

PREMIER MINISTRE

SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

Rapport de certification 99/01

Systeme d'Interconnexion Sécurisé SIS

UCC V3.2(1), LSA V3.2, C-ADM V3.2

Juin 1999

Toute correspondance relative à ce rapport de certification doit être adressée au :

SCSSI
Centre de Certification de la Sécurité des Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

© SCSSI, France 1999.

La reproduction de tout ou partie de ce document, sans altération ni coupure, est autorisée.

Tous les noms des produits ou des services de ce document sont des marques déposées de leur propriétaire respectif.

Ce document est folioté de 1 à 30 et certifié.

Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information



CERTIFICAT 99/01

Systeme d'Interconnexion Sécurisé SIS

UCC V3.2(1), LSA V3.2, C-ADM V3.2

ACE TIMING

Les caractéristiques de sécurité du produit ci-dessus identifiées dans le rapport de certification ont été évaluées par un Centre d'Évaluation de la Sécurité des Technologies de l'Information selon les critères ITSEC.

Le niveau d'évaluation atteint est le **niveau E3**. La résistance minimum des mécanismes est cotée **moyenne**.

Ce certificat est valide pour la version du produit mentionnée, sous réserve du respect des recommandations d'utilisation et des restrictions éventuelles figurant dans le rapport de certification associé.

Le 15 juin 1999,

Le commanditaire :

ACE TIMING

M. Georges Charles LE HOANGAN,
Président Directeur Général

L'Organisme de certification :

Service central de la sécurité des systèmes
d'information

Le Général Jean-Louis DESVIGNES, Chef de service

La présence du logo propre à l'Accord de Reconnaissance Mutuelle :

- *confirme que ce certificat a été délivré sous l'autorité d'un organisme de certification qualifié qui fait partie du Groupe d'Accord,*
- *indique que l'autorité de délivrance déclare qu'il s'agit d'un "certificat conforme" comme défini dans l'Accord,*
- *établit par conséquent des éléments pour baser la confiance dans le fait que le certificat est un "certificat conforme", bien que ne pouvant en donner une garantie, et qu'il sera reconnu en pratique par les autres membres du Groupe d'Accord.*

Les jugements contenus dans le certificat et le rapport de certification sont ceux de l'organisme de certification qualifié qui a procédé à la délivrance et ceux du centre d'évaluation de la sécurité des technologies de l'information qui a conduit l'évaluation. L'utilisation du logo de cet Accord n'entraîne pas la reconnaissance par les autres membres d'une quelconque responsabilité relative à ces jugements ou à tout dommage encouru en raison de la confiance accordée à ces jugements par une tierce partie.

Organisme de Certification
SCSSI
18, rue du docteur Zamenhof
F-92131 ISSY-LES-MOULINEAUX CEDEX.

Chapitre 1

Introduction

- 1 Ce document représente le rapport de certification du produit “Système d’Interconnexion Sécurisé (SIS)”.
- 2 SIS est un dispositif destiné à sécuriser les accès distants, au travers de réseaux publics, à un réseau local protégé. Le contrôle d’accès repose sur le filtrage des connexions TCP/IP en entrée et en sortie du réseau local, et l’authentification des clients munis d’une carte à puce.
- 3 Le produit SIS est constitué des trois entités logicielles suivantes :
 - L’Unité de Contrôle et de Commutation **UCC**, placée en coupure Ethernet sur le réseau local à protéger,
 - La Console d’ADMinistration **C-ADM** de l’UCC, installée sur la station d’administration SA sur le réseau protégé, permettant la télégestion de l’UCC,
 - Le module Logiciel de Sécurisation d’Accès **LSA**, installé sur chacune des stations clientes, permettant le dialogue avec le support d’authentification et l’échange des messages d’authentification avec l’UCC.
- 4 Le SIS opère une journalisation des communications, à des fins d’audit et d’imputabilité, ainsi qu’un service de télégestion déporté sur la C-ADM. Les communications entre l’UCC et la station d’administration sont sécurisées par le chiffrement des données transférées.
- 5 Le produit SIS garantit la confidentialité des échanges, au travers de réseaux publics, entre les UCC de sites distants, en offrant un service de chiffrement des données au niveau IP.
- 6 La cible d’évaluation constitue une partie du produit “Système d’Interconnexion Sécurisé SIS”. La cible d’évaluation est constituée des logiciels UCC version 3.2(1), LSA version 3.2 et C-ADM version 3.2. Les éléments matériels et logiciels qui n’ont pas été développés spécifiquement pour le produit tels que les lecteurs de carte ou les cartes à puce, les stations clientes et la station d’administration et leur système d’exploitation, ne font pas l’objet de l’évaluation.
- 7 Les fonctionnalités, vis-à-vis desquelles le niveau E3 des critères ITSEC a été atteint, sont consignées au chapitre 4 du présent rapport.

Chapitre 2

Résultats

2.1 Conclusions de l'évaluation

- 8 La cible d'évaluation détaillée au chapitre 3 du présent rapport satisfait aux exigences du **niveau d'évaluation E3**.
- 9 La résistance minimum des mécanismes de sécurité de la cible d'évaluation (ci-après "résistance minimum des mécanismes") est cotée **moyenne**.
- 10 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau E3 et par la compétence, l'opportunité et les ressources correspondant à la cotation moyenne de la résistance minimum des mécanismes.
- 11 Les vulnérabilités connues du commanditaires de l'évaluation ont été toutes communiquées aux évaluateurs et au certificateur conformément à l'ITSEC 3.35.
- 12 L'utilisation sécuritaire de la cible d'évaluation est soumise aux recommandations figurant dans le chapitre 5 du présent rapport.

