



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère du Budget
et de la Réforme de l'Etat
DGME/SDAE



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
SGDN - DCSSI

=====

Guide d'exigences de sécurité des téléprocédures types

Démarche et utilisation

=====

VERSION 1.0

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	1/14

Guide d'Exigences Types. Démarche et utilisation	
Référence	Date
Exigences Types- Démarche et utilisation V1.0.doc	15/12/2006
Identification d'objet (OID)	Racine OID et gestionnaire
1.2.250.1.137.2.2.1.2.3.8.1	DGME/SDAE
Responsable	Version
DGME/SDAE-SGDN/DCSSI	1.0
Critère de diffusion	Nombre de pages
Public	14

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
Octobre 2006	0.1	Création du document	FIDENS
Décembre 2006	1.0	Modification homologation	DCSSI/SDAE

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	2/14

SOMMAIRE

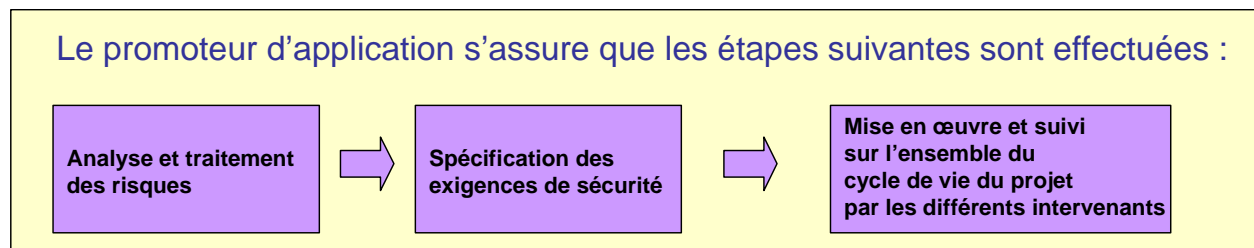
1	INTRODUCTION	4
2	STRUCTURE DU GUIDE.....	6
3	NIVEAU DE SECURITE DE LA TELEPROCEDURE.....	9
4	NAVIGATION ET USAGE DU GUIDE	11
5	PRINCIPES FONDAMENTAUX POUR LA SECURISATION DES TELEPROCEDURES	12
6	REFERENCES BIBLIOGRAPHIQUES	14

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	3/14

1 Introduction

La dématérialisation de la relation entre l'Administration et ses usagers passe par la mise en œuvre de procédures dématérialisées de confiance, c'est-à-dire mettant en œuvre des mesures techniques procédurales et organisationnelles de sécurité adaptées aux besoins des usagers.

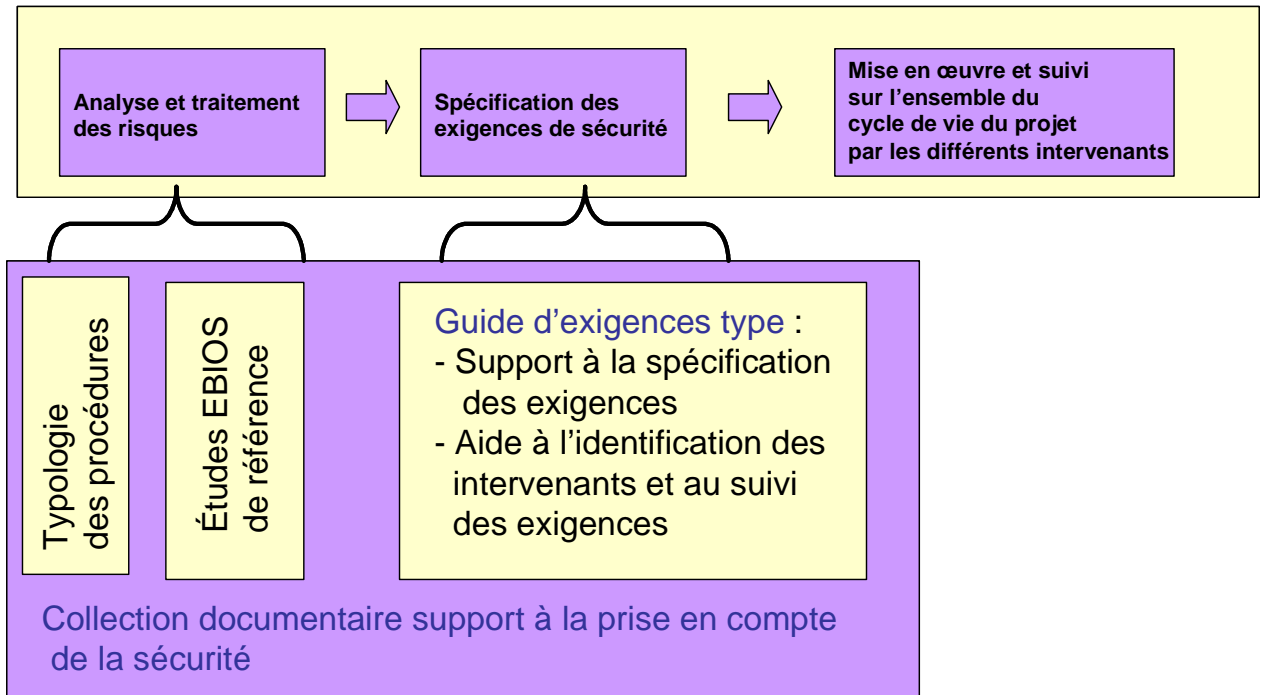
Pour ce faire, le promoteur d'application doit analyser les risques affectant la téléprocédure, identifier les exigences de sécurité nécessaires pour couvrir les risques inadmissibles, et s'assurer de la prise en compte et du suivi de ces exigences par les différents intervenants sur l'ensemble du cycle de vie de son projet.



