Arrêté Ministériel n° 2018-636 du 2 juillet 2018 portant application de l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu la loi n° 1.383 du 2 août 2011 sur l'Économie Numérique ;

Vu l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, et notamment son article 54 ;

Vu l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu l'Ordonnance Souveraine n° 6.525 du 16 août 2017 portant application des articles 18, 19 et 25 de la loi n° 1.383 du 2 août 2011 sur l'Économie Numérique, modifiée ;

Vu l'arrêté ministériel n° 2017-56 du 1er février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2018-634 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2018-635 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu la délibération du Conseil de Gouvernement en date du 20 juin 2018 ;

ARRÊTONS :

ARTICLE PREMIER.

Les règles et recommandations concernant les mécanismes d'authentification, énoncées au chiffre 1 du paragraphe 8 du Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, sont définies dans l'annexe au présent arrêté.

ART. 2.

Le Ministre d'État, le Conseiller de Gouvernement-Ministre de l'Équipement, de l'Environnement et de l'Urbanisme, le Conseiller de Gouvernement-Ministre des Finances et de l'Économie, le Conseiller de Gouvernement-Ministre des Relations Extérieures et de la Coopération, le Conseiller de Gouvernement-Ministre de l'Intérieur et le Conseiller de Gouvernement-Ministre des Affaires Sociales et de la Santé sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le deux juillet deux mille dix-huit.

Le Ministre d'État,
S. TELLE.

RÈGLES ET RECOMMANDATIONS CONCERNANT LES MÉCANISMES D'AUTHENTIFICATION

Annexe à l'Arrêté Ministériel n° 2018-636 du 2 juillet 2018

SOMMAIRE

1. Introduction

1.1. Contexte

1.1.1. Objectif de l'annexe

La présente annexe présente une modélisation permettant de décrire ou d'évaluer les mécanismes d'authentification et de conseiller sur les « meilleures pratiques » à suivre en matière d'authentification lors de l'élaboration d'un système d'information.

Elle est principalement destinée aux développeurs de produits de sécurité utilisant des fonctions d'authentification pour les aider à réaliser ces fonctions de sécurité.

La lecture de la présente annexe présuppose que le lecteur est familier avec les concepts utilisés en cryptographie.

La présente annexe ne traite que la fonction d'authentification. L'identification est considérée comme acquise et l'identité est connue par le biais d'un identifiant préalablement enregistré. De même, elle ne traite pas des méthodes d'identification consistant à reconnaître dans un ensemble d'identifiants connus, celui qui correspond à une entité donnée.

La signature électronique n'est pas l'objet de la présente annexe.

1.1.2. Rôle de l'authentification

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. L'authentification est toujours précédée ou combinée avec une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant.

S'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant.

L'authentification vise :

- soit à contrôler l'accès à des informations, des locaux, plus généralement des biens d'un système d'information, en étant dans ce cas associée à une fonction d'attribution de privilèges particuliers liés à l'identité de l'entité ;
- soit à garantir une imputabilité avec vérification forte de l'identité affichée, par exemple pour la journalisation d'actions, la facturation de communications, l'authentification de données, etc. ;
- soit à assurer une combinaison de ces fonctions d'attribution de privilèges et d'imputation.

Dans tous les cas, l'utilisation de mécanismes d'authentification sûrs est nécessaire à la réalisation de ces objectifs, mais la sécurité globale de l'authentification doit évidemment reposer également sur d'autres mesures relatives au système d'information dans sa globalité (sécurité physique, intégrité des logiciels, qualité des développements applicatifs, etc.) qui ne sont pas l'objet de la présente annexe.

1.1.3. Typologie des fonctions d'authentification

La fonction « authentification » permet l'attribution (pour autorisation ou imputation) d'une action à son auteur réel ou, que l'entité qui agit est bien celle que l'on a authentifiée. On distingue deux grands types de solutions :

- l'acte signé pour lequel le lien entre l'authentification et l'action est direct et intemporel ;
- la session authentifiée, pour laquelle l'authentification intervient ponctuellement en début de session, avant la première action, et qui nécessite par là même une traçabilité entre l'ouverture et le déroulement de la session pendant toute sa durée.

Toutefois, le fait même que l'authentification puisse conduire à imputer des actions à une personne identifiée nécessite que cette fonction soit correctement implantée et que l'utilisateur qui s'authentifie ne la considère pas comme une opération anodine.

1.1.4. Positionnement de l'annexe

La présente annexe vient en complément de l'annexe à l'arrêté ministériel n° 2018-635 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée définissant les « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographique ».

Par ailleurs, l'enregistrement éventuel de l'utilisateur dans le système d'authentification et la mise à disposition des éléments cryptographiques nécessaires ne sont pas couverts dans la présente annexe. Ce problème général est traité dans l'annexe à l'arrêté ministériel n° 2018-637 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée concernant les « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

La présente annexe décrit des règles et des recommandations relatives aux mécanismes d'authentification.

- Les **règles** définissent des principes qui doivent être suivis par tout mécanisme. L'observation de ces règles est une condition nécessaire, mais non suffisante, à la reconnaissance du bon niveau de sécurité du mécanisme. Inversement, le fait de suivre l'ensemble des règles, qui sont par nature très génériques, ne garantit pas la robustesse ; seule une analyse spécifique permet de s'en assurer.
- Les recommandations ont pour but de guider dans le choix de certains mécanismes d'authentification permettant un gain important en termes de sécurité. Il va de soi qu'en tant que recommandations, leur application peut être librement modulée en fonction d'autres impératifs tels que des contraintes de performance, d'ergonomie ou de coût.

1.1.5. Mise à jour de l'annexe

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en fonction des évolutions techniques, législatives et règlementaires en matière de sécurité des systèmes d'information. Ladite mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1.2. Modèle de la fonction d'authentification

1.2.1. Préambule

Il est habituel de faire reposer l'authentification sur un ou plusieurs éléments parmi :

- ce que l'on sait (par exemple, un mot de passe) ;
- ce que l'on a (par exemple, une carte à puce) ;
- ce que l'on est (par exemple, une empreinte digitale) ;
- ce que l'on sait faire (par exemple, une signature manuscrite).

