SCNET4 (TM)

VERSION SECURE

NCS
SCALINE

COMMUNICATIONS SÉCURISÉES BADGES CHIFFRÉS

Entreprise ou institution, toute organisation est confrontée aux problèmes de sécurité de son personnel, de protection et de défense de ses centres vitaux et de ses secrets. Une solution à ces problèmes passe par l'utilisation de systèmes intégrés de contrôle d'accès électronique, de gestion de sûreté et de vidéosurveillance.

La mise en œuvre de moyens informatiques et électroniques ne suffit cependant pas. Il faut aussi veiller à garantir l'authenticité des identités, la sécurisation des données et des procédures, ainsi que la résilience et à l'intégrité des moyens déployés.

Un système intégré de contrôle d'accès partage en effet des données et des moyens de communication avec d'autres systèmes informatiques des entreprises. Il doit donc garantir un niveau au moins égal de protection contre les attaques internes et externes et de confidentialité des communications et des informations.

Le serveur, les postes clients et les automates, qui utilisent les réseaux de l'entreprise doivent donc intégrer directement les politiques de sécurité de celle-ci.

Les liaisons filaires entre automates et lecteurs ainsi que les liaisons radio entre les lecteurs et les badges, sur lesquelles s'échangent les données d'identification nécessitent aussi d'intégrer des mécanismes inviolables de chiffrement et d'authentification.

SCNET4™ SECURE

SCNET4™ SECURE est un système SCNET4™ Version 3 complété de plusieurs options visant à garantir la sécurisation des données et des procédures de gestion, la résilience et l'intégrité des moyens déployés et l'authenticité des identités.

Communications

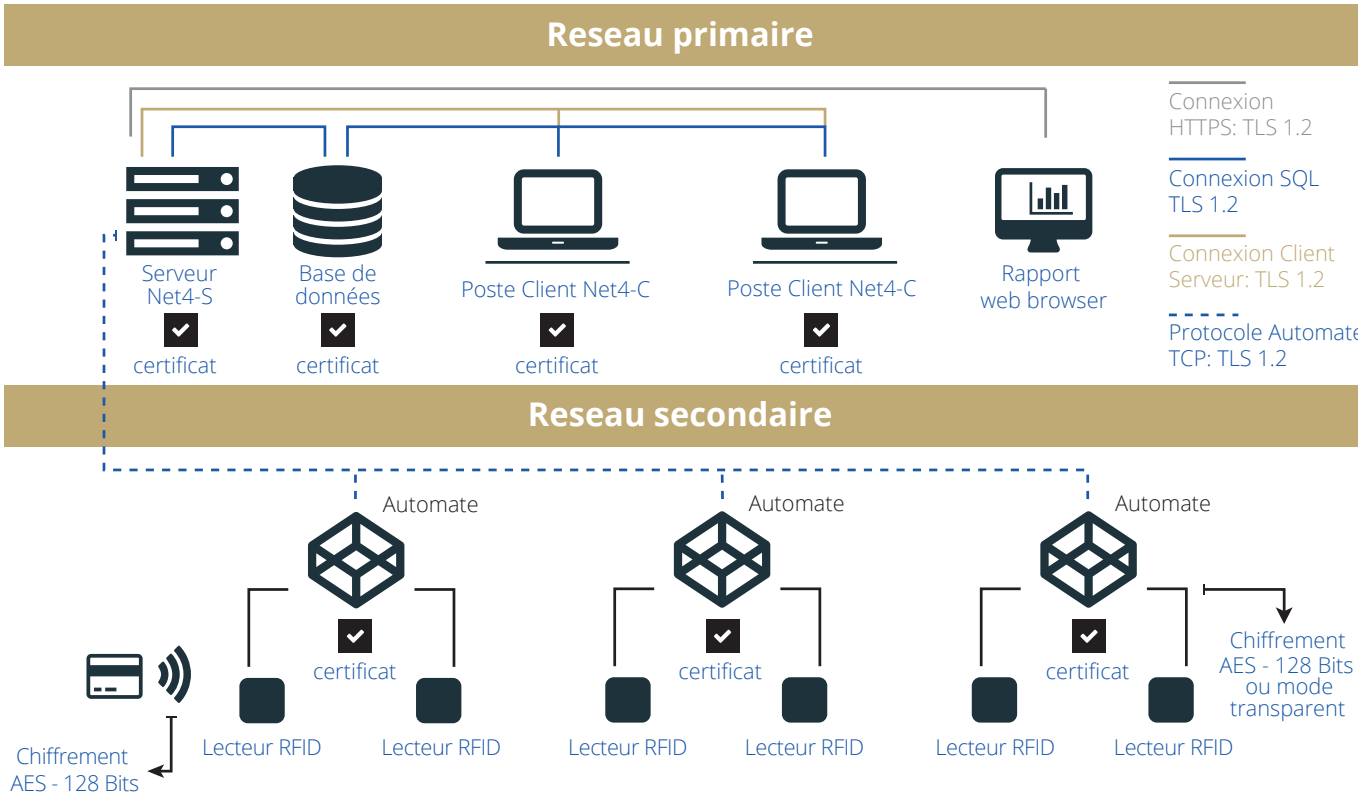
SECURE intègre des méthodes de sécurité des communications entre tous les appareils de l'installation : Serveur NET4S™, postes clients NET4C™, automates de la gamme SC4x5™ et lecteurs ARC de la gamme Architect® de STid®

