DIRECTIVE STRATEGIQUE

06. CRYPTOGRAPHIE

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DU GROUPE LA POSTE

Statut du document	Validé
Version	V 1.0
Date d'enregistrement	20/09/2019
Responsable du document	DSGG/DCG

Table des matières

1 Préambule

1.1 Objet du document

Cette directive fait partie du référentiel documentaire de la Politique de Sécurité des Systèmes d'Information du Groupe (PSSI-G). Elle décrit les mesures relatives à la cryptographie.

Elle doit établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information, en cohérence avec le Cadre Général.

1.2 Positionnement dans le cadre de référence

La Sécurité des Systèmes d'Information (SSI) du Groupe La Poste s'inscrit dans un cadre structuré en quatre niveaux :

- **Niveau 1** : *le cadre général*, qui fixe les objectifs, les principes généraux en matière de sécurité des SI et l'organisation permettant d'assurer un déploiement homogène des règles du Groupe La Poste ;
- **Niveau 2** : *les chartes et les directives stratégiques* de la PSSI-G, qui regroupent les règles permettant l'application du cadre général, dont le document présent ;
- **Niveau 3** : *les directives tactiques* décrites au niveau entité s'ajoutent aux directives stratégiques afin d'intégrer des éléments spécifiques à la gouvernance et au contexte d'emploi des SI des entités telles que mentionnées dans le champ d'application ;
- **Niveau 4** : *les procédures opérationnelles et guides techniques*, qui décrivent de manière explicite, les mesures d'application et de mise en œuvre de la PSSI-G.

Ce présent document est de niveau 2. La directive doit être lue et connue de toute personne travaillant pour le Groupe La Poste, y compris les prestataires intervenants sur le périmètre des SI du Groupe La Poste, tel que défini dans le champ d'application.

1.3 Champ d'application

La PSSI-G s'adresse à tous les acteurs du Groupe La Poste, de ses branches et de ses filiales intervenant, ou contrôlant les SI, notamment :

- Les Responsables de la Sécurité des Systèmes d'Information (RSSI) des entités ;

- L'Audit Informatique du Groupe (AIG) et les services en charge du contrôle interne ;
- Le Service de Lutte Contre la Cybercriminalité (SLCC) de la Direction des Systèmes d'Information Groupe (DSI/G) et les centres de supervision de la cybersécurité des branches et filiales ;
- Les acteurs intervenant au quotidien sur l'ensemble des SI du Groupe :
  - l'ensemble des collaborateurs,
  - les partenaires, prestataires et fournisseurs (contractuellement ou par le biais de conventions) dès lors qu'ils stockent, traitent ou utilisent des données issues du SI du Groupe La Poste.

Le RSSI complétera une matrice d'applicabilité qui déterminera :

- Le périmètre d'application des règles ;
- La possibilité de mise en œuvre ;
- La justification de non applicabilité.

1.4 Validité, révision et processus d'exception

La directive est applicable dès sa validation.

Elle doit être mise en œuvre dès publication sur tous les nouveaux projets applicatifs et d'infrastructures. La période de mise en conformité pour les SI déjà existants est de trois ans.

Cette directive pourra évoluer pour prendre en compte des retours d'expériences, imprécisions ou modifications des textes de référence.

Les demandes de révision sont à envoyer à la Direction de la Cybersécurité Groupe (DCG) : direction.cyber@laposte.fr.

La définition des exceptions aux règles est décrite dans le Cadre Général. La gestion des exceptions est documentée conformément au processus mis en place.

2 Glossaire

Terme	Description
Attaque par dictionnaire	Méthode consistant à découvrir un mot de passe en testant des mots de passe potentiels à partir d'un dictionnaire
Attaque par force brute	Méthode consistant à découvrir un mot de passe en utilisant toutes les combinaisons possibles de chaînes de caractères
Chiffrement asymétrique	Le chiffrement asymétrique s'appuie sur un ensemble de deux clés différentes. Ainsi la clef utilisée pour le chiffrement – la clé privée – est différente de celle utilisée pour le déchiffrement – la clé publique
Chiffrement symétrique	Le chiffrement symétrique permet à la fois de chiffer et de déchiffrer à l'aide d'une même clé cryptographique des informations
Clé secrète	Désigne, de façon systématique, une clé cryptographique utilisée dans un système symétrique
Clé privée	Partie qui doit rester secrète d'une bi-clé asymétrique
Clé publique	Partie publique d'une bi-clé asymétrique
Collaborateur	Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales
FIPS 197	Norme de l'algorithme de chiffrement par bloc Advanced Encryption Standard (AES)
Responsable Métier	Le responsable Métier a pour principale mission de s'assurer de la cohérence fonctionnelle globale des systèmes d'information dans un domaine particulier

3 Règles de sécurité applicables

La présente directive couvre l'ensemble des primitives cryptographiques mises en œuvre dans le cadre de services de confidentialité, d'intégrité, d'authentification et de non-répudiation.

