RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

COUR DES COMPTES

Etat de Genève - DCTI

Rapport

concernant l'audit de gestion

relatif à la gestion des identités numériques et des autorisations

Genève, le 30 juin 2011

Rapport no 45

Cour des Comptes ● 8 rue du XXXI-Décembre ● CP 3159 ● 1211 Genève 3
Tél. +41 (22) 388 77 90 ● Fax +41 (22) 388 77 99
http://www.ge.ch/cdc

LA COUR DES COMPTES

La Cour des comptes est chargée du contrôle indépendant et autonome des services et départements de l'administration cantonale, du pouvoir judiciaire, des institutions cantonales de droit public, des organismes subventionnés ainsi que des institutions communales.

La Cour des comptes vérifie d'office et selon son libre choix la **légalité** des activités et la **régularité** des recettes et des dépenses décrites dans les comptes, et s'assure du **bon emploi** des crédits, fonds et valeurs gérés par les entités contrôlées. Elle organise librement son travail et dispose de larges moyens d'investigation. Elle peut notamment requérir la production de documents, procéder à des auditions, à des expertises, se rendre dans les locaux de l'entité contrôlée.

Sont soumis au contrôle de la Cour des comptes :

- les départements,
- la chancellerie et ses services,
- l'administration du Pouvoir judiciaire,
- le Service du Grand Conseil,
- les institutions cantonales de droit public,
- les autorités communales et les institutions et services qui en dépendent,
- les institutions privées où l'État possède une participation financière majoritaire,
- les organismes bénéficiant de subventions de l'État ou des communes,
- le secrétariat général de l'Assemblée constituante.

Les rapports de la Cour des comptes sont rendus **publics** : ils consignent ses observations, les conclusions de ses investigations, les enseignements qu'il faut en tirer et les recommandations conséquentes. La Cour des comptes prévoit en outre de signaler dans ses rapports les cas de réticence et les refus de collaborer survenus lors de ses contrôles.

La Cour des comptes publie également un **rapport annuel** comportant la liste des objets traités, celle de ceux qu'elle a écartés, celle des rapports rendus avec leurs conclusions et recommandations et les suites qui y ont été données. Les rapports restés sans effets ni suites sont également signalés.

Vous pouvez participer à l'amélioration de la gestion de l'État en contactant la Cour des comptes.
Toute personne, de même que les entités soumises à son contrôle, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement de ses tâches.

Contactez la Cour par courrier postal ou par le formulaire disponible sur Internet :

http://www.ge.ch/cdc

SYNTHÈSE

Dans le cadre de son audit relatif au programme d'administration en ligne (rapport numéro 39), la Cour a identifié la gestion des identités numériques et des autorisations comme présentant des risques élevés notamment en raison du nombre d'applications à l'Etat de Genève, du projet AeL avec 250'000 utilisateurs potentiels ainsi que des exigences élevées en termes de sécurité.

La gestion des identités numériques et des autorisations peut être définie comme l'ensemble des politiques, processus et systèmes déployés pour diriger et gérer de manière efficace et effective les accès aux ressources informatiques au sein d'une organisation. GINA est issue d'une série de projets ayant démarré en 2001 et d'un ensemble de composants (open source, développés en interne ou du marché). Elle gère les droits d'accès aux applications de l'État de Genève ainsi qu'aux prestations de l'administration en ligne (AeL) tant à l'interne de l'administration que depuis l'externe (par internet). Il convient de souligner qu'une solution de gestion des identités et des autorisations pour une institution à structure hétérogène et complexe, telle qu'une administration cantonale, doit pouvoir être évolutive et intégrer des caractéristiques répondant à des standards de sécurité garantissant la confidentialité et la préservation des données sensibles.

Réalisé à l'aide d'évaluations techniques effectuées par des experts externes, l'audit de la Cour a visé à déterminer l'adéquation de la solution GINA, considérant les bonnes pratiques en matière de sécurité, sa capacité à évoluer en fonction des besoins des utilisateurs et de l'environnement technique, et son coût. Il en résulte notamment que la dépendance de la solution GINA à certaines technologies pourrait être considérée comme un élément bloquant pour permettre de répondre à l'évolution de la solution par rapport aux bonnes pratiques en la matière.

En outre, les besoins exprimés par les départements ne sont, à l'heure actuelle, ni suffisamment pris en compte, ni à temps. Le développement actuel de GINA s'opère dans un mode réactif, et le CTI répond dans l'urgence aux requêtes des départements. La solution se base sur une vision globale sécuritaire à long terme du CTI, mais cette solution évolue dans un environnement au sein duquel il est difficile d'avoir une planification à long terme s'inscrivant dans cette vision.

En conclusion, il est nécessaire d'améliorer la gestion des identités et des autorisations afin de maintenir une sécurité adéquate en prévision de l'évolution de l'environnement technologique et des besoins de l'administration. S'il convient de noter qu'un travail important a été effectué, à ce jour, dans un environnement complexe, il s'agit maintenant de démontrer la meilleure manière de faire évoluer la gestion des identités et des autorisations, constatant que son niveau de maturité doit être amélioré. A cette fin, il conviendrait de préparer un mandat d'étude qui, à court terme, permette d'évaluer la faisabilité de maintenir GINA en la faisant évoluer ou de migrer vers une solution alternative.

Comme le veut la pratique en matière de sécurité informatique et en application de l'article 9 al. 4 LICC, la Cour des comptes a choisi de ne pas publier les éléments détaillés des constats pouvant présenter des risques pour l'administration. Ces éléments ont été transmis dans un document distinct au conseiller d'Etat en charge du DCTI en date du 30 juin 2011.

TABLEAU DE SUIVI DES RECOMMANDATIONS

Dans le cadre de ses missions légales, la Cour doit effectuer un suivi des recommandations émises aux entités auditées, en distinguant celles ayant été mises en œuvre et celles restées sans effets.

À cette fin, la Cour a invité le DCTI à remplir le « tableau de suivi des recommandations et actions » qui figure au chapitre 6, et qui **synthétise les améliorations à apporter** et indique leur niveau de **risque**, le **responsable** de leur mise en place ainsi que leur **délai de réalisation**.

L'unique recommandation du rapport a été acceptée par le DCTI qui s'engage à la réaliser d'ici au 30 juin 2012.