Afin d'assister les promoteurs d'application dans leur analyse de risques et la définition des objectifs de sécurité correspondants, le Service pour le Développement de l'Administration Electronique (DGME/SDAE) a élaboré une collection documentaire définissant les besoins de sécurité de 7 téléprocédures types : consultation, simulation, démarche en ligne - déclaration, candidature, demandes, paiement en ligne - et inscription à un concours. En procédant par analogie avec l'analyse proche de sa problématique, le promoteur d'application se voit ainsi facilité dans sa démarche d'expression de besoins et de définition de ses objectifs de sécurité.

Il convient ensuite de spécifier les exigences de sécurité en réponse à ces objectifs. Afin d'aider le promoteur dans la spécification des exigences, le SDAE a réalisé le présent guide, qui présente un ensemble d'exigences de sécurité type en réponse aux besoins de sécurité que peuvent présenter les téléprocédures. Le guide facilite également l'identification des intervenants concernés par les exigences, et propose des éléments de contrôle et de suivi de la mise en œuvre des exigences.

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	4/14



Ce guide d'aide à la définition des exigences de sécurité comporte deux sections. Cette première section présente la structure du guide, et sa logique d'utilisation. Elle contient également un rappel des principales exigences qui constituent les règles fondamentales de sécurisation des téléprocédures.

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	5/14

2 Structure du guide

Ce guide d'expression d'exigences pour la sécurité des téléprocédures comporte 17 familles d'exigences, correspondant aux différents thèmes à aborder en matière de sécurité :

- **Gestion des risques**
- **Politique de sécurité**
- **Organisation de la sécurité**
- **Tiers**
- **Gestion des biens**
- **Sécurité liée au personnel**
- **Sécurité physique et environnementale**
- **Sécurité réseau**
- **Sécurité des échanges de données**
- **Sécurité des serveurs et des systèmes**
- **Sécurité des applications et des données applicatives**
- **Gestion de l'exploitation**
- **Contrôle d'accès**
- **Acquisition, développement et maintenance**
- **Gestion des incidents**
- **Gestion du PCA**
- **Conformité et vérification**

Cette structure diffère légèrement de la répartition retenue par l'ISO dans son code de bonne pratique pour la gestion de la sécurité de l'information (ISO 17799). L'approche adoptée est plus pragmatique, et facilite l'appropriation des exigences par les intervenants concernés. Une matrice de correspondance entre les rubriques de l'ISO 17799 et les exigences du présent guide est présentée en annexe de la section 2 du guide.

