
SPAC
LA SÉCURITÉ
DIGITALE
À DIMENSION
EUROPÉENNE
©SPAC

SPAC

Anne-Isabelle Parodi
ai.parodi@sp-ac.org
https://www.sp-ac.org
+33 (0)6 70 08 50 40
Baptiste Dupart
+33 (0)6 46 91 93 41

1 Des cyberattaques croissantes

2 SPAC œuvre pour une industrie de la sécurité forte et ouverte

3 Les services de SPAC

4 Le protocole SSCP

1 Des cyberattaques croissantes

Des cyberattaques croissantes

- En 2019 9/10 entreprises françaises ont été touchées par une cyberattaque

- Faiblesse de sécurité des objets connectés et des protocoles de communication

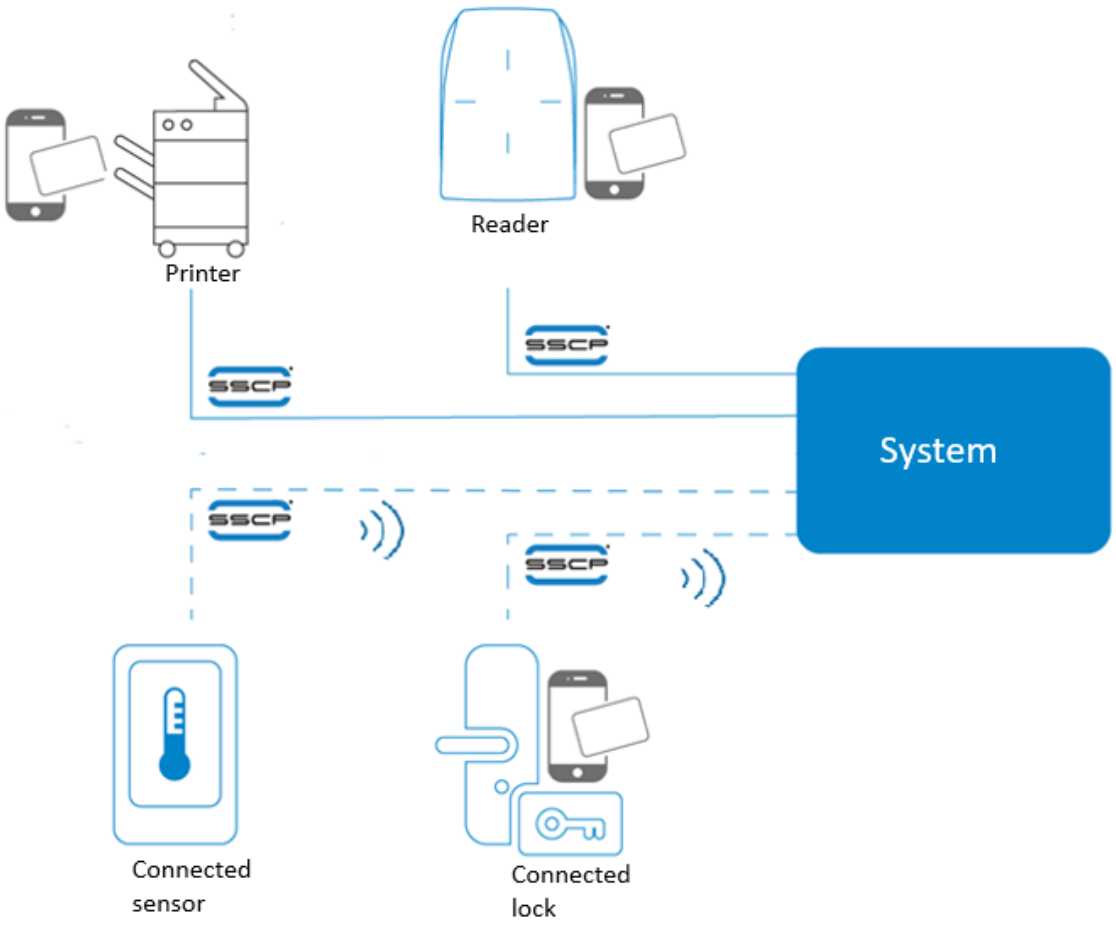
Pour Guillaume Poupard de l'ANSSI

«les objets connectés industriels sont la priorité»

ANSSI Agence nationale de la sécurité des systèmes d'information

- Absence d'autonomie, d'interopérabilité, de compatibilité et de pérennité des solutions permettant de faire face à l'avenir

SECURISER UN SYSTÈME GLOBAL



Les attaques hybrides sont en hausse

- La sécurité physique est souvent l'un des points les plus faibles d'une défense par ailleurs robuste.