3.1 Mesures cryptographiques

Objectif : garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité ou l'intégrité de l'information.

3.1.1 Politique d'utilisation des mesures cryptographiques

La politique d'utilisation des mesures cryptographiques a pour objet de définir le cadre d'usage des mesures cryptographiques au sein de chaque entité.

3.1.1.1 Politique d'utilisation des mesures cryptographiques

L'utilisation de mesures cryptographiques au sein d'une entité doit répondre à des besoins de protection des actifs en termes de confidentialité, d'intégrité, d'authentification et de non-répudiation.

3.1.1.2 Respect de la réglementation

La mise en œuvre de mesures cryptographiques doit être réalisée dans le respect strict de la réglementation nationale et internationale. En particulier, elle doit tenir compte des questions de circulation transfrontalière d'informations chiffrées.

3.1.1.3 Responsabilités

Les propriétaires d'actifs, dont les responsables Métiers sont responsables de la validation formelle des mesures de sécurité cryptographiques concernant les actifs dont ils ont la charge. Ils s'assurent notamment que les mesures proposées répondent au juste niveau aux besoins de sécurité de chaque actif.

Les RSSI des entités sont responsables de la validation technique des mesures de sécurité cryptographiques et des processus de gestion des clés.

Les Directeurs des Systèmes d'Information (DSI) des entités sont responsables de la mise en œuvre des mesures cryptographiques et des processus de gestion des clés.

Les RSSI, DSI et propriétaires d'actifs doivent faire appel à un spécialiste, au sein de leur entité, pour sélectionner les mesures cryptographiques appropriées permettant de répondre aux objectifs de sécurité conformément à l'analyse des risques du Système d'Information concerné.

Dans le cas d'un besoin de certification d'une solution cryptographique par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), les RSSI doivent piloter la conduite du processus de certification en lien avec la DCG.

3.1.1.4 Identification des niveaux de protection

La décision d'utilisation de mesures cryptographiques doit se fonder sur une démarche d'analyse des risques formelle. Cette approche par les risques a pour objectif de déterminer, au juste niveau, la pertinence d'une mesure cryptographique en évaluant le type de mesure qu'il convient d'appliquer et pour quel objectif de sécurité.

3.1.1.5 Protection des informations transportées

Tout support de stockage sur des appareils amovibles (clés et disques durs USB notamment) ou mobiles (ordinateur portable et smartphone) doit être chiffré.

Tout acheminement d'information par des voies d'intercommunication doit se faire de façon chiffrée. L'analyse des flux au niveau des passerelles d'interconnexion doit rester réalisable.

3.1.1.6 Politique de gestion des clés

Chaque entité décrit une politique de gestion des clés incluant notamment les méthodes à utiliser pour protéger les clés de chiffrement et récupérer des informations chiffrées en cas de perte, de compromission ou d'endommagement des clés.

3.1.1.7 Règles pour les algorithmes de chiffrement symétrique par bloc

La taille minimale des blocs de données pour les algorithmes symétriques est de 128 bits.

L'algorithme de chiffrement par bloc recommandé est l'Advanced Encryption Standard (AES) tel que décrit dans le FIPS 197.

L'utilisation du mode opératoire ECB est interdite.

3.1.1.8 Règles pour les algorithmes de chiffrement symétrique par flot

Il est recommandé d'employer des primitives de chiffrement par bloc et non des algorithmes de chiffrement par flot dédiés. Pour cela, il est nécessaire d'utiliser un mode opératoire par flot de chiffrement par bloc, tel que les modes OFB et CFB.

En cas d'utilisation d'un algorithme de chiffrement par flot, il est recommandé d'utiliser l'un des algorithmes suivants : HC-256, Rabbit, Salsa20, SOSEMANUK.

