SPAC
>ALLIANCE<

Retex HESTIA25 – ANSSI

[HARMONISATION EUROPÉENNE des STANDARDS des TECHNOLOGIES d'IDENTIFICATION des ACCÈS]

Projet financé par l'État dans le cadre de France 2030

22 Janvier 2026

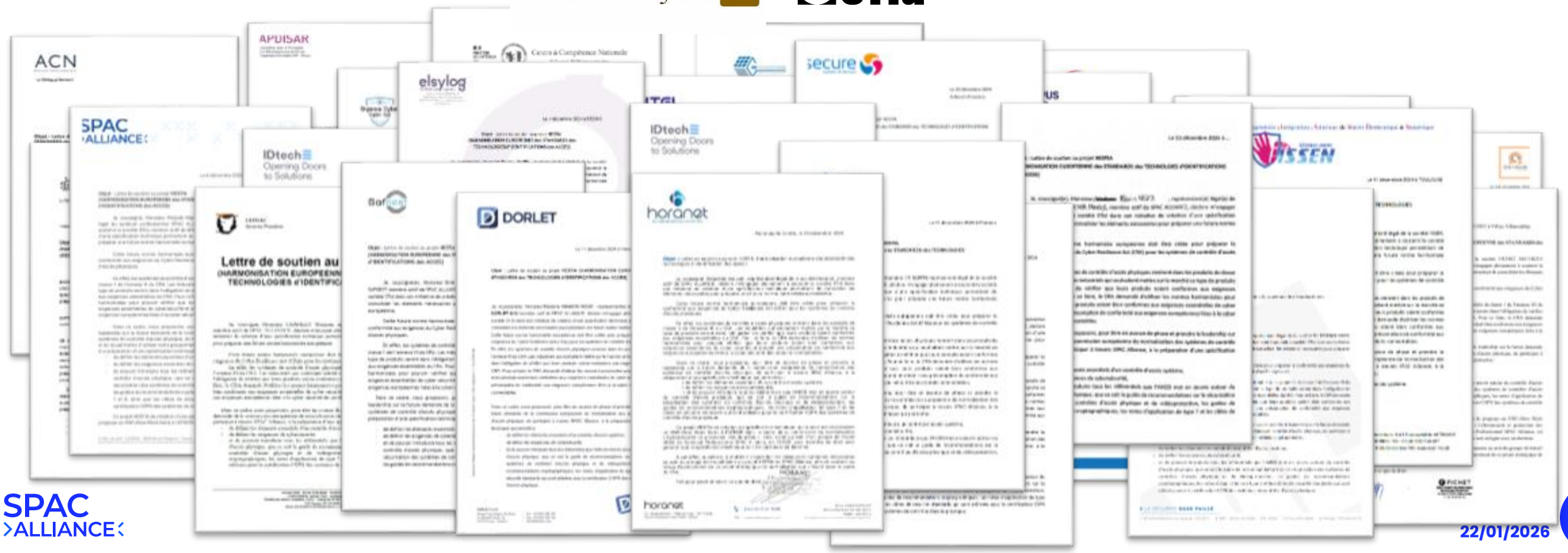
GOUVERNEMENT
Liberté
Égalité
Fraternité
FRANCE 2030

Cofinancé par
l'Union européenne

NCC-FR
FRANCE CYBERSECURITY
COORDINATION CENTRE

bpifrance
SERVIR L'AVENIR

Remerciements



Institutionnels

SPAC
>ALLIANCE<

1. Historique du projet

1. Cyber Resilience Act (CRA)
2. Normes Harmonisées
3. Enjeux de l'appel à projet

2. Le projet HESTIA

1. Roadmap du projet Hestia
2. Les livrables
3. Groupes de travail, lignes directrices et travaux

3. Les suites du projet HESTIA

CYBER RESILIENCE ACT

Normes harmonisées

SPAC
>ALLIANCE<

Cyber Resilience Act

Règlement européen officiellement publié en octobre 2024

À partir de fin 2027, tous les produits comportant des composants numériques devront renforcer leur niveau de cybersécurité et se conformer aux exigences en matière de cybersécurité listées en annexe I du règlement CRA afin de pouvoir être commercialisés sur le marché européen

Hardware et Software incluant les firmwares, le traitement de données à distance, les protocoles etc.)

