NORME INTERNATIONALE

ISO 11568-3

First édition
1994-12-01

Banque — Gestion de clés (services aux particuliers) —

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994

Banking — Key management (retail) —
Part 3: Key life cycle for symmetric ciphers

Numéro de référence
ISO 11568-3:1994(F)

Sommaire

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994

© ISO 1994
Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse

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 11568-3 a été élaborée par le comité technique ISO/TC 68 *Banque et services financiers liés aux opérations bancaires,* sous-comité SC 6, *Cartes de transactions financières, supports et opérations relatifs à celles-ci.*

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

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

ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-10f6a6220dff/iso-11568-3-1994

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

— *Partie 4 : Techniques de gestion de clés pour les algorithmes cryptographiques asymétriques*

— *Partie 5 : Cycle de vie des clés pour les algorithmes cryptographiques asymétriques*

— *Partie 6 : Schémas de gestion de clés*

Introduction

L'ISO 11568 fait partie d'un ensemble de normes décrivant des procédures destinées à sécuriser la gestion de clés cryptographiques pour protéger des messages dans un environnement de services bancaires aux particuliers, tels que les messages entre un acquéreur et un accepteur de cartes, ou un acquéreur et un émetteur de cartes. La gestion de clés employées dans le cadre des cartes à circuit intégré n'est pas traitée dans 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 de relativement haute sécurité, la présente partie de l'ISO 11568 traite des prescriptions relatives à la gestion de clés qui sont applicables dans les domaines accessibles qui sont ceux des services bancaires aux particuliers. De tels services sont les autorisations de crédit et de débit aux points de vente/points de service (TPE) et les transactions aux guichets automatiques de banques (GAB).

La présente partie de l'ISO 11568 décrit le cycle de vie de clés gérées dans un environnement sûr pour des algorithmes cryptographiques symétriques. Elle établit pour ces clés les prescriptions et les méthodes de mise en œuvre pour chaque étape de leur vie, en utilisant les principes, services et techniques de gestion de clés décrits dans l'ISO 11568-1 et l'ISO 11568-2.

Le cycle de vie consiste en trois phases :

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) Préparation : phase pendant laquelle la clé est générée.

b) Utilisation : phase pendant laquelle la clé est distribuée entre les parties en communication pour une utilisation opérationnelle.

ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-10084922001/iso-11568-3-1994

Dans un processus où les deux parties en communication participent à la génération d'une nouvelle clé, la génération et la distribution sont étroitement liées.

Certains schémas de gestion de clé sont conçus pour transformer automatiquement des clés pendant leur utilisation opérationnelle.

a) Désactivation : phase pendant laquelle une clé est archivée ou résiliée.