3.1.1.9 Règles pour les algorithmes de chiffrement asymétrique

Pour les algorithmes de chiffrement asymétrique basés sur la factorisation des entiers, la taille minimale du module est de 3072 bits et les exposants secrets doivent être de même taille que le module.

Pour les algorithmes de chiffrement asymétrique basés sur le logarithme discret, la taille minimale du module est de 3072 bits et l'ordre des sous-groupes est premier.

Pour les algorithmes de chiffrement asymétrique basés sur les courbes elliptiques, l'ordre des sous-groupes doit être multiple d'un nombre premier d'au moins 256 bits.

3.1.1.10 Règles pour les fonctions de hachage

Il est interdit d'utiliser la fonction de hachage MD5.

L'utilisation de la fonction de hachage SHA-1 est tolérée et doit être limitée au strict besoin de rétrocompatibilité avec des navigateurs obsolètes.

3.1.1.11 Règles pour les codes d'authentification de messages

Il est recommandé d'utiliser les codes d'authentification de message suivants : HMAC-SHA-2, HMAC-SHA-3.

L'utilisation de HMAC-MD5 est interdite.

L'utilisation de HMAC-SHA-1 est tolérée et doit être limitée au strict besoin de rétrocompatibilité avec des navigateurs obsolètes.

3.1.1.12 Règles pour l'authentification par défi-réponses

Les règles définies pour le chiffrement, les fonctions de hachage, la signature numérique et la génération d'aléa s'appliquent pour les mécanismes d'authentification d'une machine par une autre machine et d'un humain par une machine.

Il est recommandé que l'authentification entre deux machines soit intrinsèquement requise, c'est-à-dire qu'un mécanisme de contrôle d'accès défaillant ne puisse permettre un accès direct aux actions contrôlées en l'absence d'authentification.

Si une authentification est requise pour contrôler l'accès à des données, alors il est recommandé que la session authentifiée permette la mise en place d'un mécanisme cryptographique assurant la confidentialité et l'intégrité de ces données.

À la déconnexion d'une session authentifiée, si des éléments secrets ont été échangés lors de la phase d'authentification, ils doivent être effacés.

Au cours d'une session authentifiée, il est obligatoire d'incorporer un dispositif de déconnexion automatique en cas d'inactivité. La durée d'inactivité à prendre en compte est définie lors de l'analyse de risques.

Dans le cadre de l'authentification d'un utilisateur par une machine, l'entropie du mot de passe doit être choisie de façon à ce qu'une attaque par dictionnaire ou par force brute soit rendue inefficace dans un temps raisonnable.

3.1.1.13 Règles pour la signature numérique

Les règles définies pour les fonctions de hachage et le chiffrement asymétrique s'appliquent pour la signature numérique.

Pour la signature numérique, il est recommandé d'utiliser l'Elliptic Curve Digital Signature Algorithm (ECDSA) tel que décrit dans le FIPS 186-4.

Dans le cas de l'utilisation d'ECDSA, la courbe FRP256v1 doit être préférée. Les autres courbes utilisables sont : P-192, P-224, P-256, P-384, P-521, telles que définies dans le FIPS 186-4.

3.1.2 Gestion des clés

L'utilisation de clefs cryptographiques nécessite des mesures spécifiques de protection durant les différentes étapes de leur cycle de vie.

3.1.2.1 Procédure en cas de compromission des clés

Les procédures de récupération du système en cas d'atteinte à la confidentialité, à l'intégrité ou à l'authenticité d'une clé doivent être étudiées et documentées.

3.1.2.2 Cycle de vie des clés

Le cycle de vie d'une clé cryptographique comprend les étapes suivantes :

- la demande de clé auprès d'une autorité d'enregistrement ;
- la génération qui peut être centralisée ou locale ;
- l'affectation de la clé à une entité et à un usage ;
- l'introduction dans un système applicatif ;
- l'utilisation de la clé ;
- la fin de vie de la clé par révocation, retrait puis éventuellement par destruction ;
- le renouvellement ;
- le recouvrement permettant d'assurer la disponibilité d'un service.

La gestion de l'ensemble des étapes du cycle de vie des clés doit être réalisée conformément à la version en vigueur de l'annexe B2 du Référentiel Général de Sécurité (RGS).

3.1.2.3 Taille minimale des clés

La taille minimale des clés pour les algorithmes de chiffrement symétrique est de 128 bits.

