SCNET4 (TM)

VERSIE SECURE

NCS SCALINE

BEVEILIGDE COMMUNICATIE GECODEERDE BADGES

Elk bedrijf, elke instelling, kortom elke organisatie wordt geconfronteerd met veiligheidsproblemen op het gebied van personeel, beveiliging en verdediging van zijn of haar vitale centra en geheimen. Een oplossing voor deze problemen bestaat in het gebruik van geïntegreerde systemen voor elektronische toegangscontrole, beveiligingsbeheer en videobewaking.

De implementatie van elektronische en informaticamiddelen op zich is echter niet voldoende. We moeten ook waken over de authenticiteit van de identiteiten, de beveiliging van de gegevens en de procedures, evenals de flexibiliteit en de integriteit van de gebruikte middelen.

Een geïntegreerd systeem voor toegangscontrole deelt immers gegevens en communicatiemiddelen met andere computersystemen van de bedrijven. Het moet dus voldoende bescherming bieden tegen interne en externe aanvallen en de vertrouwelijkheid van de communicatie en informatie garanderen.

Het veiligheidsbeleid van het bedrijf moet dus direct worden geïntegreerd in de server, werkstations en automaten die gebruik maken van de netwerken van het bedrijf.

De bedrade verbindingen tussen automaten en lezers en de draadloze verbindingen tussen lezers en badges, waarop de identificatiegegevens worden uitgewisseld, moeten ook worden voorzien van onschendbare encryptie- en authenticatiemechanismen.

SCNET4™ SECURE

SCNET4™ SECURE is een SCNET4™-systeem versie 3 dat is aangevuld met verschillende opties voor de beveiliging van de gegevens en beheersprocedures, de flexibiliteit en de integriteit van de gebruikte middelen en de authenticiteit van de identiteiten.

Communicatie

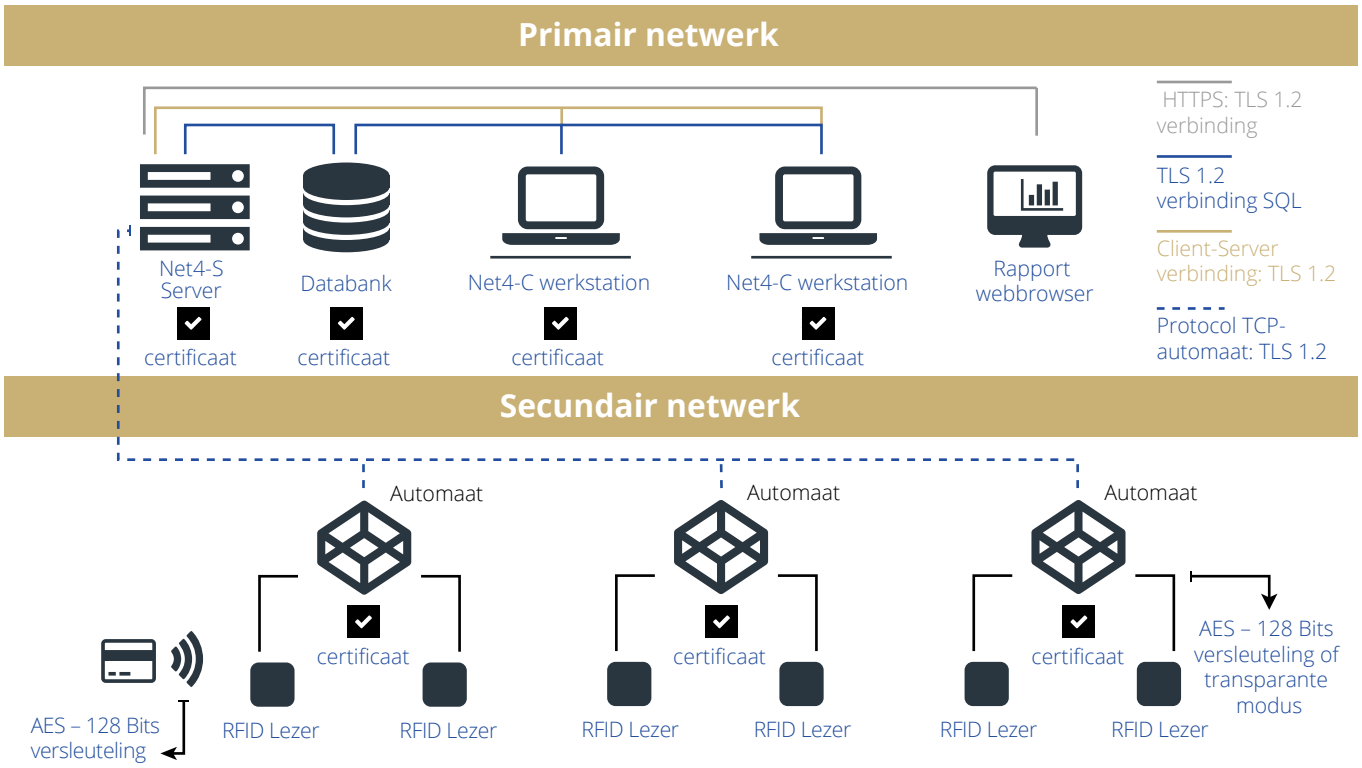
SECURE omvat beveiligingsmethoden voor communicatie tussen alle apparaten van de installatie: NET4S™-server, NET4C™-werkstations, automaten van de SC4x5™-serie en ARC-lezers van de Architect®-serie van STid®