Ces deux derniers éléments d'authentification ne s'appliquent pas à des dispositifs automatiques. Deux modèles sont traités ci-après, selon que l'authentification aura lieu entre machines ou s'il s'agit de l'authentification d'une personne vis-à-vis d'une machine.

L'authentification ne peut s'effectuer qu'après une installation préalable de clés cryptographiques ou d'informations partagées entre les acteurs concernés du système d'information.

La présente annexe ne concerne pas les processus d'enregistrement d'un utilisateur dans une entité organisatrice, mais concerne les moyens techniques et cryptographiques à mettre en place suite à cet enregistrement, pour que l'utilisateur puisse ensuite être authentifié correctement lors de l'utilisation du système d'information.

1.2.2. Modèle général du processus d'authentification

1.2.2.1. Définitions

Sont indiquées en gras et soulignées, lors de leur définition, les différentes notions utilisées par le modèle. Celles-ci sont ensuite mentionnées en italique pour rappeler qu'il s'agit de notions définies dans le modèle.

La réalisation des fonctions contrôle d'accès et imputation fait intervenir :

- un **demandeur**, qui souhaite effectuer des **actions** et doit pour cela prouver son **identité**,
- un **receveur**, qui peut permettre les *actions*, en devant au préalable vérifier l'*identité* de leur *auteur*.

La suite des actions circule sur un canal reliant le demandeur au receveur. L'authentification permet de relier de façon fiable, pour le receveur, les actions circulant sur ce canal à l'identité du demandeur.

Le temps d'exploitation du canal par le demandeur constitue une session authentifiée. Cette session peut se terminer :

- à l'initiative du demandeur ou,
- à l'initiative du receveur, s'il estime qu'il n'est plus en mesure de garantir le lien entre les actions véhiculées sur le canal et l'identité du demandeur.

    - Le modèle n'interdit pas que la *session authentifiée* soit de durée infinie.
    - S'agissant d'un modèle, il convient de ne pas confondre le *canal* avec le vecteur de transmission de données utilisé. Les données d'authentification échangées entre le *demandeur* et le *receveur* peuvent emprunter un chemin différent de celui des *actions*.

1.2.2.2. États constitutifs d'une authentification

On distingue :

- un état initial, non authentifié, dans lequel le receveur interdit les actions ;
- une phase de **connexion**, c'est-à-dire d'ouverture du canal, qui constitue le contrôle de l'identité du demandeur par le receveur ;
- un état authentifié d'une certaine durée, constituant la session authentifiée pendant laquelle les actions sont autorisées par le receveur ;
- une phase de **déconnexion** permettant le retour à l'état initial.

Tous les états peuvent potentiellement engendrer une erreur qui peut générer une alarme. Les transitions entre états, quant à elles, dépendent du contexte. Les états successifs constitutifs de l'authentification sont présentés dans la figure 1.

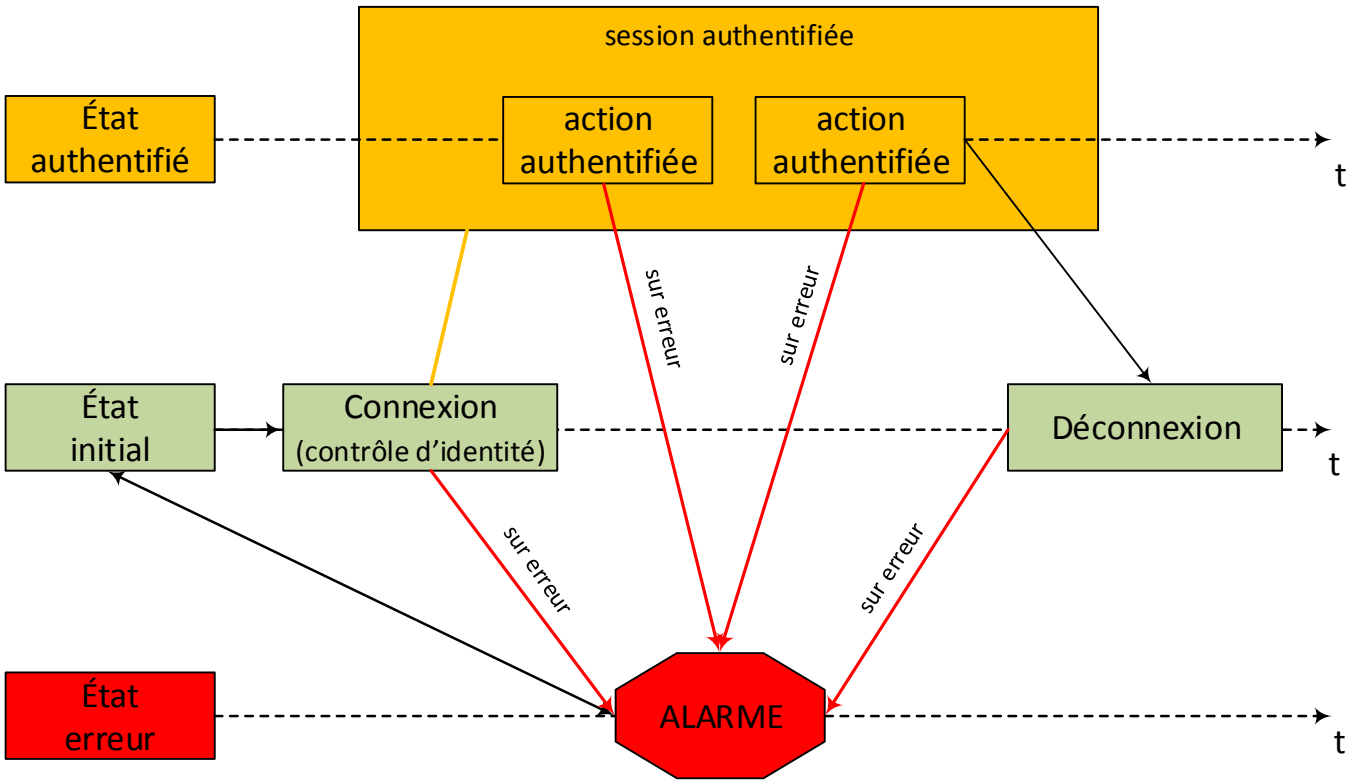

Figure 1 : États constitutifs d'une authentification

Dans beaucoup de cas, l'authentification nécessite de sécuriser le canal par un échange de clés cryptographiques au moment de la connexion. L'ensemble de la session utilise alors ces clés pour se protéger en intégrité et si besoin en confidentialité.

