FORMATION

EBIOS *Risk Manager*

Livret stagiaire

V.2 • Mars 2024

Formation CFSSI

Correction étude de cas SGTIN

Etude de cas – Renouvellement de titre d'identité numérique

Introduction

Vous êtes amené à réfléchir sur un cas d'étude se basant sur la démarche administrative de renouvellement d'un titre d'identité numérique (TIN).

Bien que s'appuyant sur une démarche concrète, l'ensemble des éléments présentés dans la suite de ce dossier est fictif (les noms des organisations, les vulnérabilités énoncées, l'architecture des différents systèmes d'information, etc.).

Les éléments décrits dans le présent dossier ont vocation à accompagner le participant à :

- **visualiser la démarche de renouvellement d'un titre d'identité numérique,**
- **visualiser l'écosystème dans lequel cette démarche s'inscrit,**
- **présenter l'architecture des différents systèmes d'information,**
- **identifier les vulnérabilités disséminées alimentant l'étude de cas.**

Contexte

Généralités

Dans le cadre de l'homologation du système d'information utilisé pour la démarche administrative de renouvellement de titre d'identité numérique, **la Société de Gestion des Titres d'Identité Numérique (SGTIN) vous sollicite pour constituer le dossier d'homologation. À ce titre, vous êtes chargé de la réalisation d'une étude des risques cyber** dont le périmètre couvre la mission de renouvellement de titres d'identité numérique.

Le système d'information étudié étant déjà en production, l'autorité d'homologation, afin de prononcer l'homologation, **a commandité un audit de la sécurité du système d'information** qui doit permettre de vérifier les pratiques de sécurité d'un point de vue organisationnel, physique et technique.

Les éléments fournis dans la suite du présent dossier de l'étude de cas sont issus :

- **des entretiens avec les « métiers »** pour la compréhension de la démarche de renouvellement d'un titre d'identité numérique,
- **des entretiens avec les « opérationnels »** pour la compréhension du système d'information, et les interconnexions associées, mis en œuvre dans le cadre du renouvellement d'un titre d'identité numérique,
- **des résultats de l'audit SSI** du système étudié qui présentent, entre autres, les points faibles relevés.

Réglementation

Compte-tenu de la nature des acteurs et des services étudiés, le Référentiel Général de Sécurité est pleinement applicable aux acteurs et aux systèmes d'information suivants :

- acteurs : la mairie et la SGTIN,
- systèmes d'information : les systèmes d'information sous la responsabilité des acteurs listés ci-après.

Présentation de la démarche administrative : renouvellement de titre d'identité numérique

L'étude de cas se penche, comme rappelé en introduction, sur la démarche administrative de renouvellement de titre d'identité numérique. La Figure 1 illustre le déroulé de ladite démarche.