2.2 Contexte de l'évaluation

- 13 L'évaluation a été menée conformément aux critères ITSEC [1], à la méthodologie définie dans le manuel ITSEM [2] et aux interprétations définies dans la bibliothèque d'interprétation commune JIL [3].
- 14 La cible d'évaluation a été développée par la société :

ACE TIMING
17 rue du Noyer
35000 Rennes - France

- 15 Le développeur de la cible d'évaluation est aussi commanditaire de l'évaluation.
- 16 L'évaluation s'est déroulée consécutivement au développement du produit d'avril 1998 à avril 1999. La phase de certification s'est déroulée en mai 1999.
- 17 Cette évaluation a été conduite par le centre d'évaluation de la sécurité des technologies de l'information :

Centre National d'Études des Télécommunications CNET Caen
42, rue des Coutures

BP 6243
14066 Caen Cedex- France

Chapitre 3

Présentation du produit

3.1 Objet

18 La cible d'évaluation est constituée de trois entités logicielles distinctes :

- L'Unité de Contrôle et de Commutation UCC version 3.2(1),
- La Console d'ADMinistration C-ADM version 3.2,
- Le Logiciel de Sécurisation d'Accès pour carte à puce LSA version 3.2.

19 Chacune de ces entités s'installe sur des machines distinctes. La cible d'évaluation offre un service de contrôle d'accès à des réseaux, sous-réseaux ou serveurs connectés sur un brin Ethernet, utilisant les services des protocoles au dessus de IP. Le contrôle d'accès repose sur le filtrage des connexions TCP/IP et l'authentification des clients munis d'une carte à puce. Les règles de contrôle d'accès sont définies au sein d'une base de données qui tient lieu de politique de sécurité. La base est configurée par l'administrateur sur la station d'administration locale, par l'intermédiaire de la C-ADM, qui est pourvue d'une IHM. La base doit ensuite être téléchargée sur l'UCC pour être active.

20 La confidentialité des échanges entre deux UCC distantes, ou entre l'UCC et la C-ADM, est garantie par le chiffrement des données lors des communications.

21 Les limites de la cible d'évaluation sont définies dans le document "SIS - Cible de Sécurité" [4].

3.2 Historique du développement

22 Le produit a été développé par la société ACE TIMING. L'évaluation est consécutive au développement.

3.3 Description du matériel

23 La cible d'évaluation ne comporte pas d'éléments matériels. Les composants logiciels de la cible nécessitent cependant une configuration matérielle minimale à leur bon fonctionnement.

24 La configuration matérielle minimale de la machine hébergeant l'UCC est un micro-ordinateur compatible PC 486, équipé de :

- 8 Mo de RAM,
- un bus ISA, PCI, ou SCSI,
- une unité de disquette 3"1/2,

- un disque dur de capacité supérieur à 300 Mo,
- deux cartes réseau Ethernet 3C509, ou WD8013 ou SMC8013,
- un écran, un clavier,
- un lecteur de carte à puce de type TLP224 (GCR200, TLP224 NV2) branché sur le port de communication série,
- une carte à puce MCOS 16K identifiant l'UCC.

25 La configuration matérielle minimale d'une station cliente LSA est un micro-ordinateur compatible PC 486, équipé de :

- 8 Mo de RAM,
- une unité de disquette 3"1/2,
- une carte réseau Ethernet,
- un lecteur de carte à puce de type TLP224 (GCR200, TLP224 NV2),
- une carte à puce MCOS 16K par utilisateur, de la même famille que celle utilisée par l'UCC.

26 La configuration matérielle minimale de la station d'administration SA est un micro-ordinateur compatible PC 486, équipé de :

- 16 Mo de RAM,
- une unité de disquette 3"1/2,
- une carte réseau Ethernet,
- un lecteur de carte à puce de type TLP224 (GCR200, TLP224 NV2),
- une carte à puce MCOS 16K, identifiant l'administrateur, de la même famille que celle utilisée par l'UCC.

3.4 Description des microprogrammes

27 Les composants logiciels de l'UCC s'appuient sur le système d'exploitation BSDI version 2.0. Le code source de l'UCC a été intégré au noyau origine de BSDI, qui demeure cependant en dehors du champ de l'évaluation en tant que mécanisme de soutien.

3.5 Description des logiciels

3.5.1 Logiciels non évalués

28 Les logiciels du produit qui n'ont pas fait l'objet d'un développement spécifique sont :

- le système d'exploitation Windows version 3.1 de la station d'administration, et les sockets pour Windows,
- le systèmes d'exploitation Windows 3.1, Windows 95 ou Windows NT 4.0, et le logiciel client TCP/IP d'accès réseau des stations clientes.
- les logiciels des cartes à puce, réalisant le calcul des clés de session.

3.5.2 Logiciels soumis à évaluation

29 Les logiciels développés spécifiquement pour le produit sont :

- l'unité de contrôle et de commutation UCC, qui met en oeuvre la politique de sécurité de manière efficace par filtrage puis commutation de datagrammes IP.
- la console d'administration C-ADM : elle permet de définir la politique de sécurité et le téléchargement de la base de données associée sur l'UCC, ainsi que le rapatriement et l'audit des journaux d'imputabilité,
- le logiciel de sécurisation d'accès LSA : son rôle est de permettre le dialogue de la station cliente avec son lecteur de carte à puce, et l'échange de messages d'authentification avec l'UCC,

3.6 Description de la documentation

30 La documentation du produit est constituée des documents suivants :

- "Manuel de référence du SIS" [5],
- "Manuel d'installation de l'UCC" [6],
- "Manuel d'exploitation des composants" [7],
- "Procédure de vérification des installations et contrôle de l'intégrité de l'UCC" [8].

