NORME INTERNATIONALE

ISO/CEI 10181-4

Première édition
1997-04-01

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité dans les systèmes ouverts: Non-répudiation

Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework

Numéro de référence
ISO/CEI 10181-4:1997(F)

Sommaire

		Page
1	Domaine d'application	1
2	Références normatives	2
	2.1 Recommandations I Normes internationales identiques	2
	2.2 Paires de Recommandations I Normes internationales équivalentes par leur contenu technique	2
3	Définitions	2
	3.1 Définitions relatives au modèle de référence de base	2
	3.2 Définitions relatives à l'architecture de sécurité	2
	3.3 Définitions relatives à l'aperçu général des cadres de sécurité	3
	3.4 Définitions supplémentaires	3
4	Abréviations	4
5	Considérations générales sur la non-répudiation	4
	5.1 Concepts de base de la non-répudiation	4
	5.2 Rôles d'un tiers de confiance	5
	5.3 Phases de la non-répudiation	5
	5.4 Formes du service de non-répudiation	7
	5.5 Exemples de preuve OSI de non-répudiation	8
6	Politiques de non-répudiation	8
7	Informations et fonctionnalités	9
	7.1 Informations	9
	7.2 Fonctionnalités de non-répudiation	10
8	Mécanismes de non-répudiation	12
	8.1 Non-répudiation au moyen d'un jeton de sécurité de tiers de confiance (enveloppe sécurisée)	12
	8.2 Non-répudiation au moyen de jetons de sécurité et de modules inviolables	13
	8.3 Non-répudiation au moyen d'une signature numérique	13
	8.4 Non-répudiation au moyen de pointages temporels	14
	8.5 Non-répudiation au moyen d'un tiers de confiance en ligne	14
	8.6 Non-répudiation au moyen d'un notaire	14
	8.7 Menaces pouvant affecter la non-répudiation	14
9	Interactions avec d'autres services et mécanismes de sécurité	16
	9.1 Authentification	16
	9.2 Contrôle d'accès	16
	9.3 Confidentialité	16
	9.4 Intégrité	17
	9.5 Audit	17
	9.6 Gestion des clés	17

Version française tirée en 1998

Imprimé en Suisse

Annexe A – Non-répudiation dans le modèle de référence de base OSI 18
A.1 Non-répudiation avec preuve d'origine 18
A.2 Non-répudiation avec preuve de remise 18
Annexe B – Description des fonctionnalités de non-répudiation 19
Annexe C – Non-répudiation dans les systèmes en mode différé 20
Annexe D – Reprise dans un service de non-répudiation 21
Annexe E – Interaction avec l'Annuaire 23
Annexe F – Bibliographie 24

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10181-4 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.813.

L'ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité dans les systèmes ouverts*:

— *Partie 1: Présentation*

— *Partie 2: Cadre général d'authentification*

— *Partie 3: Contrôle d'accès*

— *Partie 4: Non-répudiation*

— *Partie 5: Confidentialité*

— *Partie 6: Intégrité*

— *Partie 7: Audit de sécurité et alarme*

Les annexes A à F de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

Introduction

Le service de non-répudiation a pour objet de collecter, de conserver, de diffuser et de valider des preuves irréfutables concernant un événement ou une action revendiqué afin de résoudre des litiges concernant la réalité ou la non-réalité de cet événement ou de cette action. Le service de non-répudiation peut être appliqué dans un certain nombre de contextes et de situations différents. Ce service peut s'appliquer à la production de données, à la conservation de données ou à la transmission de données. La non-répudiation implique la production de preuves qui peuvent être utilisées pour prouver qu'un certain type d'événement ou d'action a eu lieu, de manière que cet événement ou cette action ne puisse être répudié ultérieurement.

Dans un environnement d'interconnexion OSI (voir la Rec. X.800 du CCITT et l'ISO 7498-2), le service de non-répudiation a deux formes:

- non-répudiation avec preuve d'origine, qui est utilisée pour contrer un faux déni d'envoi des données ou de leur contenu par leur expéditeur;
- non-répudiation avec preuve de remise, qui est utilisée pour contrer un faux déni de réception des données ou de leur contenu (c'est-à-dire ce que les données représentent) par leur destinataire.

