NUMÉRO DE DOSSIER: 2022-0941
IDENTITÉ DE CLASSIFICATION: 3 2 3

Le cadre de confiance

pour l’identité électronique suédoise

Version du 4 octobre 2022

1. Contexte et objectif

Le cadre de confiance pour l'identité électronique suédoise vise à établir des exigences communes pour les émetteurs d'identités électroniques examinés et approuvés par l'Agence suédoise pour l'administration numérique (DIGG). Les exigences sont divisées en différents niveaux de protection – appelés les niveaux de garantie – qui correspondent à différents degrés de sécurité technique et opérationnelle de la part de l'émetteur et à différents degrés de vérification que la personne à laquelle un document d'identité électronique est délivré est bien celle qu'elle prétend être.

Les exigences de ce cadre de confiance s'appliquent aux niveaux d'assurance 2 à 4, le niveau 4 correspondant au niveau de protection le plus élevé.

La conformité doit être interprétée de la manière suivante:

(a) lorsque le niveau d'assurance n'est pas précisé, l'exigence doit être respectée à tous les niveaux, et

(b) lorsque le niveau d'assurance est spécifié, la conformité est assurée au moins au niveau pertinent.

Les exigences fixées pour un niveau inférieur au niveau pertinent ne sont pas prises en considération.

2. Organisation et gouvernance

Exigences opérationnelles globales

K2.1 Les émetteurs d'identités électroniques suédoises qui ne sont pas des organismes publics doivent opérer en tant qu'entités juridiques enregistrées et souscrire et maintenir l'assurance requise pour l'activité.

K2.2 Les émetteurs d'identités électroniques suédoises doivent avoir une activité établie, être pleinement opérationnels dans toutes les parties spécifiées dans le présent document et bien connaître les exigences légales qui leur sont imposées en tant qu'émetteurs d'identités électroniques suédoises.

K2.3 Les émetteurs d'identités électroniques suédoises doivent être en mesure de supporter le risque de responsabilité en cas de dommages et disposer de ressources financières suffisantes pour mener leurs opérations pendant au moins un an.

Sécurité de l'information

K2.4 Les émetteurs d'identités électroniques suédoises ont mis en place un système de gestion de la sécurité de l'information (ISMS) pour les parties de leurs activités concernées par le cadre de confiance, qui repose, le cas échéant, sur la norme ISO/IEC 27001 ou des principes équivalents pour la gestion et le contrôle des travaux relatifs à la sécurité de l'information, y compris les éléments suivants:

(a) Tous les processus administratifs et techniques critiques pour la sécurité doivent être documentés et fondés sur une base formelle, où les rôles, les responsabilités et les pouvoirs sont clairement définis.

(b) Les émetteurs d'identités électroniques suédoises veillent à disposer à tout moment de ressources humaines suffisantes pour s'acquitter de leurs obligations.

(c) Les émetteurs d'identités électroniques suédoises mettent en place un processus de gestion des risques qui, de manière appropriée, en continu ou au moins tous les 12 mois, analyse les menaces et les vulnérabilités de l'entreprise et qui, grâce à l'introduction de mesures de sécurité, équilibre les risques à des niveaux acceptables.

(d) Les émetteurs d'identités électroniques suédoises mettent en place un processus de gestion des incidents qui garantit systématiquement la qualité du service, les formes de signalement ultérieur et que des mesures réactives et préventives appropriées sont prises pour atténuer ou prévenir les dommages résultant de tels événements.

(e) Les émetteurs d'identités électroniques suédoises établissent et testent régulièrement un plan de continuité qui répond aux exigences d'accessibilité de l'entreprise grâce à la capacité de rétablir les processus critiques en cas de crise ou d'incident grave.

(f) Les émetteurs d'identités électroniques suédoises doivent évaluer régulièrement le travail de sécurité de l'information et introduire des mesures d'amélioration dans le système de gestion.

K2.5 Portée et maturité du système de gestion:

Niveau 4: Le système de gestion de la sécurité de l'information doit être conforme à la norme SS-ISO/IEC 27001:2017 ou à des versions ultérieures ou internationales équivalentes de la norme et, dans le cadre de celle-ci, inclure toutes les exigences imposées aux émetteurs d'identités électroniques suédoises.

