SCNET4 (TM)

SECURE VERSION

NCS
SCALINE

SECURE COMMUNICATIONS ENCRYPTED BADGES

All organisations, whether companies or institutions, are confronted with the problems of keeping their staff safe and protecting and defending their centres of operations and their secrets. One solution to these problems involves the use of integrated electronic systems for access control, security management and video surveillance.

However, deploying IT and electronic resources is not enough on its own. It is also essential to guarantee that identities are authentic, that data and procedures are secure and that the resources used are resilient and reliable.

An integrated access control system shares data and communication channels with other enterprise IT systems. It must therefore guarantee at least an equal level of protection against internal and external attack and of communication and information confidentiality.

The server, client workstations and controllers that use the organisation's networks thus have to incorporate its security policies directly.

The cabled links between controllers and badge readers, and the radio links between readers and badges, across which identification data is exchanged must also incorporate inviolable encryption and authentication mechanisms.

SCNET4™ SECURE

SCNET4™ SECURE is a SCNET4™ Version 3 system supplemented with several options to guarantee the security of data and management processes, the resilience and integrity of the system and the authentication of identities.

Communications

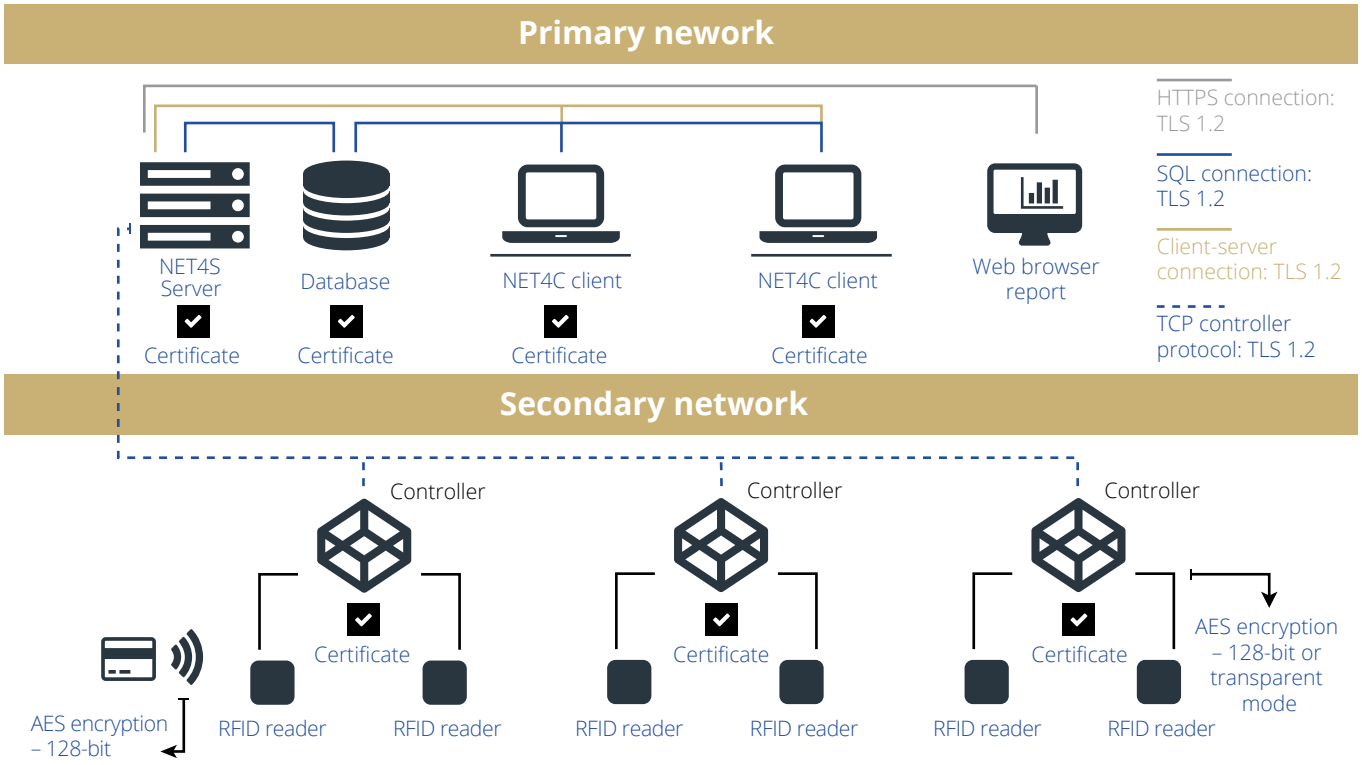
SECURE incorporates methods for secure communication between all the devices in the system: NET4S™ server, NET4C™ clients, controllers in the SC4x5™ range and ARC readers in the Architect® range from STid®.