- Attaque hybride du capitole à Washington
  - La brèche physique du bâtiment du Capitole
  - Vol d'ordinateurs, vol de clé USB

Bureau de Nancy PELOSI

La France et L'Union Européenne mettent en place un cadre règlementaire

NIS

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES GDPR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

LOI DE PROGRAMMATION MILITAIRE 2019 / 2025

EU CYBERSECURITY ACT

enisa European Network and Information Security Agency

Commission européenne

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Le Marché de la sécurité a besoin d'un cadre règlementaire français et européen !

2

SPAC œuvre pour une Industrie de la sécurité forte et ouverte

SPAC construit une Industrie de la sécurité forte, ouverte et interopérable

Si vous êtes offreur de solutions SPAC vous accompagne :

- Pour faire reconnaitre vos solutions comme solutions de confiance

Si vous êtes Directeur de la sûreté ou DSI, SPAC vous accompagne

- Pour choisir des solutions de confiance. Pour accéder à des solutions interopérables, compatibles et pérennes

SPAC, vous accompagne dans ses principales missions

- d'information
- de formation
- De normalisation

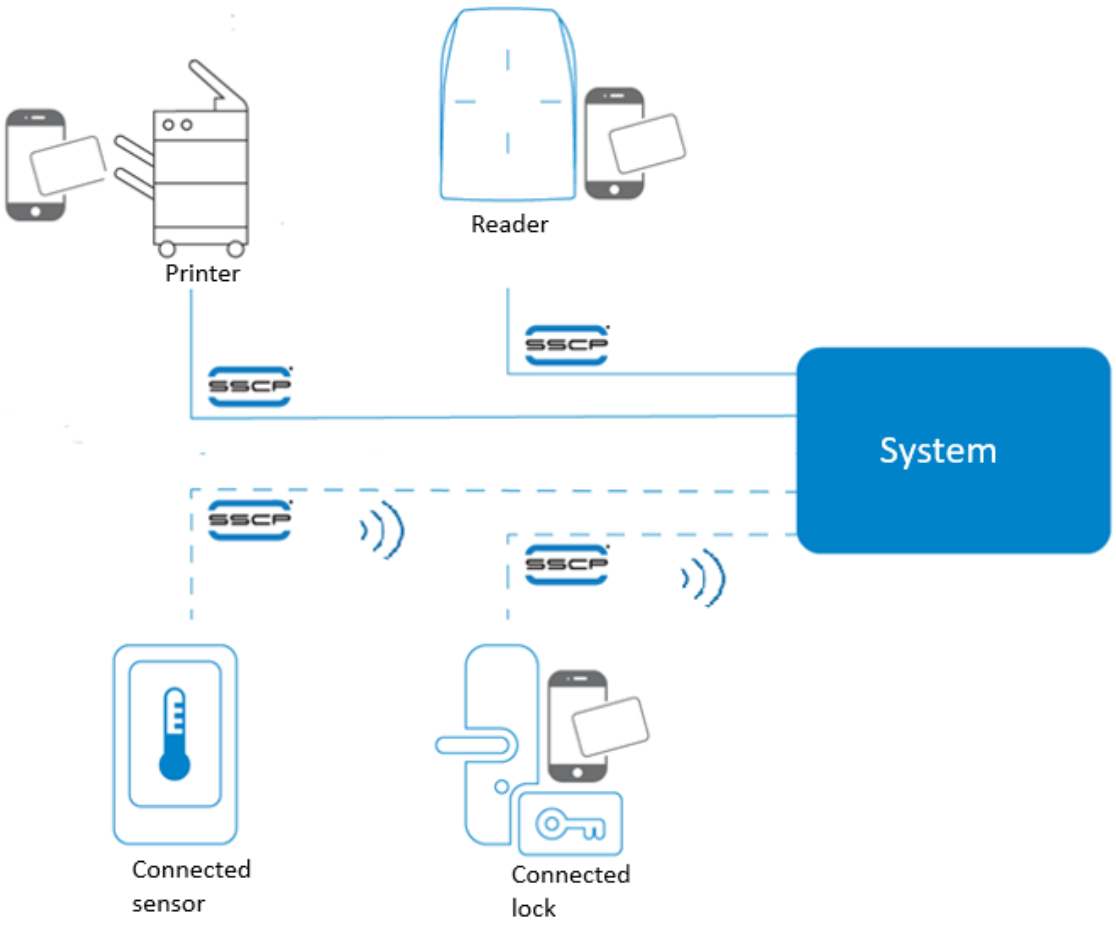
Pour cela, nous utilisons le cadre règlementaire et le protocole de communication SSCP

3 Les services de SPAC

Rester (in)formé (sensibiliser et recommander)