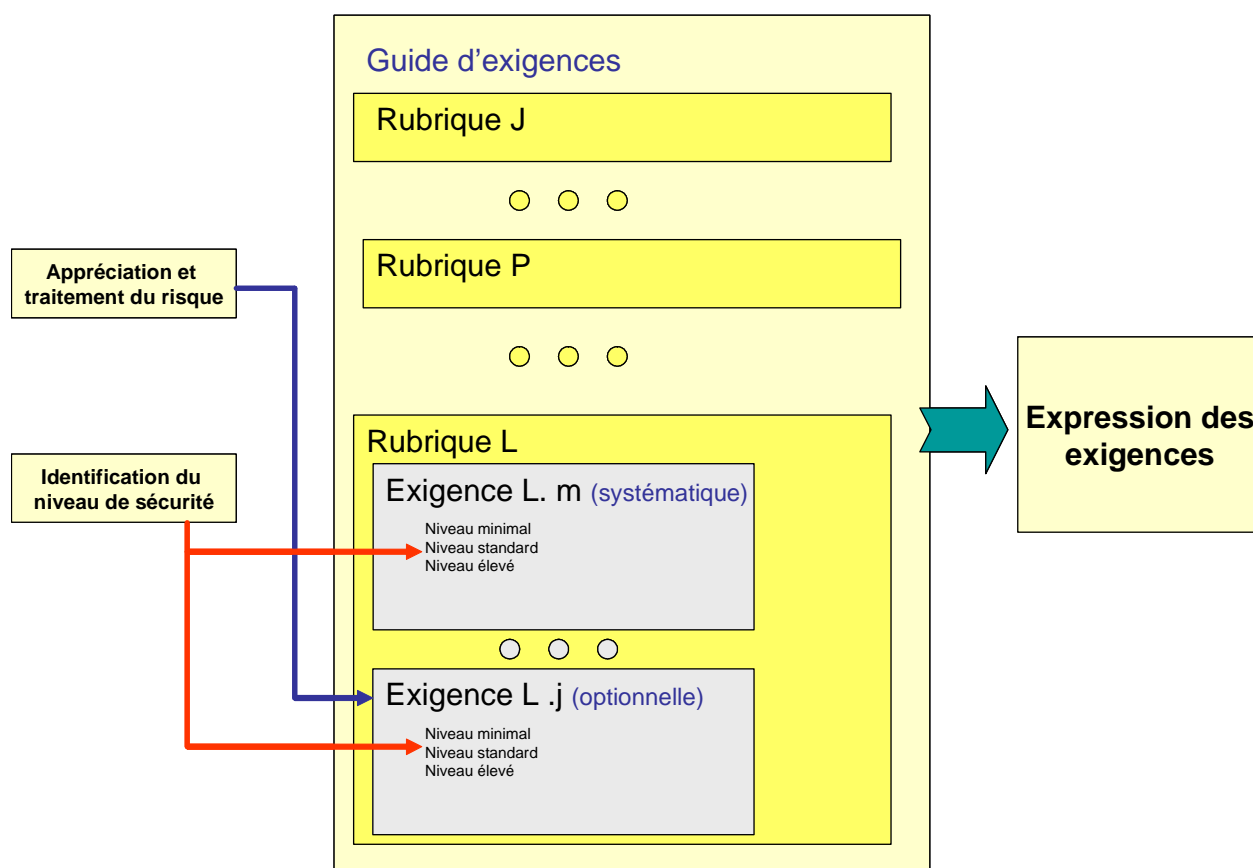
Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	6/14

Chaque famille comporte une liste des exigences propres au thème abordé. Ces exigences sont de deux natures :

- **Systematique**, auquel cas elles doivent être mises en œuvre quelle que soit la téléprocédure cible et les résultats de l'analyse de risques
- **Optionnelle**, auquel cas elles peuvent être mises en œuvre si elles participent à couvrir un objectif de sécurité identifié lors de l'appréciation des risques effectuée par le promoteur d'application

Chaque exigence, systematique ou optionnelle, est déclinée en trois niveaux correspondants au niveau de sensibilité des informations traitées : minimal, standard, élevé.

Il appartient au promoteur d'application, en fonction de l'identification du niveau de sécurité de la téléprocédure, de retenir l'exigence au niveau de sécurité correspondant.