Badges

SECURE beheert op veilige wijze toegangsbadges van het type MIFARE DESFire® EV1.

Processen

SECURE beveiligt de beheersprocessen van het systeem en de toegangsprocessen tot de werkingsgegevens.



Versleuteling: een overzicht

Het doel van versleuteling is de verstrekking van veiligheidsdiensten om de volgende eigenschappen te verzekeren

- De vertrouwelijkheid: De gegevens kunnen alleen worden gelezen door de personen die hiertoe rechten hebben ontvangen,
- De integriteit: De ontvangen gegevens zijn identiek aan de verstuurde gegevens,
- De authentificatie: De ontvanger is de effectieve begunstigde,
- en tot slot de onweerlegbaarheid: De uitwisselingsprocedure garandeert zonder enige twijfel dat de auteur van het bericht het bericht heeft verzonden en dat de ontvanger het bericht heeft ontvangen.

De vertrouwelijkheid wordt verzekerd

- ofwel door het gebruik van zogenaamde symmetrische codering van de gegevens met behulp van een geheime sleutel die is gekend door beide partijen (bijvoorbeeld: AES - Advanced Encryption System).
- ofwel door het gebruik van zogenaamde asymmetrische codering van de gegevens met behulp van een paar sleutels: een publieke sleutel die is gekend door alle zenders om de codering uit te voeren; een private sleutel die alleen is gekend door de ontvanger die deze gebruikt voor de ontcijfering. (bijvoorbeeld RSA -Rivest Shamir Adleman).

De integriteit van de gegevens wordt gegarandeerd door de ondertekening ervan. Deze handtekening wordt berekend door middel van een eenduidige samenvatting van deze gegevens. Deze samenvatting wordt berekend door een 'hashing'-algoritme (bijvoorbeeld: SHA -Secure Hash Algorithm) zodat reverse-engineering van de gegevens niet mogelijk is.

De authenticatie en de onweerlegbaarheid worden gewaarborgd door de ondertekening van de gegevens. Deze handtekening wordt berekend door versleuteling met behulp van een private sleutel, een eenduidige samenvatting van deze gegevens die wordt berekend door hashing en wordt gecontroleerd door ontcijfering met behulp van de bijbehorende publieke sleutel.

Met **deze diensten kan bijvoorbeeld worden voorkomen** dat een toegangsbadge wordt nagemaakt, dat uit een frauduleus onderschept bericht geheime sleutels kunnen worden afgeleid voor de programmatie van badges of toegangsparameters, dat valse commando's in een bericht worden ingevoerd of dat een systeem wordt gehackt, ofwel om te verhinderen dat een dergelijk systeem werkt, ofwel om te verhinderen dat vertrouwelijke gegevens over personen en over het bedrijf uit een dergelijk systeem worden geëxtraheerd, ofwel om te verhinderen dat deze worden gebruikt voor toegang tot andere bedrijfsmiddelen.

VEILIGHEID VAN DE COMMUNICATIE

De veiligheid van de netwerken

De verbindingen tussen de NET4S™-server, de NET4C™-werkstations en de SC4x5™-automaten maken gebruik van bedrijfsnetwerken (intranet of WAN) of specifieke netwerken. Het is vaak noodzakelijk om ook verbindingen met de bedrijfsbronnen te maken zoals de informatica-infrastructuur van Human Resources of om middelen voor toegang op afstand te delen. Daarom moet de beveiliging van het toegangscontrolesysteem aan dezelfde principes voldoen als de beveiliging van de IT-bedrijfsmiddelen.

