



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



PREMIER MINISTRE
SGDN - DCSSI

=====

FEROS Types

Téléprocédure de référence

Consultation

=====

VERSION 1.0

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	13/04/2006	Public	1/45

FEROS Types	
Consultation	
Référence	Date
FEROS Type_ ConsultationV1.0.doc	13/04/2006
Identification v1 d'objet (OID)	Racine OID et gestionnaire
1.2.250.1.137.2.2.1.2.3.2.1	DGME/SDAE
Responsable	Version
DGME/SDAE – SGDN\DCSSI	v1.0
Critère de diffusion	Nombre de pages
Public	45

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
15 Avril 2005	0.1		FIDENS
13/04/2006	1.0	Version publiée	DCSSI/SDAE

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	2/45

SOMMAIRE

1 INTRODUCTION 4

 1.1 CONTEXTE GENERAL 4

 1.2 DEFINITION DES RESPONSABILITES 5

2 DESCRIPTION DU SYSTEME ETUDIE 6

 2.1 PRESENTATION DU SYSTEME-CIBLE 7

 2.2 DESCRIPTION DES ELEMENTS ESSENTIELS 8

 2.3 ENJEUX 10

 2.4 ECHELLE DE BESOINS 11

 2.5 BESOINS DE SECURITE DES ELEMENTS ESSENTIELS 12

3 LES RISQUES 18

 3.1 HIERARCHISATION DES RISQUES 18

 3.2 DESCRIPTION DES RISQUES 19

4 OBJECTIFS DE SECURITE 37

5 LES RISQUES RESIDUELS 41

 5.1 METHODES D'ATTAQUE NON RETENUES 41

 5.2 TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS 44

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	3/45

1 Introduction

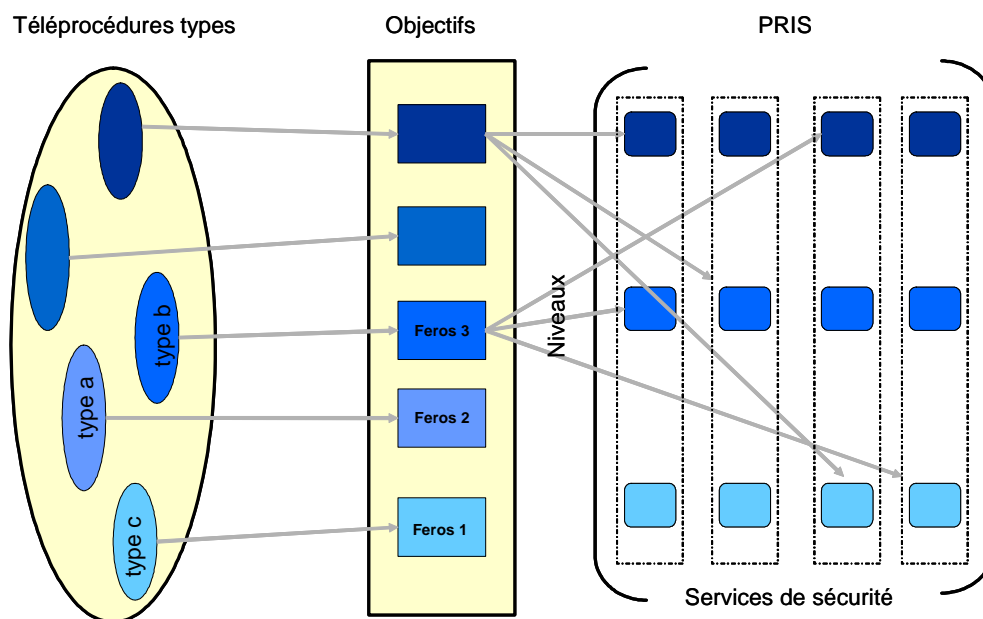
1.1 Contexte général

Poursuivant un triple objectif de modernisation des services, de simplification des démarches et de recherche d'une plus grande efficacité, l'Etat a entamé un processus de modernisation de son Administration. A ce titre, l'Etat s'est engagé dans le développement de services en ligne, gages d'amélioration de la qualité de service et de gain de productivité.

La mise en place de ces relations dématérialisées avec les usagers – citoyens, agents de l'Administration, entreprises, ... -, nécessite une confiance reconnue et partagée par les différents acteurs. Afin de favoriser l'émergence d'un climat de confiance mutuelle propre au développement de ces téléservices, la DCSSI et l'ADAE contribuent aujourd'hui à la définition d'un cadre général de sécurisation des systèmes d'information.

C'est ainsi qu'ils ont élaboré un ensemble documentaire unique baptisé PRIS, « Politique de Référencement Intersectorielle de Sécurité », déterminant pour différents services de sécurité et différents niveaux de sécurité un ensemble d'exigences juridiques et organisationnelles et de spécifications techniques ; cet ensemble deviendra la référence à laquelle les prestataires de services et les fournisseurs de produits devront se conformer.

Pour faciliter l'utilisation de cet ensemble documentaire, l'ADAE a lancé une étude, visant à établir des correspondances entre téléprocédures types et les référentiels PRIS.



FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	4/45

L'analyse générique d'objectifs de sécurité pour des téléprocédures types doit permettre de faciliter et d'homogénéiser les expressions de besoins des donneurs d'ordre en mettant à leur disposition des référentiels sur lesquels ils pourront s'appuyer pour exprimer leurs besoins spécifiques. Par exemple, le promoteur d'une téléprocédure de déclaration d'embauche pourra procéder à partir de la téléprocédure type « déclaration », en analysant les spécificités liées au contexte opérationnel et à la sensibilité des informations traitées, et en conservant les invariants de l'analyse (fonctions, éléments menaçants, ...)

Le choix des téléprocédures types a été réalisé sur une base statistique – étude des téléprocédures les plus largement mises en œuvre – ou en fonction des priorités de l'ADAE.

Les téléprocédures type retenues sont :

- **Consultation**
- **Simulation**
- **Démarche en ligne : déclaration**
- **Démarche en ligne : candidature**
- **Démarche en ligne : demandes**
- **Paiement en ligne**

Le présent document présente l'analyse des objectifs de sécurité pour la téléprocédure type consultation.

1.2 Définition des responsabilités

La présente analyse a été réalisée sous Maîtrise d'œuvre de l'ADAE, avec le soutien de la DCSSI qui a apporté son expertise technique.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	5/45

2 Description du système étudié

La consultation offre aux internautes la possibilité de consulter des informations mises en ligne par l'Administration. Les informations accessibles au travers d'Internet peuvent être en libre accès, ou nécessiter une adhésion préalable, à partir de laquelle un contrôle d'accès est mis en place de manière à limiter les informations accessibles, ou encore à personnaliser les vues des internautes en fonction de leur profil. Les informations accessibles peuvent être du domaine public, ou au contraire privées et réservées à certains profils.

