Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, 7 July 2020

No. 1530/ANSSI/SDE/PSS/CCN

Référence :

ANSSI-CSPN-NOTE-07_v1.00

APPLICATION NOTE

CSPN EVALUATION METHOD FOR PHYSICAL ACCESS CONTROL SYSTEMS

Application : Upon approval.

Distribution : Public.

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

51 Boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Revision history

Editions	Date	Amendments
0.1	21/06/2019	Draft document for public review.
1.0	07/07/2020	Creation of the final document

Pursuant to amended Decree No. 2002-535 of 18 April 2002, this application document was submitted to the Certification Steering Committee, which issued a favourable opinion.

CONTENTS

1. Purpose of the document

This application document lays down the specific details of the First Level Security Certification (CSPN) assessment when applied to physical access control systems. The document addresses the requirements of the generic methodology [P-CSPN-02].

1.1. Objective

This document specifies the elements expected from the sponsor and the ITSEF for an assessment of a physical access control system. It also aims at clarifying the applicable state of the art and may therefore require certain attacks to be taken into account, regardless of the threats defined in the security target.

1.2. Background and definitions

The physical access control systems covered by this document shall consist of at least the following components[1]:

- one or more readers ;
- one or more controllers (also called Local Processing Units or LPUs[2]), which manage the readers;
- an Access Control Management centre (ACM[3]), which ensures, among other things, event logging and data management. It includes in particular the following elements:
    - system management software, which communicates with the LPUs,
    - resources such as user databases or *active directories*, which enable system critical data, such as permissions, users, groups or badge IDs, to be managed. These resources may be part of an information system outside the system assessed[4].

  The ACM consists mainly of one or more servers, network equipment and security equipment.

The so-called *access management network* consists of interfaces between these different components of the system, as well as:

- door locking devices;
- management or enrolment stations;

The system can interface with:

- access badges[5] (or similar media);
- all or part of a company information system (or share resources with this information system, such as a directory or a PKI);
- directly or indirectly, external networks such as the Internet.

---

[1] Other access control systems do not have this type of architecture. They are excluded from the scope of this document, and their assessment is subject to a case-by-case analysis.

[2] Also referred to as processing and control units.

[3] Also known as Supervision Processing Unit.

[4] For example, when the system uses a company LDAP directly.

[5] For ease of reading, the term “badge” will be used generically to refer to any type of medium.

2. Organisation of the assessment

2.1. Eligibility for CSPN certification

The National Certification Centre (CCN) favours the assessment of complete systems but allows the assessment of isolated components, in accordance with the following rules:

- CCN may require the name and scope of the product under assessment to be changed so that the certified product is not misleading to the end user[6];
- the security target will describe the configuration assessed using the table below:

System component		**Included in the target of evaluation** (TOE)	**Not evaluated** (TOE environment)	
			Trustworthy	Is a potential attacker
ACM	**Operating system**			
	Applications			
	Cryptographic functions			
	Databases and directories			
LPU	**Operating system**			
	Applications			
	Cryptographic functions			
	SAM			
Readers	**Simple readers**			
	Keypad readers			
Badges[7]				

Table 1: Product assessment configuration

The boxes in this table will be filled in with the references and versions (software and/or hardware) of the components concerned, including for components supplied by third parties (open source, COTS, etc.).

Each component assumed to be "trustworthy" will be the subject of an assumption in the security target. On the other hand, each component considered to be a "potential attacker" will be considered as an attacker when defining the security target threats.

[6] For example, only a *complete* system can be called an "access control system".

[7] This document does not cover assessment of badges. The references of badges tested by the assessor will be listed here.

2.2. Assessment workload

The ITSEFs authorised to conduct access control system assessments are those approved for the "software and network equipment" scope. Assessment workloads and activities should follow the table below:

Assessment activity	Nominal workload	Documents
LPU and reader software functions	**20 man-days**	Assessment activities should include the analysis of exchanges: - between the LPUs and the badges; - within the system (between ACM, LPUs and readers); - on any other functional interface.
ACM software functions	**10 man-days**	Assessment activities should include the analysis of exchanges: - between the system management software and its resources (PKI, database or directory, etc.), whether or not they are part of the TOE; - with the outside of the system: Company information system, Internet, etc.; - on any other functional interface.
Hardware security	**5 man-days**	Assessment activities should include: - assessment of the security of the hardware interfaces of the LPU and the readers; - documentary analysis of badges.
Cryptography	**5 man-days / 10 man-days**	The workload is **10 man-days** if the cryptographic mechanisms are implemented by the product itself or use *open source* code. If implemented by a closed source component, then the workload will only be **5 man-days**. The assessment will then focus on the correct use of the underlying mechanisms. The certification report will indicate that the cryptographic mechanisms themselves are not assessed.

Table 2: assessment activities

The nominal workload is therefore 45 man-days (if the cryptography is implemented by the product), or 40 man-days (if the cryptography is implemented by a proprietary OS).