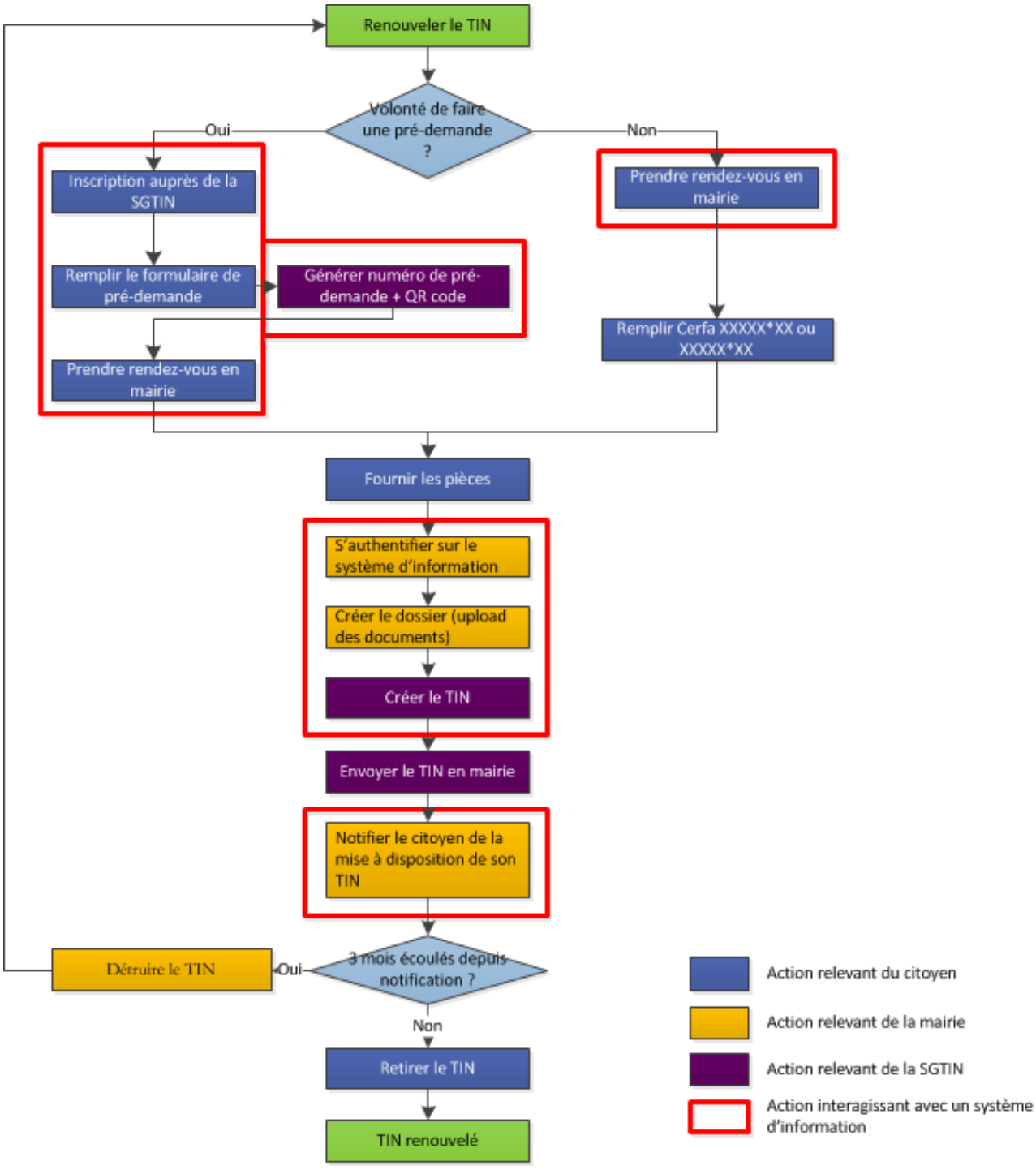


Figure 1 : Diagramme de flux de la démarche de renouvellement de titres d'identité numérique

N.B. : sont exclus de la présente étude des risques :

- **le processus de déclaration de perte ou de vol du titre d'identité numérique,**
- **le processus de destruction du titre d'identité numérique.**

Présentation de l'écosystème entourant la démarche de renouvellement de titres d'identité numérique

Les acteurs

Dans le cadre de cette démarche, nous avons retenu un certain nombre d'acteurs qui participent directement à la démarche de renouvellement de titres d'identité numérique. Ainsi nous identifions :

- l'**Autorité Nationale de Gestion des Titres d'identité numérique (ANGT)** : autorité en charge des questions relatives aux TIN, à savoir :
  - définition des caractéristiques relatives aux titres d'identité numérique,
  - agrément (définition du processus et acte de délivrance de l'agrément) des sociétés à produire des titres d'identité numérique,
  - contrôle des sociétés produisant des titres d'identité numérique,
- **le citoyen** : il est l'acteur à l'origine du processus,
- **la mairie** : elle est l'acteur en charge de :
  - la prise en compte de la demande de renouvellement,
  - la saisie de la demande dans le système d'information de renouvellement de TIN et le contrôle des pièces justificatives,
  - la remise du titre d'identité numérique (il n'est pas utile de prendre rendez-vous pour récupérer son TIN en mairie),
- la **Société de Gestion des Titres d'Identité Numérique (SGTIN)** : la SGTIN est la société qui s'occupe de l'édition des titres d'identité numérique. L'agent de cette société a pour rôle de traiter les informations contenues dans la demande saisie par la mairie, pour l'édition et l'envoi du TIN à cette dernière. Cette société fait l'objet d'inspections annuelles de la part de l'ANGT afin de s'assurer du respect des exigences contractuelles de qualité et de sécurité ;
- la **société d'administration du SI de renouvellement de TIN** : la société a pour rôle d'infogérer le système d'information (Maintien en Condition Opérationnelle (MCO), Maintien en Condition de Sécurité (MCS), évolutions fonctionnelles…) mis en œuvre dans le cadre du renouvellement des TIN ainsi que de prendre en main à distance le poste de travail de l'agent en mairie si besoin ; l'équipe en charge de l'administration du SI de renouvellement des titres d'identité numérique sera appelée « service d'administration » dans la suite de ce dossier d'étude. Cette société, sélectionnée via un marché interministériel (pour lequel des exigences de niveau de service et de sécurité sont définies), dispose d'une certification valide selon la norme ISO 9001:2015 sur le domaine d'application couvrant notamment les activités de MCO / MCS d'infrastructures et d'application ;
- **Héberweb**, la société d'hébergement du SI de renouvellement des TIN, sélectionnée via un marché interministériel (pour lequel des exigences de niveau de service et de sécurité sont définies). Cette société dispose d'une certification valide selon la norme ISO/CEI 27001:2013 sur le domaine d'application couvrant les activités d'hébergement et de services associées à l'hébergement. Elle assure notamment :
  - l'hébergement physique du SI,

  - la fourniture des gestes de proximité (redémarrage d'un serveur, installation physique d'équipement, câblage, etc.),
  - la fourniture d'un accès internet,
  - le contrôle d'accès physique,
  - la fourniture des dispositifs de protection contre les menaces environnementales (protection incendie, dispositifs de refroidissement, dispositifs de protection électrique),
- **la société d'acheminement des titres d'identité numérique** qui livre les TIN, imprimés par la SGTIN, à la mairie concernée. Le contrat entre la société d'acheminement des titres d'identité numérique et la SGTIN ne mentionne pas de clauses de sécurité particulières.

