NORME INTERNATIONALE

ISO 11568-5

Première édition
1998-07-15

Banque — Gestion de clés (services aux particuliers) —

Partie 5:
Cycle de vie pour les systèmes cryptographiques à clé publique

Banking — Key management (retail) —
Part 5: Key life cycle for public key cryptosystems

(F)

Sommaire

Page

Organisation internationale de normalisation
Case postale 56 • CH-1211 Genève 20 • Suisse
Internet iso@ iso.ch

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 11568-5 a été élaborée par le comité technique ISO/TC 68, *Banque, valeurs mobilières et autres services financiers*, sous-comité SC 6, *Services financiers liés à la clientèle.*

L'ISO 11568 comprend les parties suivantes, présentées sous le titre général *Banque — Gestion de clés (services aux particuliers)*:

— *Partie 1: Introduction à la gestion de clés*

— *Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques*

— *Partie 3: Cycle de vie des clés pour les algorithmes cryptographiques symétriques*

— *Partie 4: Techniques de gestion de clés utilisant les systèmes cryptographiques à clé publique*

— *Partie 5: Cycle de vie des clés pour les systèmes cryptographiques à clé publique*

— *Partie 6: Schémas de gestion de clés*

Introduction

L'ISO 11568 décrit les procédures de gestion sécurisée de clés cryptographiques utilisées pour protéger les messages dans le cadre des services bancaires aux particuliers, par exemple les messages entre un acquéreur et accepteur de carte ou entre un acquéreur et un émetteur de carte. La gestion des clés employées dans un environnement de carte à circuit intégré (ICC) n'est pas couverte par l'ISO 11568.

Alors que la gestion de clés dans le cadre des services bancaires aux entreprises se caractérise par l'échange de clés dans un environnement relativement bien sécurisé, la présente norme prescrit les exigences de gestion de clés, applicables dans des environnements accessibles que sont les services bancaires aux particuliers tels que les autorisations de crédit et de débit aux points de vente / points de service et les transactions aux guichets automatiques de banques (GAB).

La présente partie de l'ISO 11568 décrit le cycle de vie des clés dans la gestion sécurisée des clés cryptographiques pour les systèmes cryptographiques à clé publique.

Un système cryptographique à clé publique utilise une clé publique et une clé privée. L'ensemble de ces deux clés est appelé paire de clés dans la présente partie de l'ISO 11568.

L'article 4 décrit les prescriptions générales de sécurité pour chaque étape du cycle de vie de ce type de paire de clés, en se basant sur les principes de gestion de clés, les services et les techniques décrits dans l'ISO 11568-1 et dans l'ISO 11568-4.

L'article 5 décrit les prescriptions relatives aux méthodes de mise en œuvre liées à ces spécifications générales de sécurité.

Le cycle de vie des clés comporte trois phases:

1) Pré-active: phase pendant laquelle la paire de clés est générée et peut être transférée.

2) Active: phase pendant laquelle la clé publique est distribuée à au moins une ou plusieurs parties pour une utilisation opérationnelle.

3) Post-active: phase pendant laquelle la clé publique d'une paire de clés est archivée et la clé privée d'une paire de clés est résiliée.

Le cycle de vie de la clé privée (S) et le cycle de vie de la clé publique (P) sont décrits dans les figures 1 et 2 respectivement. Ces figures décrivent la manière dont une opération effectuée sur une clé change son état.

Une clé est considérée comme un objet unique dont il peut exister plusieurs exemplaires en différents emplacements et sous diverses formes. Une distinction claire est faite entre les opérations suivantes:

— distribution de la clé publique à une partie en communication;

— transfert d'une paire de clés à son propriétaire dans une mise en œuvre où la partie n'est pas en mesure de générer des paires de clés;

et

— destruction d'un seul exemplaire de clé privée;

— suppression d'une clé privée d'un emplacement donné, impliquant la destruction de tous les exemplaires de cette clé à cet emplacement;

— résiliation d'une clé, impliquant la suppression de la clé de tous les emplacements.