Conditions de sous-traitance

K2.6 L'émetteur d'identités électroniques suédoises qui a externalisé l'exécution d'un ou de plusieurs processus critiques pour la sécurité à une autre partie doit définir par contrat les processus critiques dont le sous-traitant est responsable et les exigences qui leur sont applicables, et clarifier la relation contractuelle dans la déclaration de l'émetteur.

Traçabilité, suppression et stockage des documents

K2.7 Les émetteurs d'identités électroniques suédoises stockent:

(a) les documents de demande et les documents relatifs à la délivrance, à la réception ou au blocage des identités électroniques;

(b) les contrats, les documents de politique et les déclarations des émetteurs; et

(c) l'historique du traitement et d'autres documents nécessaires pour prouver le respect des exigences imposées aux émetteurs d'identités électroniques suédoises et permettant un suivi démontrant que les processus et contrôles critiques pour la sécurité sont en place et efficaces.

K2.8 La durée de stockage ne peut être inférieure à cinq ans et le matériel doit pouvoir être produit sous une forme lisible tout au long de cette période, à moins qu'une exigence de suppression ne soit nécessaire du point de vue de la vie privée et ne soit étayée par une loi ou une autre réglementation.

Examen et suivi

K2.9 Les émetteurs d'identités électroniques suédoises mettent en place une fonction d'audit interne qui examine périodiquement les activités d'émission. L'auditeur interne est indépendant dans l'exercice de ses fonctions d'une manière qui garantit un examen objectif et impartial et possède la compétence et l'expérience requises pour l'exercice de ses fonctions. L'auditeur interne planifie de manière indépendante la conduite de l'audit et le documente dans un plan d'audit couvrant une période de trois ans. Les éléments d'audit sont sélectionnés sur la base d'une analyse des risques et de l'importance relative et sont fondés sur les descriptions des opérations soumises par l'émetteur à l'Agence pour l'administration numérique.

Niveaux 3 et 4: L'audit interne est effectué sur la base de normes d'audit acceptées.

3. Sécurité physique, administrative et personnelle

K3.1 Les parties centrales de l'opération sont physiquement protégées contre les dommages résultant d'événements environnementaux, d'un accès non autorisé ou d'autres perturbations extérieures. Le contrôle d'accès est appliqué de telle sorte que l'accès aux zones sensibles soit limité au personnel autorisé, que les supports d'information soient stockés et éliminés en toute sécurité et que l'accès à ces zones protégées soit surveillé en permanence.

K3.2 Avant qu'une personne n'assume l'un des rôles identifiés conformément au point K2.4 a), et qui revêtent une importance particulière pour la sécurité, l'émetteur des identités électroniques suédoises doit avoir effectué des vérifications des antécédents afin de s'assurer que la personne peut être considérée comme fiable et qu'elle possède les qualifications et la formation requises pour exécuter en toute sécurité les tâches résultant de son rôle.

K3.3 Les émetteurs mettent en place des procédures garantissant que seul le personnel spécifiquement autorisé a accès aux données collectées et conservées conformément au point K2.7.

K3.4 **Niveaux 3 et 4:** Les émetteurs veillent, tout au long de la chaîne de délivrance, à ce que la séparation des tâches soit appliquée de manière à ce qu'aucune personne ne puisse obtenir une identité électronique au nom d'une autre personne.

4. Sécurité technique

K4.1 Les émetteurs d'identités électroniques suédoises veillent à ce que les contrôles techniques en place soient suffisants pour atteindre le niveau de protection jugé nécessaire eu égard à la nature, à la portée et aux autres circonstances de l'activité, et à ce que ces contrôles fonctionnent et soient efficaces.

K4.2 Les moyens de communication électroniques utilisés pour la transmission de données sensibles doivent être protégés contre l'interception, la manipulation et la relecture.

K4.3 Le matériel de codage cryptographique sensible utilisé pour délivrer des identités électroniques, identifier les titulaires et délivrer des certificats d'identité est protégé de manière à ce que:

(a) l'accès est limité, logiquement et physiquement, aux rôles et applications strictement nécessaires;

(b) le matériel de codage n'est jamais stocké en texte brut sur un support de stockage permanent;

(c) le matériel de codage est protégé par l'utilisation d'un module matériel cryptographique doté de mécanismes de sécurité actifs qui neutralisent les tentatives physiques et logiques de compromettre le matériel de codage;

(d) les mécanismes de sécurité pour la protection du matériel de codage sont transparents et fondés sur des normes reconnues et bien établies; et

(e) **Niveaux 3 et 4 :** Les données d'activation pour la protection du matériel de codage sont gérées par un contrôle multi-personnes.

