Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Paris, le 13 janvier 2017

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Secrétariat général
pour la modernisation
de l'action publique

Direction interministérielle du numérique et du système d'information et de communication de l'Etat

AUDIT DU SYSTÈME « TITRES ELECTRONIQUES SÉCURISÉS »

MINISTÈRE DE L'INTÉRIEUR

Guillaume POUPARD
Directeur général de l'Agence nationale de la sécurité des systèmes d'information

Henri VERDIER
Directeur interministériel du numérique et du système d'information et de communication de l'Etat

1. Propos liminaires

Le ministère de l'Intérieur a engagé un plan de transformation de l'organisation des préfectures. Ce plan « Préfectures nouvelle génération » (PPNG) prévoit notamment la création de centres d'expertise et de ressources titres (CERT) concentrant la gestion des titres sur ces plateformes : cartes nationales d'identité (CNI), passeports, permis de conduire, et immatriculation des véhicules. Pour ce qui concerne la carte d'identité ou le passeport, les usagers se présenteront dans les mairies équipées de dispositifs numériques de recueil des demandes et des données biométriques. Celles-ci seront instruites par les CERT, ce qui devrait permettre d'améliorer les délais de traitement tout en renforçant les moyens de lutte contre la fraude.

Dans ce contexte, le ministère de l'Intérieur prévoit d'étendre en 2017 à la gestion des cartes nationales d'identité l'utilisation du système d'information « Titres électroniques sécurisés » (TES)[1], opéré par l'agence nationale des titres sécurisés (ANTS) et utilisé depuis 2008 pour gérer les demandes de passeports et leur production. TES remplacera ainsi le fichier national de gestion (FNG) qui est en voie d'obsolescence.

Dans le cadre de cette évolution, le ministre de l'Intérieur a saisi le 17 novembre 2016 la Direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) afin d'obtenir un avis sur la sécurité du système face aux risques de fraude, d'intrusion, de compromission ou de destruction, et sur les mécanismes de sécurité prévus pour garantir l'impossibilité de détourner le système de ses finalités.

Le ministre souhaite en particulier garantir la robustesse du lien unidirectionnel mis en place au sein du système TES permettant d'associer à des données d'identification alphanumériques des données biométriques, tout en empêchant que des données d'identification puissent réciproquement être associées à des données biométriques.

En réponse à cette saisine, la DINSIC et l'ANSSI ont réalisé une mission d'expertise conjointe du 28 novembre 2016 au 15 janvier 2017.

Il convient ainsi de préciser en préambule que cette mission a porté uniquement sur le système TES existant. En effet, l'objectif fixé n'a pas été de concevoir un nouveau système de gestion des cartes nationales d'identité, fondé sur d'autres types d'architectures techniques et logicielles, potentiellement plus distribuées et couplées à des moyens techniques différents, notamment en matière de capture de données biométriques.

Cette mission, dont les principales conclusions sont détaillées dans le présent rapport, a consisté en une analyse des fonctionnalités du système TES, de son architecture, de sa gouvernance et de son organisation, ainsi qu'en un test d'intrusion visant à apprécier le niveau de sécurité réel du système.

Les recommandations et propositions qui sont faites dans ce rapport visent à réduire les risques identifiés sur le système TES actuel tout en posant, en conclusion, les bases d'une réflexion élargie, portant notamment sur les possibilités offertes par de nouvelles architectures pour ce système.

[1] Cette extension est encadrée par le décret n°2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

2. Synthèse de l'audit

L'audit a montré que, du point de vue de la sécurité informatique, les principes de conception du système TES sont compatibles avec la sensibilité des données qu'il contient. Cependant, TES est un système complexe, incluant de multiples parties prenantes et de nombreux composants matériels et logiciels, d'où la nécessité d'une vigilance particulière pour assurer un niveau de sécurité homogène sur l'ensemble de son périmètre.