Les applications qui font usage des protocoles OSI peuvent nécessiter d'autres formes du service de non-répudiation qui soient spécifiques de classes d'application particulières. Par exemple, la messagerie MHS (Rec. UIT-T X.402 | ISO 10021-2) définit la non-répudiation du service de soumission, tandis que le système de messagerie EDI (voir la Recommandation X.435) définit la non-répudiation des services de consultation et des services de transfert.

Les concepts contenus dans le présent cadre ne sont pas limités aux communications OSI mais peuvent être interprétés plus largement afin d'inclure des usages tels que la création et la conservation des données pour usage ultérieur.

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture d'un service de non-répudiation.

Ce cadre:

- développe les concepts des services de non-répudiation qui sont décrits dans la Rec. X.800 du CCITT et l'ISO 7498-2; il décrit la façon dont ces concepts peuvent être appliqués aux systèmes ouverts;
- décrit les variantes de fourniture de ces services;
- explique la relation de ces services avec d'autres services de sécurité.

Les services de non-répudiation peuvent nécessiter:

- des arbitres qui régleront les litiges qui peuvent apparaître à la suite d'événements ou d'actions répudiés;
- des tiers de confiance qui garantiront l'authenticité et l'intégrité des données à utiliser pour la vérification des preuves.

This page intentionally left blank

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ DANS LES SYSTÈMES OUVERTS: NON-RÉPUDIATION

1 Domaine d'application

La présente Recommandation | Norme internationale traite de l'application des services de sécurité dans un environnement de systèmes ouverts, où le terme «systèmes ouverts» est considéré comme visant des domaines tels que les bases de données, les applications réparties, le traitement réparti ouvert et l'interconnexion OSI. Les cadres de sécurité concernent la définition des moyens d'assurer la protection des systèmes et des objets contenus dans ces systèmes. Ils concernent également les interactions entre ces systèmes. Les cadres de sécurité ne concernent pas la méthode de construction des systèmes ou des mécanismes.

Les cadres de sécurité traitent aussi bien des éléments de données et des séquences d'opérations (mais non des éléments de protocoles) qui sont utilisés pour obtenir des services de sécurité spécifiques. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes ainsi qu'aux données échangées entre systèmes et aux données gérées par les systèmes.

La présente Recommandation | Norme internationale:

- définit les concepts fondamentaux de la non-répudiation;
- définit les services généraux de non-répudiation;
- identifie les mécanismes permettant de fournir les services de non-répudiation;
- identifie les prescriptions générales de gestion pour services et mécanismes de non-répudiation.

Comme avec d'autres services de sécurité, la non-répudiation ne peut être fournie que dans le cadre d'une politique de sécurité définie pour une application particulière. Les définitions des politiques de sécurité sont hors du domaine d'application de la présente Recommandation | Norme internationale.

Le domaine d'application de la présente Recommandation | Norme internationale ne comprend pas la spécification des détails relatifs aux échanges protocolaires qui doivent être effectués afin d'utiliser le service de non-répudiation.

La présente Recommandation | Norme internationale ne décrit pas en détail les mécanismes particuliers que l'on peut utiliser pour prendre en charge le service de non-répudiation; elle ne donne pas non plus de détails concernant les services et protocoles de gestion de sécurité qui sont utilisés à l'appui du service de non-répudiation.

Certaines des procédures décrites dans le présent cadre réalisent la sécurité en appliquant des techniques cryptographiques. Ce cadre ne dépend pas de l'utilisation d'un algorithme cryptographique ou non cryptographique particulier, ni de techniques cryptographiques particulières (c'est-à-dire symétriques ou asymétriques) bien que certaines classes de mécanismes de non-répudiation puissent dépendre de propriétés algorithmiques particulières. En fait, il est probable qu'en pratique un certain nombre d'algorithmes différents seront utilisés. Deux entités souhaitant utiliser des données protégées par cryptographie doivent toujours prendre en charge le même algorithme cryptographique.