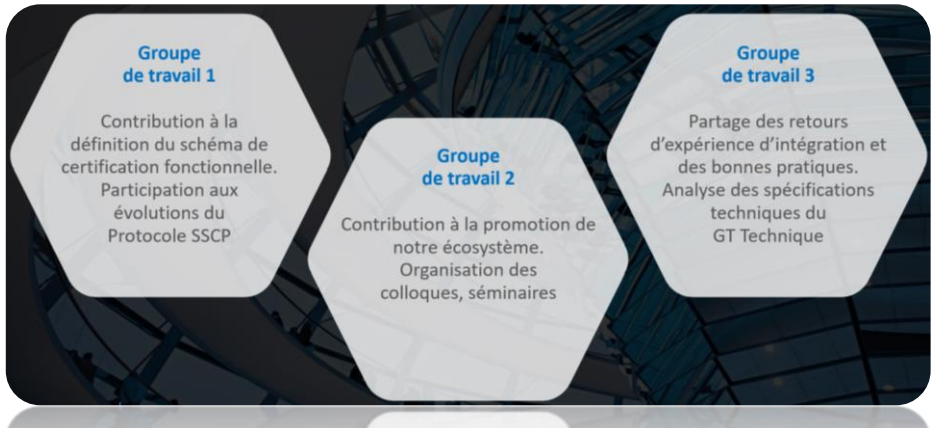
- Proposer des **sessions de formations** et des **webinars** sur la Sécurité Digitale
- Partager des **documents techniques**
- Donner accès à une **veille active** pour identifier les évolutions

SECURISER UN SYSTÈME GLOBAL



Prendre part aux actions de Normalisation / Certification

- Rejoindre des **groupes de travail** sur les évolutions du Protocole SSCP et sur la mise en place de la certification fonctionnelle
- Vous permettre de répondre aux **exigences gouvernementales** en vous recommandant des certifications de sécurité au sein de l'ANSSI
- Vous représenter auprès des **Institutions Règlementaires** françaises et Européennes.
- Accéder à l'interopérabilité des équipements en réalisant des certifications fonctionnelles au sein de SPAC



Obtenir une Certification fonctionnelle SPAC

L'ANSSI délivre **des certifications de sécurité** de type CSPN ou CC

SPAC, en complément, délivre **des certifications fonctionnelles**

Objectif : Assurer une interopérabilité globale des solutions de sécurité et de l'Industrie 4.0, et un niveau de sécurité conforme ANSSI

ANSSI	SPAC
Certifications de sécurité de type CSPN ou CC.	Certifications fonctionnelles

Principes de la certification SPAC

- Utilisation d'un **référentiel** et des **outils** de tests définis par SPAC.
- Tests réalisés par un **laboratoire externe**
- Emission d'un **rapport d'évaluation** et du **certificat de conformité**

Réaliser des mini-audits de vos installations

- **Identifier les failles de sécurité de vos installations**
  - De vos objets communicants
  - De vos protocoles de communications

- **Obtenir des recommandations pour évoluer vers des solutions de confiance**
  - Afin d'obtenir un niveau de sécurité homogène et résistant aux failles potentielles
  - D'être indépendants et autonomes dans la gestion de votre sécurité
  - En adéquation avec les recommandations des Institutions Règlementaires

4 Le protocole SSCP

SPAC s’appuie sur le protocole de communication SSCP

Ouvert et non propriétaire

Securité

- Sécurise la communication entre des objets hardware
- La communication est toujours chiffrée et signée
- C’est le premier protocole de communication certifié CSPN par l’ANSSI

Interoperabilité

- S’appuyant sur une specification très précise
- Qui peut être vérifiée par une certification fonctionnelle
- Pour une plus grande liberté des utilisateurs
- En adéquation avec le cadre règlementaire français et européen

Qui permet de s’adapter aux évolutions du futur

Agnostique du canal de communication

- Peut être utilisé sur des liaisons filaires et non filaires
- Puisqu’il est compatible au modèle OSI (open systems interconnection)

Améliore l’experience utilisateur

- Grâce à la gestion dynamique des objets hardware, il offre plus de solutions applicatives à vos clients

Modulaire et resistant aux évolutions du futur

- Grâce à la structure modulaire de SSCP, ce protocole permettra de communiquer avec de nouveaux objets hardware.

Les membres

Ad Usque Fidelis Cabinet Louis Reynaud

elsyloc

AVANTAGES

secure Systems & Services

SBA SMART BUILDINGS ALLIANCE for SMART CITIES

STid

TiL TECHNOLOGIES

SFA CONSEIL

alcea Ensemble, concevons un monde plus sûr

ASGARD

OSS ASSOCIATION

Omnitech security

TRAFIC TRANSPORT SURETE

EDEN INNOVATIONS

IDEMIA augmented identity

Les membres institutionnels

ANSSI | Agence nationale de la sécurité des systèmes d'information

Connect WAVE

SAFE CLUSTER

SPAC