ANSSI CERTIFICATION GUIDE

ACCESS CONTROL SYSTEMS

What is the ANSSI?

Presentation

The Agence Nationale de la Sécurité des Systèmes d'Information – France's national cybersecurity agency – was created in 2009. It reports to the Secretariat-General for National Defence and Security (SGDSN) to assist the Prime Minister in exercising his responsibilities in relation to defence and national security.

The ANSSI currently serves as France's national cyberdefence body for protecting sectors that are considered of vital importance.

→Missions

In order to tackle new threats to IT systems, article 22 of the Military Planning Act (voted in on 18 December 2013) now requires that operators tasked with managing vital infrastructure step up the security of the information systems that they operate.

The ANSSI is tasked with setting out the rules to be applied in order to protect these information systems and then ensuring that the measures adopted are properly applied. These obligations apply first and foremost to Information Systems that are considered of vital importance. One aspect of them focuses on access control systems.

→ Sites of vital importance

A business sector considered of vital importance is a set of activities all carried out to meet the same objective.

These are activities that are difficult to replace or find substitutes for, and which relate to the production and distribution of goods and services that are considered vital, or the absence of which can constitute a serious threat for the population.

Did you know?

- 12 sectors of vital importance have been identified
- In France, 249 operators of vital importance have been designated (confidential list drawn up by the Ministry of Defence)
- In France, 369 locations of vital importance have been identified. These should be made secure as a priority.

Operator of vital importance

In sectors of vital importance, operators of vital importance are ones which operate or use facilities that are considered essential for the country. These are designated by the relevant ministry which then sets out the security objectives for them. These operators are required to help protect establishments, facilities and infrastructure against all threats, particularly terrorist threats. They must do so at their own expense.

Location of vital importance

Among these operators of vital importance, locations of vital importance are centres, facilities or infrastructure which provide services and goods which are considered essential for the country.

The operators themselves draw up lists of their locations of vital importance.

These can include, for example, production sites, testing centres, network nodes, IT centres, etc. An operator of vital importance can have several locations of vital importance.

Geographic zones of vital importance feature locations of vital importance that can belong to several operators of vital importance.

A breakdown of the operators of vital importance by business sector:

Sector	Transport	Military	Health	Energy	Water	Finance	Civil industry	Medias	R&D	Legal	Food industry	Industry
Numbers of OVI*	68	36	22	21	16	15	10	9	7	6	5	5

*OVI = Operator of Vital Importance

→ Relevant legislation

For the operators of vital importance operating in the sectors concerned, the legislation lays out a certain number of measures provided for by articles L. 1332- 6-1 et seq. of France's defence code:

- Security regulations, that are both organisational and technical in nature, which apply to information systems considered of vital importance
- Methods for identifying information systems of vital importance and for reporting-security incidents affecting these information systems

France is the first country in the world to use regulations for developing an effective cybersecurity system to protect critical infrastructure that is considered essential for the smooth running of the country and its security.

→ ANSSI recommendations pertaining to the security of physical access control systems

As far as physical access control systems are concerned, the ANSSI has compiled its recommendations in one document – "Guide to the security of contactless technologies for physical access control systems". The fundamental principles described in this document are designed to be directly appropriate for the threat levels for each zone, based on the type of potential attack according to a scale ranging from I to IV and referred to as "Security level". They focus on:

- Protecting IDs against the risk of identity theft
- Types of architecture
- Communications encryption

The 4 levels of security for protecting IDs

Level	Description
I	The card's identification does not use any cryptography: 125 kHz transponder, ISO-14443 card UID. The ID is unencrypted and is therefore easily clonable. This level has no security guarantees.
II	Access to the card's ID is protected with a key so it can be authenticated. Authentication involves a key that is shared by all cards. This is the first level of security: in the event of the key being corrupted, access to all IDs will be rendered possible.
III	Access to the card's ID is protected with a key so it can be authenticated. Authentication involves using a key derived from a master key. If one of the keys is corrupted, the other cards are unaffected.
IV	The same as Level III + authentication of card holder when they enter a code they have memorised or using biometric data.

ANSSI principles applied to physical access control solutions

In order to provide Levels II to IV as recommended by the ANSSI, cards with read/write chips are required. Using chips that are certified as meeting common criteria EAL 4+ provides additional security guarantees. The Mifare DESFire EV1 card has established itself as the leading card in this area.

