Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 12 avril 2007

N° 729/SGDN/DCSSI/SDS/AsTeC

Authentification

Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard

Version 0.13 du 3 avril 2007

Version	Modifications
Version 0.13 du 3 avril 2007	**Version mise en application à titre expérimental.**
Version 0.12 du 27 mars 2007	**Ajout d'une partie explicative relative à l'interprétation du référentiel dans le cas des mécanismes utilisant des mots de passe à usage unique.**
Version 0.11 du 8 février 2007	**Prise en compte des remarques reçues suite à l'appel à commentaires sur la version 0.10.**
Version 0.10 du 9 octobre 2006	**Document de travail transmis pour commentaires.**
Version 0.6 du 26 avril 2006	**Première version suivant un format de référentiel.**
Version 0.5 du 1er octobre 2004	**Version présentée en atelier de référence n° 2302/SGDN/DCSSI/SDS/AsTeC du 1er octobre 2004**

Cellule d'Assistance Technique en
Conception de la DCSSI
SGDN/DCSSI/SDS/AsTeC
51 boulevard de La Tour-Maubourg,
75700 Paris 07 SP
AsTeC@sgdn.pm.gouv.fr

A. Table des matières

B. Introduction

B.1. Contexte

B.1.a. Objectif du document

L'objectif de ce document est de présenter 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.

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

La lecture de ce document présuppose que le lecteur est familier avec les concepts utilisés en cryptographie et particulièrement, ceux exposés dans « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ».

B.1.b. Rôle de l'authentification

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier c'est apporter la preuve de cette identité.

Ce document ne traite que la fonction d'authentification. L'identification est considérée comme acquise et nous supposons donc l'identité connue (c'est-à-dire qu'on ne cherche pas à reconnaître dans un ensemble d'identités ou d'identifiants connus, celui qui correspond à l'entité à authentifier).

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 du présent document.

B.1.c. Typologie des fonctions d'authentification

Le replacement de la fonction « authentification » dans son contexte permet en particulier d'introduire la question de l'intégration de cette fonction dans son environnement dans le cadre de l'objectif recherché, à savoir l'attribution (pour autorisation ou imputation) d'une action à son auteur réel ou, dit autrement, 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.

Notons tout de suite que **la problématique liée à la signature électronique n'est pas l'objet de ce document.** Toutefois, comme dans le cas de la signature, 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.

B.1.d. Positionnement du document

Ce document complète le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » édité par la DCSSI, en particulier ses paragraphes « C.1.3 authentification d'entités » et « C.2.4 authentification asymétrique d'entités et échange de clés », qui feront référence au présent document dans les éditions ultérieures.

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 ce document. Cette problématique générale est traitée dans le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

Nous décrivons dans ce document des règles et des recommandations relatives à différents niveaux de robustesse des mécanismes d'authentification. Ces niveaux sont définis dans le paragraphe B.3 du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ».

- Note importante : la diffusion du présent document est calquée sur celle du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » qui prévoit trois versions :
  - **La présente version, non classifiée, traite uniquement du premier niveau de robustesse, qualifié de « standard ». Ce document a pour vocation d'être largement diffusé, en particulier de manière électronique.**
  - Une deuxième version du document est également non classifiée mais n'est pas diffusée par voie électronique ; elle traite des deux premiers niveaux de robustesse, « standard » et « renforcé ». Les informations qu'elle contient sont issues du savoir-faire et de l'état de l'art cryptographiques publics.
  - Une troisième version traite de l'ensemble des trois niveaux de robustesse, niveau « élevé » compris. Le caractère sensible de certaines règles mettant en œuvre un principe de précaution justifie une classification du document.
- Les **règles** définissent des principes qui doivent *a priori* être suivis par tout mécanisme visant un niveau de robustesse donné. L'observation de ces règles est une condition généralement nécessaire, mais non suffisante, à la reconnaissance du niveau de robustesse visé par le 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.
- En plus des règles, nous définissons également des recommandations. Elles ont pour but de guider dans le choix de certains mécanismes d'authentification permettant un gain important en terme de sécurité. Il va de soi qu'en tant que recommandations, leur application peut être plus librement modulée en fonction d'autres impératifs tels que des contraintes de performance, d'ergonomie ou de coût.

Il importe de noter dès à présent que les règles et recommandations contenues dans ce document ne constituent pas un dogme imposé aux concepteurs de produits utilisant des mécanismes d'authentification. L'objectif est de contribuer à une amélioration constante de la qualité des produits de sécurité. A ce titre, le suivi des règles énoncées dans ce document doit être considéré comme une démarche saine permettant de se prémunir contre de nombreuses erreurs de conception ainsi que contre d'éventuelles faiblesses non décelées lors de l'évaluation des mécanismes d'authentification.

Dans la mesure du possible, chaque règle et recommandation contenue dans ce document fait l'objet d'une justification qui tient compte le plus rigoureusement possible de l'état de l'art ainsi que des contraintes pratiques liées à la mise en œuvre.

Le lecteur est invité à se référer au document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » notamment pour les différentes limitations décrites qui s'appliquent aussi au présent document.

B.1.e. Organisation du document

L'organisation de ce document est dans certains aspects similaire à celle du document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » :

- les concepts généraux de modélisation de l'authentification sont présentés au paragraphe B.2 ;
- l'ensemble des règles et recommandations s'appliquant aux différentes étapes du cycle de vie sont ensuite regroupées dans le chapitre C, à partir de la page 16;
- les règles et recommandations sont repérées selon la codification suivante : les premières lettres (**Règle** ou *Recom*) indiquent si l'on à affaire à une règle ou une recommandation, l'indice suivant () indique le niveau de robustesse standard, le domaine d'application est ensuite précisé et, finalement, un chiffre permet de distinguer les règles d'un même domaine d'application.

Ce document ne comporte volontairement aucun tableau récapitulatif. Les différentes règles et recommandations ne peuvent en effet être assimilées à une recette décrivant comment réaliser une mécanisme d'authentification, ce qui serait une source d'erreurs et de confusions.

B.1.f. Mise à jour du document

Comme pour le document « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », ce document a vocation à être révisé régulièrement pour tenir compte des évolutions constantes des menaces et des possibilités technologiques. La collecte de commentaires et la diffusion des révisions sont effectuées par la cellule d'assistance technique en conception de la DCSSI.

