Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

F.747.10

(01/2022)

SÉRIE F: SERVICES DE TÉLÉCOMMUNICATION NON TÉLÉPHONIQUES

Services multimédias

Exigences des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé

Recommandation UIT-T F.747.10

RECOMMANDATIONS UIT-T DE LA SÉRIE F

SERVICES DE TÉLÉCOMMUNICATION NON TÉLÉPHONIQUES

SERVICE TÉLÉGRAPHIQUE	
Méthodes d'exploitation pour le service télégraphique public international	F.1–F.19
Le réseau gentex	F.20–F.29
Commutation de messages	F.30–F.39
Le service international de télémessagerie	F.40–F.58
Le service télex international	F.59–F.89
Statistiques et publications des services télégraphiques internationaux	F.90–F.99
Services de télécommunication à location et à heures prédéterminées	F.100–F.104
Services phototélégraphiques	F.105–F.109
SERVICE MOBILE	
Service mobile et services multidestination par satellite	F.110–F.159
SERVICES TÉLÉMATIQUES	
Service public de télécopie	F.160–F.199
Service télétex	F.200–F.299
Service vidéotex	F.300–F.349
Dispositions générales relatives aux services télématiques	F.350–F.399
SERVICES DE MESSAGERIE	F.400–F.499
SERVICES D'ANNUAIRE	F.500–F.549
COMMUNICATION DE DOCUMENTS	
Communication de documents	F.550–F.579
Interfaces de communication de programmation	F.580–F.599
SERVICES DE TRANSMISSION DE DONNÉES	F.600–F.699
SERVICES MULTIMÉDIAS	**F.700–F.799**
SERVICES DU RNIS	F.800–F.849
TÉLÉCOMMUNICATIONS PERSONNELLES UNIVERSELLES	F.850–F.899
ACCESSIBILITÉ ET FACTEURS HUMAINS	F.900–F.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T F.747.10

Exigences des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé

Résumé

La Recommandation UIT-T F.747.10 définit les exigences générales et les capacités fonctionnelles des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé.

La présente Recommandation décrit les exigences relatives au modèle de services de registres distribués intégrant un facteur humain sécurisé, permettant de concilier les objectifs contradictoires de protection de la vie privée et d'utilisation de mégadonnées personnelles intégrant le facteur humain. Elle décrit également les capacités fonctionnelles des nœuds de partage de registres distribués intégrant le facteur humain afin de procéder à un apprentissage automatique sans déchiffrement des données chiffrées intégrant le facteur humain. Cependant, les calculs nécessaires concernant l'apprentissage automatique pour les données chiffrées peuvent être excessifs. Pour résoudre ce problème, ce modèle de services de registres distribués intégrant le facteur humain prévoit des procédures permettant d'utiliser au moins deux paires de clés de chiffrement et de notifier le type de clé. En outre, la présente Recommandation définit les exigences relatives au maintien de l'intégrité pour les services intégrant un facteur humain sécurisé afin de maintenir des registres distribués sûrs et qu'une vérification soit effectuée dès le début en vue de la distribution d'informations personnelles intégrant le facteur humain. Par conséquent, l'utilisation de systèmes de registres distribués pour la distribution d'informations personnelles sécurisées intégrant le facteur humain permet de garantir un suivi transparent depuis la distribution jusqu'à l'utilisation finale.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T F.747.10	17-01-2022	16	11.1002/1000/14644

Mots clés

Modèle de services de registres distribués, renforcement de la protection de la vie privée, facteur humain sécurisé; suivi de la transparence.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT avait été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas des renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

© UIT 2022

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Contexte	3
7	Exigences générales des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé	4
	7.1 Exigences fonctionnelles relatives aux nœuds de partage de registres distribués publics	4
	7.2 Exigences d'authentification pour les nouveaux nœuds participants	4
	7.3 Exigences de sécurité applicables au système de registre distribué	5
	7.4 Exigences relatives au maintien de l'intégrité pour les systèmes de registres distribués	6
8	Capacités fonctionnelles des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé	6
	8.1 Structure de registre distribué pour la distribution d'informations personnelles intégrant le facteur humain	7
	8.2 Deux fonctions de la structure de registre distribué pour la distribution d'informations personnelles intégrant le facteur humain	7
	8.3 Méthodes de maintenance des systèmes de registres distribués	8
Annexe A – Application concernant le modèle de services de registres distribués intégrant un facteur humain sécurisé		10
Bibliographie		11

Recommandation UIT-T F.747.10

Exigences des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé

1 Domaine d'application

La présente Recommandation, qui décrit les exigences des systèmes de registres distribués (DLS) pour les services intégrant un facteur humain sécurisé, comprend:

– le contexte;

– les exigences générales des systèmes DLS pour les services intégrant un facteur humain sécurisé;

– les capacités fonctionnelles des systèmes DLS pour les services intégrant un facteur humain sécurisé.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 bloc [b-ISO 22739]: structure de données comprenant un bloc de données et un en-tête de bloc.

3.1.2 consensus [b-ISO 22739]: accord entre les nœuds DLT selon lequel 1) une transaction est validée et 2) le registre distribué contient un ensemble et un ordonnancement cohérents de transactions validées.