Enfin, chaque exigence est accompagnée d'un tableau présentant :

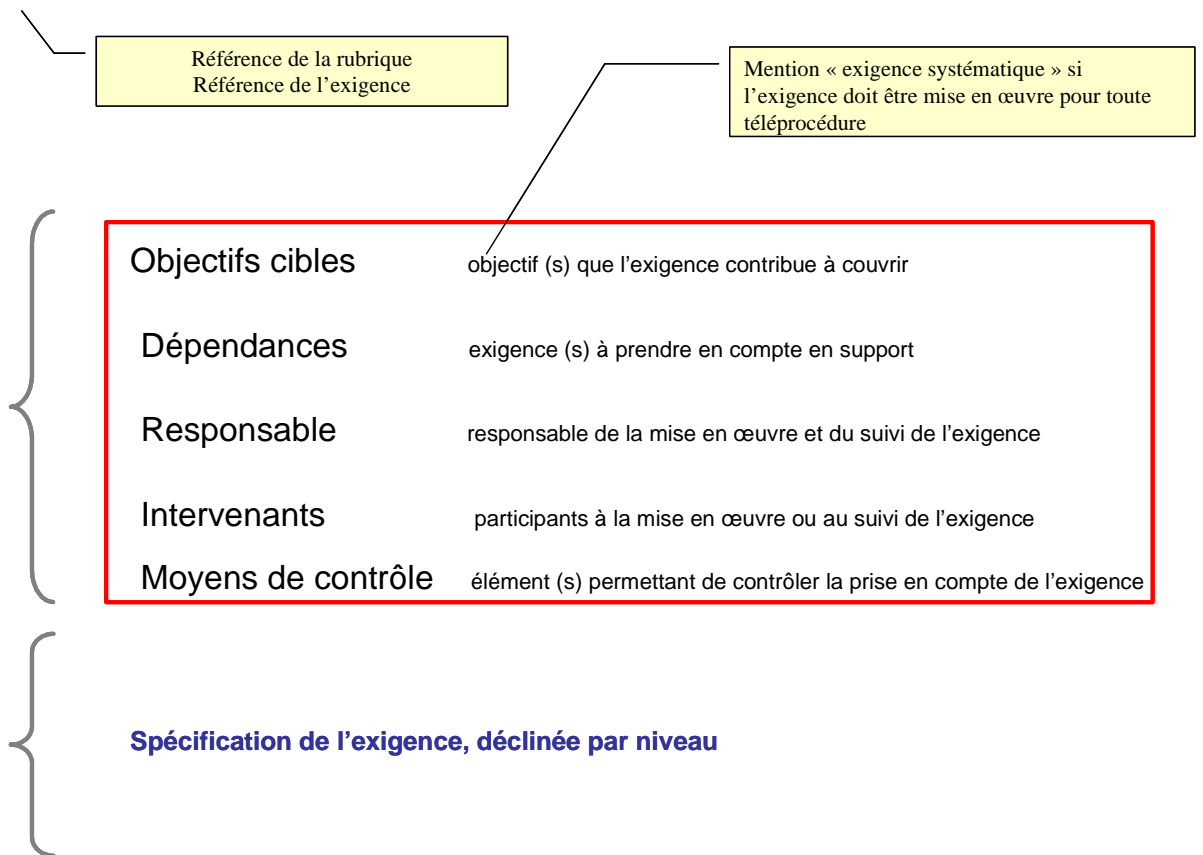
Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	7/14

- Le ou les objectifs couvert (s) par l'exigence
- Les éventuelles dépendances avec d'autres exigences, lorsqu'une exigence en appelle obligatoirement une autre
- Le responsable de la mise en œuvre et du suivi de l'exigence
- le (s) intervenant (s) impliqué (s)
- Les moyens de contrôle envisageables pour s'assurer de la prise en compte de l'exigence, les objectifs couverts, les dépendances avec d'autres exigences, le responsable de la mise en œuvre, les intervenants concernés et les moyens de contrôle de la prise en compte de l'exigence

Les restrictions suivantes doivent être mentionnées :

- L'objectif cible n'est pas identifié lorsque l'exigence est systématique
- Les dépendances ne sont pas mentionnées vis-à-vis des exigences systématiques, puisque celles-ci doivent être prises en compte dans tous les cas

[Ref rub_Ref ex] Intitulé de l'exigence



Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	8/14

3 Niveau de sécurité de la téléprocédure

Le niveau de sécurité de la téléprocédure est caractérisé par la sensibilité des informations traitées ; le promoteur d'application doit retenir un des trois niveaux suivants :

Niveau	Minimal	Standard	élevé
--------	---------	----------	-------

Minimal

Les informations traitées par la téléprocédure ont un caractère public ; ce sont des informations pour lesquelles le non respect de la confidentialité, la disponibilité ou l'intégrité aurait une incidence mineure pour leur propriétaire ou leur dépositaire.