Adresse e-mail (non sécurisée) : `AsTeC@sgdn.pm.gouv.fr`

B.2. Modèle de la fonction d'authentification

B.2.a. 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).

Notons tout de suite que ces deux derniers éléments d'authentification sont clairement anthropomorphes et ne s'appliquent pas à des dispositifs automatiques. Nous distinguerons donc deux modèles 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.

Nous supposons également que l'authentification ne peut s'effectuer qu'après partage préalable d'informations entre les acteurs concernés du systèmes d'information. En d'autres termes, nous ne nous intéressons pas au processus d'enregistrement d'un utilisateur dans une entité organisatrice, mais aux moyens techniques et cryptographiques à mettre en place suite à cet enregistrement, pour que l'utilisateur puisse ensuite être authentifié correctement lors de son utilisation du système d'information.

B.2.b. Modèle général du processus d'authentification

B.2.b.1. Définition des notions

Nous définissons ci-dessous notre modèle. 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*.

- Il s'agit bien d'une possibilité. 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 par exemple emprunter un chemin différent de celui des *actions.*

B.2.b.2. Etats constitutifs d'une authentification

On distingue donc :

- 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.

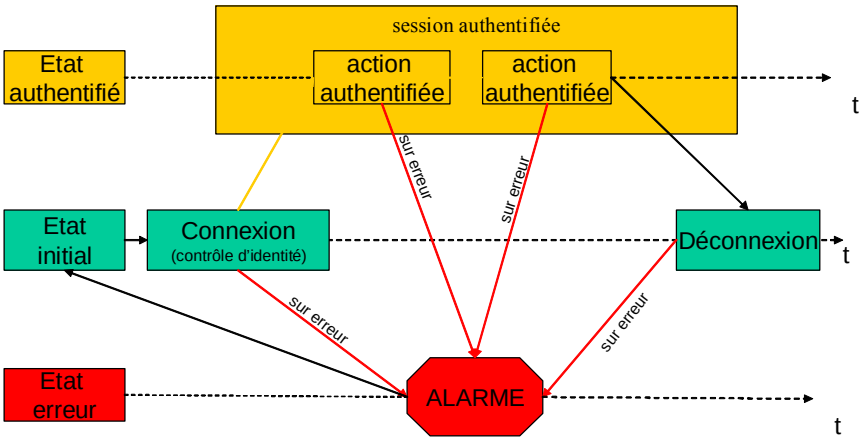

figure 1 États constitutifs d'une authentification

- 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, rappelons encore une fois que 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, en toute généralité, la *session authentifiée* peut être excessivement courte et les processus de *connexion* et de *déconnexion* peuvent ne pas correspondre à des opérations cryptographiques.

B.2.c. 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*. En effet, 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.

Partant de ce principe, nous allons préciser maintenant des modèles plus proches de réalités concrètes d'implantation pour pouvoir proposer des recommandations sur les mécanismes de sécurité à mettre en place.

B.2.c.1. Authentification de machines

B.2.c.1.1. Modèle d'authentification de machines

Nous allons distinguer dans la suite trois entités :

- l'environnement de confiance local,
- le SI distant,
- le 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 le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques ».

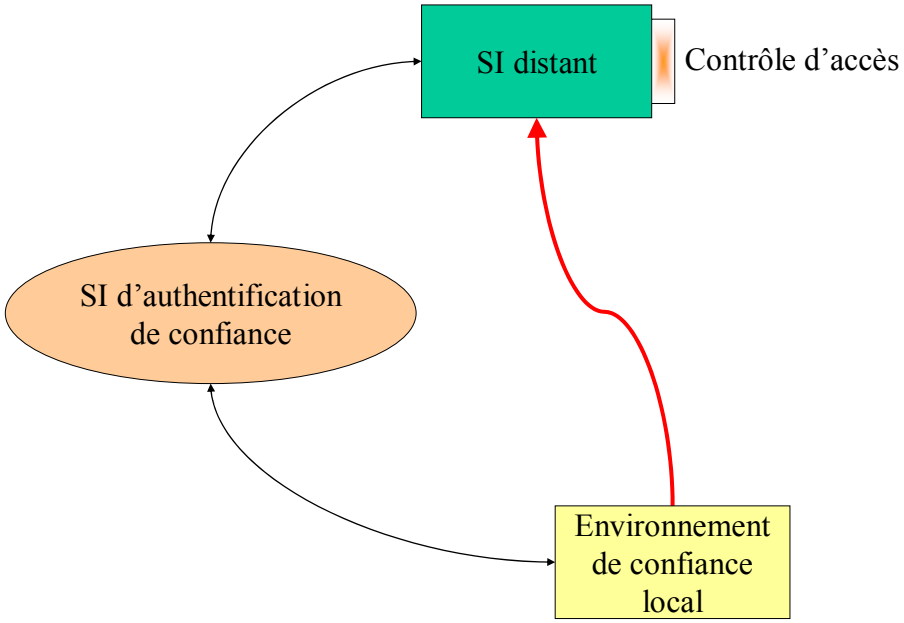

figure 2 Modèle d'authentification de machines

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. Il peut s'agir, par exemple, d'un serveur d'authentification 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 exemple totalement différent de 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 cet exemple qu'il n'y a pas authentification du porteur du badge. C'est uniquement ce dispositif qui est authentifié. En outre, on pourrait imaginer plusieurs scénarios de contrôle d'accès, par exemple :

1. 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.
2. 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.

- Un autre exemple que l'on peut considérer est celui de la télévision à péage dont la problématique est un peu différente. Le décodeur du téléspectateur doit recevoir du diffuseur, par voie hertzienne, les informations lui permettant de calculer une clé de décodage. Pour éviter la fraude, le décodeur n'accepte ces informations que si le diffuseur est bien authentifié. Dans cette application, l'environnement de confiance local est (paradoxalement) le diffuseur qui demande l'accès au SI distant, le décodeur de l'utilisateur, pour lui introduire une clé. L'opération de connexion se fait sur détection par le décodeur de la trame contenant les informations de décodage. L'action immédiate est la vérification de l'authenticité de la trame et, si certaines autres informations sont remplies, le calcul de la clé de décodage. La déconnexion est implicite du fait que chaque trame d'informations est authentifiée séparément. La seule différence avec la signature électronique réside dans le fait qu'une fois vérifiée l'authenticité de l'action, celle-ci n'a plus d'importance : le système n'a pas besoin de conserver la signature de l'information.

