SPAC
>ALLIANCE<

DISCOVER THE EUROPEAN WAY OF SECURITY

1. **SPAC Alliance**
2. **New threats**
3. **Legal response:**

   Link realms and hold stakeholders accountable
4. **Focus :**

   Obsolete technologies and protocols on access control systems

SPAC Alliance History

FOUNDED IN 2020

- > FEDERATE EUROPEAN SECURITY STAKEHOLDERS
- > ADVOCATE FOR THE MARKET BEFORE THE INSTITUTIONS
- > BUILD EUROPEAN SOVEREIGNTY WITH HIGH SECURITY STANDARDS

WE GATHER THE WHOLE ECOSYSTEM

SPAC ALLIANCE MEMBER

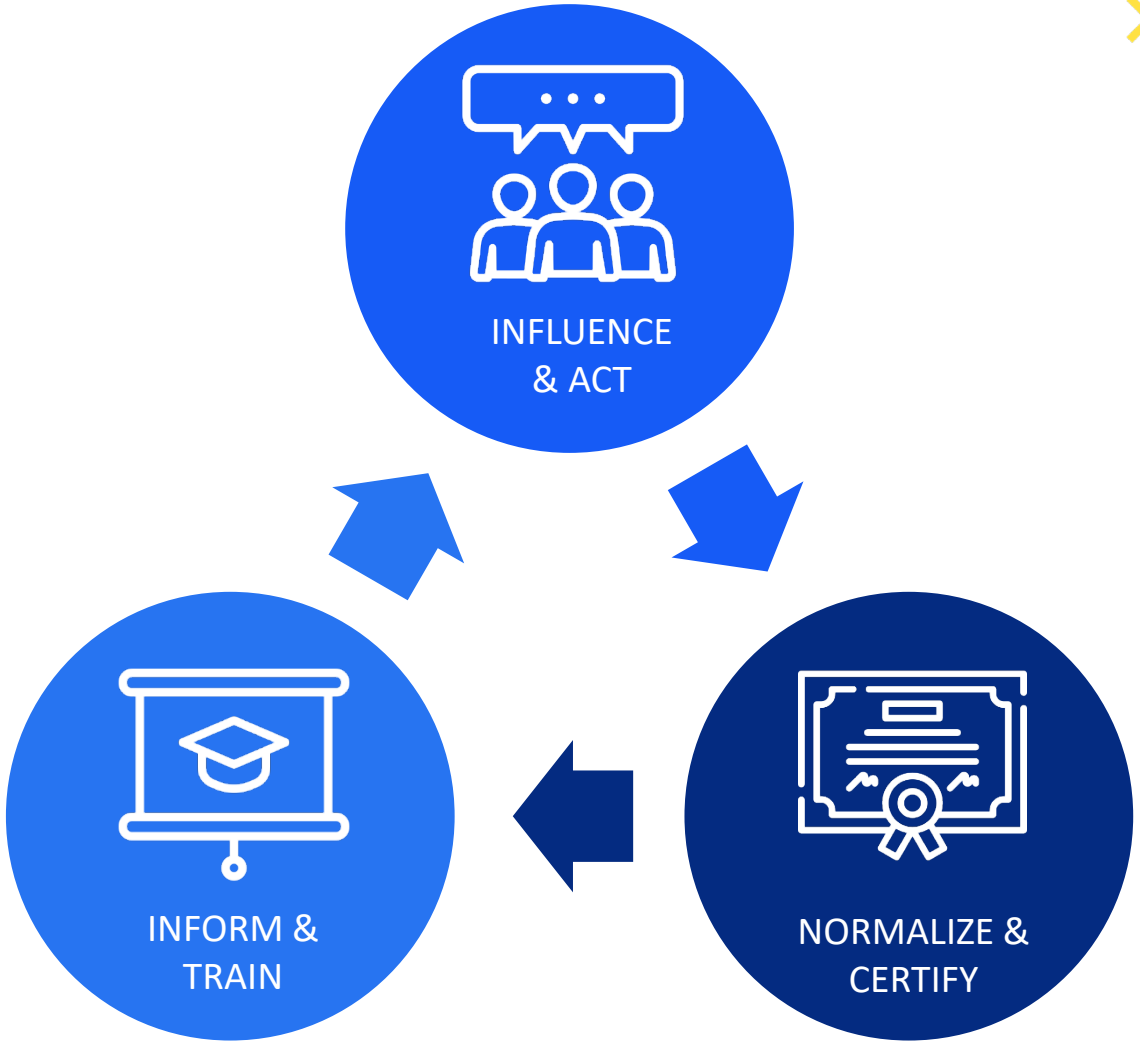
- > MANUFACTURERS
- > INTEGRATORS
- > INSTITUTIONS
- > SERVICE PROVIDERS

SPAC ALLIANCE CLUB

- > END-USERS
- > INSTALLERS / DESIGN OFFICES
- > CONSULTANTS
- > JOURNALISTS

SPAC Alliance Members

SPAC Alliance Missions



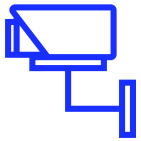
SPAC ALLIANCE

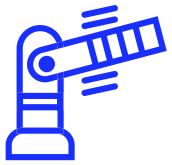
News Threats

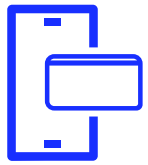
CYBER ATTACKS

PHYSICAL ATTACKS

HYBRID ATTACKS







« There should no longer be a gap between physical security and cybersecurity.. »