OBSERVATIONS DE L'AUDITE

Sauf exceptions, la **Cour ne prévoit pas de réagir aux observations de l'audité**. La Cour estime qu'il appartient au lecteur d'évaluer la pertinence des observations de l'audité eu égard aux constats et recommandations développés par la Cour.

TABLE DES MATIÈRES

Glossaire et liste des principales abréviations utilisées

Active Directory	Service d'annuaire proposé par Microsoft pour les systèmes d'exploitation Windows.
AeL	Administration en ligne
AFC	Administration fiscale cantonale
AIMP	Accord intercantonal sur les marchés publics
AMOA	Assistance à la maîtrise d'ouvrage
Annuaire	Un annuaire permet de recenser et sauvegarder des données concernant des personnes, des réseaux, des ordinateurs. Certains types d'annuaires permettent également de gérer les droits et services à des données.
CFI	Comptabilité financière intégrée
CMMI	Le CMMI, capacity maturity model integrated, est un référentiel de bonnes pratiques en matière de développement informatique. Il permet d'évaluer un service informatique sur la base d'une échelle de maturité (de 1 à 5).
CobiT	Le CobiT, control objectives for information and related technology, est un référentiel des bonnes pratiques en termes de systèmes d'information développé par l'Information systems audit and control association (ISACA).
Connecteur	Technique de connexion entre les applications et GINA (LDAP, JAAS, etc.).
Connectivité	La connectivité fait référence à la faculté des applications à s'intégrer avec d'autres applications, dans ce cas-ci, avec une solution de gestion des identités numériques et des autorisations.
CTI	Centre des technologies de l'information.
DCTI	Département des constructions et technologies de l'information.
DF	Département des finances.
DIP	Département de l'instruction publique, de la culture et du sport.

Framework	De manière simplifiée, en informatique, un framework est un cadre de travail constitué d'outils, de conventions et de bibliothèques (regroupant des codes réutilisables pour des fonctions spécifiques) visant à amener de la rigueur ainsi qu'à faciliter le développement et le maintien de logiciels.
GINA	Gestion des identités numériques et des autorisations.
Groupe	Un groupe rassemble plusieurs personnes ou sous-groupes.
Identification et authentification	Le processus d'identification permet de communiquer une identité (entité, personne) préalablement enregistrée alors que le processus d'authentification permet de vérifier l'identité communiquée.
LSE	Loi fédérale sur le service de l'emploi et la location de services.
Meta annuaire	Un meta annuaire est un annuaire central qui est composé de copies des différents annuaires du réseau. Il permet de fédérer et de synchroniser l'ensemble des bases de données des différents annuaires.
MOA	Maîtrise d'ouvrage.
Niveau de maturité	Indicateur par rapport à une échelle prédéfinie permettant d'évaluer l'adéquation de la solution de gestion des identités et des accès par rapport aux bonnes pratiques reconnues en matière de sécurité (CobiT, CMMi, etc.).
Novell	Éditeur de l'environnement réseau « Netware ».
Novell directory service (NDS)	Service d'annuaire Novell.
OPE	Office du personnel de l'État.
Proxy	Serveur faisant office d'intermédiaire entre le réseau interne et internet.
Reverse Proxy	Serveur proxy placé du côté internet du réseau par lequel passent toutes les demandes internet pour accéder à certaines parties du réseau interne.
Rôles	Ensemble de droits donnés au sein des modules d'une application.
Rôles applicatifs	Les rôles applicatifs permettent de définir et regrouper pour une application les droits liés à un rôle (consultation, saisie, suppression, statistiques, etc.).
SIRH	Système d'information propre au métier des ressources humaines.

SPOF	Un SPOF (Single Point of Failure) est un point unique d'un système d'information qui s'il venait à faillir rendrait indisponible l'ensemble du système d'information.
SSO	Un SSO (Single Sign On) permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs applications.
SuisseID[1]	La SuisseID est issue d'une initiative du secrétariat de l'État à l'économie (SECO). La SuisseID est une solution proposée soit sous forme de carte à puce soit de clé usb. Elle fournit à la fois une signature électronique valable juridiquement ainsi qu'une authentification sécurisée.
TIC	Technologies de l'information et de la communication.

[1] http://www.suisseid.ch/

1. CADRE ET CONTEXTE DE L'AUDIT

Le programme AeL (administration en ligne) a été présenté comme une ouverture de l'administration aux besoins de la société genevoise par la modernisation de son fonctionnement et la transformation de ses systèmes d'information. Il a requis un crédit d'investissement de plus de 26 millions, voté en juin 2008.

Du point de vue de l'analyse des risques de la Cour des comptes, le programme AeL présente des risques élevés notamment en raison des montants financiers en jeu (26'350'000 F pour le crédit d'investissement), des choix technologiques opérés (risque opérationnel) et de la perception des citoyens et des entreprises vis-à-vis des prestations déployées (risque d'image pour l'administration cantonale).

Dans ce contexte, la Cour a décidé de procéder à un audit de légalité et de gestion du programme de l'administration en ligne (AeL). Ainsi, par lettre du 29 avril 2010 adressée à M. Mark Muller, conseiller d'État en charge du département des constructions et technologies de l'information (DCTI), la Cour l'a informé de sa décision de procéder à un audit de légalité et de gestion relatif au programme d'administration en ligne (AeL). Cette mission a fait l'objet du rapport numéro 39.

Dans le cadre de l'audit AeL précité, la Cour a été confrontée à la solution de gestion des identités numériques et des autorisations développée par le centre des technologies de l'information (CTI). Nommée GINA, cette solution a pour objectif de gérer les droits d'accès aux applications de l'État de Genève ainsi qu'aux prestations de l'administration en ligne (AeL), tant à l'interne de l'administration que depuis l'externe (par internet).

Or, la Cour a identifié GINA comme présentant des risques élevés notamment en raison du nombre d'applications existantes à l'État de Genève (plus de 750), du projet AeL avec 250'000 utilisateurs potentiels ainsi que des exigences élevées en termes de sécurité. Compte tenu des spécificités du domaine, la Cour a décidé de mener un audit distinct afin de déterminer si GINA est une solution adéquate, considérant les bonnes pratiques en matière de sécurité, sa capacité à évoluer en fonction des besoins des utilisateurs et de l'environnement technique, et son coût.