A titre d'exemple, le niveau minimal pourrait être attribué aux téléprocédures suivantes : consultation d'information sur l'environnement, déclaration de changement d'adresse, demande d'extrait de casier judiciaire, demande de situation administrative pour un véhicule, calcul des cotisations sociales pour l'emploi d'une assistante maternelle, demande de certificat d'immatriculation, demande d'ouverture le dimanche, ...

Standard

Les informations traitées peuvent présenter un caractère privé, sans être du type sensible non classifié de défense ; ce sont des informations pour lesquelles le non respect de la confidentialité, l'intégrité ou la disponibilité pourrait avoir une incidence non négligeable en terme d'image, en terme financier, en terme de savoir faire, ... pour leur dépositaire ou leur propriétaire.

Consultation de compte cotisant (URSSAF), consultation de renseignements d'urbanisme, consultation de permis de construire, candidature au permis de conduire, demande de subventions, demande d'aide au logement, inscription à un concours, règlement de TVA ou de charges sociales, ...

Elevé

Les informations traitées par la téléprocédure sont de type sensible non classifiées de défense : ce sont des informations pour lesquelles le non respect de la confidentialité, la disponibilité ou l'intégrité mettrait en cause la responsabilité du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers. A titre d'exemple, on peut citer :

1/ Les informations citées à l'article 6 de la loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, dont la consultation ou la communication, selon les termes de la loi, porteraient atteinte :

- Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif (si elles ne sont pas, par ailleurs, protégées par le secret de défense) ;
- A la monnaie et au crédit public, à la sécurité publique ;

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	9/14

- Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ;
- Au secret de la vie privée, des dossiers personnels et médicaux ;
- Au secret en matière commerciale et industrielle ;
- A la recherche, par les services compétents, des infractions fiscales et douanières ;
- Ou de façon générale, aux secrets protégés par la loi.

2/ Les informations qui ne présentent pas un caractère de secret mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle.

3/ Les informations constitutives du patrimoine scientifique, industriel et technologique.

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	10/14

4 Navigation et usage du guide

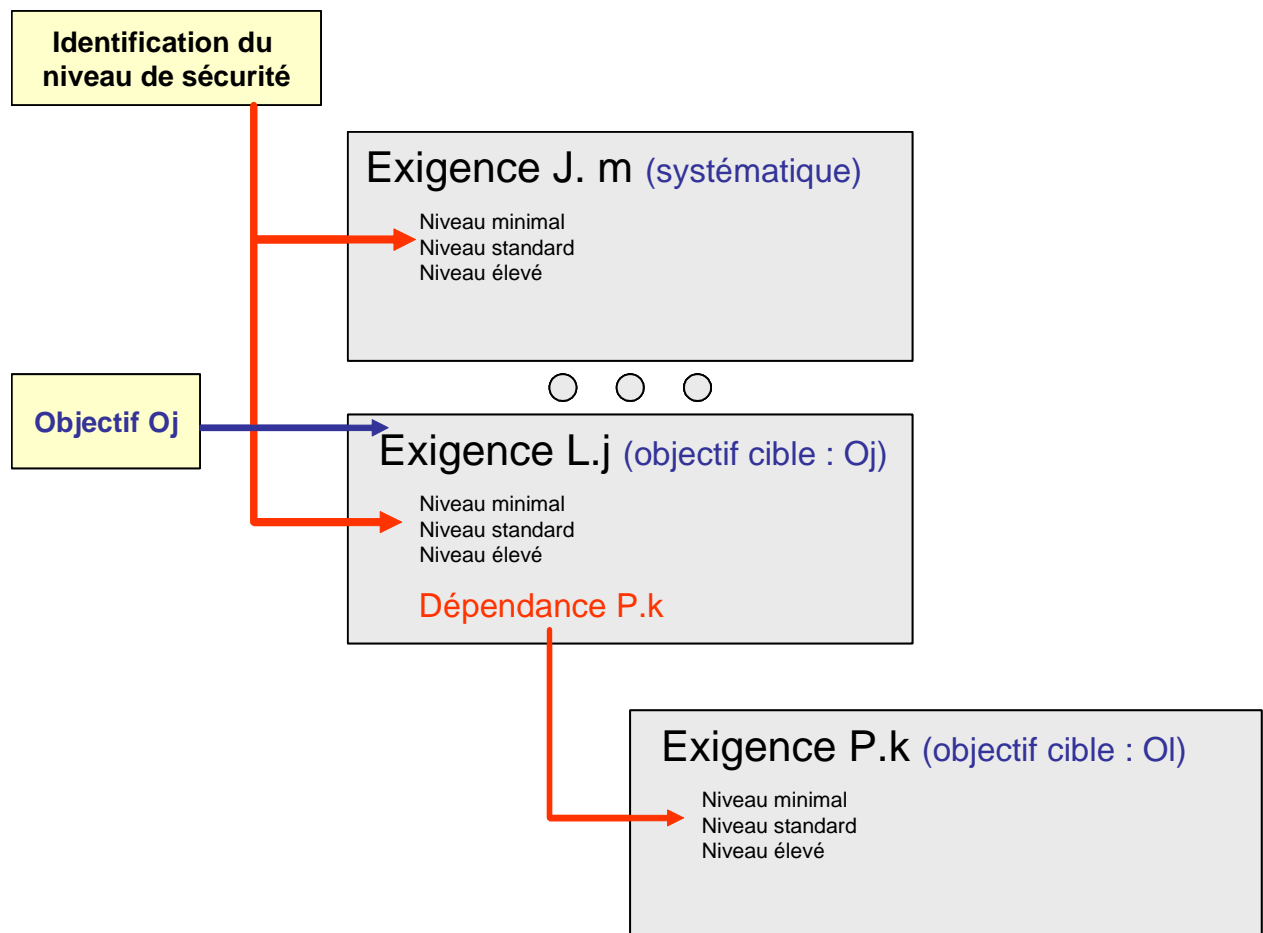
La navigation dans ce guide d'exigences est conditionnée par deux clés :