Même si les termes employés sont effectivement inspirés de modes de communication connectés car ils correspondent à beaucoup des applications visées, le canal ne doit pas être confondu avec les vecteurs utilisés pour transporter les données. L'opération de connexion du présent modèle est donc une opération virtuelle qui correspond dans un cas concret à une ou plusieurs opérations physiques ou mathématiques impliquant le demandeur, qui peut lui même être constitué de plusieurs entités (personnes ou machines).

De même, la session authentifiée peut être excessivement courte et les processus de connexion et de déconnexion peuvent ne pas correspondre à des opérations cryptographiques.

1.2.3. Applications du modèle général

L'un des objectifs recherchés par la présente proposition de modélisation est d'encourager à bien identifier dans un système d'information quelles sont les opérations constitutives de l'authentification.

Déterminer dans le système d'information : qui joue le rôle de demandeur ou de receveur, quelles sont les opérations liées à la connexion, quelles sont les actions véhiculées par quel canal, etc. permet de mieux discerner les objectifs de sécurité associés à la fonction globale d'authentification. Il devient ensuite possible de vérifier que les objectifs de sécurité sont bien couverts par des mécanismes de sécurité dont la robustesse peut être évaluée.

Des modèles plus proches de réalités concrètes d'implantation, proposés ci-après, permettent de faire des recommandations sur les mécanismes de sécurité à mettre en place.

1.2.3.1. Authentification de machines

1.2.3.1.1. Modèle d'authentification de machines

Dans la suite trois entités sont distinguées :

- l'environnement de confiance local ;
- le système d'information distant ;
- le système d'information (SI) d'authentification de confiance.

L'environnement de confiance local est le demandeur, à savoir la machine qui s'authentifie auprès du SI distant, le receveur. Ce terme « environnement de confiance » est choisi en cohérence avec l'annexe à l'arrêté ministériel n° 2018-637 du 2 juillet 2018 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée définissant les « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

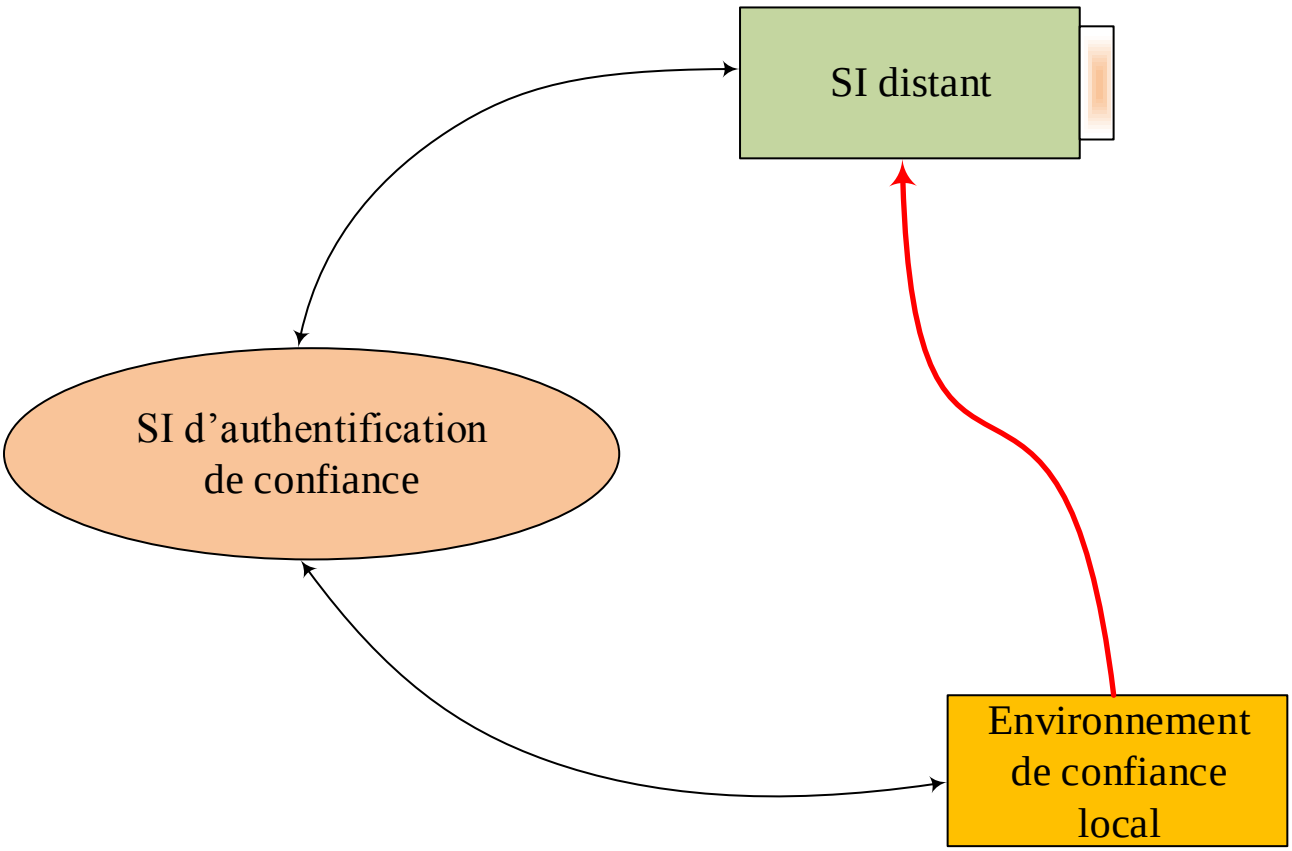

Figure 2 : Modèle d'authentification de machines

Le modèle de la figure 2 introduit aussi un SI d'authentification de confiance avec lequel les deux systèmes d'information sont en interaction. L'existence de ce système n'est pas obligatoire. S'il est présent, alors :

- Le SI distant doit faire confiance au SI d'authentification de confiance pour authentifier l'environnement de confiance local.
- L'environnement de confiance local fait confiance au SI d'authentification de confiance pour la protection des éléments d'authentification qu'il lui transmet.