Badges

SECURE manages MIFARE® DESFire EV1 access badges securely.

Processes

SECURE secures system management processes and access to operational data.



Cryptography: A brief introduction

The goal of cryptography is to provide security services to guarantee properties such as

- Confidentiality: data is only readable by people who have been given permission,
- Integrity: the data received is identical to the data sent,
- Authentication: your contact is definitely the person you think it is,
- And non-repudiation: the exchange procedure guarantees unambiguously that the author of the message definitely sent it and that the addressee definitely received it.

Confidentiality is guaranteed

- either by the use of so-called symmetrical data encryption, using a secret key known to both parties (e.g. AES – Advanced Encryption System)
- or by the use of so-called asymmetrical data encryption, using a pair of keys – a public key known to all senders, used to encrypt the data, and a private key known only to the receiver, used to decrypt the data (e.g. RSA – Rivest Shamir Adleman).

The integrity of the data is ensured by signing it. The signature is calculated with a one-way digest of the data using a «hashing» algorithm (e.g. SHA – Secure Hash Algorithm) that makes it impossible to reconstitute the data in the other direction.

Authentication and non-repudiation are achieved with a signature for the data, calculated by encrypting a one-way digest of the data, generated using hashing, with a private key and checked by decrypting it with the corresponding public key.

For example, these services avoid the risks that access badges can be counterfeited, that a message intercepted maliciously can reveal secret badge programming keys or access authorisation parameters, that fraudulent commands can be inserted into messages or that systems can be hacked, either to prevent them from operating, to extract confidential data about individuals or the company or to attack the company's other resources.

SECURE COMMUNICATIONS

Network security

The links between the NET4S™ server, the NET4C™ clients and the SC4x5™ controllers use either the company's networks (intranet or WAN) or dedicated networks. It is often necessary to establish links with company resources such as the HR information system or to share remote access. This makes it essential for the security of the access control system to comply with the same principles as those that apply to the security of the company's other IT resources.

Cryptography from the controller to the reader

In SCNET4™ SECURE, controllers can dialogue directly and transparently with MIFARE DESFire EV1 access badges, with the communication secured by AES 128-bit encryption. The security of the links between the SC4x5™ controllers and the ARC access readers in the Architect range can also be ensured, by encrypting the exchanges (AES) on one hand and by signing the exchanges on the other with a message authentication code generated by a hashing function (HMAC) and associated with a secret key. The encryption and authentication keys are session keys derived from secret keys.

Firewall

The SC4x5™ controllers are equipped with a firewall to filter the data exchanged with the network. The firewall only allows communications that have been explicitly authorised and blocks any ports that are not needed by the application.

Non-substitution

The NET4™ server is authenticated by a security key. This key identifies the server uniquely to the SC4x5™ controllers and the controllers to the server, protecting the system against any attempt at substitution.

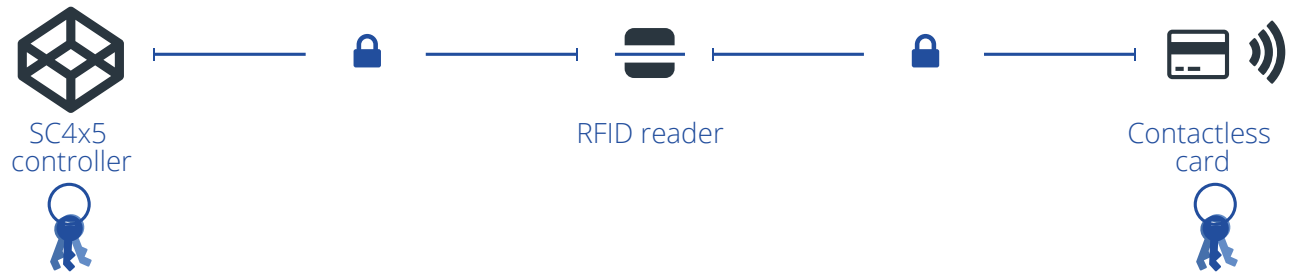
These controller-reader session keys are thus:

