cetic

CETIC

2 juin 2005

Sécurité informatique : utilisation des Common Criteria en entreprise

Eric GHEUR
GALAXIA I.S.E.
Tel : +32 2 779 85 57
eric.gheur@galaxia.be

GALAXIA I.S.E.

Note préliminaire

Afin de respecter les règles relatives aux droits d'auteur, les extraits repris de la norme ont été remplacés par leur référence dans les documents originaux.

Pour compléter l'exposer, il est donc conseillé de télécharger les documents nécessaires depuis le site des Critères communs :

http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2

Les versions françaises 2.1 des critères communs correspondent à l'ISO/IEC 15408 et peuvent être téléchargés depuis le site de la DCSSI :

http://www.ssi.gouv.fr/fr/confiance/methodologie.html

Sauf indications contraires, les références renvoient au Critères Communs, version française 2.1

Plan

- Historique de l'ISO/IEC 15408
- Ce que sont les critères communs et l'ISO/IEC 15408
  - Définitions des critères d'évaluation de la sécurité
  - La norme ISO/IEC 15408
  - Structure hiérarchique
    - Exigences fonctionnelles (15408-2)
    - Exigences d'assurance (15408-3)
- Points clés à savoir
  - Cadre méthodologique
  - L'évaluation et la certification
  - Les niveaux d'évaluation (assurance sécurité)
- Les profils de protection
- Les utilisations des critères communs
- Conclusion
- Pour en savoir plus ...

Exposé du 2/6/2005 : Approche intuitive
Pour une approche plus rigoureuse : par les documents d'introduction :
http://www.commoncriteriaportal.org/public/consumer/index.php?menu=1

Historique de l'ISO / IEC 15408

- **Critères Communs**
  = volonté de convergence, notamment des ITSEC européens et du Livre Orange américain, concrétisée par le CCEB créé à cet effet

- **ISO/IEC 15408 = Critères Communs**
  - **Transposition en norme internationale de la publication 2.0 des critères communs**
  - **V2.1 d'août 99**
  - **en cours de révision (ISO/IEC JTC1/SC27)**

- **Norme complétée par diverses normes ISO**
  (méthodologie d'évaluation, profils de protection, etc.)

- **Norme qui sera aussi complétée par l'ISO/IEC 19791**
  (critères d'évaluation de la sécurité des systèmes opérationnels)

Les critères d'évaluation - définitions

- ***Critère :***
  "caractère, signe qui permet de distinguer une chose, une notion; de porter sur un objet un jugement d'appréciation"

  (Petit Robert)

- **Critère d'évaluation de la sécurité (pour le présent exposé)**

  "caractéristique d'un objet (produit, système, processus), identifiable et mesurable ou vérifiable, et qui contribue à la sécurité de l'objet (confidentialité, intégrité, disponibilité, fiabilité, authenticité, imputabilité et non répudiation)"

  … utilisable comme l'expression d'exigences fonctionnelles de la sécurité

FIA_UAU.2.1 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

Les exigences fonctionnelles définissent le comportement de sécurité désiré

Les exigences d'assurance représentent la mise en œuvre des mesures d'assurance sécurité prévues

Les critères et l'ISO / IEC 15408

- **La norme ISO/IEC 15408**
  - **norme internationale publiée par l'ISO/IEC JTC1/SC27, téléchargeable**
  - **contient les définitions des critères à utiliser comme base pour l'évaluation des propriétés de sécurité d'un produit ou d'un système (catalogue des critères)**
  - **contient aussi la terminologie et la définition des autres concepts nécessaires à l'utilisation de ces critères**
- **L'ISO/IEC 15408 : des briques de base permettant :**
  - **de spécifier la sécurité du produit ou du système (à developper, à acquérir)**
  - **d'évaluer la sécurité d'un produit ou d'un système (après développement ou après acquisition)**
  - **contient "certaines briques" et doit souvent être complétée (PP, etc.)**
- **L'ISO/IEC 15408 se complète aussi par**
  - **des cadres méthodologiques : pour les évaluations, les PP, etc (ex. ISO/IEC 18045, 15446)**
  - **des documents plus ciblés (profils de protection enregistrés, etc.)**
  - **des schémas de certification nationaux (… pas en Belgique)**
  - **de éléments utiles dans les différentes phases de construction de la sécurité**