[NOTE – Bien que l'ISO ne normalise pas les algorithmes cryptographiques, cette organisation normalise, dans l'ISO/CEI 9979, les procédures utilisées pour les enregistrer.]

Un certain nombre de types de norme différents peuvent utiliser ce cadre, à savoir:

1) les normes qui intègrent le concept de non-répudiation;
2) les normes qui spécifient des services abstraits comportant la non-répudiation;
3) les normes qui spécifient les utilisateurs d'un service de non-répudiation;
4) les normes qui spécifient les moyens de fournir le service de non-répudiation dans une architecture de système ouvert;
5) les normes qui spécifient des mécanismes de non-répudiation.

De telles normes peuvent utiliser ce cadre comme suit:

- les normes de type 1), 2), 3), 4) ou 5) peuvent utiliser la terminologie de ce cadre;
- les normes de type 2), 3), 4) ou 5) peuvent utiliser les fonctionnalités définies dans l'article 7 de ce cadre;
- les normes de type 5) peuvent être fondées sur les classes de mécanisme définies dans l'article 8 de ce cadre.

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*
- Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*
- ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

3 Définitions

3.1 Définitions relatives au modèle de référence de base

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. UIT-T X.200 | ISO/CEI 7498-1 et fait usage du terme suivant, qui y est défini:

entité (N).

3.2 Définitions relatives à l'architecture de sécurité

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. X.800 du CCITT et l'ISO 7498-2 et fait usage des termes suivants, qui y sont définis:

- contrôle d'accès;
- audit (de sécurité);
- authentification;
- voie;
- valeur de contrôle cryptographique;
- cryptographie;
- intégrité (des données);
- authentification de l'origine des données;
- déchiffrement;

- signature (numérique);
- chiffrement;
- clé;
- gestion de clés;
- notarisation;
- répudiation;
- journal d'audit de sécurité; journal d'audit; journal;
- menace.

3.3 Définitions relatives à l'aperçu général des cadres de sécurité

La présente Recommandation | Norme internationale est fondée sur les concepts développés dans la Rec. UIT-T X.810 | ISO/CEI 10181-1 et fait usage des termes suivants, qui y sont définis:

- autorité de certification;
- empreinte numérique;
- fonction d'adressage dispersé;
- fonction à sens unique;
- clé privée;
- clé publique;
- certificat de liste de révocation;
- cachet;
- cacheté;
- clé secrète;
- certificat de sécurité;
- domaine de sécurité;
- jeton de sécurité;
- tiers de confiance.

3.4 Définitions supplémentaires

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.4.1 preuve compromise: preuve, qui avait été satisfaisante à un moment donné, mais en laquelle le tiers de confiance ou l'arbitre n'a plus confiance.

3.4.2 contresignature: signature numérique ajoutée à une unité de données déjà signée par une entité différente (par exemple un tiers habilité).

3.4.3 preuve: information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige.

3.4.4 générateur de preuve: entité qui produit une preuve de non-répudiation.

NOTE – Cette entité peut être le demandeur du service de non-répudiation, l'expéditeur, le destinataire ou des parties multiples travaillant de concert (par exemple un signataire et un cosignataire).

3.4.5 sujet de preuve: entité dont l'implication dans un événement ou une action est démontrée par une preuve.

3.4.6 utilisateur de preuve: entité qui utilise une preuve de non-répudiation.

3.4.7 vérificateur de preuve: entité qui vérifie une preuve de non-répudiation.

3.4.8 code d'authentification de message: valeur de contrôle cryptographique utilisée pour assurer l'intégrité des données et l'authentification de leur origine.

3.4.9 demandeur du service de non-répudiation: entité qui demande qu'une preuve de non-répudiation soit produite pour un événement particulier ou pour une action particulière.

3.4.10 notaire: tiers de confiance chez qui les données sont enregistrées afin de pouvoir garantir plus tard l'exactitude des caractéristiques de ces données.

3.4.11 expéditeur: dans le contexte du transfert de données, entité qui expédie les données par une action qui est sujette à un service de non-répudiation.