B.2.c.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 paragraphe C.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 paragraphe C.1.c.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 leur être applicables.

B.2.c.2. Authentification d'une personne vis-à-vis d'une machine

B.2.c.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, à notre connaissance, de mécanisme humainement exploitable permettant une authentification sans rejeu[2].

Pour bien les distinguer, nous qualifierons ces procédés 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.

Comme exemple de procédés de déverrouillage, caractérisés par la possibilité de rejeu, on peut citer :

- 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 que nous emploierons complète le précédent en faisant apparaître l'utilisateur (voir figure 3).

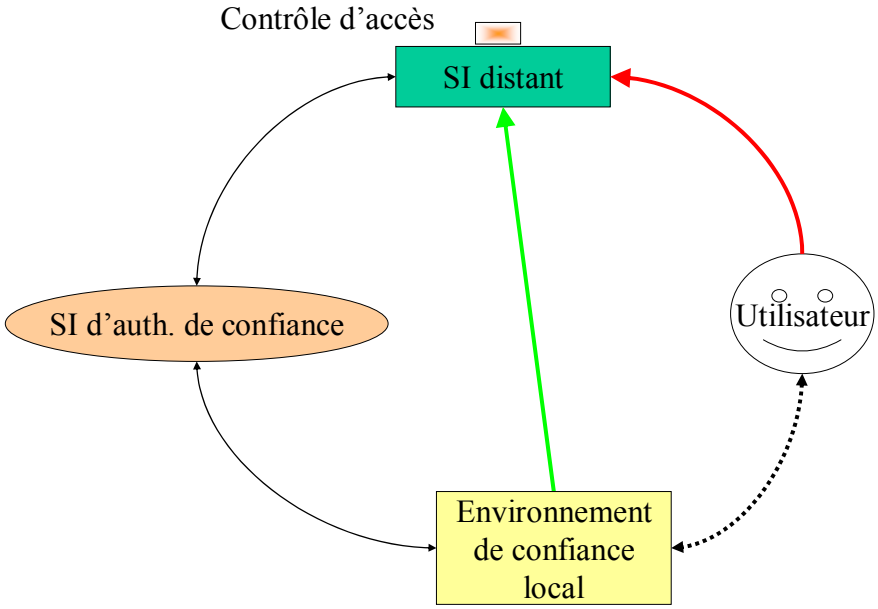

figure 3 Modèle d'authentification de personne

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

[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.

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.

- Dans un premier exemple nous reprenons celui de l'accès d'un client local à un serveur de fichiers en introduisant l'utilisateur de la machine locale. Celui-ci 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.

- Comme deuxième exemple, reprenons l'exemple du contrôle d'accès physique, mais en faisant cette fois-ci apparaître l'utilisateur. C'est en effet lui 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 traverser la porte.

  Dans cet exemple, 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 ;
  - de même, une caractéristique biométrique peut être utilisée pour déverrouiller le badge ;
  - on pourrait aussi considérer un système de mots de passe à usage unique générés par le badge 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 sur cet exemple 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.

- Dans un troisième exemple, nous pouvons revenir sur l'accès d'un client local à un serveur de fichiers en imaginant 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.

- Poursuivons sur 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 tryptique 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.

- Un autre exemple d'application du modèle est celui 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, par exemple, 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.

B.2.c.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 paragraphe C.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 paragraphe C.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 du document (cf. § B.1.d).

B.2.c.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).

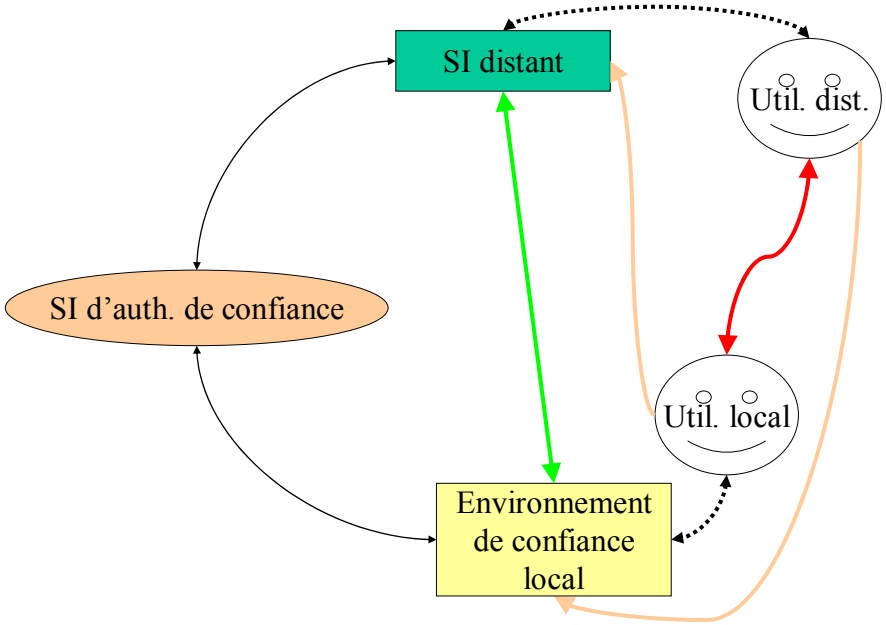

figure 4 Modèle d'authentification de bout-en-bout

C. Règles et recommandations

Dans toute la suite, nous cherchons à définir des règles et recommandations minimales pour des systèmes d'authentification de niveau standard.

C.1. Authentification de machines

C.1.a. Mécanismes cryptographiques

L'utilisation de mécanismes cryptographiques robustes est indispensable pour espérer atteindre une bonne authentification en évitant, par exemple, 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 ce document en parlant de mécanisme de déverrouillage.
- Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Par exemple, 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.

Nous ne reprendrons pas ici les « règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques ». Rappelons simplement que 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.

Bien entendu, 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.

Niveau standard

Règle$_s$Protocole. L'authentification de niveau standard entre deux machines doit faire intervenir un protocole cryptographique interactif d'authentification de niveau standard.