ENISA Threat Landscape 2024

SPAC ALLIANCE

Real Figures, hard facts

HYBRID ATTACKS:

8,5%
of data breaches*

$$
most expensive attacks*

X2
cost in US / MEA VS Europe*

*IBM Cost of data breach reports 2021 - 2025

Summary : NIS Investments 24

Publisher : ENISA October 22,2024 – NIS 2 / CRA / AI Act / PQC
Questions were asked to 1,350 companies across 27 EU countries

KEY TRENDS

90% expect an increase in cyberattacks in the coming years (cost and volume)

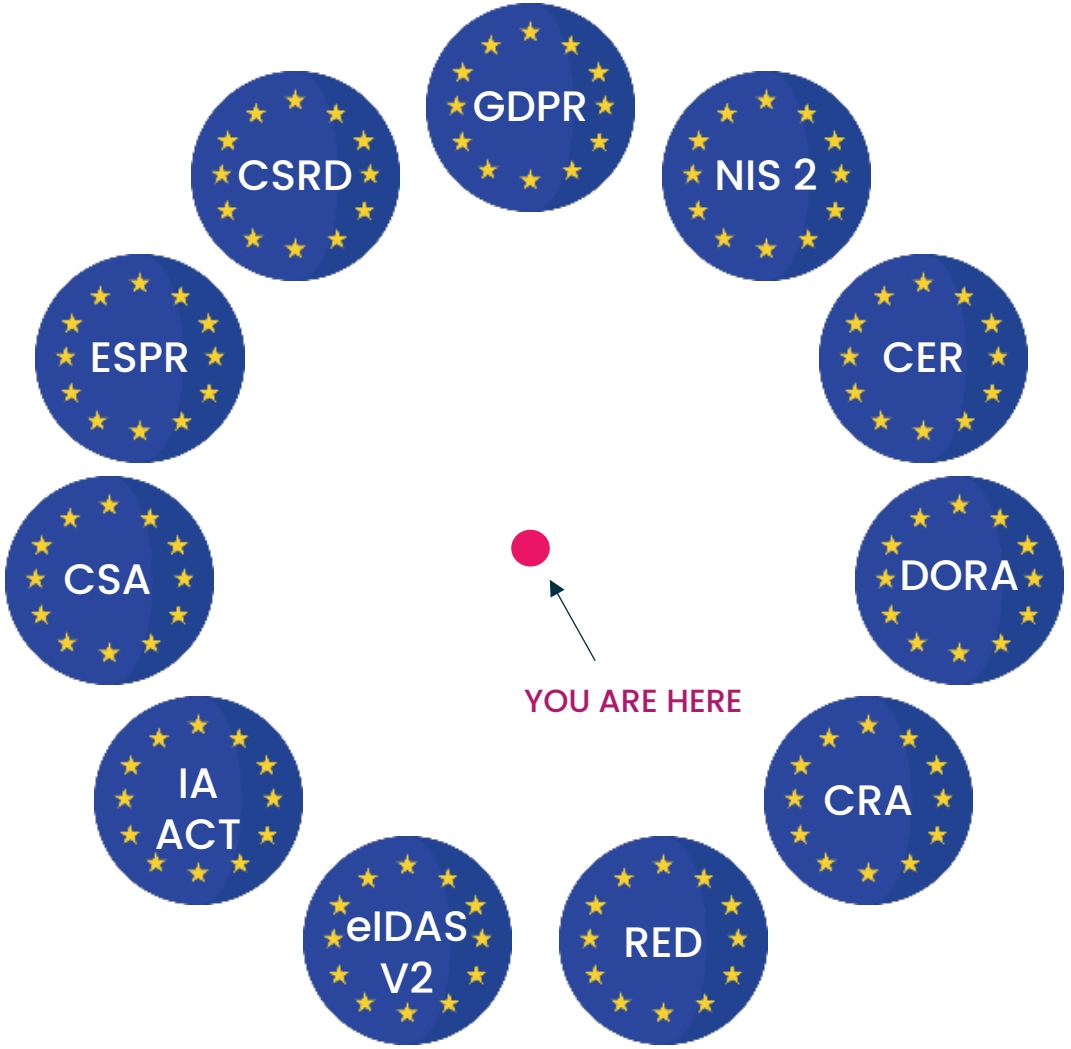
4,4M€ average cost of a data breach (+10% vs. 2023)