Les systèmes d'information en présence

A l'exception de la société d'acheminement des TIN, nous considérons l'ensemble des systèmes d'information de l'ensemble des acteurs listés ci-dessus. Nous détaillons ici le rôle de chacun des systèmes d'information (SI) :

- le **SI du citoyen** : architecture basique qui se compose :
  - du poste de travail de l'utilisateur ;
  - du routeur/pare-feu fourni et préconfiguré par le FAI (fournisseur d'accès à Internet) permettant à l'utilisateur d'accéder à Internet ;
- le **SI de la mairie**, qui est constitué :
  - du poste de travail de l'agent en mairie ;
  - d'un routeur qui permet aux agents de mairie d'accéder à Internet et qui assure également la fonction de pare-feu ;
- le **SI de renouvellement de TIN** : hébergé chez Héberweb, un hébergeur spécialisé, c'est le système central qui permet de gérer le processus de renouvellement de titres d'identité numérique. Il se présente sous la forme d'une architecture trois tiers classique avec le frontal qui permet à l'utilisateur d'interagir avec le SI (couche de présentation), un serveur de traitement des requêtes faites par l'utilisateur (couche application) et la base de données contenant les dossiers de renouvellement (couche base de données). Les fonctions assurées par le SI sont les suivantes :
  - l'enregistrement des prises de rendez-vous en mairie,
  - la saisie d'une nouvelle demande et le téléversement (upload) des pièces fournies,
  - la notification à la SGTIN de l'existence d'une nouvelle demande de renouvellement à prendre en compte,
  - le partage d'informations entre le SI de la mairie et le SI de la SGTIN au moyen d'un serveur de fichiers sur lequel sont déposées les nouvelles demandes de titres d'identité numérique via une extraction quotidienne depuis la base de données ;
- le **SI de la SGTIN** qui se décompose en deux sous-systèmes :
  - le **SI de pré-demande**, permettant aux citoyens de faciliter la démarche en mairie en effectuant une pré-demande en ligne et dont l'architecture est

similaire à celle du SI de renouvellement de titres d'identité numérique détaillée précédemment,

- le **SI d'impression des TIN** dans lequel nous retrouvons un serveur de fichiers qui permet le rapatriement des dossiers de renouvellement de titres d'identité numérique sur le SI de la SGTIN et le serveur d'impression pour l'impression des TIN.

Il est à noter que l'interconnexion entre le SI de la mairie et le SI de renouvellement de TIN repose sur un réseau homologué. Les besoins de sécurité de ce réseau sont en adéquation avec les besoins du SI de renouvellement de TIN.

Le schéma ci-après donne une représentation simplifiée des différents SI et de leurs interactions.