La Cour a exclu du champ du présent audit :

- l'analyse de la politique de sécurité ;
- l'analyse et la vérification des processus mis en place au niveau du CTI, des départements, de la chancellerie et du pouvoir judiciaire en matière de gestion des identités ;
- le bien-fondé des droits d'accès accordés ;
- la vérification de l'exhaustivité, de la validité et de la fiabilité des documents remis ;
- les tests de sécurité sur les systèmes d'informations et les applications ;
- les vérifications techniques informatiques portant sur :
    - les composants techniques GINA ;
    - des applications tierces et applications de l'État ;
    - des fonctionnalités, de la sécurité, de la connectivité de la performance et du plan de secours liés à GINA.

Ces thèmes pourront faire l'objet d'audits ultérieurs de la Cour.

Dès lors que l'article 174a al. 1 de la Constitution genevoise (À 2 00) précise que la gestion de l'État doit être économe et efficace, que la Cour doit exercer ses contrôles conformément à cette disposition (art. 8 al. 1 loi D 1 12), et qu'il appartient à la Cour notamment de s'assurer du bon emploi des crédits, fonds et valeurs mis à disposition d'entités publiques (« audit de gestion »), la Cour est compétente (art. 1 al. 2 loi D 1 12).

Souhaitant être la plus efficace possible dans ses travaux, la Cour examine lors de ses investigations **l'ensemble des rapports d'audits préalables** effectués par des tiers, tant internes qu'externes, de même que les **plans de mesures P1** / **P2** / **P+ du Conseil d'État**, portant sur les mêmes thématiques que le présent rapport.

La Cour précise au tableau comparatif présenté au chapitre 7 les constatations faites par l'inspection cantonale des finances (rapport numéro 10-06). Le cas échéant, la Cour a indiqué l'origine de celles ayant servi de base aux constats et recommandations contenus dans le présent rapport.

La Cour note également que la sécurité des systèmes d'information de l'administration cantonale a fait l'objet d'un audit par une société externe (« audit dynamique sécuritaire ») en 2010.

En outre, conformément à son souhait de **contribuer à une coordination efficace des activités des différentes instances de contrôle** actuellement à l'œuvre à l'État de Genève, la Cour a examiné la planification semestrielle des contrôles de l'Inspection cantonale des finances (ICF) et l'a informée de sa mission.

2. MODALITÉS ET DÉROULEMENT DE L'AUDIT

La Cour a conduit cet audit en analysant les documents remis par les principaux acteurs concernés ainsi qu'en menant des entretiens ciblés avec :

- le secrétaire général du département des constructions et technologies de l'information (DCTI) ;
- le directeur de la direction des infrastructures du centre des technologies de l'information (CTI) ;
- le responsable sécurité du CTI ;
- les directeurs des systèmes d'information de 5 départements ;
- le directeur des systèmes d'information du pouvoir judiciaire ;
- le responsable sécurité des systèmes d'information de la chancellerie ;
- l'officier en charge des systèmes d'information et de la sécurité informatique de la police.

La mission s'est déroulée du 8 février au 16 mai 2011.

Afin de déterminer si GINA est une solution adéquate considérant les bonnes pratiques en matière de sécurité, sa capacité à évoluer en fonction des besoins des utilisateurs et de l'environnement technique et son coût, la Cour a entrepris une démarche d'audit fondée sur les évaluations effectuées par des experts externes mandatés par la Cour. La méthodologie d'évaluation utilisée par les experts pour répondre à l'objectif de l'audit se base sur les bonnes pratiques reconnues en matière de sécurité (CobiT, ISO27001, CMMi, etc.) ainsi que sur une comparaison avec des solutions du marché.

Le résultat de ces évaluations est présenté dans le rapport selon les 10 axes suivants :
- Authentification
- Single Sign On et Mot de passe
- Connectivité des applications
- Gestion des utilisateurs et des autorisations
- Sources de vérité
- Gestion des mutations
- Ergonomie
- Plan de continuité
- Fonctionnalités
- Coûts

Pour chacun de ces axes, le chapitre 4 présente les observations de la Cour basées sur les conclusions des experts externes.

Le point 4.11 présente le niveau de maturité de la solution GINA (indicateur par rapport à une échelle prédéfinie permettant d'évaluer l'adéquation de la solution de gestion des identités et des accès par rapport aux bonnes pratiques reconnues en matière de sécurité (CobiT, ISO27001, CMMi, etc.)) compte tenu des 10 axes précités.

Au vu des constats relevés dans le présent rapport et de la nécessité de faire évoluer la solution dans un environnement hétérogène et complexe, il est nécessaire d'appréhender la solution dans sa globalité. La Cour a donc émis une recommandation conclusive au chapitre 5.

Comme prévu par sa base légale, il est à relever que la Cour privilégie avec ses interlocuteurs une démarche constructive et participative visant à la **recherche de solutions améliorant le fonctionnement de l'administration publique**. De ce fait, la Cour a pu proposer aux intervenants rencontrés différentes possibilités d'amélioration de leur gestion, dont la faisabilité a pu être évaluée et la mise en œuvre appréciée sous l'angle **du principe de proportionnalité**.

La Cour a conduit son audit conformément aux **normes internationales d'audit** et aux **codes de déontologie** de l'International Federation of Accountants (IFAC) et de l'Organisation Internationale des Institutions Supérieures de Contrôle des Finances Publiques (INTOSAI) ainsi qu'en utilisant des méthodologies de l'Information Systems Audit and Control Association (ISACA), dans la mesure où ils sont applicables aux missions légales de la Cour.

En pratique, la méthodologie de la Cour des comptes est la suivante :

1ère phase : Planification
Cette phase consiste à définir et à mobiliser les ressources et les compétences les mieux adaptées à la mission, que ce soit auprès des collaborateurs de la Cour des comptes ou auprès de tiers, et à déterminer les outils méthodologiques à utiliser.

2ème phase : Préparation de l'audit
Cette phase consiste à identifier auprès de l'entité auditée quels sont ses bases légales et ses intervenants-clés, à comprendre son organisation et son fonctionnement, à collecter des données chiffrées et à procéder à l'analyse des risques qui lui sont propres. À ce stade, un plan de mission est rédigé avec notamment les objectifs de la mission, les moyens à disposition, les travaux dévolus à chaque intervenant de la Cour et les délais impartis dans le déroulement de la mission.