Il peut s'agir, d'un portail d'authentification (single-sign-on) qui authentifierait l'environnement de confiance local pour le compte du SI distant et dont la réponse serait elle-même authentifiée par le SI distant.

Dans cette représentation, les différentes flèches représentent les canaux authentifiés possibles entre les entités. Le canal d'authentification principal (flèche rouge) relie le demandeur au receveur. Les autres canaux nécessitent dans la plupart des cas d'être authentifiés pour garantir la sécurité de l'authentification du canal principal. Ces interactions peuvent être des communications, mais aussi des relations de confiance établies, par exemple, par un enrôlement. Ces interactions ne sont pas obligatoires.

À titre d'exemple on peut chercher à appliquer ce modèle à un client et un serveur de fichiers reliés par une liaison IPSEC configurée manuellement à l'aide d'un secret partagé. Le serveur joue le rôle de SI distant contrôlant l'accès aux fichiers, tandis que le client est l'environnement de confiance local. La configuration étant manuelle, il n'y a pas de SI d'authentification de confiance.

De même, on peut appliquer le modèle à une situation similaire impliquant un client et un serveur de fichiers reliés en IPSEC, mais cette fois-ci utilisant une infrastructure de clés publiques et un protocole d'échange de clés Diffie-Hellman signé. Le modèle comprend alors en plus l'infrastructure de clés publiques qui joue le rôle de SI d'authentification de confiance. Elle participe à l'authentification mutuelle par la certification du client et du serveur.

Pour vérifier le caractère général du modèle, on peut aussi envisager un système de contrôle d'accès physique utilisant un badge sans contact. On y trouve :

- un environnement de confiance local, le badge sans contact, demandeur ;
- un SI distant, le dispositif de verrouillage de la porte, receveur ;
- un SI d'authentification, le serveur qui gère les droits d'accès en fonction de l'identité annoncée par le badge.

On voit bien sur ce cas qu'il n'y a pas authentification du porteur du badge. C'est uniquement ce dispositif qui est authentifié. En outre, on peut imaginer plusieurs scénarios de contrôle d'accès :

- Le badge s'authentifie auprès du SI d'authentification qui vérifie les droits d'accès et donne un signal au SI distant pour ouvrir la porte. Ce signal est dans ce cas « authentifié » soit par un mécanisme cryptographique soit par la sécurité physique de la connexion entre le SI d'authentification et le SI distant.
- Le badge s'authentifie auprès du SI distant qui demande ensuite au SI d'authentification si l'identité annoncée est autorisée ou pas. Là encore, la sécurité de la transmission entre le SI distant et le SI d'authentification peut être assurée par divers mécanismes.

1.2.3.1.2. Règles et recommandations applicables à l'authentification de machines

Les règles et recommandations concernant l'application de ce modèle font l'objet du point 2.1. Elles s'appliquent au canal de transmission entre l'environnement de confiance local et le SI distant qui est réputé non sûr, c'est-à-dire que la flèche rouge de la figure 2 est soumise à des menaces d'interception, d'altération, d'écoute, de rejeu, etc. Il est évident que toute réalisation pratique peut, par une analyse de risque, estimer que ce canal est sûr et dans ce cas aboutir à la conclusion qu'il n'est pas nécessaire de mettre en œuvre ces recommandations. Le retour d'expérience observé sur certains cas concrets laisse toutefois à penser que même dans le cas de canaux de transmission réputés sûrs, il est largement préférable pour la sécurité d'adopter une stratégie de défense en profondeur en mettant en œuvre les mécanismes proposés. En effet, la simple imputabilité des actions qui en découle est de nature à améliorer la sécurité globale.

Les flèches noires de la figure 2 correspondent à l'utilisation d'un tiers de confiance. Ce cas est traité au point 2.1.3.1.2.

Le caractère authentique de ces flux est indispensable à l'authentification du flux principal. Par conséquent, de façon indirecte, si ces flux sont véhiculés par des canaux de transmission non sûrs, les règles et recommandations du flux principal vont également leurs êtres applicables.

1.2.3.2. Authentification d'une personne vis-à-vis d'une machine

1.2.3.2.1. Modèle d'authentification d'une personne vis-à-vis d'une machine

L'authentification d'une personne vis-à-vis d'un système d'information est délicate à réaliser de façon directe. En effet, du point de vue de la machine, seul un procédé de nature cryptographique s'avère sûr, tandis que la personne, quant à elle, ne peut directement employer un tel mécanisme.

Les procédés « d'authentification » directe d'une personne se caractérisent tous par la possibilité de rejeu. Il est rare qu'une personne change systématiquement de mot de passe à chaque utilisation[1] et les procédés de nature biométrique ou comportementale utilisent tous, au contraire, le rejeu pour fonctionner. Il n'y a pas de mécanisme humainement exploitable permettant une authentification sans rejeu[2].

Pour bien les distinguer, ces procédés seront qualifiés de **déverrouillage**. En effet, ces procédés permettent dans la plupart des cas d'accéder à des ressources soumises, là encore, à un contrôle d'accès.

Parmi les procédés de déverrouillage, caractérisés par la possibilité de rejeu, existent :

- la saisie d'un mot de passe, qui déverrouille un ordinateur ;
- la présentation d'un badge personnel, qui « déverrouille » ce dernier en le rendant accessible aux opérations de vérification ;
- l'insertion d'un support amovible, qui donne l'accès aux données qu'il contient ;
- la saisie d'un PIN code, qui active des fonctionnalités d'une carte à puce ;
- la reconnaissance d'une caractéristique biométrique ;
- etc.

Le modèle décrit complète le précédent en faisant apparaître l'utilisateur (voir figure 3).

[1] En tout cas tant qu'elle n'est pas assistée par un dispositif technique.

[2] Les procédés de type calculette délivrant un mot de passe à usage unique sont typiquement des systèmes d'information réalisant pour le compte de l'utilisateur une opération cryptographique.

