Evropské certifikace kybernetické bezpečnosti

webinář

Digitální Česko

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Úřad vlády České republiky

13. června 2023

TLP: CLEAR

Evropské certifikace kybernetické bezpečnosti

Program:

1.	13:00 – 13:05	Organizační pokyny (NÚKIB, M. Šilhavá)
2.	13:05 – 13:15	Úvodní slovo (MMR, O. Profant; NÚKIB, A. Kučínský)
3.	13:15 – 13:30	Změna CSA: certifikace řízených bezpečnostních služeb (NÚKIB, A. Botek)
4.	13:30 – 13:50	ENISA work update: Cybersecurity Certification Schemes development (ENISA, P. Blot, AJ*)
5.	13:50 – 14:20	NXP Certification strategy and how it aligns with EU Cybersecurity Regulations (NXP, J. Boggie, AJ*)
6.	14:20 – 14:35	Certifikácia kyberbezpečnosti podľa európskych schém v podmienkach SR (SK NBÚ, M. Senčák, SJ*)
7.	14:35 – 15:00	Návrh Aktu o kybernetické odolnosti (NÚKIB, A. Botek)
8.	15:00 – 15:20	Představení činností NKC a možnosti financování z programu DEP Kyberbezpečnost (NÚKIB, N. Chvátalová)
9.	15:20 – 16:00	Networking (prostor pro navázání kontaktů volnou formou)
10.	16:00	Závěr

Evropské certifikace kybernetické bezpečnosti

Organizační pokyny

- Celý webinář nahráváme.
  Nahrávka bude zveřejněna na našem kanále Youtube a na našich webových stránkách eucertifikace.nukib.cz
- Prezentace budou zveřejněny na našich webových stránkách uvedených výše.
- V průběhu webináře neplánujeme přestávku.
- Dotazy je možné klást v průběhu prezentací v chatu a po každé z prezentací.
- Některé prezentace jsou vedeny v jiném než českém jazyce. Prosíme, respektujte toto nastavení v rámci případné diskuze.
- Prosím, vypněte si kamery a mikrofony, pokud nemluvíte k účastníkům.

ÚVODNÍ SLOVO

ONDŘEJ PROFANT

náměstek

Ministerstvo pro místní rozvoj

ÚVODNÍ SLOVO

ADAM KUČÍNSKÝ

ředitel odboru regulace
Národní úřad pro kybernetickou a informační bezpečnost

ZMĚNA CSA: CERTIFIKACE ŘÍZENÝCH BEZPEČNOSTNÍCH SLUŽEB

ADAM BOTEK

vedoucí oddělení multilaterální spolupráce I

Národní úřad pro kybernetickou a informační bezpečnost

Návrh změny CSA: certifikace řízených bezpečnostních služeb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

13. června 2023

Adam Botek

❖ Rozšíření působnosti Aktu

V současnosti se CSA vztahuje jen na ICT produkty, služby a procesy

-> umožnění certifikace řízených bezpečnostních služeb

❖ Stanovení nových bezpečnostních cílů certifikačních schémat pro ŘBS

Řízená bezpečnostní služba

- *služba spočívající v provádění nebo poskytovaní asistence při aktivitách vztahujících se k řízení kyberbezpečnostních rizik, včetně reakce na incidenty, penetračního testování, bezpečnostních auditů a konzultantství*

- ≠ ICT služba: *služba spočívající plně nebo převážně v přenosu, ukládání, získávání či zpracovávání informací prostřednictvím sítí a informačních systémů*

Bezpečnostní cíle schémat pro ŘBS

- Náležitá kompetentnost, expertíza a zkušenost při poskytování služeb, včetně technických znalostí a profesionální integrity zaměstnanců
- Interní procedury k zajištění stálého poskytování služeb ve velmi vysoké kvalitě
- …ochrana dat, používání bezpečných produktů, služeb, procesů

Přínosy

- Vytvoření důvěry v kvalitu řízených bezpečnostních služeb
- Podpora rozvoje důvěryhodných evropských poskytovatelů kyberbezpečnostních služeb
- Usnadnění implementace unijních a národních předpisů v oblasti kybernetické bezpečnosti
- NIS2 (ZKB), návrh Aktu o kybernetické solidaritě (kyberbezpečnostní rezerva)

