Evolution en matière d'évaluation des produits et de services de sécurité

13èmes Rencontres de l'ARCSI

Franck SADMI

26/11/2019 - BNF

Agenda

- **L'évaluation de conformité**
- **L'évaluation de conformité en France**
- **L'évaluation de conformité en Europe**
  - Directive NIS
  - Règlement Cybersecurity Act (CSA)
    - Les acteurs (NCCA, ECCG, SCCG, AhWG)
    - Fonctionnement du CSA
    - Les schémas de certification
- **Les enjeux du Cybersecurity Act**

L’évaluation de conformité

- Définition de l’évaluation de conformité : (ISO 17000)
  - « Démonstration que des exigences spécifiées relatives à un produit, processus, système, personne ou organisme sont respectées. (exigence spécifiée : besoin ou attente formulé - Les exigences spécifiées peuvent être formulées dans des documents normatifs tels que les règlements, les normes et les spécifications techniques »

- **L’évaluation de conformité** est une démonstration reposant sur une **auto évaluation** (émission d’une déclaration de conformité) ou sur une **certification tierce partie** (émission d’un certificat)

L’évaluation de conformité

- Intérêt de la certification :
  - Donner des éléments rationnels pour donner confiance (niveau)
  - Avoir une reconnaissance (sectorielle, géographique, sociale) de la part d’un tiers
  - Rationnaliser la relation client/fournisseur (avoir un référentiel commun)
  - Répondre à des exigences règlementaires/contractuelles/commerciales
- Point de vigilance sur la certification :
  - Il existe une multitude de certifications possibles, encore faut il connaitre son besoin et le périmètre de la certification!
- Les acteurs de la certification :
  - Le fabricant (qui est responsable du produit/service/processus)
  - L’organisme d’évaluation de conformité (CAB) regroupant
    - Les évaluateurs (qui réalisent l’évaluation)
    - Les certificateurs (qui contrôlent l’évaluation et émettent le certificat)

L’évaluation de conformité en France

- Cadre réglementaire
  - Décret n°2002-535 (décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information – 2002)
  - RGS (Administrations, 2010)
  - LPM (OIV, 2013-2015)
- Le cadre français repose sur 2 processus
  - La certification
  - La qualification

- L’évaluation des produits
  - La certification Critères Communs (7 niveaux EALs) (reconnaissance SOG-IS/CCRA)
  - La certification CSPN (approche boite noire, entre 25 et 35 jours d’évaluation)
  - La qualification de produits
    - recommandation de l’ANSSI d’un produit pour un cas d’usage spécifique
    - 3 niveaux Elémentaire/Standard/Renforcé
    - repose sur la certification, la validation de la cible de sécurité par l’ANSSI et l’engagement du fabricant

L’évaluation de conformité en France

- La qualification de services
  - Prestataires de services de sécurité (« pure player » de la sécurité)
    - Prestataire d’Audit de la Sécurité des Systèmes d’Informations (PASSI)
    - Prestataire de Détection d’Incidents de Sécurité (PDIS)
    - Prestataire de Réponse aux Incidents de Sécurité (PRIS)
    - Prestataire d’Assistance et Conseil en Sécurité* (PACS)
  - Prestataires de services
    - Prestataire de service d’informatique en nuage (SECNUMCLOUD)
    - Prestataire d’Administration et de Maintenance Sécurisées* (PAMS)
  - Prestataires de services de confiance numérique
    - Prestataire de Service de Certification Electronique (PSCE)
    - Prestataire de Service d’Horodatage Electronique (PSHE)
    - …

L’évaluation de conformité en Europe

- Cadre réglementaire
  - Directive NIS
    - Adoption par le parlement européen le 6 juillet 2016 / publication du décret d’application de la loi de transposition Fr le 25 mail 2018
    - Renforcement des capacités nationales
    - Cadre règlementaire pour les Opérateurs de Service Essentiels (OSE)
  - Règlement eIDAS
    - Règlement « eIDAS » n°910/2014 du 23 juillet 2014
    - Accroître la confiance dans les transactions électroniques au sein du marché intérieur en particuliers entre les organismes du secteur public et les prestataires de services de confiance