Concerne tous les produits comportant des éléments numériques **commercialisés en Europe**

Qui est concerné ?

Principalement les fabricants et industriels , avec une responsabilité partagée pour les distributeurs, intégrateurs, prescripteurs et utilisateurs finaux.

Pénalités financières
Jusqu'à 10 M€ / 2,5% du CA global

SPAC ALLIANCE

Cyber Resilience Act

APERÇU DES OBLIGATIONS

Évaluation des risques liés au produit **[art. 10(2)]**

Exigences essentielles **liées au produit** (Annexe I, Section 1)
Exigences essentielles relatives à la **gestion des vulnérabilités** (Annexe I, Section 2)
Dossier technique/Guide, incluant les informations et instructions d'utilisation (Annexes II + V)

Évaluation de la conformité[article 24]
Auto-évaluation – Module B + C – Module H – Certificat UE
Marquage CE, Déclaration Européenne de conformité(Annexe IV)

Phase de conception et de développement

Phase de maintenance
Assistance produit d'une durée minimale de 5 ans

Pendant la période de support, les fabricants doivent s'assurer que :

- Les vulnérabilités du produit, y compris de ses composants, sont traitées efficacement et conformément aux exigences essentielles
- Des politiques appropriées de divulgation coordonnée des vulnérabilités sont mises en place
- Un processus de remédiation des vulnérabilités est appliqué

Les mises à jour de sécurité doivent rester disponibles pendant **10 ans**

Cyber Resilience Act

PRINCIPES CLÉS DES EXIGENCES ESSENTIELLES DE SÉCURITÉ

Partie 1 : Exigences de sécurité relatives aux propriétés des PWDEs

Sécurité dès la conception et par défaut, basée sur l'évaluation des risques

Lien entre sécurité physique et logique

Concept de sécurité de bout-en-bout

Responsabilité collective et partagée

- Absence de vulnérabilités exploitables
- Configuration sécurisée par défaut
- Correction des vulnérabilités via des mises à jour automatiques et/ou manuelles
- Protection contre les accès non autorisés
- Confidentialité et intégrité des données (au repos ou en transit), grâce au chiffrement des données par des mécanismes de pointe
- Protection de l'intégrité des données stockées, transmises ou traitées

- Minimisation des données
- Disponibilité des fonctions essentielles
- Limitation des surfaces d'attaque
- Réduction de l'impact d'un incident grâce à des mécanismes d'atténuation appropriés
- Enregistrement et surveillance des événements liés à la sécurité
- Possibilité pour les utilisateurs de supprimer de manière permanente, sécurisée et simple toutes les données et paramètres