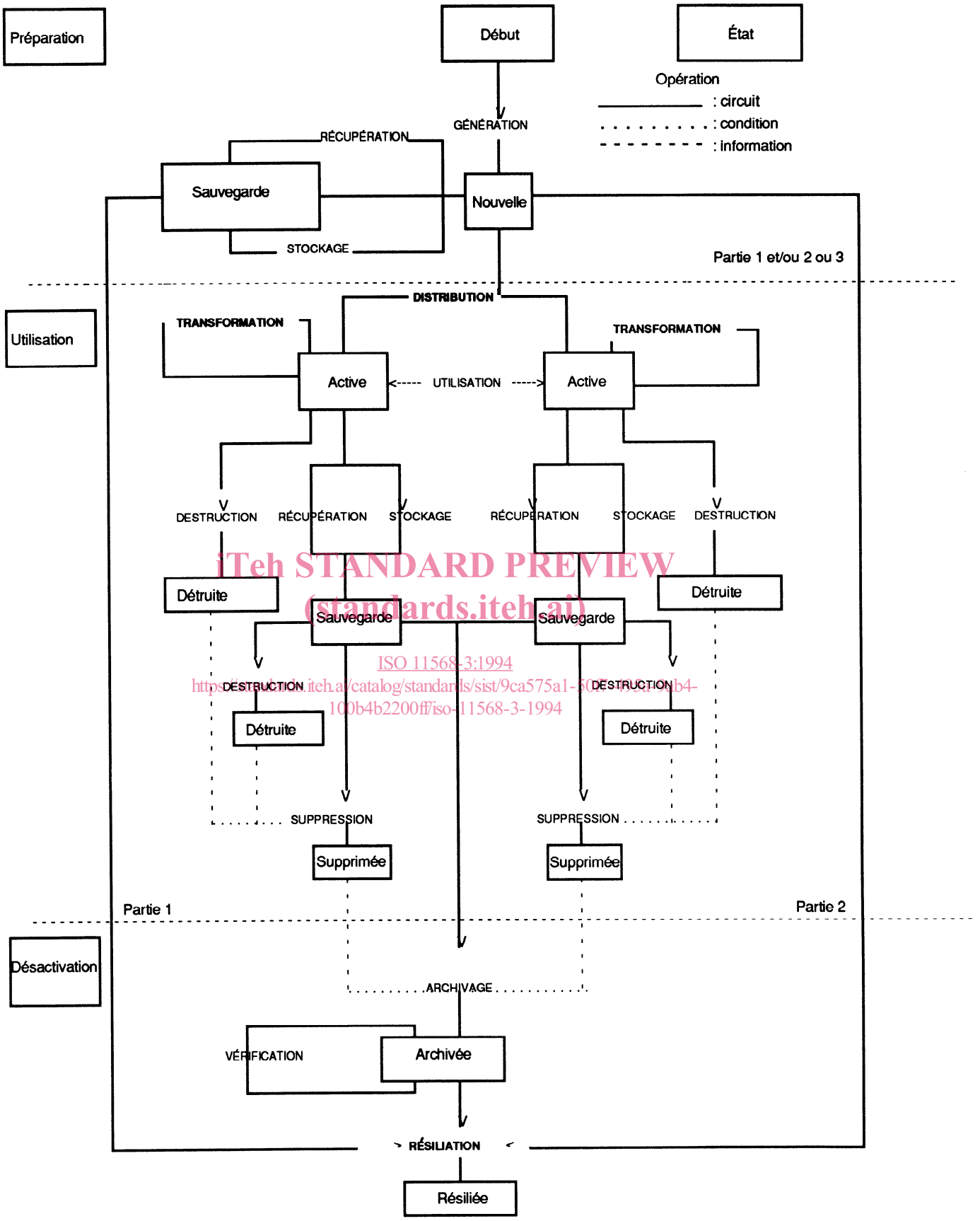
La figure 0.1 illustre schématiquement le cycle de vie de la clé. Elle montre comment l'état d'une clé change suite à une opération donnée.

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 :

— destruction d'un exemplaire d'une clé ;

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

— résiliation d'une clé, ce qui implique la suppression de la clé de tous les emplacements.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994

Figure 0.1 — Cycle de vie de la clé

Page blanche

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994

Banque — Gestion de clés (services aux particuliers) —

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

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, dans le cadre des services bancaires aux particuliers.

Le cycle de vie d'une clé s'applique à toutes les clés, quel que soit leur niveau hiérarchique.

Il est applicable à toute organisation responsable de la protection de clés utilisées dans un algorithme cryptographique symétrique.

La présente partie de l'ISO 11568 est applicable aux institutions responsables de la mise en œuvre de techniques de gestion de clés utilisées pour protéger des données dans des transactions effectuées à partir de cartes bancaires.

2 Références normatives

Les normes suivantes contiennent des dipositions 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 liés aux opérations bancaires — Vocabulaire et éléments de données.*

ISO 9564-1:1991, *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.*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-30f1-495a-9ab4-100b4b2200ff/iso-11568-3-1994

3 Définitions

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

3.1 double contrôle : Intervention de deux entités distinctes ou plus (généralement des personnes), opérant de concert pour protéger des fonctions ou des informations sensibles, aucun individu isolé ne pouvant accéder aux éléments ni les utiliser, par exemple une clé de chiffrement.

3.2 élément de clé : L'un d'au moins deux paramètres ayant les caractéristiques (par exemple : format, aspect aléatoire) d'une clé de chiffrement et qui est combiné à un ou plusieurs paramètres semblables pour former une clé de chiffrement.