Confidential:
They are never published

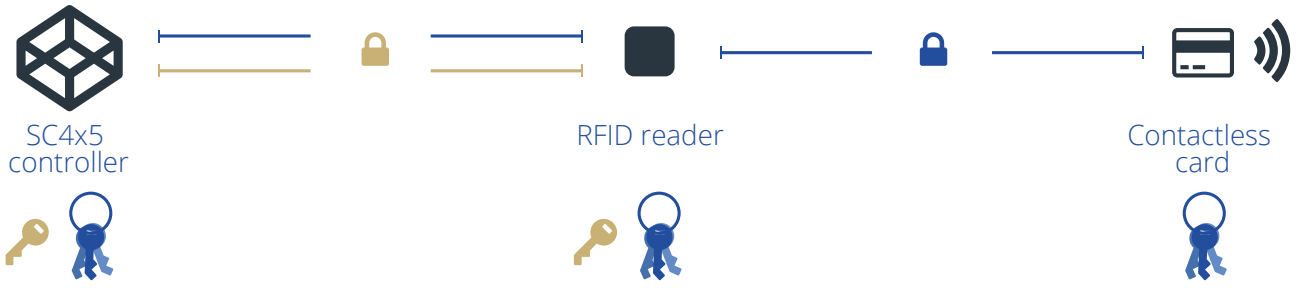
Unique:
They are different for each communicating pair

Variable:
They change for each new session

Transparent mode

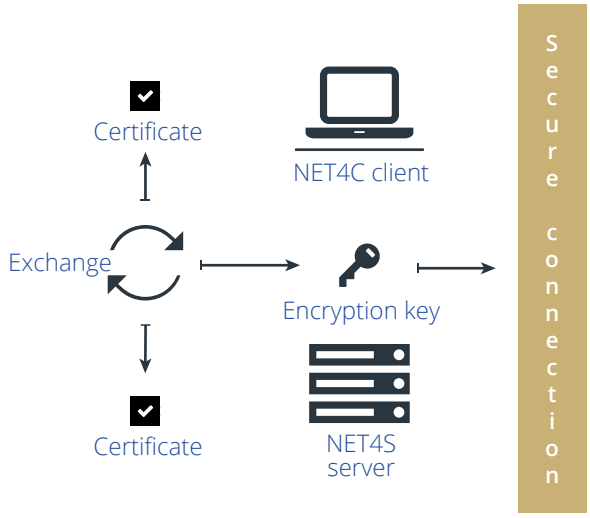


Secure Mode



The TLS and HTTPS standards

The SCNET4™ SECURE links between computers and between the server and the controllers are secured using the standard TLS 1.2 (Transport Layer Security) protocol. Due to the certification of all the parties involved and the public/private key cryptography, this method is more secure than simple AES 128-bit data encryption using a fixed secret key; it also enables the system to be incorporated into the company's policy on computer network security.



Each SC4x5™ controller contains a web server for configuration and maintenance operations. Access to this web server embedded in the controllers is secured using the HTTPS protocol, which is based on TLS.

TLS : A brief introduction

This standard protocol, used by most secure networks, enables two parties to:

- Authenticate themselves using asymmetric cryptography,
- Decide on the further cryptography they will use to secure their communications,
- Securely exchange the secret key they will use during the dialogue session when opening the dialogue and then at regular intervals.

This calculated session key is thus

Confidential:
It is never published

Unique:
It is different for each communicating pair

Variable:
It changes for each new session.