La taille minimale des clés pour les algorithmes de chiffrement asymétrique basés sur la factorisation des entiers ou sur le logarithme discret est de 3072 bits.

3.1.2.4 Contrats avec des fournisseurs externes

Les éventuels accords de service ou contrats conclus avec des fournisseurs de services cryptographiques doivent couvrirent les questions de responsabilité juridique, de fiabilité des services et de réactivité dans la fourniture de ces services.

3.1.2.5 Procédure spécifique d'accès aux clés

Chaque entité met en œuvre une procédure pour répondre aux exigences légales d'accès aux clés cryptographiques notamment dans le cadre d'une procédure judiciaire.

4 Annexe

La cryptologie est la branche des mathématiques qui traite de la conception, de la sécurité et de l'emploi de mécanismes cryptographiques. Le terme générique de mécanisme englobant à la fois les algorithmes, les modes opératoires et les protocoles cryptographiques.

La cryptologie se subdivise en deux branches selon que l'on se place du point de vue du concepteur ou de celui de l'attaquant :

1. la cryptographie qui étudie la conception de mécanismes permettant d'assurer des propriétés de sécurité comme la confidentialité, l'intégrité ou l'authenticité de l'information,
2. la cryptanalyse qui s'intéresse à la sécurité de ces mêmes mécanismes.

Les algorithmes cryptographiques se subdivisent en deux familles :

1. les algorithmes symétriques basés sur une clé secrète,
2. les algorithmes asymétriques basés sur un groupe de deux de clés : une clé publique et une clé privée.

Les algorithmes cryptographiques sont classés en fonction de l'objectif de sécurité visé :

- **La confidentialité.** La confidentialité est la propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés. La confidentialité permet de réserver l'accès aux données aux seules personnes autorisées ;
- **L'intégrité.** L'intégrité est la propriété de protection de la fiabilité, de l'exactitude et de l'exhaustivité des données et des traitements ;
- **L'authentification.** L'authentification d'une information permet d'assurer qu'elle provient bien d'un interlocuteur particulier. L'authentification d'une entité a pour but de vérifier l'identité dont se réclame une entité ;
- **La non-répudiation.** La non-répudiation vise à empêcher qu'une entité puisse nier avoir effectué une action donnée.

Service			Algorithmes	
Nom		Détail	Cryptographie symétrique	Cryptographie asymétrique
Confidentialité		Protection de l'information sensible, par le chiffrement des données, lors du stockage ou de la transmission	Chiffrement par bloc ou par flot	Chiffrement à clé publique
				Échange de clé
Intégrité		Protection contre les modifications invalides de l'information lors du stockage ou de la transmission	Fonction de hachage cryptographique	Signature numérique
Authentification	Données	Garantir l'identité de l'émetteur de l'information	Code d'authentification de message	Signature numérique
	Entités	Prouver l'identité d'une entité (humain ou machine)	Défi-réponse	Signature numérique
Non-répudiation		Protection contre le déni d'action sur des informations par une entité	Code d'authentification de message	Signature numérique
Services annexes			Génération d'aléa	
			Gestion de clés	

Le choix et la mise en œuvre de mesures cryptographiques doit s'appuyer sur la démarche formelle suivante :

3. **Analyse des risques.** Elle consiste à identifier les évènements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels. Cette étape permet d'identifier le niveau de protection requis en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement ;
4. **Définition des objectifs de sécurité.** Une fois les risques appréciés, les objectifs de sécurité à satisfaire sont énoncés. Les objectifs de sécurité cryptographiques couvrent les domaines de l'intégrité, de la confidentialité, de l'authentification et de la traçabilité ;
5. **Choix et déploiement des fonctions cryptographiques.** Cette étape permet de préciser les fonctions cryptographiques à mettre en œuvre pour atteindre les objectifs de sécurité ;

6. **Suivi opérationnel.** Les mesures de protection cryptographiques doivent être accompagnées d'un suivi opérationnel régulier afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux.

Cette approche par les risques a pour objectif de déterminer au juste niveau, la pertinence d'une mesure cryptographique, le type de mesure qu'il convient d'appliquer, dans quel but, pour quel processus métier et pour quelle typologie de données, de support et de flux.