Chapitre 4

Évaluation

4.1 Préambule

31 Les caractéristiques de sécurité sont consignées dans la cible de sécurité [4] qui est la référence pour l'évaluation.

32 Les paragraphes 4.2 à 4.4 ci-après reprennent les éléments essentiels de cette cible.

4.2 Caractéristiques de sécurité

33 Le produit SIS, Système d'Interconnexion Sécurisé, par l'intermédiaire de l'UCC, permet de contrôler le trafic entrant et/ou sortant sur un site protégé. Ce trafic peut être :

- Libre,
- Strictement interdit,
- Autorisé ou interdit après identification et authentification de l'utilisateur,
- Autorisé ou interdit, chiffré ou non, après identification et authentification de l'UCC distante.

34 Ces modes d'accès sont gérés par l'UCC au sein d'une base de données qui permet soit d'interdire par défaut l'accès à un site, suivant le principe que tout ce qui n'est pas expressément autorisé est interdit, soit de définir des filtres spécifiques. La spécification des filtres permet d'associer aux différents modes d'accès des classes de sujets et d'objets, tels que :

- des utilisateurs ou des groupes d'utilisateurs,
- des machines, des groupes de machines, ou des sous-réseaux,
- des services, des groupes de services, ou des plages de services,
- des plages horaires.

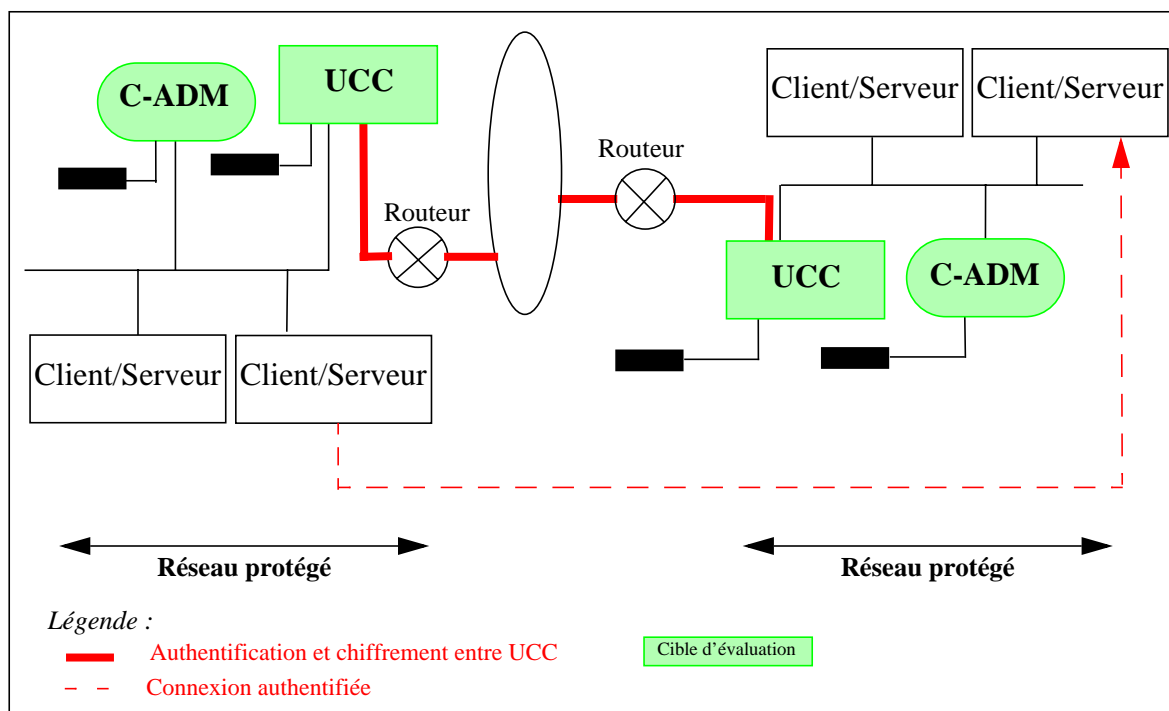
35 Afin d'établir une communication, l'UCC intercepte et stocke la demande de communication, puis recherche le mode d'accès défini par la politique de sécurité pour cette communication. L'UCC effectue alors une demande d'authentification qui permet aux deux parties de s'authentifier mutuellement. Suivant les modalités d'accès spécifiées, l'UCC commute, chiffre ou bien détruit les datagrammes de la communication.

36 L'entité distante, qui peut être une autre UCC, doit disposer d'une carte à puce pour être authentifiée. Suivant le mode d'accès défini, le code porteur de la carte est demandé systématiquement à chaque tentative de communication, ou bien n'est plus demandé après une première authentification, dans la mesure où la carte n'est pas retirée du lecteur.

- 37 L'UCC dispose d'un module de chiffrement garantissant la confidentialité des données transitant sur des réseaux ouverts, entre des sites distants équipés chacun de SIS. Le module est intégré au SIS sous compilation conditionnelle des logiciels de l'UCC : il s'agit de l'option Groupe Fermé de Machines GFM. Le chiffrement est alors mis en oeuvre pour les communications pour lesquelles ce mode d'accès est spécifié dans la base de données des filtres.
- 38 La configuration de l'UCC et la définition de la politique de sécurité s'effectuent sur la station d'administration SA, par l'intermédiaire de la C-ADM. La cohérence des données de filtrage est contrôlée avant que celles-ci ne soient transférées via le réseau, sous forme chiffrée, sur l'UCC. L'opération de transfert requiert l'authentification préalable de l'administrateur au moyen de sa carte à puce.
- 39 L'UCC enregistre les événements de sécurité dans des fichiers générés directement sur celle-ci. Les fichiers journaux d'imputabilité sont transférés sous forme chiffrée sur la station d'administration pour être audités par l'intermédiaire de la C-ADM.