3.1.3 signature numérique [b-ISO 22739]: données qui, lorsqu'elles sont associées à un objet numérique, permettent à l'utilisateur de l'objet numérique d'authentifier leur origine et leur intégrité.

3.1.4 registre distribué [b-ISO 22739]: registre partagé entre un ensemble de nœuds DLT et synchronisé entre les nœuds DLT au moyen d'un mécanisme de consensus.

3.1.5 technologie des registres distribués [b-ISO 22739]: technologie permettant d'exploiter et d'utiliser des registres distribués.

3.1.6 embranchement [b-UIT-T TS FG DLT D1.1]: création d'au moins deux versions différentes d'un registre distribué.

3.1.7 valeur de hachage [b-ISO 22739]: chaîne de bits résultant d'une fonction de hachage cryptographique.

3.1.8 santé [b-OMS]: un état de bien-être physique, mental et social avec absence de maladie ou d'infirmité.

3.1.9 registre [b-ISO 22739]: mémoire d'informations contenant des relevés de transactions censées être finales, définitives et inaltérables.

3.1.10 arbre de Merkle [b-NIST]: structure de données dans laquelle les données sont hachées et combinées jusqu'à obtenir un hachage racine unique représentant l'ensemble de la structure de données.

3.1.11 minage [b-UIT-T F.751.0]: activité réalisée au niveau de certains mécanismes de consensus, donnant lieu à récompense.

3.1.12 nœud [b-ISO 22739]: composant élémentaire sur lequel repose une structure de données.

3.1.13 système de registre distribué public [b-UIT-T F.751.0]: système DLT accessible au public à des fins d'utilisation.

3.1.14 transaction [b-ISO 22739]: plus petite unité d'un processus de travail, qui correspond à une ou plusieurs séquences d'actions requises pour produire un résultat conforme aux règles applicables.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 profondeur de bloc: niveau d'un bloc ajouté à la chaîne d'un système de registre distribué à compter du premier bloc.

3.2.2 dossiers électroniques intégrant le facteur humain: collection systématisée d'informations sur les personnes et la population intégrant le facteur humain stockées sur un support électronique dans un format numérique.

3.2.3 facteur humain: principes visant à créer des conditions de vie optimales en ce qui concerne le bien-être, la sécurité et la santé des personnes, notamment à améliorer les technologies existantes et en adopter de nouvelles.

NOTE – Adapté de [b-ISO 6385] et [b-Wickens].

3.2.4 informations personnelles intégrant le facteur humain: informations recueillies en analysant directement le corps humain et les environnements dans lesquels il évolue, qui sont transmises via un réseau de communication à des dispositifs individuels intégrant le facteur humain ou à d'autres dispositifs utilisés pour stocker les dossiers électroniques intégrant le facteur humain.

3.2.5 dispositif individuel intégrant le facteur humain: type de dispositif analysant le corps humain et les environnements dans lesquels il évolue et échangeant les informations recueillies avec d'autres dispositifs intégrant le facteur humain.

3.2.6 facteur humain sécurisé: facteur humain dans la sécurité de l'information.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CPU unité centrale de traitement (*central processing unit*)

DLS systèmes de registres distribués (*distributed ledger systems*)

DLT technologie des registres distribués (*distributed ledger technology*)

IP protocole Internet (*Internet protocol*)

PDLS systèmes de registres distribués publics (*public distributed ledger systems*)

UUID identificateur unique universel (*universally unique identifier*)

VRF fonction aléatoire vérifiable (*verifiable random function*)

5 Conventions

Dans la présente Recommandation:

– L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

– L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

– L'expression "peut, à titre d'option" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

6 Contexte

Ces dernières années, le volume d'informations personnelles intégrant le facteur humain a considérablement augmenté en raison du développement des dispositifs individuels de collecte de données de santé et de la multiplication des données personnelles issues des dossiers médicaux gérés par les hôpitaux. L'un des meilleurs modèles de gestion et de partage des données personnelles intégrant le facteur humain est le modèle de services de registres distribués. Les caractéristiques des systèmes de registres distribués garantissent la fiabilité au moyen d'une base de données répartie contenant de multiples nœuds, ainsi que la transparence des données extraites grâce à des signatures numériques et à des valeurs de hachage. Cependant, les données intégrant le facteur humain sont des informations très sensibles qu'il convient de protéger. Par conséquent, il est nécessaire d'appliquer des exigences de protection des informations personnelles intégrant le facteur humain au modèle de services de registres distribués publics (voir la Figure 1).

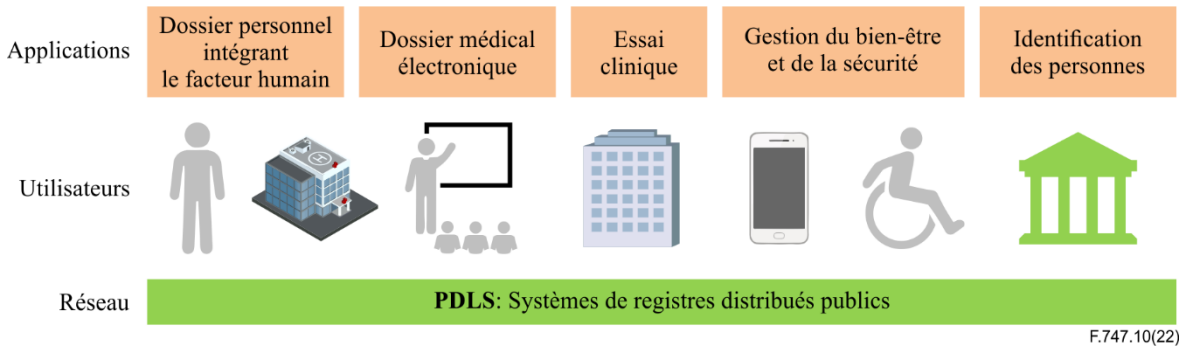

Figure 1 – Modèle de services de registres distribués intégrant le facteur humain