A ce titre, et au regard de l'évolution des technologies et de la menace cyber, l'audit a mis en évidence que la sécurité globale du système TES est perfectible. L'ANSSI a ainsi formulé des recommandations en termes de gouvernance, d'exploitation et de durcissement des mesures de sécurité, dont la mise en œuvre par le ministère de l'Intérieur et l'ANTS doit garantir un niveau de sécurité homogène et durable sur l'ensemble du système TES. Ces recommandations ont été transmises au fur et à mesure de leur élaboration aux équipes techniques en charge du système, afin de pouvoir être mises en œuvre dans les plus brefs délais.

Du point de vue des usages, l'audit a constaté que le système TES peut techniquement être détourné à des fins d'identification, malgré le caractère unidirectionnel du lien informatique mis en œuvre pour relier les données d'identification alphanumériques aux données biométriques. Cet usage illicite peut être atteint ne serait-ce que par reconstitution d'une base de données complète à partir du lien unidirectionnel existant.

Il sera néanmoins d'autant plus difficile de dévoyer ce système que des mesures de sécurité techniques, fonctionnelles et organisationnelles auront été mises en place, afin notamment d'encadrer ses usages et de limiter aux informations strictement nécessaires les données véhiculées.

La DINSIC et l'ANSSI rappellent toutefois qu'il est impossible de garantir l'inviolabilité technique absolue d'un système d'information dans le temps. La question de la sécurité du système TES renvoie *in fine* à l'arbitrage que doit faire l'Etat en matière d'acceptation des risques résiduels inévitables liés à la mise en œuvre de ce système, au regard des bénéfices escomptés pour la gestion des titres, comme c'est le cas pour tout système d'information, quelle que soit sa sensibilité.

3. Constats et recommandations

3.1 Déroulement de l'audit

Les équipes de l'ANSSI et de la DINSIC ont conduit l'audit du système TES selon les axes suivants :

- analyse fonctionnelle,
- audit organisationnel,
- audit d'architecture,
- test d'intrusion.

L'analyse fonctionnelle a eu pour objectif d'une part d'évaluer l'adéquation des usages du système TES, tels qu'ils sont pratiqués, avec ceux prévus par le décret n°2016-1460 du 28 octobre 2016, et d'autre part d'identifier les possibilités de détournement de ces usages.

L'audit organisationnel s'est attaché à évaluer le niveau de prise en compte des enjeux et besoins de sécurité pour le système TES, et leur déclinaison effective au niveau des différents intervenants, incluant notamment les sous-traitants.

L'audit d'architecture a permis d'évaluer le niveau de robustesse des fonctions de sécurité clés du système TES (cloisonnement, lien unidirectionnel, traçabilité des actions, etc.) vis-à-vis du niveau de menace et de risque estimé, et vis-à-vis des cas potentiels de détournement d'usage.

L'analyse fonctionnelle des usages, l'audit organisationnel et l'audit d'architecture ont été réalisés au travers de plusieurs entretiens avec des acteurs clés de l'exploitation et de la gouvernance du système, et via une analyse documentaire approfondie (dossier d'architecture, politique de sécurité, procédures d'exploitation, analyse de risques, précédents audits de sécurité, etc.).

Un test d'intrusion a complété cette approche afin d'apprécier le niveau de sécurité réel du système dans son état actuel.

3.2 Analyse fonctionnelle

Pour rappel, le système TES entre en jeu pour trois usages des données collectées :

- pour la gestion des titres, CNI et passeports, depuis les mairies, les centres d'expertise et de ressources titres (CERT) et les préfectures ;
- pour les forces de l'ordre concernées, qui accèdent à une application présentant les données collectées à l'exclusion des empreintes digitales ;
- pour les officiers de police judiciaire ayant indirectement accès, dans le cadre de réquisitions, à l'ensemble des données dont les empreintes digitales.

a Usage du système pour la gestion des titres

Concernant la gestion du passeport biométrique, le système TES permet :

- l'enregistrement d'une demande de passeport, en mairie ou en consulat[2] ;
- l'instruction et la validation du dossier ;
- la demande de fabrication et de personnalisation du titre par le centre de production ;
- la remise du titre sur le site où s'est fait l'enregistrement de la demande.