La structure – Les classes

Structure de classement des critères (exigences fonctionnelles)

- Classe
  - Famille
    - Composant
      - (élément)

Voir CC partie 2 figure 2.1 page 11

La structure – Les classes

11 classes fonctionnelles :

- **Security audit (FAU)**
- **Communication (FCO)**
- **Cryptographic support (FCS)**
- **User data protection (FDP)**
- **Identification & authentification (FIA)**
- **Security management (FMT)**
- **Privacy (FPR)**
- **Protection of TOE security functions (FPT)**
- **Resource utilisation (FRU)**
- **TOE access (FTA)**
- **Trusted path/channels (FTP)**

La structure – Les familles

Voir CC partie 2 figure 2.2 page 12

La structure – Les familles

Voir CC partie 2 figure 2.4 page 18

Les opérations autorisées sur les composants sont sélectionnées à partir de l'ensemble suivant :

- **itération : opération qui permet à un composant d'être utilisé plus d'une fois avec des opérations différentes,**
- **affectation : opération qui permet la spécification d'un paramètre identifié,**
- **sélection : opération qui permet la sélection d'un ou de plusieurs éléments à partir d'une liste,**
- **raffinement : opération qui permet l'addition de détails.**

La structure – Les familles

Dans la classe fonctionnelle FIA Identification & authentication), 6 familles :

- **AFL Authentification failure**
- **ATD User attribute definition**
- **SOS Specification of secrets**
- **UAU User authentication**
- **UID User identification**
- **USB User subject binding**

La structure – Les familles

- **AFL Echecs de l'authentification**
  - **Gestion du comportement de la TOE vis-à-vis des tentatives infructueuses d'accès**
    - **Ex. : Blocage du compte, alerte de l'administrateur ...**

- **ATD Définition des attributs de l'utilisateur**
  - **Définition des attributs de sécurité associés aux utilisateurs**
    - **Ex. d'attributs : Groupe(s), plage horaire de connexion**

- **SOS Spécification de secrets**
  - **Définition des règles liées à la robustesse des secrets**
    - **Ex. : Nb min. de caractères, utilisation obligatoire de chiffres ...**

- **UAU Authentification de l'utilisateur**
  - **Définition des types d'authentification supportés**
    - **Ex. : Auth. dynamique, plusieurs mécanismes, réauthentification, feedback pendant l'authentification**

- **UID Identification de l'utilisateur**
  - **Définition des conditions nécessitant l'identification des utilisateurs**
    - **Ex. : Actions autorisées ou interdites avant identification**

- **USB Lien utilisateur-sujet**
  - **Définition des attributs de sécurité sur les processus activés par les utilisateurs**

La structure – Les composants

Voir CC partie 2, figure 2.3, page 14

ISO 15408 : 206 composants fonctionnels

Voir CC partie 2 figure 7.1 page 88

La structure – Les composants

Classe FIA : Identification et authentification

Famille AFL : Echecs de l'authentification

FIA_AFL.1 Gestion d'un échec de l'authentification

- **Hiérarchique à : aucun autre composant.**
- **FIA_AFL.1.1** La TSF doit détecter quand [affectation : nombre] tentatives d'authentification infructueuses ont eu lieu en relation avec [affectation : liste d'événements liés à l'authentification].
- **FIA_AFL.1.2** Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit [affectation : liste d'actions].
- **Dépendances :** FIA_UAU.1 Programmation de l'authentification

Famille UAU : Authentification de l'utilisateur

FIA_UAU.1 Programmation de l'authentification

- **Hiérarchique à :** aucun autre composant.
- **FIA_UAU.1.1** La TSF doit autoriser que [affectation : liste d'actions transitant par la TSF] pour le compte de l'utilisateur soient effectuées avant qu'il ne soit authentifié.
- **FIA_UAU.1.2** La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
- **Dépendances :** FIA_UID.1 Programmation de l'identification