3ème phase : Récolte d'informations
Cette phase consiste à déterminer les sources de l'information pertinente, à savoir quelles sont les personnes-clés à contacter et quelles sont les informations qui sont nécessaires à l'atteinte des objectifs. Ensuite, les collaborateurs de la Cour et/ou les tiers mandatés procèdent à des entretiens et collectent les informations requises.

4ème phase : Analyse de l'information
Cette phase consiste à analyser les informations récoltées et à les restituer sous la forme de documents de travail.

5ème phase : Proposition de recommandations
Cette phase consiste à établir les constatations significatives, à déterminer les risques qui en découlent et enfin à proposer des recommandations afin de rétablir la légalité des opérations, la régularité des comptes ou d'améliorer la structure ou le fonctionnement de l'organisation.

6ème phase : Rédaction du rapport
Cette phase consiste à rédiger le rapport conformément aux documents de travail et à la structure adoptée par la Cour des comptes.

7ème phase : Validation du rapport
Cette phase consiste à discuter le contenu du rapport avec l'entité auditée, avec pour objectif de passer en revue les éventuelles divergences de fond et de forme et de s'accorder sur les priorités et délais des recommandations.

Ainsi, chaque thème développé dans ce rapport fait l'objet d'une mise en contexte, de constats, de risques découlant des constats et de recommandations (numérotées en référence aux constats) soumis aux observations de l'audité.

Les risques découlant des constats sont décrits et qualifiés en fonction de la **typologie des risques encourus**, risques définis dans le Glossaire qui figure au chapitre 9.

Afin de faciliter le suivi des recommandations, la Cour a placé au chapitre 7 un tableau qui **synthétise les améliorations à apporter** et pour lequel l'entité auditée indique le niveau de **risque**, le **responsable** de leur mise en place ainsi que leur **délai de réalisation**.

3. CONTEXTE GÉNÉRAL

3.1 Gestion des identités numériques et des autorisations[2]

3.1.1 Introduction

La gestion des identités numériques et des autorisations peut être définie comme l'ensemble des politiques, processus et systèmes déployés pour diriger et gérer de manière efficace et effective les accès aux ressources informatiques au sein d'une organisation.

3.1.2 La gestion des identités numériques et des autorisations à l'État de Genève

Dans le cadre de l'administration cantonale, GINA (gestion des identités numériques et des autorisations) est une solution de gestion centralisée des identités numériques et des autorisations développée par le centre des technologies de l'information (CTI), afin de gérer les droits d'accès aux applications de l'État de Genève ainsi qu'aux prestations de l'administration en ligne (AeL) tant à l'interne de l'administration que depuis l'externe (par internet).

Concrètement, GINA est composée des principaux éléments suivants :

- Meta annuaire : base de données centralisée contenant l'ensemble des groupes d'utilisateurs, des utilisateurs de l'administration cantonale et de leurs droits d'accès. Le meta annuaire est synchronisé avec les données des autres annuaires de l'administration cantonale (LDAP). Un meta annuaire distinct est utilisé pour les données relatives aux accès externes (accès par des personnes ou entités externes aux données, services, prestations en ligne de l'administration cantonale).

- Référentiel SIRH[3] : base de données des collaborateurs et des structures organisationnelles auxquelles ils sont rattachés. Ces données sont importées depuis la base de données SIRH vers le meta annuaire de l'administration cantonale.

- Interface utilisateur GINA : il s'agit d'un écran permettant l'identification et l'authentification d'une personne ou d'une entité (interne ou externe).

  « GINA Manager » : est un outil permettant à des administrateurs spécifiquement désignés (généralement au niveau d'une direction départementale des systèmes d'information) de gérer les groupes d'utilisateurs, les rôles applicatifs et les droits d'accès aux applications. Ces droits de gestion sont accordés par domaines organisationnels de compétence (selon les cas, un domaine peut être assimilé à un service de l'administration).

[2] Dans le domaine des technologies de l'information, la terminologie communément employée est *Identity and access management (IAM)*.

[3] Le progiciel SIRH est le nom communément utilisé pour le système d'information des ressources humaines, qui permet essentiellement d'administrer la paie et la gestion du personnel de l'administration cantonale (absences, etc.).

- « Meta Manager » : outil permettant à la centrale d'appel du CTI de gérer le cycle de vie des utilisateurs (création, etc.).

- « PM Manager » : outil gérant les processus d'inscriptions et de délégations d'autorisations à des applications de l'Etat pour les citoyens et les entreprises.

Les processus utilisés dans le cadre de GINA peuvent être résumés comme suit :

Identification et authentification : l'identification s'opère via l'interface utilisateur qui demande la saisie de l'identifiant et le mot de passe. Le processus d'identification et d'authentification se déroule donc en parallèle. Deux niveaux d'authentification sont disponibles dans GINA (simple et fort). L'authentification simple ne requiert que l'identifiant et le mot de passe. L'authentification forte peut s'effectuer de deux manières, soit par l'utilisation de la SuisseID, soit par l'envoi d'un SMS ou message vocal sur le téléphone fixe d'un deuxième mot de passe à usage unique (one time password) et de durée de vie limitée,

- Une fois l'authentification effectuée, GINA appelle l'application ou la prestation en transmettant l'identité de la personne ou de l'entité (transmission cryptée).

- Finalement, l'application ou la prestation consultent GINA pour s'assurer que la personne ou l'entité dispose bien des droits requis (rôles prédéfinis) lorsque les rôles applicatifs sont définis dans GINA (ce qui n'est pas le cas pour l'ensemble des applications).

Dans le cadre des accès aux prestations de l'administration en ligne, le règlement sur la communication électronique du canton (RCEI) précise :

« *Art. 4 Catégories [1] Les modes d'identification sont les suivants :*
a) identification simplifiée;
b) identification normale;
c) identification forte.
[2] L'autorité peut en tout temps décider de recourir à un mode d'identification d'un niveau supérieur à celui prescrit.

Art. 5 Identification simplifiée
L'identification simplifiée implique l'utilisation d'un mot ou d'un nombre communiqué préalablement à l'utilisateur par l'autorité. Elle peut aussi s'effectuer par l'utilisation de données communiquées par l'utilisateur (nom, adresse).