Cyber Resilience Act

PRINCIPES CLÉS DES EXIGENCES ESSENTIELLES DE SÉCURITÉ

Partie 2 : Exigences en matière de gestion des vulnérabilités

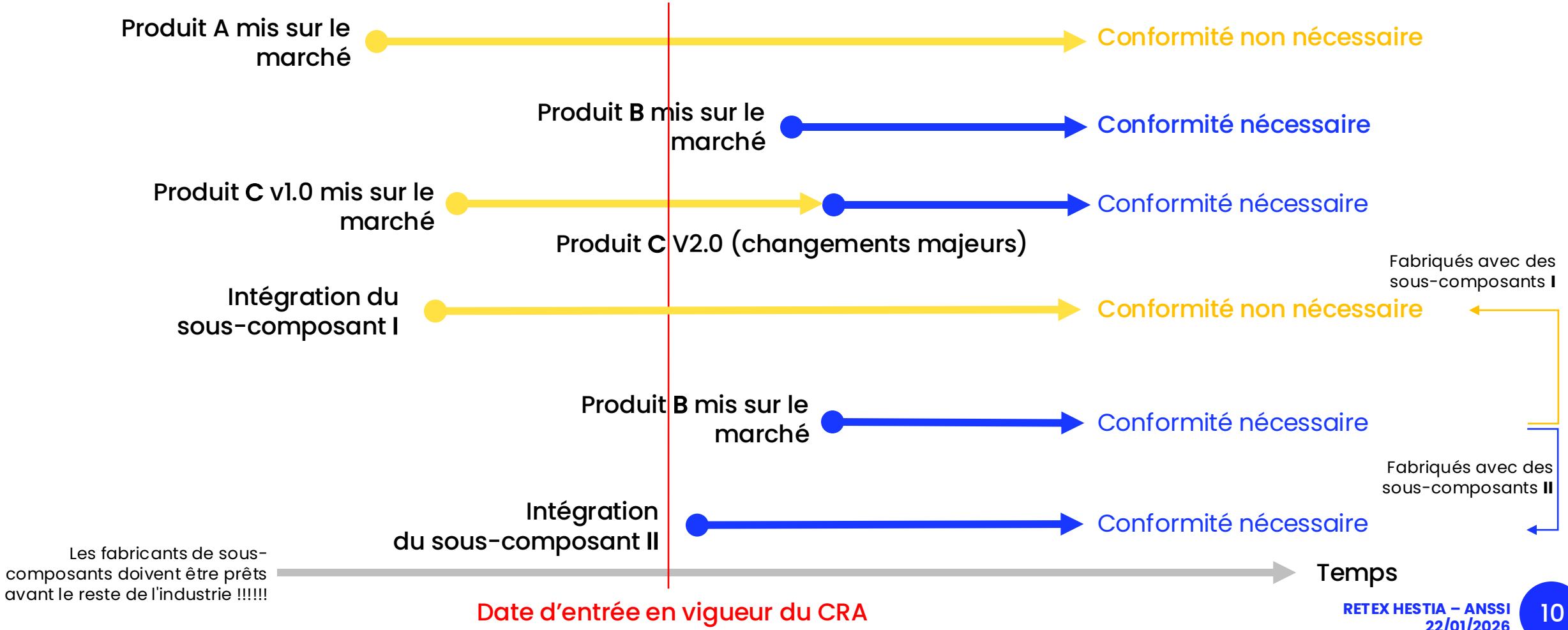
Déclaration obligatoire
des incidents

- Identifier et documenter les vulnérabilités et les composants contenus dans le produit, en établissant une liste des composants logiciels (SBOM)
- Traiter et corriger les vulnérabilités sans délai, notamment en fournissant des mises à jour de sécurité
- Tester et examiner régulièrement et efficacement la sécurité du produit
- Une fois qu'une mise à jour de sécurité est disponible, partager et divulguer publiquement les informations relatives aux vulnérabilités corrigées (peut être retardé si cela entraîne des risques pour la sécurité)

- Politique de divulgation coordonnée des vulnérabilités
- Faciliter le partage d'informations sur les vulnérabilités potentielles
- Fournir des mécanismes permettant de distribuer les mises à jour en toute sécurité, le cas échéant par le biais de mises à jour de sécurité automatiques
- Diffusion des mises à jour de sécurité sans délai et gratuitement (sauf accord contraire dans le cadre d'une relation B2B)

1 - Cyber Resilience Act

APPLICABILITÉ DE LA CRA – OBLIGATION DE CONFORMITÉ



Cyber Resilience Act

QUELS SONT EXACTEMENT LES PRODUITS CONCERNÉS ?

Produits par défaut

Représentent **90 % des produits** du marché (ex : IoT grand public, logiciels à usage général, etc.)

Nécessitent une procédure d'auto-évaluation

Produits importants

Les produits concernés sont divisés en classe I et II

Doivent être **conformes aux normes harmonisées** pour bénéficier de la présomption de conformité

Doivent faire l'objet d'une procédure **d'évaluation de la conformité par un tiers** afin de prouver leur conformité

Produits critiques

Peut nécessiter un **certificat CSA européen** (ex : EUCC) pour la présomption de conformité