60% of cyberattacks exploit known vulnerabilities that have not been patched

86% strongly believe that an EUCC (cyber certification) is beneficial

55% rely on supplier certifications to ensure security

EU Legal Framework



SPAC ALLIANCE

EU Legal Framework

NIS 2 | CER | DORA

REQUIREMENTS
Public and private entities

CRA | RED

TRUSTED PRODUCTS
Manufacturers, Importers

eIDAS V2 | AI ACT

INNOVATIONS
Physical and Logical

CSA

CERTIFICATION
Common EU scheme

+ RESPONSABILITY

GDPR | CSRD | ESPR

SPAC ALLIANCE

NIS 2 : a new paradigm

Network and Information Security 2 (10/2024)

PROTECT MORE

More entites covered(IE - EE)

Collective and cross-border responsability

PROTECT BETTER

End-to-end security concept

Link Between Cyber and Physical Security

SUPPORTS

Mandatory incident reporting

Cross-border Network CSIRT – CERT EU

TO SANCTION

Financial Penalties

SPAC ALLIANCE

CER : to maintain vital activities

Critical Entities Resilience Directive (10/2024)

RESILIENCE

PROTECT

RESPOND

RESIST

MITIGATE

ABSORB

ADAPT

RECOVER

PHYSICAL RISKS

TERRORISM

MALICIOUS ACT

NATURAL DISASTERS

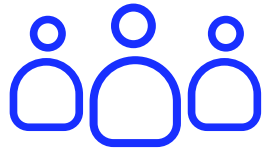
CLIMATE CHANGE

"Ensure appropriate physical security for facilities and critical infrastructure"

ART 13.1.b

OVERSIGHT

Mandatory incident Reporting



Periodic external audits and oversight

TO SANCTION

Financial Penalties

SPAC ALLIANCE

2 - NIS 2 / CER : a new paradigm

NIS 2

Network and Information Security Directive

RAISE AND HORMANIZE THE SECURITY LEVELS OF ENTITIES ACROSS EUROPE

End-to-end security

Link between cyber and physical realms

CER

Critical Entites Resilience Directive

MAINTAIN VITAL ACTIVITIES FOR CRITICAL ENTITIES

Highlights more physical threats

Defines and enforces resilience

INCLUDES SUPPLY CHAIN

MANDATORY INCIDENT REPORTING

FINANCIAL PENALTIES

DIRECTIVES WILL EVOLVE REGARDING THREATS

SPAC ALLIANCE

Cyber Resilience Act

(10/2025)

CONCERNS EVERY PRODUCT WITH DIGITAL ELEMENTS

MANUFACTURERS RESPONSABILITY

SHARED WITH IMPORTERS AND DISTRIBUTORS

Hardware & Software

Enforces lifecycle maintenance

FINES : UP TO 15 M€ / 2.5% OF GLOBAL TURNOVER

CREATION OF 41 HARMONIZED STANDARDS
GENERIC OR VERTICAL

#16 : ACCESS CONTROL

DRIVEN BY SPAC ALLIANCE (HESTIA WG)

COMPLIANCE
SELF-ASSESSMENT OR CERTIFICATIONS

Mandatory for products (including IoT) or services with a digital sold within European Union.
No compliance = No CE mark = product banned from EU

CE

SPAC ALLIANCE

Ensuring High Security

AIM FOR CERTIFICATION

Physical & Cyber Security

INTERNATIONAL REFERENCES

ISO 27001

NIST CSF 2.0

NATIONAL CERTIFICATIONS / FRAMEWORKS

CSPN

CENTRE FOR CYBERSECURITY BELGIUM

CYFUN

ADOPT STANDARDS

Interoperability & resilience

INDUSTRIAL STANDARDS

SSCP

- OPEN & HIGH SECURITY
- INTROPERABLE
- CERTIFIABLE

STANDARDS ENFORCED BY REGULATIONS

CE

- CYBER RESILIENCE ACT
- RED DIRECTIVE

SPAC ALLIANCE

RÉGLEMENTATION EUROPÉENNE

CER / NIS 2

AUDITS- FORMATIONS
AMELIORATION PROGRESSIVE

CERTIFICATIONS / CONFORMITÉ
APPLICATION DES AMENDES

CRA

AUDITS- FORMATIONS
AMELIORATION PROGRESSIVE

CERTIFICATIONS / CONFORMITÉ
APPLICATION DES AMENDES

CSA

EU CC — EU CS — EU 5G — Certification basée sur FITCEM ...?