Did you know?

Obtaining cards that can support encryption systems is not sufficient. These systems have to be correctly activated, otherwise the cards will only be used as a means of identification, meaning they can be cloned.
The encryption keys used in them can be of varying levels of complexity. They are the property of the organisation that uses them and clearly defined organisational methods should be applied in order to ensure that they are distributed.

The architectures needed to provide security levels

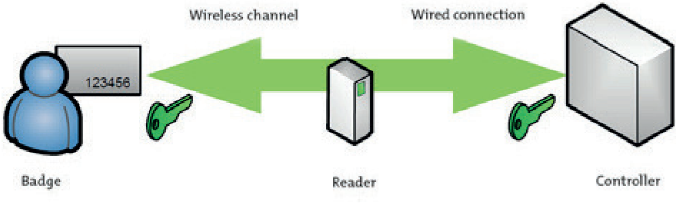
Security levels II to IV require architectures that need to provide appropriate levels of protection. Indeed, just as access to identifiers is protected by keys, the storage of these keys also needs to be secured. Depending on the architecture in question, these keys are located either in the reader, or in the controller.

The ANSSI has defined 4 types of architecture (numbered 1 through to 4). Only architectures no. 1 and no. 2 are accepted.

Architecture no. 1, highly recommended

The secured card is identified and authenticated directly by the controller located in a secure zone. The reader head sends messages without making any changes to them and is not involved in encryption. It is "transparent".

This architecture is highly recommended by the ANSSI: since the reader head does not integrate any secret components, it is impervious to attack. Particular attention should be paid to the controller used to protect encryption keys. These should be stored in a secure module (SAM: Secure Access Module), which can be either firmware or hardware, depending on the circumstances.

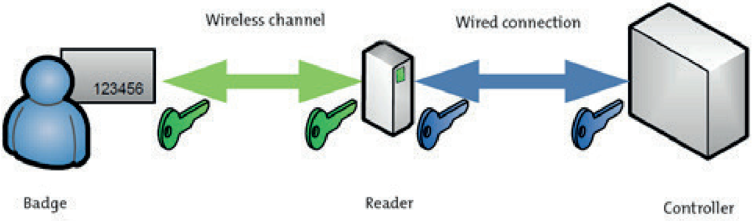


Sources: ANSSI

Architecture no. 2, acceptable if...

The secure card is identified and authenticated by the reader head. The reader head should have a secure cable connection, with authentication and encryption in order to ensure that information exchanged with the controller is protected. The reader head, located outside the security zone, contains both the secret information for authenticating the card and the secret information for protecting data transiting over the cable connection.

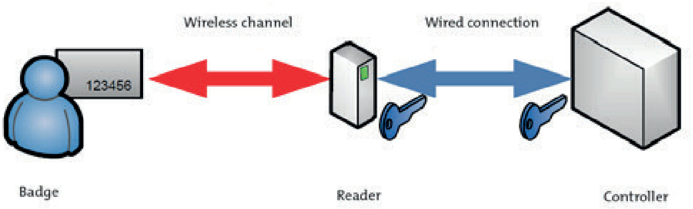
This architecture is acceptable if a detailed analysis has been conducted of the reader head that is guaranteed by the first-level security certification. The way in which the controller’s cable connection is protected must also be guaranteed. This architecture also involves management of several sets of security keys, making it more limiting. Most of the time, activating the reader involves distributing keys to a third party and requires a documented procedure of which everybody has a sound understanding.



Sources: ANSSI

Architecture no. 3, not recommended

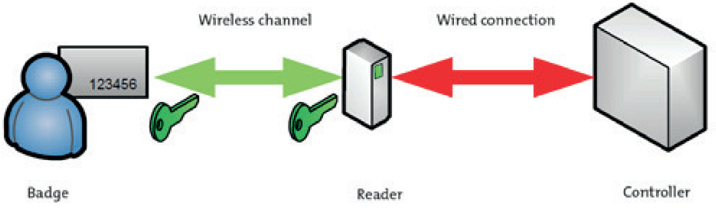
The non-secure card is identified directly by the controller. The cable connection between the reader head and the controller is protected.
The card can be cloned, including off-site. This makes protecting the cable connection pointless. It is only used for identification.