Justification :

- 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 dans ce cas. 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 ce document, nous parlons dans ce cas de déverrouillage.

C.1.b. 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.

Nous ne reprendrons pas 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 paragraphe C.1.a ci-dessus.

Niveau standard

Règle$_s$GestionClés. L'authentification de niveau standard entre deux machines doit faire intervenir une architecture de gestion des clés du protocole cryptographique utilisé de niveau standard.

Justification :

- Comme un procédé cryptographique est indispensable, la gestion de ses clés est nécessaire et doit viser un niveau de sécurité cohérent.

C.1.c. Etats du processus d'authentification

C.1.c.1. Connexion

C.1.c.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.

Niveau standard

Le respect de cette recommandation apporte énormément en termes de sécurité, puisque la présence de l'environnement de confiance local devient nécessaire pour accéder aux actions contrôlées par le SI distant.

Toutefois, la difficulté inhérente d'implantation d'une telle méthode d'authentification justifie qu'elle ne fasse pas l'objet d'une recommandation au niveau standard.

C.1.c.1.2. Tiers de confiance

Il faut, dans la mesure du possible, éviter l'authentification « transitive » (je m'authentifie auprès de A, qui s'authentifie auprès de B, etc.) qui cumule les sources de vulnérabilités.

Toutefois, ce type d'authentification présente également des intérêts en termes d'administration de la sécurité. Par exemple, le modèle des « *web services* » prévoit une administration des identités par une portion du système et une administration des droits d'accès par les applications. Dans ce modèle, l'application fait confiance au tiers pour authentifier l'environnement de

confiance local. Elle n'a à gérer que ses propres droits, associés à l'identité de l'environnement de confiance local.

Niveau standard

Règle$_S$TiersDeConfiance-1. Si un tiers de confiance est utilisé de façon directe pour une authentification de niveau standard entre deux machines, alors les mécanismes d'authentification du système local vis-à-vis de ce tiers de confiance doivent être de niveau standard.

Règle$_S$TiersDeConfiance-2. Si un tiers de confiance est utilisé de façon directe pour une authentification de niveau standard entre deux machines, alors les mécanismes d'authentification du système distant vis-à-vis de ce tiers de confiance doivent être de niveau renforcé.

Justification :

- Si le mécanisme utilisé pour l'authentification consiste à demander à un tiers de confiance de réaliser l'authentification pour son compte, alors l'authentification de l'environnement de confiance local vis-à-vis du tiers de confiance doit être de niveau similaire. Par contre, la réponse du tiers de confiance doit aussi être authentifiée et il est crucial que cette authentification soit d'un niveau de sécurité supérieur car le tiers de confiance, s'il est usurpé, donne la possibilité d'usurper toute identité.
- Rappelons qu'il convient de ne pas confondre ce tiers de confiance avec celui d'une architecture de gestion de clés qui peut être par ailleurs indispensable.

C.1.c.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.

Niveau standard

Recom$_S$Confidentialité. Si une authentification de niveau standard 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 de niveau standard assurant la confidentialité et l'intégrité de ces données.

Justification :

- L'authentification nécessitant l'emploi d'un protocole cryptographique, il y a un réel avantage à en profiter pour chiffrer les données dont l'accès est contrôlé. Toutefois, au niveau standard, ceci n'est qu'une recommandation car on peut considérer que des mesures de sécurité physique (par exemple, non-accessibilité au réseau informatique) peuvent suffire à protéger la confidentialité des données, l'authentification n'intervenant alors que pour garantir le cloisonnement du besoin d'en connaître.

C.1.c.3. Déconnexion

C.1.c.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.

Niveau standard

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

Justification :

- Il convient de bien insister sur la nécessité d'un effacement physique : les données correspondantes ne doivent plus être présentes pour garantir la sécurité du protocole d'authentification.

➢ La suppression des moyens d'accéder à ces données (pointeurs) n'est pas suffisante pour respecter cette règle. On prendra soin, par exemple, de mettre l'ensemble des mémoires correspondantes à zéro et de vider les éventuels tampons intermédiaires avant de supprimer les références aux valeurs sensibles.

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

Justification :

- L'effacement de données stockées sur un support magnétique est très délicat à mettre en œuvre. Il est donc largement préférable de s'assurer que les données correspondantes ne sont jamais stockées sur un tel support.
- L'utilisation d'une mémoire volatile garantit dans une certaine mesure que si le processus d'authentification est interrompu par une panne, les éléments sensibles ne seront pas compromis.
- Sur un ordinateur, cette recommandation vise à éviter que les pages mémoire utilisées pour stocker les éléments sensibles d'authentification puissent être stockées sur le disque de l'ordinateur par les mécanismes habituels de mémoire virtuelle ou zone d'échanges (*swap*). Le fait qu'il ne soit pas toujours possible de garantir que le système d'exploitation ne recopie pas une page mémoire dans une zone virtuelle stockée sur disque justifie le fait que cette mesure ne soit que recommandée.

C.1.c.3.2. Inactivité

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

Niveau standard

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

Justification :

- L'inactivité d'une session authentifiée est la première étape de scénarios d'attaque classique d'usurpation de session. Il est donc important de réduire ce risque en prévoyant un tel dispositif.
- Au niveau standard, ceci n'apparaît que comme une recommandation pour tenir compte des cas où la détection de l'inactivité pourrait être délicate à réaliser.

- Il est important de noter que nous nous plaçons ici dans le cas de l'authentification de machines. Cette recommandation n'implique donc pas une action d'un utilisateur.

C.1.d. 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.

Niveau standard

Recom$_S$Audit. Il est recommandé que toute erreur survenant au cours d'une session authentifiée de niveau standard génère une trace d'alarme ne pouvant être modifiée ni effacée.

Justification :

- Au niveau standard, le minimum recommandé est de pouvoir tracer des tentatives d'authentification ayant conduit à des anomalies.
- L'objectif d'intégrité des traces d'audit est naturel, s'agissant d'un élément d'enquête potentiel en cas d'usurpation d'identité.

C.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.

C.2.a. Utilisation d'un environnement de confiance local

Niveau standard

Règle$_S$Authentification. L'authentification de niveau standard d'un utilisateur auprès d'un SI distant doit faire intervenir un environnement de confiance local déverrouillé par l'utilisateur et réalisant une authentification de machine à machine de niveau standard pour le compte de l'utilisateur.