FIA_UAU.2 Authentification de l'utilisateur avant toute action

- **Hiéarchique à** : FIA_UAU.1
- **FIA_UAU.2.1** La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
- **Dépendances** : FIA_UID.1 Programmation de l'identification

Cadre méthodologique

Cadre normalisé pour les spécifications et pour les évaluations (notamment ISO/IEC 18045, transposition de la CEM v2)

Démarche générale :

- **Définition de la cible d'évaluation (TOE)**

- **Définition des ressources en présence**
- **Définition des menaces, des hypothèses de sécurité et des politiques de sécurité organisationnelles**

- **Définition des objectifs de sécurité**
  - **Sur la cible d'évaluation**
  - **Sur son environnement**
- **Définition des exigences de sécurité TI**
  - **Exigences fonctionnelles**
    - ***En option : Exigences fonctionnelles sur l'environnement TI***
  - **Exigences d'assurance**

Evaluation et certification

- **Evaluation : examen systématique pour déterminer dans quelle mesure une entité est capable de satisfaire aux exigences spécifiées [AFNOR].**

  2 objectifs d'évaluation :
  - **de conformité - le produit/système fait ce qu'il est censé faire, les fonctions de sécurité demandées existent**
  - **d'efficacité - le produit/système fait correctement ce qu'il doit faire : il satisfait aux objectifs de sécurité**

  Mais, en CC, on distingue aussi :
  - **l'évaluation fonctionnelle : quelles exigences fonctionnelles évaluer**
  - **l'évaluation d'assurance : comment évaluer le critère, selon les exigences**
- **Certification : procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus ou un service satisfait aux exigences spécifiées (ISO)**

  Pour les critères communs, selon un schéma de certification , appliqué par des organismes accrédités (procédures formelles pour l'accréditation et les certifications)

Objectif des critères communs :

Obtenir des évaluations reproductibles, impartiales, objectives, comparables

Exigences d'assurance

Assurance : degré de confiance que l'on peut accorder

Les critères d'exigences fonctionnelles selon des niveaux de vérification appelés niveaux d'assurancede l'évaluation (EAL) :

Niveau 1 (EAL1) - testé fonctionnellement

Niveau 2 (EAL2) - testé structurellement

Niveau 3 (EAL3) - testé et vérifié méthodiquement

Niveau 4 (EAL4) - conçu, testé et revu méthodiquement

Niveau 5 (EAL5) - conçu à l'aide de méthodes semi-formelles et testé

Niveau 6 (EAL6) - conception vérifiée à l'aide de méthodes semi-formelles et testé

Niveau 7 (EAL7) - conception vérifiée à l'aide de méthodes formelles et testé

Une évaluation atteint un niveau d'assurance lorsqu'elle répond aux critères exigés pour ce niveau

Exigences d'assurance

Voir CC partie 3, figure 2.1, page 6

Voir CC partie 2, fyableau 6.8, page 73

Niveaux d'évaluation d'assurance

- **Plusieurs degrés de vérification => plusieurs niveaux d'évaluation**

- **L'ISO 15408-3 propose des niveaux dits EAL :**
  - **EAL1 à EAL7 (le plus fort)**
  - **A partir d'EAL4 : vérifications sur le travail des développeurs**
  - **État de l'art : EAL4**
  - **Au-delà : langage semi-formel voire formel**
    (à réserver à des cas très particuliers)
- **A noter :**
  - **Les EAL sont proposés mais pas obligatoires**
  - **Les EAL sont définis pour la compatibilité avec les niveaux ITSEC (E1 à E6)**
  - **Les EAL sont définis pour des produits, pas pour des systèmes**

Voir CC partie 3, tableau B.1, page 223

EAL 7 (maximum) correspond à une évaluation effectuée selon 68 composants de critères d'assurance