K4.4 Les émetteurs disposent de procédures documentées pour garantir que le niveau de protection requis dans l'environnement informatique concerné peut être maintenu au fil du temps et en liaison avec les changements, y compris des évaluations régulières de la vulnérabilité et une préparation appropriée pour faire face à l'évolution des niveaux de risque et aux incidents qui se produisent.

5. Demande, identification et enregistrement

Informations sur les conditions

K5.1 Les émetteurs d'identités électroniques suédoises doivent fournir des informations sur les contrats, les modalités et conditions, ainsi que des informations connexes et toute restriction relative à l'utilisation du service, aux utilisateurs connectés, aux prestataires de services électroniques et à d'autres personnes susceptibles de recourir au service de l'émetteur.

K5.2 L'émetteur d'identités électroniques suédoises fait clairement référence aux modalités et conditions et conçoit les procédures de manière à ce que les modalités et conditions soient fournies au demandeur dans le cadre du processus d'émission.

K5.3 Les émetteurs d'identités électroniques suédoises fournissent une déclaration de l'émetteur qui comprend:

(a) l'identité et les coordonnées de l'émetteur;

(b) une brève description des services et solutions fournis par l'émetteur, y compris les méthodes appliquées pour l'application, l'émission et le blocage;

(c) les conditions associées au service fourni, y compris les obligations de l'utilisateur de protéger son identité électronique, les obligations et responsabilités de l'émetteur, les garanties données et la disponibilité promise;

(d) des informations sur le traitement des données à caractère personnel et sur la manière dont il est réalisé; et

(e) les modalités de modification des modalités ou autres conditions du service fourni, y compris les mesures à prendre pour interrompre le service de manière contrôlée.

K5.4 **Niveaux 3 et 4:** À la demande de l'Agence pour l'administration numérique (DIGG) ou d'une autre partie contractante qui s'appuie sur les services fournis par l'émetteur, les émetteurs d'identités électroniques suédoises fournissent des informations sur la manière dont l'entreprise est détenue et gérée.

K5.5 L'émetteur d'identités électroniques suédoises qui cesse ses activités doit suivre un plan préétabli de cessation du service. Le plan comprend l'information de tous les utilisateurs du service et de la DIGG. L'émetteur doit en outre tenir à disposition les documents archivés conformément aux points K2.7 et K2.8 après la cessation.

Demande

K5.6 Une identité électronique suédoise ne peut être délivrée qu'à la demande du demandeur ou dans le cadre d'une autre procédure d'acceptation équivalente, et uniquement après que le demandeur a été informé des conditions dans lesquelles elle est délivrée et de la responsabilité qui lui incombera.

Toutefois, la délivrance d'une identité électronique qui remplace ou complète un document d'identité électronique valide ou récemment bloqué précédemment délivré par le même émetteur peut avoir lieu sans procédure de demande préalable.

K5.7 Une demande d'identité électronique suédoise doit être liée à un numéro d'identité personnel ou à un numéro de coordination, ainsi qu'aux informations qui sont autrement nécessaires à l'émetteur pour fournir cette identité électronique.

Détermination de l'identité du demandeur

K5.8 Les émetteurs d'identités électroniques suédoises doivent vérifier que les informations liées à la demande sont complètes et correspondent à des informations enregistrées dans un registre officiel.

K5.9 Lorsque les informations à vérifier dans un registre officiel sont marquées comme confidentielles («identité protégée»), les contrôles nécessaires peuvent être effectués par d'autres moyens équivalents.

K5.10 Identification du demandeur lors d'une visite en face à face:

Les émetteurs d'identité électroniques suédoises peuvent vérifier l'identité du demandeur lors d'une visite en face à face, de la même manière que lors de la délivrance d'un document d'identité standard.

K5.11 Identification à distance du demandeur dans la relationexistante :

Niveau 3 Les émetteurs d'identités électroniques suédoises qui ont déjà identifié le demandeur dans le cadre d'une relation impliquant des transactions économiquement ou juridiquement importantes, et lorsque le demandeur peut être identifié à distance par d'autres moyens fiables équivalents aux exigences de niveau 3 du label de qualité «Identité électronique suédoise», peuvent utiliser cette méthode pour établir l'identité du demandeur.