Exemples de mise en œuvre

Consultation des remboursements de la sécurité sociale
Consultation des statistiques industrielles de production
Consultation des demandes d'aides pour les agriculteurs du Cantal (Suivi)
Consultation des formations professionnelles / formations à distance
Consultation de résultats de concours / examens
Consultation d'informations d'organisation de concours
Consultation d'informations relatives à l'environnement
Consultation des archives militaires
Consultation des déclarations, avis d'imposition et paiement
Restitution d'information auprès des entreprises enquêtées
Consultation d'informations économiques
Consultation d'informations sur les fonds structurels européens
Consultation du journal officiel
Consultation des brevets et qualification des marins professionnels
Informations de l'usager sur les conditions de circulation (temps réel)
Mise en ligne des enquêtes DGAFP
Consultation de comptes individuels de retraite dans la fonction publique
Consultation des renseignements d'urbanisme
Consultation d'offres d'emploi
Consultation de permis de construire
Consultation des activités d'animation pour les pro de l'animation V de Paris
Consultation de la nomenclature des voies
Consultation de résultats d'analyse

Scénario retenu pour l'analyse

DESCRIPTION

Au titre de la téléprocédure type, on a retenu la consultation avec inscription préalable, réalisée directement par l'intéressé à partir de ses moyens informatiques personnels. Les données mises en ligne ou conservées peuvent présenter un caractère personnel.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	6/45

USAGER

- Particulier

MODE OPERATOIRE

- Accès depuis les moyens informatiques propres de l'utilisateur

DOMAINE D'APPLICATION

- Consultation d'information pouvant avoir un caractère personnel

2.1 Présentation du système-cible

Afin de rapprocher le modèle de la réalité, l'analyse est menée sur la base d'une téléprocédure existante – ici la consultation d'informations mises en ligne par le Ministère des Finances pour permettre aux usagers de consulter leur déclaration

Systeme-cible

Présentation

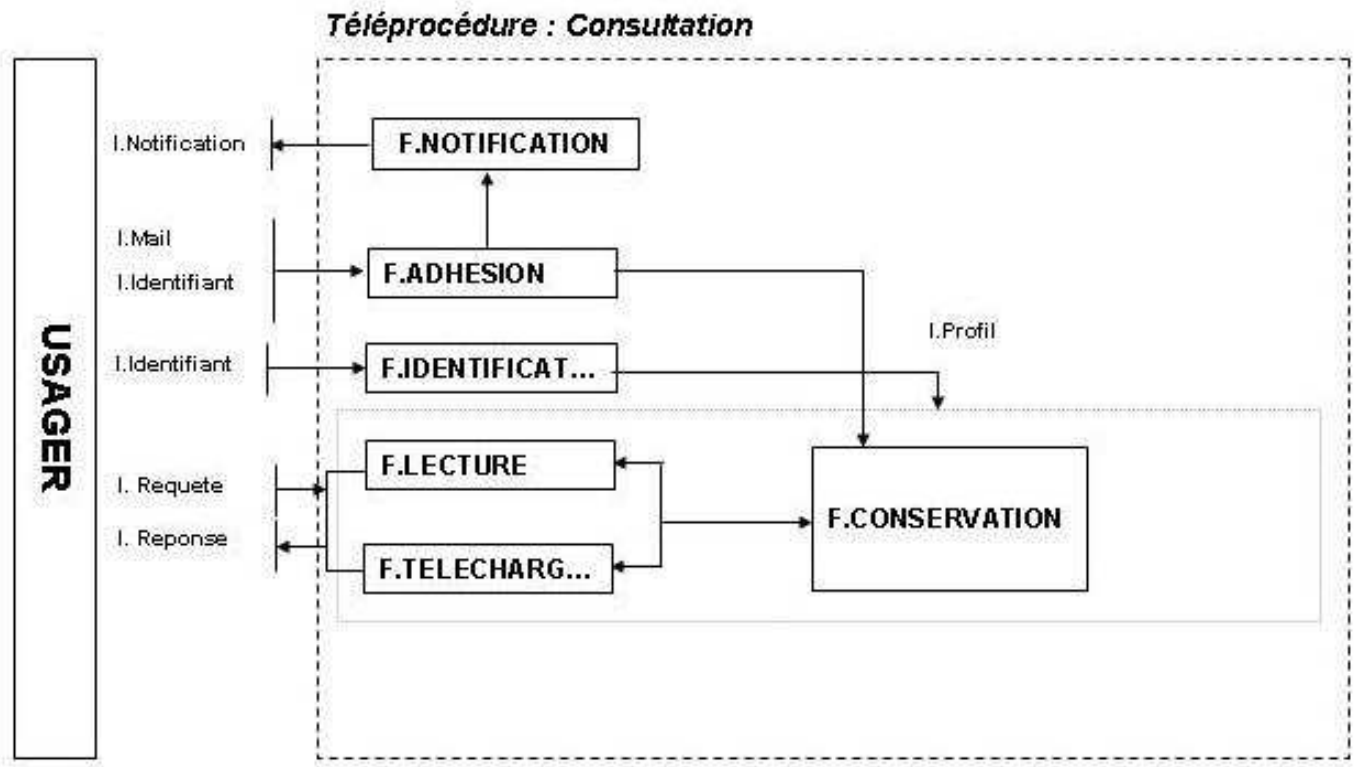
Le portail "www.impots.gouv.fr" offre aux usagers (particuliers et professionnels) des services en ligne facilitant leurs démarches administratives. Le système d'information du ministère des finances propose cinq téléprocédures :

- Gestion des calculs
- Gestion des consultations
- Gestion des déclarations
- Gestion des réductions
- Gestion des paiements

Le système cible retenu pour supporter l'analyse est la téléprocédure "Gestion des Consultations". Elle offre aux usagers la possibilité de prendre connaissance des informations mises en ligne par l'administration.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	7/45

2.2 Description des éléments essentiels



Éléments essentiels

F.NOTIFICATION

Cette fonction finalise le processus d'inscription des usagers en notifiant la prise en compte de l'administration par l'intermédiaire d'un mèl. Les informations de connexion sont communiquées à l'utilisateur par l'intermédiaire de ce mèl.

F.IDENTIFICATION

La sous-fonction "F.IDENTIFICATION" permet de contrôler l'identité des usagers et de charger leurs contextes applicatifs "I.PROFIL". La vérification est réalisée en comparant l'identifiant fourni avec ceux présents dans une base interne. Deux cas sont envisageables:

- L'identifiant existe, le profil est chargé et l'utilisateur peut consulter ses données.
- Aucun enregistrement correspond à l'identifiant fourni, l'utilisateur est invité à s'inscrire ou à en saisir un nouveau.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	8/45

	Il est impératif de passer par le processus d'inscription afin d'obtenir un identifiant de connexion valide.
F.ADHESION	<p>Cette sous-fonction gère les inscriptions des usagers. Ils doivent au préalable accepter les conditions générales d'utilisation du service et ensuite fournir plusieurs informations dont une adresse mèl valide.</p> <p>Cette dernière est utilisée par la fonction "F.NOTIFICATION" afin d'envoyer le mèl de notification qui permet à l'usager de prendre connaissance de son identifiant de connexion.</p>
F.CONSERVATION	<p>Cette fonction est chargée du stockage des informations nécessaires pour le fonctionnement de la téléprocédure. A ce stade de l'analyse, "F.CONSERVATION" couvre la totalité de la problématique de conservation de données et gère:</p> <ul style="list-style-type: none"> • Les identifiants, adresses mèl, profils des usagers • Les informations fiscales des usagers <p>L'interaction avec l'usager est assurée par l'intermédiaire de la fonction "F.LECTURE" qui offre une vue cohérente et personnelle de la partie conservation de données.</p> <p>L'information "I.PROFIL" permet de fixer les autorisations et restrictions qui s'appliquent à l'usager.</p>
F.LECTURE	<p>Cette fonction est au centre de la téléprocédure consultation puisqu'elle permet d'accéder aux informations en mode connecté. On dégage deux types d'utilisation:</p> <ul style="list-style-type: none"> • Lecture d'informations publiques • Lecture d'informations personnelles <p>Dans le premier cas, la fonction "F.IDENTIFICATION" n'est pas appelée et les utilisateurs accèdent aux informations mises en ligne avec un profil générique.</p> <p>Dans le second, l'utilisateur doit fournir son identifiant. En cas de validité, le profil de l'utilisateur est chargé et la fonction "F.LECTURE" offre à l'utilisateur une vue cohérente de ses informations fiscales stockées par la fonction "F.CONSERVATION".</p>
F.TELECHARGEMENT	Cette fonction "F.TELECHARGEMENT" offre la possibilité à l'utilisateur de consulter ses informations fiscales en mode déconnecté.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	9/45