HARMONISATION DES SCHÉMAS DE CERTIFICATION

ESPR

ADOPTION DU PLAN DE ROUTE

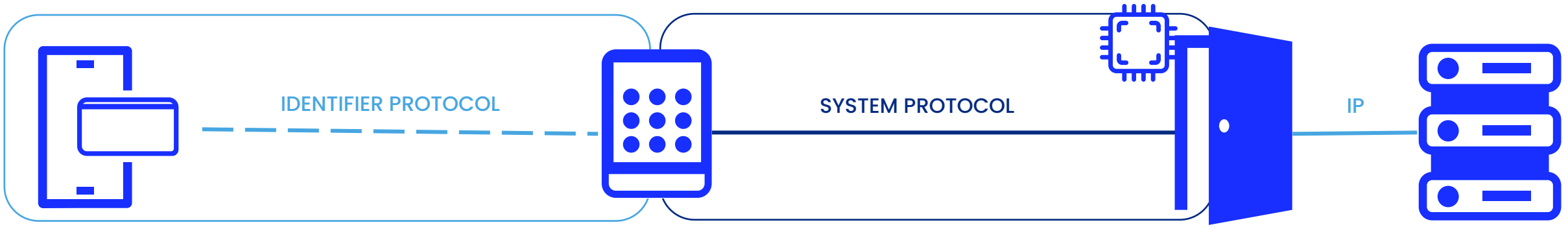
LIVRAISON DE PRODUITS RESPECTANT LE RÉGLEMENT

SPAC ALLIANCE

Key Take-aways

1. New Regulations are reshaping the ecosystem
2. They evolve towards ever-stronger requirements
3. Compliance is temporary, you need to stay up to date

4- Communication protocols



UNSECURE	125 KHZ	WEAK READER	WIEGAND – TTL – DATA CLOCK
END-TO-END SECURITY	13,56 MHZ ISO 14443	ROBUST READER	OSDP SC / SSCP

SPAC ALLIANCE

OSDP and SSCP

	SIA (USA)	SPAC ALLIANCE (Europe)
	The most used	The most integrated into CSPN-certified solutions
	OPTIONAL SECURITY (Secure Channel) OPENNESS & INTEROPERABILITY DRIVEN BY SIA	MANDATORY SECURITY OPENNESS & INTEROPERABILITY DRIVEN BY SPAC ALLIANCE
CONFIDENTIALITY	AES 128	AES 128
INTEGRITY	AES CMAC truncated to 64 bits	HMAC SHA 256
AUTHENTICITY		

EUROPEAN BY DESIGN

SSCP Technical Report

SSCP embeds a Secure Transport Layer able to encrypt all assets between an IS (Inspection System, like a reader) and a Host (like a controller) after a prior mutual authentication.

SSCP Technical Report describes all commands, grouped into modules, required to be SSCPv2.1.7 certified. A **Module** defines a set of commands will be supported by the IS according to the GetDeviceCapabilities command.

MANDATORY MODULE

All commands defined into a mandatory module have to be supported by the Host and the IS.

