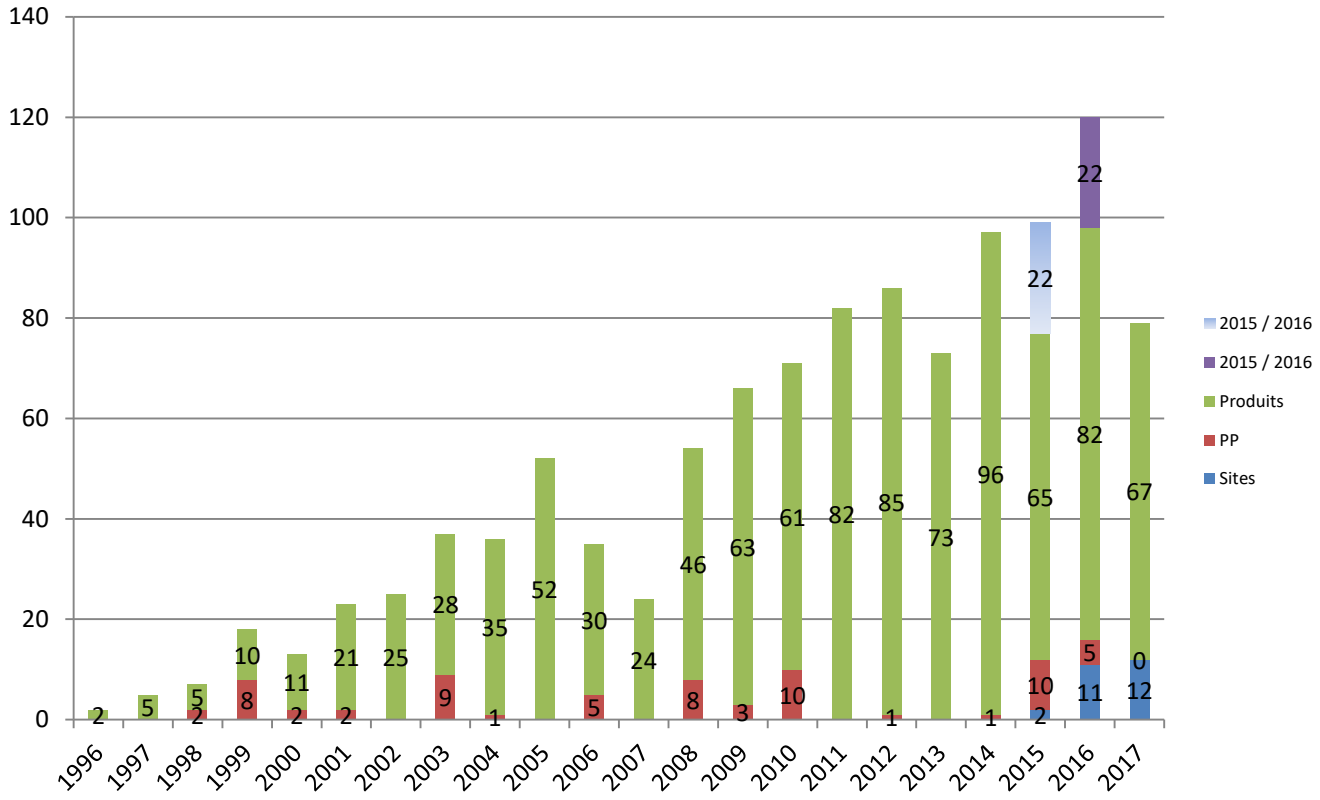
Retours d'expérience - CC

Nombre de certificats émis entre le 01/01/2017 et le 13/12/2017 :
79 à comparer avec 120 en fin d'année 2016 (-34%)

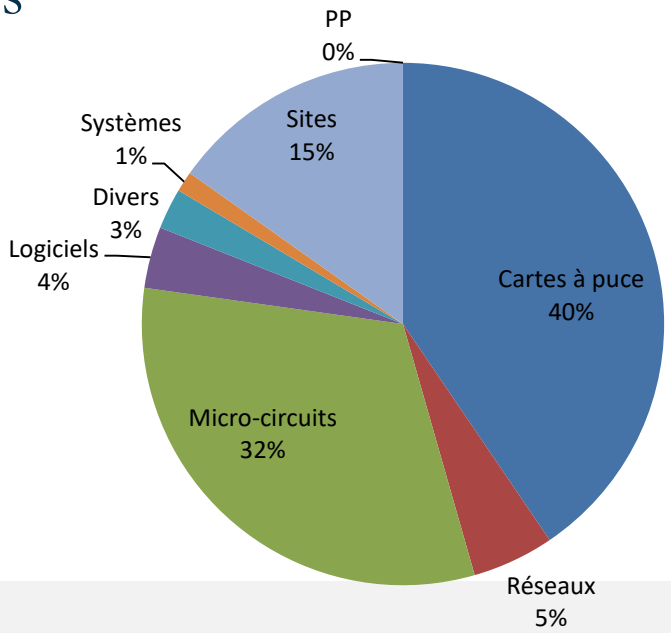


Retours d'expérience - CC

> Produits entrant en qualification

	S1/2016	S2/2016	2016	S1/2017	S2/2017	2017
Nb de produits CC entrant en qualif.	22	21	43	13	3	16
Ratio Qualif / CC	33,3%	38,9%	**35,8%**	34,2%	7,3%	20,3%

> Répartition des certifications



Retours d'expérience - CC

> Délai d'enregistrement des évaluations

	Délais entre la Demande et l'Enregistrement (mois)	
	Moyen	Ecart type
S1/2016	0,84	0,56
S2/2016	1,12	0,66
S1/2017	0,65	0,38
S2/2017	0,80	0,35

> Délai de traitement

	Délais entre la réception du 1er RTE PASS et le certificat (mois)		Délais entre le dernier RTE et le certificat (mois)	
	Moyen	Ecart type	Moyen	Ecart type
S1 2016	3,09	1,33	1,62	0,86
S2 2016	1,81	1,61	0,71	0,57
S1/2017	1,93	1,26	1,48	1,25
S2/2017	0,81	0,82	0,80	0,63

Retours d'expérience - CC

- Nombre de dossiers en cours : 82 alors qu'il était de 86 l'année dernière
- Nombre de produits certifiés entrant en qualification : 20% à comparer aux 36% de 2016
- Nombre de produits en maintenance : 22
- Nombre de produis sous-surveillance : 68

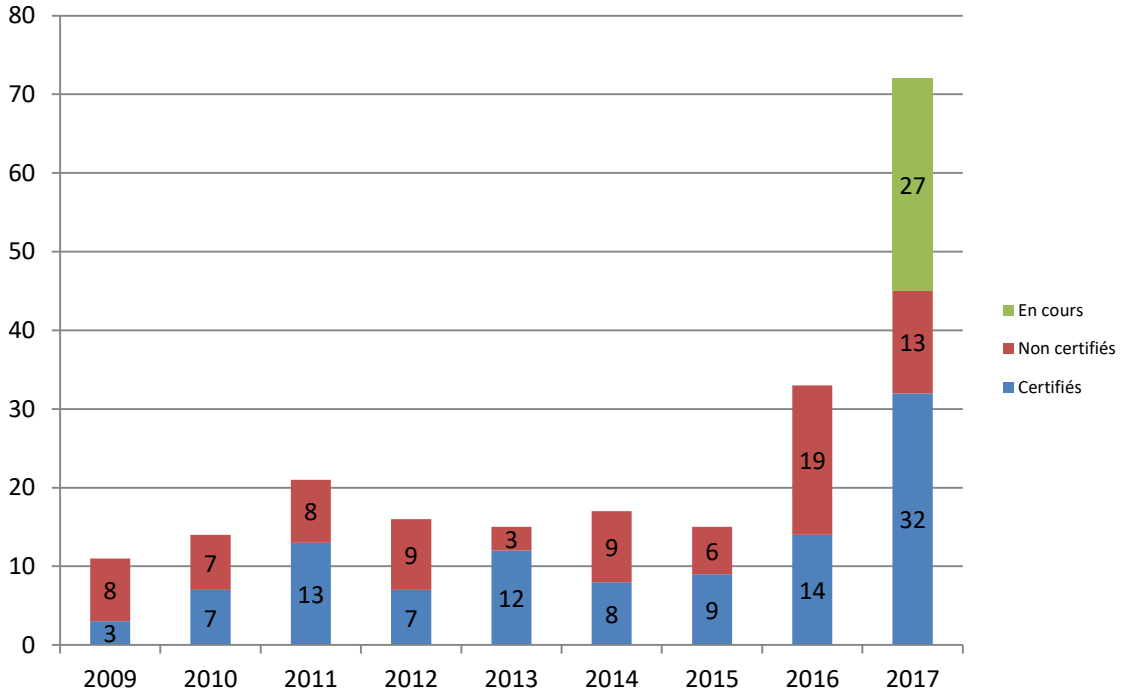
Retours d'expérience - CC

> Conclusion

- Le nombre de certificats émis au premier semestre est en diminution par rapport à la même période de l'année 2016 (-34%)
- Le nombre de dossiers en cours est semblable à celui de 2016
- Les délais d'enregistrement continuent de s'améliorer
- Les délais de traitement sont en voie d'amélioration par rapport à ceux de 2016
- Le pourcentage de produits certifiés entrant en qualification est en diminution par rapport à la même période 2016 (-14%)
- La répartition des certificats par rapport à la même période 2016 montre une forte augmentation de microcircuits (+100%) au détriment des « cartes à puce ». Cette situation a été périodiquement constatée par CCN (alternance années IC / années cartes)
- Pour 2018, la direction a demandé que le ratio entre les nouveaux produits évalués et ceux en réévaluation soit déterminé