3.4.12 destinataire: dans le contexte du transfert de données, entité qui reçoit les données par une action qui est sujette à un service de non-répudiation.

NOTE – Dans le modèle logique de non-répudiation, d'autres entités peuvent intervenir. Par exemple, le propriétaire est l'entité qui formule un message original et un agent de transfert est l'entité qui transfère le message; dans ce contexte, les entités seront assimilées à des entités expéditrices ou destinataires.

4 Abréviations

CA Autorité de certification (*certification authority*)

MAC Code d'authentification de message (*message authentication code*)

OSI Interconnexion des systèmes ouverts (*open systems interconnection*)

TTP Tiers de confiance (*trusted third party*)

5 Considérations générales sur la non-répudiation

5.1 Concepts de base de la non-répudiation

Le service de non-répudiation implique la production, la vérification et l'enregistrement de preuves, ainsi que la consultation et la revérification ultérieures de ces preuves, en cas de besoin. Les litiges ne peuvent être résolus que si les preuves ont été enregistrées au préalable.

L'objet du service de non-répudiation décrit dans ce cadre est de fournir une preuve au sujet d'un événement particulier ou d'une action particulière. Le service de non-répudiation peut être demandé par des entités autres que celles qui participent à l'événement ou à l'action. Exemples d'action pouvant être protégée par un service de non-répudiation:

- expédition d'un message X.400;
- insertion d'un article dans une base de données;
- invocation d'une opération distante.

Lorsqu'il s'agit de messages, l'identité de l'expéditeur et l'intégrité des données doivent être confirmées pour prouver l'origine des messages. Pour apporter la preuve d'une remise des données, il faut confirmer l'identité du destinataire et l'intégrité des données remises. Dans certains cas, des preuves peuvent également être requises concernant le contexte (par exemple, la date, l'heure, l'emplacement de l'expéditeur/destinataire).

Ce service offre les options supplémentaires suivantes, qui peuvent être utilisées en cas de tentative de répudiation:

- production de preuve;
- enregistrement de preuve;
- vérification de la preuve produite;
- consultation et revérification de la preuve.

Les litiges peuvent être réglés directement entre parties prenantes, par examen des preuves. Un litige peut parfois devoir être réglé par un arbitre, qui évalue les preuves et détermine si l'action ou l'événement litigieux a eu lieu. L'arbitrage ne peut être assuré efficacement que si les parties au litige acceptent l'autorité de l'arbitre. Pour que les preuves fournies soient acceptées par l'arbitre, il faut généralement qu'elles soient confirmées par un ou par plusieurs tiers de confiance. En option, l'arbitre peut être le tiers de confiance qui confirme la preuve. Les mécanismes de non-répudiation font appel à un certain nombre de types de tiers de confiance et de formes de preuve.

5.2 Rôles d'un tiers de confiance

Un ou plusieurs tiers de confiance peuvent être impliqués dans le service de non-répudiation.

Les tiers de confiance qui assurent la non-répudiation sans être activement impliqués dans chaque utilisation du service sont appelés «*tiers de confiance déconnectés*». Un tiers de confiance qui est activement impliqué dans la production ou dans la vérification de preuves est appelé «*tiers de confiance connecté*». Un tiers de confiance connecté qui fait office d'intermédiaire dans toutes les interactions est appelé «*tiers de confiance en ligne*».

Un tiers de confiance peut être appelé à enregistrer et/ou à recueillir des preuves; il peut également être appelé à attester la validité des preuves. Un certain nombre de tiers de confiance peuvent être impliqués dans divers rôles (par exemple les rôles de notaire, de pointeur temporel, de surveillant, de certificateur de clé, de producteur de signature, de vérificateur de signature et d'autorité de remise). Un même tiers de confiance peut agir au titre d'un ou de plusieurs de ces rôles.

Dans le rôle de producteur de preuve, un tiers de confiance coopère avec un demandeur de service de non-répudiation pour produire des preuves.