Versleuteling van de automaat naar de lezer

In SCNET4™ SECURE kunnen de automaten direct in 'transparante' modus communiceren met de MIFARE DESFire EV1-toegangsbadges, deze dialoog wordt beveiligd door een 128-bits AES-encryptie. De veiligheid van de verbindingen tussen de SC4x5™-automaten en de ARC-toegangslezers van de Architect™-serie kan enerzijds ook worden verzekerd door de codering van de uitwisselingen (AES) en anderzijds door de ondertekening van deze uitwisselingen met behulp van een berichtauthenticatiecode die wordt gegenereerd door een hashing-functie (HMAC) en gekoppeld is aan een geheime sleutel. De encryptie- en authenticatiesleutels zijn sessiesleutels die worden afgeleid van geheime sleutels.

Firewall

De SC4x5™-automaten zijn voorzien van een firewall die de gegevens filtert die met het netwerk worden uitgewisseld. Hij ondersteunt alleen uitdrukkelijk toegelaten communicatie en blokkeert de poorten die niet noodzakelijk zijn voor de toepassing.

Niet-substitutie

De Net4™-server wordt geauthenticeerd door een beveiligingssleutel. Deze sleutel zorgt voor een unieke identificatie van de server door de SC4x5™-automaten en de automaten door de server, en beschermt het geheel tegen alle pogingen van substitutie.

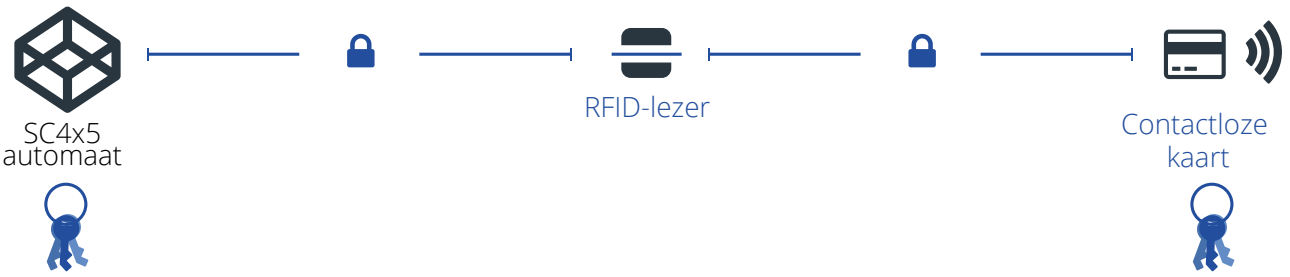
Deze sessiesleutels voor automaat-lezer zijn dus:

Vertrouwelijk:
Ze worden niet gepubliceerd

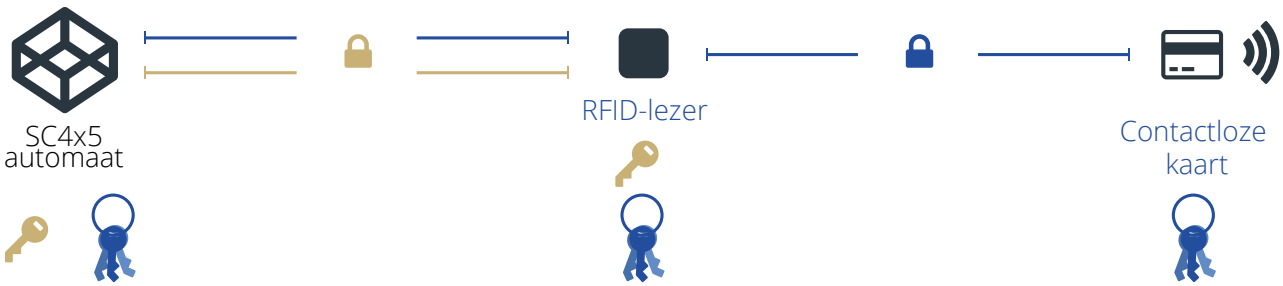
Uniek:
Ze zijn verschillend per koppel dialoogdeelnemers