4.2.1 Modes d'utilisation prévus

- 40 L'UCC est installée sur une machine placée en coupure Ethernet, en "entrée" du sous-réseau à sécuriser, comme un point de passage obligé et donc incontournable. La machine doit être stockée dans un lieu sûr.
- 41 L'UCC intercepte systématiquement toutes les communications et y applique la politique de sécurité définie par l'administrateur réseau. Elle doit permettre de contrôler l'accès à un réseau, un sous-réseau ou un serveur isolé. Cet accès filtré doit être accompagné d'une authentification de l'entité distante.
- 42 La station d'administration SA doit être connectée à l'UCC, du côté sécurisé afin d'effectuer les transferts de fichiers. Elle doit être munie d'un lecteur de carte de manière à ce que l'administrateur puisse s'authentifier auprès de l'UCC au moyen de sa carte à puce.
- 43 Chaque station cliente susceptible d'établir une communication doit être munie du logiciel d'accès LSA, et d'un lecteur de carte à puce pour être en mesure de s'authentifier auprès de l'UCC.
- 44 Les modes d'utilisation supposés du SIS dans le cadre de l'évaluation sont schématisés ci-dessous. Ces trois configurations forment un sous-ensemble des modes d'exploitation possibles du SIS.



Topologie 3 : **Configuration réseau** - les UCC protègent leur réseau local des accès depuis d'autres sites par authentification mutuelle. Elles garantissent aussi la confidentialité des échanges par le chiffrement des connexions.

4.3 Menaces

45 Dans le contexte de la cible d'évaluation, la liste des menaces identifiées dans la cible de sécurité [4] est la suivante :

- Etablissement d'une communication au travers de l'UCC par un utilisateur non autorisé,
- Utilisation de la session ouverte d'un utilisateur ayant quitté son poste et laissé sa carte à puce dans le lecteur sans se déconnecter,
- Contournement de l'UCC,
- Visualisation et modification des données de l'UCC,
- Visualisation ou altération des données échangées lors d'une communication entre deux UCC ou entre l'UCC et sa station d'administration.

4.4 Fonctions dédiées à la sécurité de la cible d'évaluation

4.4.1 Identification et authentification

- **FS1: Identification et authentification mutuelle**

C'est la fonction permettant à un utilisateur autorisé, à l'administrateur de l'UCC, ou à une UCC distante de s'authentifier auprès de l'UCC.

La fonction garantit l'identification et l'authentification mutuelle de chacune des parties en s'appuyant sur un dispositif de lecture de carte à puce.

- **FS2 : Déconnexion automatique**

Un utilisateur est automatiquement déconnecté après un temps d'inactivité paramétrable par l'intermédiaire de la C-ADM.

- **FS3 : Ré-authentification périodique**

Lors de la demande de connexion d'un utilisateur à une machine hôte au travers de l'UCC, l'authentification mutuelle initiale est suivie du contrôle des droits d'accès de l'utilisateur. Une fois la connexion établie, l'UCC adresse aléatoirement une nouvelle demande d'authentification de la carte à puce de l'utilisateur ou de l'administrateur. La période séparant deux authentifications successives est aléatoire à l'intérieur d'une plage de temps définie par l'administrateur.

4.4.2 Contrôle d'accès

- **FS4: Filtrage logiciel au niveau IP**

L'UCC est placée en coupure Ethernet sur le réseau. Tous les datagrammes sont systématiquement interceptés et contrôlés par l'UCC.

A chaque tentative de connexion au travers de l'UCC, celle-ci effectue une recherche de droits d'accès pour la communication dans la base de données chargée sur l'UCC. Selon les modalités d'accès obtenues, la communication est établie ou non.

Le contrôle d'accès est mis en oeuvre par des filtres logiciels en "entrée" et en "sortie" qui combinent les identifiants d'utilisateurs, les noms et adresses des stations clientes, les serveurs, les services, les plages horaires. A chacun de ces filtres peut être rattachée une politique de sécurité particulière : accès libre (PASSANT), accès interdit (BLOQUANT), accès autorisé après authentification (SESSION ou SERVICE), accès chiffré après authentification (CHIFFRE).

Les filtres sont définis au moyen de la C-ADM et concernent exclusivement les protocoles TCP, UDP et ICMP.

- **FS5: Commutation conditionnelle sur protocole**

La fonction permet d'autoriser ou d'interdire la commutation de certains protocoles par l'intermédiaire de la C-ADM. Le mode non commuté conduit à la destruction systématique de tous les datagrammes par l'UCC, quelle que soit l'interface de réception. Tout protocole non défini dans la base de données chargée sur l'UCC est par défaut non commuté. L'UCC offre un troisième mode filtrant pour les protocoles TCP, UDP et ICMP au travers de la fonction FS4.

4.4.3 Confidentialité

- **FS6 : Chiffrement des sessions authentifiées entre deux UCC**

La fonctionnalité de chiffrement est activée pour la partie données des protocoles TCP et UDP lorsque le filtre correspondant est activé en mode CHIFFRE sur l'UCC. La clé de chiffrement est une clé obtenue à partir de la clé de session calculée par les cartes à puce de chacune des UCC. Les clés de chiffrement résident en mémoire sur les UCC le temps de la communication. Elles sont effacées de la mémoire en fin de communication, puis enregistrées dans un fichier sur le disque de chacune des UCC.