Le système apporte plusieurs fonctionnalités de simplification et de fiabilisation du processus de traitement des titres :

- grâce à l'écosystème dans lequel il s'intègre, il permet de lutter plus efficacement contre les usurpations d'identité. Il permet notamment la vérification automatisée des données d'état-civil auprès des mairies de naissance qui ont adhéré au dispositif COMEDEC, la

[2] Dans le cas d'une personne résidant à l'étranger.

consultation préalable du fichier des personnes recherchées, ou encore la vérification automatique de la validité des justificatifs de domicile sécurisés par un contrôle d'un code sécurisé à barre à deux dimensions (solution 2D-DOC) ;

- il apporte plusieurs simplifications au profit de l'usager. Par exemple, il permet la pré-demande de titre en ligne, le recours au timbre fiscal dématérialisé et le renouvellement simplifié du passeport par l'authentification du demandeur, lui évitant de produire à nouveau un acte d'état-civil ou une preuve de sa nationalité. Lorsqu'un particulier demande un renouvellement de son passeport biométrique, il dépose ses empreintes digitales et celles-ci sont comparées à celles contenues dans la puce de son passeport ou, à défaut dans la base centrale lorsque le passeport a été perdu, volé, endommagé ou détruit. Le service instructeur ne connait que le résultat de la comparaison qui, si elle est conclusive, permet d'aller beaucoup plus vite dans l'instruction ;
- il renforce les conditions d'accès et de traçabilité de l'instruction des données personnelles du demandeur. Les agents du ministère de l'Intérieur chargés de l'instruction et de la validation de la demande de titre accèdent au logiciel de traitement au moyen d'une carte à puce nominative. Le système permet par ailleurs un archivage électronique des documents.

Sous réserve d'offrir un niveau de sécurité suffisant, le système TES devrait permettre d'étendre ces garanties de contrôle et de simplification aux demandes de CNI.

A l'heure actuelle, les demandes sont effectuées en mairie sur la base de formulaires de demande et du recueil de la photographie et des empreintes digitales sur un support papier. Les images ainsi collectées sont transmises et conservées en préfecture. Les autres informations alimentent le fichier national de gestion (FNG).

Le système TES contribuera ainsi à simplifier, dématérialiser et mutualiser les dispositifs de recueil et d'instruction de ces deux titres, avec pour conséquences la suppression de la charge de travail directement liée à la manutention locale des formulaires contenant les données, ainsi que la rationalisation des applications du ministère.

En revanche, la centralisation des données biométriques pour la carte nationale d'identité n'a pas actuellement un intérêt direct pour leur gestion. Leur utilisation se borne en effet au cas des réquisitions judiciaires.

D'un point de vue de la gestion des titres, il est ainsi important de noter que l'existence dans TES d'un système de base de données conservant au niveau central les empreintes digitales collectées lors des demandes de titres ne se justifie que pour faciliter des contrôles lors des renouvellements des titres. De plus, cela concerne uniquement les passeports puisqu'aucune fonctionnalité de ce type n'est à ce jour implémentée concernant la carte nationale d'identité.

Recommandation n°1

L'usage des données biométriques issues des demandes de cartes nationales d'identité se limitant actuellement à la réponse à de potentielles réquisitions judiciaires, mettre en place à court terme un mécanisme de chiffrement de ces données biométriques, confiant à une autorité tierce la capacité de les déchiffrer. Ni le ministère ni l'autorité tierce n'aurait seul les moyens de déchiffrer complètement ces données, dès lors que plusieurs clés de chiffrement seraient utilisées.

b *Usage du système pour les forces de l'ordre*

Les forces de l'ordre accèdent à une application permettant de consulter les données à l'exception des empreintes. Ils ont notamment accès aux données d'identité, y compris aux photographies (qui sont des données biométriques).

c *Usage du système dans le cadre des réquisitions judiciaires*

En 2016, le système TES, limité à la gestion des passeports, a fait l'objet d'environ un millier de réquisitions judiciaires. En effet, la réquisition judiciaire prévue par le code de procédure pénale permet aux officiers de police judiciaire, procureurs et juges d'instruction d'obtenir communication des informations détenues par TES ou par les préfectures.

