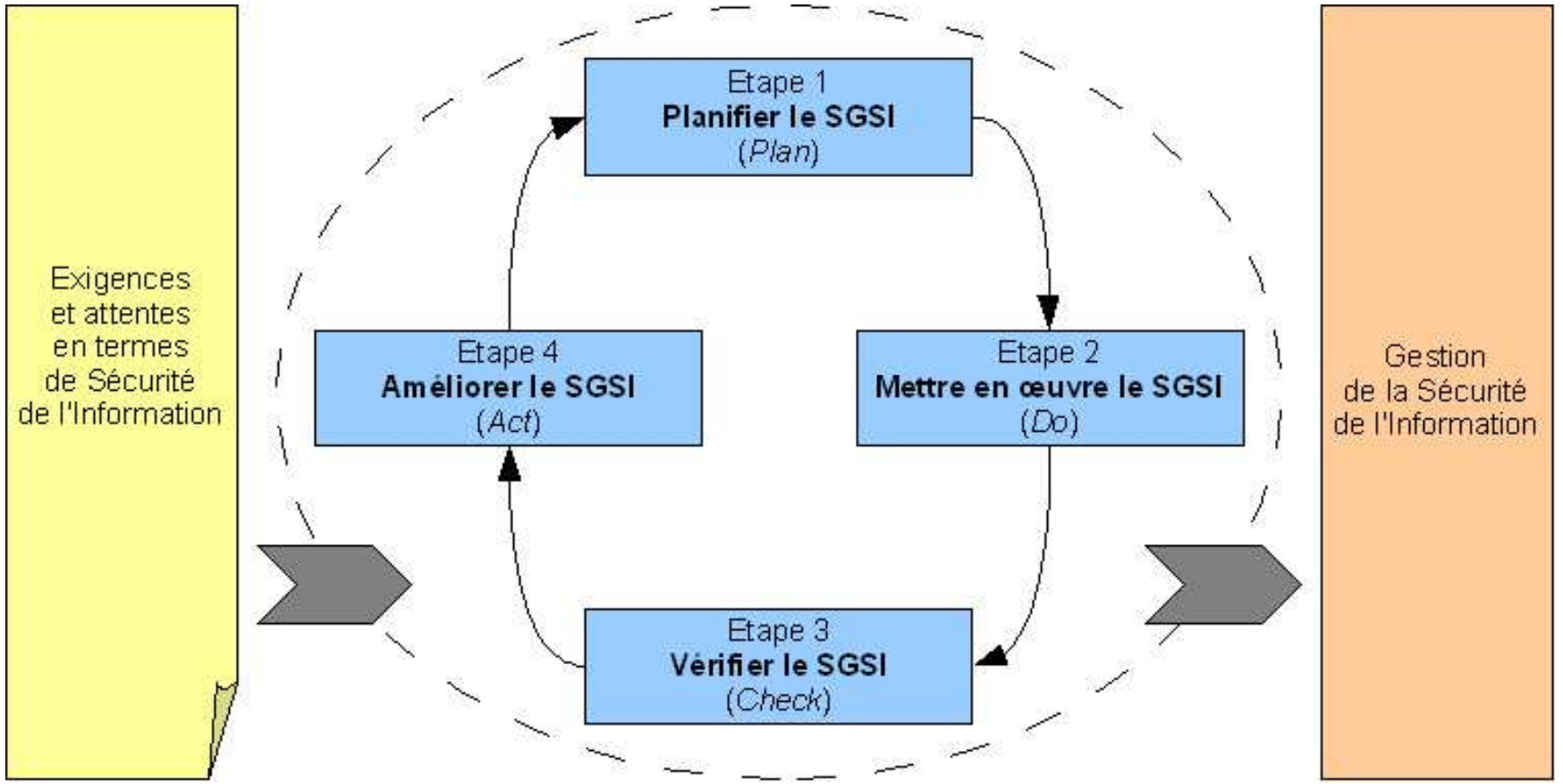
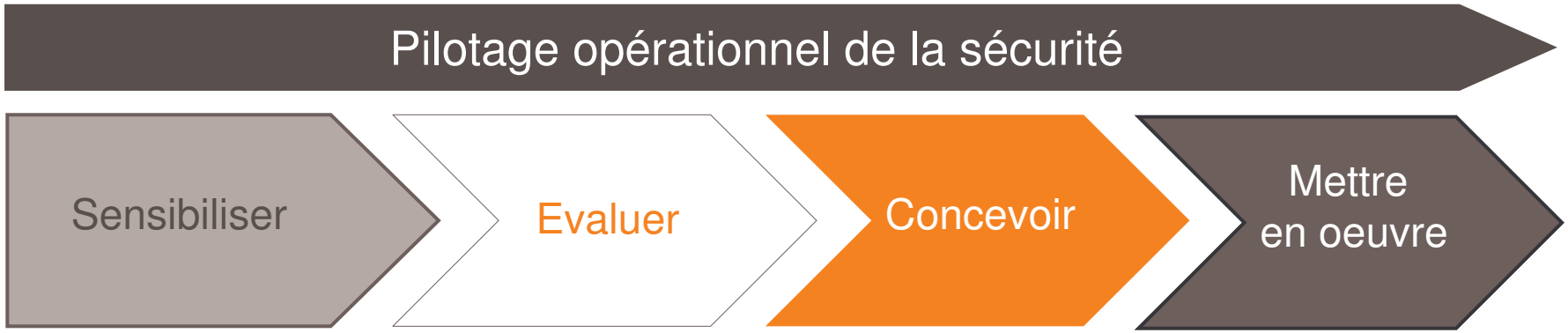