	Elle génère dynamiquement un document sur la base des informations contenues par la fonction "F.CONSERVATION" (Ex: génération d'un fichier PDF) et le rend disponible à l'utilisateur sous une forme téléchargeable.
I.IDENTIFIANT	Identifiant de connexion de l'utilisateur défini lors de son inscription puis fourni lors de chaque accès à la téléprocédure.
I.MAIL	Adresse mël fournie par l'utilisateur lors du processus d'inscription. La validité de l'inscription n'est effective qu'après l'envoi du mël de notification à cette adresse.
I.NOTIFICATION	Mël envoyé par l'administration afin de notifier l'inscription d'un usager. Il requiert un besoin en confidentialité et en intégrité. En effet, le mël contient les informations de connexion de l'utilisateur.
I.PROFIL	Information contenant les autorisations d'accès au contenu et aux fonctions. Le profil de l'utilisateur est chargé après l'identification et définit ce qu'il a le droit de faire. Pour la téléprocédure "Consultation feuilles d'imposition", cette information permet d'identifier les données accessibles en lecture au niveau de la fonction "F.CONSERVATION".
I.REPONSE	Flux de donnée contenant les informations consultées. Suivant la nature de la réponse (données publiques ou personnelles), ces informations peuvent être soumises à un besoin plus ou moins important de confidentialité et d'intégrité.
I.REQUETE	Requête indiquant la ressource à laquelle l'utilisateur souhaite accéder. Elle n'est soumise à aucun critère particulier de sécurité puisqu'elle identifie uniquement l'action à réaliser.

2.3 Enjeux

H.ATTENTES

Description Les récents sondages indiquent une hausse notable des attentes des utilisateurs vis à vis de l'administration électronique. L'augmentation de

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	10/45

l'utilisation d'Internet, la confiance grandissante des usagers ou encore la simplicité d'utilisation sont autant de catalyseurs qui favorisent le développement des téléprocédures. La consultation constitue une pierre angulaire de la mise en place des téléprocédures.

H.ECHANGES

Description L'amélioration des échanges entre les différents services administratifs constitue un enjeu capital du développement de l'administration électronique.

H.DEMATÉRIALISATION

Description Favorisée par l'émergence du projet ADELE, la dématérialisation des procédures administratives correspond à un triple objectif:

- Modernisation des services administratifs.
- Simplification des démarches.
- Recherche d'une plus grande efficacité.

2.4 Echelle de besoins

	Confidentialité	Disponibilité	Intégrité
0	Public	Aucun besoin de disponibilité	Aucun besoin d'intégrité
	Informations publiques.	Une indisponibilité ne provoque aucune perturbation au niveau du système d'information.	La perte d'intégrité n'entraîne aucune gêne.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	11/45

1	Restreinte	Long terme (quelques jours)	Restreint
	Informations personnelles mais dont la divulgation n'engendre aucune conséquence.	Une indisponibilité de quelques jours de l'application ou de la ressource est tolérable.	Une perte d'intégrité est dommageable mais les conséquences restent restreintes.
2	Confidentiel	Moyen terme (quelques minutes)	Besoin moyen d'intégrité
	Informations confidentielles ne devant pas être divulguées. Une perte de confidentialité est grave mais n'entraîne aucune conséquence au niveau économique ou médiatique.	Une indisponibilité momentanée de l'application ou de la ressource est tolérable.	Une perte d'intégrité des informations est grave mais ne touche qu'un nombre limité d'utilisateurs. Les conséquences restent donc restreintes.
3	Confidentiel	Court terme (temps réel)	Important
	Informations confidentielles ne devant pas être divulguées. La fonction des personnes, leur exposition médiatique engendrent de graves conséquences.	Une indisponibilité à une incidence grave.	Une perte d'intégrité des informations est très grave et impacte le fonctionnement global de la téléprocédure. Elle entraîne une perte importante au niveau financier et/ou de l'image de marque.

2.5 Besoins de sécurité des éléments essentiels

Les besoins de sécurité sont listés dans le tableau ci-dessous. En résumé, il y a lieu de distinguer d'une part :

Les éléments personnels relatifs à la gestion de l'utilisateur : identifiant de connexion, adresse e-mail, profil, ... qui présentent des besoins de confidentialité

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	12/45

Les éléments et fonctions relatifs à la gestion et à l'accès à l'information (identification, inscription, lecture, profil, ...) qui présentent des besoins d'intégrité et à un degré moindre de disponibilité

Ces besoins sont génériques, quelque soit la nature des informations consultées (c'est-à-dire qu'ils valent dans le contexte générique de la téléprocédure type, et ne sont pas spécifiques à la consultation des éléments fiscaux).

Et d'autre part :

Les informations consultées, qui présentent dans le cas de la consultation de dossiers fiscaux des besoins de confidentialité et d'intégrité. Ces besoins varient en fonction de la nature des informations mises en ligne : dans le cas d'informations personnelles à caractère social ou médical (dossier médical du patient en ligne par exemple), les besoins de confidentialité et d'intégrité sont maximum. Au contraire, dans le cas de mise en ligne d'informations publiques (rapport d'activité d'un ministère par exemple), les besoins de confidentialité sont inexistantes, et les besoins d'intégrité limités. Il appartient au promoteur de la téléprocédure d'analyser la sensibilité des informations mises en ligne en terme de confidentialité, et d'intégrité.