Badges

SECURE gère de façon sécurisée les badges d'accès de type MIFARE DESFire® EV1.

Processus

SECURE sécurise les processus de gestion du système et d'accès aux données d'exploitation.



Cryptographie : Un aperçu.

Le but de la cryptographie est de fournir des services de sécurité pour garantir des propriétés comme

- La confidentialité : Les données ne sont lisibles que par ceux qui en ont reçu le droit,
- L'intégrité : Les données reçues sont bien celles envoyées,
- L'authentification : L'interlocuteur est bien celui que l'on croit,
- ou encore la non répudiation : La procédure d'échange garantit sans équivoque que l'auteur du message l'a bien envoyé et que le destinataire l'a bien reçu.

La confidentialité est assurée

- soit par l'usage du chiffrement dit symétrique des données au moyen d'une clé secrète connue des deux parties (Par exemple : AES - Advanced Encryption System).
- soit par l'usage du chiffrement dit asymétrique des données au moyen d'une paire de clés : une clé publique connue de tous les émetteurs pour réaliser le chiffrement; une clé privée connue du seul récepteur avec laquelle celui-ci réalise le déchiffrement. (Par exemple RSA -Rivest Shamir Adleman).

L'intégrité des données est assurée par la signature de celles-ci. Cette signature est calculée via un condensé univoque de ces données. Ce condensé est calculé par un algorithme de « hachage » (Par exemple : SHA -Secure Hash Algorithm) tel que la reconstitution inverse des données n'est pas possible.

L'authentification et la non répudiation sont assurées par la signature des données calculée en chiffrant au moyen d'une clé privée un condensé univoque de ces données calculé par hachage et vérifiée en la déchiffrant au moyen de la clé publique correspondante.

Ces services évitent par exemple qu'un badge d'accès soit contrefait, qu'un message intercepté frauduleusement ne permette de connaître des clés secrètes de programmation de badges ou des paramètres d'autorisation d'accès, que des commandes frauduleuses soient insérées dans un message ou qu'un système soit hacké, soit pour l'empêcher de fonctionner, soit pour en extraire des données confidentielles sur les personnes et sur l'entreprise, soit pour s'en servir pour atteindre d'autres ressources de l'entreprise.

SÉCURITÉ DES COMMUNICATIONS

La sécurité des réseaux.

Les liaisons entre le serveur NET4S™, les postes clients NET4C™ et les automates SC4x5™ utilisent soit les réseaux de l'entreprise (intranet ou WAN) soit des réseaux dédiés. Il est souvent nécessaire d'établir aussi des liens avec des ressources d'entreprise comme l'informatique des Ressources Humains ou de partager des moyens d'accès distants. Il est donc obligatoire que la sécurisation du système de contrôle d'accès réponde aux mêmes principes que ceux appliqués à la sécurisation des moyens informatiques de l'entreprise.