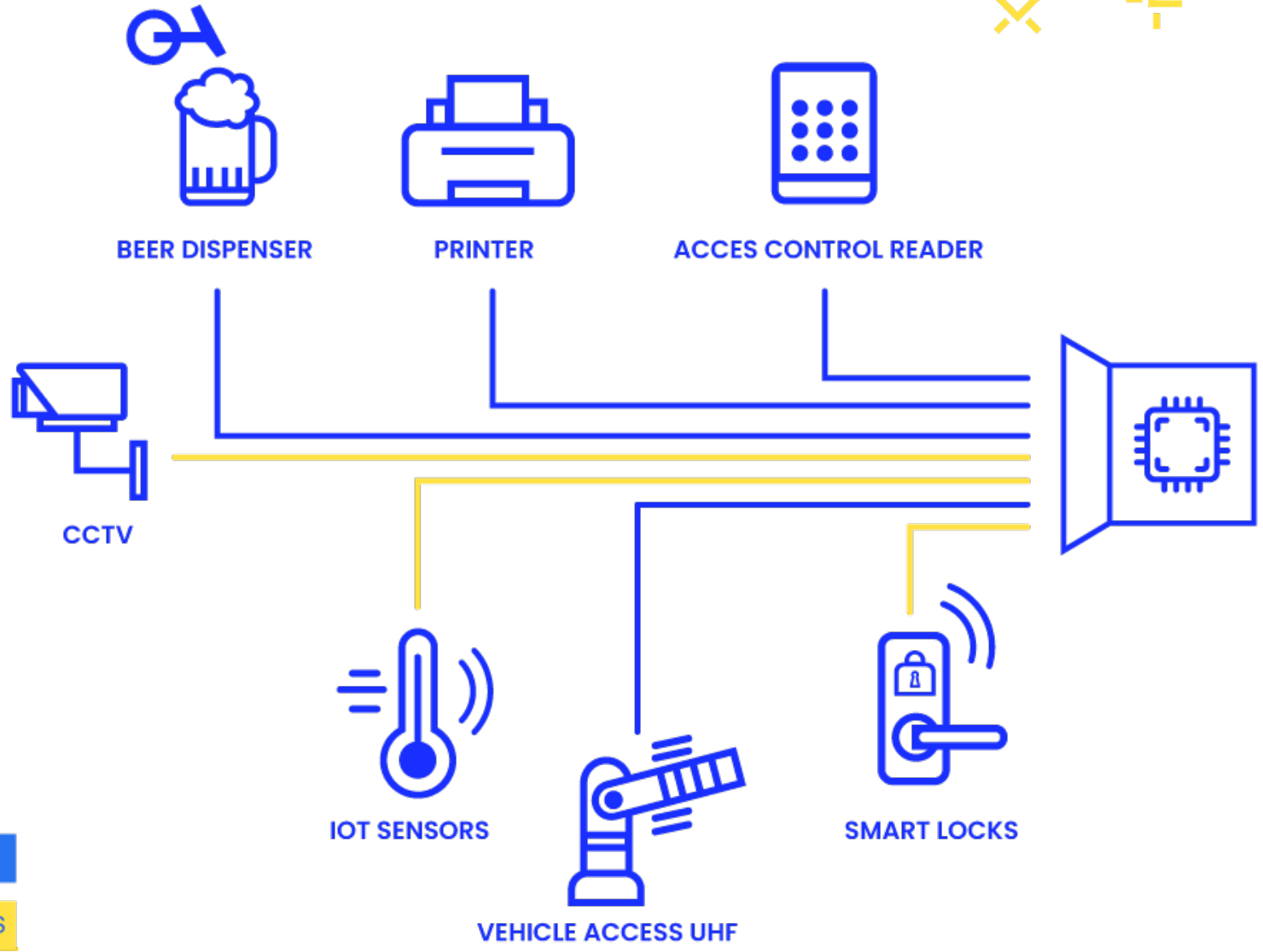
OPTIONAL MODULE

All commands defined into an optional module have to be supported by the IS.
Host selects which commands defined into an optional module have to be supported.

SSCP Certification Compliancy

MODULES	MANDATORY / OPTIONAL	COMMANDS
AUTHENTICATION & TRANSPORT	MANDATORY	Authenticate / ChangeISKeys / GetInfos / SetBaudRate / Set485address / GetDeviceCapabilities
TRANSPARENT	OPTIONAL	ScanGlobal(13.56MHz) / TransceiveAPDU
TRANSPARENT PROXIMITY	OPTIONAL	ScanGlobal(13.56MHz) / TransceiveAPDU / ProxiCheckFirst (Option 01h) / ProxiCheckVerify
LEDs	OPTIONAL	OutputRGB (only LEDs bits)
Buzzer	OPTIONAL	OutputRGB (only Buzzer bits)
TAMPER	OPTIONAL	SetTamperSwitchSettings / GetTamperSwitchInfos
Inputs	OPTIONAL	GetInputState
Outputs	OPTIONAL	SSRelay_Config / SSRelay_Action
Low Frequency RFID Reader (125kHz)	OPTIONAL	ScanGlobal (125kHz)
High Frequency RFID Reader (13.56MHz)	OPTIONAL	ScanGlobal (13,56 MHz)
Ultra High Frequency RFID Reader (850-960MHz)	OPTIONAL	ScanGlobal (UHF)
Bluetooth - BLE	OPTIONAL	ScanGlobal (BlueTooth)
Keyboard	OPTIONAL	ScanGlobal (Keyboard)
Touchscreen	OPTIONAL	ScanGlobal (TouchCoordinates
Screen	OPTIONAL	TS_LoadPictureScreenIndex
Matrix Code	OPTIONAL	ScanGlobal (Image Scan Engine)

SSCP Ecosystem



FONCTIONAL

IN PROGRESS

SPAC ALLIANCE

ANSSI evolutions

Update of the Recommendation Guide on Securing Physical Access Control and Video Surveillance Systems - Link

Shift toward biometric authentication	Offline Locks
R31-	R43

Configuration between reader and LPU

Recommanded new architecture

SPAC ALLIANCE

Multi-factor Architecture

Update of the Recommendation Guide on Securing Physical Access Control and Video Surveillance Systems- Link

New Transparent architecture recommended by the ANSSI

In cases where multi-factor authentication is used, it is necessary to protect the second factor exchanged between the device connected to the reader head and the LPU (Logical Processing Unit). To achieve this, a secret shared by both devices is required.