L'évaluation de conformité en Europe : le Cybersecurity Act

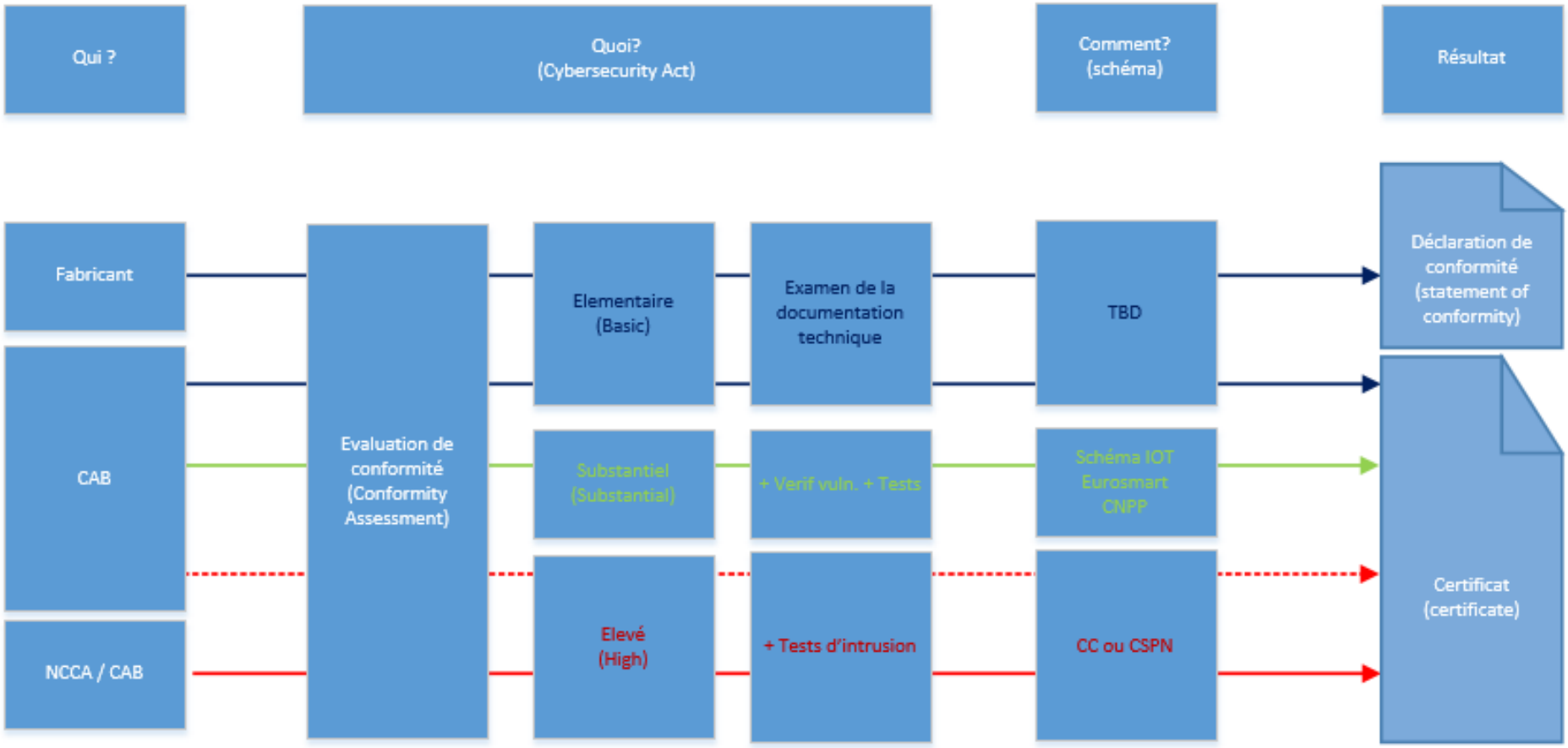
- Règlement (UE) 2019/881 du parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013