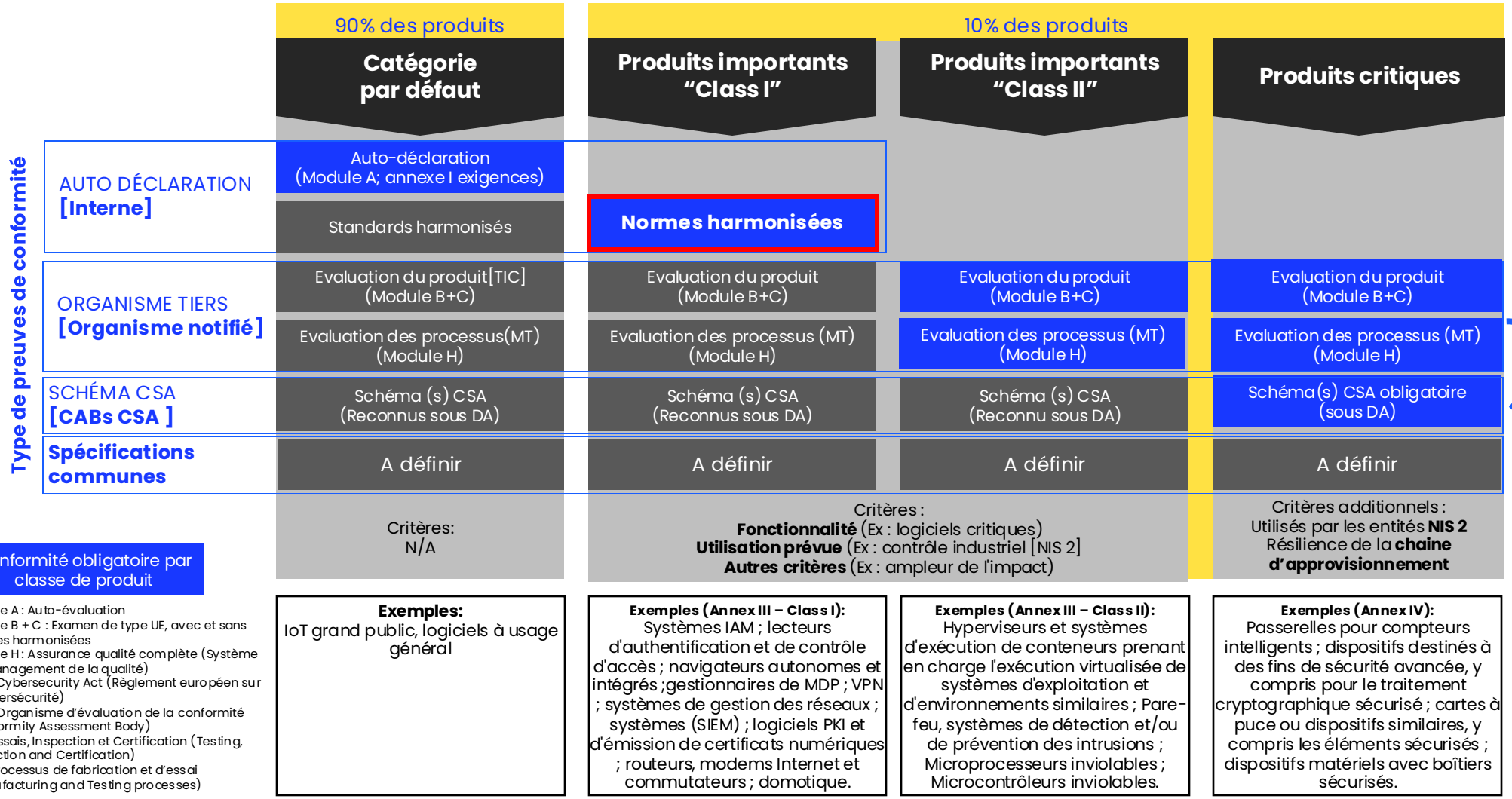
Cyber Resilience Act

FOCUS SUR LES PRODUITS IMPORTANTS – CLASSE 1

1. Systèmes de gestion des identités et logiciels et matériels de gestion des accès privilégiés, y compris les lecteurs d'authentification et de contrôle d'accès, y compris les lecteurs biométriques ;
2. Navigateurs autonomes et intégrés;
3. Gestionnaires de mots de passe;
4. Logiciel qui recherche, supprime ou met en quarantaine les logiciels malveillants;
5. Produits comportant des éléments numériques ayant la fonction de réseau privé virtuel (VPN) ;
6. Systèmes de gestion de réseau ;
7. Systèmes de gestion des informations et des événements de sécurité (SIEM) ;
8. Gestionnaires de démarrage;
9. Infrastructure à clé publique et logiciel d'émission de certificats numériques;
10. Interfaces réseau physiques et virtuelles;
11. Systèmes d'exploitation
12. Routeurs, modems destinés à la connexion à Internet et commutateurs
13. Microprocesseurs dotés de fonctionnalités liées à la sécurité;
14. Microcontrôleurs dotés de fonctionnalités liées à la sécurité;
15. Circuits intégrés spécifiques à une application (ASIC) et réseaux de portes programmables sur site (FPGA) dotés de fonctionnalités liées à la sécurité;
16. Assistants virtuels polyvalents pour maisons intelligentes;
17. Produits domotiques dotés de fonctionnalités de sécurité, notamment des serrures intelligentes, des caméras de sécurité, des systèmes de surveillance pour bébés et des systèmes d'alarme;
18. Jouets connectés à Internet couverts par la directive 2009/48/CE qui ont des fonctionnalités sociales interactives (par exemple, parler ou filmer) ou qui ont des fonctionnalités de localisation;
19. Produits portables destinés à être portés ou placés sur le corps humain, qui ont pour finalité la surveillance de la santé (par exemple, le suivi) et auxquels le règlement (UE) 2017/745 ou le règlement (UE) 2017/746 ne s'appliquent pas, ou produits portables destinés à être utilisés par et pour les enfants.