Les profils de protection

Les profils de protection (PP) et les cibles de sécurité (ST) :

Un "paquet" d'exigences de sécurité pour une cible d'évaluation déterminée

Le PP : "Je demande", générique, exprime un souhait

La ST : "Je décris", spécifique, fournit des spécifications

Security Requirement		**Functional Component**
Logon controls	Identification of users	FIA_UID.1-2
	Authentication of users	FIA_UAU.1-2
	Limits on repeated login failures (e.g. enforcement of lockout or time delay)	FIA_AFL.1
	Trusted path for logon	FTP_TRP.1-2
	Time of day restriction of access to TOE	FTA_TSE.1
Password selection	Controls on selection of user-generated passwords (e.g. minimum length, password filters, password history)	FIA_SOS.1
	Automated generation of passwords by TOE	FIA_SOS.2
	Password lifetime (expiry) enforcement	FMT_SAE.1

ISO/IEC 15446

Guide for the production of protection profiles and security targets

Domaines de compétences

- **Cartes à puce**
- **Internet, firewalls, sécurisation de message, codes mobiles, codes embarqués, …**
- **Systèmes d'exploitation**
- **Bases de données**

Exemples

Des exemples de profils de protection aisément compréhensibles peuvent être téléchargés depuis le site des CC :

http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5

notamment :

- Firewall with strict requirements April 1999 EAL5+ PPCR9905.pdfPP9905.pdf
- Labeled Security Protection Profile October 1999 EAL3- lspp.pdf
- Role-Based Access Control Protection September 1998 EAL2+- RBAC_987.pdf
- Controlled Access Protection October 1999 EAL3- capp.pdf

ou en version française, sur le site de la DCSSI

http://www.ssi.gouv.fr/fr/confiance/pp.html

- Firewall à exigences réduites v2.2 19 avril 1999
- Firewall à exigences élevées v2.2 19 avril 1999

La norme, un outil

- **L'ISO 15408 est un <u>outil</u>**
  - **Souple**
    - ***Façon dont sont libellées les exigences***
  - **Puissant**
    - ***Exhaustif dans l'identification des types d'exigences sécurité***
  - **Utilisable sans aller jusqu'à l'évaluation formelle, complète et rigoureuse**

- **Mais :**
  - **Pas évident manipuler**
  - **Démarche d'analyse des risques toujours nécessaire**
  - **Pas suffisant pour mettre en œuvre une évaluation**
    - **Il faut en plus :**
      - ***Une démarche d'évaluation***
      - ***Un schéma d'évaluation garanti par le gouvernement***

Structure de la norme

- **3 parties, 3 tomes**
  - **Partie 1 : Introduction - Modèle général**
  - **Partie 2 : Exigences fonctionnelles**
  - **Partie 3 : Exigences d'assurance**

- **Exigences définies de façon arborescente :**
  - **Classes -> Familles -> Composants -> Éléments**
  - **Chaque objet de l'arborescence est référencé :**
    - **par un code**
    - **par un libellé**
  - **Exemples**
    - **FAU : Classe d'exigence fonctionnelle (Fxx) "Security audit"**
    - **FAU_GEN : Famille "Security audit data generation"**
    - **FAU_GEN.2 : Composant n°1 "User identity association"**

Utilisations de l'ISO 15408

- **Définition d'un vocabulaire interne de référence**
  - **TOE, biens, menaces, objectifs de sécurité ...**
- **Spécification de la sécurité**
  - **Définition d'exigences fonctionnelles et d'assurance**
    - **Intégration possible dans un cahier des charges (pas forcément pour un PP)**
  - **Élaboration d'un PP**
    - **Évalué ou non**
    - **Intégration possible dans un cahier des charges**
  - **Élaboration d'une cible de sécurité**
- **Evaluation de la sécurité**
- **Evaluation (assurance) de l'évaluation**