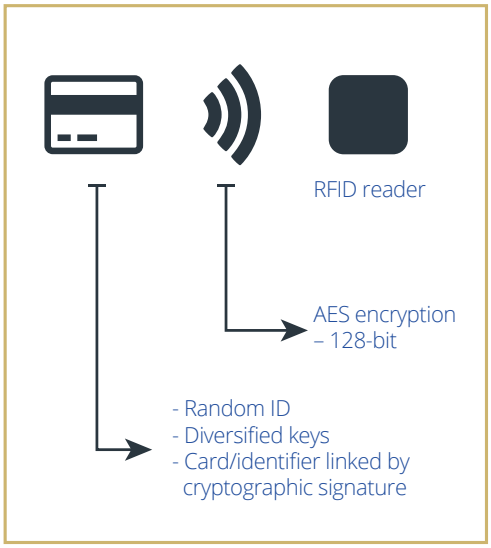
Exchanges are then encrypted by the selected algorithm using this session key. A hashing function is also used to ensure data integrity and authentication.

MIFARE DESFIRE EV1 ACCESS BADGES AND SECURE APPLICATIONS

The MIFARE DESFire EV1 badges used in SCNET4™ SECURE contain a secure access control application. This includes files containing the bearer's identification code. Access to these files is protected with keys.

The security of the badge is strengthened by:

- The use of a random card identifier (Random Identification – RID), wrongly referred to as a «serial number», rather than a fixed UID (Unique Identification Code), which is not accessible;
- The use of diversified keys for gaining read, write or modification access to content, so that each badge will contain different keys;
- The use of an identification code for the person together with a signature linking the code to the badge (anti-cloning).