		Besoin de sécurité	Commentaires
F.NOTIFICATION	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. La manière dont est implémentée la fonction peut être connue de tous sans pour autant nuire à la sécurité du système d'information.
	Disponibilité	1	L'indisponibilité de cette fonction n'empêche pas les utilisateurs déjà inscrits de consulter leurs feuilles d'imposition. Une indisponibilité momentanée est donc acceptable dans la mesure où elle ne touche que les usagers en attente du mèl de notification confirmant leur inscription.
	Intégrité	2	La fonction "F.NOTIFICATION" fait partie intégrante du processus d'inscription. Une perte d'intégrité au niveau de cette fonction est donc grave puisqu'elle empêche toutes nouvelles inscriptions

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	13/45

F.IDENTIFICATION	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. Seules les informations traitées par la fonction expriment ce besoin.
	Disponibilité	2	Une indisponibilité momentanée de la fonction "F.IDENTIFICATION" est tolérable puisque l'utilisateur peut réitérer sa requête ultérieurement.
	Intégrité	2	Une perte d'intégrité au niveau de la fonction "F.IDENTIFICATION" peut avoir des conséquences graves pour les usagers comme pour l'administration.
F.ADHESION	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. La manière dont est implémentée la fonction peut être connue de tous sans pour autant nuire à la sécurité du système d'information.
	Disponibilité	1	Une indisponibilité prolongée au niveau de la fonction "F.ADHESION" est tolérable dans la mesure où celle-ci n'intervient pas dans une période proche d'une échéance fiscale.
	Intégrité	2	Tout comme pour "F.IDENTIFICATION", cette fonction est soumise à un fort besoin en intégrité.
F.CONSERVATION	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. Seules les informations traitées par la fonction expriment ce besoin.
	Disponibilité	2	La fonction "F.CONSERVATION" est soumise à de forts besoins au niveau de la disponibilité puisqu'elle est liée à toutes les autres fonctions.
	Intégrité	2	Une perte d'intégrité serait très préjudiciable car la majorité des informations sont stockées par cette fonction.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	14/45

F.LECTURE	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. La manière dont est implémentée la fonction peut être connue de tous sans pour autant nuire à la sécurité du système d'information.
	Disponibilité	2	Une indisponibilité de cette fonction empêche la consultation d'informations publiques ou personnelles. Cependant, une interruption momentanée est tolérable puisque l'utilisateur peut réitérer sa requête ultérieurement.
	Intégrité	2	Une perte d'intégrité au niveau de "F.LECTURE" est grave. Cependant, les conséquences resteront limitées étant donné que la téléprocédure "Consultation" n'est pas une démarche administrative ayant des conséquences fiscales/réglementaires.
F.TELECHARGEMENT	Confidentialité	0	Les besoins en confidentialité sont nuls vis à vis de cette fonction. La manière dont est implémentée la fonction peut être connue de tous sans pour autant nuire à la sécurité du système d'information.
	Disponibilité	1	Une indisponibilité de cette fonction empêche les usagers de télécharger directement les documents sur leurs postes. Une interruption momentanée est tolérable puisque les utilisateurs possèdent toujours la possibilité de consulter leurs données en mode connecté.
	Intégrité	2	Comme pour la fonction "F.LECTURE", une perte d'intégrité est grave mais les conséquences restent limitées puisque la téléprocédure "Consultation" n'est pas une démarche administrative ayant des conséquences fiscales/réglementaires.
I.IDENTIFIANT	Confidentialité	2	L'identifiant de connexion est une information strictement personnelle. Une perte de confidentialité peut avoir des conséquences très importantes.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	15/45

	Disponibilité	1	La perte des identifiants est tolérable puisque l'utilisateur peut généralement le récupérer via un mail de notification. Les conséquences sont limitées, il devra dans le pire des cas recommencer le processus d'inscription.
	Intégrité	1	Le besoin en intégrité s'apparente à celui en disponibilité. En effet, l'indisponibilité de l'identifiant et la perte d'intégrité sont très similaires.
I.MAIL	Confidentialité	1	L'adresse mail de l'utilisateur est une information personnelle mais son besoin en confidentialité est faible.
	Disponibilité	1	Afin de compléter son inscription, l'utilisateur doit posséder une adresse mail. Le besoin en disponibilité est faible puisque l'utilisateur peut retarder son inscription afin de remplir cette condition.
	Intégrité	1	Une perte d'intégrité au niveau de cette information rend impossible la validation de l'inscription. Cependant, le besoin en intégrité est faible puisque l'utilisateur peut toujours recommencer son inscription en spécifiant une adresse mail valide.
I.NOTIFICATION	Confidentialité	2	Les informations contenues dans le mail de notification sont confidentielles. Il contient un rappel des informations d'identification de l'utilisateur, cette information possède donc le même besoin que "I.IDENTIFIANT".
	Disponibilité	1	Une indisponibilité momentanée est acceptable dans la mesure où seuls les utilisateurs récemment inscrits sont touchés et un retour à la normale est envisageable.
	Intégrité	1	Cette information possède le même besoin en intégrité que "I.IDENTIFIANT" puisque ce dernier est transmis via le mail de notification.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	16/45

I.PROFIL	Confidentialité	1	Le profil est soumis à un besoin de sécurité jugé moindre par rapport à l'identifiant car sa portée est interne.
	Disponibilité	2	Une indisponibilité momentanée de cette information empêche les usagers de consulter leurs données personnelles. Si le retour à la normale est rapide, cette situation est tolérable.
	Intégrité	2	Le besoin en intégrité de cette information est important car elle fixe les autorisations des usagers.
I.REPONSE	Confidentialité	2	Suivant la nature de la réponse, le niveau de confidentialité peut atteindre des niveaux très élevés.
	Disponibilité	2	Une indisponibilité de cette fonction empêche la consultation d'informations publiques ou personnelles. Cependant, une interruption momentanée est tolérable, si le retour à la normal s'effectue rapidement.
	Intégrité	2	Une perte d'intégrité est grave mais les conséquences restent limitées puisque la téléprocédure "Consultation" n'est pas une démarche administrative ayant des conséquences fiscales/réglementaires.
I.REQUETE	Confidentialité	0	La requête de l'utilisateur ne possède aucun besoin de confidentialité.
	Disponibilité	0	La requête de l'utilisateur ne possède aucun besoin de disponibilité.
	Intégrité	1	Les besoins d'intégrité au niveau de la requête sont moindres. Elle peut être ré-émise à tous moments.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	17/45

3 Les risques

Un premier paragraphe présente une hiérarchisation des risques, qui sont décrits de manière exhaustive par la suite.

3.1 Hiérarchisation des risques

	Critère de sécurité	Opportunité
R.DIVULGATION-PERSISTANCE	2	4
R.DIVULGATION-SENSIBILITE	2	4
R.USURPATION-SESSION	2	4
R.VOL-SUPPORT	2	4
R.SATURATION-DIMENSIONNEMENT	2	4
R.PANNE-MATERIELLE	2	3
R.TELECOM-PERTE	2	3
R.PANNE-SAUVEGARDE	2	3
R.ERREUR-ADMINISTRATION	2	3
R.ABUS-AUTORISATION	2	3
R.LOGICIEL-CODE	2	3
R.ORIGINE-NOTIFICATION	2	3
R.DYSFONCTIONNEMENT-ERREUR	2	2
R.ABUS-INJECTION	2	2
R.DIVULGATION-CHIFFREMENT	2	2
R.RECYCLAGE-REMANENCE	2	2

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	18/45

R.ECOUTE-EQUIPEMENT	2	2
R.LOGICIEL-FONCTIONS	2	2
R.ABUS-IDENTIFICATION	2	2
R.SATURATION-RESSOURCES	2	2
R.ABUS-DEBORDEMENT	2	1
R.ALTERATION-CANAL	2	1

3.2 Description des risques

Le tableau suivant détaille les risques identifiés lors de l'analyse.

R.ABUS-AUTORISATION

Libellé R.ABUS-AUTORISATION

Méthode d'attaque 39 - ABUS DE DROIT

Description Le contrôle d'accès doit garantir que seul l'utilisateur autorisé à la possibilité de visualiser ses documents après identification. Dans la pratique, la multiplication des profils peut induire des failles au niveau de ce dispositif.