Dans ce cadre, les officiers de police judiciaire peuvent obtenir auprès de l'ANTS toutes les informations collectées lors des demandes de titres correspondant à une identité donnée. Cela comprend notamment les photographies et les empreintes digitales. Cet usage n'est pas spécifique au système TES puisqu'il existe à l'heure actuelle le même processus concernant les empreintes digitales collectées sur formulaire papier.

Alors que le déploiement de TES pour les cartes nationales d'identité va mécaniquement induire une augmentation des réquisitions de données du système, il n'y a actuellement pas d'application dédiée permettant de traiter et tracer ces requêtes.

Recommandation n°2

Analyser de manière approfondie, en fonction des différents usages, les risques de dévoiement de l'utilisation des données traitées par TES ou d'exfiltration de tout ou partie de ces données.

3.3 Audit organisationnel

Les entretiens et analyses documentaires effectués montrent que les besoins et enjeux de sécurité du système TES sont pris en compte et déclinés dans un processus d'amélioration continue de la sécurité, notamment à travers une démarche d'homologation[3] visant à garantir que le niveau de sécurité du système est adapté aux risques.

Un dossier d'homologation largement documenté a été constitué dans ce cadre, comportant en particulier une analyse de risque et des mesures de sécurité. Un certain nombre de scénarios de risque y sont examinés, incluant différentes catégories d'actes malveillants et d'attaques informatiques. Des mesures de réduction du risque sont déduites de chaque scénario étudié, en fonction de ses niveaux de gravité et de vraisemblance estimés, et déclinées dans un plan d'amélioration continue.

Recommandation n°3

Affiner l'analyse de risque conduite dans le cadre de l'homologation du système TES, notamment en adaptant davantage les scénarios de risque à la nature des données à protéger (empreintes digitales, pièces justificatives, données administratives).

Il a par ailleurs été noté que l'ANTS s'appuie fortement sur ses sous-traitants pour le développement et l'exploitation du système TES, ce qui est susceptible d'augmenter la surface d'exposition du système à d'éventuelles attaques.

Recommandation n°4

Mettre en place une gestion stricte et formalisée des sous-traitants intervenant sur le système TES, notamment à travers des exigences contractuelles adaptées.

[3] L'homologation d'un système d'information est une décision formelle prise par l'autorité responsable du système (au sein du ministère de l'Intérieur, dans le cas de TES) attestant que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre.

Il est à noter que cette démarche est d'ores et déjà engagée, le projet de renouvellement du marché de prestation relatif au système TES se caractérisant par une élévation du niveau d'exigences de sécurité imposées aux prestataires, déclinant ainsi le plan d'amélioration continue.

Enfin, la gouvernance globale du système TES et de ses évolutions pourrait être améliorée.

Recommandation n°5

Formaliser précisément les modalités de coordination et de partage de responsabilité entre les différents intervenants sous la forme d'un schéma directeur, permettant de s'assurer que l'ensemble des besoins, évolutions et risques sont pris en compte et effectivement déclinés de façon cohérente sur les différents périmètres de responsabilité.

3.4 Audit d'architecture

a Mise en œuvre du lien unidirectionnel

L'architecture du système TES repose sur plusieurs sous-systèmes, correspondant aux différentes étapes de la demande et de l'instruction des titres : le sous-système « enregistrement-remise », correspondant principalement aux dispositifs de recueils déployés en mairie et dans les consulats, le sous-système « information », utilisé pour l'instruction des demandes, le sous-système « production », chargé de la production des titres, le sous-système « sécurité-traçabilité », chargé notamment de la gestion des droits d'accès des différents acteurs, et le sous-système « conservation des dossiers », dédié au stockage.

Ce dernier sous-système répartit les dossiers en deux compartiments : un compartiment alphanumérique de données d'état civil (nom, prénom, date de naissance, etc.) et un compartiment de données biométriques (photographies, empreintes de deux doigts, signatures). Au sein de ce dernier compartiment, les différentes catégories de données biométriques sont gérées de manière indépendante dans l'optique d'assurer leur cloisonnement.