Dans le rôle d'enregistreur de preuve, un tiers de confiance enregistre des preuves qui pourront être consultées ultérieurement par un utilisateur de preuve ou par un arbitre.

Dans le rôle de pointeur temporel, un tiers de confiance est censé apporter une preuve telle que le moment où la demande de pointage temporel a été reçue.

Dans le rôle de surveillant, un tiers de confiance contrôle l'action ou l'événement et est censé donner la preuve de ce qui a été surveillé.

Dans le rôle de certificateur de clé, un tiers de confiance fournit des certificats de non-répudiation associés à un générateur de preuve afin de garantir la validité d'une clé publique à utiliser pour des fins de non-répudiation.

Dans le rôle de distributeur de clés, un tiers de confiance fournit des clés aux générateurs de preuve et/ou aux vérificateurs de preuve. Il peut aussi imposer des contraintes à l'utilisation des clés, en particulier lorsque des techniques symétriques sont utilisées.

Dans le rôle de producteur de signature, un tiers de confiance est censé fournir une preuve sous la forme d'une signature numérique au nom du sujet de preuve.

Dans le rôle de vérificateur de preuve, un tiers de confiance vérifie la preuve à la demande d'une autre entité.

Dans le rôle de vérificateur de signature, un tiers de confiance est censé vérifier une preuve, pour le compte d'un utilisateur de preuve, sous la forme d'une signature numérique.

NOTE – Le rôle de producteur de signature est un cas particulier du rôle de producteur de preuve. Le rôle de vérificateur de signature est un cas particulier du rôle de vérificateur de preuve.

Dans le rôle de notaire, un tiers de confiance fournit une assurance au sujet des propriétés des données communiquées entre deux ou plus de deux entités, telles que l'intégrité, l'origine, l'heure ou la destination des données.

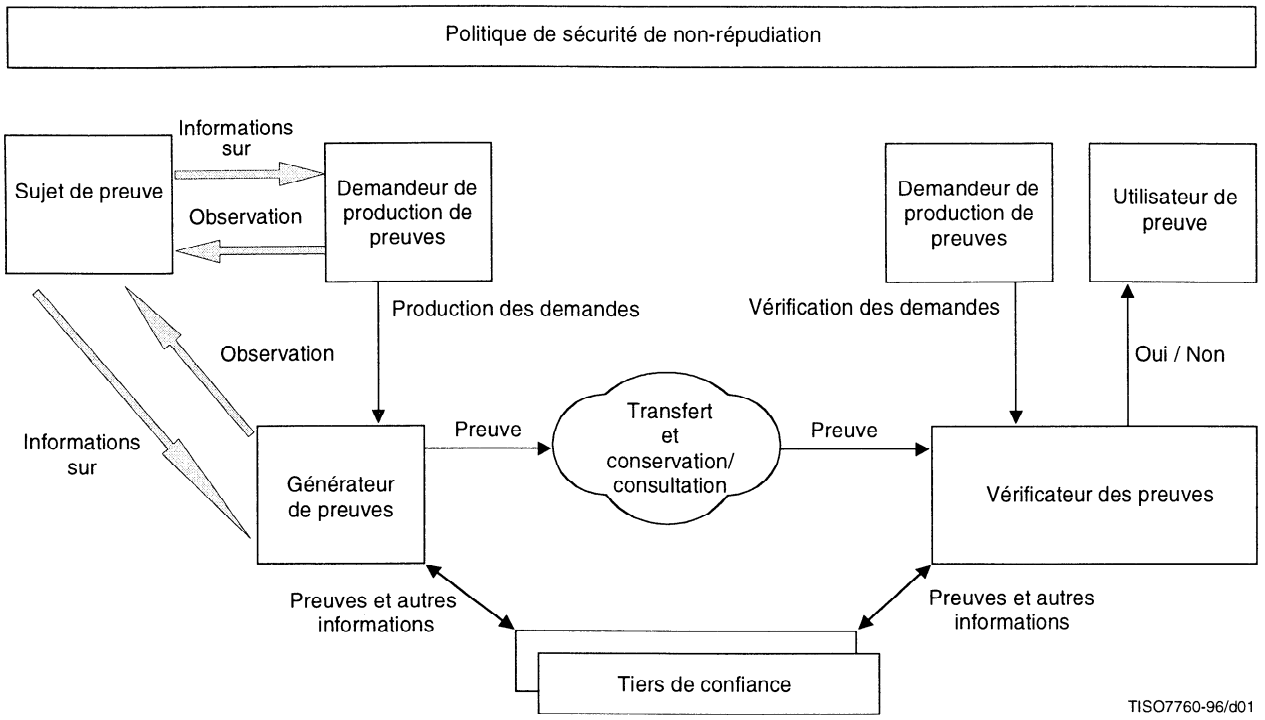
Dans le rôle d'autorité de remise, un tiers de confiance entre en interaction avec le destinataire prévu des données et essaye de les lui remettre. Il fournit ensuite la preuve que les données ont été remises, qu'elles n'ont pas été remises ou que la remise a été tentée mais qu'aucune confirmation de réception n'a été reçue. Dans ce dernier cas, l'utilisateur de la preuve ne peut pas déterminer si les données ont été reçues par le destinataire prévu ou non.