Art. 6 Identification normale
[1] L'identification normale implique l'utilisation d'un nom d'utilisateur et d'un mot de passe.
[2] Le mot de passe peut être choisi par l'utilisateur ou déterminé par l'autorité.

Art. 7 Identification forte
[1] L'identification forte implique l'utilisation d'un nom d'utilisateur, d'un mot de passe et d'un code à usage unique.
[2] Le mot de passe peut être choisi par l'utilisateur ou déterminé par l'autorité.
[3] Le code à usage unique est déterminé par l'autorité et communiqué à l'utilisateur par SMS ou message vocal sur un téléphone fixe. »

Le rapport numéro 39 de la Cour relève que le terme d'identification est mal choisi, puisqu'il s'agit en réalité d'authentification à laquelle il est fait référence dans le cadre du RCEI. En outre, également comme mentionné dans le rapport numéro 39 de la Cour, le processus mis en place pour l'identification des personnes mériterait d'être amélioré pour certains types de prestations (sauf pour les utilisateurs de la SuisseID[4] ainsi que pour la procédure relative à GE-Tax Internet[5]). En effet, il n'est pas possible de s'assurer avec un haut degré de vraisemblance de l'identité de la personne ayant sollicité la prestation, puisque les types d'authentification mis en place dans le cadre de l'AeL ne permettent pas d'assurer à *l'initium* l'identité de la personne ayant créé un compte utilisateur pour particulier, faute de vérification effective de l'identité de la personne. Pour les prestations actuellement déployées, le risque lié à l'authentification apparaît toutefois comme faible au niveau de la probabilité d'occurrence. Cependant, en cas de litige, ce risque sur les prestations en ligne augmenterait la difficulté pour l'autorité cantonale de prouver la vraisemblance de l'identité de la personne ayant sollicité une prestation en ligne.

3.1.3 Historique

GINA est issue d'une série de projets ayant démarré en 2001, décrits brièvement ci-dessous :

- **2001 : META**
  Ce projet visait à faciliter la gestion des comptes des utilisateurs de l'administration cantonale en mettant en œuvre un meta annuaire.

- **2002 : Composant Sécurité Applicative**
  Composant développé à l'interne par le CTI afin de gérer les accès et les autorisations des applications développées dans le cadre du framework java[6] (par exemple les applications métiers de l'administration fiscale cantonale : taxation, perception, etc.).

- **2004 PUMA :**
  Migration des domaines d'authentification de NT4.0 vers Microsoft (Active Directory).

- **2007 Mise en place des liens entre le meta annuaire et le composant de sécurité applicative du CTI :**
  Il s'agit de la mise en place d'une maîtrise centralisée de la gestion des identités numériques et des autorisations pour l'administration cantonale.

- **2007 ID-DIP :**
  Le projet ID-DIP avait pour objectif de revoir les différents processus de création des identités du département de l'instruction publique (DIP), afin de les rationaliser, et d'automatiser la création des comptes des enseignants en se basant sur les données du progiciel SIRH comme référentiel.

[4] La SuisseID est issue d'une initiative du secrétariat de l'État à l'économie (SECO). La SuisseID est une solution proposée soit sous forme de carte à puce soit de clé usb. Elle fournit à la fois une signature électronique valable juridiquement ainsi qu'une authentification sécurisée.
[5] Il s'agit de la version web du CD Rom GE-Tax permettant la saisie sur ordinateur de la déclaration d'impôt du canton de Genève.
[6] Cadre de développement initial utilisé au CTI (se référer également au rapport 21 de la Cour).

- **2008 SIRH-META :**
  Suite au projet ID-DIP, le projet SIRH-META a été lancé afin d'appliquer les processus de création de comptes automatiques depuis SIRH à l'ensemble des collaborateurs internes de l'administration cantonale. La première étape avait pour objectif le rapprochement entre SIRH et le meta annuaire, ce qui répondait notamment au besoin du projet de dématérialisation des bulletins de salaires pour les collaborateurs de l'administration cantonale.

- **2009 Administration en ligne (AeL) :**
  Dans le cadre de l'AeL, divers services de gestion d'identités ont été développés à partir de GINA pour gérer les connexions aux prestations en ligne de l'administration cantonale (authentification faible et forte).

3.1.4 Chiffres clés

En date de l'audit (état à avril 2011), environ 40 % des applications de l'État sont intégrées à GINA (environ 750 applications différentes). GINA permet de gérer l'identification et l'authentification d'environ 23'000 collaborateurs de l'État. En outre, GINA gère l'accès depuis l'externe à des applications de l'administration cantonale et/ou aux prestations en ligne (AeL) pour environ 7'000 citoyens et environ 15'800 personnes agissant au nom d'une personne morale.

4. ANALYSE

Comme le veut la pratique en matière de sécurité informatique et en application de l'art. 9 al. 4 LICC, la Cour des comptes a choisi de ne pas publier les éléments détaillés des constats pouvant présenter des risques pour l'administration. Ces éléments ont été transmis dans un document distinct au conseiller d'Etat en charge du DCTI en date du 30 juin 2011.

Ainsi, les chapitres 4.1 à 4.10 (Authentification, Single Sign On et Mot de passe, Connectivité des applications, Gestion des utilisateurs et des autorisations, Sources de vérité, Gestion des mutations, Ergonomie, Plan de continuité, Fonctionnalités, Coûts) ne présentent que les contextes.

Le chapitre 4.11 (Modèle de maturité) présente le contexte et les constats non détaillés.

Quant à elles, les recommandations conclusives ainsi que les observations de l'audité sont intégralement présentées au chapitre 5.

4.1 Authentification

4.1.1 Contexte

De manière générale, un processus d'identification permet de communiquer une identité (entité, personne) préalablement enregistrée, alors qu'un processus d'authentification permet de vérifier l'identité communiquée.

L'authentification peut s'effectuer par divers moyens (mot de passe, clé usb, biométrie, etc.). Une authentification peut être simple (utilisation d'un seul critère, tel que le mot de passe) ou forte (utilisation d'au moins deux critères, par exemple un mot de passe et une clé usb). Il convient de noter que seule l'authentification forte permet d'assurer cumulativement le contrôle des accès, la confidentialité, la traçabilité et l'intégrité.