Un usager malintentionné peut donc exploiter l'une de ces failles en lançant une attaque de type "force brute" sur le nom et le chemin d'accès aux documents afin de visualiser les données d'autres utilisateurs.

Dans un cas extrême, si les documents se trouvent dans des répertoires accessibles depuis Internet, il est même envisageable que ces documents soient référencés par certains moteurs de recherche.

Ce risque touche essentiellement la confidentialité des éléments essentiels.

Les informations "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE" présentent un besoin élevé en confidentialité et sont donc particulièrement exposées à ce risque.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	19/45

	Cela peut engendrer : <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'image de marque
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.ABUS-DEBORDEMENT

Libellé	R.ABUS-DEBORDEMENT
Méthode d'attaque	39 - ABUS DE DROIT
Description	<p>Les problèmes de débordement de tampon constituent une menace de sécurité récurrente au niveau des applications. Généralement, les pirates profitent de ce dysfonctionnement pour faire exécuter à l'application des opérations non conformes avec des privilèges avancés. Cependant, pour les applications Web, l'injection de code (cf. R.ABUS-INJECTION) est une technique plus couramment employée.</p> <p>Une personne malintentionnée soumet une requête qui provoque un débordement de tampon. Elle lui permet de gagner des privilèges administratifs et de dégrader le contenu de certaines pages Web. Cette modification non sollicitée du contenu du site est plus communément appelée "défacement".</p> <p>Dans la majorité des cas un débordement de tampon permet une élévation des privilèges ; les conséquences envisageables sont donc multiples et variées. Ce risque touche aussi bien la disponibilité, l'intégrité ou la confidentialité des éléments essentiels.</p> <p>Les informations "I.IDENTIFIANT", "I.REPONSE", "I.NOTIFICATION" qui présentent un fort besoin en confidentialité peuvent être fortement affectées.</p> <p>Concernant la disponibilité, les fonctions, "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" sont particulièrement impactées puisqu'elles présentent un fort besoin sur ce critère de sécurité. Les informations liées à ces fonctions "I.REPONSE", "I.PROFIL", sont aussi touchées.</p> <p>Pour l'intégrité, toutes les fonctions sont atteintes ainsi que les informations "I.PROFIL", "I.REPONSE".</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	20/45

Cela peut entraîner :

- Une perturbation du fonctionnement interne
- Une interruption de service
- Une perte d'efficacité et de confiance
- Une perte d'image de marque

Opportunité

Moyennement probable où nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.ABUS-IDENTIFICATION

Libellé

R.ABUS-IDENTIFICATION

Méthode d'attaque

39 - ABUS DE DROIT

Description

Les accréditations de compte et jetons de session présentent des failles exploitables. Une personne malintentionnée, douée de très bonnes connaissances techniques, peut compromettre les mots de passe (Force Brute), des clés, des cookies de session afin de faire échouer les restrictions liées à l'identification. Dès lors, il peut consulter les feuilles d'imposition d'autres usagers ou gagner des privilèges élevés.

Comme pour tous les risques issus de cette méthode d'attaque, les trois critères de sécurité peuvent être touchés.

Les informations "I.IDENTIFIANT", "I.REPONSE", "I.NOTIFICATION" qui présentent un fort besoin en confidentialité peuvent être fortement affectés.

Concernant la disponibilité, les fonctions, "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" sont particulièrement impactées puisqu'elles présentent un fort besoin sur ce critère de sécurité. Les informations "I.REPONSE", "I.PROFIL" sont aussi touchées.

Pour l'intégrité, toutes les fonctions sont atteintes ainsi que les informations "I.NOTIFICATION", "I.PROFIL", "I.REPONSE".

Les impacts sont multiples si l'élément menaçant parvient à disposer de privilèges élevés. Cela peut entraîner :

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	21/45

	<ul style="list-style-type: none"> • Une perturbation du fonctionnement interne • Une interruption de service • Une atteinte à la vie privée • Une perte d'image de marque
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.ABUS-INJECTION

Libellé	R.ABUS-INJECTION
Méthode d'attaque	39 - ABUS DE DROIT
Description	<p>Les applications Web passent des paramètres à des applications externes (Ex : Base de données) ou au système d'exploitation local. En contournant les filtres de validation, il devient possible d'insérer des commandes malveillantes et d'attaquer des composants secondaires à travers l'application Web.</p> <p>Par exemple, une personne malintentionnée dissimule une requête SQL dans un des champs d'un formulaire de saisie et visualise, modifie ou supprime la table contenant les accréditations des utilisateurs (Ex: SQL injection).</p> <p>Le scénario ci-dessus montre que ce risque touche les trois critères de sécurité : Confidentialité, Intégrité, Disponibilité.</p> <p>Les informations "I.IDENTIFIANT", "I.REPONSE", "I.NOTIFICATION" qui présentent un fort besoin en confidentialité peuvent être fortement affectés.</p> <p>Concernant la disponibilité, les fonctions, "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" sont particulièrement impactées puisqu'elles présentent un fort besoin sur ce critère de sécurité. Les informations "I.REPONSE", "I.PROFIL" sont aussi touchées.</p> <p>Pour l'intégrité, toutes les fonctions sont atteintes ainsi que les informations "I.NOTIFICATION", "I.PROFIL", "I.REPONSE".</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	22/45

	<p>Cela peut entraîner :</p> <ul style="list-style-type: none"> • Une perturbation du fonctionnement interne • Une interruption de service • Une atteinte à la vie privée • Une perte d'image de marque
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.ALTERATION-CANAL

Libellé	R.ALTERATION-CANAL
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	<p>Le but d'une attaque de type "Man In The Middle" est de se faire passer pour le client auprès du serveur et inversement. L'attaquant agit comme un relais transparent et peut surveiller/modifier l'intégralité du trafic réseau. Ainsi, une personne malintentionnée, douée d'un bon niveau technique, détourne, et modifie les données fiscales transmises.</p> <p>Ce risque porte uniquement atteinte à la confidentialité et l'intégrité des informations qui transitent par le canal de communication.</p> <p>Au niveau de la confidentialité, les informations les plus durement exposées sont celles qui présentent le plus fort besoin ("I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE"). Pour l'intégrité, les éléments essentiels fortement touchés sont les informations "I.PROFIL" "I.REPONSE".</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée • Une perte d'image de marque
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	23/45

R.DIVULGATION-INFORMATIONS

Libellé	R.DIVULGATION-INFORMATIONS
Méthode d'attaque	23 – DIVULGATION
Description	<p>Etant donnée la faible protection en confidentialité des informations sur les supports (pas de chiffrement), par opportunité, une personne ayant accès aux bandes de sauvegarde ou au contenu des disques durs divulgue des informations fiscales.</p> <p>Ce risque touche uniquement les éléments essentiels qui présentent un besoin en confidentialité important. Il s'agit des informations "I.IDENTIFIANT", I.NOTIFICATION", "I.REPONSE".</p> <p>Comme tous les risques qui touchent la confidentialité des informations, cela peut engendrer:</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'image de marque
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.DIVULGATION-PERSISTANCE

Libellé	R.DIVULGATION-PERSISTANCE
Méthode d'attaque	23 - DIVULGATION
Description	<p>Lors de la consultation d'informations sensibles, les données ne doivent pas être conservées dans un emplacement accessible à d'autres utilisateurs. Etant donné le mode de transmission et les directives HTTP employés pour communiquer les documents, une personne peut avoir l'opportunité de visualiser des données fiscales conservées dans le cache du navigateur Web de l'utilisateur.</p> <p>Ce risque porte uniquement atteinte à la confidentialité des informations. Il est particulièrement important pour les informations susceptibles d'être</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	24/45

conservées au niveau du navigateur du client ou du client de messagerie. Il s'agit de "I.REPONSE", "I.NOTIFICATION", "I.IDENTIFIANT".