This workload can be increased if the system is unusually complex (up to 50 man-days). It can also be reduced, for example if only one single component of the system is subject to assessment.

2.3. Possible subcontracting of hardware tests

With regard to hardware tests, the ITSEF in charge of the assessment may decide, depending on his/her competence, to carry out this part of the assessment[8], or to entrust it to another ITSEF approved by CCN in this area of competence.

2.4. Inputs

It is the responsibility of the ITSEF to only start the assessment once all the inputs necessary to complete the assessment have been delivered. As a reminder, [NOTE-20] authorises the ITSEF to refuse a delivery that is incomplete or of insufficient quality. The minimum inputs required by the CSPN are the supplies listed below.

1) hardware inputs:
   a) all the components of the TOE and its environment listed in *Table 1: Product assessment configuration*. The components of the TOE must be provided in their *production* configuration[9];
   b) a hardware or software setup allowing to simulate door locking devices, which can be a model.
2) software inputs:
   a) any additional means of administration required by the solution (if dedicated software is required, for example, for provisioning or keying, software updates, etc.)
   b) the source code (not pre-processed) of the TOE cryptographic mechanisms;
   c) firmware allowing to test the software update of the system components (if the update is included in the functions of the security target);
   d) any licences required by the solution.
3) documentary inputs:
   a) all the installation, configuration, administration and user documentation for the entire system, regardless of the scope of the product assessed. This includes, but is not limited to, user enrolment procedure guides. This also includes system components provided by third parties (e.g. readers);
   b) the description of the cryptographic mechanisms.

[8] This will require the CESTI to demonstrate his/her ability to do so, in accordance with the accreditation rules in force.

[9] Here, “production configuration” means that the components are in their “final” state, or “in the state in which they would be supplied to a customer (or an integrator)”. This is opposed to development, test or maintenance configurations, in which the components may have preferred interfaces (such as JTAG) or be configured with passwords, keys or “test” certificates. This also means that all countermeasures (such as detachment detection) must be activated.

The production configuration can be a software input rather than hardware, if this corresponds to the developer’s standard delivery format (for example, for the system management software).

3. State of the art and specific instructions for the evaluator

An access control system must protect the user against two essential risks:

R1. unauthorised entry into the premises;
R2. concealment (non-detection by the system) of an entry into the premises.

The evaluator will base their opinion on the possibility for an attacker to realize either of these critical threats[10].

3.1. Installation

The evaluator must decide on the risks caused by a poor installation and incompleteness of the developer's installation guides. This therefore requires the evaluator to carry out the software installation[11] of the product themselves. The evaluator may ask for additional assessment men*days if necessary.

At the end of the installation, the evaluator will ensure in particular that a procedure confirms that the versions of the installed components correspond to those listed in *Table 1: Product assessment configuration.*

3.2. Analysis of the security target

The security problem definition of the security target must at least respond to the two essential risks R1 and R2, otherwise the target will be considered misleading.

These risks are expected to be broken down into lists of threats, which may differ from one system to another. This document does not require a detailed list of threats because such a list would evolve according to the technological choices of developers and the state of the art.

3.3. Vulnerability analysis

3.3.1. Interpretation of vulnerabilities

The vulnerabilities discovered on the product should be interpreted from the perspective of the essential risks of the product (R1 and R2)[12].

In particular, the evaluator must take into account the fact that physical access control products are intended to be used over long periods of time (up to 10 or 15 years). The evaluator must therefore take into account the risks of undersizing cryptographic mechanisms, or the risks associated with a long product exposure (for example, the absence of firmware or key updating mechanisms).

3.3.2. Attack surface

In his/her arguments, the evaluator will have to consider the different attack paths described in the table below.

---

[10] It is understood that each of these threats can be carried out by various means. For example, *unauthorised entry into the premises* may result from disclosure of secrets, unauthorised modification of a component's firmware, etc.

[11] The hardware installation can be carried out by the evalautor if he/she has the required skills (in particular electrical accreditation). However, by default, it will be considered to be done by the developer.

[12] Examples: poor protection of software updates will be a point of attention, *even if this is not an explicit security function of the product*, as this can help an attacker to realise risk R1. Similarly, a user enrolment process that is non robust may be considered to be a product vulnerability, *even if the vulnerability stems from documentation rather than the software or hardware.*

Location of the attacker		**Hardware attacks**	**Logic attacks**
On-site	Core area	The hardware attack is not considered because the core area is assumed to be secure.	Attack via system **management functions** (see §A.2ii) or via connection to the **company network** (see A.2iii)
	Protected area	Hardware attack of the **LPUs**[13] (see §A.1i)	Attack of the **access management network** (see §A.2i) typically between LPUs, or between LPUs and system management software.
	Public area	Physical attack of **badges** or **readers** (see §A.1ii)	Attack of the **access management network** (see §A.2i) typically between readers and LPUs.
Off-site		Hardware attack of **any component** of the system **before installation** or **after end of life** (see §A.1iii)	Attack via the **Internet** (see A.2iv)

Table 3: Attack paths to be considered during the assessment

Each attack path gives rise to detailed points of attention in Annexe A. These points of attention do not, however, constitute an exhaustive list of scenarios to be studied.