Selon les bonnes pratiques, le mot de passe utilisé par les collaborateurs internes de l'administration cantonale pour son réseau interne doit différer du mot de passe utilisé pour le réseau externe (internet).

4.2 Single Sign On (SSO)

4.2.1 Contexte

Un SSO (Single Sign On) permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs applications.

Il convient de noter que l'objectif premier de la mise en place d'un SSO est le confort pour l'utilisateur. Ainsi, les solutions de gestion des identités et des autorisations offrent généralement un mécanisme d'authentification unifiée à travers toutes les ressources de l'organisation, comprenant les postes de travail, les client-serveur, les applications développées en interne et les progiciels.

4.3 Connectivité des applications

4.3.1 Contexte

La connectivité fait référence à la faculté des applications à s'intégrer avec d'autres applications, dans ce cas-ci, avec une solution de gestion des identités numériques et des autorisations. Elle doit être aisée et basée sur les standards.

La stratégie d'intégration des applications avec la solution de gestion des identités et des autorisations prend en compte la question de la gestion des rôles applicatifs.

Les rôles applicatifs consistent à définir et regrouper pour une application les droits liés à un rôle (consultation, saisie, suppression, statistiques, etc.). Les bonnes pratiques recommandent, dans un souci de simplicité, d'efficacité et de maîtrise, de les administrer au niveau des applications métiers. Les départements en charge de ces applications métiers doivent effectuer la gestion de leurs propres rôles applicatifs.

En outre, selon les bonnes pratiques, la stratégie d'intégration des applications à un système fédérateur et centralisé de gestion des identités et des accès doit permettre à ce système de rester maître et gérant des identifiants utilisateurs, chaque identifiant devant être considéré comme unique par les applications.

4.4 Gestion des utilisateurs et des autorisations

4.4.1 Contexte

De manière générale, les solutions de gestion des identités et des autorisations intègrent une gestion des utilisateurs, des accès et des autorisations dans leurs outils. Une administration et une gestion adéquates des identités et des utilisateurs, combinées avec des contrôles d'accès appropriés, permettent de renforcer la conformité tout en protégeant les ressources au point d'accès, ainsi que de déléguer les décisions d'authentification et d'autorisation au sein d'une autorité centrale.

4.5 Source de vérité

4.5.1 Contexte

La notion de source de vérité fait référence à la notion de référentiel unique des utilisateurs et de leurs attributs (données personnelles, etc.).

Les bonnes pratiques informatiques recommandent la mise en place d'une source de vérité unique afin de notamment garantir l'intégrité des annuaires et de minimiser les risques de doublons et de non-identification des utilisateurs.

4.6 Gestion des mutations

4.6.1 Contexte

Les mutations peuvent être définies dans le cadre du présent chapitre comme la création, la modification, et la désactivation de comptes utilisateurs.

De manière générale, les solutions de gestion des identités numériques et des autorisations permettent d'effectuer une gestion de mutations dans leurs fonctionnalités de base (fonctionnalité automatisée de désactivation des comptes de services et génériques, etc.), sans la nécessité de développements ad hoc.

4.7 Ergonomie

4.7.1 Contexte

De manière générale, les solutions du marché offrent aux utilisateurs une grande convivialité, une utilisation souple, et une ergonomie permettant d'une part de générer une large panoplie de requêtes standardisées et d'autre part de personnaliser des rapports d'audit à travers un cockpit. De plus, elles offrent la possibilité d'une évolution en fonction des besoins des utilisateurs, afin de développer ou faire développer facilement des rapports spécifiques.

4.8 Plan de continuité

4.8.1 Contexte

Le concept de plan de continuité et de fonctionnalités alternatives est généralement directement proposé dans les solutions de gestion des identités et des autorisations afin de permettre la continuité des activités de l'administration en cas de pannes. Ces solutions proposent généralement des moyens secondaires dans leurs fonctionnalités de base.

4.9 Fonctionnalités

4.9.1 Contexte

De manière générale, les solutions de gestion des identités et des autorisations offrent les fonctionnalités de base suivantes : annuaire, méta annuaire, gestion des identités et des accès, gestion des mutations, gestion du SSO, gestion des mots de passe, gestion des accès Web, suivi des ségrégations des tâches, gestion des autorisations.

4.10 Coût de la solution GINA

4.10.1 Contexte

Coûts de la solution GINA

Les coûts de développement, d'intégration, d'exploitation des annuaires (y compris au niveau de la qualité des données) et le support d'une solution interne sont essentiellement composés des rémunérations des collaborateurs internes et externes du CTI. Les tableaux ci-dessous résument en termes d'ETP (équivalent temps plein) et nombre de collaborateurs les ressources du CTI en la matière pour la solution GINA :

Ressources en ETP (annualisées)

	2005	2006	2007	2008	2009	2010
ETP Internes	0.6	1.3	5.6	5.6	6.0	6.6
ETP Externes	0.5	0.8	1.4	1.8	1.8	2.2
Total	**1.1**	**2.1**	**7.0**	**7.4**	**7.8**	**8.8**

Ressources en nombre de collaborateurs

	2005	2006	2007	2008	2009	2010
Nombre de collaborateurs internes	2.0	3.0	3.0	7.0	8.0	8.0
Nombre de collaborateurs externes	1.0	1.0	2.0	2.0	2.0	3.0
Total	**3.0**	**4.0**	**5.0**	**9.0**	**10.0**	**11.0**

Par ailleurs, en plus des ressources indiquées ci-dessus, les départements ont ponctuellement mis à disposition des ressources afin d'implémenter la solution. En effet, les responsables des systèmes d'information des départements participent à la mise en place de GINA pour les applications les concernant.

De plus, il convient de noter que des développements spécifiques peuvent également être effectués par les éditeurs de certaines applications du marché appelées à être connectées avec la solution GINA.

Finalement, des coûts d'infrastructures doivent également être pris en compte dans le coût de la solution.