La conception du système TES prévoit que l'accès aux données biométriques se fasse uniquement au moyen de liens unidirectionnels depuis le compartiment de données alphanumériques vers le compartiment de données biométriques (un lien par type de donnée et par dossier).

Recommandation n°6

Prendre en compte les préconisations du Référentiel Général de Sécurité concernant les mécanismes cryptographiques mis en œuvre pour construire les liens unidirectionnels.

L'ajout des CNI dans le système TES nécessitant un allongement de la durée de conservation des données (vingt ans au maximum contre quinze pour les passeports), il conviendra d'accroître le niveau de robustesse des éléments cryptographiques utilisés dans la construction du lien unidirectionnel.

Il est à noter que l'ANTS a déjà prévu de mettre en œuvre cette recommandation en 2017.

Recommandation n°7

Dans le cadre du renforcement de la défense en profondeur du système, mettre en place à court terme un chiffrement des données biométriques et des pièces justificatives.

Il est à noter que l'ANTS a déjà prévu de mettre en œuvre cette recommandation en 2017.

b *Traçabilité dans le cadre des réquisitions judiciaires*

Le système TES, tel qu'il est conçu, inclut des outils répondant aux besoins des réquisitions judiciaires, sans autoriser l'identification d'une personne à partir d'une empreinte digitale. La traçabilité de ces réquisitions judiciaires est actuellement assurée par des moyens organisationnels.

Recommandation n°8

Renforcer la traçabilité des actions menées dans le cadre des réquisitions judiciaires par des mécanismes techniques robustes et automatisés de contrôle d'accès et de journalisation.

3.5 Test d'intrusion

Le test d'intrusion conduit par l'ANSSI a permis de confirmer que l'architecture actuellement mise en place prend en compte les problématiques de cloisonnement et de filtrage. Par exemple, les postes de recueil de demandes de titres ne sont pas pourvus de connexion à Internet ; les dossiers de demande et de retrait des titres sont quant à eux transmis de manière chiffrée entre les postes de recueil et les serveurs hébergeant les données biométriques.

Un certain nombre de vulnérabilités de gravité variable ont néanmoins été relevées.

Recommandation n°9

Appliquer des mécanismes de cloisonnement et de filtrage robustes à l'ensemble des éléments du système TES afin de renforcer sa défense en profondeur.

La configuration et les pratiques d'administration de certains équipements du centre serveurs ne sont pas conformes à l'état de l'art. Des vulnérabilités ont par ailleurs été identifiées au niveau des applications « métier ». Il a néanmoins été constaté que l'environnement utilisateur du poste de recueil est durci, ce qui permet de limiter les éventuelles actions malveillantes de l'agent.

Recommandation n°10

Définir et mettre en œuvre un référentiel de sécurisation applicable à l'ensemble des équipements du système TES, ainsi qu'un référentiel de développement sécurisé des applications.

Ces référentiels devront être respectés par les prestataires.

Recommandation n°11

Améliorer le processus de suivi des mises à jour des correctifs de sécurité sur les systèmes et applications, ainsi que la politique de durcissement des mots de passe.

Note : le détail des vulnérabilités découvertes ainsi que des correctifs à appliquer au système sont fournis dans un rapport séparé, protégé par le secret de la défense nationale pour des raisons évidentes de protection du système.

4. Propositions d'évolution à moyen et long terme

L'ensemble des constats et recommandations de cet audit posent la question de la trajectoire fonctionnelle et technique du système TES à moyen et long terme.