Ce risque peut provoquer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque

Opportunité Certain ou réalisable par tout public

R.DIVULGATION-SENSIBILITE

Libellé R.DIVULGATION-SENSIBILITE

Méthode d'attaque 23 - DIVULGATION

Description Etant donné le manque d'identification des données sensibles, suite à une erreur d'administration ou par vengeance, une personne interne rend accessible, par l'intermédiaire du site Web, des informations fiscales situées dans la même base de données que les informations publiques.

Comme tous les risques tirés de cette méthode d'attaque, seul le critère de sécurité "Confidentialité" est touché.

Ce risque est particulièrement important pour les informations stockées présentant un fort besoin en confidentialité. Il convient donc de reconsidérer les résultats obtenus pour "I.NOTIFICATION". Il touche essentiellement les informations "I.REPONSE", "I.IDENTIFIANT".

Ce risque peut provoquer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque

Opportunité Certain ou réalisable par tout public

R.DYSFONCTIONNEMENT-ERREUR

Libellé R.DYSFONCTIONNEMENT-ERREUR

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	25/45

Méthode d'attaque 31 - DYSFONCTIONNEMENT LOGICIEL

Description

La prise d'empreinte constitue une étape préalable à l'intrusion au sein d'une application Web. Elle consiste à glaner le maximum d'informations sur la cible afin d'entrevoir les possibilités offertes pour mener à bien les attaques. La présence de bannières explicites, le code source des pages, la nature des erreurs de traitement constituent des informations précieuses.

Une personne externe, possédant des connaissances approfondies dans le domaine des applications Web, soumet la téléprocédure à des conditions d'utilisation extrêmes afin de générer des erreurs non traitées pour prendre connaissance de sa structure interne ou la rendre indisponible. Il obtient toute une série de dumps de base de données lui permettant de mettre en oeuvre des attaques plus complexes.

Un dysfonctionnement au niveau logiciel peut entraîner une perte d'intégrité ou de disponibilité.

Pour la disponibilité, les éléments essentiels les plus touchés sont les fonctions "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.PROFIL", "I.REPONSE".

Au niveau de l'intégrité, il s'agit de la totalité des fonctions et des informations "I.PROFIL", "I.REPONSE"

Cela peut engendrer :

- Une perturbation du fonctionnement interne.
- Des frais financier de secours et de remise à niveau.
- Une interruption de service.
- Une perte d'efficacité, de confiance.
- Une perte d'image de marque.

Opportunité

Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.ECOUTE-EQUIPEMENT

Libellé

R.ECOUTE-EQUIPEMENT

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	26/45

Méthode d'attaque	19 - ÉCOUTE PASSIVE
Description	<p>Profitant de la faible protection des équipements de communication et de la surestimation de la protection fournie par les moyens cryptographiques employés, une personne malintentionnée, très expérimentée, capture et déchiffre une feuille d'imposition transitant entre l'utilisateur et la téléprocédure.</p> <p>Ce risque peut porter atteinte à la confidentialité des informations émettant un fort besoin en sécurité au niveau de ce critère.</p> <p>Les éléments essentiels le plus fortement touchés sont "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE".</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'image de marque
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.ERREUR-ADMINISTRATION

Libellé	R.ERREUR-ADMINISTRATION
Méthode d'attaque	38 - ERREUR D'UTILISATION
Description	<p>La téléprocédure devient indisponible suite à la détérioration de données due à une mauvaise manipulation lors de l'administration, la maintenance ou la mise à jour des serveurs.</p> <p>Les erreurs d'administration portent atteinte à la disponibilité et à l'intégrité des éléments essentiels.</p> <p>Pour la disponibilité, les plus touchées sont les fonctions "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.PROFIL", "I.REPONSE".</p> <p>Au niveau de l'intégrité, la totalité des fonctions et les informations "I.PROFIL", "I.REPONSE"</p> <p>Cela peut engendrer :</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	27/45

	<ul style="list-style-type: none"> • Une interruption de service • Une perte d'efficacité, de confiance • Des perturbations du fonctionnement interne • Une perte d'image de marque • Le limogeage de personnel
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.LOGICIEL-CODE

Libellé	R.LOGICIEL-CODE
Méthode d'attaque	26 - PIÉGEAGE DU LOGICIEL
Description	<p>L'application Web peut être utilisée comme un vecteur d'attaque. Une personne malveillante possédant un très bon niveau technique, par l'intermédiaire d'une requête falsifiée, insère un script au niveau d'une page Web de la téléprocédure. Grâce à la relation de confiance établie entre l'utilisateur et le site de l'administration, le script sera exécuté de manière transparente au niveau du navigateur de tous les clients qui visualiseront cette page. La divulgation de fichiers (cookies), l'installation de chevaux de Troie devient possible par l'intermédiaire de cette technique.</p> <p>Suivant la nature des scripts, ce risque touche les trois critères de sécurité.</p> <p>Les informations "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE" sont fortement touchées au niveau de la confidentialité.</p> <p>Pour la disponibilité, les éléments essentiels "F.IDENTIFICATION", "F.LECTURE", "F.TELECHARGEMENT", "I.PROFIL", "I.REPONSE" possèdent des besoins importants susceptibles d'être impactés.</p> <p>Enfin, ce risque peut aussi porter atteinte à l'intégrité des fonctions "F.NOTIFICATION", "F.IDENTIFICATION", "F.LECTURE", "F.TELECHARGEMENT" et des informations "I.PROFIL", "I.REPONSE".</p> <p>Cela peut engendrer :</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	28/45

	<ul style="list-style-type: none"> • Des interruptions de service • Une atteinte à la vie privée des usagers • Une perte d'efficacité, de confiance • Une perte d'image de marque
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.LOGICIEL-FONCTIONS

Libellé	R.LOGICIEL-FONCTIONS
Méthode d'attaque	26 - PIÉGEAGE DU LOGICIEL
Description	<p>Une personne malintentionnée, qui possède des connaissances approfondies sur le fonctionnement interne de la téléprocédure, outrepassa les règles de sécurité en utilisant des fonctionnalités cachées introduites durant la phase de conception de l'application.</p> <p>De la même manière que pour "R.LOGICIEL-CODE", ce risque touche les trois critères de sécurité.</p> <p>Les informations "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE" sont fortement touchées au niveau de la confidentialité.</p> <p>Pour la disponibilité, les éléments essentiels "F.IDENTIFICATION", "F.LECTURE", "F.TELECHARGEMENT", "I.PROFIL", "I.REPONSE" possèdent des besoins importants.</p> <p>Enfin, ce risque peut aussi porter atteinte à l'intégrité des fonctions "F.NOTIFICATION", "F.IDENTIFICATION", "F.LECTURE", "F.TELECHARGEMENT" et des informations "I.PROFIL", "I.REPONSE".</p> <p>Les impacts peuvent être multiples. Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers. • Une perte d'image de marque.
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	29/45

matériel spécifique

R.ORIGINE-NOTIFICATION

Libellé	R.ORIGINE-NOTIFICATION
Méthode d'attaque	24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE
Description	<p>Dans le but de perturber la téléprocédure ou d'obtenir des informations confidentielles, une personne malveillante émet des notifications falsifiées afin de détourner les communications sur son propre site. Sous couvert de la similitude avec la téléprocédure du ministère des finances, les utilisateurs trompés sont amenés à communiquer des informations sensibles (Ex: Identifiants).</p> <p>Ce risque porte atteinte aux éléments essentiels possédant un fort besoin en confidentialité. Il s'agit des informations "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE".</p> <p>Les impacts sont :</p> <ul style="list-style-type: none"> • Perte d'efficacité, de confiance • Atteinte à la vie privée des usagers
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.PANNE-MATERIELLE