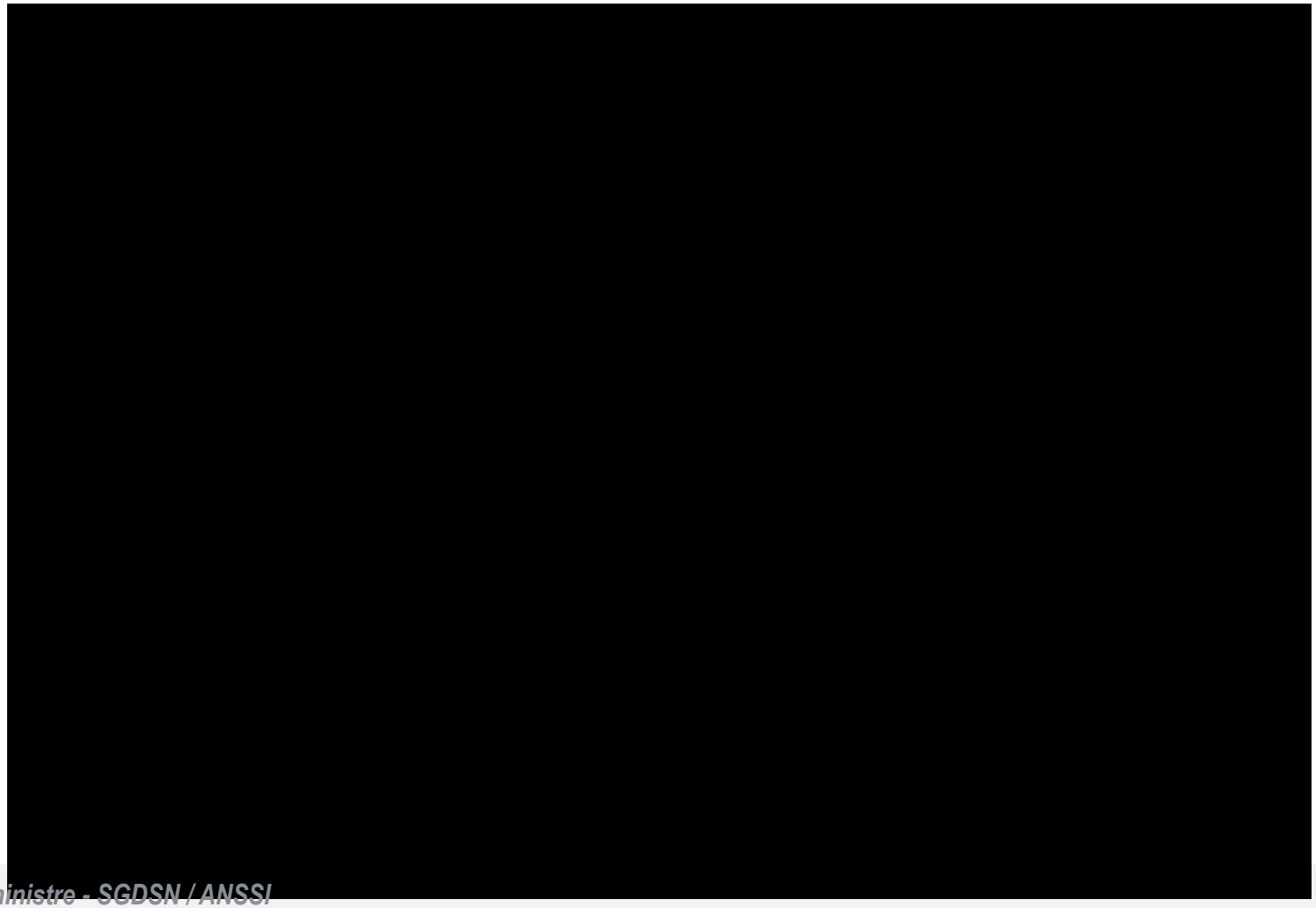
Retours d'expérience - CSPN

> Nombre de dossiers CSPN traités entre 01/01/2017 et le 13/12/2017



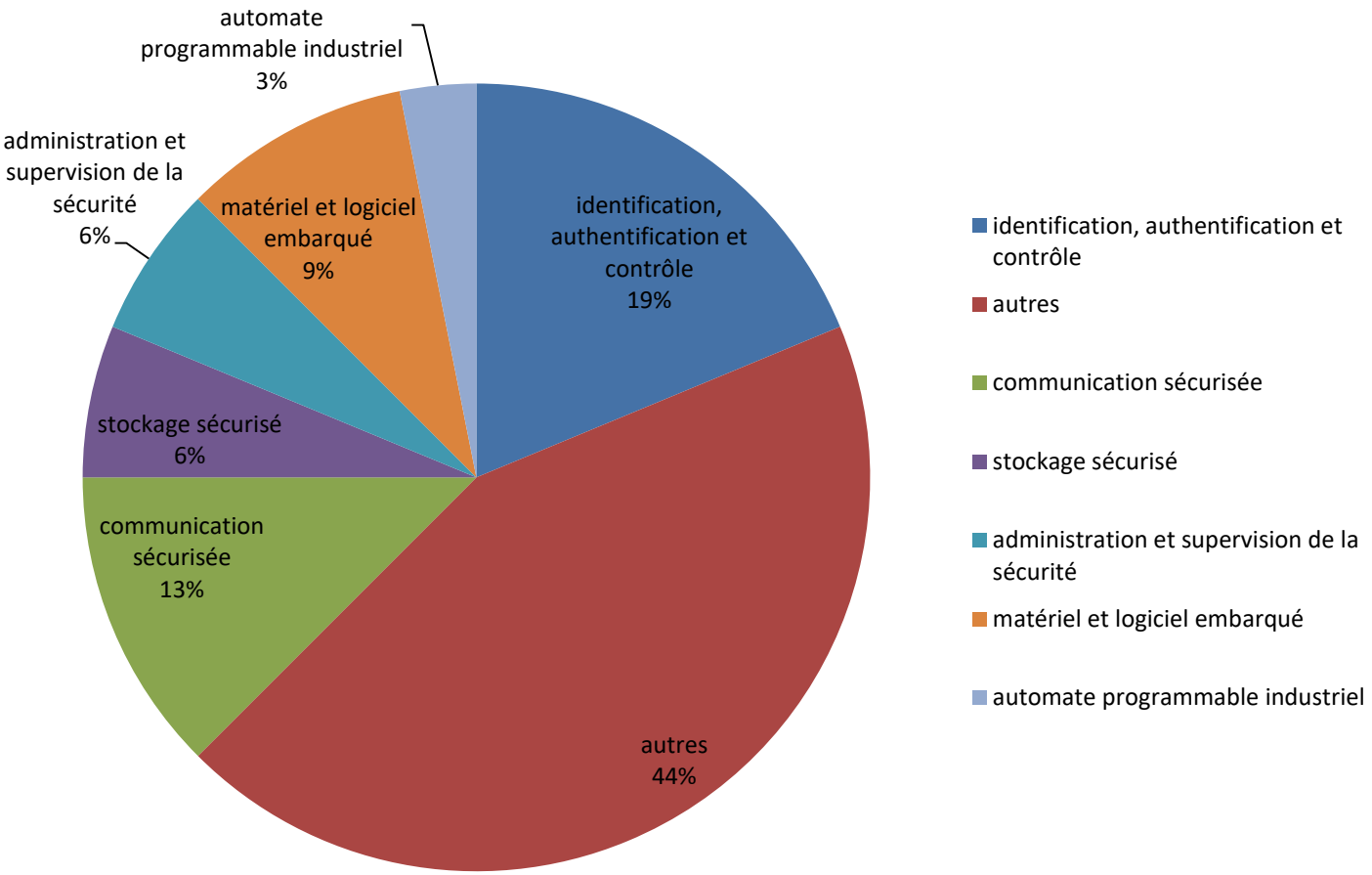
Retours d'expérience - CSPN

Répartition des certificats par donneurs d'ordre



Retours d'expérience - CSPN

Répartition des certificats par type de produit



Retours d'expérience - CSPN

> Délai d'enregistrement :

	Délais entre la Demande et l'Enregistrement (mois)	
	Moyen	Ecart type
S1/2016	0,75	0,73
S2/2016	0,79	0,34
S1/2017	0,75	0,43
S2/2017	1,00	0,54

> Délai de traitement :

	Délais entre le 1er RTE et certificat (mois)	
	Moyenne	Ecart type
S1/2016	1,42	1,77
S2/2016	0,98	0,88
S1/2017	2,57	1,87
S2/2017	4,35	2,57

	Délais entre le dernier RTE et le certificat (mois)	
	Moyen	Ecart type
S1/2017	2,40	1,92
S2/2017	2,71	2,49

Retours d'expérience - CSPN

> Conclusion

- Le nombre de certificats émis depuis le début de l'année 2017 est en forte augmentation par rapport à la même période de l'année 2016 (+128%)
- Les délais d'enregistrement sont stabilisés
- Les délais moyens entre le 1er RTE et la délivrance du certificat sont en forte augmentation dus aux multiples RTE
- Les délais de traitement des derniers RTE à PASS sont à améliorer. A ce jour, ces résultats sont principalement dus à la forte augmentation des dossiers CSPN avec un effectif constant
- Les produits certifiés entrant en qualification sont en très forte diminution par rapport à 2016 (57% en 2016 contre 15% depuis le début de l'année 2017)

[redacted]

Effectifs du centre de certification

Evolutions du référentiel CCN

- Travaux achevés en 2017 :
  - Méthode d'évaluation pour une famille de produits (Note ANSSI-CC-NOTE-21)
  - Procédure d'évaluation de composants d'assurance ALC (évaluation selon les CC du cycle de vie des produits) génériques : ANSSI-CC-SITE-P-02
- Travaux en cours :
  - NOTE14 : interprétation PP0084 (protection technique du composant en sortie de fabrication, chargement sécurisé de la mémoire Flash)
  - Méthodes d'évaluation CSPN pour application mobile