Justification :

- Comme indiqué en préambule, la simple utilisation à distance d'un mécanisme de déverrouillage ne saurait constituer un dispositif d'authentification de niveau standard.
- Le simple chiffrement des données transmises n'est pas suffisant pour empêcher le rejeu. Par exemple, 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.
- Il existe aussi des attaques « en paradoxe des anniversaires » qui peuvent s'appliquer, par exemple si une liste d'empreintes de mots de passe d'accès à un système distant est disponible.
- L'utilisation d'un environnement de confiance local paraît largement envisageable dès lors que l'utilisateur dispose forcément d'un système d'information pour réaliser les actions que le SI distant va lui autoriser.
- La notion d'environnement de confiance définie dans le document « règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques » est cohérente avec cette règle. En effet, d'une part l'authentification de machines réalisée peut faire intervenir des clés cryptographiques, d'autre part le mécanisme de déverrouillage ne peut être utilisé que dans un environnement de confiance, puisqu'il est intrinsèquement vulnérable au rejeu.

➢ Pour réaliser l'authentification de machine entre l'environnement de confiance local et le SI distant, on pourrait souhaiter dériver des clés secrètes à partir de mots de passe, ces derniers doivent être suffisamment longs et « non devinables » pour offrir une sécurité compatible avec les règles relatives aux tailles de clé. À titre d'exemple, des mots de passe de 8 caractères alphanumériques (chiffres et lettres majuscules ou minuscules) ne permettent pas de générer des clés de plus de 47 bits, et encore, sous l'hypothèse très optimiste que ces mots de passe sont choisis aléatoirement… De tels mots de passe ne permettent donc pas d'atteindre un niveau standard. Même en allongeant la taille des mots de passe, ce type de procédé resterait vulnérable aux attaques en hameçonnage évoquées ci-dessus. Il est donc encore préférable que l'authentification réalisée exploite aussi l'identité de l'environnement de confiance local employé.

Recom$_S$Périmètre. Dans une authentification distante de niveau standard 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.

Justification :

- L'environnement de confiance local accède par définition aux informations de déverrouillage propres à l'utilisateur. Il est fortement souhaitable que ces informations n'aient pas à être validées ou exploitées en dehors d'un périmètre dont l'utilisateur a conscience.
- Les informations de déverrouillage doivent être considérées comme des données personnelles. Les exploiter en dehors d'un périmètre physique sur lequel l'utilisateur peut exercer un certain contrôle entraîne des objectifs de sécurité importants sur ce périmètre.

➢ À titre d'exemple, on peut considérer le cas concret d'une base de données biométriques. L'authentification d'une personne peut être envisagée par comparaison au niveau d'un serveur des données acquises. Dans ce cas, l'environnement de confiance « local » s'étend par définition jusqu'au serveur qui réalise cette opération de comparaison. Il est possible de réaliser un tel mode de fonctionnement, mais il est évident que le serveur doit dans ce cas garantir la protection des données rejouables qu'il exploite. C'est la raison pour laquelle nous ne souhaitons pas interdire un tel mode de fonctionnement au niveau standard, mais nous recommandons une architecture pour laquelle les objectifs de sécurité peuvent être moins exigeants.

Recom$_S$Cloisonnement. Dans une authentification distante de niveau standard 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 soit cloisonnées des autres fonctions de l'environnement de confiance local.

Justification :

- L'authentification de personnes repose sur des mécanismes de déverrouillage qui permettent le rejeu. L'obtention des informations correspondantes constitue donc une cible de choix pour un attaquant, d'autant que ces informations sont faiblement modifiables. Les différents mots de passe utilisés sont souvent des variations les uns des autres et les caractères biométriques sont intrinsèques à la personne. Plus que toute autre fonction, celles de l'environnement de confiance local qui gèrent ces informations doivent donc être protégées. Les autres fonctions de l'environnement de confiance local doivent être empêchées d'accéder aux informations traitées dans le cadre de l'authentification de personne. Les vulnérabilités éventuelles de ces autres fonctions ne doivent pas compromettre les informations sensibles que l'utilisateur emploie dans son authentification distante.
- Au niveau standard, l'utilisation de systèmes non totalement maîtrisés justifie que cette mesure ne soit qu'une recommandation.

Recom$_S$CloisonnementPhysique. Dans une authentification distante de niveau standard 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.

Justification :

- S'agissant d'une authentification de personne, il est raisonnable que l'utilisateur ait le moyen de conserver sous son contrôle physique les éléments déterminants de l'authentification de son identité.

C.2.b. Mécanismes de déverrouillage

Niveau standard

Règle$_S$Déverrouillage. L'environnement de confiance local intervenant dans l'authentification de niveau standard d'un utilisateur auprès d'un SI distant doit nécessiter un déverrouillage par l'utilisateur avant de pouvoir réaliser une authentification de machine à machine de niveau standard pour le compte de l'utilisateur.

Justification :

- L'environnement de confiance local doit être protégé par un dispositif de verrouillage afin qu'il ne puisse pas être utilisé à l'insu de l'utilisateur.

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

Justification :

- L'autonomie de l'environnement de confiance local doit être recherchée au niveau du dispositif de verrouillage car la mise en œuvre de tiers est très délicate à envisager s'agissant d'un mécanisme intrinsèquement vulnérable au rejeu.

➢ L'utilisation d'un serveur d'authentification peut permettre de déverrouiller la session d'un utilisateur. Au niveau standard, ce type d'architecture est possible et correspond à des architectures de systèmes d'information largement utilisées (Kerberos, Radius, SRP, etc…). La mise en œuvre de ce type d'architecture est toutefois délicate à gérer du fait de l'authentification à réaliser entre le serveur tiers et l'environnement de confiance local. Elle peut donc présenter des vulnérabilités dans l'implantation rendant le mécanisme global non éligible au niveau standard.

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

Justification :

- Pour que le mécanisme de verrouillage protège effectivement l'utilisation de l'environnement de confiance local à l'insu de l'utilisateur légitime, il est nécessaire que ce mécanisme mette en œuvre un élément caractéristique de la personne authentifiée.