La présente Recommandation décrit les exigences de sécurité applicables au modèle de services de registres distribués intégrant le facteur humain, permettant d'atteindre des objectifs de protection de la vie privée et d'utilisation de mégadonnées personnelles de santé. La Recommandation présente également les exigences fonctionnelles relatives aux nœuds de partage de registres distribués afin de procéder à un apprentissage automatique sans déchiffrement des données chiffrées. Elle décrit les exigences d'incitation appliquées dans le modèle de services de registres distribués visant à améliorer la qualité de vie en automatisant la distribution des produits de santé directement vers les

consommateurs et les producteurs. L'utilisation de la technologie des registres distribués permet d'abord de suivre et gérer la production et la distribution d'informations de santé. En d'autres termes, l'utilisation de la technologie des registres distribués pour la distribution d'informations personnelles intégrant le facteur humain permet de garantir un suivi transparent depuis la distribution jusqu'à l'utilisation finale. C'est pourquoi les individus représentés par des nœuds individuels dans le système de registre distribué peuvent se fier aux informations distribuées et les utiliser. En outre, il est possible d'appliquer une méthode permettant de bloquer naturellement la distribution illicite d'informations personnelles intégrant le facteur humain.

7 Exigences générales des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé

La présente section décrit les exigences relatives à une procédure de gestion des mouvements dans les registres distribués en toute sécurité permettant de concilier les objectifs contradictoires de protection des informations personnelles et d'utilisation de mégadonnées personnelles intégrant le facteur humain. Elle présente les exigences fonctionnelles relatives aux nœuds de partage de registres distribués afin de procéder à un apprentissage automatique sans déchiffrement des données chiffrées. Par exemple, le chiffrement homomorphe est une technique cryptographique permettant d'effectuer tous les calculs réalisés par un ordinateur sans même déchiffrer les données chiffrées. Y compris dans le cas d'une analyse de données avec des informations personnelles à protéger, on peut, à titre d'option, procéder à un apprentissage automatique sans provoquer de fuite d'informations personnelles ou de perte de données.

7.1 Exigences fonctionnelles relatives aux nœuds de partage de registres distribués publics

Les exigences fonctionnelles relatives aux nœuds de partage de registres distribués publics sont présentées ci-après:

– Il est obligatoire que les nœuds stockent les données de la chaîne du système de registre distribué qui s'accumulent depuis le premier bloc.

– Il est obligatoire que le statut d'achèvement soit notifié aux autres nœuds, dès lors qu'un nœud exécute un algorithme de confirmation de distribution, lorsque la transaction est vérifiée.

– Afin de vérifier la validité du registre distribué généré à chaque cycle, il est obligatoire que le nœud vérifie la validité du bloc généré en le comparant à la valeur de hachage cible.

– Il est obligatoire que chaque nœud mette à jour et gère les données partagées telles que la liste des clés publiques de tous les autres nœuds et le registre distribué.

– Il est obligatoire que le nœud propage la transaction vers les autres nœuds jusqu'à la phase d'accord (par exemple l'achèvement de la confirmation de la transaction) dans le processus de vérification de la transaction.

– Il est obligatoire que le nœud chiffre les données d'une transaction devant être sécurisées à l'aide de clés de chiffrement (exemples: certificat de clé publique [b-UIT-T X.509], chiffrement homomorphe [b-ISO 18033-6] et fonction aléatoire vérifiable (VRF) [b-IETF draft-irtf-cfrg-vrf-08]) et notifie le type de clé de chiffrement.

– Il est obligatoire que le nœud détermine si le déchiffrement est nécessaire. Si tel est le cas, il déchiffre les données et les transmet au nœud demandeur. Dans le cas contraire, le nœud chiffre les données en utilisant la clé publique du nœud demandeur et les lui transmet.

7.2 Exigences d'authentification pour les nouveaux nœuds participants

Il est recommandé que les nœuds existants proposent les fonctions décrites dans les § 7.2.1 à 7.2.3, afin d'authentifier les nouveaux nœuds participants dans un système partagé de registre distribué.

7.2.1 Exigences relatives à la demande d'authentification de nouveaux nœuds

– Il est recommandé qu'un nouveau nœud utilise au moins deux paires de clés de chiffrement (par exemple un certificat de clé publique [b-UIT-T X.509] et le chiffrement homomorphe [b-ISO 18033-6]) avant de présenter une demande.

– Il est recommandé que le nouveau nœud chiffre le message contenant sa demande avec sa propre clé privée et envoie à la fois les données chiffrées et sa clé publique aux autres nœuds.