Kyberbezpečnostní rezerva (Akt o kybernetické solidaritě)

- Zahrnuje služby spočívající v reakci na rozsáhlé incidenty poskytované ze strany důvěryhodných poskytovatelů

- Výběrová kritéria důvěryhodných poskytovatelů:

  - *Certifikace podle schématu CSA pro BŘS*
  - *…*

Adam Botek

E-mail: adam.botek@nukib.cz

ENISA WORK UPDATE: CYBERSECURITY CERTIFICATION SCHEMES DEVELOPMENT

PHILIPPE BLOT

Head of Cybersecurity Certification Sector, Market, Certification and Standardisation Unit

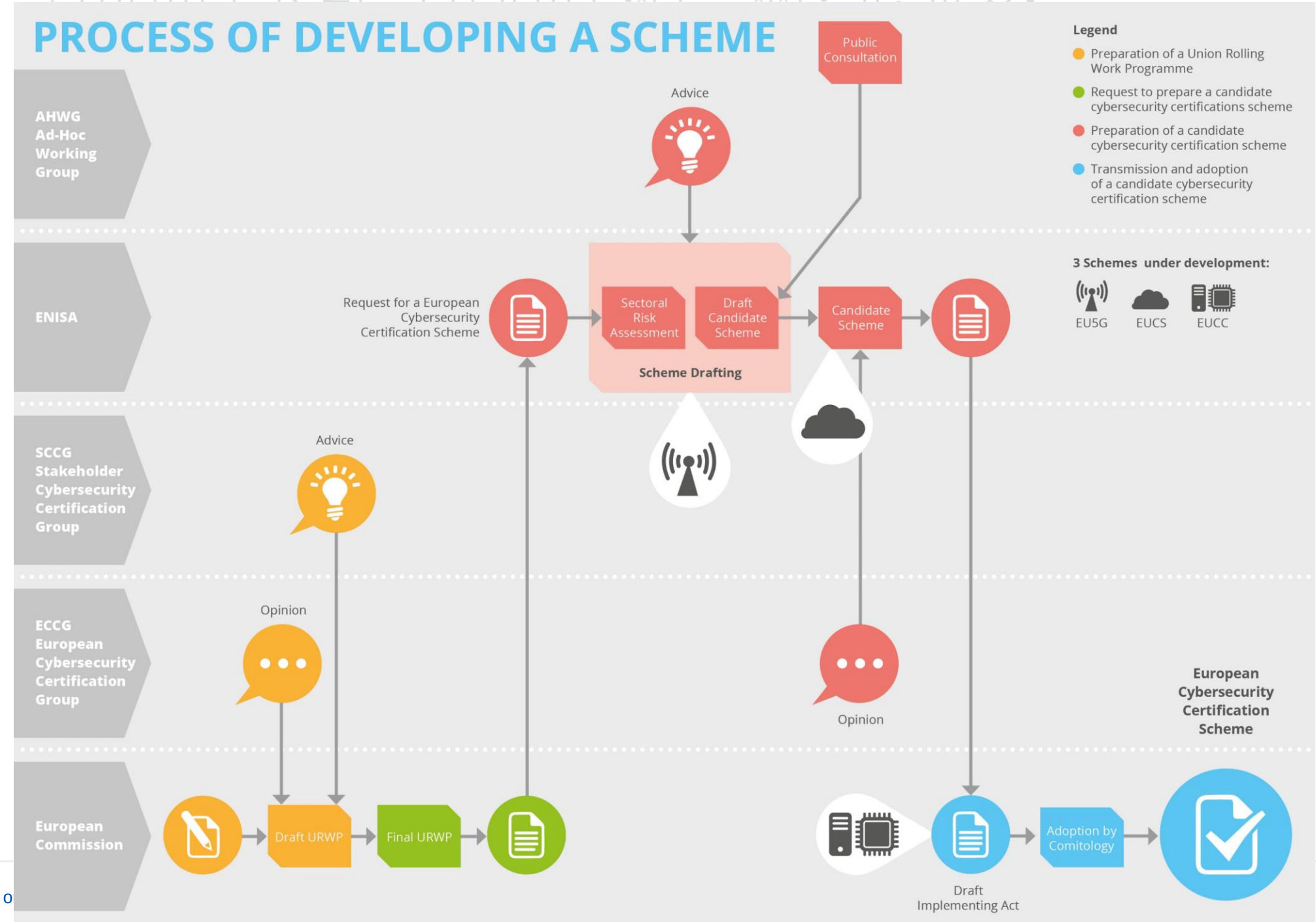
European Union Agency for Cybersecurity

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AN UPDATE ON SCHEMES DEVELOPMENTS