Niveau 4: Non applicable.

K5.12 Identification au moyen de l'identité électronique suédoise:

Un émetteur d'identité électronique suédoises peut identifier le demandeur à distance au moyen d'une identité électronique suédoise valide existante d'au moins le même niveau de garantie que celle à délivrer, s'il peut, sans obstacles contractuels, utiliser cette identification comme base pour délivrer une nouvelle identité électronique.

Niveau 4: La période de validité de la nouvelle identité électronique délivrée est limitée à une période ne dépassant pas la période de validité de l'identité électronique existante.

K5.13 Identification à distance du demandeur:

Niveau 2 Les émetteurs d'identités électroniques suédoises peuvent utiliser des enregistrements d'images fiables d'un document d'identité standard valide et de l'image faciale du demandeur comme base pour établir l'identité du demandeur à distance si la comparaison ne donne pas lieu à des doutes quant à la véritable identité du demandeur.

Niveau 3 Les émetteurs d'identités électroniques suédoises peuvent, au moyen d'une lecture sécurisée d'un document d'identité standard en cours de validité contenant des données biométriques stockées électroniquement, établir l'identité du demandeur à distance sur la base de ces données si les données biométriques correspondantes de la personne à identifier peuvent être collectées de manière suffisamment sûre pour qu'une comparaison puisse être effectuée avec une fiabilité équivalente à celle d'une visite en face à face, et lorsque la comparaison ne suscite pas de doutes quant à la véritable identité du demandeur.

Niveau 4: Non applicable.

Enregistrement

K5.14 Les émetteurs d'identités électroniques suédoises tiennent, en tenant compte des règles applicables en matière de protection des données à caractère personnel, un registre des utilisateurs connectés et des documents d'identité électronique attribués, et tiennent ce registre à jour.

6. Délivrance et blocage de l’identité électronique

Conception des moyens techniques

K6.1 Moyens techniques:

Niveaux 2 et 3: Les moyens techniques d'identification électronique au moyen du label de qualité «Identité électronique suédoise» doivent être conçus selon un principe à deux facteurs, selon lequel une partie consiste en des informations stockées électroniquement que l'utilisateur doit détenir, et l'autre partie consiste en ce que l'utilisateur doit utiliser pour activer l'identité électronique.

Niveau 4: Les moyens techniques d'identification électronique au moyen de l'identité électronique portant le label de qualité «Identité électronique suédoise» doivent être conçus selon un principe à deux facteurs, selon lequel une partie consiste en un module de sécurité personnel que l'utilisateur doit posséder, et l'autre partie consiste en ce que l'utilisateur doit utiliser pour activer le module de sécurité.

K6.2 Le mécanisme d'activation et le code personnalisé sont conçus de telle sorte qu'il est peu probable que des tiers enfreignent la protection, même par des moyens mécaniques.

Niveaux 3 et 4: La protection comprend des mécanismes visant à empêcher la copie et la manipulation du document d'identité électronique.

K6.3 Les utilisateurs de l'identité électronique portant le label de qualité «Identité électronique suédoise» doivent pouvoir, de leur propre initiative, pendant la période de validité de l'identité électronique, gratuitement et sans inconvénient majeur, échanger ou demander un nouveau code personnel et, grâce à des conseils ou à la production automatique, être aidés à respecter les exigences du point K6.2.

Si l'identité électronique est conçue de telle sorte qu'un code personnalisé ne peut pas être échangé, l'utilisateur devrait plutôt, dans les mêmes conditions, être en mesure d'obtenir rapidement une nouvelle identité électronique avec un nouveau code personnalisé qui remplace la précédente via une procédure de blocage.

K6.4 Les émetteurs d'identités électroniques suédoises veillent à ce que les données enregistrées pour l'identification électronique des titulaires représentent de manière unique le demandeur et soient attribuées à la personne en question lors de la délivrance du document d'identité électronique.

K6.5 La durée de validité des identités électroniques délivrées est limitée compte tenu des caractéristiques de sécurité du document d'identité électronique et des risques d'utilisation abusive. La durée maximale de validité de l'identité électronique est de cinq ans.

