SPAC
ALLIANCE

HESTIA25 feedback report – ANSSI

[European harmonization of standards for access identification technologies]

Project funded by the French government as part of the France 2030 program

22 January 2026

GOUVERNEMENT
Liberté
Égalité
Fraternité

FRANCE 2030

Cofinancé par l'Union européenne

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

bpifrance
SERVIR L'AVENIR

Acknowledgements

FRANCE 2030

bpifrance SERVIR L'AVENIR

NCC-FR FRANCE CYBERSECURITY COORDINATION CENTRE

ANSSI

Ad Usque Fidelis Cabinet Louis Reynaud

STid

Institutional stakeholders

SPAC
>ALLIANCE<

1. Project Background

1. Cyber Resilience Act (CRA)
2. Harmonized Standards
3. Challenges of the call for projects

2. The HESTIA project

1. HESTIA project roadmap
2. Delivrables
3. Working groups, guidelines, and activities

3. Nexts steps for the HESTIA project

CYBER RESILIENCE ACT

Harmonized standards

SPAC
ALLIANCE

Cyber Resilience Act

European Regulation officially published in October 2024

From the end of 2027 onwards, all products containing digital components will be required to strengthen their level of cybersecurity and comply with the cybersecurity requirements listed in annex I of the CRA regulation in order to be placed on the european market.

Hardware & Software including firmwares, Remote data processing, Protocols etc.)

Concerns every Product With Digital Elements (PWDEs) **sold** within the European Union

WHO'S CONCERNED?

Mainly manufacturers, with shared responsibility for distributors, integrators, prescribers and final users as well

Financial Penalties
Up to 10 M€ /2,5% of Global turnover

SPAC ALLIANCE

Cyber Resilience Act

OBLIGATIONS OVERVIEW

Product risk assessment [art 10(2)]

Product-related essential requirements (Annex I, Section 1)
Vulnerability handling essential requirements (Annex 1, Section 2)
Technical file, including information and instructions for use (Annex II + V)

Conformity assessment [article 24]
Self-assessment – Module B+C - Module H – EU certificate
CE marking, EU Declaration of Conformity (Annex IV)

Design and development phase

Maintenance phase
minimum 5 year-Product support

During the support period, manufacturers shall ensure:

- Vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential requirements
- Appropriate coordinated vulnerability disclosure polices
- Process for vulnerability remediation

Security update to remain available 10 years

Cyber Resilience Act

KEY PRINCIPLES OF ESSENTIAL SECURITY REQUIREMENTS

Part 1: Security Requirements related to properties of PWDEs

Security by design / default based on risk assessment

Link Between Cyber and Physical Security

End-to-end security concept

Collective & shared responsability

- No exploitable vulnerabilities
- Secure by default configuration
- Correction of vulnerabilities through automatic/manual updates
- Protection from unauthorised access
- Confidentiality and integrity of data (at rest or in transit), by encryption data by state-of-the-art mechanisms
- protection of the integrity of stored, transmitted or otherwise processed data

- Minimisation of data
- Availability of essential functions
- Limit attack surfaces
- Reduce impact of an incident with proper mitigation mecanism
- Recording and monitoring security relevant events
- Ability for users to permanently, securely, and easily delete all data and settings