- **Tout ceci pour :**
  - **Un produit**
  - **Un système**

Aides à l'utilisation des CC

- **Les aides documentaires sont multiples :**
  - **Guide méthodologique pour les évaluations, pour tous types de TOE (CEM V1, en cours d'actualisation par l'ISO : ISO/IEC 18045)**
  - **Guides et compléments d'interprétation, pouvant ne concerner que certains types de TOE (cf. http://www.commoncriteriaportal.org/)**
  - **Guide d'aide à l'élaboration de PP (ISO/IEC 15446)**
  - **Procédures pour l'enregistrement de PP (ISO/IEC 15292)**
  - **Framework pour l'assurance de la sécurité TI (ISO/IEC WD 15443)**
  - **Catalogues des PP existants (la plupart sont publiés) et des ST**
  - **Proposition d'une étude sur les évaluations de systèmes (N 3169)**
  - **Documents relatifs aux schémas d'évaluation – certification**
  - **…**

Aides à l'utilisation

- **Quelques outils logiciels existent également :**
  - **CC Toolbox (NIAP)**
  - **CC Profiling Knowledge Database (NIAP)**

- **Il existe d'autres types d'aide :**
  - **Formations (notamment par les certificateurs et évaluateurs)**
  - **Assistances externes**
  - **...**

Incitations à l'utilisation

- **L'apprentissage de l'ISO/IEC 15408 est lourd, d'autant qu'il faut y ajouter tous les aspects connexes (schéma d'évaluation-certification, interprétations …). Une utilisation "dans les règles" est onéreuse**
- **Néanmoins :**
  - **Beaucoup d'investissements déjà consentis**
  - **Outils oprivilégiés des militaires**
  - **Lobbying des organismes certificateurs**
  - **PP dejà publiés et appliqués : PKI, chrono-tachygraphe, etc.**
  - **Évaluation "dans les règles" pas toujours nécessaire**
  - **Incitations de certaines autorités**

    Ex. : La résolution du Conseil de l'Union Européenne du 28/01/2002 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information (n° 2002/C 43/02)

Incitations à l'utilisation

- **Extraits de la résolution 43/02 du Conseil de l'UE :**

Le Conseil de l'UE, (…)

Considérant ce qui suit :

(…)

(10) La norme internationale ISO-15408 (Critères communs) est désormais un système reconnu pour définir les exigences de sécurité des produits d'ordinateurs et de réseaux et évaluer si un produit donné satisfait à ces exigences.

(…)

Invite les États membres :

1) (…)

5) à promouvoir l'utilisation de la norme relative aux critères communs (ISO-15408) et à faciliter la reconnaissance mutuelle des certificats qui s'y rapportent;

(…)

Se félicite de l'intention de la Commission :

1) (…)

3) d'ici la fin 2002, de proposer des mesures appropriées destinées à promouvoir la norme ISO 15408 (critères communs) , à faciliter la reconnaissance mutuelle des certificats et à améliorer le processus d'évaluation des produits, par exemple en définissant des profils de protection appropriés;

(…)

Conclusion

- **L'ISO/IEC 15408 peut servir pour spécifier la sécurité**

- **L'utilisation de l'ISO/IEC 15408 nécessite généralement un investissement important**
- **Son utilisation s'impose dans certains contextes**

- **L'ISO vise originellement des produits (dont l'évaluation porte notamment sur les phases de développement et est donc coûteuse)**

- **Constat sur les systèmes :**
  - **De plus en plus de systèmes créés par intégration de produits divers**
  - **=> impossible d'évaluer ce qui touche à leur développement**

- **Tolérance : considérer certains composants (produits) comme des boites noires**

  => Accent sur les PP et les ST

  => Accent sur les tests de qualification (EAL4, voire EAL3)

  => Coût et durée nettement réduits

Où trouver l'information ?

- **Principaux Sites Web :**
  - **CC.org** http://www.commoncriteriaportal.org/
  - **DCSSI :** http://www.ssi.gouv.fr/fr/dcssi/ **et** http://www.ssi.gouv.fr/fr/confiance/methodologie.html
  - **NIST :** http://csrc.nist.gov/cc

....