Sources: ANSSI

Architecture no. 4, not recommended

The secure card is identified and authenticated by the reader head. The reader head sends the non-protected identity to the controller. Authentication can be bypassed if there is a physical attack to the cable connection in an exposed area.



Sources: ANSSI

→ Glossary

Card identification

This is the act of sending an identity. In a system that uses contactless technology, identification involves presenting a card to a reader.

Card authentication

This involves providing proof of one's identity: it is therefore in addition to identification. For an access control system that uses contactless technology, most of the time cards are authenticated by a cryptographic exchange whereby the card can prove that it contains secret information without actually divulging it.

Bearer authentication

Once the card has been authenticated, the card's bearer has to prove that they are the legitimate holder of it.

Authenticating the bearer involves using a second component: either what one is or what one knows. For example, it can involve entering data (a code) that only the legitimate bearer of the card could possibly know, or using biometric data.

→ Certification Procedure

CSPN

Certification de Sécurité de Premier Niveau or first-level security certification is evidence, provided by an independent and impartial third party certification body, that at a given moment, a product is in compliance with a level of security represented by the security services that it provides and that it is able to withstand a given level of attack.

The target security level

The assessment can focus on all or part of the product. During the assessment, the target security level must be specified. This target is for the component(s) to be assessed, and therefore certified.

Assessment aim

The purpose of the assessment process is to enable an authorised assessment centre to check whether or not the product is in compliance with its specifications, to determine the effectiveness of its safety and security functions, and to record the results in a technical assessment report.

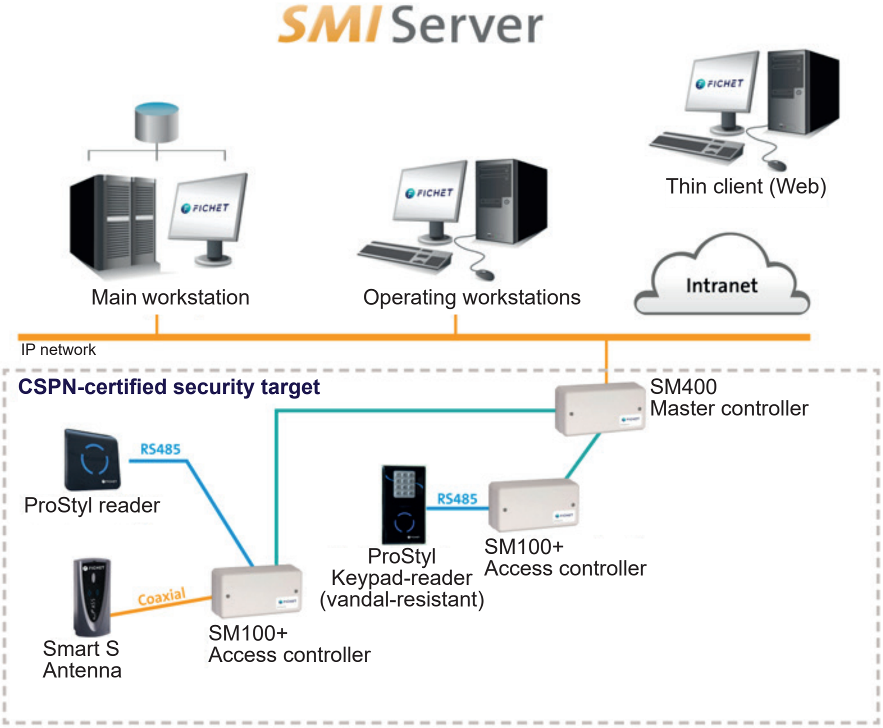
The certification centre (the ANSSI, France's national cybersecurity agency) uses this technical assessment report to decide whether or not to issue first-level security certification for the product.

→ The milestones involved

There are four milestones involved in the standard qualification process:

- M0: acceptance of the qualification project,
- M1: acceptance of the product's target security level,
- M2: acceptance of the assessment tasks,
    - M2.1: analysis of the cryptographic mechanisms,
    - M2.2: assessment of hardware and software implementation
- M3: Product certification

Security target



For more information about the Fichet SMI CSPN 01-01 version Certification:
http://www.ssi.gouv.fr/entreprise/certification_cspn/Fichet-smi-version-cspn_01-01/

FICHET

www.fichetgroup.com

The data given in this material may be subject to change without further notice.