– Il est recommandé que chaque nœud, lorsqu'il vérifie et transmet les informations authentifiées, mette à jour la liste des clés publiques vérifiées des nœuds nouveaux et existants et stocke la liste des clés publiques du système partagé de registre distribué pour participer.

7.2.2 Exigences fonctionnelles d'authentification applicables aux nœuds

– Il est recommandé que le nœud vérifie la validité en déchiffrant les données chiffrées transmises par le nouveau nœud désireux de participer et la clé publique qui les accompagne, chiffre les informations vérifiées et la liste des clés publiques en utilisant la clé publique du nouveau nœud, et transmette les informations chiffrées.

– Il est recommandé que le nœud dispose d'une liste des clés publiques de tous les nœuds participant au système partagé de registre distribué et mette à jour sa liste de clés publiques à chaque fois qu'il procède à l'authentification d'un nouveau nœud.

– À chaque fois qu'il est recommandé que le nœud mette à jour sa liste de clés publiques, il est obligatoire pour celui-ci de chiffrer la liste des clés publiques à l'aide de sa propre clé privée et de l'envoyer à tous les nœuds participant au système partagé de registre distribué.

– Il est recommandé que le nœud stocke en permanence les informations vérifiées concernant les nœuds participant au système partagé de registre distribué, ainsi que l'heure de la vérification et l'adresse du nœud participant.

7.2.3 Exigences applicables aux nœuds existants en matière de vérification de l'authentification d'un nouveau nœud

– Il est recommandé que les nœuds existants vérifient la signature numérique de la liste des clés publiques envoyée par le nœud et actualisent celle-ci avec la nouvelle liste des clés publiques.

– Il est recommandé que les nœuds existants vérifient la participation du nouveau nœud authentifié en consultant la nouvelle liste des clés publiques.

7.3 Exigences de sécurité applicables au système de registre distribué

Il est recommandé que les nœuds existants respectent les dispositions énoncées dans le présent paragraphe.

– Il est obligatoire que les tentatives de manipulation des informations dans un registre distribué partagé existant fassent l'objet d'une vérification au moyen d'une signature électronique et soient rejetées dans le registre distribué.

– Parmi les principales chaînes utilisées dans le système de registre distribué, il est obligatoire de rejeter dans le registre distribué les chaînes dont le contenu diffère de celui de la chaîne la plus longue jusqu'à une profondeur de bloc arbitraire b au moment de la création d'un nouveau bloc. Dans le cas présent, b est un nombre supérieur à 1.

– Il est obligatoire de rejeter les données au cours de la création du registre distribué lorsque des données avec des adresses dupliquées (IP et UUID, par exemple) sont ajoutées au système de registre distribué.

– Il est obligatoire que la source aléatoire commune (par exemple un nonce cryptographique [b-NIST]) soit identique pour les blocs de toute profondeur d. Il est obligatoire que les blocs ajoutés aux blocs d'une profondeur d actualisent la source aléatoire commune d'une profondeur de bloc g. Une fois la mise à jour effectuée, il est recommandé d'utiliser la valeur de hachage du bloc nouvellement ajouté en tant que source aléatoire.

  NOTE – Profondeur de bloc d et profondeur de bloc g correspondent ici à des blocs d'une profondeur supérieure à 1.

– Il est obligatoire de rejeter dans le registre distribué les chaînes contenant des blocs dont les valeurs de hachage diffèrent de celles des blocs précédents et de la racine de l'arbre de Merkle.

– Si une erreur concernant un nœud se produit parmi les nœuds constituant le système de registre distribué, il est recommandé que les nœuds sans erreur soient conservés s'ils se trouvent au-dessus du niveau de consensus prédéfini pour le système DLS.

7.4 Exigences relatives au maintien de l'intégrité pour les systèmes de registres distribués

Il est recommandé que les nœuds existants respectent les dispositions du présent paragraphe.

– Il est recommandé que chaque nœud mette un terme à toute tentative de manipulation des informations dans le registre distribué partagé existant. Si une telle attaque est détectée, il est recommandé de comptabiliser le nombre de nœuds afin d'obtenir le ratio de la force de hachage. Il est recommandé de comparer le nombre actuel d'arbres de blocs avec la valeur seuil pour évaluer la sécurité et transmettre (diffuser) les informations correspondantes et les adresses des nœuds à tous les nœuds.

– Il est recommandé que chaque nœud supprime du système de registre distribué les chaînes les plus longues communément utilisées dans ledit système et les chaînes avec des contenus différents.

– Il est recommandé que chaque nœud supprime les chaînes contenant des blocs avec des valeurs de hachage ou des racines de l'arbre de Merkle différentes de celles des blocs précédents dans le registre distribué, comptabilise le nombre de nœuds qui ont fait l'objet d'attaques pour savoir si le registre distribué est sûr, et transmette (diffuse) les informations correspondantes et les adresses des nœuds.

– En cas d'erreur ou de falsification concernant un nœud au sein des composantes du système de registre distribué, il est recommandé que chaque nœud supprime et comptabilise le nombre de nœuds pour lesquels il y a eu tentative d'erreur ou d'attaque afin d'obtenir un ratio de puissance de hachage. Dans le registre distribué, il est recommandé de maintenir un nombre de nœuds sécurisés supérieur à la valeur seuil, et il est recommandé de transmettre (diffuser) les informations correspondantes et les adresses des nœuds.