Variabel:
Ze veranderen bij elke nieuwe sessie

Transparante modus

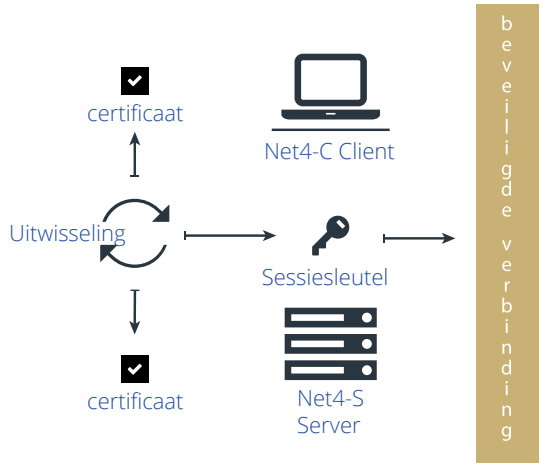


Beveiligde modus



De TLS- en HTTPS-standaarden

De SCNET4™ SECURE-verbindingen tussen werkstations en tussen server en automaten worden beveiligd door het standaard TLS 1.2-protocol (Transport Layer Security). In het bijzonder dankzij de certificering van de deelnemers aan de dialoog en de versleuteling met publieke/private sleutels, is deze methode veiliger dan een eenvoudige versleuteling van de gegevens door AES 128-bits met behulp van een vaste geheime sleutel; deze methode ondersteunt ook de integratie van het systeem in het bedrijfsbeleid betreffende de beveiliging van de computernetwerken.



De uitwisselingen worden vervolgens versleuteld door het geselecteerde algoritme en met behulp van deze sessiesleutel. Er wordt ook een hashing-functie gebruikt om de integriteit en authenticatie van gegevens te garanderen.

TLS: een overzicht

Dit standaardprotocol, dat wordt gebruikt door de meerderheid van de beveiligde netwerken, biedt aan twee partijen de mogelijkheid

- om zich te authenticeren met behulp van asymmetrische cryptografie,
- om te beslissen welke coderingssuite zij zullen gebruiken om hun communicatie te beveiligen,
- om de geheime sleutel die ze tijdens de dialoogsessie zullen gebruiken te bepalen
- tijdens het opzetten van hun dialoog en vervolgens op gezette tijden de sessiesleutel veilig uit te wisselen.

Deze berekende sessiesleutel is dus

Vertrouwelijk:
hij wordt niet gepubliceerd,

Uniek:
hij is verschillend per twee dialoogdeelnemers

Variabel:
hij verandert bij elke nieuwe sessie

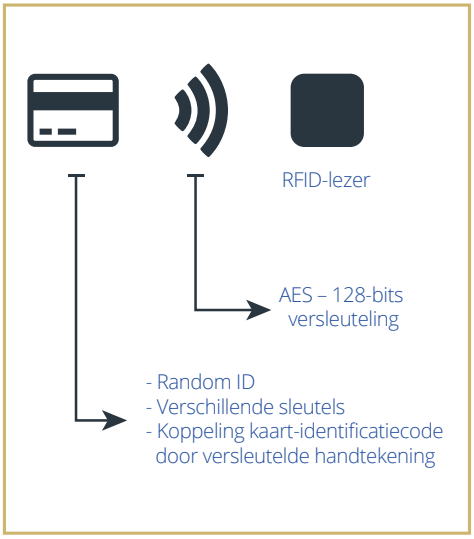
De uitwisselingen worden vervolgens versleuteld door het geselecteerde algoritme en met behulp van deze sessiesleutel. Er wordt ook een hashing-functie gebruikt om de integriteit en authenticatie van gegevens te garanderen.

MIFARE DESFRE EV1-TOEGANGSBADGES EN BEVEILIGDE APPLICATIES

De MIFARE DESFire EV1-badges die worden gebruikt in SCNET4™ SECURE bevatten een beveiligde toepassing voor toegangscontrole. Deze toepassing bevat bestanden met de identificatiecode van de drager. De toegang tot deze bestanden wordt beschermd met sleutels.