Cyber Resilience Act

KEY PRINCIPLES OF ESSENTIAL SECURITY REQUIREMENTS

Part 2: Vulnerability handling requirements

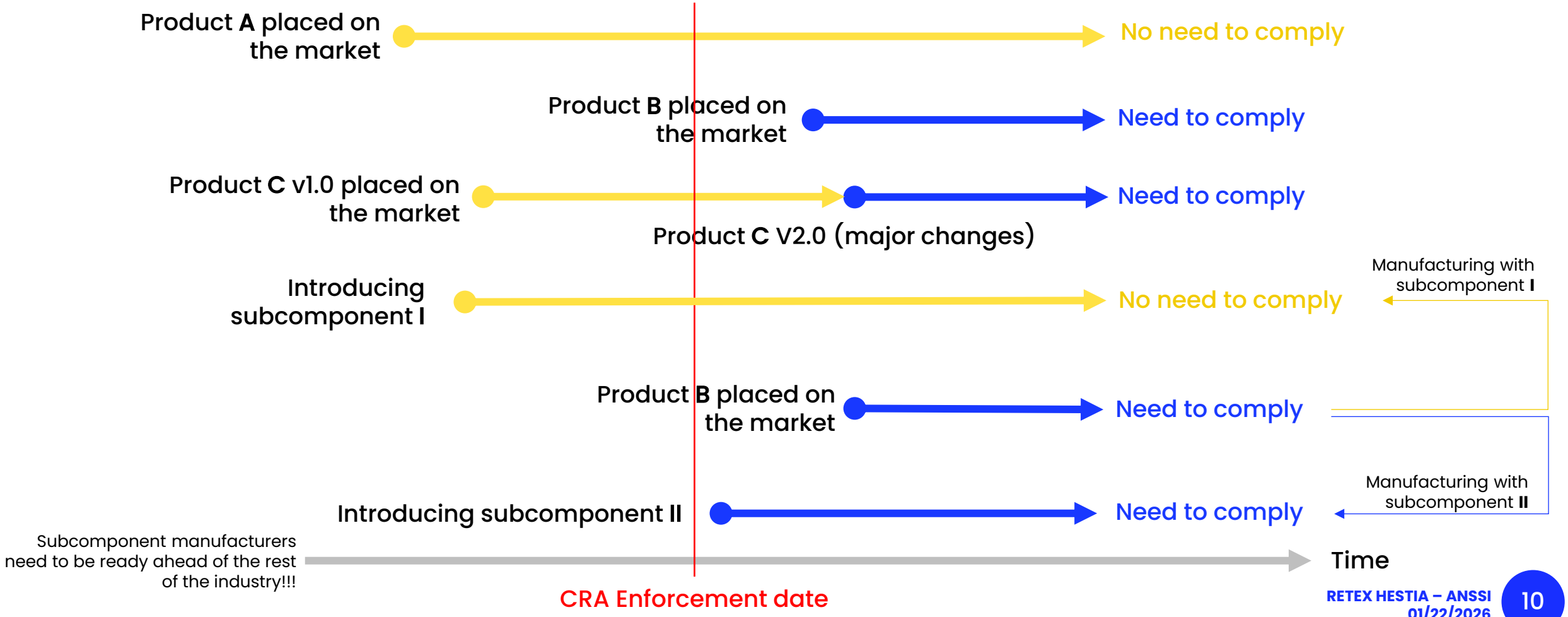
Mandatory incident reporting

- Identify and document vulnerabilities and components contained in the product, drawing up SBOM
- Address and remediate vulnerabilities without delay, including by providing security updates
- Effective and regular tests and reviews of the security of the product
- Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities (could be delayed if it cause security risks)

- Policy on coordinated vulnerability disclosure
- Facilitate sharing of information about potential vulnerabilities
- Provide for mechanisms to securely distribute updates, where applicable through automatic security updates
- Dissemination of security updates without delay, free of charge (unless otherwise agreed in B2B situation)

1 - Cyber Resilience Act

CRA APPLICABILITY – COMPLIANCE OBLIGATION



Cyber Resilience Act

WHAT EXACTLY ARE THE CONCERNED PRODUCT?

Default products	Important products	Critical products
Represent 90% of the market products (ex : Consumer IoT, general-purpose software etc.) Require a Self-assessment procedure	PWDEs divided into class I and II Require a **conformity to Harmonized standards** for the presumption of conformity Require a **Thrird-party conformity assessment** procedure to prove its conformity	May require a **EU CSA certificate** (ex: EUCC) for the presumption of conformity

Cyber Resilience Act

FOCUS ON THE IMPORTANT PRODUCTS – CLASS 1

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Security information and event management (SIEM) systems;
8. Boot managers;
9. Public key infrastructure and digital certificate issuance software;
10. Physical and virtual network interfaces;
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. Microprocessors with security-related functionalities
14. Microcontrollers with security-related functionalities;
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities;
16. Smart home general purpose virtual assistants;
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems;
18. Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features;
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children.