– Il est recommandé que chaque nœud, lors du processus de création de registre distribué, rejette les données lorsque de nouvelles données avec des adresses dupliquées sont ajoutées aux données du système de registre distribué.

8 Capacités fonctionnelles des systèmes de registres distribués pour les services intégrant un facteur humain sécurisé

À titre d'incitation, il est obligatoire d'améliorer la qualité de vie dans un modèle de services de registres distribués en automatisant la distribution directe d'informations personnelles intégrant le facteur humain. L'utilisation de la technologie de registres distribués permet d'abord de suivre et gérer la production et la distribution d'informations intégrant le facteur humain. En d'autres termes, l'utilisation de la technologie de registres distribués pour la distribution d'informations personnelles intégrant le facteur humain permet de garantir un suivi transparent depuis la distribution jusqu'à l'utilisation finale. C'est pourquoi les individus représentés par des nœuds individuels dans le système

de registre distribué peuvent se fier aux informations distribuées et les utiliser. En outre, il est possible d'appliquer une méthode permettant de bloquer fondamentalement la distribution illicite d'informations personnelles intégrant le facteur humain.

8.1 Structure de registre distribué pour la distribution d'informations personnelles intégrant le facteur humain

Traditionnellement, la première transaction du registre est une transaction spéciale consistant à offrir une récompense (par exemple de la monnaie virtuelle [b-UIT-T F.751.0]) au créateur du registre. Cette récompense est offerte aux nœuds dès le début en vue de tenir un registre distribué visant à distribuer des informations personnelles intégrant le facteur humain. Il est recommandé d'approuver préalablement les techniques permettant d'offrir et de distribuer ces récompenses, car les nœuds évoluent dans des systèmes répartis. De nouvelles incitations sont ajoutées continuellement pour récompenser les nœuds (mineurs) qui consomment des ressources pour exploiter le système de registre distribué. Ces nœuds utilisent la puissance de calcul de l'unité centrale de traitement (CPU), de la mémoire et des pièces.

8.2 Deux fonctions de la structure de registre distribué pour la distribution d'informations personnelles intégrant le facteur humain

Pour réduire le temps d'attente tout en augmentant la vitesse de minage, on peut utiliser, à titre d'option, une technique de décomposition de la structure du registre distribué de base en trois fonctions. Cette technique revient à sélectionner la principale chaîne dans le protocole de registre distribué (par exemple la chaîne la plus longue), ce qui conduit à sélectionner le registre sécurisé parmi tous les registres pour chaque profondeur de l'arbre du registre. Ici, la profondeur d'un registre est définie comme la distance par rapport au registre d'origine (nombre de blocs connectés dans le registre).

Dans un registre distribué, le registre répond à trois objectifs: choisir le capitaine, ajouter des transactions à la principale chaîne et voter pour le registre ancêtre au moyen d'un lien parent-enfant. En exprimant le registre sous la forme d'une action conceptuelle, on procède à une subdivision en deux fonctions (voir la Figure 2). La fonction de proposition consiste à regrouper les transactions de la même profondeur dans l'arbre du registre d'origine. La fonction de vote consiste à choisir la partie de registre en votant pour une même profondeur de transactions dans l'arbre du registre. Le registre choisi reprend les registres partiels des transactions et forme le registre final. Cette fonction de vote est utilisée à la même profondeur de l'arbre du registre et permet de créer une connexion parent-enfant. Par conséquent, le lien parent-enfant de l'arbre du registre d'origine a deux fonctions explicitement distinctes: 1) assurer un certain ordre au niveau des registres dans la partie des transactions de la même profondeur; et 2) voter pour l'une ou l'autre partie du registre à des fins de filtrage. La structure globale du registre distribué pour la distribution d'informations personnelles intégrant le facteur humain est présentée ci-dessous dans la Figure 2.

Compte tenu de sa nature distribuée, le système de registre distribué (DLS) rencontre des problèmes de stabilité. Dans un système DLS, chaque nœud peut enregistrer une transaction, mais en définitive, le choix du nœud est le résultat de l'algorithme de consensus [b-UIT-T F.751.0]. Il est obligatoire de prendre en considération la conception d'un système DLS parmi les nombreux facteurs ayant une influence sur la stabilité, et il est recommandé de stabiliser le registre distribué en appliquant au système un traitement adaptatif. Pour remédier aux problèmes de stabilité du système DLS, la source aléatoire commune (par exemple le nonce cryptographique [b-NIST]) est identique pour les profondeurs de blocs d, et les blocs ajoutés aux blocs d'une profondeur d devraient mettre à jour la source aléatoire commune d'une profondeur de bloc g. Une fois la mise à jour effectuée, la valeur de hachage du bloc nouvellement ajouté est utilisée comme source aléatoire. Si $d = 1$, on revient à la règle de mise à jour de base qui fait faire un embranchement pour chaque "epoch", la vulnérabilité face aux attaques (équilibrées) par contamination étant très grande. Afin d'augmenter normalement le seuil de sécurité, d peut être augmenté. Lorsque $d = \infty$, tous les blocs utilisent le nonce du bloc

d'origine en tant que source aléatoire commune. Il s'agit du protocole de la chaîne la plus longue, dans lequel il est impossible de faire des embranchements, laissant ainsi le propriétaire infecté de la clé secrète établir des prévisions personnelles concernant la chaîne.