→ Application à partir du 27 juin 2019 (mise en place de l'ensemble sur 2 ans)

2 OBJECTIFS PRINCIPAUX :

- **PÉRENNISATION DE L'ENISA**
- **MISE EN PLACE D'UN CADRE EUROPÉEN DE CERTIFICATION DE CYBERSECURITE (BASÉ SUR DES SCHÉMAS DE CERTIFICATION AVEC DIFFÉRENTS NIVEAUX D'ASSURANCE)**

Le fonctionnement du CSA : évaluation de conformité & niveaux d'assurance



Les acteurs du CyberSecurtiy Act

- ENISA : Agence de l'union européenne pour la cybersécurité

Nouveau

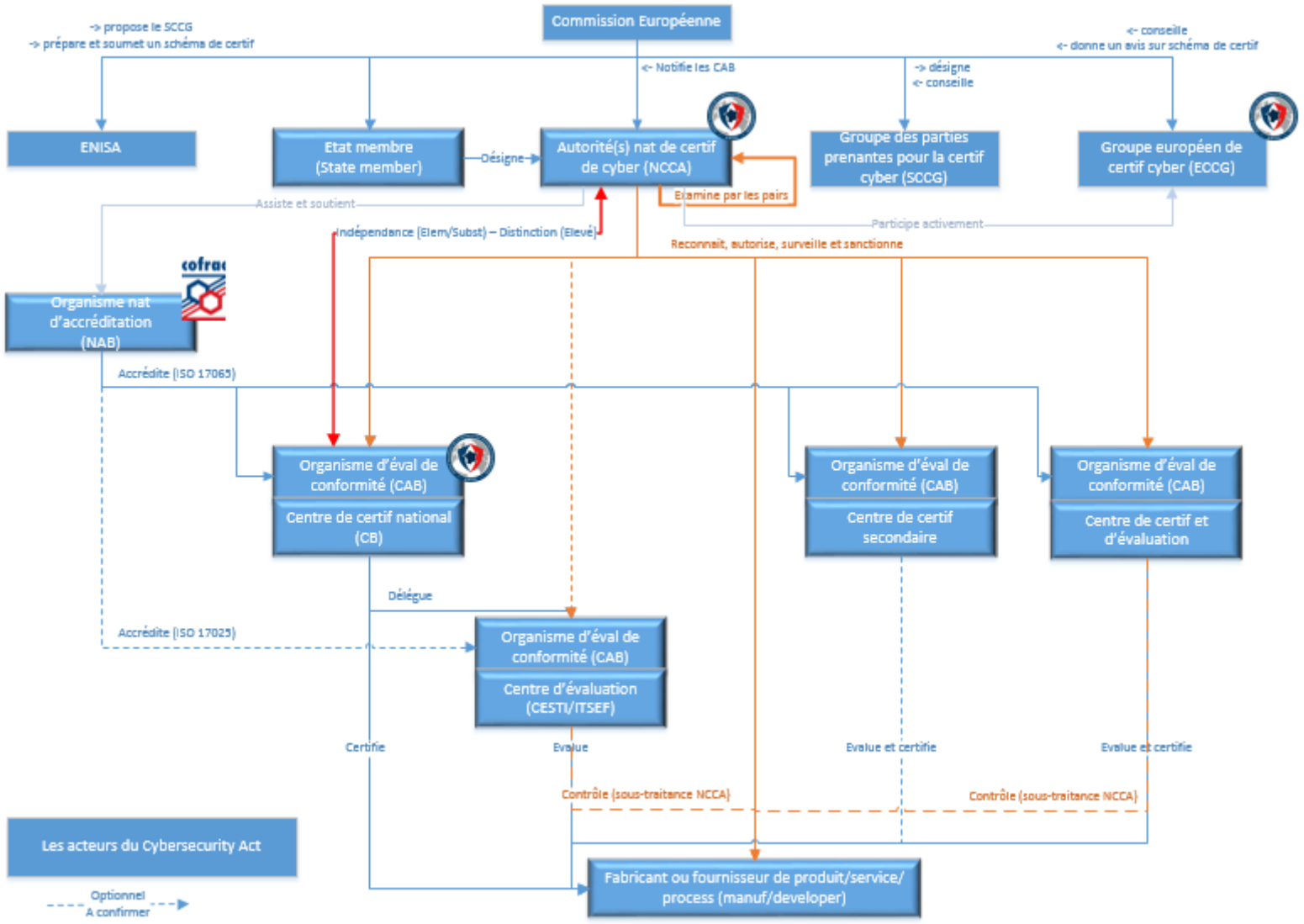
- **SCCG : Groupe des parties prenantes pour la certification de cybersécurité**
- **ECCG : Groupe européen de certification de cybersécurité**
- **NCCA : Autorité nationale de certification de cybersécurité**
- **AhWG : Groupe de travail ad hoc**

