



PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI

Exploitation des résultats de la méthode EBIOS[®]
pour rédiger une politique de certification

Version du 21 mars 2003

Qu'est-ce qu'une politique de certification ?

Une politique de certification (PC) définit la politique à mettre en œuvre par une infrastructure de gestion des clés (IGC) pour gérer des certificats de clé publique.

Une fois formalisée, elle peut servir de base à l'établissement d'accords d'interopérabilité entre IGC. Elle permet également la rédaction de déclarations des procédures de certification (DPC), qui représentent l'ensemble des mesures et moyens techniques et juridiques mis en œuvre pour satisfaire les exigences de sécurité définies dans la PC.

Le guide PC² ¹, publié par la DCSSI, décrit des politiques de certification génériques de différents niveaux qui suivent le même plan basé sur le RFC 2527². De plus, il constitue un guide pour la rédaction des DPC.

Quels sont les avantages de la méthode EBIOS pour la rédaction d'une PC ?

La réalisation préalable d'une étude EBIOS offre plusieurs avantages :

- la pertinence des exigences de sécurité de la PC qui couvrent les objectifs de sécurité identifiés dans l'étude (la PC est réellement adaptée au contexte particulier du système qui va mettre en œuvre l'IGC),
- une vision globale de la sécurité, qui ne se limite pas aux seuls aspects concernant l'IGC pour laquelle est rédigée la PC,
- l'exhaustivité et la complétude de l'étude grâce à sa démarche structurée,
- l'implication des parties prenantes, et notamment de l'autorité qui devra valider la PC,
- le recueil de certaines informations devant figurer dans la PC facilité par une démarche méthodologique.

Comment rédiger une PC en utilisant EBIOS ?

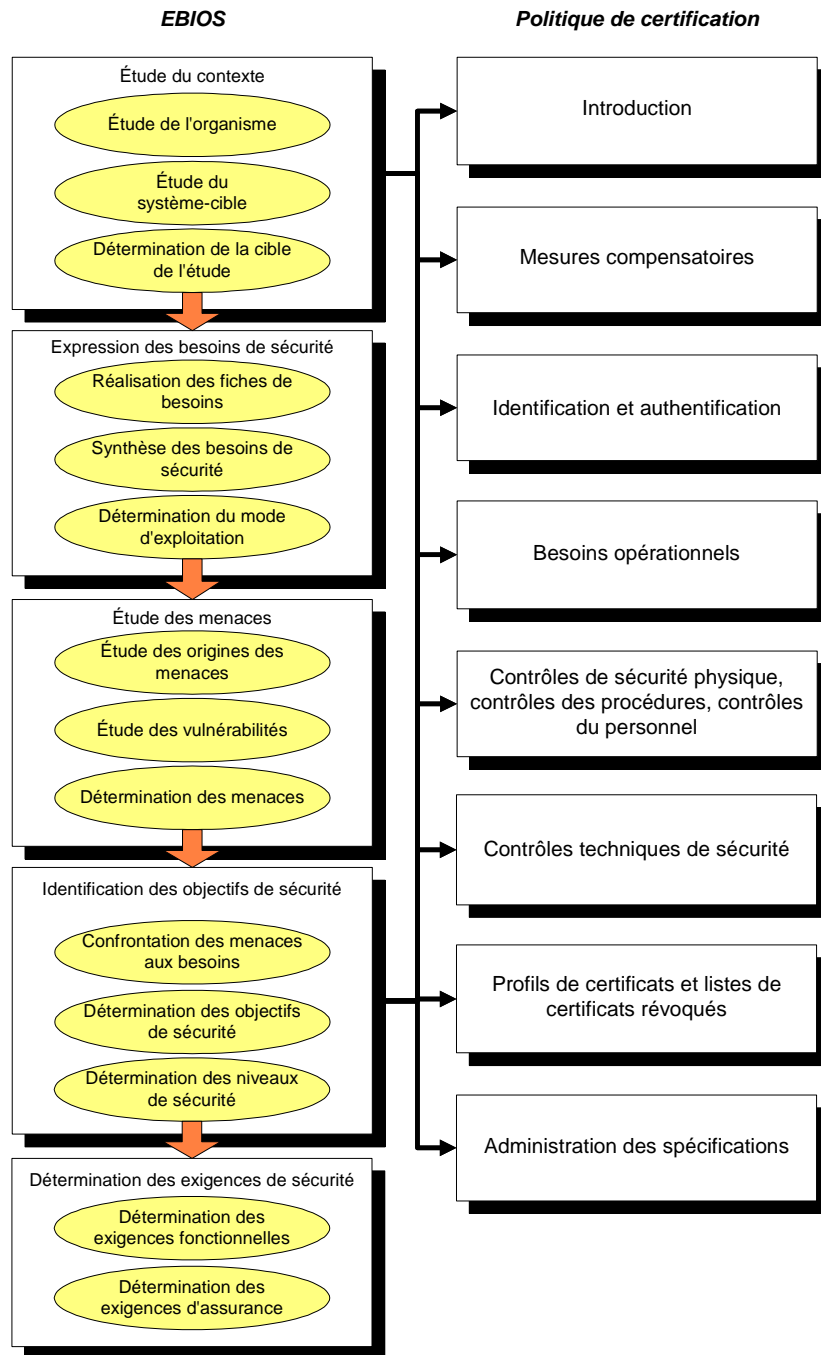
Une solution efficace pour rédiger une PC consiste à :

- réaliser une étude EBIOS sur le périmètre concerné par l'IGC,
- extraire les données nécessaires dans l'étude du contexte (étude de l'organisme, étude du système-cible, détermination de la cible de l'étude de sécurité) et l'identification des objectifs de sécurité de l'étude EBIOS,
- les exploiter en utilisant le guide PC² et éventuellement des exemples de politiques de certification comparables afin de rédiger une politique de certification appliquée au système étudié.

¹ *Procédures et politiques de certification de clés (PC²)* - CISSI - version 2.17 (2001).

² *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* – IETF – Network Working Group (1999).

Pour cela, les données exploitables sont les suivantes :



(pour tout complément d'information : ebios.dcssi@sgdn.pm.gouv.fr)