Cyber Resilience Act

APERÇU DE L'ÉVALUATION DE LA CONFORMITÉ



Certification obligatoire
Par voie d'acte d'exécution, la Commission définit les produits critiques dotés des fonctionnalités essentielles listées l'annexe III bis, devant obtenir un certificat CSA de l'UE

Conformité obligatoire par classe de produit

Module A : Auto-évaluation
Module B + C : Examen de type UE, avec et sans normes harmonisées
Module H : Assurance qualité complète (Système de management de la qualité)
CSA : Cybersecurity Act (Règlement européen sur la cybersécurité)
CAB : Organisme d'évaluation de la conformité (Conformity Assessment Body)
TIC : Essais, Inspection et Certification (Testing, Inspection and Certification)
MT : Processus de fabrication et d'essai (Manufacturing and Testing processes)

3 FÉVRIER 2025

La Commission a publié une décision d'exécution demandant aux trois organismes européens de normalisation (CEN, CENELEC, ETSI) d'élaborer 41 normes harmonisées concernant les produits comportant des éléments numériques, afin de permettre l'application du CRA

Normes verticales #16

Norme(s) européenne(s) relative(s) aux exigences essentielles en matière de cybersécurité pour les systèmes de gestion des identités et les logiciels et matériels de gestion des accès privilégiés, y compris les lecteurs d'authentification et de contrôle d'accès, y compris les lecteurs biométriques

Norme à définir pour le 30 octobre 2026...

SPAC
>ALLIANCE<

Enjeux de l'appel à projet

Cadre concurrentiel

Besoin de s'assurer que la conformité au CRA se réalise à travers une norme stricte, basée sur des référentiels de cybersécurité exigeants

Projet lauréat de l'AAP « Soutien aux PME et startups pour renforcer leurs compétences dans le domaine de la cybersécurité – Axe 3 : Soutien aux activités de normalisation » co-financé par France 2030 et Digital Europe.

HESTIA

Phase 1
Rédaction d'une spécification technique de pré-normalisation définissant les exigences d'un système de contrôle d'accès physique, en conformité avec le référentiel de cybersécurité du Cyber Resilience Act et les référentiels de l'ANSSI + dépôt NWI

Phase 2
Se positionner comme leader au niveau des commissions de normalisation européennes dans l'élaboration de la future norme harmonisée des produits de sécurité physique électronique dont le contrôle d'accès

APPEL À PROJET

Soutien aux activités de normalisation

SPAC
>ALLIANCE<

Projet HESTIA

[HARMONISATION EUROPÉENNE des STANDARDS des TECHNOLOGIES d'IDENTIFICATION des ACCÈS]

Le projet a reçu un financement public dans le cadre du programme France 2030

SPAC
>ALLIANCE<

GOUVERNEMENT
Liberté
Égalité
Fraternité

FRANCE 2030

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

bpifrance
SERVIR L'AVENIR

Cofinancé par l'Union européenne

Roadmap HESTIA (Phase 1)

PHASE 1

Nov. – Dec. 24 | Jan. 25 | Fév. 25 | Mar. 25 | Avr. – jui.25 | juil. – sept.25 | Oct. 25

NCC-FR FRANCE CYBERSECURITY COORDINATION CENTRE

bpifrance

Projet HESTIA25

Identification / préparation du dossier de candidature à l'AAP dédié au renforcement des compétences en cybersécurité et aux activités de normalisation