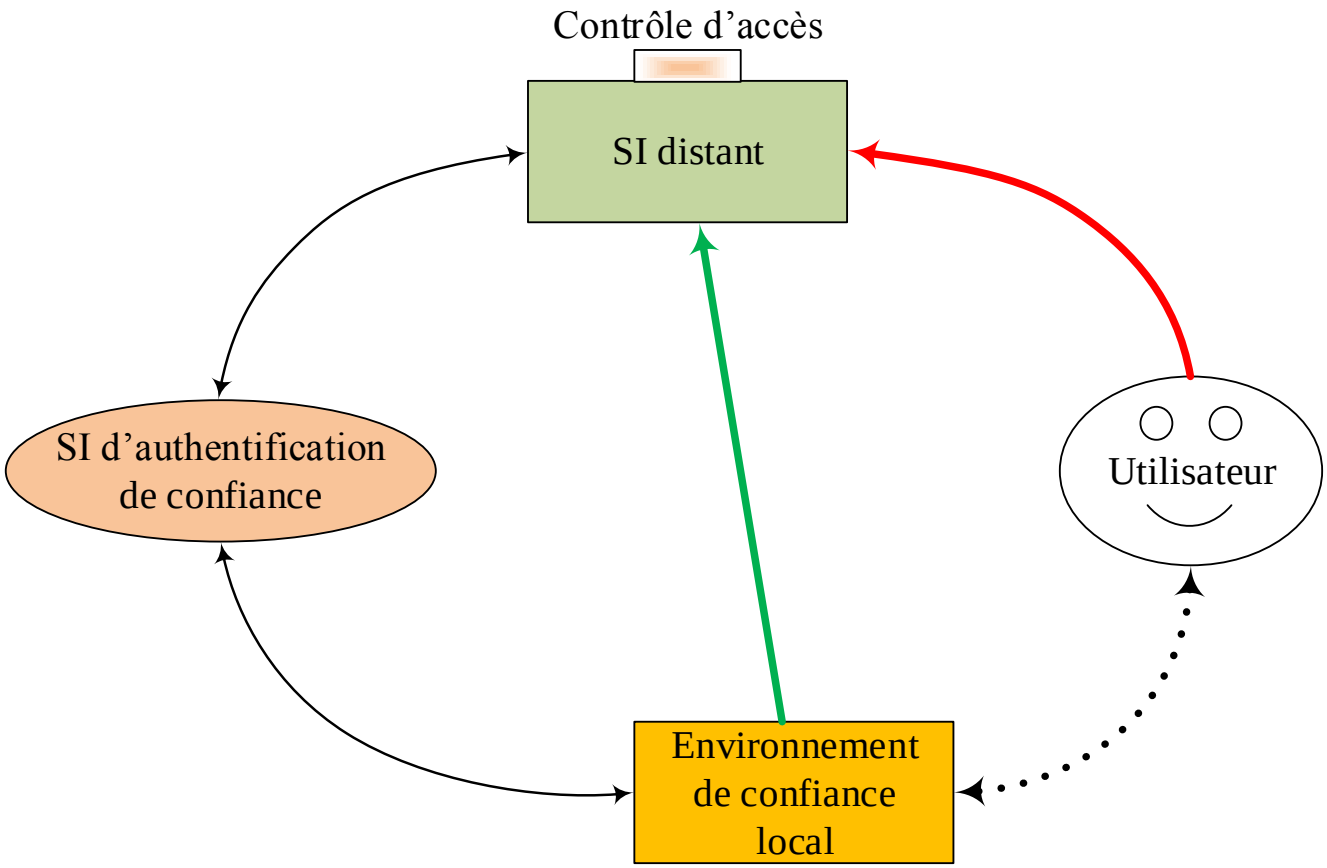

Figure 3 : Modèle d'authentification de personne

Dans ce modèle, c'est l'utilisateur qui s'authentifie, mais les droits d'accès qui seront ainsi ouverts, le seront vis-à-vis du SI distant pour l'environnement de confiance local, lequel effectuera les actions au bénéfice de l'utilisateur. L'authentification s'effectue donc de machine à machine entre l'environnement de confiance local et le SI distant, mais grâce à un déverrouillage de l'environnement de confiance local par l'utilisateur.

Premier cas : accès d'un client local à un serveur de fichiers en introduisant l'utilisateur de la machine locale. Le client va déverrouiller localement la machine avec un mot de passe, ce qui permet l'utilisation des informations secrètes stockées sur la machine locale dont le verrouillage est contrôlé par le système d'exploitation local. On voit que la machine locale joue le rôle d'environnement de confiance local. Elle héberge également les informations secrètes de l'utilisateur qui constituent le support d'authentification de l'utilisateur.

Par la suite, l'environnement de confiance local utilisera ces données pour authentifier l'utilisateur auprès du SI distant (le serveur) et lui permettre d'accéder aux fichiers.

Deuxième cas : un contrôle d'accès physique, mais en faisant cette fois-ci apparaître l'utilisateur. C'est l'utilisateur qui est demandeur de l'ouverture d'un canal authentifié : la porte. Pour cela, il utilise un support, le badge, qui va obtenir pour lui l'ouverture du loquet de la porte. Le receveur, le SI distant, est par définition chargé de garantir l'authenticité des actions transitant par le canal « porte ». C'est la raison pour laquelle, il peut, par exemple, commander la fermeture du loquet au bout de quelques secondes s'il estime qu'il n'a plus de garantie d'authenticité entre l'identité authentifiée au départ et la personne qui a effectivement la possibilité de franchir la porte.

Dans ce cas, plusieurs mécanismes de déverrouillage sont possibles :

- la simple présentation du badge est un mécanisme de déverrouillage, puisque elle met le badge en situation d'activité ;
- si le badge dispose d'un code PIN, la saisie du code est une opération de déverrouillage ;
- une caractéristique biométrique peut être utilisée pour déverrouiller le badge ;
- un système de mots de passe à usage unique générés par le badge peut être utilisé et, dans ce cas, c'est l'activation du mécanisme de génération et/ou la saisie du mot de passe généré qui constituent le déverrouillage.

On voit toutefois que tous les mécanismes de déverrouillage n'ont pas la même robustesse, notamment par rapport à la menace de perte ou de vol du badge.

Troisième cas : accès d'un client local à un serveur de fichiers par un support de clés de type clé USB de stockage de masse, sans capacité de calcul. Dans ce cas, les données secrètes ne peuvent être accédées de l'environnement de confiance local que si le support est présent, ce qui constitue le déverrouillage de l'environnement de confiance local. Ce mécanisme peut être amélioré en chiffrant les données sur la clé à l'aide d'un mot de passe. Dans ce cas, le déverrouillage consiste à introduire le support ET à saisir un mot de passe.