Cyber Resilience Act

CONFORMITY ASSESSMENT OVERVIEW

Type of proof of compliance	90% of products	10% of products		
	Default category	**Important Product "Class I"**	**Important Product "Class II"**	**Critical Products**
SELF ASSESSMENT **[in-house]**	Self-assessment (Module A; annex I requirements)			
	Harmonized standards	**Harmonized standards**		
THIRD-PARTY **[Notified Body]**	Product assessment [TIC] (Module B+C)	Product assessment (Module B+C)	Product assessment (Module B+C)	Product assessment (Module B+C)
	Processes assessment (MT) (Module H)	Processes assessment (MT) (Module H)	Processes assessment (MT) (Module H)	Processes assessment (MT) (Module H)
CSA SCHEME **[CSA CABs]**	CSA Scheme(s) (Recognized under DA)	CSA Scheme(s) (Recognized under DA)	CSA Scheme(s) (Recognized under DA)	Mandatory CSA Scheme(s) (under DA)
Common Specifications	TBD	TBD	TBD	TBD
	Criteria: N/A	Criteria: **Functionality** (e.g. critical software) **Intended use** (e.g. industrial control [NIS2]) **Other criteria** (e.g. extent of impact)		Additional criteria: Used by **NIS2** entities Resilience of **supply chain**
Mandatory conformance per product class	**Examples:** Consumer IoT, general-purpose software	**Examples (Annex III – Class I):** IAM systems; authentication and access control readers; Standalone and embedded browsers; Password managers; VPNs; Network management systems; (SIEM) systems; PKI and digital certificate issuance software; Routers, Internet modems and switches; Smart Home products,	**Examples (Annex III – Class II):** Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments; Firewalls, intrusion detection and/or prevention systems; Tamper-resistant microprocessors; Tamper-resistant microcontrollers;	**Examples (Annex IV):** Smart meter gateways; devices for advanced security purposes, including for secure crypto processing; Smartcards or similar devices, including secure elements; Hardware Devices with Security Boxes

Mandatory certification
By implementing act, the Commission to define critical products with core functionality listed in Annex IIIa – that must obtain a EU CSA certificate

Module A: Self-assessment
Module B+C: EU-type examination with and without harmonized standards
Module H: Comprehensive Quality assurance (Quality Management System)
CSA: Cyber Security Act
CAB: Conformance Accreditation Body
TIC: Testing, Inspection and Certification
MT: Manufacturing and Testing processes

3RD FEBRUARY 2025

The Commission published an Implementing Decision, requesting to the 3 European Standardization bodies (CEN, CENELEC, ETSI) to elaborate 41 harmonized standards regarding products with digital elements in support of the Cyber Resilience Act

Vertical standards #16

European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

The standard is to be defined by October 30, 2026

SPAC
>ALLIANCE<

Challenges of the call for projects

Competitive landscape

Need to ensure that CRA compliance is achieved through a strict standard, based on demanding cybersecurity frameworks

NCC-FR
bpifrance

Project **selected as a winner of the call for projects** “Support for SMEs and startups to strengthen their skills in the field of cybersecurity – Axis 3: Support for standardization activities”, co-funded by France 2030 and Digital Europe.

HESTIA

Phase 1
Drafting of a pre-standardization technical specification defining the requirements of a physical access control system, in compliance with the Cyber Resilience Act cybersecurity framework and ANSSI frameworks, along with the submission of the NWI.

Phase 2
Position ourselves as a leader within European standardization committees in the development of the future harmonized standard for electronic physical security products, including access control.

CALL FOR PROJECT

Support for standardization activities

SPAC ALLIANCE

HESTIA Project

[European harmonization of standards for access identification technologies]

Project funded by the French government as part of the France 2030 program

GOUVERNEMENT
Liberté
Égalité
Fraternité

FRANCE 2030

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

bpifrance
SERVIR L'AVENIR

Cofinancé par l'Union européenne

HESTIA Roadmap (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

HESTIA25 Project

- Identification and preparation of the application file for the call for projects dedicated to strengthening cybersecurity skills and standardization activities.
- Call for projects application file
- **Start of the HESTIA project**
- Publication of the request for the 41 standards by the European Commission
- Publication of the STAN4CR2 Call for Tender
- Publication of the preliminary document
- Response file for the STAN4CR2 call
- European Commission meetings and consultations
- Submission of the NWI and establishment of the CEN TC224 WG17
- Update of the pre-standardization specification
- Publication of the CRA / standard training material
- **Fin du projet HESTIA**