4.11 Modèle de maturité

4.11.1 Contexte

Le modèle utilisé pour mesurer le degré de maturité de la gestion des identités et des accès à l'État[7] est spécialement adapté à cette problématique. Il se base sur des référentiels reconnus (notamment CobiT, ISO27001 et CMMi). Son échelle de mesure définit cinq niveaux de maturité : peu fiable, informel, standardisé, maîtrisé et optimisé. Cette échelle permet de situer le niveau de maturité de l'administration cantonale par rapport aux bonnes pratiques du domaine et facilite la prise de décisions stratégiques concernant les orientations à prendre ainsi que la mesure des progrès accomplis par rapport aux objectifs fixés. Un niveau de maturité adéquat en termes de gestion des identités et des accès, au sein de l'administration cantonale, est essentiel, notamment au vu de la nécessité de garantir la confidentialité, l'intégrité et la disponibilité de certaines données, par exemple les données fiscales.

Le tableau ci-dessous synthétise les cinq niveaux de maturité et leurs principales caractéristiques :

Échelle	Niveau de maturité	Principales caractéristiques
5	Optimisé	Les processus sont régulièrement améliorés au niveau de la qualité et de l'efficacité.
4	Maîtrisé	La hiérarchie effectue une surveillance du système, les déviations sont détectées et les mesures correctives sont prises lorsque nécessaires.
3	Standardisé	Les processus et procédures sont formalisés et généralement suivis. Cependant, les déviations ne sont probablement pas détectées.
2	Informel	Forte probabilité d'erreur. Certaines tâches sont effectuées de manière similaire par les employés. La connaissance et l'autorité sont principalement centralisées sur un employé.
1	Peu fiable	Forte probabilité d'erreur. Le bon fonctionnement dépend exclusivement de l'autorité et de la bonne volonté des employés.

En règle générale, en termes de gestion des identités et des autorisations, le niveau 3 est considéré comme adéquat en moyenne.

4.11.2 Constats

1. D'une manière générale, un modèle d'évaluation de la maturité d'une solution de gestion des identités et des autorisations n'a pas été utilisé à ce jour par le CTI.
2. Dans le cadre de l'audit, un niveau de maturité a été évalué, par les experts externes, pour chaque axe d'analyse de la solution (authentification, connectivité, SSO, etc.). Le détail de ce niveau de maturité n'est pas présenté, en application de l'article 9, alinéa 4 LICC. Toutefois, ce niveau de maturité devra encore être amélioré.

[7] Le modèle est celui développé et utilisé par les experts externes mandatés par la Cour sur de nombreuses organisations.

5. RECOMMANDATIONS CONCLUSIVES

Il convient de souligner qu'une solution de gestion des identités et des autorisations pour une institution à structure hétérogène et complexe, telle qu'une administration cantonale, doit pouvoir être évolutive et intégrer des caractéristiques répondant à des standards de sécurité garantissant la confidentialité et la préservation des données sensibles.

La solution GINA est issue d'un ensemble de composants (open source, développés en interne ou du marché). La majorité des analyses ont été conduites par le CTI et la plupart des considérations et des choix technologiques sont issus de décisions propres au CTI afin d'assurer la sécurité des systèmes d'information de l'Etat. Par ailleurs, il apparaît à ce jour que la dépendance de la solution GINA à certaines technologies pourrait être considérée comme un élément bloquant pour permettre de répondre à l'évolution de la solution par rapport aux bonnes pratiques en la matière.

En outre, les besoins exprimés par les départements ne sont, à l'heure actuelle, ni suffisamment pris en compte, ni à temps. Le développement actuel de GINA s'opère dans un mode réactif, et le CTI répond dans l'urgence aux requêtes des départements. La solution se base sur une vision globale sécuritaire à long terme du CTI, mais cette solution évolue dans un environnement au sein duquel il est difficile d'avoir une planification à long terme s'inscrivant dans cette vision.

Néanmoins, il convient de noter qu'un travail important a été effectué à ce jour, dans cet environnement complexe. Il ressort des analyses menées que la gestion des identités et des autorisations est coûteuse, tant par rapport aux fonctionnalités requises que par rapport aux évolutions prévisibles de l'administration (administration en ligne, intégration éventuelle de plusieurs centaines d'applications hétérogènes de l'État). Selon les experts mandatés par la Cour, les coûts d'études et de mise en œuvre d'une solution standard du marché s'élèveraient approximativement entre 2 et 3 millions, auxquels viendraient s'ajouter les coûts de licence, comprenant la maintenance, estimés entre 2.5 à 3.8 millions par année sur la base d'une analyse comparative préliminaire succincte.

Il s'agit maintenant de démontrer la meilleure manière de faire évoluer la gestion des identités et des autorisations. A cette fin, il conviendrait de préparer un mandat d'étude qui, à court terme, permette d'évaluer la faisabilité de maintenir GINA en la faisant évoluer ou de migrer vers une solution alternative. En particulier, il serait nécessaire d'examiner les coûts et bénéfices offerts par des solutions alternatives (solutions commerciales ou open source) et la solution GINA en tenant compte des besoins sécuritaires et de confort des utilisateurs, telle que l'opportunité de mettre en place un SSO pour l'ensemble des applications de l'administration cantonale. Ce mandat devra être validé par le DCTI et mené par le Collège spécialisé des systèmes d'information.

5.1. Observations de l'audité

Nous partageons la recommandation de la Cour des comptes pour préparer un mandat d'étude qui, à court terme, permettra d'évaluer la faisabilité de maintenir la solution Gina en la faisant évoluer ou de migrer vers une solution du marché.

Nous partageons les observations apportées dans les constats mais ceux-ci doivent faire l'objet d'une analyse coûts/bénéfices dans le cadre de l'étude à réaliser.

Nous partageons la proposition de la Cour d'intégrer le modèle de maturité que nous avons découvert dans cet audit pour qu'il puisse nous aider à mesurer le niveau de notre système actuel et d'autre part nous permette chaque année de suivre son évolution sur la base d'un modèle reconnu. Nous ferons le nécessaire pour que cette étude soit lancée très rapidement.