Dossier de réponse à l'AAP

Début du projet HESTIA

Publication de la demande des 41 normes par la CE

Publication Call For Tender STAN4CR2

Publication document préliminaire

Dossier de réponse au STAN4CR2

Réunions & consultations CE

Dépôt du NWI et constitution du CEN TC224 WG17

Mise à jour de la spécification de pré-normalisation

Publication formation CRA/norme

Fin du projet HESTIA

Lot 1

Lot 2

Lot 3

Lot 4

SPAC ALLIANCE

Livrables HESTIA

LOT 1

Document de synthèse des exigences provenant du C.R.A pour les produits de classe 1


Cahier des charges de la future norme portant sur les systèmes de gestion des identité et logiciels et matériels de gestion des accès privilégiés, y compris les lecteurs d'authentification et de contrôle d'accès, y compris les lecteurs biométriques

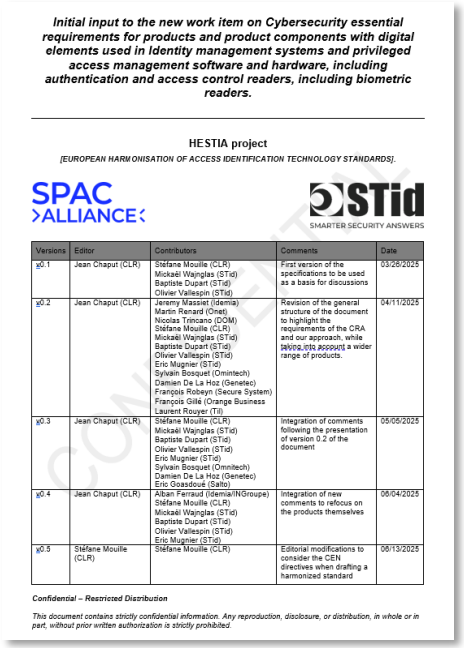
Projet HESTIA

SPAC ALLIANCE

STid

LOT 2

Spécifications techniques de pré-normalisation / Cahier des charges


Initial input to the new work item on Cybersecurity essential requirements for products and product components with digital elements used in Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers.

HESTIA project

[EUROPEAN HARMONISATION OF ACCESS IDENTIFICATION TECHNOLOGY STANDARDS].

SPAC ALLIANCE

STid SMARTER SECURITY ANSWERS

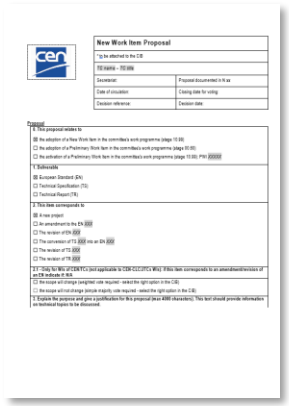
Versions	Editor	Contributors	Comments	Date
v0.1	Jean Chaput (CLR)	Stéfane Mouille (CLR) Mickaël Wajnglas (STid) Baptiste Dupart (STid) Olivier Vallespin (STid)	First version of the specifications to be used as a basis for discussions	03/26/2025
v0.2	Jean Chaput (CLR)	Jeremy Massiet (Idemia) Martin Renard (Onet) Nicolas Trincano (DOM) Stéfane Mouille (CLR) Mickaël Wajnglas (STid) Baptiste Dupart (STid) Olivier Vallespin (STid) Eric Mugnier (STid) Sylvain Bosquet (Omnitech) Damien De La Hoz (Genetec) François Robeyn (Secure System) François Gillé (Orange Business Laurent Rouyer (Til)	Revision of the general structure of the document to highlight the requirements of the CRA and our approach, while taking into account a wider range of products.	04/11/2025
v0.3	Jean Chaput (CLR)	Stéfane Mouille (CLR) Mickaël Wajnglas (STid) Baptiste Dupart (STid) Olivier Vallespin (STid) Eric Mugnier (STid) Sylvain Bosquet (Omnitech) Damien De La Hoz (Genetec) Eric Goasdoué (Salto)	Integration of comments following the presentation of version 0.2 of the document	05/05/2025
v0.4	Jean Chaput (CLR)	Alban Ferraud (Idemia/INGroupe) Stéfane Mouille (CLR) Mickaël Wajnglas (STid) Baptiste Dupart (STid) Olivier Vallespin (STid) Eric Mugnier (STid)	Integration of new comments to refocus on the products themselves	06/04/2025
v0.5	Stéfane Mouille (CLR)	Stéfane Mouille (CLR)	Editorial modifications to consider the CEN directives when drafting a harmonized standard	06/13/2025

Confidential – Restricted Distribution

This document contains strictly confidential information. Any reproduction, disclosure, or distribution, in whole or in part, without prior written authorization is strictly prohibited.