Cryptographie de l'automate au lecteur

Dans SCNET4™ SECURE, les automates peuvent dialoguer directement en mode « transparent » avec les badges d'accès MIFARE DESFire EV1, ce dialogue étant sécurisé par un chiffrement AES 128 bits. La sécurité des liaisons entre les automates SC4x5™ et les lecteurs d'accès ARC de la gamme Architect peut aussi être assurée d'une part par le chiffrement des échanges (AES) et d'autre part par la signature de ces échanges au moyen d'un code d'authentification de message généré par une fonction de hachage (HMAC) et associé à une clé secrète. Les clés de chiffrement et d'authentification sont des clés de session dérivées de clés secrètes.

Pare-feu.

Les automates SC4x5™ sont équipés d'un pare-feu (« Firewall ») qui filtre les données échangées avec le réseau. Il n'autorise que les communications explicitement autorisées et bloque les ports non indispensables à l'application.

Non substitution.

Le serveur NET4™ est authentifié par une clé de sécurité. Cette clé induit une identification unique du serveur par les automates SC4x5™ et des automates par le serveur, protégeant l'ensemble contre toute tentative de substitution.

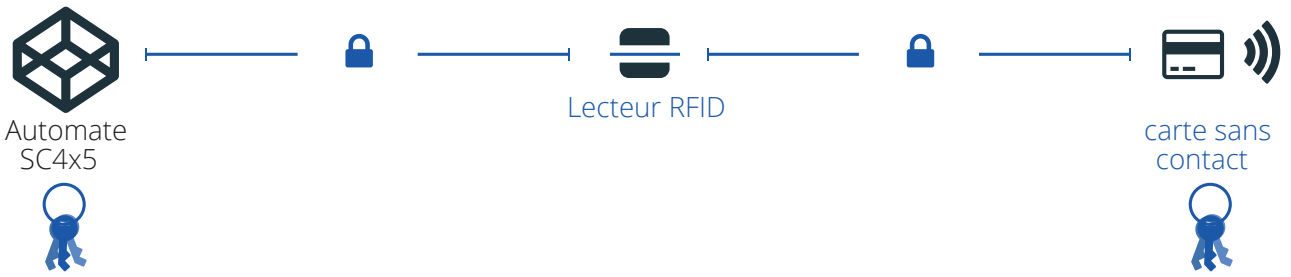
Ces clés de session automate-lecteur sont donc:

Confidentielles :
Elles ne font l'objet d'aucune publication

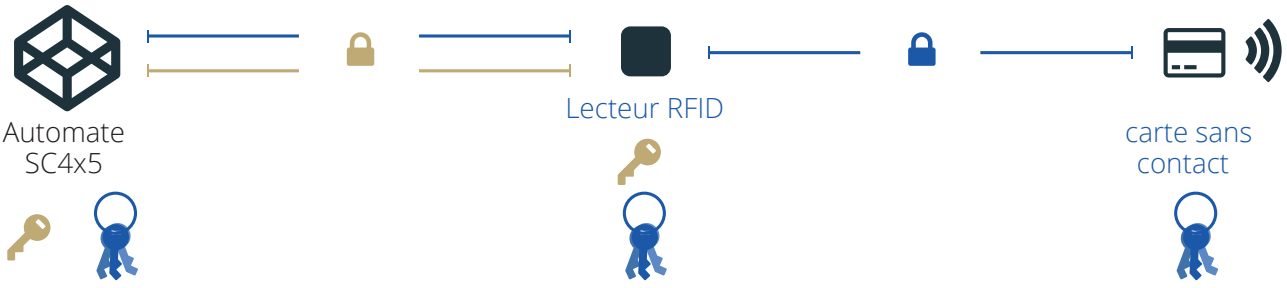
Uniques:
Elles sont différentes pour chaque couple en dialogue