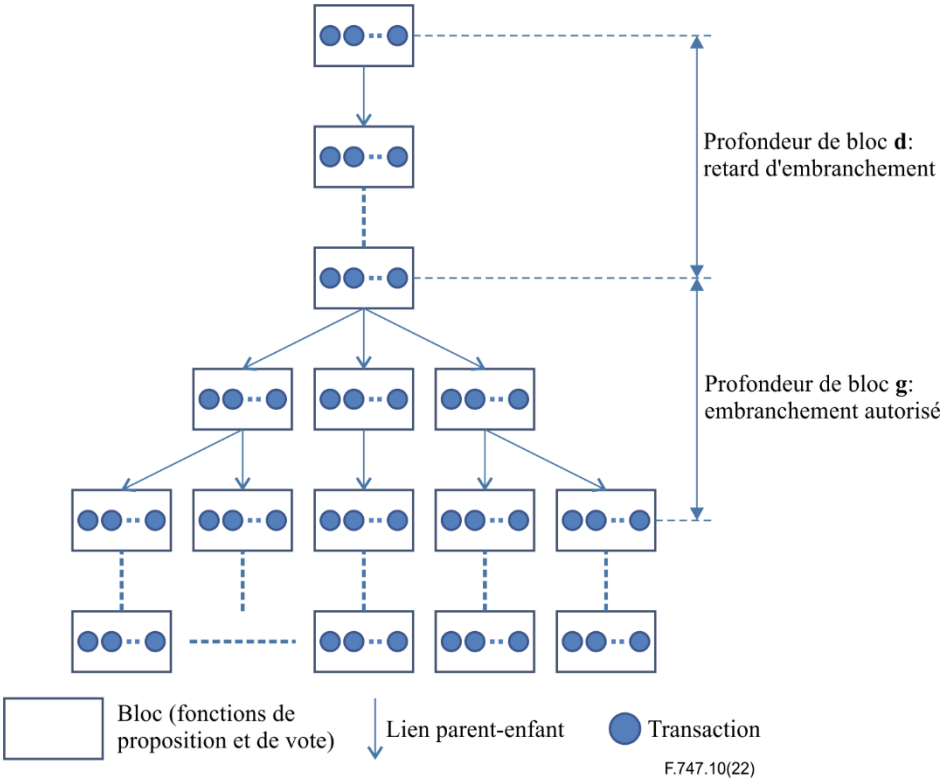

Figure 2 – Structure du modèle de services de registres distribués

8.3 Méthodes de maintenance des systèmes de registres distribués

Cette représentation de la décomposition fonctionnelle d'un registre distribué est beaucoup plus complexe que celle d'un registre distribué classique, mais elle peut améliorer les performances du registre distribué en obtenant un consensus plus rapide, ce qui permet d'augmenter le nombre de registres dans la partie des transactions sans compromettre la sécurité du registre distribué dans la fonction proposée. Par conséquent, le nombre de registres sera limité uniquement par la capacité du réseau de communication sous-jacent. Le consensus peut, à titre d'option, être confirmé avec un temps de latence faible et une fiabilité élevée, puisque de multiples transactions feront l'objet d'un vote en même temps que le registre proposé pour obtenir une confirmation rapide. Le système de registre distribué pour les informations personnelles intégrant le facteur humain est facile à gérer, car la vitesse générale de génération des registres a considérablement augmenté, et le nombre de registres partiels de la fonction proposée par profondeur peut être faible.

Ce système de registre distribué peut compromettre la transparence si la puissance de hachage est concentrée dans la fonction proposée d'une transaction particulière lors du choix du registre. Comme indiqué dans la Figure 3, si la puissance de hachage d'un attaquant est forte dans un registre précis de la fonction proposée, alors la sécurité peut être fortement compromise. La Figure 3 présente un exemple de chaîne de registres détruite ou infectée en raison de la concentration de la puissance de hachage d'un attaquant. Si un attaquant était en mesure de rassembler plus de puissance de calcul de la CPU, plus de mémoire et plus de pièces en un seul endroit plutôt que dans tous les nœuds sécurisés, il aurait le choix de les utiliser soit pour voler des récompenses offertes à des nœuds honnêtes, soit pour coopérer. Il conviendrait d'établir une politique d'incitation pour qu'un attaquant ait davantage intérêt à suivre les règles qu'à nuire à la transparence du système de registre distribué pour les informations personnelles intégrant le facteur humain. Il est obligatoire que cette incitation soit

adaptée en vue d'être répartie entre les nœuds participants. Avec une telle règle, il serait plus rentable pour l'attaquant de s'associer à tous les autres nœuds. Il est recommandé que, dans cette règle, le nombre de nœuds honnêtes reste supérieur à la valeur seuil (par exemple, CD $(1 + \alpha)/(\alpha-1)/\log(\alpha)$) en fonction du ratio de la force de hachage de l'attaquant (α). Dans le cas présent, C et D désignent la capacité et le retard des réseaux de communication.