6. TABLEAU DE SUIVI DES RECOMMANDATIONS ET ACTIONS

Réf.	Recommandation/Action	Mise en place (selon indications de l'audité)			
		Risque 4 = Très significatif 3 = Majeur 2 = Modéré 1 = Mineur	**Responsable**	**Délai au**	**Fait le**
1	Préparer un mandat d'étude qui, à court terme, permette d'évaluer la faisabilité de maintenir GINA en la faisant évoluer ou de migrer vers une solution alternative. En particulier, il serait nécessaire d'examiner les coûts et bénéfices offerts par des solutions alternatives (solutions commerciales ou open source) et la solution GINA en tenant compte des besoins sécuritaires et de confort des utilisateurs, telle que l'opportunité de mettre en place un SSO pour l'ensemble des applications de l'administration cantonale.	4	DCTI/CSSI	30.06.2012	

7. RECUEIL DES POINTS SOULEVES PAR LES AUTRES AUDITS PORTANT SUR LES MEMES THEMES

Comme le veut la pratique en matière de sécurité informatique et en application de l'article 9 al. 4 LICC, la Cour des comptes a choisi de ne pas publier les éléments détaillés de certains constats pouvant présenter des risques pour l'administration. Ces éléments ont été transmis dans un document distinct au conseiller d'Etat en charge du DCTI en date du 30 juin 2011.

8. DIVERS

8.1. Glossaire des risques

Afin de définir une **typologie des risques pertinente aux institutions et entreprises soumises au contrôle de la Cour des comptes**, celle-ci s'est référée à la littérature économique récente en matière de gestion des risques et de système de contrôle interne, relative tant aux entreprises privées qu'au secteur public. En outre, aux fins de cohésion terminologique pour les entités auditées, la Cour s'est également inspirée du « Manuel du contrôle interne, partie I » de l'État de Genève (version du 13 décembre 2006).

Dans un contexte économique, le **risque** représente la « possibilité qu'un événement survienne et nuise à l'atteinte d'objectifs ». Ainsi, la Cour a identifié trois catégories de risques majeurs, à savoir ceux liés aux objectifs **opérationnels** (1), ceux liés aux objectifs **financiers** (2) et ceux liés aux objectifs de **conformité** (3).

1) Les risques liés aux objectifs opérationnels relèvent de constatations qui touchent à la structure, à l'organisation et au fonctionnement de l'État et de ses services ou entités, et dont les conséquences peuvent avoir une incidence notable sur la qualité des prestations fournies, sur l'activité courante, voire sur la poursuite de son activité.

Exemples :

- engagement de personnel dont les compétences ne sont pas en adéquation avec le cahier des charges ;
- mauvaise rédaction du cahier des charges débouchant sur l'engagement de personnel ;
- mesures de protection des données entrantes et sortantes insuffisantes débouchant sur leur utilisation par des personnes non autorisées ;
- mauvaise organisation de la conservation et de l'entretien du parc informatique, absence de contrat de maintenance (pannes), dépendances critiques ;
- accident, pollution, risques environnementaux.

2) Les risques liés aux objectifs financiers relèvent de constatations qui touchent aux flux financiers gérés par l'État et ses services et dont les conséquences peuvent avoir une incidence significative sur les comptes, sur la qualité de l'information financière, sur le patrimoine de l'entité ainsi que sur la collecte des recettes, le volume des charges et des investissements ou le volume et coût de financement.

Exemples :

- insuffisance de couverture d'assurance entraînant un décaissement de l'État en cas de survenance du risque mal couvert ;
- sous-dimensionnement d'un projet, surestimation de sa profitabilité entraînant l'approbation du projet.

3) Les risques liés aux objectifs de conformité (« compliance ») relèvent de constatations qui touchent au non-respect des dispositions légales, réglementaires, statutaires ou tout autre document de référence auquel l'entité est soumise et dont les conséquences peuvent avoir une incidence sur le plan juridique, financier ou opérationnel.

Exemples :

- dépassement de crédit d'investissement sans information aux instances prévues ;
- tenue de comptabilité et présentation des états financiers hors du cadre légal prescrit (comptabilité d'encaissement au lieu de comptabilité d'engagement, non-respect de normes comptables, etc.) ;
- absence de tenue d'un registre des actifs immobilisés ;
- paiement de factures sans les approbations requises, acquisition de matériel sans appliquer les procédures habituelles.

À ces trois risques majeurs peuvent s'ajouter trois autres risques spécifiques qui sont les risques de **contrôle** (4), de **fraude** (5) et **d'image** (6).

4) Le risque de contrôle relève de constatations qui touchent à une utilisation inadéquate ou à l'absence de procédures et de documents de supervision et de contrôle ainsi que de fixation d'objectifs. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- absence de tableau de bord débouchant sur la consommation des moyens disponibles sans s'en apercevoir ;
- procédures de contrôle interne non appliquées débouchant sur des actions qui n'auraient pas dû être entreprises ;
- absence de décision, d'action, de sanction débouchant sur une paralysie ou des prestations de moindre qualité.

5) Le risque de fraude relève de constatations qui touchent aux vols, aux détournements, aux abus de confiance ou à la corruption. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- organisation mise en place ne permettant pas de détecter le vol d'argent ou de marchandises ;
- création d'emplois fictifs ;
- adjudications arbitraires liées à l'octroi d'avantages ou à des liens d'intérêt ;
- présentation d'informations financières sciemment erronées par exemple sous-estimer les pertes, surestimer les recettes ou ignorer et ne pas signaler les dépassements de budget, en vue de maintenir ou obtenir des avantages personnels, dont le salaire.

6) Le risque d'image (également connu sous « risque de réputation ») relève de constatations qui touchent à la capacité de l'État et de ses services ou entités à être crédible et à mobiliser des ressources financières, humaines ou sociales. Ses conséquences peuvent avoir une incidence sur la réalisation des objectifs opérationnels, financiers et de conformité.

Exemples :

- absence de contrôle sur les bénéficiaires de prestations de l'État ;
- bonne ou mauvaise réputation des acheteurs et impact sur les prix ;
- porter à la connaissance du public la mauvaise utilisation de fonds entraînant la possible réduction ou la suppression de subventions et donations.

8.2. Remerciements

La Cour remercie l'ensemble des collaborateurs qui lui ont consacré du temps.

L'audit a été terminé le 16 mai 2011. Le rapport complet a été transmis au CTI le 14 juin 2011 dont les observations remises le 24 juin 2011 ont été dûment reproduites dans le rapport.

La synthèse a été rédigée après réception des observations des entités auditées.

Genève, le 30 juin 2011

Stanislas Zuin	Antoinette Stalder	Stéphane Geiger
Président	Magistrat titulaire	Magistrat titulaire