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

Justification :

- Cette recommandation est en cohérence avec la notion traditionnelle « d'authentification forte », qui préconise de combiner deux mécanismes parmi ce que l'on sait, ce que l'on a, ce que l'on est ou ce que l'on sait faire.
- Nous considérons qu'au niveau standard, les applications doivent définir leur besoin éventuel « d'authentification forte » des utilisateurs. C'est la raison pour laquelle ce type d'authentification n'est pas une règle au niveau standard.

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

Justification :

- L'un des moyens simples de respecter cette règle est de faire intervenir un secret (mot de passe, code PIN, etc.) sans que ceci soit le seul moyen possible au niveau standard.

- La simple présentation d'un badge personnel est un mécanisme de déverrouillage de niveau standard.
- Le contrôle d'une caractéristique biométrique peut être un mécanisme de déverrouillage de niveau standard. Il est toutefois recommandé que le contrôle de cette caractéristique soit effectué par l'environnement de confiance local.

Recom$_S$TauxFausseAcceptation. Il est recommandé que le mécanisme de déverrouillage de l'environnement de confiance local intervenant dans l'authentification de niveau standard 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^{11}.

Justification :

- Cette probabilité est relativement faible. Elle correspond à environ une chance sur deux mille. S'agissant de mécanismes de niveau standard et du déverrouillage d'un environnement de confiance local, cette probabilité semble suffisante et correspondre à l'état de l'art actuel.
- Cette recommandation ne doit pas être comprise uniquement vis-à-vis d'un potentiel attaquant extérieur. L'authentification vise à garantir l'identité d'une personne. La notion d'administrateur est donc très délicate à gérer dans ce contexte. Le fait qu'un administrateur dispose de droits d'accès lui permettant d'usurper l'identité d'un utilisateur peut dans certains cas conduire à des conséquences non négligeables.
- Cette probabilité s'entend comme une mesure de la sécurité intrinsèque du mécanisme et non des dispositifs de protection éventuels de celui-ci.

- Si des serveurs d'authentification distants sont mis en œuvre, alors la mesure d'une telle probabilité est insuffisante à estimer la solidité du mécanisme de déverrouillage contre des attaques en force brute parallélisées sur plusieurs comptes. L'analyse de risque devra alors être affinée.

- Un code porteur de 4 chiffres présente une entropie de $4.\log_2(10) \approx 13{,}29$ bits. Si trois codes peuvent être présentés avant blocage de l'environnement de confiance local, alors la probabilité de fausse acceptation est de 3 sur $2^{13,29}$ soit un sur $2^{13,29 - \log_2(3)} \approx 2^{11,7}$. Un tel mécanisme est conforme à la recommandation.

- Un mot de passe de 6 caractères pris dans un alphabet de 32 symboles présente une entropie de 30 bits. De façon locale, un tel mot de passe répond bien à la recommandation dès lors qu'il y a une limitation du nombre de tentatives, mais si ce mot de passe peut être présenté dix fois à un serveur distant qui héberge cent mille sites, alors la probabilité de fausse acceptation est théoriquement d'environ $2^{30 - 19.93} = 2^{10.07}$. En outre, dans la pratique, l'attaque peut très bien consister à ne présenter chaque jour que cinq mots de passe en comptant que l'utilisateur légitime va régulièrement réactiver son compte. Ce faisant, la possibilité d'une recherche exhaustive devient envisageable avec dans ce cas une quasi-certitude de pouvoir contourner le mécanisme de déverrouillage d'un utilisateur.

D. Guide d'interprétation dans certains cas particuliers

D.1. Mot de passe à usage unique

D.1.a. Préambule

Parmi tous les mécanismes de déverrouillage, l'utilisation d'un secret connu de l'utilisateur est de loin le plus répandu. Ceci est lié au fait que ce mécanisme est d'une part facile à mettre en œuvre par l'utilisateur et d'autre part qu'il ne nécessite pas de dispositif coûteux, la présence d'un clavier étant dans la plupart des cas nécessaire au-delà du simple processus d'authentification.

Ainsi que nous l'avons défini, un mécanisme de déverrouillage souffre toutefois du grave défaut intrinsèque d'être rejouable, si bien que la connaissance du mot de passe par un adversaire lui permet immédiatement d'usurper l'identité de la personne si aucun autre dispositif n'est en place.

Pour pallier cette vulnérabilité, des mécanismes de mot de passe à usage unique peuvent être imaginés. Ces mécanismes permettent, lorsqu'ils sont correctement conçus et implantés, d'atteindre un niveau de sécurité bien supérieur à celui du mot de passe statique, sans toutefois prétendre atteindre un niveau comparable à un protocole d'authentification cryptographique. Cette limitation est essentiellement due à des contraintes ergonomiques qui font qu'on ne peut demander à l'utilisateur de saisir régulièrement des données aléatoires de taille importante. Rappelons en effet que l'entropie d'un mot de passe ne peut être comparée à celle d'une clé cryptographique symétrique qu'il est recommandé de choisir au minimum de 128 bits (voir tableau de la figure 5).

Caractéristiques du mot de passe	Nombres total de symboles	10 symboles (chiffres)			26 symboles (lettres)			62 symboles (chiffres, majuscules, minuscules)			90 symboles (jeu de caractères complet)		
	Nombre de symboles par mot de passe	4	7	10	8	10	16	8	10	16	8	10	16
Taille de clé équivalente (bits)		13	23	33	38	47	75	48	60	95	52	65	104
Ordre de grandeur du temps d'énumération du dictionnaire des mots de passe possibles par un ordinateur personnel		~0	~0	3 min	1h	1 mois	∞	1 mois	5 siècles	∞	2 ans	200 siècles	∞

figure 5 : Entropie d'un mot de passe

Du fait de cette limitation, il est assez facile de réaliser des schémas d'authentification par mot de passe à usage unique dont la sécurité est faible. L'objet de cette partie est donc de préciser pour ces mécanismes particuliers les règles et recommandations à respecter.

D.1.b. Description du mécanisme

D.1.b.1. Adaptation du modèle d'authentification

Le modèle d'authentification de personne que nous avons introduit reste valable (voir figure 6). La particularité d'un mécanisme d'authentification par mot de passe à usage unique est toutefois que l'utilisateur est amené à intervenir pour que son environnement de confiance local puisse réaliser l'authentification de machine pour son SI local. En effet, ainsi que nous l'avons indiqué, l'utilité d'un mécanisme par mot de passe est qu'il ne nécessite pas de dispositif supplémentaire au niveau du SI local comme un lecteur de carte. L'environnement de confiance local n'est donc pas en mesure d'interagir directement ni avec le SI local, ni avec le SI distant.