3.3 courrier de clé : Enveloppe conçue pour transmettre un élément de clé vers une personne autorisée.

3.4 connaissance répartie : Contexte dans lequel au moins deux entités se partagent en les gardant secrets les éléments d'une clé unique qui, pris isolément, ne permettent pas de déduire la clé de chiffrement de leur combinaison.

3.5 dispositif cryptographique sûr : Dispositif offrant un stockage sûr pour des informations secrètes telles que des clés et fournissant des services de sécurité basés sur ces informations secrètes.

4 Prescriptions

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

4.1 Génération de clé

Chaque clé ou élément de clé doit être généré par un processus aléatoire ou pseudo-aléatoire, de telle façon qu'il ne soit pas possible de prévoir une clé quelconque, ni de déterminer que certaines clés ont une plus grande probabilité d'être générées que d'autre dans l'espace des clés possibles.

La découverte d'une clé secrète ne doit pas permettre d'obtenir d'information utile concernant toute autre clé secrète, excepté dans les cas suivants : les variantes de clé, les transformations non réversibles d'une clé, les clés chiffrées sous une clé ou les clés dérivées à partir d'une clé.

4.2 Stockage de clé

La finalité d'un stockage sûr est de protéger les clés contre une divulgation et une substitution non autorisées, et d'assurer une séparation des clés.

4.2.1 Formes permises

Une clé ne doit exister que sous les formes suivantes comme défini dans ce paragraphe :

— clé en texte clair ;

— éléments de clé ;

— clé chiffrée.

4.2.1.1 Clé en texte clair

Une ou des clés secrètes en texte clair dont la divulgation affecterait plusieurs parties ne doivent exister qu'à l'intérieur d'un dispositif cryptographique sûr.

Une ou des clés secrètes en texte clair dont la divulgation affecterait seulement une partie ne doivent exister qu'à l'intérieur d'un dispositif cryptographique sûr ou dans un environnement physiquement sûr exploité par ou pour le compte de cette partie.

4.2.1.2 Éléments de clé

Une clé existant sous la forme d'au moins deux éléments de clé séparés doit être protégée par les techniques de séparation des connaissances et de double contrôle.

Chaque bit de la clé résultante doit être une fonction de tous les éléments de clé.

Lorsque la même valeur de clé doit être créée en plus d'une occasion, plusieurs jeux d'éléments de clés devraient être utilisés. Dans ce cas, les valeurs de chacun de ces éléments de clé ne doivent pas être les mêmes, sauf par hasard.

Un élément de clé ne doit être accessible qu'à la personne ou au groupe de personnes habilité pour la durée minimale nécessaire.

Si un élément de clé existe sous une forme compréhensible par l'homme (par exemple imprimé en clair dans un courrier) il ne doit être connu que par une seule personne, autorisée à un moment donné, et seulement pour la durée nécessaire à l'entrée de l'élément de clé dans un dispositif cryptographique sûr.

Une personne ayant accès à un élément de la clé ne doit pas avoir accès à tout autre élément de cette clé.

Les éléments de clé doivent être stockés de telle sorte qu'un accès non autorisé ait une forte probabilité d'être détecté.

Si des éléments de clé sont stockés sous une forme chiffrée, toutes les prescriptions relatives aux clés chiffrées doivent s'appliquer.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9ca575a1-50f7-495a-9ab4-100b4b2200ff/iso-11568-3-1994

4.2.1.3 Clé chiffrée

Le chiffrement d'une clé par une clé de chiffrement de clé doit s'effectuer à l'intérieur d'un dispositif cryptographique sûr.

4.2.2 Protection contre la substitution

La substitution non autorisée de clés stockées doit être empêchée par au moins l'un des moyens suivants :

a) obstacle physique et procédural contre un accès non autorisé à l'espace de stockage des clés ;

b) stockage d'une clé chiffrée sous la forme d'une fonction de son utilisation prévue ;

c) impossibilité de connaître à la fois une valeur en clair et le cryptogramme correspondant au chiffrement de cette valeur sous une clé de chiffrement de clé.