Fourniture d'un document d'identité électronique

K6.6 Prestation à distance :

Niveau 2 Un émetteur d'identités électroniques suédoises fournit le document d'identité électronique d'une manière qui confirme les coordonnées conservées dans le registre officiel ou les informations enregistrées dans le cadre de la procédure électronique conformément au point K5.13 Niveau 2.

Niveau 3 Un émetteur d'identités électroniques suédoises qui fournit une identité électronique au moyen d'une procédure électronique conforme aux points K5.11 Niveau 3, K5.12 Niveau 3 ou K5.13 Niveau 3 doit, lorsqu'elle vient d'être émise, s'assurer, séparément et indépendamment de la fourniture en termes de sécurité, que l'utilisateur est informé que ce document d'identité électronique a été remis, ou, par d'autres mesures, garantir un degré équivalent de contrôle pour alerter la personne du risque d'usurpation d'identité lié à la fourniture.

Niveau 4: L'émetteur d'identités électroniques suédoises qui fournit une identité électronique au moyen d'une procédure électronique conforme au point K5.12 Niveau 4 veille, lorsqu'elle vient d'être émise, séparément et indépendamment de la fourniture en termes de sécurité, à ce que l'utilisateur soit informé de la remise de ce document d'identité électronique.

K6.7 Prestation lors d'une visite en face-à-face:

Lors d'une visite en face à face et après un contrôle d'identité conformément au point K5.10, l'émetteur d'une identité électronique suédoise fournit le document d'identité électronique contre reçu signé et fournit en outre la partie que l'utilisateur doit utiliser pour activer l'identité électronique séparément et indépendamment de la fourniture du document d'identité électronique en termes de sécurité, sur la base des coordonnées conservées dans un registre officiel ou d'autres informations de crédibilité équivalente.

Service de blocage

K6.8 Les émetteurs d'identités électroniques suédoises doivent fournir un service de blocage offrant une bonne accessibilité pour que l'utilisateur puisse bloquer son identité électronique.

K6.9 Les émetteurs d'identités électroniques suédoises doivent traiter et exécuter rapidement et en toute sécurité les demandes de blocage, et prendre des mesures pour empêcher une utilisation abusive systématique du service de blocage ou d'autres actions intentionnelles qui conduisent au blocage généralisé des documents d'identité électronique, en veillant à ce que les identités électroniques des utilisateurs soient disponibles en cas de besoin

7. Vérification de l'identité électronique des titulaires

K7.1 Les émetteurs d'identités électroniques suédoises veillent à ce que, lors de la vérification de l'identité du titulaire, des contrôles fiables soient effectués sur l'authenticité et la validité du document d'identité électronique.

K7.2 Les émetteurs d'identités électroniques suédoises veillent à ce que des contrôles de sécurité techniques aient été mis en œuvre lors de la vérification de l'identité électronique des titulaires, de sorte qu'il soit peu probable que des tiers, en devinant, en écoutant, en relisant ou en manipulant le processus, puissent enfreindre les mécanismes de protection.

8. Délivrance de certificats d'identité

Les émetteurs d'identités électroniques suédoises qui fournissent un service de délivrance de certificats d'identité à des services électroniques payants se conforment également aux dispositions de la présente section.

K8.1 Les émetteurs d'identités électroniques suédoises veillent à ce que le service de délivrance des certificats d'identité soit bien accessible et à ce que la délivrance des certificats d'identité soit précédée d'une identification fiable conformément aux dispositions de la section 7.

Niveau 4: Les certificats contiennent une référence au matériel de codage cryptographique dont l'émetteur a vérifié qu'il était en la possession exclusive du titulaire.

K8.2 Les certificats d'identité présentés ne sont valables que le temps nécessaire pour permettre à l'utilisateur d'accéder au service d'identité électronique, et sont protégés de manière à ce que les informations ne puissent être lues que par le destinataire prévu et que l'authenticité des certificats puisse être vérifiée par les destinataires des certificats.

K8.3 Les émetteurs d'identités électroniques suédoises doivent, compte tenu des risques d'utilisation abusive du service de certification, limiter le délai dans lequel plusieurs certificats d'identité consécutifs peuvent être délivrés à un titulaire particulier avant que le titulaire ne soit réidentifié conformément aux dispositions de la section 7.