De veiligheid van de badge wordt verhoogd:

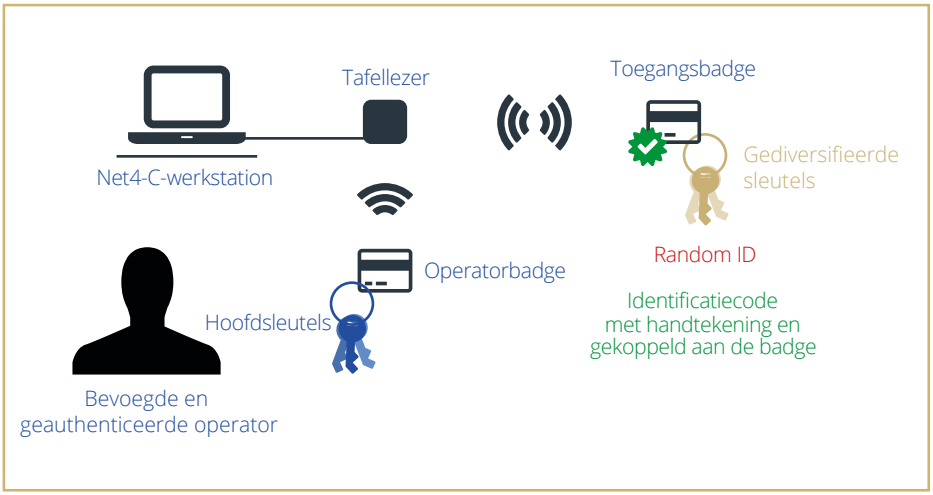
- door het gebruik van een willekeurige identificatie (ten onrechte 'serienummer' genoemd) (Random Identification - RID) van de kaart in plaats van de vaste UID (Unique Identification Code), die niet toegankelijk is;
- door het gebruik van verschillende toegangssleutels tot de inhoud voor het lezen, schrijven of wijzigen ervan; zo zal elke badge verschillende sleutels bevatten;
- door het gebruik van een identificatiecode van de persoon in combinatie met een handtekening die de code en badge koppelt (bescherming tegen klonen).



Veiligheid van de inhoud van de badges

SCNET4™ SECURE maakt gebruik van basissleutels die worden gedefinieerd door de systeemverantwoordelijke. Alleen hij kent deze sleutels. Bepaalde basissleutels voor de beveiliging van de badges maken het mogelijk om verschillende sleutels te genereren, die uniek zijn voor elke gebruikersbadge, die toegang bieden bieden tot de inhoud van de badges en die in de in de badges zijn opgeslagen. Andere basissleutels ondersteunen het gebruik van handtekeningen, door versleuteling van de identificatiecode van elke persoon, die wordt geprogrammeerd door hiertoe aangestelde operators. Deze code zal in de badge worden opgeslagen.

De MIFARE DESFire EV1-badges die worden uitgedeeld aan de gebruikers, voor toegang tot bepaalde ruimtes, worden aangemaakt door bevoegde en geauthenticeerde operators. Zij gebruiken hun individuele toegangskaart tot het systeem om zich te authenticeren. Deze individuele operatorkaart bevat, in beveiligde vorm, basissleutels voor beveiliging van de badges, die deze personen niet kennen, niet kunnen lezen noch kunnen wijzigen.



Deze basissleutels worden versleuteld en worden via het netwerk van de individuele legitimatiekaart van de operators naar de automaten verzonden. Zodra het proces is voltooid, worden deze basissleutels uit de computers gewist, er worden geen basissleutels bewaard door het systeem. Afhankelijk van het feit dat de optie 'transparante modus' al dan niet actief is, worden de sleutels ofwel in versleutelde vorm (AES256) in de automaat opgeslagen, waarbij de versleutelingssleutel zelf wordt opgeslagen in een beschermd hardwareregister, ofwel wordt deze bewaard in een beveiligde en niet-toegankelijke ruimte in de lezers; deze sleutels worden gewist als de stroom uitvalt of bij een poging tot fraude of losrukken.