Philippe Blot
Head of Cybersecurity Certification sector
Market, Certification & Standardisation Unit

02 | 06 | 2023


PROCESS OF DEVELOPING A SCHEME
AHWG Ad-Hoc Working Group
ENISA
SCCG Stakeholder Cybersecurity Certification Group
ECCG European Cybersecurity Certification Group
European Commission
Public Consultation
Advice
Request for a European Cybersecurity Certification Scheme
Sectoral Risk Assessment
Draft Candidate Scheme
Scheme Drafting
Candidate Scheme
Legend
Preparation of a Union Rolling Work Programme
Request to prepare a candidate cybersecurity certifications scheme
Preparation of a candidate cybersecurity certification scheme
Transmission and adoption of a candidate cybersecurity certification scheme
3 Schemes under development:
EU5G
EUCS
EUCC
Advice
Opinion
Opinion
Draft URWP
Final URWP
Draft Implementing Act
Adoption by Comitology
European Cybersecurity Certification Scheme

CURRENT ACTIVITIES ON EUCC

- **Implementing Act (ENISA support to the EC) based on the candidate scheme**
- **Maintenance strategy**
- **Catalogue of national supporting documents (a lot of them!)**
- **ENISA website dedicated to certification**
- **Cryptography**

OTHER ACTIVITIES IN LIAISON WITH EUCC

EU5G: will reuse EUCC for eUICC certification

eIDAS/wallet and CRA: may mandate EUCC certification or reuse EUCC certificates as a presumption of conformity

AI feasibility: will analyse how to reuse EUCC certification

CURRENT ACTIVITIES ON EUCS

- **CEN-CENELEC is making progress on the elements passed by ENISA (security controls) for their transformation and maintenance into Technical Specifications**

- **Guidance development has been launched**

- **The discussion at ECCG has been re-engaged**

CURRENT ACTIVITIES ON EU5G

- **Based on the outcome of phase 1, and the launch of phase 2, ENISA plans a first draft of the scheme to be available for public review in 23**

- **The AHWG supporting ENISA has been maintained for phase 2, it is composed of a rich representation of relevant stakeholders (in total around 100 participants):**
  - **eUICC and network products developers**
  - **CABs**
  - **MNOs**
  - **standardisation organisations**
  - **national authorities both telco and cybersecurity regulators**

CURRENT ACTIVITIES ON EU5G

- **The scheme will be organized into 3 different components:**
  - **eUICC certification will be based on the EUCC scheme with the appropriate Protection Profile(s) to allow also convergence with the eIDAS/wallet**
  - **Existing GSMA/3GPP schemes and structures on NESAS will be transformed into a relevant EU scheme, reusing the lessons learned from BSI implementation**
  - **SAS processes on SIM provisioning and eUICC secure development will be transformed to the possible extend into a relevant EU scheme, in close relation with the eUICC certification strategy**

CURRENT ACTIVITIES ON EU5G

- **GSMA has engaged into publishing their documentation through ETSI**
- **ENISA is investigating the different options to get the necessary influence at 3GPP**

CURRENT ACTIVITIES ON EU5G

- **We have set up a dedicated Thematic group for future version(s) of the scheme, including Open-RAN, virtualisation and roaming security functionalities; a link with the Cloud scheme might make sense**

- **We will soon start developing accreditation requirements (specific where necessary), in cooperation with EA**

More to learn on the progress of ENISA's developments in certification at the ENISA Cybersecurity Certification Conference, on May 25th!