4.1 Chiffrement symétrique par bloc

Les algorithmes de chiffrement par bloc permettent, au moyen d'une clé secrète, connue seulement de l'émetteur et du récepteur, de protéger la confidentialité de l'information, même si le canal de communication employé est écouté. L'opération inverse du chiffrement est le déchiffrement. Les algorithmes de chiffrement par bloc permettent également de sécuriser le stockage de l'information.

Un algorithme de chiffrement par bloc traite les données à chiffrer par blocs de taille fixée. Son mode de fonctionnement consiste à combiner un bloc de données claires de taille fixe avec une clé secrète afin d'obtenir un bloc de contenu chiffré de même taille. À chaque algorithme de chiffrement correspond un algorithme inverse de déchiffrement. Le déchiffrement consiste alors à combiner un bloc de données chiffrées avec une clé secrète pour obtenir un bloc de données claire. Dans les algorithmes de chiffrement symétriques la clé de chiffrement est la même que celle utilisée pour le déchiffrement. Seuls les détenteurs de la clé secrète sont capables de transformer des données claires en données chiffrées et, inversement, des données chiffrées en données claires.

Les principaux algorithmes de chiffrement symétriques par bloc sont :

Nom	Taille de bloc	Taille de la clé
Advanced Encryption Standard (AES)	128 bits	128 ou 192 ou 256 bits
Twofish	128 bits	128 ou 192 ou 256 bits
Serpent	128 bits	128 ou 192 ou 256 bits
MARS	128 bits	128 ou 192 ou 256 bits
Camellia	128 bits	128 ou 192 ou 256 bits
GOST Magma	64 bits	256 bits
International Data Encryption Algorithm (IDEA)	64 bits	128 bits

En plus du choix de l'algorithme de chiffrement il faut également définir un mode opératoire. Un mode opératoire décrit comment appliquer de façon répétée l'opération de chiffrement d'un seul bloc pour chiffrer en toute sécurité des quantités de données supérieures à un bloc. Les cinq modes opératoires sont les suivants :

Nom	Détail
Electronic codebook (ECB)	Le message à chiffrer est subdivisé en plusieurs blocs qui sont chiffrés séparément les uns après les autres
Cipher Block Chaining (CBC)	Chaque bloc est additionné, avec un XOR, au chiffré du bloc précédent. L'opération est initialisée à l'aide d'un vecteur d'initialisation (IV)
Cipher Feedback (CFB)	À partir de la clé et d'un vecteur d'initialisation, ce mode génère un flux de clés qui est ensuite appliqué à chaque bloc de clair
Output Feedback (OFB)	Ce mode fonctionne selon le même principe que le CFB à la différence que chaque clé du flux est en plus chiffrée avec la clé précédente
Counter (CTR)	Comme OFB, le mode Compteur transforme un chiffrement par bloc en un chiffrement par flux. Il génère le flux de clés en chiffrant les valeurs successives d'un compteur

4.2 Chiffrement symétrique par flot

Les primitives de chiffrement par flot considèrent le message à chiffrer comme une suite de bits qui sont combinés à l'aide d'un XOR avec une séquence de bits dérivée de la clé secrète et d'un vecteur d'initialisation. Les primitives de chiffrement par flot sont particulièrement bien adaptées au chiffrement des flux de données continus (voix, vidéo).

Les principaux algorithmes de chiffrement symétriques par flot sont :

Nom	Taille du vecteur d'initialisation	Taille de la clé
HC-256	256 bits	256 bits
Rabbit	64 bits	128 bits
Salsa20	64 bits	256 bits
SOSEMANUK	128 bits	128 bits
RC4		40 – 2048 bits
E0		128 bits

4.3 Chiffrement asymétrique

Contrairement aux algorithmes de chiffrement symétriques, le chiffrement asymétrique s'appuie sur un ensemble de deux clés différentes. Ainsi la clef utilisée pour le chiffrement – la clé privée – est différente de celle utilisée pour le déchiffrement – la clé publique. Les deux clés sont mathématiquement liées entre elles de telle façon que la connaissance de la clé publique ne permet pas de retrouver la clé privée.

Les principaux algorithmes de chiffrement asymétriques sont :

Nom	Problème mathématique
RSA	Factorisation des entiers
Rabin	Factorisation des entiers
ElGamal	Logarithme discret dans un corps fini ou sur une courbe elliptique

4.4 Fonction de hachage cryptographique

Une fonction de hachage cryptographique a pour objectif de transformer, de manière déterministe, une suite de données de taille arbitraire en un condensat de taille fixée. La fonction de hachage cryptographique a les propriétés suivantes :

- Résistance à la préimage (fonction à sens unique) : à partir d'un condensat connu il est difficile de construire un message de même condensat ;
- Résistance à la seconde préimage, à partir d'un message connu il est difficile de construire un message différent ayant le même condensat ;
- Résistance aux collisions, il est difficile de construire deux messages différents ayant le même condensat.