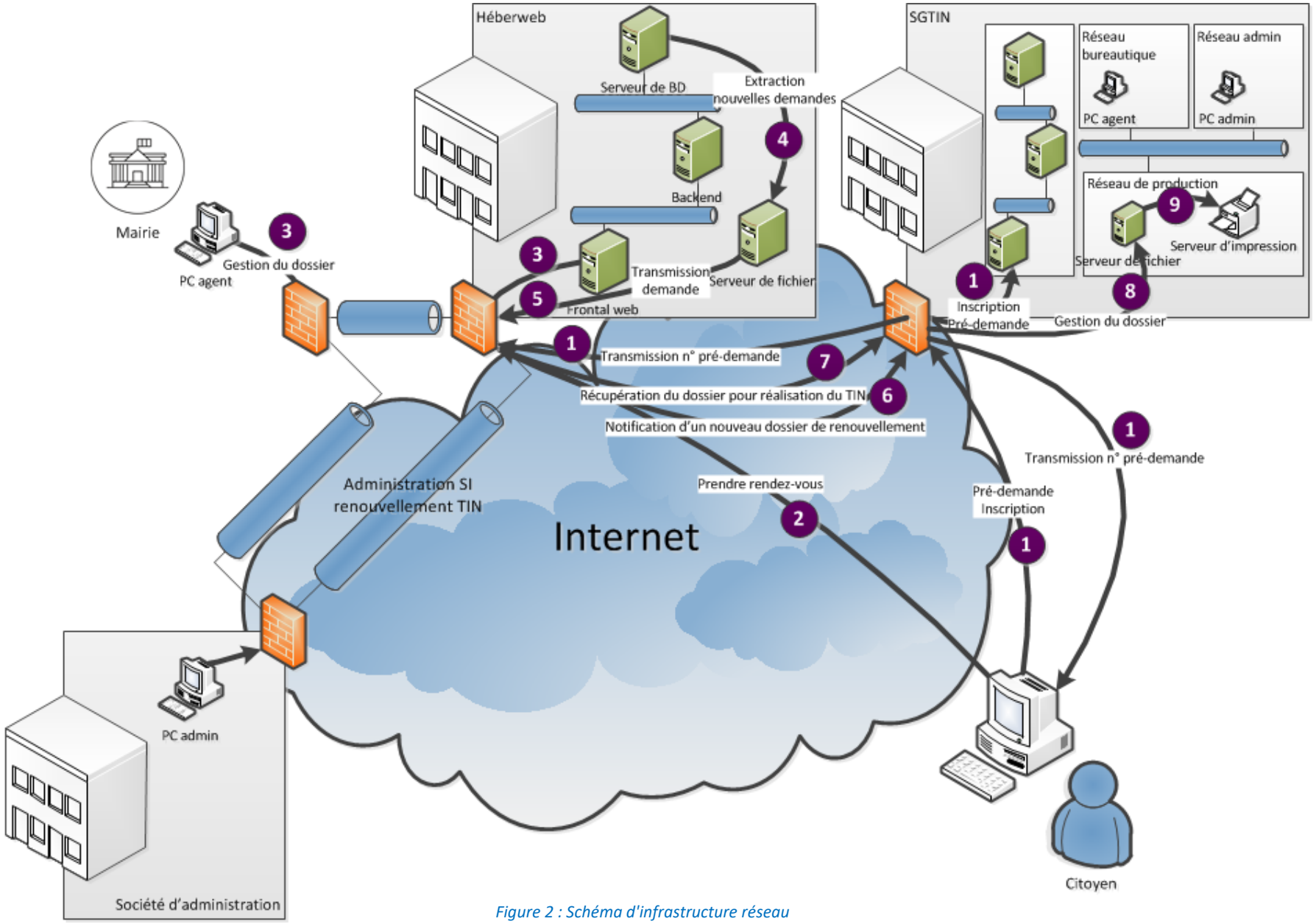


Figure 2 : Schéma d'infrastructure réseau

SGTIN – Définir le périmètre métier et technique

Mission	**Renouveler des titres d'identité numérique**								
Nom de la valeur métier	**Gestion des pré-demandes**		**Gestion des demandes de renouvellement de TIN**		**Impression des TIN**		**Distribution des TIN**	**Informations des citoyens et TIN**	
Nature de la valeur métier	Processus		Processus		Processus		Processus	Information	
Propriétaire	SGTIN (Responsable de la valeur métier même si elle peut déléguer l'exécution des processus à un prestataire)								
Nom du/des biens supports associés	SI de pré-demande	Locaux	SI de renouvellement de TIN	Locaux	SI d'impression des TIN	Locaux	Coursier	SI de la mairie	SI d'impression des TIN
Entité ou personne en charge de la mise en œuvre	SGTIN	SGTIN et Mairie	SGTIN	Mairie et Hébergeur	SGTIN	SGTIN	Société d'acheminement des TIN	Mairie	SGTIN

SGTIN – Identifier les événements redoutés

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	CATÉGORIES D'IMPACT	GRAVITÉ	COMMENTAIRES / JUSTIFICATION
Impression des TIN	Certains TIN imprimés ne correspondent pas à des demandes légitimes	• Impact financier lié au coût de réimpression du TIN • Impact juridique lié à l'implication de la SGTIN dans les procès pour création de fausses identités	4	• Usurpation d'identité • Fraude (création de faux TIN)
Distribution des TIN / TIN	Vol de TIN légitimes durant leur acheminement à la mairie	• Impact juridique (RGPD) • Impact financier lié au coût de renouvellement de TIN	4	• Usurpation d'identité
Informations des citoyens	Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	• Impact juridique (RGPD) • Impact d'image	4	• Usurpation d'identité
Gestion des demandes de renouvellement de TIN	Le service permettant à un agent de mairie de faire une demande de renouvellement de TIN est indisponible	• Impact d'image • Impact financier lié au coût d'investigation et de retour à la normale	3	Pas d'existence de solution de contournement, impossibilité de réaliser la mission pendant la durée d'indisponibilité
Gestion des demandes de renouvellement de TIN	Le service de notification de renouvellement de TIN n'est pas accessible aux utilisateurs	• Impact d'image lié au délai d'obtention du TIN • Impact financier lié au coût d'investigation et de retour à la normale	2	Existence d'une solution de contournement avec une dégradation des performances (la mairie peut contacter par téléphone ou mail le citoyen pour le notifier)
Gestion des pré-demandes	Le service permettant de réaliser une pré-demande par internet auprès de la SGTIN est indisponible	• Impact d'image • Impact financier lié au coût d'investigation et de retour à la normale	1	Existence d'une solution de contournement (possibilité de renseigner les informations directement à la mairie)