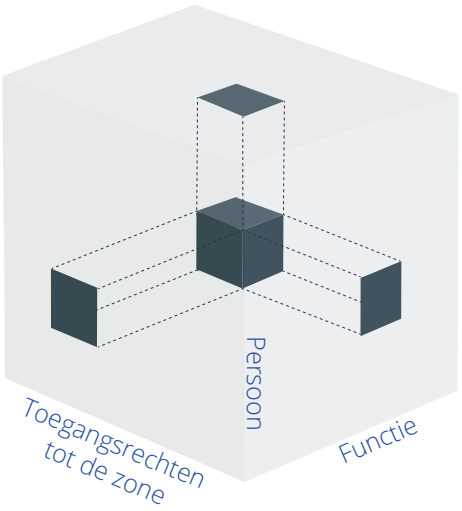
SECURE BEHEERSPROCES

De hoofdbadge

In SCNET4™ SECURE worden de hoofdsleutels van het systeem gedefinieerd door de hoofdbeheerder van het systeem; ze dienen voor het definiëren van andere beveiligingssleutels die nodig zijn voor de werking van het systeem. De sleutels worden gegenereerd door middel van berekening en worden niet gepubliceerd. Deze hoofdsleutels worden na gebruik niet bewaard door de server. Ze worden veilig opgeslagen in een MIFARE DESFire EV1-hoofdbadge die wordt beschermd door een sterke authenticatie: operators hebben de badge en het wachtwoord nodig voor toegang tot de beveiligde informatie. De hoofdbeheerder van het systeem draagt de volledige verantwoordelijkheid voor deze unieke badge.

De toegangen tot het systeem

De toegang tot de clients (werkstations van de operatoren) wordt beveiligd door de authentificatie van elke operator die een individuele legitimatiekaart (MIFARE DESFire® EV1) nodig heeft; elke kaart wordt aangemaakt door de hoofdbeheerder van het systeem door middel van zijn hoofdkaart. Deze operatorkaarten beveiligen hun individuele toegangsrechten tot informatie en functies. Deze rechten worden toegewezen door de hoofdbeheerder van het systeem met behulp van de werkingsklassen: ze hebben betrekking op de systeemfuncties, de controle- en beheersgegevens, de zones van de locatie op basis van hun veiligheidsniveau en de gegevens van elke persoon met toegang tot de locatie op basis van zijn rechten.



De programmatie van de badges

De toewijzing van een identiteitscode aan een toegangsbadge wordt beheerst door de hoofdbeheerder van het systeem op basis van vastgestelde regels. Deze kan mogelijk bevoegd zijn voor de definiëring van KPF™-formaten (Key-Protocol-Format) waarmee het formaat kan worden geprogrammeerd dat moet worden toegepast op de identificatiecodes van de toegangsbadges. (Opmerking: Hij heeft al controle over de toegangsleutels tot de inhoud van de badges). Dit formaat kan zodanig worden gedefinieerd dat de opgeslagen fysieke code nooit in de beschikbare gegevens verschijnt.

De toewijzing van de toegangsrechten tot de locatie

De toewijzing van de toegangsrechten aan de toegangsbadges wordt beheerst door de hoofdbeheerder van het systeem op basis van vastgestelde regels. Hij kan de toegang tot de definitie van de toegangsgroepen vergrendelen en deze bijvoorbeeld voorbehouden aan de verschillende operatoren op basis van het beveiligingsniveau van bepaalde zones. Hij kan de toewijzing van toegangsrechten tot gevoelige zones vergrendelen en deze bijvoorbeeld voorbehouden aan de verschillende operatoren op basis van het beveiligingsniveau van bepaalde zones of op basis van de toegangsperiode.

KWALITEIT EN TRACEERBAARHEID

Elke wijziging van de werkingsgegevens wordt bijgehouden zodat in geval van een incident een audit kan worden uitgevoerd. Door de controle kunnen de gewijzigde gegevens worden teruggevonden en kan de auteur van deze handelingen worden bepaald.

FYSIEKE BESCHERMINGEN

Het SCNET4™-controlenetwerk bestaat uit één enkele krachtige, beveiligde en geminiaturiseerde SC4x5™-automaat die tot in het oneindige kan vermenigvuldigd worden. Deze structuur biedt een hogere flexibiliteit en weerstand tegen aanvallen dan systemen met meerdere controlelagen.

De fysieke verdediging van de systeemcomponenten omvat

- de zelfbescherming van de behuizingen en de detectoren tegen opening of inbraak;
- de concentratie van de actieve elementen (automaten ...) in de beschermde gebieden;
- de bewaking op afstand van de lezers, in het bijzonder in niet-beschermde gebieden (bescherming tegen losrukken, wissen van het geheugen in geval van een incident);
- de opslag van de veiligheidsparameters in beschermde geheugens;
- de autonome werking van de automaten bij een onderbreking van het hoger gelegen systeem;
- de continue bewaking van de werking van alle elementen en de onmiddellijke melding van afwijkingen.

Referenties

SCNET4™ SECURE voldoet aan de aanbevelingen van de veiligheidsgids van het ANSSI (FR), de norm IEC 60839 en de eisen van de Agent-kaart van het Ministerie van Binnenlandse Zaken (EN) en de CIMS-kaart van de DGSIC (FR).

SCNET4 (TM)
VERSIE 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