Illustration 1 : Modèle PDCA de la norme ISO 27001:2005

Les démarches de sécurité



- Séminaire de direction stratégique
- Séminaire de direction technologique
- Groupe de réflexion métier

- Recueil du besoin
- Analyse de risque
- Audit flash
- Etude d'opportunité
- Schéma Directeur
- Benchmark

- Plan d'action pour la mise en place du scénario cible
- Formalisation des besoins détaillés
- Choix des solutions
- Rédaction des procédures

- Spécification / plan détaillé de mise en en oeuvre
- Validation
- Mise en œuvre
- Audit / bilan
- Certification (?)

Conduite du changement

- Préparer le changement et définir la stratégie à mettre en oeuvre

- Mettre en œuvre et conduire le changement

- Evaluer et mesurer l'adéquation, l'efficacité et l'appropriation, ajuster et pérenniser

Les démarches de sécurité

OBJECTIFS ET MOYENS

> Améliorer le niveau de sécurité de son système d'information nécessite en tout premier lieu de connaître son besoin de sécurité :

- quels sont les éléments sensibles à protéger (identification des flux sensibles, classification des actifs du système d'information) ?
- contre quelles menaces internes, externes (analyse du risque : démarches telles que EBIOS[1], MEHARI[2],…) ?

[1] Cf http://www.ssi.gouv.fr/fr/confiance/methodes.html

[2] Cf https://www.clusif.asso.fr/fr/production/mehari/

Les démarches de sécurité

DEFINITION ET MISE EN ŒUVRE DE MOYENS

A partir de la connaissance du besoin de sécurité, il est possible de mettre en place des solutions technologiques et des processus (référentiel ISO17799[1], ISO27001) tout en gardant présent à l'esprit la nécessité de communiquer auprès des acteurs concernés de l'entreprise :

[1] Cf http://www.iso-17799.com/

- prise en compte de la sécurité dans les démarches de développement sur les projets internes de l'entreprise,
- définition d'une politique de sécurité de l'information,
- définition d'une architecture de sécurité appropriée,
- choix de produits certifiés selon les Critères Communs (norme ISO15408),
- définition et mise en œuvre d'un Plan de Continuité d'Activité,
- réalisation d'audits de sécurité internes et externes périodiques.

Les démarches de sécurité

OBJECTIFS ET MOYENS

> Acquérir un niveau de confiance dans le système d'information de l'entreprise.

> Protéger les activités vitales de l'entreprise et son savoir-faire, tout en facilitant l'ouverture du système d'information sur l'extérieur, l'interopérabilité, l'ergonomie et la facilité d'emploi.

➔ **une question de compromis.**

> Il faut s'appuyer sur des démarches, référentiels éprouvés (normalisés), sur des solutions (produits et services) ainsi que sur des prestataires de confiance.

Quelques référentiels de certification

- La norme ISO17024 et les référentiels de certification des individus.
- La norme ISO27001 pour les processus et l'organisation de la sécurité.
- Le référentiel des Critères Communs ou norme ISO15408 pour les produits, systèmes informatiques, solutions et services à valeur ajoutée.