SGTIN – Évaluer les couples SR/OV

SOURCES DE RISQUE	OBJECTIF VISÉ	MOTIVATION	RESSOURCES	PERTINENCE
Organisation de malfaiteurs	Gagner de l'argent en collectant des informations ou en revendant des TIN	Fortement motivé	Ressources importantes	**Très pertinent**
Hacktiviste	Perturber la fabrication de TIN	Fortement motivé	Ressources importantes	**Très pertinent**
État	Faire fabriquer des faux TIN pour faire circuler des espions sur le territoire	Fortement motivé	Ressources illimitées	**Très pertinent**
Agent malveillant SGTIN	Discréditer ou saboter le service de renouvellement de TIN	Assez motivé	Ressources significatives	**Plutôt pertinent**
Terroriste	Créer un faux TIN pour entrer sur le territoire	Assez motivé	Ressources limitées	**Moyennement pertinent**
Citoyen malhonnête	Créer une fausse identité	Très peu motivé	Ressources limitées	**Peu pertinent**
Hacker amateur	Tester ses compétences sur un système « grandeur nature »	Peu motivé	Ressources limitées	**Peu pertinent**

SGTIN – Établir le lien entre les événements redoutés et les couples SR/OV

SR/OV les plus pertinents

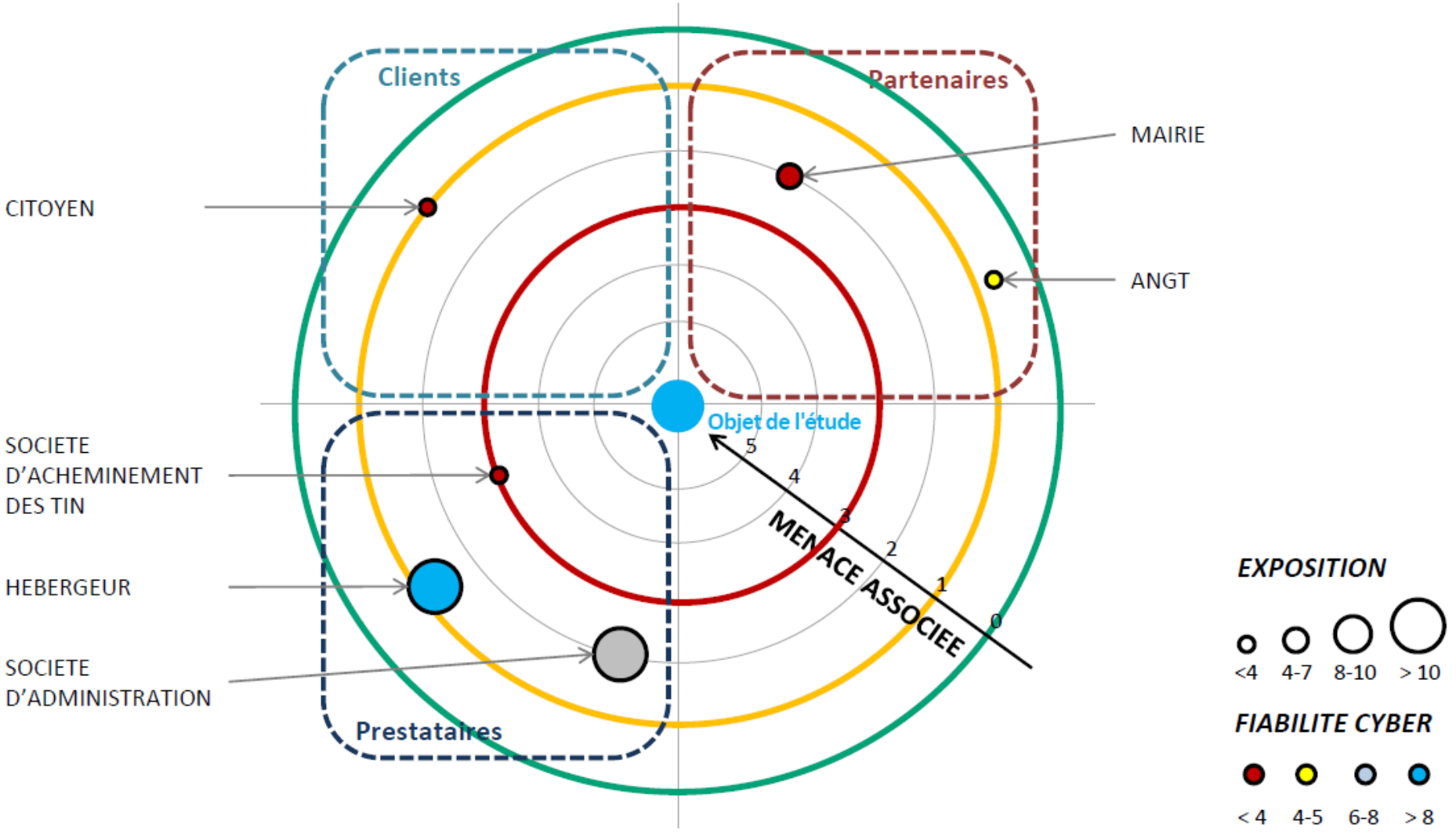
SOURCES DE RISQUE	OBJECTIF VISÉ
Organisation de malfaiteurs	Gagner de l'argent en collectant des informations ou en revendant des TIN
Hacktiviste	Perturber la fabrication des TIN
État	**Faire fabriquer des faux TIN** pour faire circuler des espions sur le territoire