Dans ce cadre, si la volonté de réaliser une base complète des images des empreintes est confirmée, la DINSIC et l'ANSSI suggèrent d'étudier l'intérêt et la faisabilité de dissocier le système mis en jeu pour la production des titres de celui sollicité dans le cadre des réquisitions judiciaires. Cette approche présenterait plusieurs avantages :

- d'une part, cela permettrait de mieux encadrer l'usage que souhaite faire l'Etat des données biométriques recueillies dans le système TES et de limiter le nombre de personnes accédant à ces données ;
- d'autre part, cela permettrait de ne conserver qu'un ensemble minimal d'informations biométriques au sein du système TES, permettant aux services de l'Etat de confirmer l'identité d'un demandeur de titre avec une assurance raisonnable, sans pour autant identifier ce demandeur de manière certaine. L'utilisation d'un « gabarit » pour les empreintes digitales pourrait à cette fin être envisagée pour le système TES.

Dans le même temps, au regard de la sensibilité des données biométriques, qu'elles soient totales ou partielles, une gouvernance interministérielle permettant de systématiquement aligner les solutions d'architecture, de sécurité et des besoins fonctionnels serait à étudier.

Quelles que soient les évolutions qui seront *in fine* retenues, une traçabilité renforcée des accès et des sollicitations du système est souhaitable. Au-delà de la recommandation n°8, des pistes visant à renforcer la transparence sur ces accès et sollicitations devraient être étudiées. A cet effet, la mise en place de registres pourrait être envisagée.

5. La généralisation du recours aux identités numériques et à la biométrie

Avant de conclure ce rapport, il convient de souligner que les questions techniques, organisationnelles ou de sécurité, mais aussi les enjeux juridiques et éthiques soulevés par le système TES et ses usages sont appelées à se reposer, de plus en plus souvent, à la société française, tant dans le secteur public que dans le secteur privé.

La généralisation des moyens de collecte et de traitement des informations, la banalisation de la biométrie, désormais utilisée par les industries de grande consommation, la demande croissante de services de plus en plus personnalisés, la demande de sécurité, l'effort de simplification et de maîtrise des coûts au sein de l'Etat comme dans de nombreuses industries, conduiront à la démultiplication du recours à l'identification, à l'authentification, et à des formes plus ou moins précises de biométrie.

Certes, le devoir envers les citoyens de transparence sur les usages, la nécessité de privilégier des principes d'architecture garantissant le respect de la vie privée dès la conception (*privacy by design*), les contrôles et la traçabilité sont d'autant plus forts que les services émanent de la puissance publique, qu'ils concernent des démarches rendues nécessaires par la loi ou par l'organisation du service public et que les traitements gèrent des données personnelles. Mais il convient de souligner que ces pratiques se banalisent, qu'elles concernent de plus en plus les services commerciaux et pénètrent peu à peu la sphère privée et les interactions sociales. Ce mouvement est appelé à s'amplifier dans une économie de plus en plus numérisée, posant la question de la légitimité du recours à certains moyens d'identification et d'authentification, notamment aux informations biométriques, qui, de par leur nature non révocable, soulèvent des questions de sécurité collective en cas de divulgation non-contrôlée.

Ces questions émergentes, dont chacun pressent le caractère essentiel, sont aujourd'hui posées de manière distincte dans le champ des activités régaliennes et de sécurité, dans le champ de l'efficacité et de la simplification administrative, et dans le champ de l'activité économique.

Elles portent sur des valeurs essentielles et parfois contradictoires: sécurité, efficacité, protection des libertés fondamentales, souveraineté, croissance économique, confiance des citoyens et des consommateurs..., qui ne peuvent être articulées que par des décisions politiques après un important débat de société.

Elles mobilisent des concepts techniques insuffisamment maîtrisés par de nombreux acteurs et généralement absents du débat public : identification, authentification, traçabilité, chiffrement, *privacy by design*, systèmes distribués, mutabilité des systèmes d'information, construction de systèmes d'identités proposant des niveaux variables et mobilisant le consentement des utilisateurs, etc.

Elles méritent la construction progressive d'une vision partagée, avec une forte acceptation sociale, des sécurités nécessaires, des principes de gouvernance des systèmes, de la transparence souhaitée, et des enjeux industriels, économiques voire géostratégiques. Cette réflexion devrait mobiliser l'ensemble des parties prenantes : administrations et société civile, entreprises et recherche académique, experts, citoyens et élus.