Quelques référentiels de certification

Normes d'accréditation des organismes d'évaluation et de certification (en France par le Cofrac)

Domaine d'application / Portée	Organisme d'évaluation	Organisme de certification
Produits et systèmes technologiques	ISO17025 (ex-EN45001)	EN45011 / ISO/CEI Guide 65
Organisation et processus de la sécurité	ISO17021 (ex-EN45012)	
Certification des individus	ISO17024 (ex-EN45013)	

Quant aux référentiels d'évaluation et de certification :

Domaine d'application / Référentiels	Référentiels
Produits et systèmes technologiques	Critères Communs (norme ISO15408)
Organisation et processus de la sécurité	Norme ISO27001
Certification des individus	CISSP, ISO27001 Lead Auditor, etc.

Le Schéma Français d'évaluation et de certification des TI

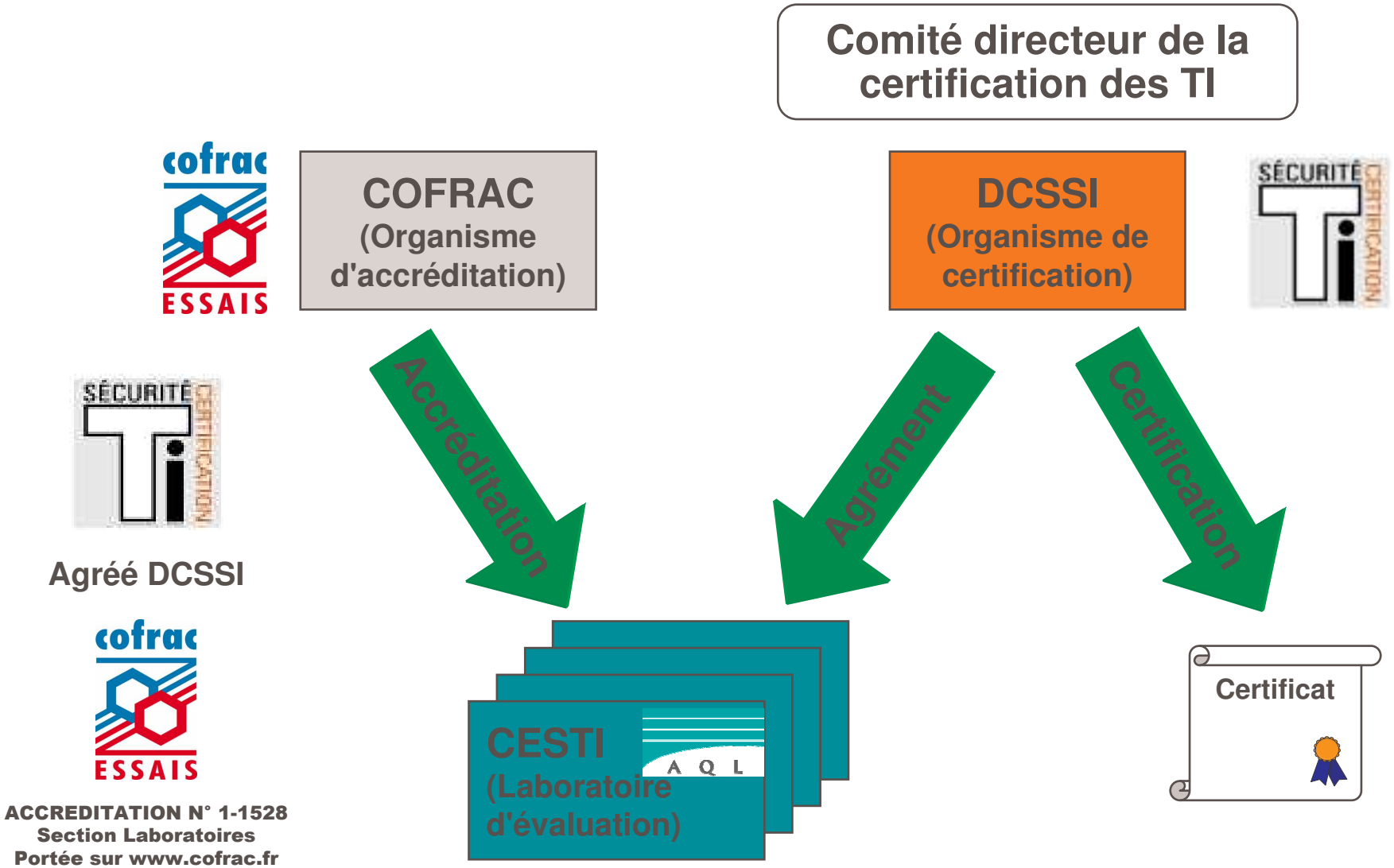
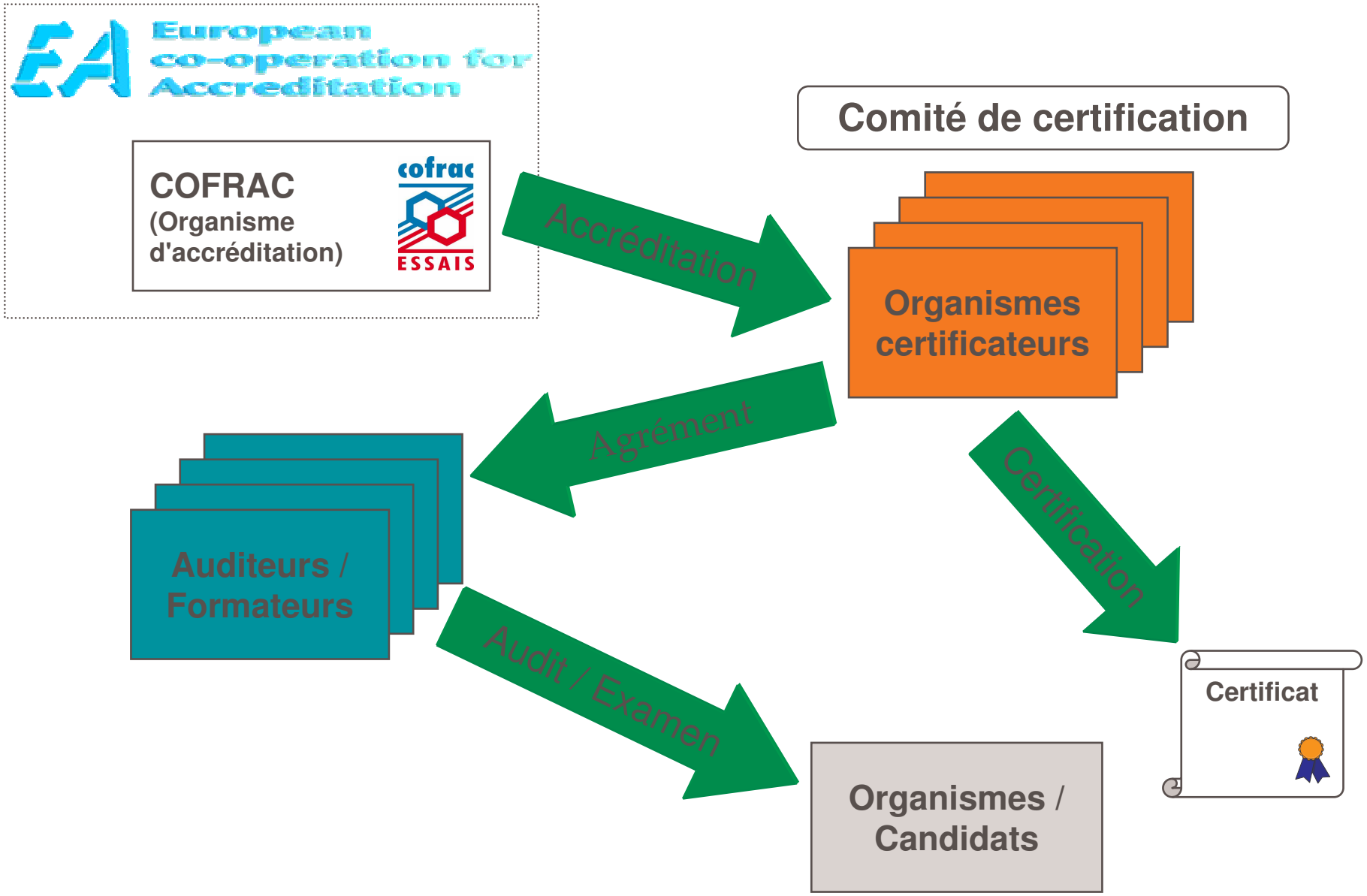