Pour l'accès d'un client local à un serveur de fichiers : si le support est une carte à microprocesseur, alors on peut laisser la ressource effectuer les calculs cryptographiques. L'environnement de confiance local n'a dans ce cas jamais accès aux clés qui lui permettent d'obtenir l'ouverture du canal. Le mécanisme de déverrouillage reste dans ce cas la présentation du support. Il peut être amélioré si la carte contrôle elle-même un code PIN. On peut également demander à ce que ce code PIN ne soit pas accessible à l'environnement de confiance local, par exemple par l'emploi d'un lecteur sécurisé. Certains systèmes vont même jusqu'à un triptyque : poste local, lecteur intelligent, support carte à mémoire. Le déverrouillage de l'environnement de confiance local est alors plus complexe : il implique une authentification de machines entre le lecteur et la carte, qui est elle-même déverrouillée par un code PIN.

Enfin, cas de l'accès distant à un serveur par un système à mot de passe unique. Dans ce cas, l'utilisateur dispose d'une calculette qui lui fournit son mot de passe. Ce dernier est saisi par l'utilisateur sur l'interface d'accès du serveur distant. Le mot de passe calculé peut résulter de l'application d'une fonction cryptographique à un challenge généré par le serveur, ou de la synchronisation antérieure d'un générateur de pseudo-aléa entre le serveur et la calculette. Dans ce cas, l'environnement de confiance local est constitué du poste d'accès ET de la calculette. Le déverrouillage de l'utilisateur consiste à assembler ces deux composants par la saisie croisée du challenge sur la calculette et du mot de passe à usage unique sur le poste d'accès.

1.2.3.2.2. Règles et recommandations applicables à l'authentification d'une personne vis-à-vis d'une machine

Les règles et recommandations concernant l'application de ce modèle font l'objet du point 2.2. Elles s'appliquent au canal de transmission entre l'environnement de confiance local et l'utilisateur, c'est-à-dire la flèche en pointillés noirs de la figure 3. La flèche verte de la figure 3 est évidemment supposée soumise à des menaces d'interception, d'altération, d'écoute, de rejeu, etc. Les règles et recommandations du point 2.1 lui seront donc applicables.

L'authentification de l'utilisateur vis-à-vis du système distant (flèche rouge de la figure 3) résulte de ces différentes règles et des procédures d'enregistrement et de gestion des clés de l'utilisateur dans le système qui ne sont pas l'objet de la présente annexe (cf. § 1.1.4).

1.2.3.3. Authentification de personnes de bout-en-bout

L'authentification de bout-en-bout de deux personnes ne nécessite pas de règle supplémentaire. Elle peut en effet être modélisée en symétrisant le modèle précédent (voir figure 4). L'authentification mutuelle des utilisateurs distants (flèche rouge de la figure 4) résulte de la double authentification des utilisateurs vis-à-vis des SI (flèches orange de la figure 4) et de la confiance de chaque utilisateur dans son propre SI du fait des mécanismes de déverrouillage utilisés (flèches en pointillés noirs de la figure 4).