- **FS7 : Chiffrement des données transférées entre SA et UCC**

La fonctionnalité de chiffrement assure un service de télégestion sécurisé entre la C-ADM et l'UCC. Les échanges entre la SA et l'UCC concernent les fichiers de la base de données téléchargés sur l'UCC, et les fichiers d'audit rapatriés vers la SA. Le chiffrement des données est réalisé à la volée durant leur transfert, datagramme par datagrammes. La clé de chiffrement est obtenue à partir de la clé de session calculée par les cartes à puce de l'UCC et de la SA. Les clés de chiffrement résident en mémoire sur l'UCC et la SA le temps de la communication. Elles sont effacées de la mémoire en fin de communication. Le paramétrage est réalisé par

l'administrateur du SIS directement sur l'UCC. Il consiste à définir les paramètres des droits d'utilisation de la télégestion (interface de communication, adresse IP des SA, identité des administrateurs).

4.4.4 Imputabilité

- **FS8 : Journalisation des communications**

Toutes les tentatives de communication effectuées au travers de l'UCC sont enregistrées en continu dans deux types de fichiers binaires : le fichier journal et le fichier catalogue contenant la liste des fichiers journaux. Les informations enregistrées sont les adresses IP des machines source et destination de la communication, le protocole utilisé, le type de service réseau demandé, le nom de l'utilisateur, la cause de fin de connexion, le numéro de filtre mis en oeuvre, l'horodatage de début et fin de communication, le nombre de datagrammes échangés et le volume d'informations échangées en nombre d'octets. Ces fichiers résidant sur l'UCC sont transférés pour analyse sur la SA via le service de télégestion sécurisée.

- **FS9 : Journalisation des opérations de transfert de fichiers**

Toutes les opérations de télégestion entre l'UCC et la SA, relatives au chargement de la configuration ou au rapatriement des journaux des communications, sont enregistrées dans un fichier texte sur l'UCC. Les informations enregistrées sont la date et l'heure du transfert, l'identité de la carte à puce de l'administrateur authentifié, le type de l'opération réalisée (téléchargement ou télérapatriement), la cible de l'opération (nom de la base de données, nom du fichier journal).

- **FS10 : Enregistrement des clés de chiffrement**

Les clés utilisées pour le chiffrement des données échangées dans les communications entre deux UCC distantes, sont enregistrées dans un fichier binaire sur l'UCC. Ce fichier peut être visualisé directement sur l'UCC. Les informations enregistrées sont la date et l'heure de création du fichier, la durée de conservation des enregistrements, la clé utilisée pour le chiffrement et/ou le déchiffrement, la date et l'heure de la communication chiffrée, les adresses IP source et destination de la communication, les ports source et destination de la communication, le sens de la communication, les adresses IP des UCC locale et distante.

4.4.5 Audit

- **FS11 : Visualisation et impression des journaux des communications**

La visualisation et/ou l'impression des journaux est réalisée sur la SA, après rapatriement par le service de télégestion.

- **FS12 : Visualisation des opérations de transfert de fichiers**

La visualisation des enregistrements des opérations de transfert de données entre l'UCC et la SA, s'opère sur la SA, après leur rapatriement sur la SA par le service de télégestion, par l'intermédiaire de la C-ADM.

4.4.6 Réutilisation d'objet

- **FS13 : Remise à zéro de chaque contexte de sécurité après usage**

Une zone mémoire est allouée statiquement par les modules logiciels de l'UCC. Lors de chaque tentative de communication un emplacement ou contexte de sécurité est réservé au sein de cette zone pour stocker les données relatives à la communication. En fin de communication, cet emplacement est effacé et rendu disponible à une autre communication.

4.5 Rapport Technique d'Évaluation

50 Les résultats de l'évaluation sont exposés dans le rapport technique d'évaluation portant la référence FT.CNET.3C.KLA.RE.001 [9].

4.6 Principaux résultats de l'évaluation

4.6.1 Exigences de conformité

Spécifications des besoins

51 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.2, E3.3 et E3.4 du document ITSEC.

52 La cible de sécurité rédigée par le commanditaire décrit l'ensemble des fonctions dédiées à la sécurité. L'argumentaire du produit précise l'environnement d'utilisation prévu ainsi que le mode d'utilisation prévu. Les objectifs de sécurité sont précisés. Une correspondance est établie entre les fonctions dédiées à la sécurité et les menaces.

53 Le document cible de sécurité [4] précise comment les fonctions dédiées à la sécurité sont appropriées au mode d'utilisation prévu et adéquates pour contrer les menaces supposées. Les évaluateurs se sont assurés de l'absence d'incohérence dans la cible de sécurité.

Conception générale

54 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.5, E3.6 et E3.7 du document ITSEC.

55 Le dossier intitulé "Architecture de la cible d'évaluation" décrit la structure générale du produit, ainsi que l'ensemble des composants logiciels, qui sont tous

dédiés à la sécurité. Les interfaces externes des composants logiciels sont également décrites. La réalisation des fonctions dédiées à la sécurité de la cible de sécurité [4] est décrite pour chacun des composants. La manière dont les composants principaux réalisent chacune des fonctions dédiées à la sécurité est également décrite.

Conception détaillée

56 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.8, E3.9 et E3.10 du document ITSEC.

57 Le dossier de conception détaillée fournit la conception des composants élémentaires qui mettent en oeuvre les composants principaux issus de la conception générale. La spécification ainsi que les interfaces des composants élémentaires sont décrites. Toutes les fonctions dédiées à la sécurité de la cible de sécurité [4] sont décrites dans la conception détaillée. Les mécanismes de sécurité réalisant l'ensemble des fonctions dédiées à la sécurité sont décrits ; leurs spécifications (rôle et fonction) sont définies. Les liens qui existent entre les fonctions dédiées à la sécurité et les mécanismes sont établis. La manière dont les mécanismes procurent les fonctions est décrite. La traçabilité entre les fonctions dédiées à la sécurité et les mécanismes de sécurité puis les composants est vérifiée.