Schéma de certification : organismes et personnes



Les Critères Communs : référentiel de certification

Vecteur de la confiance

- Laboratoire accrédité par le Cofrac et agréé par les services du Premier Ministre
- Évaluation selon des critères normalisés
  (ITSEC, Critères Communs – norme ISO15408)
- Reposant sur des référentiels et des normes
  - ISO 17025 / ISO 15408 / ISO 18045
- Reconnaissance mondiale des certificats
  - accords européens : SOG-IS (Senior Official Group – Information Security) qui permettent une reconnaissance des certificats tous niveaux confondus entres les pays signataires.
  - accords mondiaux : CCRA (Common Criteria Recognition Arrangement) qui permettent une reconnaissance des certificats entres les pays signataires, pour les niveaux EAL1 à EAL4.
- Pays dits « producteurs de certificats » vs pays dits « consommateurs de certificats »

Le C.E.S.T.I. de Silicomp-AQL

> *vers la certification de la sécurité de vos produits ou systèmes selon des critères reconnus mondialement* ***(norme ISO 15408)***

centre d'évaluation de la sécurité des technologies de l'information

Agréé DCSSI

- évaluations ITSEC ou Critères Communs
- rédaction de fournitures
- formation, conseil et assistance

Accréditation n° 1-1528
section laboratoires
portée sur www.cofrac.fr

> portée de l'agrément : tout type de logiciel, système, réseau ITSEC (E1-E4)

> ou CC (EAL1–EAL4)

Limitations de la certification : les pièges à éviter, conseils et solutions (1/4)

- Validité du certificat (une photographie à l'instant « t » du produit/système) :
  - Vérifier la date d'émission et s'il existe un processus de « surveillance », ou de « continuité de l'assurance ».
- Version du produit couverte par le certificat :
  - A vérifier car la validité du certificat ne porte pas sur les évolutions du produit, sauf dans le cas où un processus de « maintenance de certificat » ou « continuité de l'assurance » est mis en œuvre par l'éditeur.
- Le périmètre ou portée de la certification :
  - Voir le document Cible de Sécurité (Security Target) en Critères Communs (norme ISO15408) / la Déclaration de Conformité (Statement of Applicability) pour la norme ISO27001. A vérifier car un sous-ensemble plus ou moins représentatif du produit peut être inclus dans la portée du certificat décerné, ce qui signifie que toutes les fonctionnalités utilisées du produit/système cible peuvent ne pas être couvertes.

Limitations de la certification : les pièges à éviter, conseils et solutions (2/4)

- Le niveau de confiance atteint : exemple en Critères Communs, les niveaux de confiance (d'assurance) prédéfinis : Evaluation Assurance Level (EAL1-EAL7) :
  - EAL1 : **testé fonctionnellement**
  - EAL2 : **testé structurellement**
  - EAL3 : **testé et vérifié méthodiquement**
  - EAL4 : **conçu, testé et revu méthodiquement**
  - EAL5 : **conçu de façon semi-formelle et testé**
  - EAL6 : **conception vérifiée, de façon semi-formelle et testé**
  - EAL7 : **conception vérifiée, de façon formelle et testé**
- A vérifier car ce niveau d'assurance apporte un niveau de confiance dans la sécurité du produit, tout en restant limité au périmètre visé.

Limitations de la certification : les pièges à éviter, conseils et solutions (3/4)

- Les éventuelles conditions sous lesquelles le produit ou système peut être considéré comme sûr (d'après le certificat)
  - Voir le document Cible de Sécurité (Security Target) en Critères Communs (norme ISO15408).
  - A vérifier car dans le contexte spécifique ayant présidé à la délivrance du certificat (Cf « Cible de Sécurité »), il peut exister des restrictions / conditions.
    - par exemple, nécessité de mettre en place, dans l'environnement d'exploitation cible du produit, des mesures de sécurité techniques, physiques, organisationnelles ou liées au personnel :
      - ➔ existence d'un firewall destiné à filtrer les accès réseau au produit,
      - ➔ utilisation du produit dans un local à accès contrôlé,
      - ➔ gestion des personnels habilités à accéder physiquement au produit,
      - ➔ etc.

Limitations de la certification : les pièges à éviter, conseils et solutions (4/4)

- Conditions d'emploi du produit/système
  - par exemple, nécessité de ne pas utiliser ou de désactiver certaines fonctionnalités ou certains services du produit :
    - ➔ utilisation du chiffrement 3-DES et pas DES pour des questions de résistance à la cryptanalyse,
    - ➔ absence de connexion au réseau afin d'empêcher une attaque via le réseau,
    - ➔ absence de lecteur de CD-ROM afin d'empêcher un boot de la machine sur CD-ROM apporté par un attaquant,
    - ➔ désactivation des ports USB (idem),
    - ➔ etc.