5.3 Phases de la non-répudiation

La non-répudiation se compose de quatre phases distinctes:

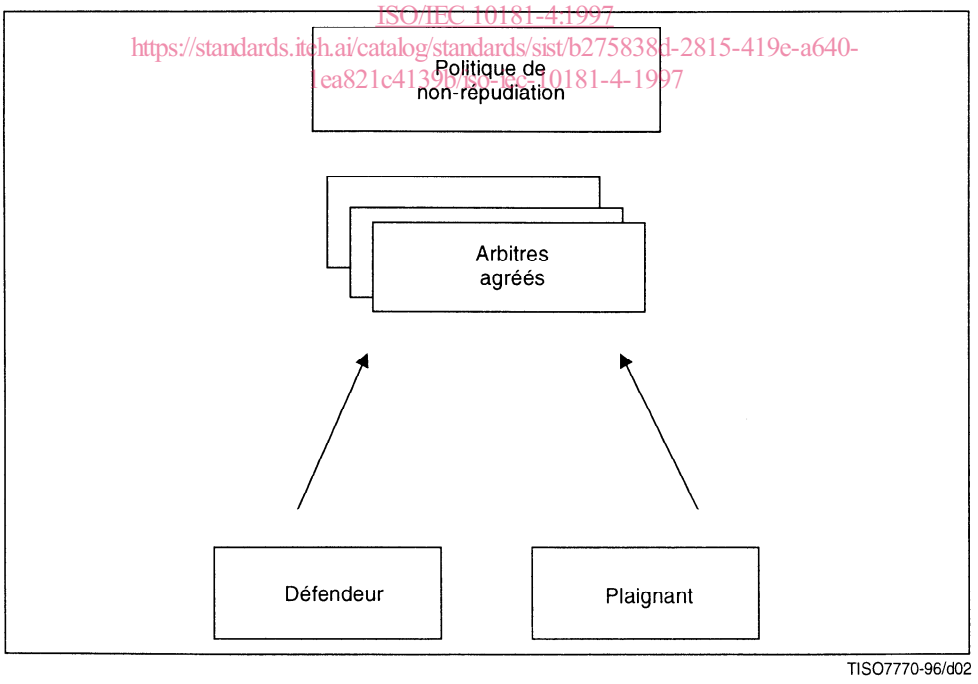
- la production des preuves;
- le transfert, la conservation et la consultation des preuves;
- la vérification des preuves;
- la résolution des litiges.

La Figure 1 montre les trois premières phases. La Figure 2 montre la quatrième phase.



NOTE – Cette figure, donnée à titre d'illustration, n'est pas définitive.

Figure 1 – Entités impliquées dans les phases de production, de transfert, de consultation/conservation et de vérification des preuves



NOTE – Cette figure, donnée à titre d'illustration, n'est pas définitive.

Figure 2 – Phase de résolution des litiges lors d'un processus de non-répudiation