Le corollaire de cette intermédiation de l'utilisateur est également que l'environnement de confiance local n'a pas de moyen d'authentifier le SI distant. On en déduit que c'est l'interface de saisie d'une authentification par mot de passe dynamique qui doit authentifier le serveur distant par une authentification de machines.

- L'exemple d'implantation classique consiste à réaliser une connexion SSL au SI distant. Cette connexion permet, par la vérification du certificat du serveur, d'authentifier ce dernier.

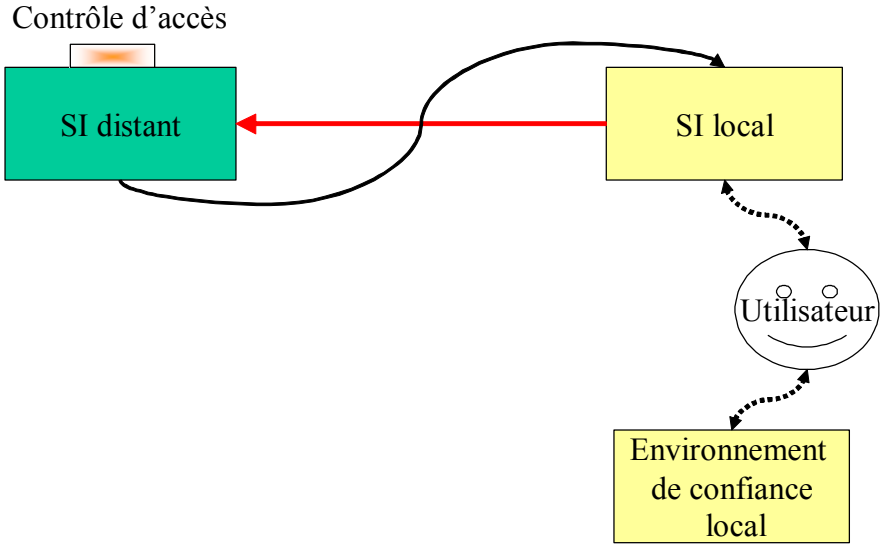

figure 6 Authentification par mot de passe dynamique

D.1.b.2. Description du protocole

Les protocoles d'authentification par mot de passe dynamique peuvent être décrits de façon générique de la façon suivante.

Les différentes entités du protocole disposent respectivement :

- pour l'utilisateur :
  - d'un identifiant *id*,
  - d'un éventuel mot de passe statique *smdp*,
  - d'un environnement de confiance local, qui peut également mettre en œuvre un mécanisme de déverrouillage propre (pin-code, empreinte digitale, etc.).

- pour l'environnement de confiance :
  - o d'une clé $K_\pi^{(id)}$ dépendant de l'identifiant et permettant de « prouver » cette identité,
  - o éventuellement d'un compteur interne *t*.
- pour le SI distant :
  - o éventuellement de la valeur $H^{(id)}(smdp)$.
  - o d'une clé $K_v^{(id)}$ dépendant de l'identifiant et permettant de « vérifier » cette identité,
  - o éventuellement d'un compteur interne *t'*,
  - o éventuellement d'un générateur de défi aléatoire *chall*.

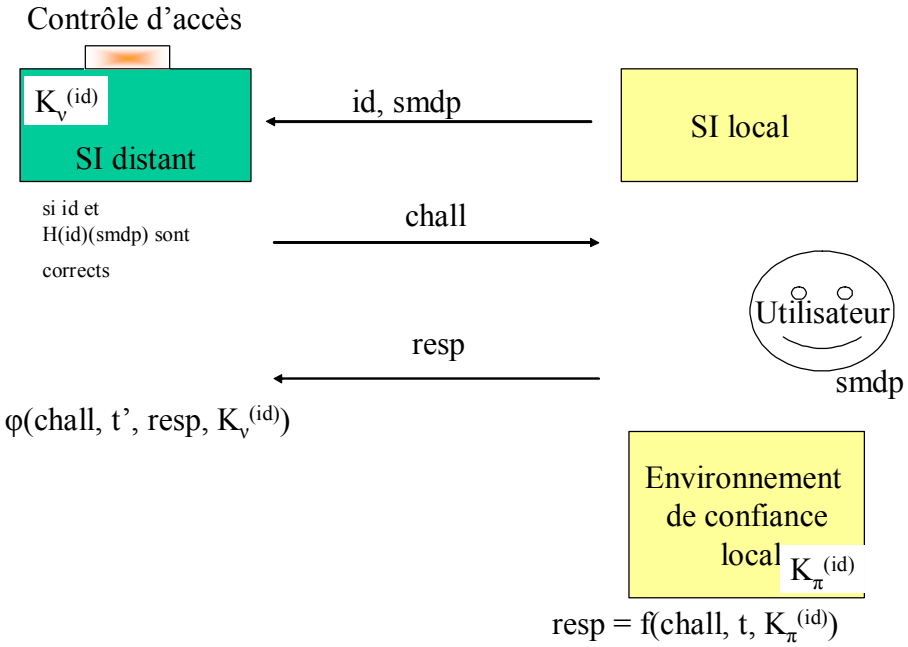

figure 7 : Protocole générique de mot de passe dynamique

Le protocole peut alors se décomposer en étapes successives (voir figure 7) :

1. La première étape du protocole consiste à envoyer au SI distant l'identifiant *id*. Cet identifiant peut être accompagné du mot de passe statique *smdp*.

➢ L'intérêt de mettre en place un mot de passe statique est de ne poursuivre le protocole que si cette première vérification est correctement réalisée. S'il n'y a pas de mot de passe statique, alors il est possible de rechercher les identifiants valides en les énumérant pour détecter ceux qui donnent lieu au démarrage du protocole.

2. Le SI distant compare alors le résultat de l'application de la fonction $H^{(id)}$ au mot de passe transmis avec la valeur de référence qu'il possède.