Réalisation

58 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.11, E3.12 et E3.13 du document ITSEC.

59 La description de la correspondance entre le code source du SIS et la conception détaillée a permis de vérifier la traçabilité des fonctions et des mécanismes dédiés à la sécurité. Cette correspondance met en relation chacun des composants élémentaires de la conception détaillée avec les éléments descriptifs de la réalisation. Chacune de ces relations a pu être vérifiée par les évaluateurs. Par ailleurs, une analyse détaillée du code source ainsi que de la description de la correspondance a été effectuée par les évaluateurs pour rechercher des vulnérabilités potentielles.

60 Une documentation détaillée de tests a été fournie par le biais des cahiers de recette des principales fonctionnalités du SIS : la C-ADM, le logiciel d'accès sécurisé, la télégestion, la réauthentification périodique, le filtrage IP, le passage à l'an 2000; ces documentations décrivent le plan des tests, l'objectif des tests, les procédures de tests à réaliser ainsi que les résultats des tests. Le document chapeau intitulé "Documentation de test" décrit la correspondance entre les tests et les mécanismes de sécurité tels qu'ils sont décrits dans la conception détaillée, et les fonctions dédiées à la sécurité spécifiées dans la cible de sécurité.

61 Les évaluateurs ont procédé à un échantillonnage des programmes de tests sur la configuration de tests qui leur a été livrée par le développeur. La procédure d'échantillonnage a été jugée conforme aux exigences du niveau d'évaluation E3 et en accord avec la Bibliothèque d'interprétation commune [3].

62 Les résultats des tests correspondent effectivement aux résultats attendus. La couverture des tests de la cible d'évaluation a été estimée comme acceptable.

Gestion de configuration

63 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.15, E3.16 et E3.17 du document ITSEC.

64 Le système de gestion de configuration du développeur a été analysé. Chacune des tâches a fait l'objet d'une inspection des procédures et d'une visite sur site pour vérifier que les procédures sont appliquées.

65 Le développement du SIS s'appuie sur un système de gestion de configuration comportant une procédure de réception des composants élémentaires de la cible d'évaluation ainsi que de sa documentation. La liste de configuration du produit énumère l'ensemble des composants de la cible d'évaluation. Ce système de gestion de configuration apporte la garantie nécessaire permettant de préciser que seuls les changements autorisés sont possibles. Un ensemble de procédures intégrées dans le système qualité de l'entreprise décrivent l'utilisation pratique du système de gestion de configuration du produit.

66 La visite du site de développement du SIS à Rennes (ACE Timing) a permis de vérifier que les procédures décrites sont appliquées.

67 La préparation et la portée de ces visites (chaîne de développement et de production de la cible d'évaluation) sont en accord avec la Bibliothèque d'interprétation commune [3].

Langages de programmation

68 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.18, E3.19 et E3.20 du document ITSEC.

69 Les langages utilisés pour la réalisation du code source sont les langages C, Shell Unix, Perl, Microsoft Access Basic. Le langage C utilisé est conforme à la norme ANSI : les instructions du langage sont de fait clairement définies. Les autres langages sont correctement définis et accompagnés des documents de référence. Les directives de compilation du code source écrit en langage C n'ont pas été analysées puisqu'il s'agit d'un compilateur C ANSI. Le compilateur Access Basic 2.0 pour Windows 3.1 n'admet pas de directive particulière. Les options du langage de script shell sont complètement documentées et disponibles par la commande Unix *man*.

Sécurité des développeurs

70 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.21, E3.22 et E3.23 du document ITSEC.

71 Les évaluateurs ont analysé la sécurité du développement chez le développeur. Chacune des tâches a fait l'objet d'une inspection des procédures.

72 Des procédures physiques, organisationnelles, techniques, liées au personnel assurent un niveau de protection de la cible d'évaluation, de ses constituants ainsi que de sa documentation qui répond aux exigences du niveau d'évaluation E3.

73 Une visite sur le site de développement a permis de vérifier l'application de ces procédures.

Documentation utilisateur

74 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.25, E3.26, E3.27 du document ITSEC.

75 Deux catégories d'utilisateurs finals sont définies : l'utilisateur porteur d'une carte à puce et l'utilisateur non authentifiable. Les modes d'utilisation supposés de la cible d'évaluation identifiés dans la cible de sécurité excluent le dernier type d'utilisateur. Par conséquent, dans le cadre de l'évaluation les utilisateurs finals sont assimilés aux utilisateurs authentifiables.

76 Les fonctions dédiées à la sécurité concernant l'utilisateur final apparaissent dans la documentation qui donne les lignes directrices pour une utilisation sûre.

Documentation d'administration

77 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.28, E3.29, E3.30 du document ITSEC.

78 La documentation d'administration du SIS définit trois rôles distincts : l'administrateur principal, le responsable de la politique de sécurité et le responsable de l'audit des traces et des historiques.

79 La documentation d'administration décrit comment la cible d'évaluation doit être administrée de façon sûre. La documentation identifie les paramètres de sécurité qui sont de la responsabilité de l'administrateur.

Livraison et configuration

80 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.32, E3.33 et E3.34 du document ITSEC.

81 Le processus de génération de la cible d'évaluation a été vérifié chez l'évaluateur. La génération des supports d'installation n'admet pas d'option. En revanche, les options choisies lors de l'installation de l'UCC sont auditées afin de pouvoir a posteriori reconstituer exactement comment et quand la cible d'évaluation a été générée.

Démarrage et exploitation

82 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.35, E3.36 et E3.37 du document ITSEC.