And also: we have now a website dedicated to certification

Cybersecurity Certification (europa.eu)

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

certification@enisa.europa.eu

www.enisa.europa.eu

NXP CERTIFICATION STRATEGY AND HOW IT ALIGNS WITH EU CYBERSECURITY REGULATIONS

JOHN BOGGIE

Senior Director, Head of Cybersecurity Certification
NXP Semiconductors

NXP CERTIFICATION STRATEGY AND EU CYBERSECURITY LEGISLATION

John BOGGIE
Senior Director, Head of Cybersecurity Certification

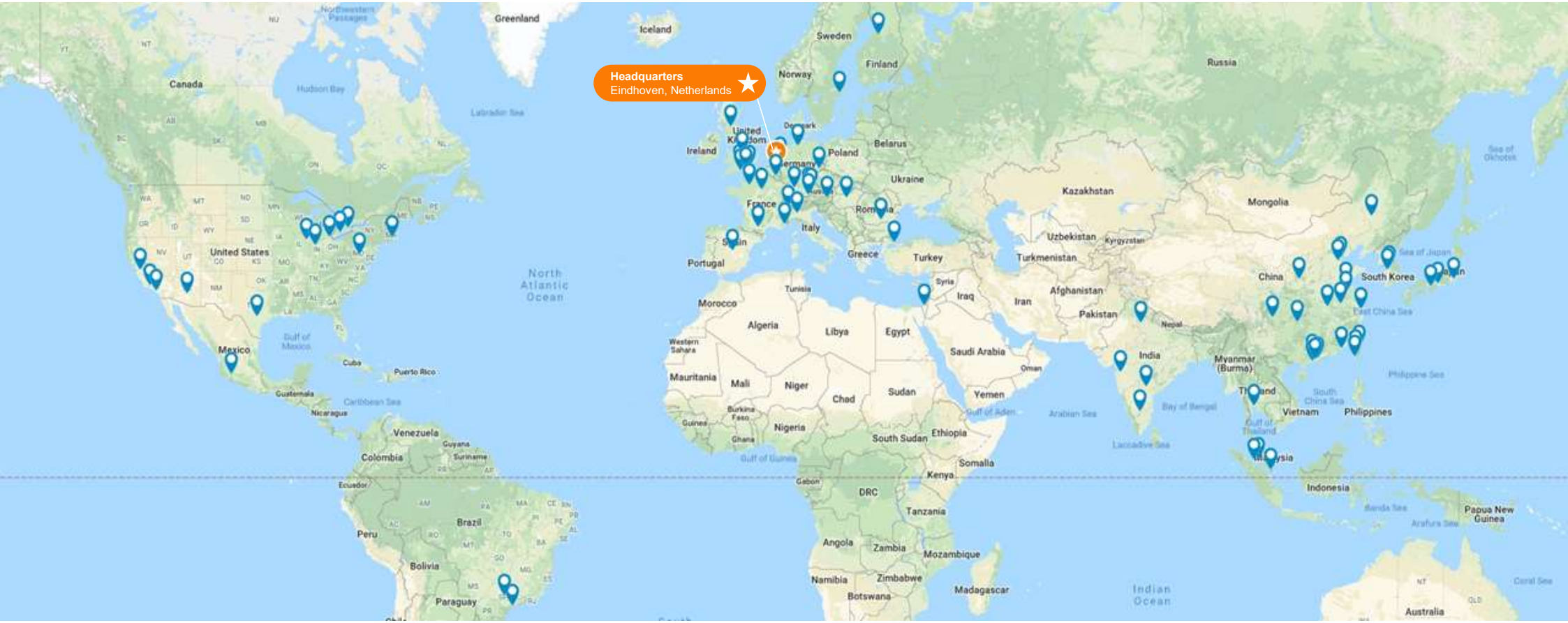
Competence Centre Cryptography and Security
CTO NXP Semiconductors Scotland