LOT 3

NWI et spécifications techniques de pré-normalisation en annexe du NWI


New Work Item Proposal


Initial input to the new work item on Cybersecurity essential requirements for products and product components with digital elements used in Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers.

HESTIA Project operated by the SPAC Alliance

[EUROPEAN HARMONISATION OF ACCESS IDENTIFICATION TECHNOLOGY STANDARDS]

LOT 4

Formation pour comprendre les exigences/normes harmonisées du CRA

Groupes de travail, lignes directrices et travaux

Lignes directrices pour l'élaboration du document de pré-normalisation

SUIVI DE 4 TYPES EXIGENCES

CRA
Sécurité & Gestion des vulnérabilités

Checklist UE
Pour les standards cités au JOUE

Exigences ANSSI
Guides & référentiels

Marché
x10 groupes de travail

Exigences ANSSI

Ex. 1	Ex. 2	Ex. 3	Ex. 4
Guide de recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection – v2.2 + Profil de protection CSPN pour système de contrôle d'accès	Note 7 - v2.0 + Note 9 – v1.0 + Procédure CER-P-02	Catalogue SOGIS + Référentiels crypto. ANSSI • RGS • Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques • Guide de sélection d'algorithmes cryptographiques	Guide d'hygiène informatique ANSSI – v2.0 EBIOS Risk Manager ISO/IEC 27005

Travaux en groupes de travail (1/2)

Définition du scope produits

- Descriptions des sous systèmes de contrôle d'accès et de gestion des identités
- Liste des produits concernés

Elargissement du scope produits

- Vu avec la CE
- Intégration des produits de l'écosystème de la vidéoprotection, de l'intrusion et de l'incendie

Elaboration documentaire

- Listes de l'ensemble des référentiels sources
- Structuration du document
- Rédaction d'exigences

Travaux et problématiques identifiées/traitées

- Sécurité de l'IT, de l'architecture et des processus fonctionnels hors scope
- Exigences orientées initialement solutions/systèmes opérés, réorientées produits
- Adaptation des exigences haute sécurité de l'ANSSI avec les besoins marchés, cas d'application
- Elaboration des exigences qui puissent se recouper avec des normes existantes pour
  - optimiser la cohérence des exigences
  - faciliter et accélérer la mise en conformité du marché

  => Recoupement avec l'ISO/IEC 62443-4 (IACS)

Travaux en groupes de travail (2/2)

Définition des profils de sécurité

- Basique, substantiel, élevé

Mise en place d'une méthodologie spécifique

- Identification des « Intended purposes » (*destinations prévues*) et des Reasonably foreseeable use (*usage raisonnablement prévisible*)
- Analyse de risque basée sur des référentiels et normes reconnues (ISO 31073:2022, ISO/IEC 27005, EU Risk Management Framework, EBIOS Risk Manager de l'ANSSI)
- Définition des profils de sécurité basé sur l'outil OASIS de l'ANSSI

Problématique hors scope de la norme mais importante pour le marché

- Travaux en cours : comment permettre aux intégrateurs/installateurs/utilisateurs finaux de s'assurer facilement que le produit conforme CRA sur profils basique, Substantiel ou élevé, est bien adapté pour le cas d'usage terrain.

LES SUITES DU PROJET HESTIA

CEN TC224 WG17

SPAC ALLIANCE

Les suites du projet HESTIA (Phase 2)