Compléments sur la certification : liens utiles

- ✓ http://www.commoncriteriaportal.org/
- ✓ http://www.ssi.gouv.fr/fr/dcssi/
- ✓ http://www.nsa.gov/ia/industry/niap.cfm
- ✓ Registre international des certificats Critères Communs :
  http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5
- ✓ Registre international des certificats ISO27001 :
  http://www.iso27001certificates.com/
- ✓ Registre international des certificats BS7799-2 et ISO27001
  http://www.17799central.com/cert.htm
- ✓ Registre international des certificats BS7799-2
  http://www.certificationregister.org/
- ✓ Organisme de Certification français et organismes certifiés
  http://www.lsti.fr/
- ✓ Formations certifiantes ISO27001 Lead Auditor
  http://www.hsc.fr/services/formations/formations_lsti.html.fr
- ✓ Registre français des auditeurs certifiés
  http://www.lsti.fr/Portal_Asp/Portal.asp?h_catid=16&h_groupid=2&h_layid=39&h_catbg=Portal_Upload/Backgrounds/bg_general.gif&h_tmplid=1&h_tmpltype=4&h_tmplobj=GNV2004.Portal&h_tmplframe=top.portail.main&h_mode=LoadLayout&my_from=1

LSTI est le premier organisme certificateur spécialisé dans le domaine de la sécurité des technologies de l'information accrédité (dossier n°4-0063) par le COFRAC (comité français d'accréditation). En fonction des résultats de l'examen, le certificat ISO27001 Lead Auditor (anciennement BS7799 Lead Auditor) est attribué ou non aux stagiaires par LSTI deux semaines après la formation.
http://www.hsc.fr/services/formations/index.html.fr#formations_lsti

Conclusion

- **Le marché de la certification de la sécurité est promis à un brillant avenir, compte tenu des enjeux :**
  - mondialisation et dématérialisation des échanges,
  - mutations technologiques majeures en cours (solutions de mobilité, convergence voix-données-images, vers le tout communicant en tout lieu et à tout moment,…)
  - augmentation inéluctable de la dépendance des organisations vis-à-vis des technologies de l'information
  - montée de la criminologie informatique tant en interne qu'en externe (fortement liée à l'intérêt d'une attaque réussie qui augmente)
- **Parmi les meilleures pistes de développement de la certification de la sécurité :**
  - Le domaine de la carte à puce (80% des certificats CC émis en France).
  - Le domaine de la Défense nationale et de l'OTAN (raisons réglementaires).

Conclusion

> **Parmi les meilleures pistes de développement de la certification de la sécurité :**

- Les travaux du gouvernement français autour du Référentiel Général de Sécurité (RGS) et de la PRIS V2 (ou Politique de Référencement Intersectorielle de Sécurité, V2.1).
- Le domaine de la signature électronique qualifiée (avec effet juridique de renversement de la charge de la preuve) / Directive européenne n°1999/93/CE sur la signature électronique.
- Les travaux de la DCSSI autour de la rédaction, de la certification et de la normalisation par l'Afnor de Profils de Protection : futurs textes de référence applicables dans le domaine des appels d'offres publics (conformément au Code des Marchés Publics).
- La mise en place par la DCSSI des processus de qualification aux niveaux standard, renforcé et élevé s'appuyant sur le processus d'évaluation et de certification selon les Critères Communs et bientôt la qualification au niveau élémentaire.
- L'agrément en préparation des CESTI en matière de cryptographie.

Questions & réponses

Activité Sécurité et Protection de l'Information

Christian Damour
Responsable Activité Sécurité

SGDN-DCSSI

Certificat
N°1994-/2759h

Accréditation N° 1-1528
Section Laboratoires
Portée sur www.cofrac.fr

Silicomp-AQL, un pôle sécurité pour OBS

- 60 intervenants – 15 ans d'existence
  Une offre de service globale
  Indépendance en tant que CESTI agréé
  Plus de 300 audits réalisés
- **un CESTI agréé par les Services du Premier Ministre** (l'un des deux seuls laboratoires de ce type en France, reconnus pour l'évaluation de la sécurité de produits, systèmes et réseaux - le plus ancien CESTI encore en activité - depuis 1991)
- Vigil@nce **: une veille permanente sur les vulnérabilités/correctifs**, sur les virus, et sur les actualités depuis 1998 - **offre certifiée compatible CVE (Common Vulnerabilities & Exposures).**
- **Audits et conseil en sécurité : tests d'intrusion ; audits organisationnels ; ISO27001 ; PCA/PRA ; chartes, politiques de sécurité,**
  une équipe dédiée de 15 auditeurs ; 10 ans d'expérience ; + de 300 audits réalisés.
- **Etudes, expertises, formations et sensibilisations SSI depuis plus de 15 ans !**
  Et de nombreuses autres prestations…