4.2.3 Dispositions pour assurer la séparation de clés

Afin d'assurer qu'une clé stockée n'est utilisable que dans son but prévu, la séparation de clés stockées doit être réalisée par au moins l'un des moyens suivants :

a) séparation physique des clés stockées sous la forme d'une fonction de son utilisation prévue ;

b) stockage d'une clé chiffrée sous une clé de chiffrement de clé dédiée au chiffrement d'un type particulier de clé ;

c) modification ou ajout d'information à une clé, sous la forme d'une fonction de son utilisation prévue, préalablement à son chiffrement pour le stockage.

4.3 Restauration de clé à partir d'une sauvegarde

La sauvegarde de clé est le stockage d'une copie dans le but d'une réinstallation suite à la destruction accidentelle d'une clé dont la divulgation n'est pas suspectée.

Les prescriptions relatives à la restauration de clé à partir d'une sauvegarde sont identiques à celles relatives à la distribution et au chargement de clé, décrites en 4.4.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.4 Distribution et chargement de clé

Un dispositif cryptographique sûr devrait rester dans un environnement physiquement sûr jusqu'à ce qu'il soit chargé par au moins une clé.

ISO 11568-3:1994
https://standards.iteh.ai/catalog/standards/sist/9...
100b4b2200ff/iso-11568-3-1994

4.4.1 Clés en texte clair

Les prescriptions générales relatives à la distribution et au chargement de clés en texte clair sont les suivantes :

a) le processus de distribution de clé ne doit divulguer aucune partie d'une clé en texte clair ;

b) une clé en texte clair ne doit être chargée dans un dispositif cryptographique que lorsqu'il est certain que celui-ci n'a subi aucune agression préalable susceptible de conduire à une divulgation de clés ou de données sensibles ;

c) une clé en texte clair ne doit être transférée entre des dispositifs cryptographiques sûrs que lorsqu'il est certain qu'il n'existe aucune écoute clandestine risquant de divulguer les clés transmises ;

d) un dispositif cryptographique sûr ne doit transférer une clé en texte clair qu'après avoir identifié au moins deux personnes autorisées, par exemple au moyen de mots de passe ;

e) lorsqu'un dispositif est utilisé pour transférer des clés entre le dispositif cryptographique qui les a générées et le dispositif cryptographique qui les utilisera, ce doit être un dispositif cryptographique sûr. Après chargement de la clé dans le dispositif cible, le dispositif de transfert de clés ne doit pas conserver d'informations qui pourraient entraîner la découverte de cette clé.

4.4.2 Éléments de clé

Les prescriptions générales relatives à la distribution et au chargement d'éléments de clés sont les suivantes :

a) le processus de distribution d'éléments de clé ne doit divulguer aucune partie d'un élément de clé à une personne non autorisée ;

b) un élément de clé ne doit être chargé dans un dispositif cryptographique que lorsqu'il est certain que celui-ci n'a subi aucune agression préalable susceptible de conduire à une divulgation de clés ou de données sensibles ;

c) un élément de clé ne doit être transféré dans un dispositif cryptographique que lorsqu'il est certain qu'il n'existe aucune écoute clandestine risquant de divulguer les éléments de clés transmis ;

d) le processus de distribution et de chargement de clé doit être effectué selon les principes du double contrôle et de la connaissance répartie.

4.4.3 Clés chiffrées

Les clés chiffrées peuvent être distribuées et chargées de manière électronique via un canal de communication.

Le processus de distribution de clés chiffrées doit être protégé contre la substitution et la modification de clé.

4.5 Utilisation de clé

L'utilisation non autorisée de clé doit être proscrite. En conséquence

— une clé ne doit être utilisée que pour une seule fonction. Cependant, une variante de clé peut être utilisée pour une fonction différente de celle de la clé d'origine ;

— une clé doit être utilisée uniquement pour sa fonction prévue à ses emplacements prévus ;

— une clé ne doit exister que dans le minimum d'emplacements nécessaires à une exploitation efficace. Toute clé qui existe dans un dispositif générant des transactions ne doit pas exister dans aucun autre dispositif de ce type ;

— une clé doit cesser d'être utilisée lorsque sa découverte est connue ou suspectée.