- CAB (Conformity Assessment Body) : Organismes d'évaluation de la conformité (National/Public/Privé)
- AB (Accreditation Body) : Organisme d'accréditation
- Fabricant ou du fournisseur de produits TIC (technologies de l'information et des communications), services TIC ou processus TIC

LA CIBLE DU CADRE DE CERTIFICATION :

- **PRODUITS TIC** **(CARTE À PUCE, VOITURE, AUTOMATE, JOUET CONNECTÉ,…)**
- **SERVICES TIC** **(CLOUD, PDIS,…)**
- **PROCESSUS TIC** **(ISO 27001)**

Le fonctionnement du CSA : positionnement de l'ANSSI



Les schémas de certification

- Le contenu d'un schéma de certification (Art. 54 du CSA) :
  - Champ d'application (produits/services/processus)
  - Les niveaux d'assurance visés (Elémentaire/Substantiel/Elevé)
  - Les méthodes d'évaluation
  - Les références aux normes (ou spécifications techniques)
  - Le type d'évaluation (autoévaluation (déclaration de conformité) et/ou certification (certificat))
  - La gestion des certificats et déclaration (maintenance, retrait, renouvellement, durée, …)
  - La gestion des signalements et traitements des vulnérabilités
  - Les éventuelles conditions de reconnaissance mutuelle

SCHÉMA DE CERTIFICATION : PILIER DU CSA POUR LA CERTIFICATION
(MAIS PAS D'OBLIGATION DE CERTIFICATION)

Les schémas de certification

- Développés en fonction de l'URWP (Union Rolling Work Programme)
- Le premier identifié :
  - Transposition du SOG-IS (CC) (Première réunion de l'AhWG1 : 28/11/2019)
- Les suivants :
  - Cloud (suite CSPCert)
  - 5G
  - IOT
  - Industrial Automation Control Systems
  - Véhicules connectés-autonomes / dispositifs médicaux / …
- Premier URWP : juin 2020

OBJECTIF DE LA COMMISSION : DEVELOPER 3 SCHÉMAS PAR AN

Les enjeux du CSA

- Harmonisation au niveau européen
- Possibilité de la dérive de la certification de complaisance (compétitivité de notre écosystème – maintien de la compétitivité)
- Avancement rapide du CSA mais le premier schéma sera opérationnel en juin 2020
- Cadre volontaire à faire adopter par les domaines sectoriels (+ possibilités des actes d'exécution)
- De la souveraineté nationale à l'ouverture européenne (champ géographique et technique)

Conclusion

- Cadre réglementaire en place européen pour
  - Adresser les produits/services/processus des différents domaines sectoriels
  - Elever le niveau de cybersécurité
  - Harmoniser les pratiques au sein de la Communauté européenne
- En basant sur des solutions existantes et le schéma français

Des questions ?