Zoom sur l'activité Sécurité et Protection de l'Information : une offre globale (1/2)

CONSEIL ET ETUDES DIVERSES

(Définition d'architectures sécurisées, comparaison de solutions, études des solutions de DRM, protection des logiciels contre la rétro-ingénierie, …)

FT R&D/Viaccess :Etude des solutions de protection de contenu & benchmarking de ces solutions

ETUDES A CARACTERE PROSPECTIF

(Etudes amont en SSI de la DGA, études d'opportunité, études de faisabilité, études techniques, préparation à l'homologation de systèmes, …)

SPOTI : PEA VAR – Réalisation d'un démonstrateur de veille alerte réponse vis à vis des menaces cybernétiques pesant sur les systèmes et réseaux du ministère de la défense.

ANALYSES DE RISQUE & PRISE EN COMPTE DE LA SECURITE DANS LES PROJETS

(Analyses de risque, Spécifications de sécurité produit/système, Cibles de Sécurité, intégration des exigences de sécurité dans les démarches projet)

CNES : Analyses de risque satellite liaisons sol-bord-sol et liaisons sol (PLEIADES HR)

ASSISTANCE A MAITRISE D'OUVRAGE

(Elaboration de cahiers de charges, pilotage de consultations, dépouillement, support technique)

SPOTI : Redéfinition des processus et outils de gestion des composants cryptographiques au sein des armées

ASSISTANCE A RSSI & CENTRE DE SERVICES

(Coaching, politiques de sécurité, chartes, TDBSSI, plans de continuité, services intégrés de veille sécurité forfaitisée, …)

EDF-RTE : Cellule Surveillance Sécurité et d'Exploitation

Zoom sur l'activité Sécurité et Protection de l'Information : une offre globale (2/2)

AUDITS / TESTS INTRUSIFS
(Audits techniques, tests intrusifs en Boîte Noire, Grise ou Blanche, audits organisationnels, audit d'applications Web, audits de code source, Wifi, VoIP, …)

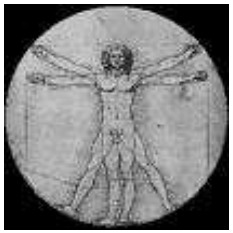
Audit Boîte Noire Worldwide des accès internet du Groupe Air Liquide / équipe audit de 15 personnes / plus de 300 audits réalisés

VEILLE SUR LES PRODUITS
(OS, crypto, PKI, authentification, contrôle d'accès, Firewalls, antivirus, …)

CELAR : Analyse sécurité des produits civils : plus de 150 produits du marché expertisés !

VEILLE SUR LES VULNERABILITES / CORRECTIFS / VIRUS / VEILLE ACTUALITE
Vigil@nce

Notre veille interne et offre d'abonnement à nos clients



FORMATIONS
(Mastère SSI de l'ENST, formation continue ENSTB, formations/sensibilisations à la carte)

Min Educ. Nationale : Formation/sensibilisation de tous les rectorats d'académie /
GMSIH : Accompagnement SSI des établissements de santé hospitaliers

EVALUATION SECURITE
selon les CC (ISO15408) et ITSEC
& PREPARATION / SUPPORT A L'EVALUATION
(Profils de Protection, produits, systèmes)

CNES : Accompagnement et expertises sécurité sur le segment sol du programme PLEIADES HR
NEC (Japon) : Evaluations systèmes pour NEC Japon (2 sites certifiés)
Ministère de la Défense : Evaluation des SI embarqués des frégates HORIZON et FREMM

AUDITS/EVALUATIONS ISO27001
CONSEIL ISO17799

MINEFI / C3OP : Elaboration d'un guide d'audit dérivé d'ISO17799 pour les organismes payeurs et accompagnement des auditeurs de la C3OP