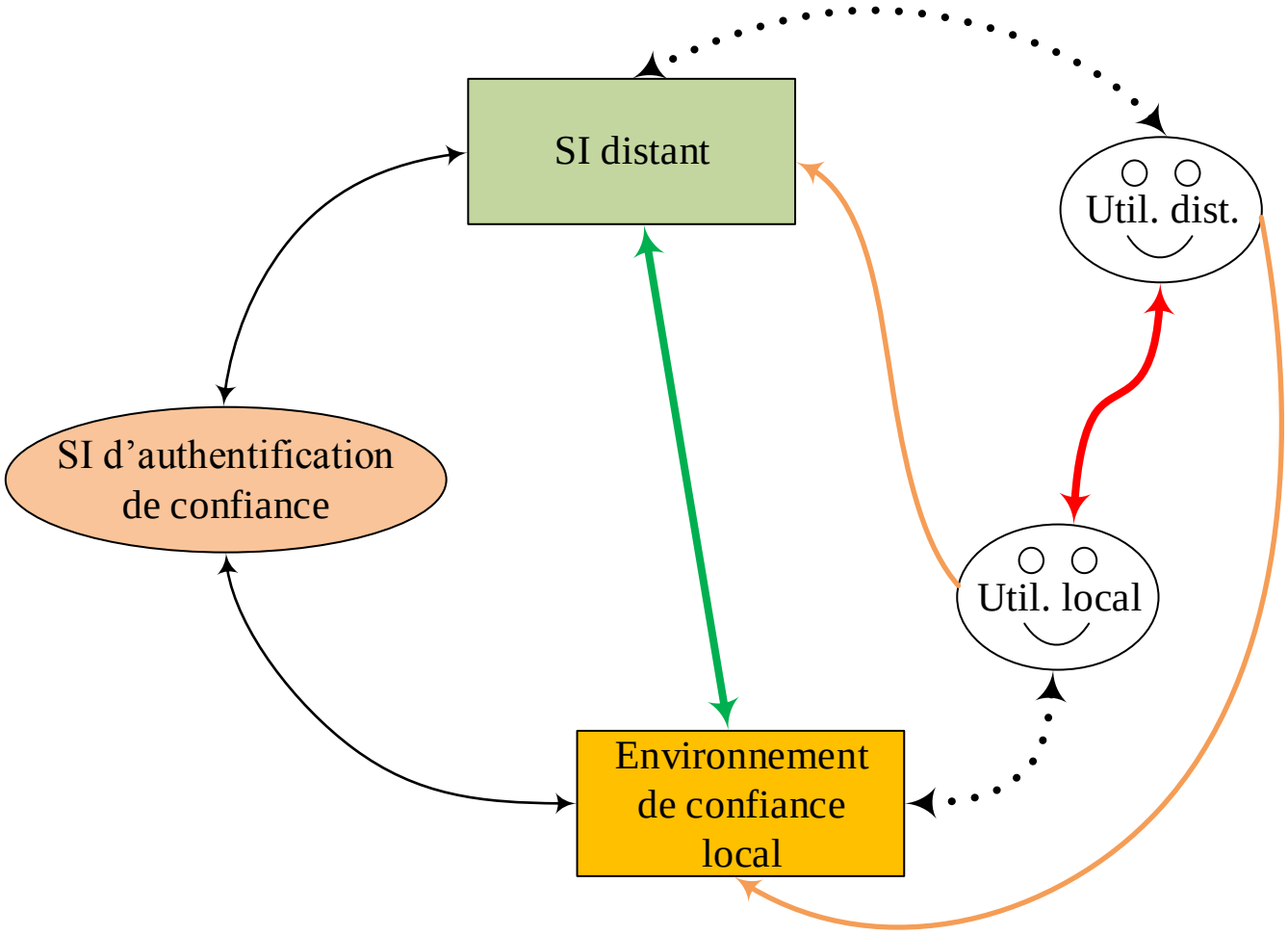

Figure 4 Modèle d'authentification de bout-en-bout

2. Règles et recommandations

Les ***règles*** et ***recommandations*** sont repérées selon la codification suivante : les premières lettres (Règle ou Recom) indiquent si l'on a affaire à une règle ou une recommandation, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

2.1. Authentification de machines

2.1.1. Mécanismes cryptographiques

L'utilisation de mécanismes cryptographiques robustes est indispensable pour espérer atteindre une bonne authentification en évitant l'usurpation d'identité ou le rejeu d'une authentification. Ils mettent en œuvre une preuve de possession d'un élément secret (clé cryptographique) par l'intermédiaire d'un protocole d'authentification garantissant la confidentialité de l'élément secret.

Une autre propriété recherchée pour un protocole d'authentification est qu'il doit être impossible pour un attaquant, même s'il récupère les données secrètes d'authentification, de déchiffrer ou de modifier les communications d'une session qu'il n'a pas ouverte.

- Les mécanismes utilisant des mots de passe sous une forme quelconque (pass-phrase, code d'identification personnel, …) ainsi que les mécanismes s'appuyant sur des procédés biométriques ne sont pas de nature cryptographique. Bien entendu, ceci ne signifie pas qu'ils ne présentent aucun intérêt dans un processus d'authentification, mais nous les distinguons dans la présente annexe en parlant de mécanisme de déverrouillage.
- Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Pour un système d'authentification par mot de passe, si le haché du mot de passe est simplement transmis, alors il est possible de simuler le comportement de l'environnement de confiance local sans disposer du mot de passe originel.

Les mécanismes interactifs d'authentification d'entités reposent en général sur des mécanismes symétriques ou asymétriques de génération d'aléa, de hachage, de chiffrement ou de signature ; les règles énoncées par ailleurs pour ces mécanismes s'appliquent donc directement.

L'évaluation du niveau de robustesse du mécanisme global d'authentification doit être effectuée avec soin, même si des primitives de niveau compatible sont employées.

Règle-Protocole. L'authentification entre deux machines doit faire intervenir un protocole cryptographique conforme au Référentiel Général de Sécurité.

L'authentification de deux machines est un processus automatique qui doit s'appuyer sur un protocole interactif pour être sûr. Entre deux machines, seul un procédé cryptographique permet d'éviter l'usurpation d'identité. Tout autre procédé ne peut être considéré comme un procédé d'authentification. La simple présentation d'un élément, même si son intégrité est garantie par une signature, ne saurait constituer un mécanisme d'authentification robuste du fait des possibilités de rejeu. Dans la présente annexe, nous parlons dans ce cas de déverrouillage.

2.1.2. Gestion de clés

À partir du moment où un mécanisme cryptographique est nécessaire pour l'authentification, une gestion des clés cryptographiques doit être mise en place. Cette gestion peut faire intervenir des outils techniques, des mesures organisationnelles ou des combinaisons de ces moyens. En matière d'authentification, la gestion des clefs doit permettre d'interdire à un environnement de confiance local corrompu de se connecter sans pour autant perturber le fonctionnement du SI distant.

Ne sont pas reprises ici les « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques » ; elles s'appliquent directement aux mécanismes cryptographiques employés dans les protocoles d'authentification interactifs du point 2.1.1 ci-dessus.

Règle-GestionClés. L'authentification entre deux machines doit faire intervenir une infrastructure de gestion des clés du protocole cryptographique utilisé conforme aux arrêtés ministériels découlant du Référentiel Général de Sécurité.

2.1.3. États du processus d'authentification

2.1.3.1. Connexion

2.1.3.1.1. Authentification intrinsèque

Il est préférable, lorsque c'est possible, que l'authentification soit intrinsèquement requise plutôt qu'artificiellement imposée, c'est-à-dire qu'un mécanisme de contrôle d'accès défaillant ne puisse donner l'accès en l'absence d'authentification.

Recom-AuthIntrinsèque. Il est recommandé que dans un système d'authentification entre deux machines, la défaillance du SI distant ou sa prise de contrôle par un adversaire malfaisant ne permette pas l'accès direct aux actions contrôlées.

2.1.3.1.2. Tiers de confiance

Règle-TiersDeConfiance-1. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors les mécanismes d'authentification du système local vis-à-vis de ce tiers de confiance doivent être conformes au Référentiel Général de Sécurité.

Règle-TiersDeConfiance-2. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors les mécanismes d'authentification du système distant vis-à-vis de ce tiers de confiance doivent être conformes au Référentiel Général de Sécurité.

Recom-TiersDeConfiance. Si un tiers de confiance est utilisé de façon directe pour une authentification entre deux machines, alors il est recommandé que les mécanismes d'authentification du système distant vis-à-vis de ce tiers de confiance respectent de plus l'ensemble des recommandations du Référentiel Général de Sécurité.

2.1.3.2. Session authentifiée

Si l'authentification sert à établir un accès à des données confidentielles, le canal ouvert doit être protégé en intégrité et en confidentialité. On fera en particulier attention à la suppression ou au rejeu des échanges en protégeant l'intégrité de l'intégralité des communications. De plus, le lien entre l'authentification et l'échange de clés qui va permettre de sécuriser les communications doit être effectué avec précaution.

Recom-Confidentialité. Si une authentification est utilisée pour contrôler l'accès à des données confidentielles, alors il est recommandé que la session authentifiée permette la mise en place d'un mécanisme cryptographique conforme au Référentiel Général de Sécurité, assurant la confidentialité et l'intégrité de ces données.