Actualité du schéma

Laboratoires (CESTI) Agréés - CC

Composants électroniques, microélectroniques et logiciels embarqués

Laboratoires (CESTI) Agréés - CC

Logiciels et réseaux

Laboratoires (CESTI) Agréés - CC

Equipements matériels avec boitiers sécurisés

Laboratoires (CESTI) Agréés - CSPN

Logiciels et réseaux

Laboratoires (CESTI) Agréés - CSPN

Matériel et logiciel embarqué

Bilan CESTI

> Un

Accréditation ISO 17065

- L'objectif affiché d'effectuer un premier passage pour une accréditation ISO 17065 avant fin 2017 ne sera pas respecté et ce, pour plusieurs raisons
  - Difficulté de définir le périmètre de l'Organisme de Certification et non CCN seulement
  - Difficulté de réaliser l'analyse de risques
  - Non respect de la norme pour la surveillance (durée de validité des certificats, mise en place de surveillances systématiques)
  - Audit interne 2017 non effectué d'où une nécessité d'effectuer deux audits en 2018
- Nouvel objectif : effectuer un premier passage devant le COFRAC en Q4/2018

Satisfaction clients

> Le formulaire « ANSSI-CC-QUA-F-03 Formulaire Satisfaction Client » a été refondu, il est maintenant systématiquement joint aux différents rapports. Depuis le début de l'année, 84 formulaires ont été envoyés et, seules 10 réponses (12%) ont été retournées à CCN. Parmi ces réponses, il en ressort que :

POINT FORT	POINT FAIBLE
La qualité du rapport de la réunion de démarrage (CC uniquement)	Le manque de communication d'information sur les possibilités de maintenance et surveillance
Le temps de traitement du dossier de demande de maintenance	Le déroulement de la réunion de démarrage (CC uniquement)
L'écoute et la disponibilité du certificateur	La réactivité du certificateur face aux problèmes

Plaintes

Amélioration de l'efficacité du système de management et de ses processus

- Axes d'amélioration pour 2017/2018
  - Améliorer l'encadrement des nouveaux arrivants
  - Apporter les corrections nécessaires dans les documents qualité et en rédiger de nouveaux si nécessaire
  - Améliorer l'information auprès des prospects par la publication d'une brochure concernant la certification [redacted]
  - Etudier la possibilité de publier une brochure sur la maintenance et la surveillance
  - Rédiger une matrice de conformité afin de s'assurer que les audits d'agrément des CESTI couvrent correctement la norme ISO 17020 L'objectif est d'éviter aux CESTI de devoir être accrédités en apportant la preuve qu'ils le sont déjà au travers les audits d'agrément.

Accords de reconnaissance

CCRA

- Participation aux instances de management (CCDB, CCES, CCMC)

- 28 membres

- Pays consommateurs seuls
  - l'Autriche, le Danemark, l'Ethiopie, la Finlande, la Grèce, la Hongrie, Israël, le Pakistan, Singapour, le Qatar

- Pays émetteurs
  - l'Allemagne, l'Australie, le Canada, l'Espagne, les États-Unis, la France, l'Inde, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie

Accords de reconnaissance

- SOG-IS
  - Participation au comité de management (SOG-IS MC) [redacted]
  - Participation au JIL Working Group [redacted]
- 14 membres
- Pays consommateurs seuls
  - Autriche, Finlande, **Pologne, Croatie, Estonie**
  - **Demande officielle du Danemark**
- Pays émetteurs
  - Allemagne (CP+HW), Espagne (CP+HW), France (CP+HW), Italie, Norvège, Pays-Bas (CP+HW), Royaume-Uni (CP+HW), Suède
- Liaisons
  - Japon, Turquie
  - En cours de création : CEN?

Accords de reconnaissance

- CCRA [redacted]
- SOG-IS
  - Participation au SOG-IS *Management Committee* [redacted]
  - Participation au JIL *Working Group* [redacted]
- Principe de validité administrative des certificats et processus de surveillance FR acceptés au niveau du CCRA, SOG-IS devrait suivre

Participation CCN 2017 aux audits CCRA et SOG-IS

Groupes de travail

JHAS- JIWG Hardware Attack Subgroup

- Groupe de travail dédié au domaine « Smartcards and similar devices »

- Objectif : évolution du référentiel d'évaluation des produits de type composant sécurisé et cartes à puce

[redacted]

Groupes de travail

ISCI – International Smartcard Certification Initiative

- Groupe de travail dédié à l'évolution des référentiels d'évaluation SOG-IS hors analyse de vulnérabilité (JHAS, JEDS, etc.)
- Participation CCN [redacted]
- Travaux en cours : évolution de la méthodologie d'audit des sites de développement (MSSR), finalisation et mise en œuvre d'une méthodologie de mutualisation des travaux d'audits de site à l'initiative de l'ANSSI

Groupes de travail

JEDS - JIWG Embedded Devices Subgroup

- Groupe de travail dédié au domaine « Hardware Device with Security Boxes »

- Objectif : création d'un référentiel pour l'évaluation de produits combinant contre-mesures matérielles et logicielles
  - JEDS Minimum Lab Requirements presque terminé
    - ANSSI a travaillé pour ajouter la partie logiciel qui manquait
    - Commentaires de la JIL à prendre en compte avant finalisation
  - Prochain travaux
    - *Attack method*
    - *Attack potential*

Groupes de travail

JRC – ERNCIP (Cybersécurité des systèmes industriels)

- Participation CCN : [redacted]

- Rédaction rapport France
  - Détaille les étapes PP → ST → Evaluation
  - Création de cible de sécurité basée sur PP CSPN Pare-feu
  - Création de plan de test
  - Promotion de la CSPN au niveau européen

- Contributions

[redacted]

Groupes de travail

GlobalPlatform TEE

- Schéma de certification propre mis en place par GP pour les produits respectant les spécifications TEE de GP
- Accord GP – ANSSI : les certificats émis par l'ANSSI sur la base du PP GP TEE sont reconnus par GP comme équivalents à ceux émis dans le cadre de son schéma propre
- Participation de CCN au groupe de travail GP TEE Attack Expert Group
  - Élaboration d'un référentiel pour l'évaluation des TEE
- Echanges techniques avec GP sur les besoins et les évolutions souhaitées en terme de référentiels d'évaluation (TEE et autres types de produits)
  - Peuvent alimenter les schémas « traditionnels » afin de mieux répondre aux attentes des utilisateurs (nouveaux entrants et acteurs historiques)

Cybersecurity Package Européen

COM (2017)477 publiée le 13 septembre 2017

- L'ANSSI accueille positivement l'initiative de la commission visant à étendre et harmoniser la certification de sécurité au sein de l'UE
- L'ANSSI est favorable à ce que l'ENISA se voit confier un rôle de soutien et secrétariat dans la gestion du cadre européen de certification et la définition des référentiels d'évaluation
- L'ANSSI est favorable à l'intégration d'acteurs privés pour les premiers niveaux de certification afin de permettre le passage à l'échelle
- Mais la proposition de la CE pêche par un certain nombre de dispositions malvenues ou manquantes

Cybersecurity Package Européen

En l'état, la proposition de règlement

- Transfère la prérogative de la certification de sécurité à des organismes privés quel que soit le niveau
  - Les acteurs de la certification de conformité ne disposent pas de la compétence et de l'expérience de la certification de sécurité
- Autorise le cumul du rôle d'évaluateur et de certificateur
  - Disparition du principe de certification « tierce partie »
- Ne prévoit qu'une analyse de la conformité des produits
  - Ignore l'agrément des laboratoires par une autorité compétente au profit de la seule accréditation 17025 qui ne permet par l'évaluation de la compétence technique des évaluateurs

Cybersecurity Package Européen

En l'état, la proposition de règlement

- N'intègre pas de dispositif de *Peer Review* (en vigueur au sein du CCRA et SOG-IS) qui permet de construire la confiance dans la compétence des CB à émettre des certificats à haut niveau
- Ne fait pas mention des critères et référentiels d'évaluation existants et servant de base aux accords signés par l'ANSSI (CC et *supporting documents*)
  - En l'état le cadre proposé par la commission n'est pas compatible avec les accords de reconnaissance existants
- Fait fi de l'existant et ne prévoit pas de plan de transition

Cybersecurity Package Européen

Position FR

- Contribution CCN à la construction de la position FR
  - Position « publique » sur site de l'ANSSI – 20 novembre
  - Position détaillée disponible
- Position en ligne avec
  - Acteurs privés (position de l'ACN et Eurosmart)
  - Sénat, voir avis n°79 du 9 novembre 2017 (concentre ses critiques sur la subsidiarité)
  - BSI
- L'ANSSI cherche à faire valoir sa position
  - Dans le cadre des cPPP (ECSO)
  - Directement en tant qu'Etat Membre (négociations CE/Parlement/EMs)

Cybersecurity Package Européen

Etat des négociations

Cybersecurity Package Européen

Lien avec SOG-IS

- FR soutient avec DE l'extension du SOG-IS à tous les états membres de l'UE
  - Travail d'influence entamé il y a déjà plusieurs mois auprès des autres EM, accélération suite à la publication de la proposition de règlement
  - [redacted]
- Demande au Comité Directeur de la Certification son accord tacite pour l'adhésion automatique de nouveaux EM

Normalisation ISO

- Mise à jour des Critères communs (ISO 15408 et ISO 18045)
- Participant CCN : [redacted] coéditeur de la partie 1 de l'ISO 15408, éditeur du TR 22216
- Le nouveau standard entérine le divorce des pratiques
  - iTC et collaborative PP, pas de tests de robustesse (principalement UK/US)
  - Approche « traditionnelle » s'appuyant sur les tests de robustesse (principalement Europe)
- Inclut les modifications des CC3.1r5, mais ne s'y limite pas
  - Divergence avec la version de référence utilisée au sein du CCRA

[redacted]

Evaluation de la cryptographie

Point sur les travaux au sein du SOG-IS

- Travaux engagés en 2014 à l'initiative de plusieurs membres dont la France

- Groupe de travail mené par l'ANSSI
  - Un *draft* de référentiel pour les mécanismes approuvés a été publié Q4 2016
  - Un guide d'intégration de la crypto dans les cibles de sécurité CC a été rédigé (Q2 2017)
  - Un *draft* de méthodologie CC (intégration des travaux dans la méthodologie générique – CEM) a été rédigé et soumis aux groupes de travail de la JIL pour commentaires (Q2 2017)
  - L'ANSSI est en charge de la rédaction de la méthodologie d'évaluation crypto
    - Travaux suspendus en attendant la finalisation d'un marché pour une prestation de soutien par un CESTI agréé
    - Marché notifié en décembre 2017, les travaux devraient reprendre début Q1 2018

Points divers

[redacted]

Initiatives autour de la CSPN

- CCN a échangé/accompagné les schémas DE et NL sur la création d'un schéma national similaire à la CSPN
  - NL : en place depuis un an environ
  - DE : phase pilote en 2017, mise en œuvre prévue début 2018 et objectif affiché d'une reconnaissance mutuelle FR-DE

[redacted]

Relations avec les potentiels nouveaux acteurs privés

Suivi des produits qualifiés et surveillance

- Mise en place au niveau BQA d'un outil de suivi des produits qualifiés, impliquant les CESTI ayant réalisés les évaluations

- Participation CCN

Rappel sur les missions du comité

Article 15 du décret 20002-535:

Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :

a) De formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;

b) D'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;

c) D'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;

d) D'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.