ER les plus graves

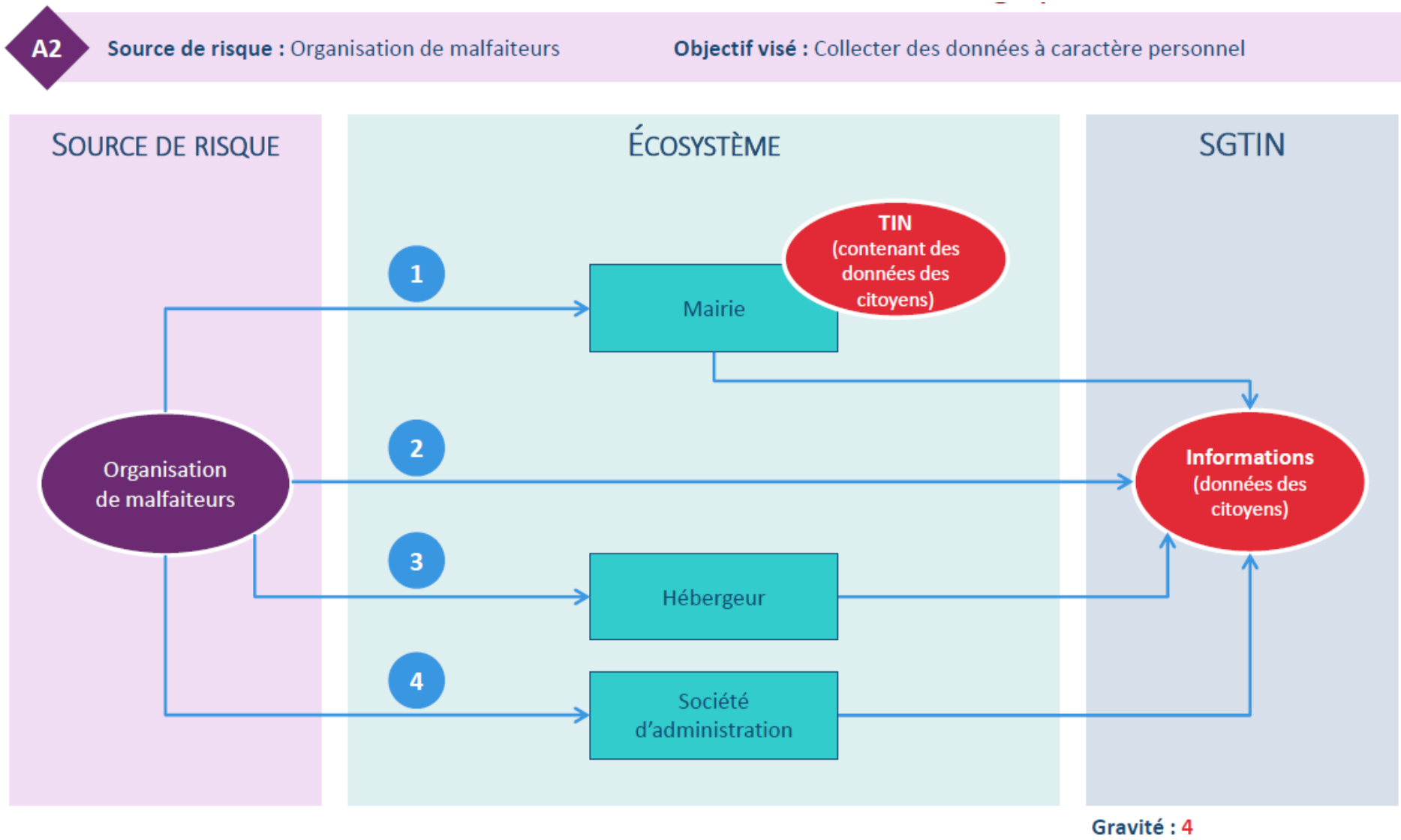
ÉVÉNEMENT REDOUTÉ	VALEUR MÉTIER
Certains TIN imprimés ne correspondent pas à des demandes légitimes	**Impression des TIN**
Vol de TIN légitimes durant leur acheminement à la mairie	**Distribution des TIN**
Divulgation ou vol des informations concernant le citoyen (nom, prénom, justificatif de domicile, etc.)	**Informations des citoyens**