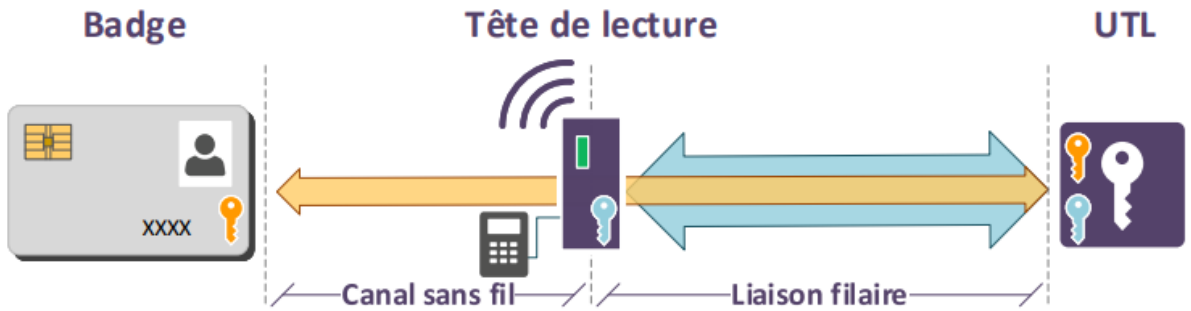


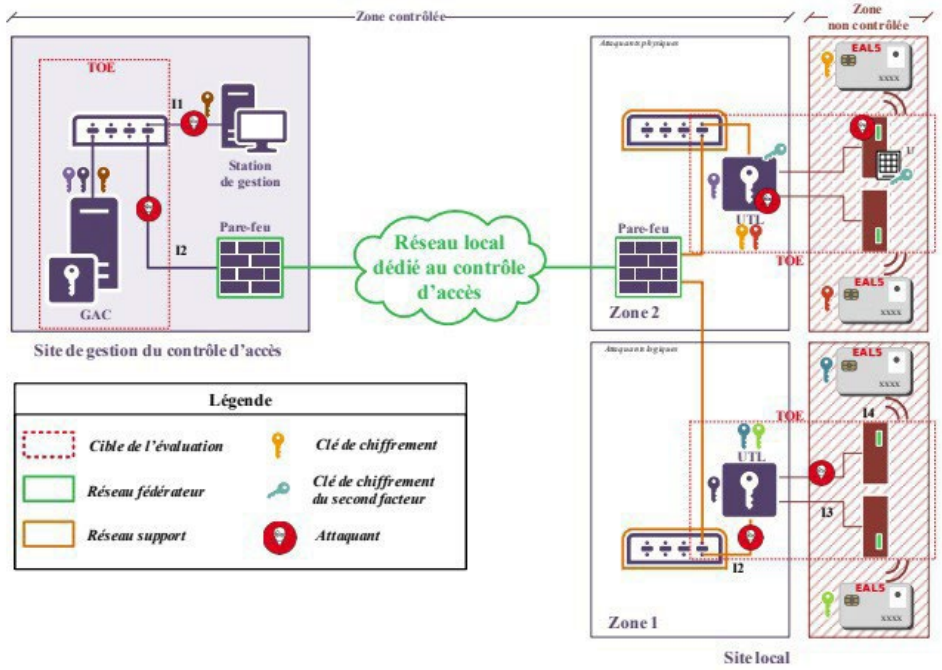
FIGURE 14 – Configuration type n°1 avec introduction d'un double facteur d'authentification : tête de lecture transparente, authentification de bout en bout, chiffrement du second facteur

SPAC ALLIANCE

CSPN for Acces Control

Publication of the New Protection Profile for CSPN Certification of Access Control Systems- Link

EXTENDED TOE



SECURING COMMUNICATIONS

B3 Échanges entre les UTL et le GAC
Le GAC pilote les UTL et assure une transmission périodique de la base de données nécessaire au traitement local des demandes d'accès. Ces flux doivent être protégées en confidentialité, en intégrité et en authenticité.

B4 Échanges entre le lecteur de badge et l'UTL
Les UTL assurent la gestion de toutes les demandes d'accès en provenance des têtes de lecture qui lui sont rattachées. Les flux entre les UTL et les têtes de lecture doivent être protégées en confidentialité, en intégrité et en authenticité.

SPAC ALLIANCE

SSCP & Certifications

CSPN Certification

SSCP is the most used communication protocol in CSPN Certified Solutions

GENETEC - SECURITY CENTER SYNERGIS / CLOUD LINK

Company: GENETEC
Certified Solution: Security Center Synergis Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0)

Solution Details:
The evaluated product is "Security Center Synergis, Version Security Center Synergis 5.12.2, Synergis Cloud Link 3.1.2 (Firmware 3.1.855.0)" developed by GENETEC EUROPE.
This product is a component of GENETEC's unified security platform, Security Center, providing physical access control functions and offering centralized, real-time management of secured areas.

This certification also includes the secure I/O modules developed by STid, including the Architect range readers (ARC-A, ARC-B, and ARC-1) that were presented during the certification process, as well as the SSCP V2 protocol and MIFARE DESFire EV3 credentials.