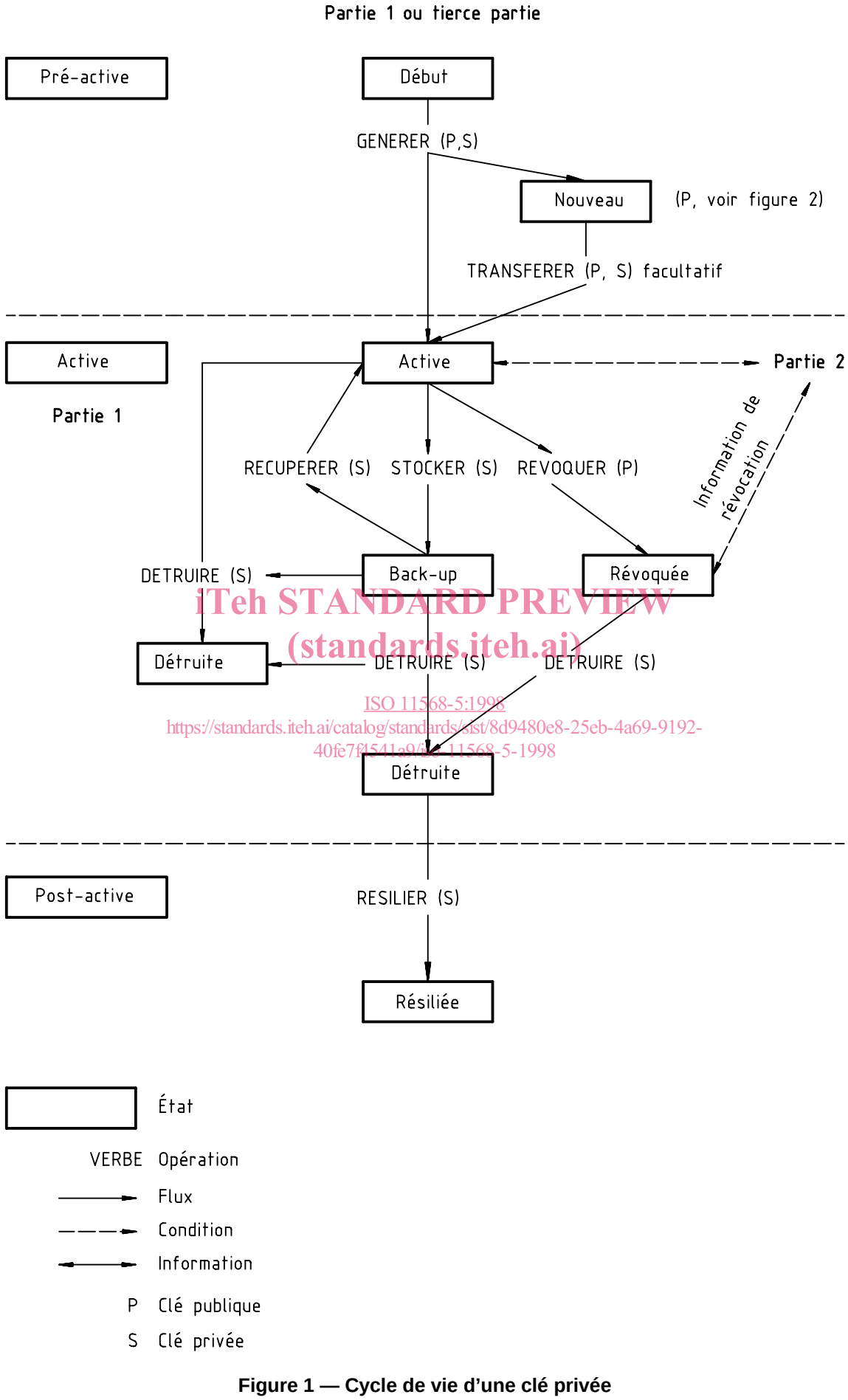

Figure 1 — Cycle de vie d'une clé privée

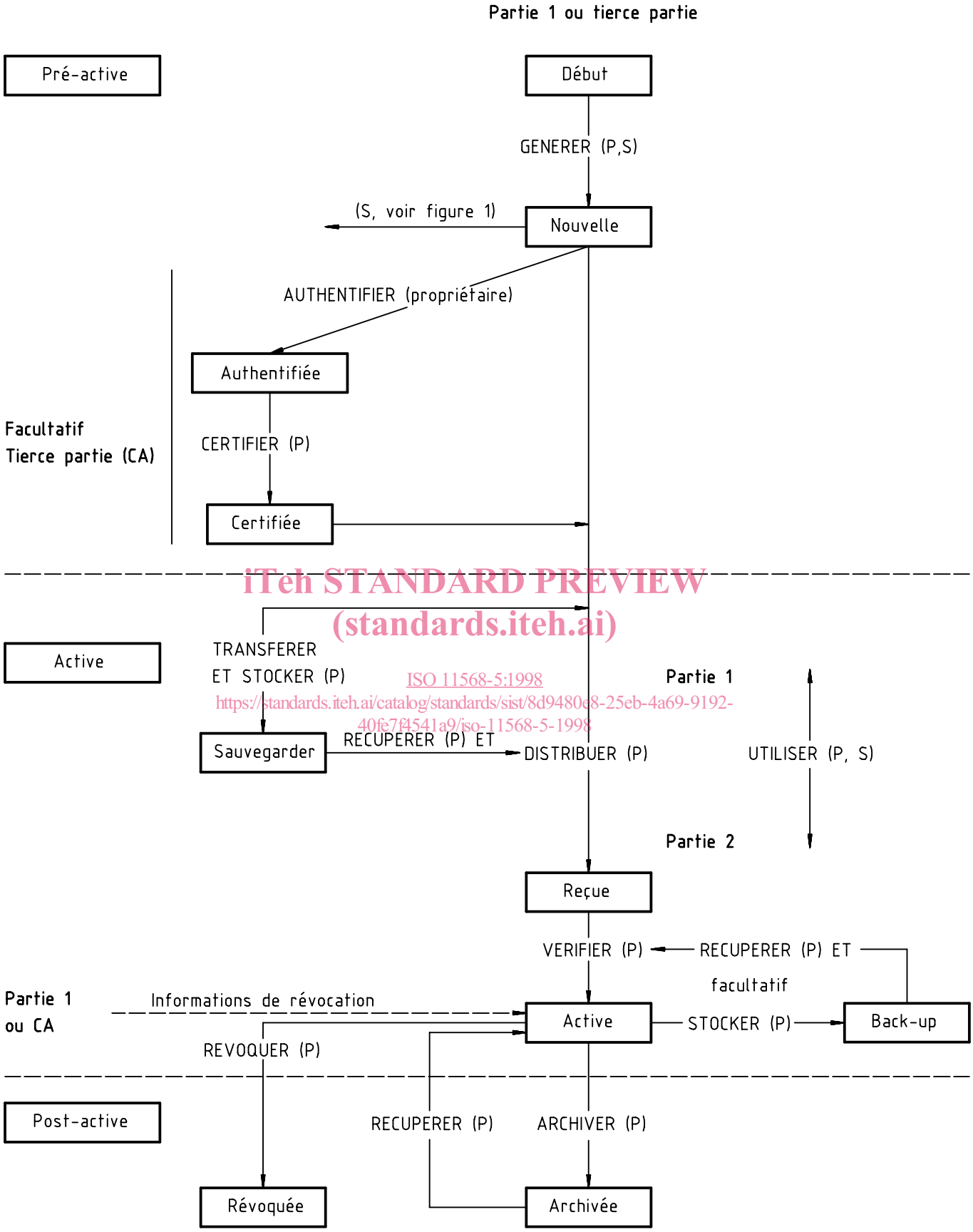

Figure 2 — Cycle de vie d'une clé publique

Banque — Gestion de clés (services aux particuliers) —

Partie 5:
Cycle de vie pour les systèmes cryptographiques à clé publique

1 Domaine d'application

La présente partie de l'ISO 11568 fixe les prescriptions de sécurité et les méthodes de mise en œuvre pour chaque étape du cycle de vie d'une clé, publique ou privée, appartenant à une paire de clés asymétrique, dans le cadre des services bancaires aux particuliers.

Elle est applicable à toute organisation responsable de la mise en œuvre de techniques basées sur les systèmes cryptographiques à clé publique pour la gestion des clés utilisées dans le cadre de la protection des données.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 11568. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 11568 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 8908:1993, *Banque et services financiers connexes — Vocabulaire et éléments de données.*

ISO 9564-1:—[1)], *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN.*

ISO 11568-1:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 1: Introduction à la gestion de clés.*

ISO 11568-2:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques.*

ISO 11568-3:1994, *Banque — Gestion de clés (services aux particuliers) — Partie 3: Cycle de vie des clés pour les algorithmes cryptographiques symétriques.*

ISO 11568-4: —[2)], *Banque — Gestion de clés (services aux particuliers) — Partie 4: Techniques de gestion de clés utilisant les systèmes cryptographiques à clé publique.*

ISO/CEI 11770-1:1996, *Technologies de l'information — Techniques de sécurité — Gestion des clés — Partie 1: Cadre général.*

---

1) À publier. (Révision de l'ISO 9564-1:1991)

2) À publier.

ISO/CEI 11770-3:— [2], *Technologies de l'information — Techniques de sécurité — Gestion des clés — Partie 3: Mécanismes utilisant des techniques asymétriques.*

ISO 13491-1:1998, *Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) — Partie 1: Concepts, prescriptions et méthodes d'évaluation.*

ISO 13491-2: — [2], *Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) — Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les systèmes de cartes à bande magnétique.*

3 Définitions

Pour les besoins de la présente partie de l'ISO 11568, les définitions données dans l'ISO 8908 ainsi que les suivantes s'appliquent.