SGTIN – Construire la cartographie de menace de l'écosystème

Catégorie	Nom	Dépendance	Pénétration	Maturité cyber	Confiance	Niveau de menace
Utilisateur	Citoyen	1	1	1	1	**1**
Partenaire	Mairie	2	3	1	3	**2**
Partenaire	Autorité Nationale de Gestion des Titres (ANGT)	1	3	1	4	**0,75**
Prestataire	Société d'administration	3	4	2	3	**2**
Prestataire	Hébergeur (Héberweb)	3	4	3	3	**1,3**
Prestataire	Société d'acheminement des TIN	1	3	1	1	**3**


Clients
Partenaires
Prestataires
CITOYEN
MAIRIE
ANGT
SOCIETE D'ACHEMINEMENT DES TIN
HEBERGEUR
SOCIETE D'ADMINISTRATION
Objet de l'étude
MENACE ASSOCIEE
0
1
2
3
4
5
EXPOSITION
<4
4-7
8-10
> 10
FIABILITE CYBER
< 4
4-5
6-8
> 8

SGTIN – Élaborer des scénarios stratégiques



Les conclusions de l'audit

Les conclusions de l'audit ont remonté un certain nombre de points dont voici une synthèse.

Sécurité de Héberweb

L'audit de la sécurité physique de l'hébergeur du SI de renouvellement de titres d'identité numérique a permis de vérifier qu'un contrôle d'accès strict était mis en œuvre pour permettre aux seules personnes en ayant le besoin, d'accéder aux zones d'hébergement. Les personnes amenées à intervenir ponctuellement dans les locaux de Héberweb (prestataires, fournisseurs, visiteurs, etc.) sont systématiquement accueillies et enregistrées dans un cahier d'émargement. Elles sont accompagnées en permanence, pendant toute la durée de leur intervention dans les zones d'hébergement.

La sécurité physique chez Héberweb a permis de vérifier que des bonnes pratiques quant au dimensionnement et au maintien en condition de sécurité des équipements de sûreté environnementale (refroidissement, protection incendie, protection électrique) étaient en place.

De plus l'audit a permis de démontrer un bon maintien en condition de sécurité des équipements sous la responsabilité de l'hébergeur (parc homogène avec des systèmes d'exploitation et des applicatifs maintenus par leurs éditeurs et pour lesquels les correctifs de sécurité très récents avaient été appliqués).

En revanche, l'audit a mis en évidence une absence de gestion de l'acquisition, de la maintenance et de la fin de vie des équipements informatiques. En effet les auditeurs ont constaté que les équipements en attente de mise en production ou désengagés étaient entreposés dans un local dont l'accès était ouvert à l'ensemble du personnel de Héberweb. Pour le cas particulier de la fin de vie, l'hébergeur a confié attendre d'avoir accumulé un volume conséquent de matériels avant de les jeter dans un point de collecte.

De même, pour ces équipements informatiques, les entrevues ont permis d'identifier que l'hébergeur ne disposait pas de procédure de renvoi au fournisseur et que les informations sensibles (règles de filtrage, fichiers de configuration, mots de passe, etc.) pouvaient être amenées à sortir de l'organisation sans contrôle particulier (échange ou réparation de matériel dans le cas d'une garantie par exemple).

Sécurité des moyens d'administration du SI de renouvellement de TIN

Lors de cette phase de l'audit, les auditeurs ont pu observer les pratiques suivantes :

- la connexion de l'administrateur sur les équipements du SI de renouvellement de mot de passe s'effectue via le protocole SSH[1] sur le pare-feu qui sert de machine rebond pour administrer les équipements du SI. La configuration du service d'authentification SSH est une authentification simple par mot de passe,
- le poste de travail de l'administrateur est utilisé aussi bien pour des tâches bureautiques (messagerie, navigation sur Internet, etc.) que pour des tâches d'administration du SI de renouvellement de titres d'identité numérique,

[1] **Secure SHell** : protocole d'authentification et de communication, successeur de Telnet, apportant des fonctions de sécurité liées à la confidentialité (chiffrement) et l'intégrité (somme de contrôle) des échanges.