Certification Date: May 27, 2025

Download the ANSSI CSPN Certificate

TIL TECHNOLOGIES - MICRO SESAME / TILLYS-CUBE / MLP2

SYNCHRONIC – LPU for XScur

SSCP certified products

3 levels of certification inline with the European model (Basic / Substantial / High)

- STid ARC B HIGH
- STid ARC B - SUBSTANTIAL
- STid ARC A HIGH
- STid ARC A - SUBSTANTIAL
- STid ARC C HIGH
- STid ARC C - SUBSTANTIAL
- ELSYLOG SYRIUS (181101) - SUBSTANTIAL
- ELSYLOG SYRIUS (181101) HIGH

› SSCP is a reliable standard that simplifies certification efforts

SPAC ALLIANCE

SSCP Certifications

BASIC LEVEL

This evaluation level relies on unit tests dedicated to assessing the security of the SSCP protocol supported by SPAC Alliance:

- authentication command tests
- encryption tests
- signature tests

SUBSTANTIAL LEVEL

Basic level +:

- tests for commands related to the “Transparent” communication mode
- tests for optional functional commands related to modules

HIGH LEVEL

Substantial + specific test scenarios

- **UTL**: functional documents provided by the developer (flow diagrams, command tables, etc.)
- **Readers**: verification of support and functionality of all commands associated with functional modules reported by the GetDeviceCapabilities command.

Project history

Cyber Resilience Act

EUROPEAN REGULATION

PUBLISHED ON 23/10/2025

HARDWARE & SOFTWARE IMPACTS

ACCESS CONTROL : CLASS 1

SELF-ASSESSMENT / CERTIFICATIONS

CREATION OF HARMONIZED STANDARDS

«Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers» – Annex 3 – Important products - Class I

EUROPEAN INSTITUTION

European Commission

European Parliament

enisa European Network and Information Security Agency

Bundesamt für Sicherheit in der Informationstechnik

ANSSI

CEN CENELEC ETSI

EUROPEAN STANDARDIZATION ORGANIZATIONS

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

Liberté
Égalité
Fraternité

SURETE BATIMENTAIRE CCN SGAMI NORD DSIC

SPAC ALLIANCE

Certification Schéma

Basique

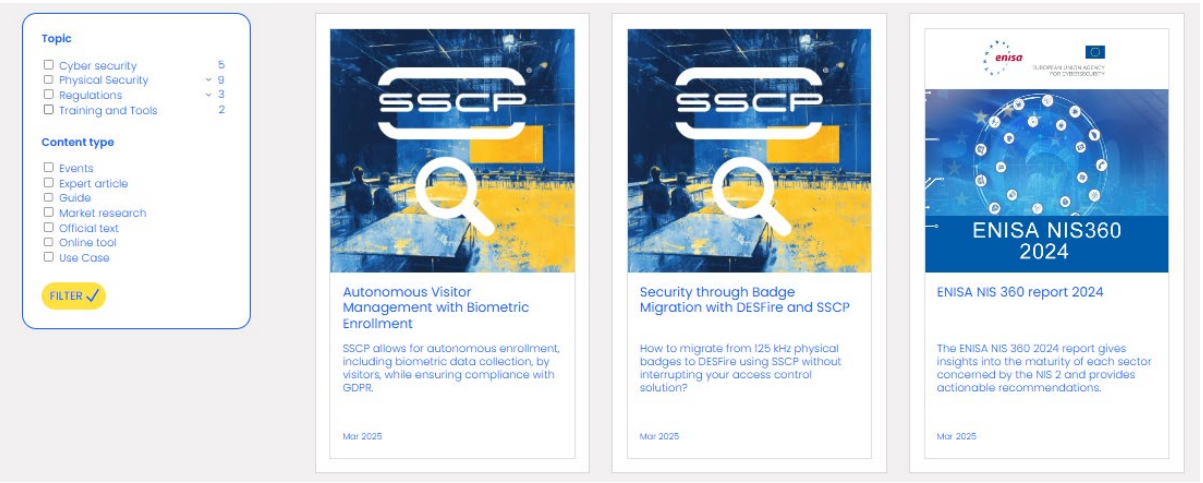
Substantiel

Elevé

5 – SPAC Alliance SERVICES

LIBRARY

General Security Knowledge



ONLINE SECURITY AUDIT

Free and anonymous

Services shop

From audit to certification

www.spac-alliance.org

SPAC ALLIANCE

5 – BECOME A MEMBER!

SPAC ALLIANCE MEMBER

MANUFACTURER	MAKE YOUR VOICE HEARD
INSTITUTIONALS	PARTICIPATE TO WORKING GROUPS
INTEGRATORS	BOOST YOUR VISIBILITY
INSTALLERS	MEET END-USERS
SPECIFIERS	CONTRIBUTE TO STANDARDIZATION

www.spac-alliance.org

5 – JOIN THE CLUB!