La mission prévue au c ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

+ rôle dans dispositif Préservation de l'impartialité

Fonctionnement du comité

Fonctionnement régi par le règlement intérieur du comité directeur de la certification (https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-reg-01-reglement-interieur-comdir-v2.0.pdf)

Création 08/2019

Mis à jour 05/2020 pour simplifier son fonctionnement suite à requête de membres du comité

Comité non réuni depuis 12/2017

- Décision de réunir le comité en début d'année plutôt qu'en fin d'année pour présenter le bilan de l'année précédente => comité 2018 était prévu donc début 2019
- Comité 2019 non réuni (CR de réunion de direction qualité diffusé 02/2019)
- Comité 2020 non réuni : réunion prévue le 20/03/20, annulée car crise COVID1

Bilan 2018/2019/2020 à faire ici

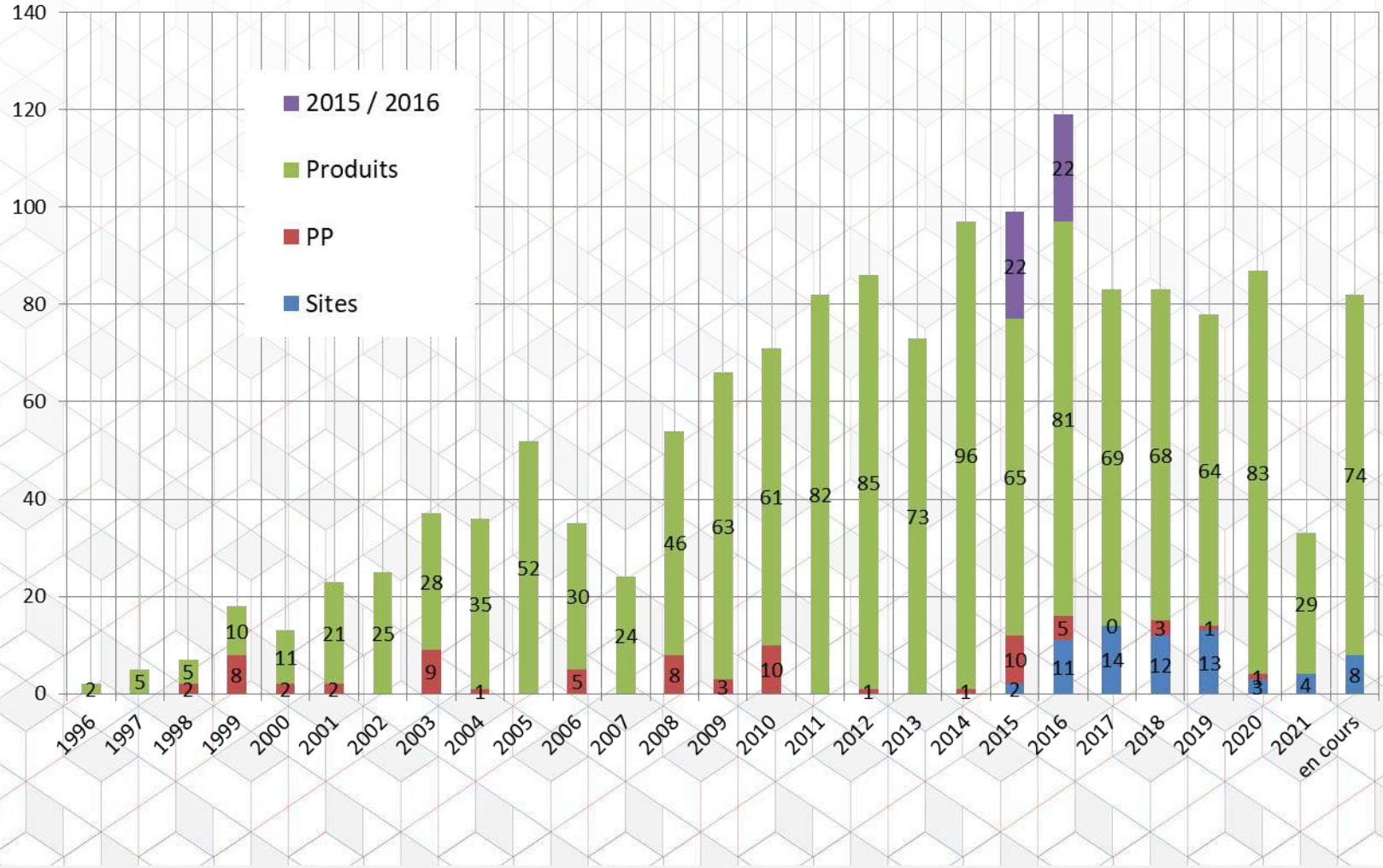
Activité du Centre de certification

Positionnement du schéma FR vis-à-vis de ces homologues (certificats CC en cours de validité)

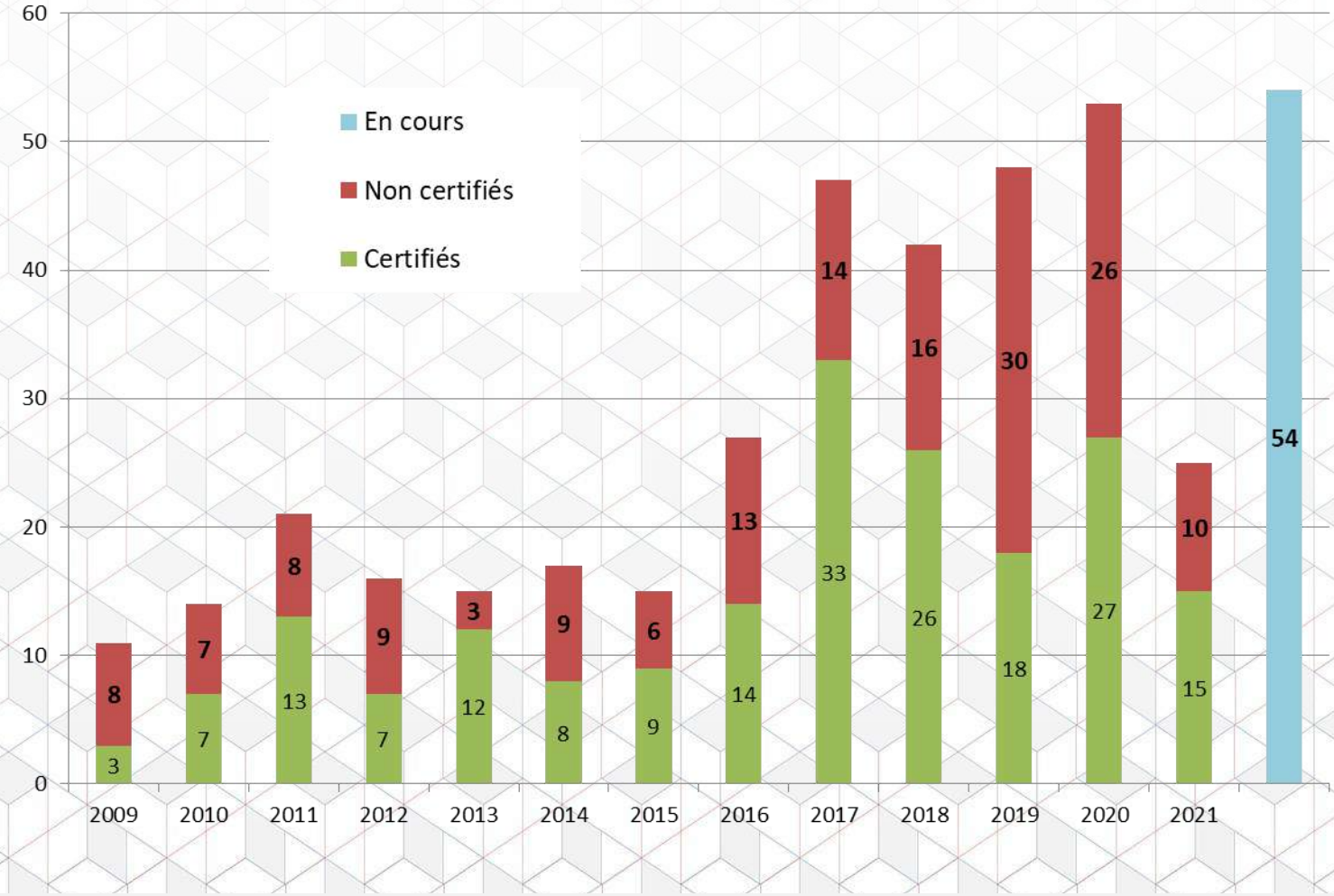
Certified Products by Scheme and Assurance Level																			
Scheme	**B**	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**M**	**N**	**S**	**Total**
Australia	0	0	0	4	6	0	0	0	0	0	0	0	0	0	0	0	21	0	31
Canada	0	2	0	6	62	0	0	0	1	0	0	0	0	0	0	0	65	0	136
Germany	2	2	0	16	6	10	18	8	90	1	47	0	51	0	1	0	5	0	257
Spain	0	2	0	8	20	3	6	2	25	0	15	0	1	0	0	0	10	0	92
France	0	0	0	0	2	0	15	2	56	6	186	0	25	2	0	0	0	0	294
India	0	2	0	6	1	3	0	0	0	0	0	0	0	0	0	0	1	0	13
Italy	0	4	3	2	5	0	0	1	32	1	0	0	0	0	0	0	2	0	50
Japan	0	0	0	3	84	0	7	0	2	0	1	0	0	0	0	0	50	0	147
Republic of Korea	0	7	0	3	3	0	0	0	1	0	5	0	0	0	0	0	25	0	44
Malaysia	0	1	0	24	18	0	3	0	3	0	0	0	0	0	0	0	0	0	49
Netherlands	0	0	0	9	5	1	6	1	46	0	38	0	22	0	1	0	1	0	130
Norway	0	1	0	1	16	2	5	8	13	1	9	0	0	0	0	0	0	0	56
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	7	0	22	9	16	8	7	3	3	0	0	0	0	0	0	15	0	90
Singapore	0	0	0	3	0	0	0	0	4	0	0	0	0	0	0	0	0	0	7
Turkey	0	0	0	13	1	4	0	1	19	0	1	0	0	0	0	0	0	0	39
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	126	0	126
Totals:	**2**	**28**	**3**	**120**	**238**	**39**	**68**	**30**	**295**	**12**	**302**	**0**	**99**	**2**	**2**	**0**	**321**	**0**	**1570**