PHASE 2

Juil. – Déc. 25 | Janv. – Oct.26

CEN TC224 WG17

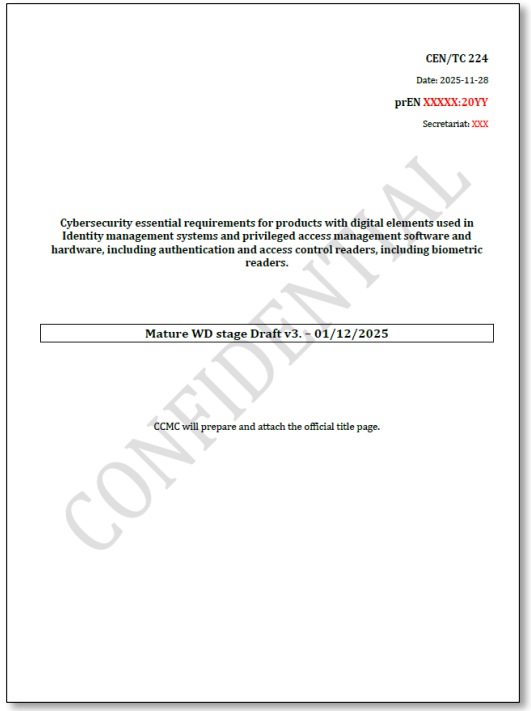
- Demande d'intégration STid au CEN TC 224 WG 17 via l'AFNOR
- **Dépôt du NWI et constitution du CEN TC224 WG17**
- Validation du NWI
- 1er Draft template d'audit de conformité
- Envoi du 1er Mature Draft au HAS Consultant de la CE
- 1er retour du HAS Consultant de la CE
- Meeting Rapporteur
- Meeting Rapporteur
- Envoi draft maj
- Meeting Rapporteur
- Meeting Rapporteur
- Meeting Rapporteur
- Meeting Rapporteur
- Dernière soumission de commentaires
- **Publication de la norme #16**

Travaux d'élaboration de la norme au CEN TC224 WG17 / réunions hebdomadaires

Suivi et contribution en groupes de travail HESTIA / Réunions bi-mensuels

Livrables produits dans le cadre du WG17 CEN TC 224

Mature Working Draft – v3



CEN/TC 224

Date: 2025-11-28

prEN XXXXX:20YY

Secretariat: XXX

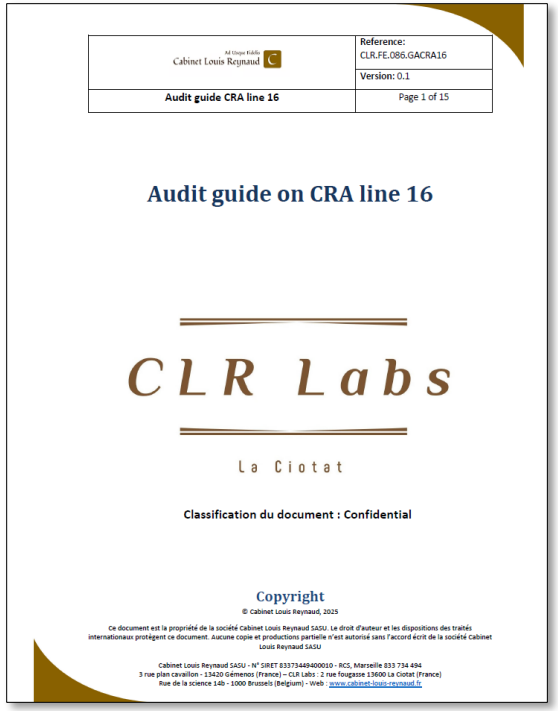
Cybersecurity essential requirements for products with digital elements used in Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers.

Mature WD stage Draft v3. – 01/12/2025

CCMC will prepare and attach the official title page.

CONFIDENTIAL

Audit guide draft on line 16



Cabinet Louis Reynaud	Reference: CLR.FE.086.GACRA16
	Version: 0.1
Audit guide CRA line 16	Page 1 of 15

Audit guide on CRA line 16

CLR Labs

La Ciotat

Classification du document : Confidential

Copyright

© Cabinet Louis Reynaud, 2025

Ce document est la propriété de la société Cabinet Louis Reynaud SASU. Le droit d'auteur et les dispositions des traités internationaux protègent ce document. Aucune copie et productions partielle n'est autorisé sans l'accord écrit de la société Cabinet Louis Reynaud SASU

Cabinet Louis Reynaud SASU - N° SIRET 83373449400010 - RCS, Marseille 833 734 494
3 rue plan cavaillon - 13420 Gémenos (France) – CLR Labs : 2 rue fougasse 13600 La Ciotat (France)
Rue de la science 14b - 1000 Brussels (Belgium) - Web : www.cabinet-louis-reynaud.fr

Merci !!!