Variables :
Elles changent à chaque nouvelle session

Mode transparent

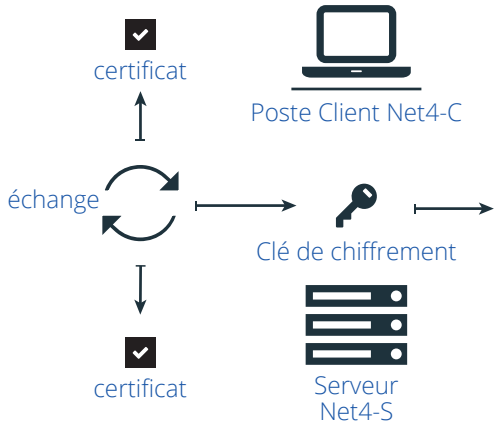


Mode sécurisé



Les standards TLS et HTTPS

Les liaisons SCNET4™ SECURE entre postes informatiques et entre serveur et automates sont sécurisées par le protocole standard TLS 1.2 (Transport Layer Security). Grâce notamment à la certification des interlocuteurs et à la cryptographie à clés publique/privée, cette méthode est plus sécurisée qu'un simple chiffrement des données par AES 128 bits au moyen d'une clé secrète fixe ; elle permet aussi d'intégrer le système dans la politique de l'entreprise relative à la sécurisation de ses réseaux informatiques.



Chaque automate SC4x5™ contient un serveur Web qui permet des opérations de paramétrage et de maintenance. L'accès à ce serveur web embarqué dans les automates est sécurisé par le protocole HTTPS qui s'appuie sur TLS.

TLS : Un aperçu

Ce protocole standard, utilisé par la majorité des réseaux sécurisés, permet à deux parties

- De s'authentifier au moyen de la cryptographie asymétrique,
- De décider de la suite cryptographique qu'elles vont employer pour sécuriser leurs communications,
- D'échanger de manière sécurisée pendant l'ouverture de leur dialogue, puis à intervalles réguliers, la clé secrète qu'elles vont utiliser pendant la session de dialogue.

Cette clé de session calculée est donc

Confidentielle :
elle ne fait l'objet d'aucune publication,

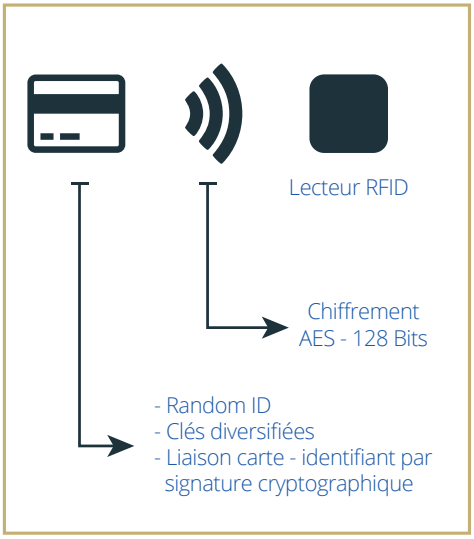
Unique :
elle est différente pour chaque couple en dialogue

Variable :
elle change à chaque nouvelle session.

Les échanges sont ensuite chiffrés par l'algorithme sélectionné et au moyen de cette clé de session. Une fonction de hachage est également utilisée pour assurer l'intégrité et l'authentification des données.

BADGES D'ACCÈS MIFARE® DESFIRE® EV1 ET APPLICATION SÉCURISÉE

Les badges MIFARE DESFire EV1 utilisés dans SCNET4™ SECURE contiennent une application sécurisée de contrôle d'accès. Celle-ci comporte des fichiers contenant le code d'identification du porteur. L'accès à ces fichiers est protégé par des clés.



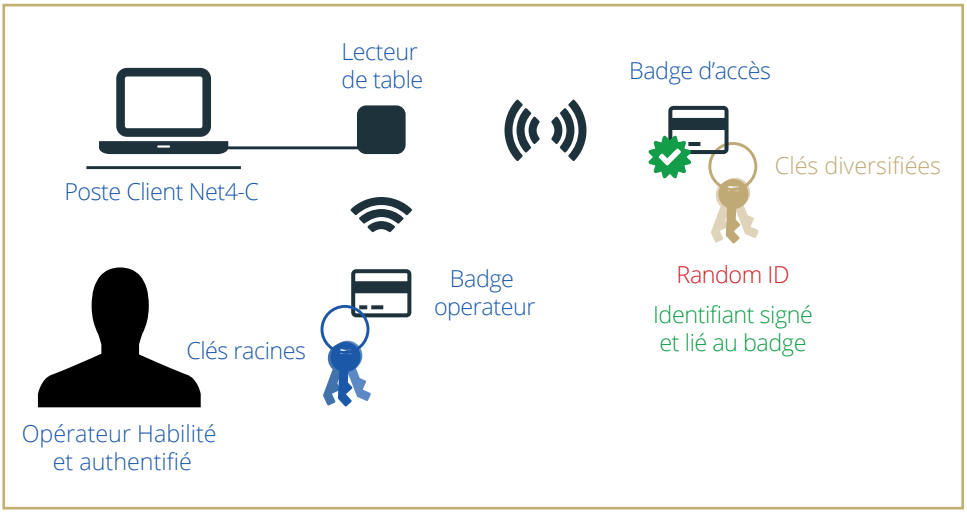
La sécurité du badge est renforcée :