NB les rapports de surveillance FR ne sont pas inclus (pour l'instant), contrairement aux reassessments allemands et néerlandais

Nombre de certificats CC délivrés par année



Nombre de projets CSPN gérés par année



Effectifs CCN

- CCN sera composé de 10 personnes (9,5 ETP) au 09/2021
  - 2018 : 2 arrivées de certificateurs
  - 2019: départ de l'assistant CCN, remplacé la même année
  - 2020: 2 départs (1 certificateur CC HW et le chef de bureau adjoint, également certificateur CC/CSPN SW et HW)
  - 2021:
    - 2 départs à l'été 2021 (le responsable qualité et son suppléant, également certificateurs CC SW et HW)
    - 1 nouveau certificateur arrive en 08/2021 (priorité formation CSPN SW, profil pouvant intervenir en HW et HW _DEV)
    - 1 gestionnaire de planning arrive en 09/2021
- Effectif de certificateurs en décroissance => besoin de renforts
- Les délais de certification seront nécessairement impactés…

Organisation CCN

- Nouvelle organisation prévue
  - un nouveau poste de soutien créé: gestionnaire de plannings
    - NB tâche de gestion requise par l'accréditation
    - Objectif1 : permettre d'identifier le certificateur qui pourrait traiter un projet dans les meilleurs délais
    - Objectif2 : mieux connaître la charge des certificateurs
    - assurera aussi des tâches de soutien aux certificateurs
  - une nouvelle fiche de poste publiée de responsable qualité
    - recrutement externe, contrairement à la pratique usuelle de CCN
    - poste non encore pourvu

Suivi de l’agrément des CESTI

Impact COVID

Impacts directs et indirects sur les audits d'agrément des CESTI

Impacts directs

- Des audits non réalisés avant la date d'échéance des décisions d'agrément pour cause de restriction des déplacements et mesures de distanciation imposées ;

-Plusieurs dérogations sollicitées et acceptées pour

- soit étendre les décisions d'agrément de quelques mois sans audit avec planification de nouveaux audits en 2021

- soit étendre les décisions d'1 an sur la base d'audits partiels, avec suivi renforcé via les évaluations

Impact indirect

- Problème de bande passante: trop d'audits à faire sur un période courte

[redacted]

Agréments Logiciels et équipements réseaux » (dit Soft): 1/3

Nom	CC	CSPN	Date fin agrément	Audit

Agréments Logiciels et équipements réseaux » (dit Soft): 2/3

Nom	CC	CSPN	Date fin agrément	Audit

Agréments Logiciels et équipements réseaux » (dit Soft): 3/3

Nom	CC	CSPN	Date fin agrément	Audit

Agréments « Composants électroniques, microélectroniques et logiciels embarqués » (dit Hard)

Nom	CC	CSPN	Date fin agrément	Audit

Agréments « Equipements matériels avec boîtiers sécurisés» (dit HW devices)

Nom	CC	CSPN	Date fin agrément	Audit

Qualité et accréditation du centre

Accréditation ISO 17065

- Le centre de certification doit être accrédité ISO 17065 pour se mettre en conformité au CyberSecurityAct / schéma EUCC
- Projet bloqué par pb contractuel/juridique avec le COFRAC, *a priori* résolu (Convention non encore signée…)
- Dérogation / politique de sécurité à prononcer pour les auditeurs COFRAC
- Nouvelle version du Manuel Qualité à venir cet été
- Diffusion prochaine, pour validation, de l'analyse des risques sur l'impartialité du centre
- Précisions sur les responsabilités à formaliser
  - supervision de la situation financière de l'OC
  - fourniture des ressources appropriées
  - décision de suspension et retrait de certificat

Traitement des écarts relevés lors des audits internes (réalisés selon 17065 depuis 2016)

		Nb d'écarts identifiés	Statut des écarts		
			Ouverts (traitement non identifié)	En cours de traitement	abandonné
Sources	Audit interne du centre de certification 2015	31	0	2	1
	Audit interne du centre de certification 2016 - ONX	30	0	3	2
	Audit interne du centre de certification 2018 - LNE	35	0	5	0
	Audit interne du centre de certification 2019 - LNE	6	0	1	0
	Audit interne du centre de certification 2020 - LNE (réalisé début 2021)	10	0	10	0
TOTAL		**116**	**0**	**21**	**3**

Qualité/ travaux réalisés

Évolution pratique de certif

Autres màj Qualité

> **Beaucoup de màj pour répondre aux écarts d'audits internes**

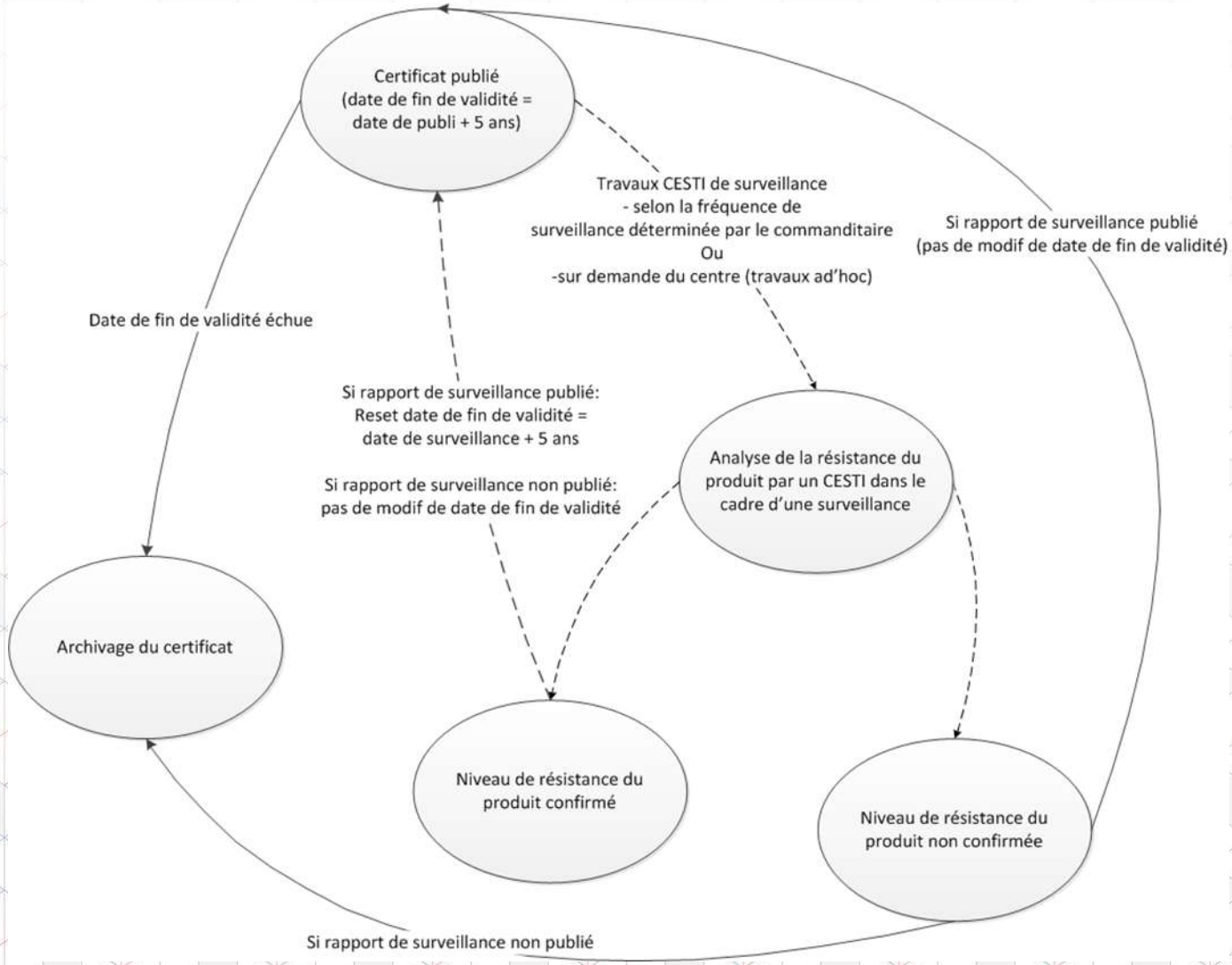
ANSSI-CSPN-CER-P-01 Certification_de_securite_de_premier_niveau_v3.0	16/04/2021 14:06
ANSSI-CSPN-CER-P-02 Criteres_pour_evaluation_en_vue_d'une_CSPN_v4.0	13/04/2021 15:36
ANSSI-CC-PER-P-01 Recrutement et qualification du personnel_v6.1	16/03/2021 15:22
ANSSI-CC-CRY-P-01 Modalités pour la réalisation des analyses cryptographiques	08/03/2021 14:49
ANSSI-CC-SECU-P-01 Gestion de la confidentialité à CCN_v3.0	29/01/2021 17:44
ANSSI-CC-MAI-P-01 Continuité de l'assurance_v4.2	29/01/2021 17:39
ANSSI-CC-MAR-P-02 Utilisation des logotypes CCRA et SOGIS_v2	29/01/2021 17:38
ANSSI-CC-AGR-P-01 Agrément des centres d'évaluation_v5.1	29/01/2021 17:36
ANSSI-CC-MOD-P-01 Modification des exigences de certification v2.3	29/01/2021 17:35
ANSSI-CC-QUA-P-03 Audits internes_v3.3	06/01/2021 15:23
ANSSI-CC-CER-P-01 Certification de produits_v4.0	27/11/2020 15:28
ANSSI-CC-SUR-P-01 Surveillance des produits certifiés_v5.0	27/11/2020 15:25
ANSSI-CC-DOC-P-01 Document système qualite_v4.1	13/01/2020 13:08
ANSSI-CC-ANO-P-01 Traitement des anomalies_v5.1	13/01/2020 13:03
ANSSI-CC-QUA-P-01 Revues de direction_v3.0	24/10/2018 10:29