- les **objectifs de sécurité retenus** suite à l'analyse de risques réalisée par le promoteur d'application
- le **niveau de sensibilité des informations traitées**

Le promoteur identifie les objectifs de sécurité de la téléprocédure, ainsi que le niveau de sensibilité des informations traitées.

Il sélectionne ensuite pour chacune des 17 rubriques du guide d'exigences :

- L'ensemble des exigences systématiques, au niveau de sensibilité correspondant
- Les exigences optionnelles lorsqu'elles répondent à un objectif de sécurité retenu, au niveau correspondant
- Les exigences optionnelles induites par une dépendance avec une exigence sélectionnée, au niveau correspondant.



Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	11/14

5 Principes fondamentaux pour la sécurisation des téléprocédures

① Tout promoteur d'application doit mettre en évidence les risques pesant sur sa téléprocédure (analyse des risques) et les hiérarchiser (évaluation des risques). Il est recommandé de procéder à l'appréciation des risques (analyse et évaluation) à l'aide de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), publiée par la DCSSI. Le Promoteur d'Application pourra s'appuyer sur les dossiers d'analyse des besoins des téléprocédures type élaborés par la DGME, en se référant à la téléprocédure proche de sa problématique.

② Le promoteur d'application doit ensuite identifier le niveau de sensibilité des informations traitées parmi les trois niveaux minimal, standard ou élevé possibles.

③ L'homologation est systématique et conditionne la décision d'emploi de la téléprocédure. Elle est prononcée par l'autorité d'homologation sur la base de :

- l'analyse de risque réalisée
- la justification du niveau de sécurité retenu

Ces exigences devront être complétées par une politique de sécurité, dès lors que le niveau de sécurité retenu est standard.

Pour une téléprocédure traitant d'informations d'un niveau de sécurité élevé, la condition *sine qua non* d'une homologation repose sur l'élaboration d'un dossier de sécurité. Ce dernier devra comporter les éléments suivants :