Lot 1

Lot 2

Lot 3

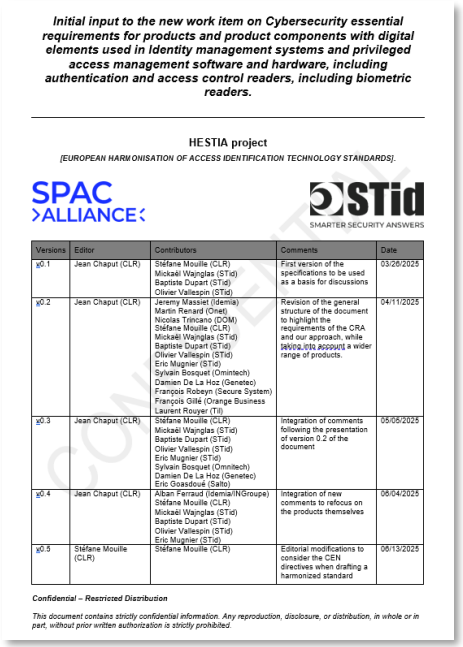
Lot 4

SPAC ALLIANCE

Livrables HESTIA

LOT 1
Summary document of requirements stemming from the CRA for Class 1 products

LOT 2
Pre-standardization technical specifications / Technical specifications document



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].

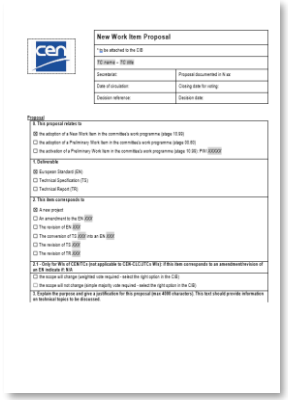
SPAC ALLIANCE — STid SMARTER SECURITY ANSWERS

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 (Orlet) Nicolas Trinicano (DOM) Stéfane Mouille (CLR) Mickaël Wajnglas (STid) Baptiste Dupart (STid) Olivier Vallespin (STid) Eric Mugnier (STid) Sylvain Bosquet (Omintech) Damien De La Hoz (Genetec) François Robeyn (Secure System) François Gillé (Orange Business Laurent Rouyer (TII)	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 Farraud (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	05/04/2025
v0.5	Stéfane Mouille (CLR)	Stéfane Mouille (CLR)	Editorial modifications to consider the CEN directives when drafting a harmonized standard	05/13/2025

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 and pre-standardization technical specifications included as annexes to the NWI



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
Training to understand the CRA requirements and harmonized standards

Working groups, guidelines, and activities

Guidelines for drafting the pre-standardization document

MONITORING OF FOUR TYPES OF REQUIREMENTS

CRA
Security & vulnerability management

EU checklist
For standards published in the OJEU

ANSSI requirements
Guidelines & frameworks

MARKET
x10 working groups

ANSSI requirements

Ex. 1	Ex. 2	Ex. 3	Ex. 4
Guidelines on securing physical access control and video surveillance systems + v2.2CSPN Protection Profile for access control systems	Note 7 - v2.0 + Note 9 – v1.0 + CER-P-02 Procedure	SOGIS Catalog + ANSSI cryptographic frameworks • RGS • Rules and recommendations for selecting and sizing cryptographic mechanisms • Guide for selecting cryptographic algorithms	ANSSI IT hygiene guide – v2.0 EBIOS Risk Manager (ISO/IEC 27005)

Working group activities (1/2)

Definition of the product scope

- Descriptions of access control and identity management subsystems
- List of affected products

Expansion of the product scope

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

Documentation development

- List of all source frameworks
- Document structure
- Requirements drafting

Work carried out and issues identified and addressed

- IT security, architecture, and functional process requirements kept out of scope
- Requirements initially oriented toward solutions and operated systems, then refocused on products
- Adaptation of ANSSI high-security requirements to market needs and use cases
- Development of requirements designed to overlap with existing standards in order to:
  - optimize overall requirements consistency
  - facilitate and accelerate market compliance

⇒ Alignment with ISO/IEC 62443-4 (IACS)

Working group activities (2/2)

Definition of security profiles

- Basic, substantial, high

Implementation of a dedicated methodology

- Identification of “intended purposes” and reasonably foreseeable use
- Risk analysis based on recognized frameworks and standards (ISO 31073:2022, ISO/IEC 27005, EU Risk Management Framework, ANSSI’s EBIOS Risk Manager
- Definition of security profiles based on ANSSI’s OASIS tool

Issue outside the scope of the standard but important for the market

- Ongoing work: how to enable integrators, installers, and end users to easily ensure that a CRA-compliant product, certified at basic, substantial, or high profile levels, is well suited to real-world use cases.