3.1
générateur de paire de clés asymétrique
dispositif cryptographique sûr utilisé pour la génération de clés cryptographiques asymétriques

3.2
partie en communication
partie qui reçoit la clé publique pour la communication avec la partie propriétaire de la clé publique

3.3
communication indépendante
processus permettant à une entité de contre-vérifier l'exactitude de ocuments d'accréditation et de documents d'identification avant de produire un certificat (par exemple rappel téléphonique, identification visuelle, etc.)

4 Prescriptions générales

Toute opération effectuée sur une clé modifie son état. Cet article décrit les conditions nécessaires à l'obtention d'un état donné ou à l'exécution d'une opération donnée.

Les prescriptions qui s'appliquent à des étapes spécifiques du cycle de vie sont spécifiées dans les paragraphes qui suivent.

Il est à noter que les conditions qui suivent peuvent dépendre de la mise en œuvre de la génération des paires de clés. En particulier, les conditions diffèrent si la paire de clés est générée par une tierce partie générant des paires de clés asymétriques appartenant à un tiers, ou si le propriétaire génère et stocke sa paire de clés.

4.1 Génération de paire de clés asymétriques

La génération de paires de clés asymétriques est le processus par lequel une nouvelle paire de clés composée d'une clé privée et de la clé publique correspondante est générée pour utilisation dans un système cryptographique asymétrique spécifique. Il est possible que d'autres informations relatives aux clés asymétriques soient produites au cours de ce processus. Les données en entrée de ce processus peuvent avoir des valeurs prédéterminées.

Le processus de génération d'une paire de clés est effectué par ou au nom d'une seule partie. Cette dernière devient propriétaire de la paire de clés.

Chaque clé privée et chaque élément de clé privée doivent être générés de telle façon qu'il ne soit pas possible de prédire une clé privée quelconque, ni de déterminer que certaines clés privées ont une plus grande probabilité d'être générées que d'autres dans l'espace des clés possibles. Lorsque la situation s'y prête, le processus doit intégrer des valeurs aléatoires ou pseudo-aléatoires, selon l'algorithme cryptographique asymétrique.

---

[2] À publier.

Une paire de clés asymétriques doit être générée de manière à assurer la confidentialité de la clé privée et l'intégrité de la clé publique. Lors de la génération d'une paire de clés asymétriques pour un service de non-répudiation, l'intégrité de la clé publique et la confidentialité de la clé privée doivent être démontrables à une tierce partie.

La clé privée ne doit pas exister sous une forme compréhensible par l'homme, pour qui que ce soit, et ce à aucun moment du processus de génération.

Si la paire de clés est générée par un système qui ne l'utilisera pas:

— la paire de clés et tous les éléments secrets des valeurs de départ correspondants doivent être détruits immédiatement après le transfert;

— en outre, l'intégrité de la clé privée doit être assurée.

Il convient que les paires de clés asymétriques, une fois générées, aient une date d'expiration qui détermine leur cycle de vie.

Le processus de génération doit être conforme aux prescriptions décrites dans l'ISO 11658-4.

NOTE Il convient d'ajouter des informations supplémentaires à la clé publique, notamment l'identification du propriétaire, le type de clé et la date d'expiration, de manière à éviter la répudiation par substitution de la clé publique.

4.2 Authenticité avant utilisation

L'authenticité de la clé publique doit être garantie avant son utilisation et tout au long de sa vie. Cette garantie doit être assurée par la certification.

4.3 Certification de clé publique

La certification de clé publique est le processus par lequel une tierce partie de confiance, désigné sous l'appellation d'Autorité de Certification, établit la preuve qui relie une clé publique, ainsi que d'autres informations pertinentes, à son propriétaire.

La certification de clé et l'Autorité de Certification sont décrites dans l'ISO 11568-4.

La clé publique de l'Autorité de Certification, utilisée pour vérifier la clé publique d'un certificat, doit être transférée au propriétaire de la paire de clés de manière authentifiée.

4.4 Transfert de paire de clés asymétriques

Le transfert de paire de clés asymétriques est le processus par lequel la paire de clés et le certificat de la clé publique sont transmis au propriétaire de la paire de clés. Ce processus intervient lorsque le propriétaire n'a pas la capacité de générer sa paire de clés.

L'identité du propriétaire doit être authentifiée avant que ce dernier puisse recevoir sa paire de clés.

4.4.1 Transfert de clé privée

Une clé privée ne doit être transférée que sous les formes suivantes, comme défini dans le présent paragraphe:

— clé en texte clair;

— éléments de clé;

— clé chiffrée.