➢ L'utilisation d'une fonction différenciée par identifiant permet, si le fichier des mots de passe du SI distant est compromis, d'éviter qu'une attaque par dictionnaire pré-calculé puisse s'appliquer à l'ensemble des utilisateurs.

➢ Le mot de passe statique doit être transmis tel quel par le SI local. En effet, si le SI local transmettait $H^{(id)}(smdp)$, alors la compromission du fichier des mots de passe du SI distant donnerait immédiatement le moyen de passer la première étape du protocole.

➢ Par conséquent, le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant doit également permettre la protection en confidentialité de la session authentifiée.

3. Le SI distant peut alors générer un défi aléatoire.

- Cette étape peut ne pas intervenir si le mécanisme de mot de passe dynamique emploie uniquement un mécanisme de synchronisation. Dans ce cas, l'utilisation d'un mot de passe statique est inutile.
- S'il y a utilisation d'un défi, celui-ci doit être aléatoire, c'est-à-dire imprédictible. Dans le cas contraire, un attaquant pourrait se retrouver dans une situation telle qu'il puisse demander à l'avance le calcul de réponses à des défis futurs.

4. L'utilisateur retranscrit le défi sur son environnement de confiance.

- L'utilisation de l'environnement de confiance peut nécessiter un déverrouillage particulier. Ce déverrouillage est toutefois indépendant du protocole de mot de passe dynamique.
- Les contraintes ergonomiques font que l'entropie de ce défi ne peut être comparée à celle obtenue dans un protocole d'authentification cryptographique. C'est là une nouvelle raison pour que le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant assure également la protection en confidentialité de la session authentifiée.

5. L'environnement de confiance calcule la réponse à partir des différents éléments dont il dispose :
    1. la clé de prouveur $K_{\pi}^{(id)}$,
    2. un éventuel compteur de synchronisation t,
    3. le défi *chall* éventuellement reçu.

- La clé de prouveur peut être symétrique ou asymétrique. Il s'agit d'une clé cryptographique à part entière qui doit être gérée et protégée comme telle.
- La clé de prouveur peut aussi prendre la forme d'un tableau de mots de passe. Dans ce cas le défi s'apparente à « répondre le mot de passe n° N » et chaque nouvelle réponse dévoile petit-à-petit l'intégralité de la clé.
- Le compteur de synchronisation peut être synchronisé à une horloge interne. Il peut également être incrémenté à chaque utilisation de l'environnement de confiance.

6. L'utilisateur retranscrit la réponse sur son SI local qui le transmet au SI distant.

- Les contraintes ergonomiques font que l'entropie de la réponse ne peut être comparée à celle obtenue dans un protocole d'authentification cryptographique. Au contraire du mot de passe statique ou du défi qui ne sont pas indispensables, la protection de la réponse est obligatoire. Il est donc indispensable que le mécanisme d'authentification de machines employé par le SI local pour authentifier le SI distant assure également la protection en confidentialité de la session authentifiée.

7. Le SI distant vérifie la réponse à partir des différents éléments dont il dispose :
    1. la clé de vérifieur $K_{v}^{(id)}$,
    2. son éventuel propre compteur de synchronisation t',
    3. le défi *chall* éventuellement envoyé,
    4. la réponse *resp* reçue.

- Le caractère symétrique ou asymétrique de la clé de vérifieur est évidemment lié à celui de la clé de prouveur.
- Si le temps est utilisé comme compteur de synchronisation, la période temporelle devra être suffisamment large pour garantir que les compteurs t et t' sont bien synchronisés.
- Si le compteur est incrémenté à chaque authentification réussie, alors il faudra prévoir que l'environnement de confiance puisse être en avance si une erreur de transmission a, par exemple, interrompu l'exécution d'une instance du protocole. La fenêtre de synchronisation a dans ce cas un impact sur la sécurité, car si on autorise s avances de l'environnement de confiance, un attaquant a s fois plus de chances de tomber sur une réponse qui satisfera le SI distant.

D.1.c. Conséquences sur les règles et recommandations à appliquer

D.1.c.1. Mécanismes cryptographiques

Les différents mécanismes cryptographiques utilisés doivent évidemment respecter les règles et recommandations du document « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard». Il s'agit :

1. D'une part, du mécanisme d'authentification de machines qu'utilise le SI local pour authentifier le SI distant. Ce mécanisme doit en outre assurer la confidentialité de la session authentifiée.
2. D'autre part, des fonctions de preuve f et de vérification φ qui doivent notamment ne pas divulguer d'information sur les clés cryptographiques employées.

D.1.c.2. Gestion des clés

Les différents mécanismes cryptographiques utilisent des clés dont la gestion doit évidemment respecter les règles et recommandations du document « Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard ».

D.1.c.3. Cas particulier du défi / réponse

Les contraintes ergonomiques font qu'il n'est pas possible d'employer des données de défi / réponse d'entropie comparable à celle obtenue dans un protocole d'authentification cryptographique. C'est la raison pour laquelle la session authentifiée entre le SI local et le SI distant doit être protégée en confidentialité, car statistiquement, la probabilité qu'un défi soit proposé plusieurs fois n'est pas négligeable.

D.1.c.3.1. Cas particulier de l'absence de synchronisation

Il est possible dans le protocole générique proposé de reposer uniquement sur le défi pour réaliser l'authentification par mot de passe dynamique. Il faut toutefois noter que dans ce cas, si un attaquant est en mesure d'observer des couples défi / réponse, il est en mesure de se constituer progressivement un dictionnaire et la probabilité que le SI distant lui propose un défi qu'il connaît déjà est soumise au paradoxe des anniversaires.

- Par exemple, si le défi peut être codé par 7 chiffres décimaux, le tableau de la figure 5 donne une entropie de 23 bits. Ceci donne une probabilité de contournement du mécanisme de $2^{11,5}$.

D.1.c.3.2. Cas général avec synchronisation anti-rejeu

Dans le cas général, le compteur de synchronisation peut être considéré comme un compteur anti-rejeu. Dans ce cas, et sous réserve que ce compteur ne soit jamais réinitialisé et ne boucle pas, l'entropie de la réponse est le facteur discriminant de la sécurité du protocole. Cette entropie doit le cas échéant être corrigée du nombre de tentatives possibles et de l'existence ou non d'une fenêtre de synchronisation.