SPAC ALLIANCE CLUB

CISOs	ACCESS LIBRARY AND GUIDES
CIOs	UNDERSTAND THE REGULATORY FRAMEWORK
EXECUTIVES	LEARN THROUGH WORKSHOPS AND WEBINARS
SECURITY MANAGERS	INTERACT WITH MEMBERS
ACCESS MANAGERS	ACCESS OUR SERVICE OFFERINGS

www.spac-alliance.org

Contacts

Mickaël Wajnglas

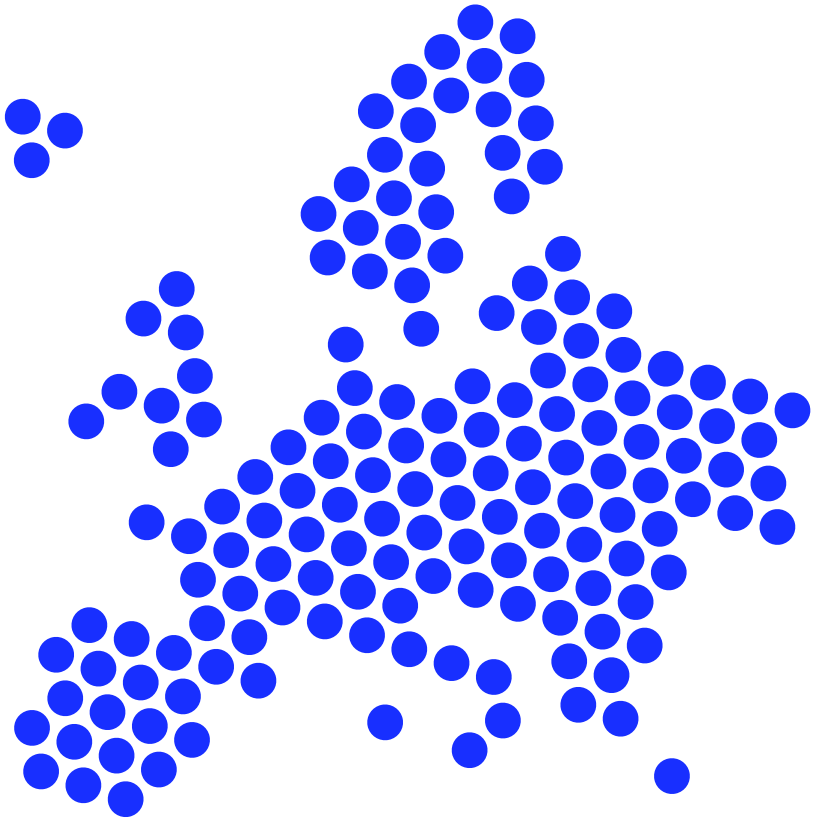
m.wajnglas@spac-alliance.org

Sandrina Castillo

s.castillo@spac-alliance.org

Tibaud Estienne

t.estienne@spac-alliance.org



www.spac-alliance.org

SPAC
ALLIANCE

Contact

Tibaud Estienne

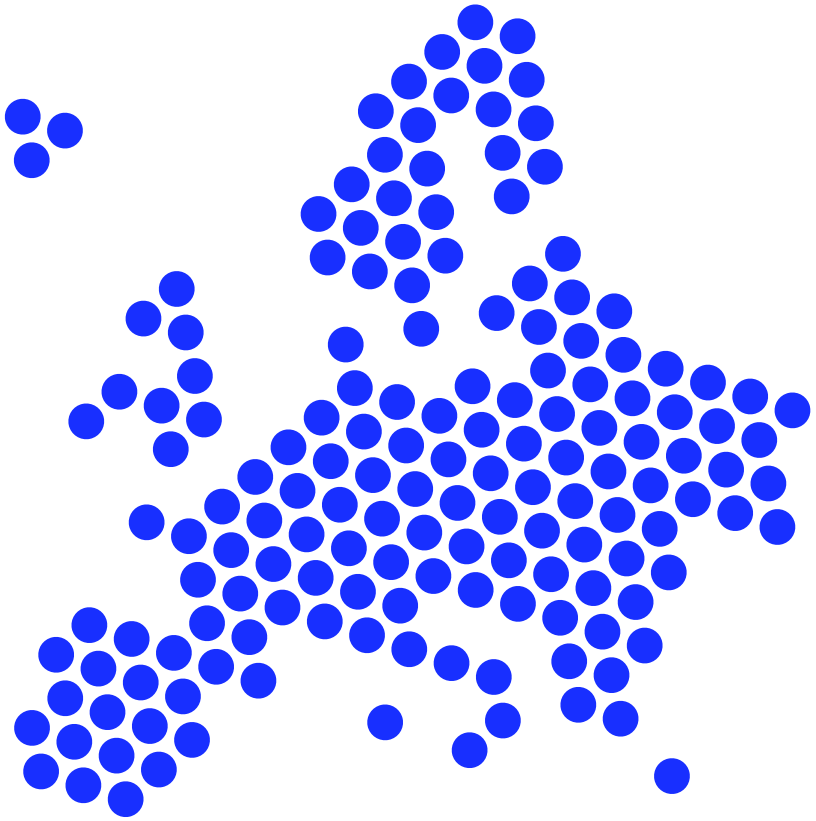
t.estienne@spac-alliance.org

Mickaël Wajnglas

m.wajnglas@spac-alliance.org

Sandrina Castillo

s.castillo@spac-alliance.org



www.spac-alliance.org

SPAC
ALLIANCE