- 83 Les procédures de démarrage de la C-ADM et du LSA n'ont pas d'impact sur la sécurité.
- 84 La vérification des traces d'audit générées au cours du démarrage initial de la cible d'évaluation, ou suite à une opération de maintenance, ou encore lors d'un démarrage courant, permet de contrôler l'intégrité de l'UCC.
- 85 Les justifications données par le développeur permettent de montrer le maintien de la sécurité lors des phases de démarrage et d'exploitation, spécialement lorsque certaines fonctions dédiées à la sécurité se trouvent désactivées.
- 86 Dans le cadre de la cible d'évaluation, il n'existe aucun composant matériel dédié à la sécurité.

4.6.2 Exigences en efficacité

Pertinence

- 87 Les critères ITSEC pour cet aspect de l'efficacité sont définis dans les paragraphes 3.14, 3.15 et 3.16 du document ITSEC.
- 88 L'analyse de pertinence a été faite à deux niveaux : une analyse de pertinence des fonctions qui montre comment les menaces sont contrées par les fonctions dédiées à la sécurité et une analyse de pertinence des mécanismes dédiés à la sécurité qui montrent comment les menaces sont contrées par ces mécanismes.
- 89 Les analyses de pertinence des développeurs s'appuient sur la conception détaillée de la cible d'évaluation.
- 90 Pour cela, chaque menace identifiée dans la cible de sécurité a été décrite ; la description des liens entre les fonctions dédiées à la sécurité et les menaces d'une part puis entre les mécanismes dédiés à la sécurité et les menaces d'autre part a permis de montrer que chacune des menaces est convenablement contrée, dans le contexte de la cible d'évaluation, par une ou plusieurs fonctions dédiées à la sécurité.

Cohésion

- 91 Les critères ITSEC pour cet aspect de l'efficacité sont définis dans les paragraphes 3.18, 3.19 et 3.20 du document ITSEC.
- 92 L'analyse de cohésion a également été faite à deux niveaux : une analyse de cohésion des fonctions qui montre qu'aucune interaction entre deux fonctions dédiées à la sécurité ne crée de faiblesse pour la sécurité ; puis une analyse de cohésion des mécanismes dédiés à la sécurité qui montre que les mécanismes dédiés à la sécurité coopèrent pour former un ensemble intégré et efficace.
- 93 Les analyses de cohésion des développeurs ont pris en compte la conception détaillée de la cible d'évaluation. Les évaluateurs ont vérifié l'absence de conflit ou

de contradiction d'une part, entre les fonctions dédiées à la sécurité, et d'autre part entre les mécanismes dédiés à la sécurité.

Résistance des mécanismes

94 Les critères ITSEC pour cet aspect de l'efficacité sont définis dans les paragraphes 3.22, 3.23 et 3.24 du document ITSEC.

95 Le développeur a rédigé une analyse de la résistance des mécanismes. La liste des mécanismes critiques du SIS a été établie. Les évaluateurs ont analysé cette documentation. La cotation indépendante des mécanismes faite par les évaluateurs est en accord avec les analyses du développeur. La cotation globale des mécanismes est considérée comme moyenne. Les tests de pénétration ont permis de confirmer cette cotation.

Facilité d'emploi

96 Les critères ITSEC pour cet aspect de l'efficacité sont définis dans les paragraphes 3.31, 3.32 et 3.33 du document ITSEC.

97 La fourniture de facilité d'emploi associée à la documentation d'exploitation de la cible d'évaluation identifie les modes d'exploitation de la cible d'évaluation ainsi que les conséquences et les implications de ces modes sur le maintien d'une exploitation sûre de la cible d'évaluation. Les évaluateurs ont réalisé des tests complémentaires afin de confirmer les résultats de la facilité d'emploi.

Vulnérabilités de construction et en exploitation

98 Les critères ITSEC pour ces aspects de l'efficacité sont définis dans les paragraphes 3.26, 3.27, 3.28 et 3.35, 3.36, 3.37 du document ITSEC.

99 Les développeurs ont décrit une liste de vulnérabilités potentielles connues sur la cible d'évaluation. Les évaluateurs ont mené des tests de pénétration sur la cible d'évaluation, en prenant en compte un niveau moyen de ressources de l'attaquant tel que défini par la cotation de la résistance des mécanismes.

4.6.3 Verdicts

100 Pour tous les aspects des critères ITSEC identifiés ci-dessus, un avis "réussite" a été émis.

Chapitre 5

Recommandations d'utilisation

- 101 Le produit “ Système d'Interconnexion Sécurisé ” est soumis aux recommandations d'utilisation précisées ci-après.
- 102 Le produit doit être utilisé conformément à l'environnement d'utilisation prévu et au mode d'utilisation prévu tels qu'ils sont définis dans la cible de sécurité [4].
- 103 La station d'administration SA doit être placée du côté sécurisé du réseau protégé par l'UCC.
- 104 Chaque station cliente, pour établir une communication avec une machine du réseau protégé, doit être munie du logiciel d'accès LSA et d'un lecteur de carte à puce pour être en mesure de s'authentifier auprès de l'UCC.
- 105 L'UCC doit obligatoirement être placée derrière un routeur qui interdit l'option IP de source-routing et rejette les paquets ARP.
- 106 Aucun modem ne doit être installé sur l'une quelconque des machines du réseau protégé.
- 107 L'UCC n'opérant qu'un filtrage au niveau IP, il est recommandé d'installer des relais applicatifs à l'entrée du réseau protégé, et de mettre en place des mécanismes d'authentification et de chiffrement au niveau applicatif.
- 108 Il est conseillé d'héberger le serveur DNS secondaire sur un autre site lui-même protégé.
- 109 Les filtres de l'UCC doivent être configurés de manière à :
- rejeter les messages “Echo Reply” en provenance de l'extérieur,
 - interdire le protocole *ftp* sur l'interface externe de l'UCC,
 - rejeter toute requête de re-routage (RIP, OSPF...) en provenance de l'extérieur,
 - rejeter toute requête SNMP en provenance de l'extérieur,
 - activer la commande d'interception de données qui permet d'interrompre les connexions *ftp* invoquant la commande PORT,
 - rejeter tout accès depuis l'extérieur vers le serveur DNS primaire du réseau protégé.
- 110 L'administration du SIS requiert, de la part de l'administrateur, une expertise dans le domaine des réseaux.
- 111 Il est recommandé d'équiper les machines des utilisateurs de logiciels anti-virus.