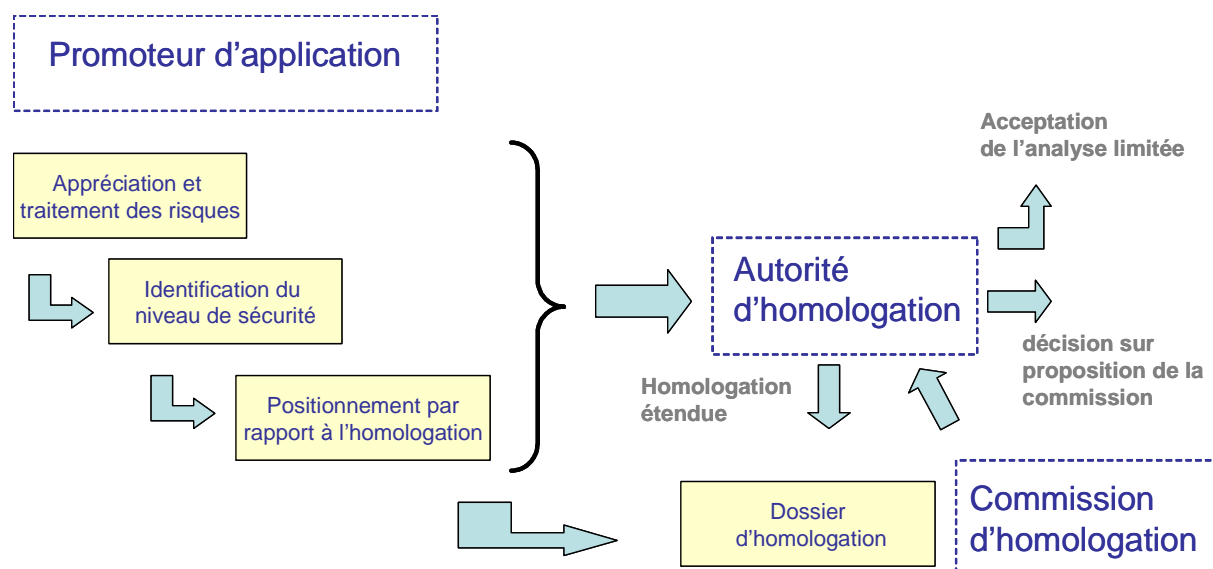
- L'analyse de risques
- L'identification du niveau de sécurité
- La politique de sécurité
- La déclaration d'applicabilité
- Les documents d'applications
- Un rapport d'audit

Les résultats de l'homologation peuvent être les suivants :

- Une homologation provisoire, qui peut devenir définitive après l'application des préconisations formulées par la commission
- Un refus d'homologation
- Une homologation « définitive » pour une durée maximale de 5 ans.

Il appartient à l'autorité d'homologation, au vu des contrôles des réévaluations de l'analyse de risques, de maintenir ou non cette homologation.

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	12/14



④ Dans tous les cas, dès la phase de définition du projet, un document de politique de sécurité doit être formalisé qui définit l'organisation de la sécurité dans le projet, les responsabilités des intervenants concernés et les mesures de sécurité mises en place pour répondre aux objectifs identifiés.

La politique de sécurité pourra référencer d'autres documents de l'organisation (politique de sécurité interne, politique de sécurité physique...) pour un certain nombre de mesures déjà mises en place et tracées dans le référentiel sécurité de l'organisation.

Cette politique de sécurité doit être élaborée à partir des exigences du guide applicables à la téléprocédure, particularisées au contexte opérationnel du projet. La politique de sécurité sera révisée lorsque la téléprocédure entrera en phase d'exploitation, puis en cas d'évolution significative du contexte d'emploi.

⑤ Les mesures de sécurité physiques consistent essentiellement à cloisonner les ressources en fonction de leur sensibilité, et à contrôler les accès sur zones.

⑥ Les mesures de sécurité logiques concernent les composantes, réseau, serveurs et systèmes, échanges de données et applicatives. Au niveau élevé, les dispositifs matériels et logiciels de sécurité utilisés devront avoir été qualifiés au niveau standard par la DCSSI.

⑦ La gestion des incidents, le contrôle et le suivi des mesures préconisées constituent également un volet important de la sécurité des téléprocédures.

⑧ La décision de définir ou non un plan de continuité d'activité pour la téléprocédure appartient au promoteur d'application, en fonction des résultats de l'analyse de risques.

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	13/14

6 Références bibliographiques

CNIL 78-17	Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée le 6 Août 2004
DGME	Analyse de risques des téléprocédures types
DGME PRIS	Politique de Référencement Intersectorielle de Sécurité
ISO 17799	Code de bonnes pratiques pour la gestion de la sécurité de l'information
OTAN AC/35-D/1034	Document complémentaire sur la protection des informations Nato Restricted
SGDN EBIOS	Expression des besoins et identification des objectifs de sécurité
SGDN PSSI	Guide d'élaboration des politiques de sécurité
SGDN GISSIP	Guide d'intégration de la sécurité des systèmes d'information dans les projets
UE, 19 mars 2001	Règlement de sécurité du conseil de l'UE

Guide d'Exigences Types		Démarche et utilisation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.8.1	1.0	15/12/2006	Public	14/14