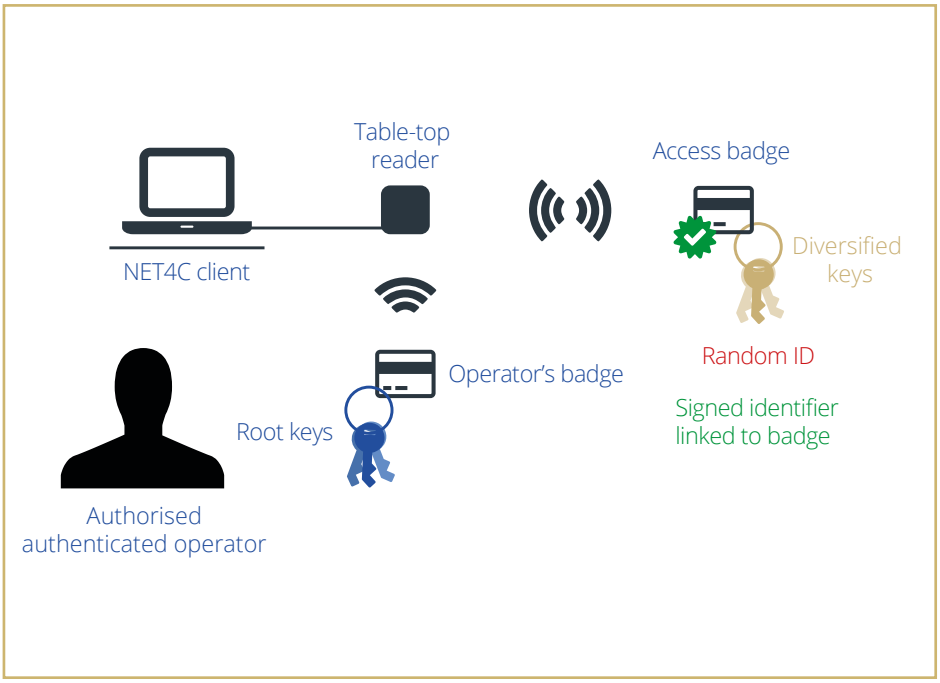


Badge content security

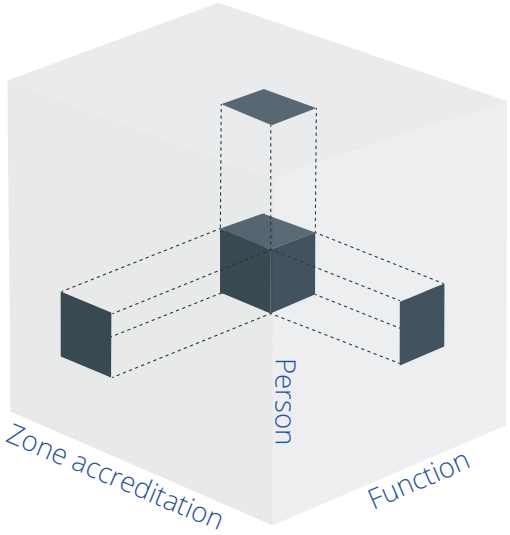
SCNET4™ SECURE uses root keys defined only by the system administrator, who is the only person that knows them. Some root keys for securing badges are used to generate diversified keys specific to each user's badge, providing access to its content and stored in the badge. Other root keys are used to sign communications by encrypting each person's identification code, programmed by authorised operators and stored in the badge.

The MIFARE DESFire EV1 badges that are distributed to users to enable them to access premises are created by authorised, authenticated operators, who use their individual system access authorisation cards to authenticate themselves. The individual operator's card contains, in secure form, root keys for securing badges which the operator does not know and can neither read nor modify.

These root keys are sent in encrypted form from the operator's individual authorisation card to the controllers via the network. Once this operation has taken place, the root keys are deleted from the computers, and no root keys are conserved by the system. Depending on whether or not the «transparent mode» option is active, the keys are either conserved in encrypted form (AES 256) in the controller, the encryption key itself being conserved in a protected hardware register, or conserved in an inaccessible secure zone in the readers; these keys will be deleted in the event of a power cut, attempted fraud or physical attack.



SECURE MANAGEMENT PROCESSES



The Master badge

In SCNET4™ SECURE, the system's master keys are defined by the main system administrator; they are used to define other security keys needed for the system's operation, which are generated through calculations and not published. Once used, these master keys are not conserved by the server. They are stored securely in a master MIFARE DESFire EV1 badge protected by strong authentication – both the badge and the password are needed to access the secret keys. This unique badge is the exclusive responsibility of the main system administrator.

Access to the system

Access to client workstations (the operators' computers) is secured by authenticating each operator with an individual MIFARE DESFire® EV1 card. Each card is created by the main system administrator using the master card. These operators' cards secure their individual rights to access information and functions. These rights are granted by the system administrator based on classes of operation, and they govern access to the system's functions, control and management data, zones of the site based on their security level and the data of each individual with access to the site based on their level of accreditation.

Badge programming

The allocation of an identity code to an access badge is governed by rules established by the system administrator. He or she can retain the exclusive authorisation to define the KPFs™ (Key Protocol Format) that enables the programming of the format to apply to access badge identification codes. (Note: the system administrator already has control over the keys for accessing badge contents.) This format can be defined in such a way that the physical code never appears in the accessible data.

Allocating site access rights

The allocation of access rights to access badges is governed by rules established by the system administrator. He or she can lock access to the definition of access groups, e.g. reserving it for different operators depending on the security level of certain zones. He or she can lock the allocation of access rights for sensitive areas, e.g. reserving it for different operators depending on the security level of certain zones or on the access period.

QUALITY AND TRACEABILITY

All changes to operational data are tracked so that audits can be conducted in the event of an incident. The log shows the modified data and the person who made the changes.

PHYSICAL PROTECTION

The SCNET4™ control network consists of the powerful, secure, miniaturised SC4x5™ controller multiplied as many times as needed. This structure offers a high level of resilience and stronger resistance to attack than systems consisting of multiple layers of control.

The physical defence of the system's components includes

- protected casings and opening/intrusion sensors;
- active elements (controllers etc.) collected together in protected areas;
- remote surveillance of readers, particularly in non-protected areas (guarding against physical attack, erasing the memory in the event of an incident);
- storing security parameters in protected memory;
- controllers function autonomously in the event of an upstream power cut;
- continuous monitoring of the operation of all components, with any anomalies reported instantly.

References

SCNET4™ SECURE complies with the recommendations of the ANSSI security guide (FR), the IEC 60839 standard and the requirements of the Agent du Ministère de l'intérieur card (FR) and the DGSIC CIMS card (FR).

SCNET4 (TM)
SECURE VERSION

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