- 112 Il est recommandé aux utilisateurs du réseau protégé de ne pas télécharger d'applets java ou de contrôles Active-X, ainsi que de ne pas exploiter Javascript sur leurs stations.

Chapitre 6

Certification

6.1 Objet

113 Le produit “Système d’Interconnexion Sécurisé SIS (référence : SIS - UCC V3.2(1), LSA V3.2, C-ADM V3.2)” dont les caractéristiques de sécurité sont définies dans le chapitre 4 du présent rapport, satisfait aux exigences du **niveau d’évaluation E3**.

114 La résistance minimum des mécanismes est cotée **moyenne**.

115 La recherche de vulnérabilités exploitables au cours de l’évaluation a été définie par la quantité d’informations disponibles pour le niveau E3 et par la compétence, l’opportunité et les ressources correspondant à la cotation moyenne de la résistance minimum des mécanismes.

6.2 Portée de la certification

116 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle (d’autant plus faible que le niveau d’évaluation est élevé) que des vulnérabilités exploitables n’aient pas été découvertes.

117 Le certificat ne s’applique qu’à la version évaluée du produit (référence : SIS - UCC V3.2(1), LSA V3.2, C-ADM V3.2).

118 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

119 L’utilisation du logo propre à l’Accord de Reconnaissance Mutuelle :

- confirme que ce certificat a été délivré sous l’autorité d’un organisme de certification qualifié qui fait partie du Groupe d’Accord,
- indique que l’autorité de délivrance déclare qu’il s’agit d’un “certificat conforme” comme défini dans l’Accord,
- établit par conséquent des éléments pour baser la confiance dans le fait que le certificat est un “certificat conforme”, bien que ne pouvant en donner une garantie, et qu’il sera reconnu en pratique par les autres membres du Groupe d’Accord.

120 Les jugements contenus dans le certificat et le rapport de certification sont ceux de l'organisme de certification qualifié qui a procédé à la délivrance et ceux du centre d'évaluation de la sécurité des technologies de l'information qui a conduit l'évaluation. L'utilisation du logo de cet Accord n'entraîne pas la reconnaissance par les autres membres d'une quelconque responsabilité relative à ces jugements ou à tout dommage encouru en raison de la confiance accordée à ces jugements par une tierce partie.

Annexe

Glossaire

C-ADM

Console d'administration.

Datagramme IP

Unité d'information échangée sur une interconnexion TCP/IP.

DNS

Domain Name Server - Serveur de noms de domaines exécutant sur requêtes des conversions de noms en adresse IP et la conversion réciproque.

FTP

File Transfer Protocol - Protocole utilisé pour le transfert de fichiers.

HTTP

HyperText Transfer Protocol - Protocole utilisé pour le transfert de pages web.

ICMP

Internet Control Message Protocol - Protocole utilisé pour la signalisation de cas d'erreur et le contrôle des opérations de la couche IP.

IHM

Interface Homme Machine.

IP

Internet Protocol.

ITSEC

Critères d'évaluation de la sécurité des systèmes informatiques, version 1.2.

ITSEM

Manuel d'évaluation de la sécurité des technologies de l'information, version 1.0.

LSA

Logiciel de Sécurisation d'Accès.

SA

Station d'administration.

SIS

Système d'Interconnexion Sécurisé.

SNMP

Simple Network Management Protocol - Protocole utilisé pour le diagnostic de matériels distants.

SMTP

Simple Mail Transfer Protocol - Protocole de transfert de messages.

TCP

Transmission Control Protocol - Protocole de la famille TCP/IP de niveau transport, orienté connexion.

TFTP

Trivial File Transfer Protocol - Protocole utilisé pour le transfert de fichiers, en mode non connecté sans authentification sur le serveur (UDP).

UCC

Unité de Contrôle et de Commutation.

UDP

User Datagram Protocol - Protocole de la famille TCP/IP de niveau transport sans contrôle de flux.

Références

- [1] Critères d'évaluation de la sécurité des systèmes informatiques version 1.2 de juin 1991.
- [2] Manuel d'évaluation de la sécurité des technologies de l'information version 1.0 de septembre 1993.
- [3] Bibliothèque d'interprétation commune (Joint Interpretation Library v1.0).
- [4] "SIS - Cible de sécurité" référencée SIS-CS.DOC, version 1.31 du 29/04/99.
- [5] "Manuel de référence pour SIS v3.2/4.0" version 2.1(b) du 16/11/98,
- [6] "Manuel d'installation de l'UCC" référencé MAINSUCC.DOC version 2.11 du 02/11/98.
- [7] "Manuel d'exploitation des composants" référencé ME-CMP.DOC version 1.01 du 11/03/98.
- [8] "Procédure de vérification des installations et contrôle de l'intégrité de l'UCC" version 1.20 du 03/03/99.
- [9] "Rapport technique d'évaluation" référencé FT.CNET.3C.KLA.RE.001 version 1.0 du 31/03/99.