On constate dans cette formule que si α est proche de 0, alors la puissance de hachage de l'attaquant est faible. On peut dire qu'il n'y a pas de problèmes de sécurité dans les systèmes de registres distribués même si le nombre d'arbres de blocs votants est limité. Toutefois, si α est proche de 1, c'est-à-dire si la puissance de hachage de l'attaquant est forte, alors le nombre d'arbres de blocs votants devrait croître de manière exponentielle. À ce stade, on peut observer que la sécurité peut être fortement compromise.

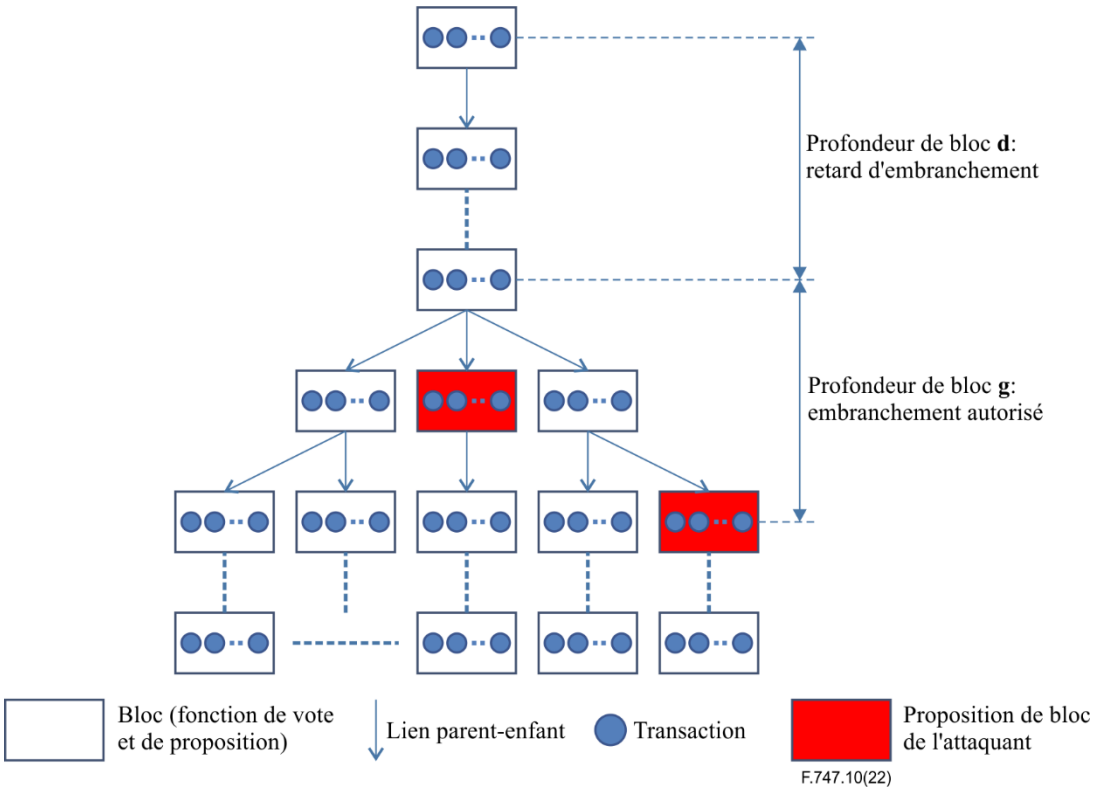

Figure 3 – Exemple de prévention de la contamination dans un modèle de services de registres distribués

Au cours du processus de sélection du bloc proposé, il est recommandé que la fonction du bloc soit déterminée en adaptant la puissance de hachage et les pièces. À ce moment-là, on peut observer que si la puissance de hachage et les pièces de l'attaquant sont fortes, la sécurité est grandement menacée. Si un attaquant pouvait rassembler davantage de puissance de calcul et de pièces que tous les nœuds honnêtes, il devrait décider de les utiliser soit pour voler les récompenses offertes aux nœuds honnêtes, soit pour coopérer. Il est recommandé de mettre en place des politiques d'incitation afin que les attaquants aient davantage intérêt à respecter les règles qu'à nuire au système et à la légitimité de leur propre richesse. En appliquant une politique qui vise à empêcher que les profits soient concentrés dans un bloc proposé précis, il est recommandé d'établir une règle en vertu de laquelle les attaquants auraient plus à gagner si les profits étaient répartis entre tous les nœuds.

Annexe A

Application concernant le modèle de services de registres distribués intégrant un facteur humain sécurisé

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Le système de registre distribué présenté dans la Figure A.1 permet de gérer en toute sécurité et transparence non seulement des données personnelles intégrant le facteur humain stockées à l'hôpital, mais aussi des données personnelles intégrant le facteur humain stockées sur des dispositifs individuels de collecte de données de santé. Dans l'exemple du partage d'informations de santé personnelles présenté dans la Figure A.1, la fiabilité peut être assurée en utilisant un registre distribué dans lequel participent de multiples nœuds, et des signatures numériques et des valeurs de hachage peuvent être utilisées pour garantir la transparence en matière de recherche de données. Cependant, les données personnelles intégrant le facteur humain sont particulièrement sensibles et il convient de les protéger. Ces données sensibles sont enregistrées sous forme chiffrée au moyen d'une technique de chiffrement capable de traiter des mégadonnées. Pour se conformer aux exigences et aux procédures du système partagé de registre distribué décrit dans le § 7.2, un algorithme de chiffrement est utilisé dans le cadre de la procédure de mobilité pour les informations personnelles sensibles intégrant le facteur humain (voir la Figure A.1). En outre, il est obligatoire que le système de registre distribué pour les informations personnelles intégrant le facteur humain soit exploité de manière à respecter les exigences de la fonction incitative décrite dans le paragraphe 8.3 en matière d'activation et de maintenance.