> **Plusieurs màj du Manuel Qualité (2 en 2019, 1 en 2020 et 2021)**

Validité des certificats CC

- Mise en place de la validité des certificats CC: 5 ans à partir de la dernière analyse de vulnérabilités
  - MàJ procédure « Certification Critères Communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les PP » :
    - définition de la validité initiale
    - retrait en cas d'identification de vulnérabilité
  - MàJ procédure « Surveillance des produits certifiés »
    - capacité à étendre la validité si surveillance confirme le niveau de résistance du produit et est publiée
  - Mise en place page web d'archive des certificats CC

Cycle de vie des certificats CC



Qualité/ travaux réalisés

Evolutions des méthodologies d'évaluation

Evolution du référentiel d'évaluation CC/méthodologies

- Prise en compte des outils dans les évaluations logicielles, v2.0, 06/09/2018
- Cotation de l'utilisation d'*open samples/samples with known secrets*, v1.0, 29/11/2019
- Décision sur la sécurité algorithmique résiduelle («*remaining strength* »), v1.0, 30/11/2019
- Modalités pour la réalisation des analyses cryptographiques et des évaluations de générateurs de nombre aléatoires, v4.1, 21/01/2021
- Evaluations de générateurs d'alea selon AIS20/31 dans le schéma français, v1.0, 08/03/2021
- Visite de l'environnement de développement, v6.0, 29/04/2021

Evolution du référentiel d'évaluation CSPN/ méthodologies

- Méthodologie d'évaluation en vue d'une CSPN - contenu et structure du RTE, v3.0, 06/09/2018

- Critères pour l'évaluation en vue d'une CSPN , v4.0, 28/06/2020 (prise en compte des composants tiers ou librairies obsolètes)

Evolution du référentiel d'évaluation CSPN/méthodologies

- **Méthodologie pour l'évaluation de systèmes de contrôle d'accés physique en vue d'une CSPN, v1.0 , 07/07/2020**
- **Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, v1.0, 02/03/2021**
- **Méthodologie pour l'évaluation d'applications mobiles, v1.0, publication à venir**

Qualité/ travaux prévus

Méthode de réduction de portée d'un certificat (1/3)

- **Objectif**
  - **Permettre de traiter les attaques qui impactent la sécurité d'une partie des fonctions du produit sans en affecter d'autres**
  - **Sans imposer coût et délai d'une réévaluation complète (i.e. sans mise à jour AVA et ni ALC)**
  - **Permettre de répondre dans le temps imparti aux traitements des vulnérabilités (3 mois actuellement, 1 mois dans EUCC)**

Méthode de réduction de portée d'un certificat (2/3)

- Nouvelle démarche d'évaluation permettant de réduire ou restreindre la portée d'un certificat précédemment émis
  - évaluation partielle d'un produit déjà évalué (non modifié) où n'est considéré que l'analyse de l'impact de la réduction de portée fonctionnelle (i.e. même produit mais TOE réduite) sans mise à jour AVA
- Résultats :
  - nouveau rapport de certification v2 qui annule et remplace le précédent
  - certificat non mis à jour : date de validité initiale inchangée

Méthode de réduction de portée d'un certificat (3/3)

- Consultations:
  - Consultation CESTI en cours
  - Présentation aux homologues faites, accord pour apposition marque de reconnaissance SOG-IS
  - Développeurs présentent dès à présent la démarche à ISCI
- NB Démarche prévue dans le cadre du CSA, bien que méthodo non disponible
- Objectif calendaire FR : mise en place pour l'automne 2021

Abandon démarche actuelle de surveillance (1/2)

- Difficultés rencontrées
  - La démarche étant optionnelle, pb vis-à-vis des exigences d'accréditation 17065
  - Problème procéduraux
    - Interaction entre maintenance et surveillance (la surveillance de produit maintenu peut conduire à la mise à jour du nom du produit surveillé)
    - Process d'enregistrement sans validation des charges d'évaluation

Abandon démarche actuelle de surveillance (2/2)

- Proposition : abandon partiel et progressif de cette spécificité FR au profit d'un processus de réévaluation mineure (travaux ASE, AGD et AVA)
  - partiel: pour permettre de continuer à pouvoir établir des résultats négatifs , niveau dégradé (besoin gestionnaire de risques type BQA et GIE-CB)
  - Progressif: pour permettre de faire valoir les travaux déjà entrepris (validité étendue)
- Les CESTI et développeurs récurrents concernés en cours de consultation pour évaluer l'impact de cette évolutions
- Objectifs: mise en œuvre en 2022

CSPN

- Introduire la validité des certificats CSPN fixée à 3 ans
- Envisager la définition d'un domaine CSPN *HW device*
  - Rextex en cours suite au challenge 2019 WOOKEY qui a permis d'évaluer les spécificités du domaine / compétences CESTI attendues

Analyse de vulnérabilités logiciel

- Volonté à long terme de disposer d'un référentiel opposable en évaluation logicielle à la manière de ce qui existe en matériel
- Plusieurs sujets explorés en parallèle
  - Attendues de l'analyse de code (sujet prioritaire, en partenariat avec GE)
  - Analyse de l'exploitabilité/Analyse du durcissement et de la défense en profondeur
  - Analyse documentaire pour l'analyse de surface d'attaque …

Autres travaux

- **Gestion des vulnérabilités post-certification : travaux en cours en partenariat avec SDO et le CERT prenant en compte le retex des évènements récents**

Évolution politique de sécurité à envisager

- Objectif:
  - Prise en compte évolutions IGI1300
  - prise en compte de la flexibilité offerte par le télétravail
- Contraintes
  - des développeurs sont attachés à la politique de sécurité FR actuelle (critère de sélection du schéma)
  - homogénéité politiques de sécurité CESTI et CCN
  - code source prochainement à disposition de tous les CESTI CC suite à la màj du niveau requis en QS
- Opportunité
  - Volonté des développeurs et CESTI de définir une modalité de télé-travail

Cyber Security Act (CSA)

- Principaux impacts
  - Une entité de supervision des activités de CCN doit être mise en place; sa création pourrait impacter l'organisation du Comité directeur de la certification
  - CCN ne gérera plus toute l'échelle des évaluations CC. Le schéma EUCC considère 2 niveaux
    - *Substantial* : évaluations < VAN.3; gérées pas des CB privés
    - *High* : évaluations >= VAN.3; gérées pas CCN

    => peu d'impact sur les activités de CCN : env. 10 certificats < VAN.3 émis les 10 dernières années

Evolutions prévues

Cyber Security Act (CSA)

- Principaux impacts
  - Les processus de VPA CCRA et SOG-IS remplacés par un processus de *peer-assessment* moins contraignant; pourrait favoriser le « *certificate shopping* »
  - Abandon du schéma national à clarifier
    - Capacité à suivre et à éditer des certificats non publics ou non conformes aux particularités du CSA EUCC/CC
  - Capacité à disposer d'interprétations nationales à clarifier; actuellement un facteur différenciant du CCN
  - Certificat à produire en EN

Activités à l'international

Validité des certificats

- **Influence FR pour mettre en place la validité des certificats et que soit prise en compte la démarche de surveillance de produits (spécifique FR) à l'international**
  - **Démarche acceptée par le SOG-IS en 2019**
  - **Convergence des approches SOG-IS et CCRA (d'ici l'été 2021 à priori)**
  - **Approche reprise par le schéma EUCC du CSA**

CB allemand

- **Mise en place d'échanges mensuels avec l'homologue allemand pour traiter sujets d'intérêt commun**
  - **Coopération réussie sur l'usage des méthode formelle en éval CC (position commune intégrée à l'ISO)**
  - **Travaux en cours sur analyse de code**
- **Reconnaissance bilatérale GE/FR des certificats CSPN/BSZ**
  - **En cours de formalisation au niveau technique**
  - **Reconnaissance basée sur échanges techniques GE/FR**
  - **Objectif: texte à officialiser d'ici fin 2021**
  - **À terme (2 ans après init) pourrait être étendue à d'autres CB et potentiellement s'appuyer sur un processus de VPA comme en CC**

Travaux de normalisation

- CCN participe aux standard ISO (SC27 WG3) et CEN/CENELEC (JTC13 WG3) en tant qu'expert et éditeur
- Processus de patch management permettant prise en compte des correctifs pour màj des certificats précédemment émis
  - objectif CCN: se préparer au plus tôt à l'avenir de la certification
- Normalisation CSPN (FITCEM)
  - objectif CCN : pérenniser la démarche FR
- Prochaines versions des CC:
  - objectif CCN : simplification des critères d'évaluation de la conformité pour qu'ils soient plus clairement orientés construction de l'analyse de l'efficacité

Cybersecurity Act (CSA)

- **Participation aux travaux de préfiguration du schéma CC: EUCC**
- **Point d'attention: processus de transition entre certificats SOG-IS et EUCC, la position FR au niveau international ne doit pas être dégradée et une continuité de services doit être assurée pour les usagers**

Participation à des GT

- SOG-IS crypto
- JIWG et sous-groupes
  - JHAS
  - JEDS
  - ISCI WG1

Productions prises en compte par le CSA EUCC

- GP /Security expert group (TEE)

[redacted]

1. RAPPEL SUR LES MISSIONS DU COMITÉ

Rappel sur les missions du comité

Article 15 du décret 2002-535

Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :

- de formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;
- d'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;
- d'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;
- d'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.