NEXT STEPS OF THE HESTIA PROJECT

CEN TC224 WG17

SPAC ALLIANCE

Les suites du projet HESTIA (Phase 2)

PHASE 2

Juil. – Déc. 25

Janv. – Oct.26

CEN TC224 WG17

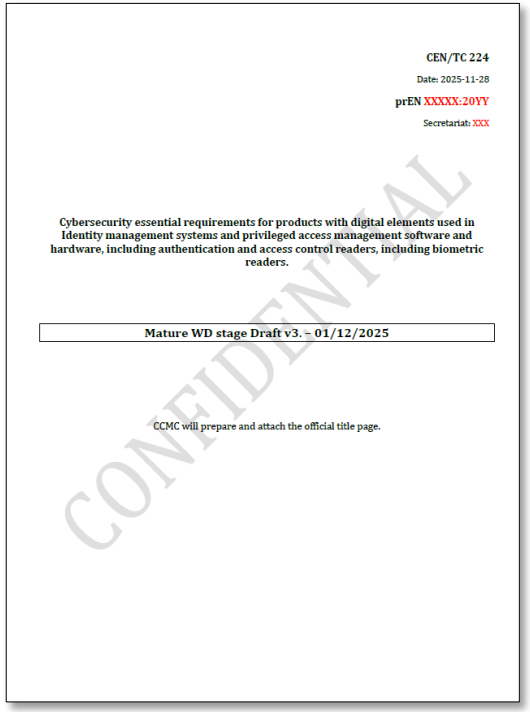
- Request for STid's integration into CEN TC 224WG 17 via AFNOR
- **Submission of the NWI and establishment of the CEN TC224 WG17**
- Validation of the NWI
- First compliance audit draft template
- Submission of the first Mature Draft to the European Commission's HAS Consultant
- First feedback from the EC's HAS Consultant
- Rapporteur Meeting
- Meeting Rapporteur
- Updated draft submission
- Rapporteur Meeting
- Rapporteur Meeting
- Rapporteur Meeting
- Final submission of comments
- **Publication de la norme #16**

Drafting work on the standard within CEN TC224 WG17 / weekly meetings

Monitoring and contributions within the HESTIA working groups / bi-monthly meetings

Deliverables produced within the CEN TC 224 WG17 working group

Mature Working Draft – v3



CEN/TC 224

Date: 2025-11-28

prEN XXXXX:20YY

Secretariat: XXX

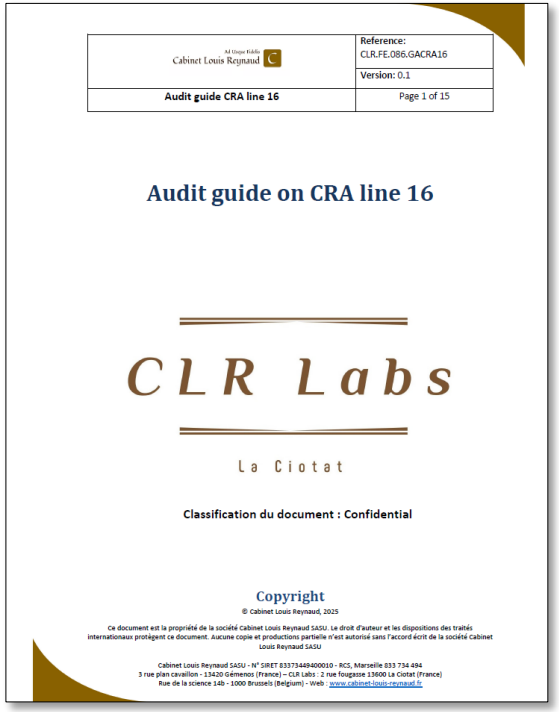
Cybersecurity essential requirements for products with digital elements used in Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers.

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 cavallon - 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

Thank you !!!