4. References

[P-CSPN-02]	Procedure – Criteria for First Level Security Certification assessment, Reference: ANSSI-CSPN-CER-P-02, version in force.
[MET_CSPN]	Application document – Methodology for the assessment of First Level Security Certification – RTE content, Reference: ANSSI-CSPN-NOTE-01, version in force.
[NOTE-20]	Application document – Rules for the implementation of security assessments, Reference: ANSSI-CC-NOTE-20, version in force.
[GUIDE-ACCES-PHYS]	Guide – Security of non-contact technologies for physical access control, version in force

[13] The rating must therefore take into account the effort required to access the LPUs, but physical attacks are not excluded in principle.

Annexe A Points of attention for the evaluator

A.1 Hardware attacks

Assessment of the security of the hardware interfaces is limited to attacks of relatively moderate difficulty[14]:

- identification of components present on the PCB;
- operation of JTAG or UART debug interfaces;
- extraction of flash memory (and possible reverse engineering);
- communications probing on the PCB[15];
- tearing detection and detection of enclosure opening.

i. LPUs

If a SAM is present, the evaluator must take into account the risks associated with its life cycle (provisioning, key renewals, etc.), particularly if it is removable and can be handled outside the protected area. The evaluator must also check that the system complies with the SAM developer's guides in order to avoid accidental deterioration of security. Finally, as with any third-party component, the evaluator must pay attention to the presence of non-certified elements not controlled by the developer[16].

ii. Readers and interface with badges

The evaluator must check the robustness of the system against attacks exploiting the wireless interface, in particular relay attacks[17].

iii. Any components before installation or after end of life

The evaluator must check whether sensitive assets can be compromised before installation or after the end of life of the components[18].

The evaluator will take care to consider the compromise of an asset on equipment that has been scrapped or that has not yet installed, in view of the essential risks R1 or R2[19].

---

[14] The assessor is not expected to provide a proof of concept for *all* the hardware vulnerabilities identified. The opening detection, in particular, will be rated in a purely theoretical way based on experience. Proof of concept will be realised when necessary, for example to demonstrate compromise by a debug port or recovery of in-memory secrets.

[15] Example: recovery of a PIN on the ribbon cable connecting the keypad to the microcontroller of a badge reader.

[16] Example: a non-certified third-party app on a certified SAM.

[17] Example: regarding relay attacks, the assessor can check that the badges and/or readers implement distance bonding or equivalent countermeasures.

[18] Example: the assessor will seek to demonstrate the presence and effectiveness of mechanisms such as:

- erasure of sensitive information;
- pairing or other measures prohibiting the insertion of an illegitimate or altered component;
- protection of sensitive information by access control, software cryptographic protection or use of a hardware cryptographic component.

[19] Example: the compromise of a diversified key, on a component at the end of life, will not necessarily threaten the system. However, the attacker could exploit the presence of non-diversified keys on copies available for sale.

A.2 Logic attacks

i. Via the access management network

In view of critical risk R2, the evaluator must consider the risks of denial of service of the access management network and transmission of alarms. In particular, it must check that such a denial of service cannot be easily carried out from public areas[20].

If a fuzzing campaign is being conducted, the ITSEF will have to describe the method used (in particular the transfer rules and the volume of traffic sent). The certification centre may require the fuzzing script to be provided if this description is not sufficient.

ii. Via management functions

Management functions play a central role in the system. The evaluator will therefore pay attention to scenarios in which the ACM or its components are attacked. This typically includes, but is not limited to:

- compromise of databases or directories (keys, user permissions, etc.);
- compromise of the management or remote updating of system components.

The preferred vectors of these scenarios will in particular be:

- exploitation of ACM interfaces[21];
- partitioning weaknesses between ACM resources and other applications[22];
- the life cycle of trusted data[23].

iii. Via the company network

The evaluator will, by default, assume that the system is connected to the company network and will therefore focus on studying the exposed interfaces of the system as well as the system's dependence on data from the company network[24]. If the security target provides for the system to be disconnected from the company network, the evaluator will have to decide on the ease of use in this mode.

iv. Via the Internet

From a system perspective, this scenario is the same as an attack from the company network (see previous section), even more so if the system is connected to the Internet through the company network. However, the rating of vulnerabilities will be lower if a remote attacker can act directly from the Internet without needing to bounce from the company network.

---

[20] Example: replay of a reader's detachment alert.

[21] Example: assessment of a non-preferential user privileges from a management interface - only the most privileged roles (administrator) should be considered "trustworthy".

[22] Example: if the assumptions of the security target allow the installation of software on the same server as the system management software, the assessor will check whether this server restricts access rights to the sensitive data of the system management software.

[23] Example: the mechanisms for revocation or renewal of user keys.

[24] Example: the use of digital certificates from a company PKI.