Libellé	R.PANNE-MATERIELLE
Méthode d'attaque	28 - PANNE MATÉRIELLE
Description	<p>Suite à la panne involontaire de l'un des équipements matériel, l'administrateur se trouve dans l'impossibilité de rétablir rapidement le fonctionnement de la téléprocédure. Cette menace est amplifiée si le principe de redondance n'est pas appliqué.</p> <p>Ce risque porte atteinte à la disponibilité et à l'intégrité des éléments essentiels.</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	30/45

Pour la disponibilité, les plus touchés sont les fonctions "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.PROFIL", "I.REPONSE".

Au niveau de l'intégrité, il s'agit de la totalité des fonctions et des informations "I.PROFIL", "I.REPONSE".

Cela peut engendrer :

- Une perturbation du fonctionnement interne.
- Des frais financier de secours et de remise à niveau.
- Une interruption de service.
- Une perte d'efficacité, de confiance
- Une perte d'image de marque.

Opportunité

Certain ou réalisable par tout public

R.PANNE-SAUVEGARDE

Libellé R.PANNE-SAUVEGARDE

Méthode d'attaque 28 - PANNE MATÉRIELLE

Description A cause du mauvais stockage des supports de sauvegarde, l'administrateur se trouve dans l'impossibilité de récupérer les données perdues suite à la panne du disque dur d'un serveur.

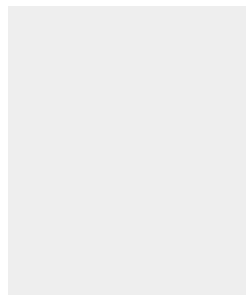
Tout comme M.PANNE-MATERIEL", ce risque porte atteinte à la disponibilité et à l'intégrité de certains éléments essentiels.

Pour la disponibilité, les plus touchés sont les fonctions "F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.PROFIL", "I.REPONSE".

Au niveau de l'intégrité, il s'agit de la totalité des fonctions et des informations "I.PROFIL", "I.REPONSE".

Cela peut engendrer :

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	31/45



- Une perturbation du fonctionnement interne.
- Des frais financiers de secours et de remise à niveau.
- Une interruption de service.
- Une perte d'image de marque.

Opportunité

Certain ou réalisable par tout public

R.RECYCLAGE-REMANENCE

Libellé

R.RECYCLAGE-REMANENCE

Méthode d'attaque

22 - RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS

Description

Profitant de sa bonne connaissance du principe de rémanence des données, une personne malintentionnée récupère des informations stockées sur des supports mal recyclés et rend publique toute une série de données fiscales.

Ce risque touche uniquement les éléments essentiels qui présentent un fort besoin en confidentialité. Il s'agit des informations "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE".

Comme tous les risques qui touchent la confidentialité des informations, cela peut engendrer :

- Une atteinte à la vie privée des usagers.
- Une perte d'image de marque.

Opportunité

Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.SATURATION-DIMENSIONNEMENT

Libellé

R.SATURATION-DIMENSIONNEMENT

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	32/45

Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Lors du dimensionnement des ressources, il convient de bien étudier le contexte d'utilisation global de la téléprocédure. Une mauvaise appréciation de l'usage du système provoque des problèmes de performance ou d'indisponibilité pour les usagers.</p> <p>De la même manière que pour "R.SATURATION-DENI", ce risque touche la disponibilité des éléments essentiels.</p> <p>Les plus touchés sont les fonctions " F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.IDENTIFIANT", "I.PROFIL", "I.REPONSE".</p> <p>Ce risque peut provoquer :</p> <ul style="list-style-type: none"> • Une perturbation du fonctionnement interne • Une interruption de service • Une perte d'efficacité, de confiance • Une perte d'image de marque
Opportunité	Certain ou réalisable par tout public

R.SATURATION-RESSOURCES

Libellé	R.SATURATION-RESSOURCES
Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Une attaque courante consiste à soumettre volontairement le dispositif à un nombre important de requêtes afin d'empêcher les utilisateurs légitimes de se connecter.</p> <p>Dans le cas présent, une personne malintentionnée, possédant un niveau élevé de compétence, s'attaque aux services réseaux (Ex: Syn Flooding) ou directement à l'application Web (Ex: Saturation du pool de connexion de la base de donnée) afin de paralyser la téléprocédure.</p> <p>Ce risque touche uniquement la disponibilité des éléments essentiels. Ceux qui présentent le besoin en sécurité le plus important au niveau de ce critère sont particulièrement impactés.</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	33/45

Il s'agit des fonctions " F.IDENTIFICATION", "F.CONSERVATION", "F.LECTURE", "F.TELECHARGEMENT" et des informations "I.PROFIL", "I.REPONSE".

Ce risque peut provoquer :

- Une perturbation du fonctionnement interne
- Une interruption de service
- Une perte d'efficacité et de confiance
- Une perte d'image de marque

Opportunité

Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

R.TELECOM-PERTE

Libellé

R.TELECOM-PERTE

Méthode d'attaque

13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

Description

Une personne malintentionnée, possédant des connaissances techniques pointues, s'attaque à un des éléments de communication afin de rendre indisponible la téléprocédure. L'impossibilité de basculer rapidement vers une ligne de secours et l'absence de clauses contractuelles traitant du délai maximum d'indisponibilité aggrave d'autant plus la situation.

Ce risque touche la disponibilité des informations qui transitent par le canal de communication et possèdent un besoin en disponibilité important.

Il s'agit principalement de "I.IDENTIFIANT", "I.REPONSE". Il convient d'écartier "I.PROFIL" qui ne circule qu'en interne.

Cela peut provoquer :

- Une interruption de service
- Une perte d'efficacité, de confiance
- Une perte d'image de marque

Opportunité

Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	34/45

R.USURPATION-SESSION

Libellé	R.USURPATION-SESSION
Méthode d'attaque	40 - USURPATION DE DROIT
Description	<p>Par opportunité, une personne malintentionnée se substitue à un autre utilisateur et visualise ses données fiscales en utilisant une session laissée ouverte.</p> <p>Ce risque porte atteinte à la confidentialité des informations.</p> <p>Etant donné le scénario de menace émis, l'élément essentiel le plus fortement touché est "I.REPONSE". En effet, l'attaquant consulte les données fiscales d'un autre usager.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'efficacité, de confiance • Une perte d'image de marque
Opportunité	Totalement improbable ou infaisable

R.VOL-SUPPORT

Libellé	R.VOL-SUPPORT
Méthode d'attaque	20 - VOL DE SUPPORTS OU DE DOCUMENTS
Description	<p>Par opportunité, du fait d'un manque de formalisation ou de protection au niveau des supports, une personne malintentionnée dérobe un jeu de sauvegarde ou le disque dur d'un serveur positionné sur un rack. Cette menace est d'autant plus importante si elle s'accompagne d'une absence ou d'une surestimation de la protection offerte par le chiffrement (M.DIVULGATION-CHIFFREMENT).</p> <p>Ce risque touche la confidentialité des informations stockées sur les</p>

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	35/45

supports.