- Par l'utilisation d'une identification (dite abusivement « numéro de série ») aléatoire (Random Identification – RID) de la carte au lieu de l'UID fixe (Unique Identification Code) qui n'est pas accessible ;
- Par l'utilisation de clés diversifiées d'accès au contenu pour la lecture, l'écriture ou le changement ; ainsi chaque badge contiendra des clés différentes ;
- Par l'utilisation d'un code d'identification de la personne accompagné d'une signature appariant le code et le badge (Anti clonage).

Sécurité du contenu des badges

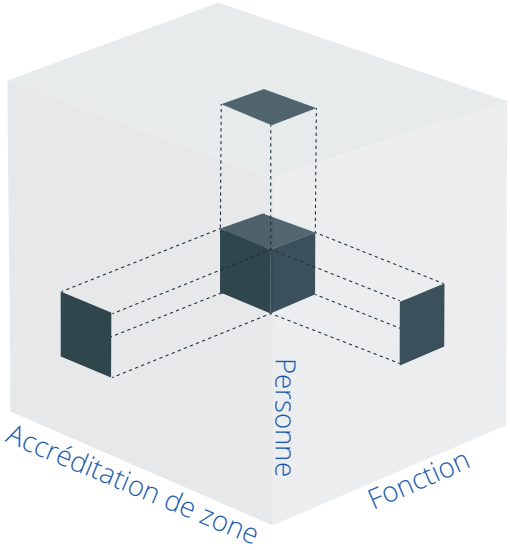
SCNET4™ SECURE utilise des clés racines dont la définition est le privilège du responsable du système. Elles ne sont connues que de lui seul. Certaines clés racines de sécurisation des badges permettent de générer les clés diversifiées, propres à chaque badge utilisateur, ouvrant l'accès à leur contenu et qui y seront inscrites. D'autres clés racines permettent de signer, par chiffrement le code d'identification de chaque personne, programmé par des opérateurs habilités à cette fin, code qui sera inscrit dans le badge.

Les badges MIFARE DESFire EV1 qui seront distribués aux utilisateurs pour leur permettre l'accès aux locaux, sont créés par des opérateurs habilités et authentifiés. Ceux-ci utilisent pour s'authentifier leur carte individuelle d'habilitation d'accès au système. Cette carte individuelle d'opérateur contient, sous forme sécurisée, des clés racines de sécurisation des badges, que ces opérateurs ne connaissent pas, ne pouvant ni les lire ni les modifier.



Ces clés racines sont envoyées sous forme chiffrée, à partir de la carte individuelle d'habilitation des opérateurs, à travers le réseau aux automates. Une fois l'opération réalisée, ces clés racines sont effacées des ordinateurs, aucune clé racine n'étant conservée par le système. Suivant que l'option « mode transparent » est activée ou non, les clés sont soit conservées sous forme cryptée (AES256) dans l'automate, la clé de chiffrement étant elle-même conservée dans un registre hardware protégé, soit conservées dans une zone sécurisée inaccessible dans les lecteurs ; ces clés seront effacées en cas de coupure de courant ou de tentative de fraude ou d'arrachement.

SECURE
PROCESSUS DE GESTION



Le badge Maître.

Dans SCNET4™ SECURE, des clés maîtresses du système sont définies par le gestionnaire principal du système ; elles servent à définir d'autres clés de sécurité nécessaires au fonctionnement du système, générées par calcul et non publiées. Ces clés maîtresses, une fois utilisées, ne sont pas conservées par le serveur. Elles sont enregistrées de façon sécurisée dans un badge MIFARE DESFire EV1 maître protégé par une authentification forte : Il faut posséder le badge et le mot de passe sécurisant les secrets pour accéder à ceux-ci. Ce badge unique est sous la responsabilité exclusive du gestionnaire principal du système.