Les principaux algorithmes de hachage cryptographiques sont :

Nom	Taille du hash
MD5	128 bits
SHA-1	160 bits
RIPE Message Digest (RIPEMD)	128, 160, 256 ou 320 bits
SHA-2	224, 256, 384, ou 512 bits
SHA-3	Variable

4.5 Code d'authentification de messages

La principale technique permettant d'assurer l'authentification des données consiste à calculer un code d'authentification de message (MAC) à partir des données à protéger et d'une clé secrète partagée avec le destinataire du message. Ce code d'authentification est ensuite ajouté au message à transmettre. Après réception, le code d'authentification est recalculé à l'aide de la clé secrète et du message reçu. Le résultat obtenu est comparé au MAC reçu. Si le MAC calculé et le MAC reçu sont identiques on peut raisonnablement affirmer que les données sont intègres et qu'elles proviennent de la bonne personne.

Les principaux algorithmes de code d'authentification de message sont :

Nom	Détail
CBC-MAC	Utilisation du DES ou de l'AES comme mécanisme de chiffrement. Vecteur d'initialisation nul
HMAC	Utilisation d'une fonction de hachage cryptographique en combinaison avec une clé secrète. (HMAC-MD5, HMAC-SHA-1, HMAC-SHA-3, etc.)
CMAC	Version plus sûre du CBC-MAC. Utilisation de l'AES

4.6 Défi-réponse

L'authentification par défi-réponse a pour objectif de prouver l'identité d'une entité. Le processus défi-réponse fait intervenir :

- Un demandeur qui doit prouver son identité pour pouvoir effectuer des actions ;
- Un receveur qui doit vérifier une identité avant d'autoriser une action ;
- Un canal de communication entre l'acteur et le receveur. Ce canal est réputé non sûr ;
- Une session authentifiée qui définit :
  - les capacités d'actions du demandeur,
  - un temps de validité au-delà duquel la session se termine.

En résumé, l'authentification d'une entité par défi-réponse permet de relier de façon fiable un demandeur et un receveur au travers d'un canal de communication dans le cadre d'une session authentifiée.

L'exemple le plus simple d'un protocole de défi-réponse est l'authentification par mot de passe, où le défi consiste à demander le mot de passe et la réponse valide est le mot de passe correct.

L'utilisation de mécanismes cryptographiques robustes est indispensable pour la mise en œuvre d'une authentification fiable. L'objectif étant d'éviter notamment, l'usurpation d'identité ou le rejeu d'une authentification.

Le défi-réponse permet l'authentification :

- D'un humain par une machine, par la saisie d'un mot de passe ou d'un code PIN, par la présentation d'un badge ou par la reconnaissance d'une caractéristiques biométriques… ;
- D'une machine par une autre machine, principalement par l'utilisation du protocole Internet Key Exchange (IKE) avec les méthodes d'authentification Pre-Shared Key (PSK), RSA certificates (RSA-SIG), Elliptic Curve Digital Signature Algorithm certificates (ECDSA-SIG) ou Extensible Authentication Protocol (EAP) ;
- D'un humain par un autre humain, obtenue en symétrisant le modèle d'authentification d'un humain par une machine.

Les mécanismes interactifs d'authentification d'entités reposent sur des algorithmes de génération d'aléa, de hachage cryptographiques, de chiffrement ou de signature numériques. Les règles énoncées pour ces mécanismes s'appliquent donc directement.

4.7 Signature numérique

Les protocoles de signature numérique s'appuient sur la combinaison d'algorithmes de cryptographie asymétrique et de fonction de hachage cryptographique pour garantir l'intégrité d'un message, la non-répudiation d'une action ou l'authentification.

Les principaux algorithmes de signatures numériques sont :

Nom	Principe
Digital Signature Algorithm (DSA)	Exponentiation modulaire et problème du logarithme discret
RSA	Factorisation des entiers
Elliptic Curve Digital Signature Algorithm (ECDSA)	Variante de DSA basée sur les courbes elliptiques