Les informations présentant un besoin élevé en confidentialité "I.IDENTIFIANT", "I.NOTIFICATION", "I.REPONSE" sont particulièrement touchées par ce risque.

Cela peut engendrer :

- Une infraction aux lois, aux règlements
- Le limogeage de personnel
- Une atteinte à la vie privée des usagers
- Une perte d'image de marque

Opportunité

Certain ou réalisable par tout public

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	36/45

4 Objectifs de sécurité

O.ADMINISTRATION

Contenu Des mesures doivent être prises afin de faciliter l'administration du système et de limiter l'impact d'éventuelles erreurs.

O.AUTORISATION

Contenu Des mesures techniques doivent être prises afin de garantir que seul l'utilisateur dûment identifié peut accéder à ses données fiscales.

O.CANAL

Contenu Des mesures doivent être prises afin d'empêcher l'altération par une tierce personne des informations transitant par le canal de communication.

O.CHIFFREMENT

Contenu Seules les informations absolument nécessaires doivent être conservées. Des mesures cryptographiques adaptées à la sensibilité des informations doivent être prises pour garantir la confidentialité des informations sur les supports.

O.CODE

Contenu Des mesures doivent être prises pour s'assurer que les paramètres saisis par l'utilisateur ne permettent pas d'insérer du code malveillant au niveau des pages Web.

O.DEBORDEMENT

Contenu Des mesures techniques doivent être prises afin d'empêcher d'éventuelles attaques de type "Débordement de Tampon".

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	37/45

O.DIMENSIONNEMENT

Contenu Des mesures doivent être prises afin de quantifier et d'adapter les ressources nécessaires à l'exploitation du système.

O.CANAL CONF

Contenu Des mesures doivent être prises pour garantir la confidentialité, l'authentification d'origine des informations en transit

O.ERREUR

Contenu Des mesures doivent être prises pour éviter la divulgation d'informations techniques sensibles en cas de dysfonctionnement de la téléprocédure ou de l'utilisation d'outils de prise d'empreinte.

O.FONCTION

Contenu Des mesures doivent être prises pour s'assurer qu'aucune fonction cachée ne permet de compromettre le fonctionnement de la téléprocédure.

O.IDENTIFICATION

Contenu Des mesures doivent être prises pour renforcer le dispositif d'identification et de gestion des sessions.

O.INJECTION

Contenu Des mesures doivent être prises afin d'éviter la transmission de commandes malveillantes sur des composants externes grâce à l'application Web.

O.NOTIFICATION

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	38/45

Contenu Des mesures doivent être prises afin d'empêcher la falsification de la source et du contenu des notifications.

O.PANNE

Contenu Le système doit être dimensionné de manière à ce qu'un dysfonctionnement matériel présente un impact limité dans le temps

O.PERSISTANCE

Contenu Des mesures doivent être prises afin d'éviter la duplication persistante des informations au niveau du poste de l'utilisateur.

O.PERTE

Contenu Les dysfonctionnements des moyens de télécommunication ne doivent pas entraver la disponibilité de la téléprocédure.

O.REMANENCE

Contenu Des mesures doivent être prises afin de s'assurer qu'aucune donnée ne subsiste sur les supports destinés à être recyclés.

O.RESSOURCES

Contenu Des mesures doivent être prises afin de limiter les ressources attribuées à chaque utilisateur au niveau de l'application et de protéger les équipements contre la surcharge.

O.SAUEGARDE

Contenu Des mesures doivent être prises afin de garantir la récupération des informations à partir des sauvegardes effectuées.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	39/45

O.SESSION

Contenu Des mesures doivent être prises pour éviter la reprise de sessions laissées ouvertes.

O.SENSIBILITE

Contenu Des mesures doivent être prises afin d'identifier la sensibilité des données et réduire au maximum la divulgation involontaire d'informations confidentielles.

O.VOL

Contenu Des mesures techniques et organisationnelles doivent être prises afin d'empêcher le vol des supports de stockage et de sauvegarde.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	40/45

5 Les risques résiduels

5.1 Méthodes d'attaque non retenues

01- INCENDIE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

02- DÉGÂTS DES EAUX

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

03 - POLLUTION

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

04 - SINISTRE MAJEUR

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

06 - PHÉNOMÈNE CLIMATIQUE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

07 - PHÉNOMÈNE SISMIQUE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	41/45

08 - PHÉNOMÈNE VOLCANIQUE

Justification Méthode d'attaque jugée inadaptée dans le cadre de cette analyse.

09 - PHÉNOMÈNE MÉTÉOROLOGIQUE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

10 - CRUE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

11 - DÉFAILLANCE DE LA CLIMATISATION

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES

Justification Méthode d'attaque jugée trop improbable.

15 - RAYONNEMENTS THERMIQUES

Justification Méthode d'attaque jugée trop improbable.

16 - IMPULSIONS ÉLECTROMAGNÉTIQUES

Justification Méthode d'attaque jugée trop improbable.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	42/45

17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS

Justification Méthode d'attaque jugée trop improbable.

18 - ESPIONNAGE A DISTANCE

Justification Méthode d'attaque retenue uniquement pour des opérations très sensibles où la quantité d'information est limitée.

21 - VOL DE MATÉRIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette étude.

25 - PIÉGEAGE DU MATÉRIEL

Justification Méthode d'attaque écartée initialement dans le cadre de cette étude.

27 - GÉOLOCALISATION

Justification Méthode d'attaque initialement écartée dans le cadre de cette analyse.

29 - DYSFONCTIONNEMENT DU MATÉRIEL

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

33 - UTILISATION ILLICITE DES MATÉRIELS

Justification Méthode d'attaque jugée improbable pour la téléprocédure consultation.

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	43/45

34 - COPIE FRAUDULEUSE DE LOGICIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

41 - RENIEMENT D'ACTIONS

Justification Aucune action ayant une réelle incidence lors de l'utilisation de la téléprocédure consultation.

42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

5.2 Tableau de couverture des risques par les objectifs

	O.SESSION	O.VOL	O.SENSIBILITE	O.RESSOURCES	O.SAUVEGARDE	O.REMANENCE	O.PERTE	O.PERSISTANCE	O.PANNE	O.NOTIFICATION	O.INJECTION	O.IDENTIFICATION	O.FONCTION	O.ERRREUR	O.CANAL CONF	O.DIMENSIONNEMENT	O.DEBORDEMENT	O.CODE	O.CHIFFREMENT	O.CANAL	O.AUTORISATION	O.ADMINISTRATION	
R.DIVULGATION-PERSISTANCE								X															
R.DIVULGATION-SENSIBILITE																							X
R.USURPATION-SESSION																							X

FEROS Types		Consultation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.2.1	v1.0	04/04/2008	Public	44/45