La mission prévue ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

Rappel sur les missions du comité

Fonctionnement du comité

Fonctionnement régi par le règlement intérieur du comité directeur de la certification (https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-reg-01-reglement-interieur-comdir-v2.0.pdf)

- création 08/2019
- mis à jour 05/2020 pour simplifier son fonctionnement suite à requête de membres du comité
- dernière réunion du ComDir en juin 2021

2. ACTIVITÉS DU CENTRE DE CERTIFICATION

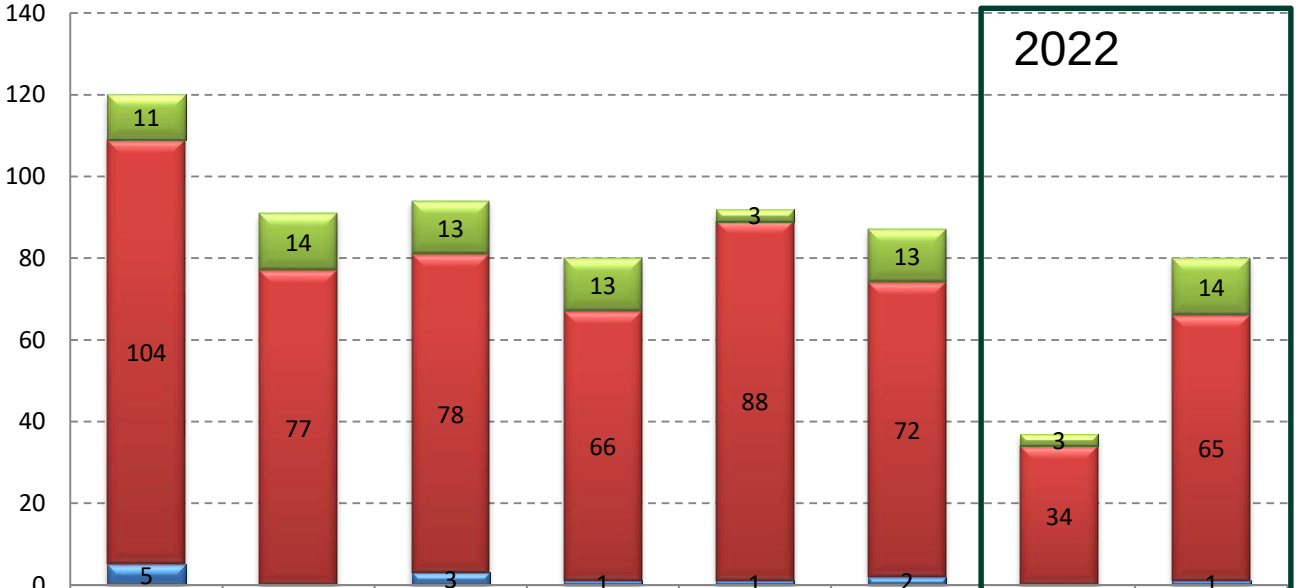
Positionnement du schéma FR vis-à-vis de ses homologues

Certificats CC en cours de validité (au 05/07/2022)

Certified Products by Scheme and Assurance Level																			
Scheme	**B**	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**M**	**N**	**S**	**Total**
Australia	0	0	0	4	6	0	0	0	0	0	0	0	0	0	0	0	15	0	25
Canada	1	2	0	3	36	0	0	0	4	0	0	0	0	0	0	0	68	0	114
Germany	4	2	0	21	10	12	32	8	105	1	40	0	65	0	1	0	5	0	306
Spain	0	2	0	8	22	3	8	3	28	0	17	0	1	0	0	0	11	0	103
France	1	0	0	0	3	0	11	3	61	6	179	0	32	2	0	0	0	0	298
India	0	2	0	8	1	2	0	0	0	0	0	0	0	0	0	0	1	0	14
Italy	0	5	4	2	10	0	0	1	37	1	0	0	0	0	0	0	12	0	72
Japan	4	0	0	6	72	0	0	0	2	0	1	0	0	0	0	0	57	0	142
Republic of Korea	0	6	0	3	2	0	0	0	2	0	4	0	0	0	0	0	28	0	45
Malaysia	0	1	0	28	21	0	3	0	3	0	0	0	0	0	0	0	0	0	56
Netherlands	0	0	0	6	9	1	7	1	59	1	42	0	23	0	1	0	0	0	150
Norway	0	1	0	1	16	2	5	8	13	1	9	0	0	0	0	0	0	0	56
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	8	7	0	28	9	16	13	8	5	3	0	0	0	0	0	0	18	0	115
Singapore	0	1	0	3	2	0	0	0	7	0	0	0	0	0	0	0	0	0	13
Turkey	0	0	0	3	1	1	0	0	12	0	1	0	0	0	0	0	0	0	18
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	141	0	141
Totals:	**18**	**29**	**4**	**124**	**220**	**37**	**79**	**32**	**338**	**13**	**293**	**0**	**121**	**2**	**2**	**0**	**356**	**0**	**1669**

Nombre de certificats CC délivrés par année

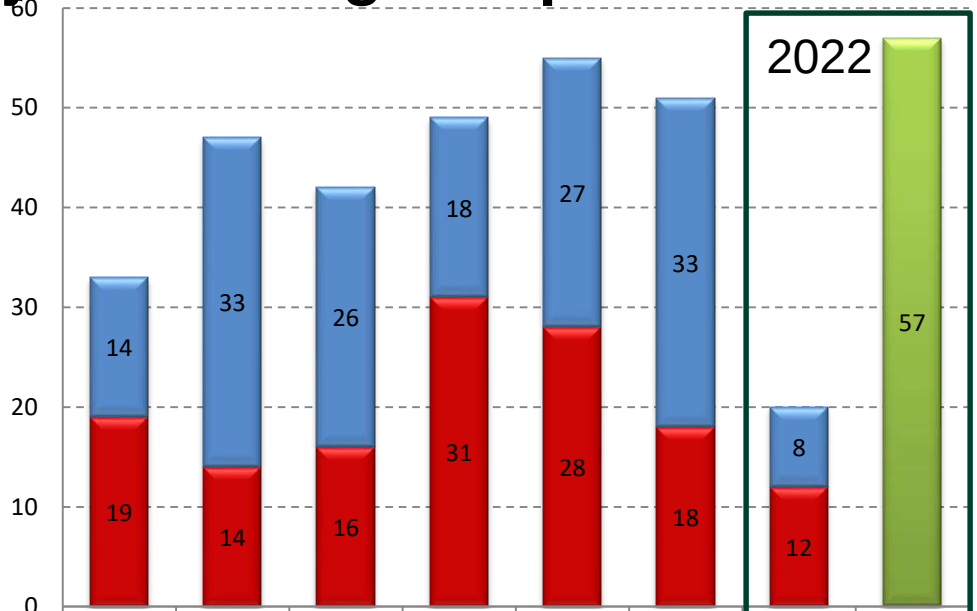
Au 05/07/2022



	2016	2017	2018	2019	2020	2021	2022	En cours
Sites	11	14	13	13	3	13	3	14
Produits	104	77	78	66	88	72	34	65
PP	5		3	1	1	2		1

Nombre de projets CSPN gérés par année

Au 05/07/2022



	2016	2017	2018	2019	2020	2021	2022	En cours
En cours								57
Certifié	14	33	26	18	27	33	8	
Lettre clôture	19	14	16	31	28	18	12	

Centre de certification national

Effectifs

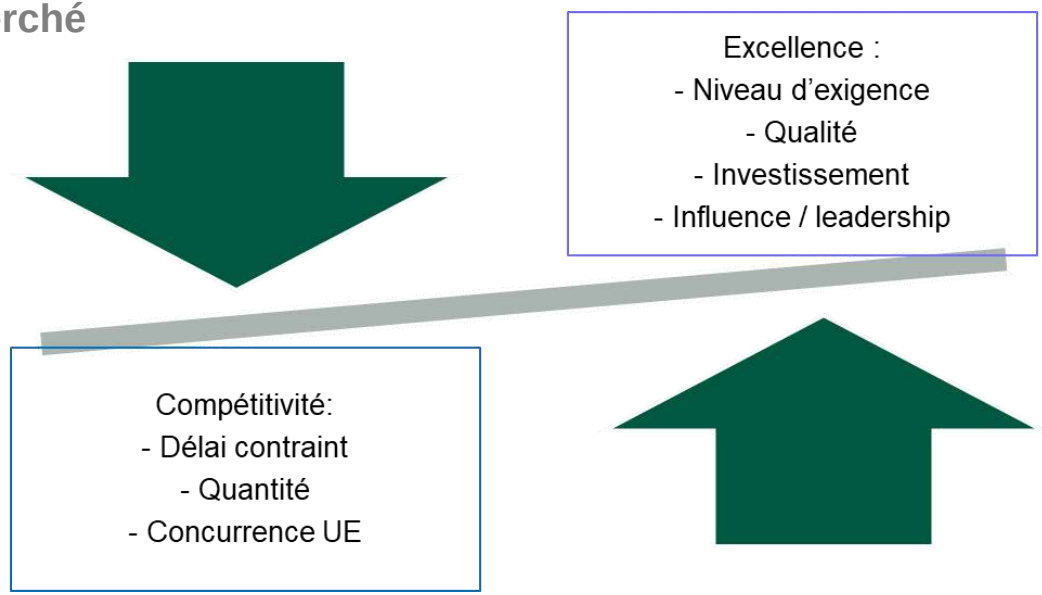
- CCN est composé de 13 personnes (12,5 ETP) au 07/2022
  - 2021 :
    - 2 départs (2 certificateurs CC HW également responsables qualité)
    - 3 arrivées (1 certificateur CSPN SW , 1 responsable qualité et 1 gestionnaire de planning)
  - 2022 :
    - 1 départ (certificateur CSPN SW) + 2 départs à venir (1 certificateur CC HW et 1 assistant certificateur)
    - 2 arrivées (1 certificateur CSPN SW + 1 certificateur CC HW)