2.1.3.3. Déconnexion

2.1.3.3.1. Effacement

La sécurité du processus d'authentification repose souvent sur la confidentialité des éléments temporaires échangés au cours du protocole d'authentification. Il est donc important que les développeurs soient attentifs à l'effacement de ces données dès lors qu'elles ne sont plus utilisées.

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

Recom-MémoireVolatile. Il est recommandé que les éléments secrets échangés lors de la connexion d'une session authentifiée soient uniquement stockés en mémoire volatile et jamais sur un support magnétique.

2.1.3.3.2. Inactivité

Dans une session authentifiée, il est souhaitable d'incorporer un dispositif de déconnexion automatique en cas d'inactivité.

Recom-Inactivité. Au cours d'une session authentifiée, il est recommandé d'incorporer un dispositif de déconnexion automatique en cas d'inactivité.

2.1.4. Audit

Pour détecter une utilisation frauduleuse il est nécessaire que puissent être consultées les traces des authentifications réussies. En outre, tous les états d'une session authentifiée peuvent potentiellement engendrer une erreur qui peut révéler un comportement anormal, voire une tentative d'usurpation d'identité. De même, les transitions entre états, quant à elles, dépendent du contexte et peuvent aussi être le révélateur d'anomalies.

Règle-Audit. Toute erreur survenant au cours d'une session authentifiée doit générer une trace d'alarme ne pouvant être modifiée ni effacée.

Recom-Audit. Il est recommandé que toute transition d'état survenant au cours d'une session authentifiée génère une trace d'alarme ne pouvant être modifiée ni effacée.

2.2. Authentification de personnes

Rappelons encore une fois ici que les règles et recommandations ci-dessous ne s'appliquent pas à la problématique de la signature électronique qui répond à des enjeux différents. En effet, nous cherchons ici à définir les mécanismes de sécurité applicables à la protection d'une session authentifiée qui, par nature, est limitée dans le temps, alors que la signature électronique doit protéger l'intégrité et l'authenticité d'une donnée dans la durée.

2.2.1. Utilisation d'un environnement de confiance local

Règle-Authentification. L'authentification d'un utilisateur auprès d'un SI distant doit faire intervenir un environnement de confiance local déverrouillé par l'utilisateur et réalisant, pour son compte, une authentification de machine à machine conforme au Référentiel Général de Sécurité.

Remarque :

La simple utilisation à distance d'un mécanisme de déverrouillage ne saurait constituer un dispositif d'authentification.

Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Pour un système d'authentification par mot de passe, si le haché du mot de passe est simplement transmis, alors il est possible de simuler le comportement de l'environnement de confiance local sans disposer du mot de passe originel.

La faiblesse intrinsèque d'un mécanisme de déverrouillage réside dans le fait que l'utilisateur ne peut, de façon ergonomique, que répéter une même opération (saisie de mot de passe, empreinte biométrique, etc.) à chaque nouvelle occurrence. Dans une authentification à distance, ceci ouvre des possibilités de fraude d'ores et déjà largement employées dans le hameçonnage, qui visent à récupérer les informations rejouées par l'utilisateur à chaque nouvelle authentification.

Recom-Périmètre. Dans une authentification distante d'un utilisateur, il est recommandé que le périmètre physique de l'environnement de confiance local utilisé pour réaliser l'authentification de machine avec le SI distant reste sous le contrôle de l'utilisateur.

Recom-Cloisonnement. Dans une authentification distante d'un utilisateur, il est recommandé que les fonctions employées par l'environnement de confiance local pour réaliser l'authentification de machine avec le SI distant soient cloisonnées des autres fonctions de l'environnement de confiance local.

Recom-CloisonnementPhysique. Dans une authentification distante d'un utilisateur, il est recommandé que l'utilisation d'un support physique amovible soit indispensable à l'environnement de confiance local pour utiliser les clés cryptographiques nécessaires à l'authentification de machines avec le SI distant.

Recom-InterdictionAccèsClés. Dans une authentification distante d'un utilisateur, il est recommandé que les clés cryptographiques employées par l'environnement de confiance local pour réaliser l'authentification de machine avec le SI distant ne puissent être extraites par l'utilisateur.

2.2.2. Mécanismes de déverrouillage

Règle-Déverrouillage. L'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant doit nécessiter un déverrouillage par l'utilisateur avant de pouvoir réaliser, pour son compte, une authentification de machine à machine conforme au Référentiel Général de Sécurité.

Recom-DéverrouillageLocal. Il est recommandé que l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant gère de façon autonome son mécanisme de déverrouillage.

Règle-DéverrouillagePersonnel. L'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant nécessite la présentation d'un élément personnel à l'utilisateur légitime.

Recom-DéverrouillagePersonnel. Il est recommandé que l'activation de l'environnement de confiance local intervenant dans une authentification d'un utilisateur auprès d'un SI distant nécessite la présentation de deux éléments personnels à l'utilisateur légitime.

Recom-SecretDéverrouillage. Il est recommandé que l'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant nécessite la présentation d'un secret connu uniquement de l'utilisateur légitime.

Recom-TauxFausseAcceptation. Il est recommandé que le mécanisme de déverrouillage de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant ne puisse pas être contourné par quiconque avec une probabilité de succès supérieure à une chance sur 2.

Recom-CheminSûr. Il est recommandé que les informations dont dépend l'activation de l'environnement de confiance local intervenant dans l'authentification d'un utilisateur auprès d'un SI distant soient directement introduites au niveau des fonctions de l'environnement de confiance local qui les exploitent sans possibilité d'écoute ni de perturbation.

2.2.3. Audit

Outre les mécanismes d'audit de l'authentification de machine réalisée vis-à-vis du SI distant par l'environnement de confiance local pour le compte de l'utilisateur, il convient de prévoir, dans le cas de l'authentification de personnes, des mécanismes complémentaires permettant à l'utilisateur lui-même d'être en mesure de contrôler que son identité n'est pas usurpée.

Recom-AuditPersonnel. Il est recommandé que dans une authentification distante d'un utilisateur, ce dernier soit en mesure de consulter de manière sécurisée les audits de ses authentifications, mais sans pouvoir ni les modifier, ni les effacer.