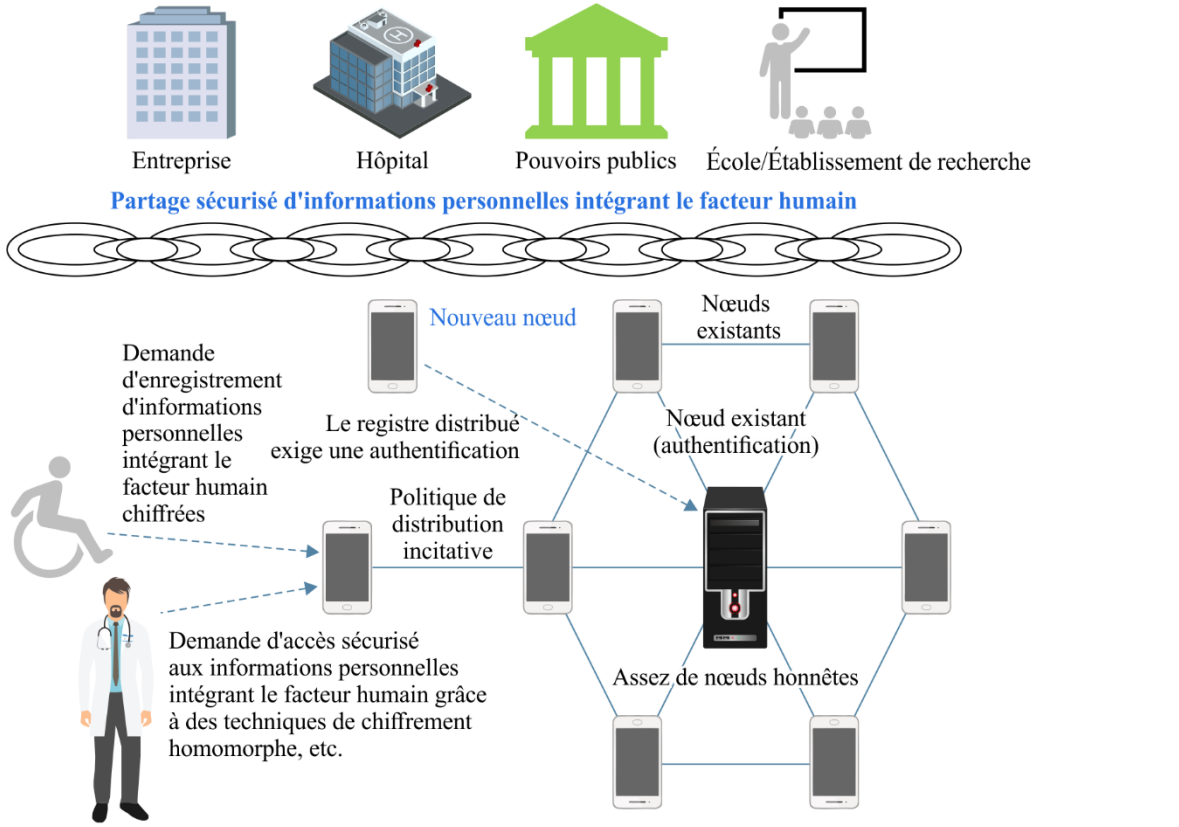

Figure A.1 – Situations d'utilisation du modèle de services de registres distribués sécurisés

Bibliographie

[b-UIT-T F.751.0] Recommandation UIT-T F.751.0 (2020), *Exigences pour les systèmes de registres distribués.*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019) | ISO/CEI 9594-8:2020, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[b-UIT-T TS FG DLT D1.1] Spécification technique UIT-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions.*

[b-IETF draft-irtf-cfrg-vrf-08] IETF draft-irtf-cfrg-vrf-08 (2020), *Verifiable Random Functions (VRFs).* https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-vrf-08

[b-ISO 6385] ISO 6385:2016, *Principes ergonomiques de la conception des systèmes de travail.*

[b-ISO 18033-6] ISO 18033-6:2019, *Techniques de sécurité IT – Algorithmes de chiffrement – Partie 6: Chiffrement homomorphe.*

[b-ISO 22739] ISO 22739:2020, *Chaîne de blocs et technologies de registres distribués – Vocabulaire.*

[b-NIST] NISTIR 8202 (2018). *Blockchain Technology Overview*.

[b-OMS] Organisation mondiale de la santé (2006), *Constitution de l'Organisation mondiale de la santé – Documents fondamentaux, quarante-cinquième édition, Supplément.*

[b-Wickens] Wickens, D., Gordon, S., Liu, Y. (1997), *An Introduction to Human Factors Engineering*. pp.2-7. New York, NY: Longman.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	**Services de télécommunication non téléphoniques**
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022