- le frontal web, bien que privilégiant le protocole HTTPS[2], autorise, lors de l'établissement de la session, l'utilisation de SSL[3]v3. De plus, un aperçu des ports a permis d'identifier que les ports TCP 137, 139 et 445 (SMBv1[4]) n'étaient pas filtrés alors que les services SMB sont actifs sur ce frontal.
- Globalement, les audits de configuration effectués sur le SI de renouvellement de TIN (dont le service d'administration à la charge) ont montré une forte hétérogénéité et l'existence de serveurs Windows 2008 R2, notamment pour le serveur de fichier. Ce constat est renforcé par l'observation d'outils de télé-administration (TeamViewer) sur ces serveurs pour lesquels l'administrateur n'a su fournir d'explication ; les entretiens ont mis en évidence que l'authentification par l'agent de mairie sur le SI de renouvellement de titres d'identité numérique s'effectue par mot de passe, sans application d'une politique contraignante de format de mot de passe. De plus, les comptes utilisateurs ne sont pas automatiquement verrouillés après saisie d'un certain nombre de tentatives de connexion infructueuses consécutives. Ces constats ont été confirmés par l'audit de configuration.

Sécurité de la mairie

L'audit a mis en évidence des lacunes au niveau de la sécurité physique, compte tenu du fait que la zone d'accueil des visiteurs est mitoyenne à la zone de travail, sans présence de contrôle d'accès.

De plus, les entretiens ont montré que le poste de travail de l'agent en mairie était utilisé aussi bien pour les aspects bureautiques (messagerie, navigation sur Internet, etc.) que pour les actions relevant de la mairie dans le cadre de la démarche de renouvellement de TIN. Pour des raisons opérationnelles, le poste de travail de l'agent est portable. Il utilise un système d'exploitation maintenu par l'éditeur et, afin d'alléger le service d'administration, les droits d'administration ont été octroyés à l'utilisateur pour lui permettre d'installer les outils dont il a besoin dans la limite définie dans la charte informatique. L'audit a permis, également, d'identifier qu'aucun mécanisme de chiffrement de disque n'était mis en œuvre.

Sécurité du SI de la SGTIN

L'audit de la SGTIN a permis d'identifier qu'aucune vérification particulière n'était effectuée sur les dossiers de demande de renouvellement de titres d'identité numérique qu'elle récupérait depuis le serveur de fichier du SI de renouvellement de TIN. Ce constat a été appuyé, lors de l'entretien, par la survenance par le passé d'incidents de qualité impliquant des informations erronées sur les titres d'identité numérique imprimés pour lesquels aucune investigation n'avait été menée mais qui avaient contraint la SGTIN à réimprimer les TIN incriminés.

De plus, les entretiens avec les personnes de la SGTIN ont permis d'identifier que la récupération des dossiers de demande de renouvellement depuis le serveur de fichier du SI de

---

[2] **HyperText Transfer Protocol Secure** : protocole de communication sur Internet apportant les fonctions de sécurité (confidentialité, intégrité, authenticité) qui manquaient au protocole HTTP

[3] **Secure Socket Layer** : protocole de sécurisation des échanges dont les fonctions de sécurité sont la confidentialité, l'intégrité et l'authenticité. Au moment de l'écriture de l'étude de cas, le protocole SSL est reconnu vulnérable à différentes attaques et les experts du domaine conseillent l'adoption du protocole TLSv1.2 (TLSv1.3 ayant fait l'objet d'une approbation en mars 2018 par l'IETF, son implémentation n'est pas encore répandue)

[4] **Server Message Block** : protocole de partage de ressources (fichiers et imprimantes)

renouvellement de titres d'identité numérique s'effectue via le protocole d'échange de fichier FTP[5].

L'authentification au sein de la SGTIN est centralisée au moyen du SSO[6] qui s'appuie sur un annuaire d'entreprise géré par un Active Directory. Les entretiens ont permis de constater que le serveur de fichiers est utilisé pour d'autres activités de la SGTIN (RH, Achat, etc.) et que le cloisonnement entre les différentes activités est assuré par des répertoires distincts pour chaque activité. Cependant, un contrôle plus poussé a permis aux auditeurs de constater que l'accès au répertoire propre à l'activité de renouvellement des TIN était ouvert à l'ensemble des collaborateurs de la SGTIN.

[5] **File Transfer Protocol** : protocole de transfert de fichier qui ne fournit pas de fonction de sécurité particulière
[6] **Single Sign On** : dispositif de centralisation de l'authentification permettant aux utilisateurs grâce à un moyen unique d'authentification, d'accéder à un ensemble de ressources (serveurs, applications, fichiers, etc.)

SGTIN – Élaborer des scénarios opérationnels

A3 **Scénario stratégique :** Organisation de malfaiteurs qui veut voler des données personnelles

Chemin d'attaque : n°2 – « attaque directe »

Gravité : 4