Les accès au système.

L'accès aux postes clients (Postes de travail des opérateurs) est sécurisé par l'authentification de chaque opérateur nécessitant une carte (MIFARE DESFire® EV1) individuelle d'habilitation ; chaque carte est créée par le gestionnaire principal du système grâce à sa carte maîtresse. Ces cartes des opérateurs sécurisent leurs droits individualisés d'accès à des informations et à des fonctions. Ces droits sont accordés par le gestionnaire principal du système par le biais des classes d'opération : ils portent sur l'accès aux fonctions du système, aux données de contrôle et de gestion, aux zones du site en fonction de leur niveau de sûreté et aux données de chaque personne ayant accès au site en fonction de son degré d'accréditation.

La programmation des badges

L'attribution d'un code d'identité à un badge d'accès est régie par des règles établies par le gestionnaire principal du système. Celui-ci peut se réserver l'habilitation à la définition des KPF™ (Key-Protocol-Format ou Clé-Protocole-Format) qui permet de programmer le format à appliquer aux codes d'identification des badges d'accès. (Note : Il détient déjà le contrôle sur les clés d'accès au contenu des badges). Ce format peut être défini de telle façon que le code physique inscrit n'apparaisse jamais dans les données accessibles.

L'attribution des droits d'accès au site.

L'attribution des droits d'accès aux badges d'accès est régie par des règles établies par le gestionnaire principal du système. Il peut verrouiller l'accès à la définition des groupes d'accès, pour le réserver par exemple à des opérateurs différents suivant le niveau de sécurité de certaines zones. Il peut verrouiller l'attribution de droits d'accès à des zones sensibles, pour la réserver par exemple à des opérateurs différents suivant le niveau de sécurité de certaines zones, ou suivant la période d'accès.

CONTRÔLE ET TRAÇABILITÉ

Toute modification des données d'exploitation est tracée pour permettre d'en faire l'audit en cas d'incident. Le contrôle permettra de retrouver les données modifiées et l'auteur de ces opérations.

PROTECTIONS PHYSIQUES

Le réseau de contrôle de SCNET4™ est composé d'un même automate SC4x5™ puissant, sécurisé et miniaturisé multiplié à l'infini. Cette structure offre une résilience plus élevée et une résistance plus forte à l'agression que les systèmes composés de multiples couches de contrôle.

La défense physique des composants du système comprend

- l'autoprotection des boîtiers et des détecteurs d'ouverture ou d'intrusion ;
- le rassemblement des éléments actifs (Automates…) dans des zones protégées ;
- la télésurveillance des lecteurs, en zone non protégée notamment (Anti-arrachement, effacement mémoire en cas d'incident) ;
- le stockage des paramètres de sécurité dans des mémoires protégées ;
- le fonctionnement autonome des automates en cas de coupure en amont ;
- la surveillance continue du fonctionnement de tous les éléments et le report instantané d'anomalies.

Références

SCNET4™ SECURE répond aux recommandations du guide de la sécurité de l'ANSSI (FR), à la norme IEC 60839 et aux exigences de la carte Agent du Ministère de l'intérieur (FR) et de la carte CIMS de la DGSIC (FR).

SCNET4™
VERSION SECURE

NCS SCALINE

National Control Systems S.A.
BELGIQUE

PAEPSEM BUSINESS PARK - Bât. 1
Boulevard Paepsemlaan 18C
1070 - Bruxelles / Brussel
Tél : +32 2 245 22 39
ncs.belgium@ncs-scaline.com
ncs.service.be@ncs-scaline.com

National Control Systems S.A.R.L.
FRANCE

Les Flamants ZAC Paris Nord II
13 Rue de la Perdrix
93290 Tremblay-en-France
Tél : +33 1 48 17 81 86
ncs.france@ncs-scaline.com
ncs.service.fr@ncs-scaline.com

Mention légale – STid et Architect® sont des marques déposées de STid SA. MIFARE et MIFARE DESFire sont des marques déposées de NXP B.V.
NCS®, Scaline, SECURE et SCNET4 sont des marques déposées de NCS S.A. Toutes les marques citées dans ce documenta ppartiennent à leur propriétaires respectifs.
© 2016 Scaline International et NCS S.A., tous droits réservés