- Effectif de certificateurs en décroissance => besoin de renforts
  - recrutements ouverts

- Constat d'un problème de charges à CCN

Problème de charges à CCN

Equilibre recherché



=> CCN ne peut pas traiter un nombre infini de dossiers en entrée avec un nombre de certificateurs fini

Problème de charges à CCN

Plan d'actions

- Renforcement des plannings et transparence sur les délais de traitement
- Amélioration du suivi continu des CESTI
- Renforcement des RH consacrées aux « critères communs »
- Refuser systématiquement les évaluations CSPN de produits
  - « exotiques » (càd « qu'on ne sait pas évaluer dans de bonnes conditions ») ou
  - ne respectant pas une liste élémentaire de bonnes pratiques (càd « qui sont certains d'échouer »)

Centre de certification national

Activités

> Accréditation 17025 des CESTI : manque de ressources ↗
> Participation aux audits CCRA et SOG-IS : aucun (situation COVID) ↘
> Participation aux GT internationaux (JIWG, JHAS, JEDS, ISCI) →
> Participation aux GT nationaux (inter-CESTI, ComUsers): reprise suite COVID ↗
> Audits agréments: reprise suite COVID ↗
> Normalisation ↗

3. SUIVI DE L'AGRÉMENT DES CESTI

Agréments Logiciels et équipements réseaux

Software

Nom	CC	CSPN	Date fin agrément	Audit

Agréments Logiciels et équipements réseaux

Software

Nom	CC	CSPN	Date fin agrément	Audit

Agréments Logiciels et équipements réseaux

Software

Nom	CC	CSPN	Date fin agrément	Audit

Agréments composants électroniques, microélectroniques et logiciels embarqués

Hardware

Nom	CC	CSPN	Date fin agrément	Audit

Agréments équipements matériels avec boitiers sécurisés

Hardware devices

Nom	CC	CSPN	Date fin agrément	Audit

4. QUALITÉ ET ACCRÉDITATION DU CENTRE

Centre de certification national

Objectifs

> Obtenir l'accréditation 17065 de CCN

> Mettre en place le plan d'actions pour assurer l'adéquation entre charges et effectifs CCN

> Faire une proposition permettant la mise en place du télétravail dans le schéma de certification

Accréditation

Actions réalisées

- Mis en place du Dispositif de préservation de l'impartialité
  - publication d'une nouvelle procédure ANSSI-CC-QUA-P-02
  - refonte de l'analyse de risques de CCN
  - organisation des réunions du Comité (*2)
  - approbation par le comité de l'analyse de risques

Accréditation

Actions à mener avant dépôt de la demande d'accréditation

- Mise à jour de la procédure de gestion des compétences CCN ANSSI-CC-PER-P-01
  - sera soumis à approbation cet été

- Disposer de l'engagement d'impartialité des membres du ComDir
  - en cours

- Dérogation / politique de sécurité à prononcer pour les auditeurs COFRAC

- Mise à jour du manuel qualité
  - sera soumis à approbation cet automne

Accréditation

Planning

- Dépôt de la demande d'accréditation mi-octobre 2022
  - une fois matrice de compétences mise à jour avec prise en compte de la dernière procédure, qui doit être diffusée avec cette demande
- Analyse documentaire par le COFRAC
- Et si résultats positifs, visite COFRAC de l'ANSSI et de CESTI

Plaintes 2022

Traitement des écarts relevés lors des audits internes

Audits depuis 2015

		Statut des écarts		
		Ouverts (traitement non identifié)	En cours de traitement en 2022 (actions correctives identifiées)	Clos en 2021-2022
Sources	Audit interne du centre de certification N°5	0	0	1
	Audit interne du centre de certification N°6 - 2016 - ONX	1	2	1
	[redacted]			
	Audit interne du centre de certification N°8 - 2018 - LNE	0	2	8
	Audit interne du centre de certification N°9 - 2019 - LNE	0	0	1
	Audit interne du centre de certification N°10 - 2020 - LNE	0	2	8 (dont 1 abandon)
	Audit interne du centre de certification N°11 - 2021 - LNE	0	10	8
TOTAL		**1**	**16**	**27**

4. EVOLUTIONS

Qualité/travaux réalisés

Evolutions des méthodologies d'évaluation

- Base méthodologique d'analyse de code, CC (HW et SW)
  - a été soumise pour revue aux CESTI
  - démarche partagée avec le BSI
  - sera soumis à approbation ComDir cet été

Travaux à venir

Evolutions prévues CC HW

> Abandon du processus de surveillance au profit de réévaluation mineure:

> réévaluation mineure = Rééval AVA obligatoire + prise en compte évolution méthodologie obligatoire (exemple: analyse crypto)

> Formulaire associé retiré du site web

> Les derniers rapports de surveillance seront émis par l'ANSSI début 2023

Travaux à venir

Evolutions prévues (CC et CSPN SW)

> Pour participer à la réduction de charges à CCN, décision a été prise de mieux formaliser les attentes des évaluations logicielles CSPN et CC pour éviter les débats tant interne qu'externe qui ont actuellement lieu dans le cadre des restitutions

> Objectifs :

- Améliorer la comparabilité des résultats des CESTI (assurer l'homogénéité)
- Améliorer la comparabilité des retours des experts ANSSI intervenants sur les évaluations en soutien à CCN (assurer l'indépendance de CCN)
- Améliorer la prévisibilité des résultats pour les commanditaires

Travaux à venir

Evolutions prévues (CC et CSPN SW)

- Priorités à titre indicatif, correspondantes aux objectifs internes de CCN (P0: 2022/2023, P1:2023/2024)
  - analyse logicielle
    - analyse statique de code (en cours)
    - analyse applicative (P2)
  - analyse Système
    - linux (P0)
    - windows (P1)
    - mobile (P0)
    - virtualisation / cloisonnement (P1)
  - analyse réseau (reconnaissance, fuzzing…) (P0 ou P1)
  - analyse logiciel embarqué et HW élémentaire (P1)
  - analyse de vulnérabilités publiques et génériques (P0)

Travaux à venir

Evolutions prévues (CC et CSPN SW et HW)

- Challenge inter-CESTI 2022 dédié crypto
  - sur la base d'une application de messagerie instantanée développée pour les besoins du challenge
  - tous les CESTI sont impliqués
  - travaux sur l'analyse cryptographique uniquement

- Objectifs
  - comparaisons du niveau des CESTI
  - + publicité via publication du véhicule de test et un article avec les résultats des CESTI
  - création d'un modèle de rapport d'analyse crypto pour homogénéisation des travaux

5. ACTIVITÉS À L'INTERNATIONAL

Normalisation

FITCEM

- Norme EU (prEN 17640) vise à être intégrée à un schéma CSA: CESTI invités à anticiper les besoins d'accréditation si volonté de maintenir les activités
- NB le CSA impose aux CB d'abandonner leurs schémas nationaux quand un équivalent européen est mis en place
- Publication du standard prévue début 2023
- Objectif CCN : pérenniser la démarche FR

Normalisation

CC

> Nouvelle version ISO2022/CCv4.0 devait être publiée en juin

> Règles de transition en cours de discussion au CCRA ; seront certainement reprises par CSA EUCC

> Accord ISO pour conserver disponibilité d'une version gratuite CCRA: qui devrait être publiée en même temps que la version ISO (prévue courant juin)

Cybersecurity Act /EUCC

▪	EUCC v1.0	✓ Juillet 2020
▪	ECCG opinion	✓ Décembre 2020
▪	EUCC v1.1.1 transmitted to the European Commission	✓ Mai 2021
▪	Working document (1st draft IR)	✓ Juin 2021
▪	Draft Implementing regulation	⏳ Printemps - été 2022
▪	(Public) draft Implementing Regulation	? Automne 2022
▪	Committee	? Automne 2022
▪	Adoption	? Hiver 2022-2023

Cybersecurity Act /EUCC

Calendrier d'application

- **T0** : publication au journal officiel de l'UE
- **T1** = T0 + 20 jours :
  - entrée en vigueur du règlement
  - application partielle du règlement : autorisation et notification des OECs **(Q1 2023 ?)**
- **T1 + 1 an** : application complète du règlement **(premiers certificats émis, Q1 2024 ?)**
- **T1 + 2 ans** : les schémas de certification dont le périmètre est couvert par EUCC cessent d'opérer **(fin de l'émission de certificats, Q1 2025 ?)**
- **T0 prévisionnel** : Décembre 2022 - Janvier 2023

Reconnaissance

Reconnaissance bilatérale GE/FR des certificats BSZ/CSPN

> Accord signé en juin, une communication faite via site web ANSSI et réseaux sociaux

> Principe de l'accord :

> tous les certificats FR émis jusqu'à 3 ans avant signature de l'accord sont reconnus, sauf mention explicite [redacted]

> réunion d'échanges biannuels sur fonctionnement

> Dans le cadre de la mise en place de cet accord, la durée de validité a été fixée à 3 ans en FR (vs 2 ans en GE)