JUNE 2023

SECURE CONNECTIONS FOR A SMARTER WORLD

NXP SEMICONDUCTORS

~30,000 employees with operations in more than 30 countries

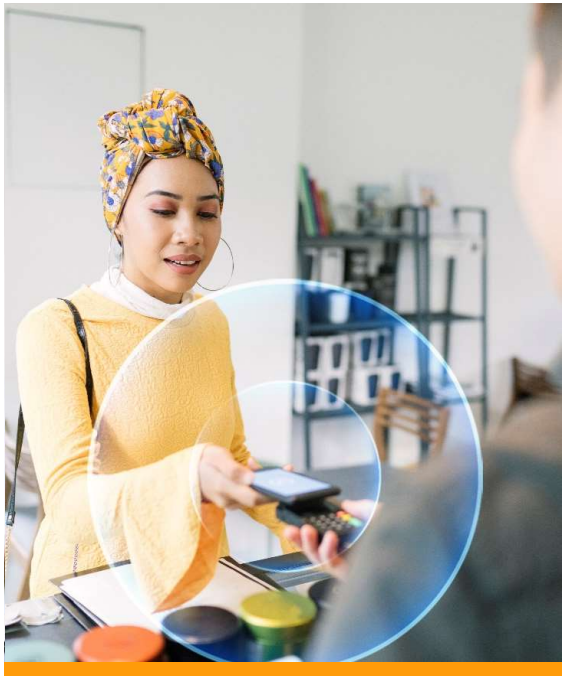


OUR TARGET MARKETS

AUTOMOTIVE

INDUSTRIAL & IOT

MOBILE



COMMUNICATION INFRASTRUCTURE

EVERYTHING CONNECTED

SENSE

THINK

ACT

The Importance of Security

SECURE CONNECTIONS
FOR A SMARTER WORLD

There are billions of connected devices and systems worldwide

Every part of the system is potentially vulnerable to hacking

ATTACK PATHS

LOGICAL
By sending malicious messages, the software will misbehave.

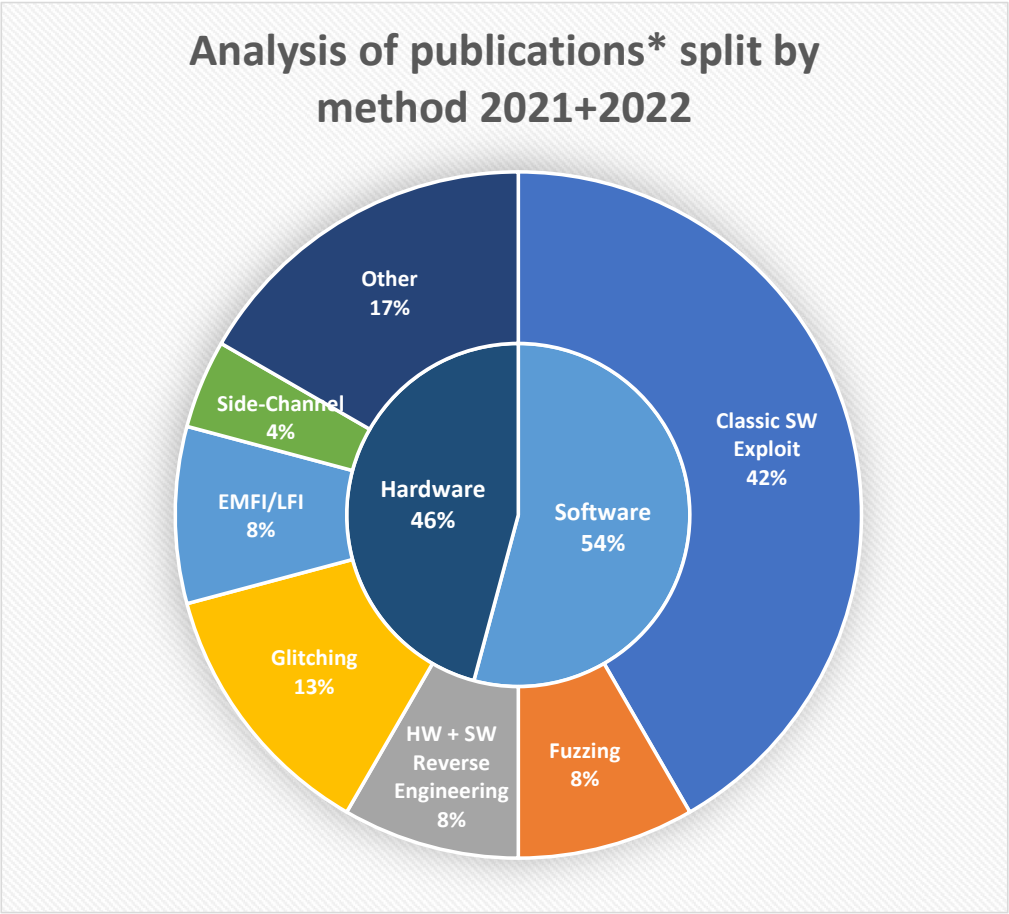
PHYSICAL
Making use of physical properties or deficiencies in the device.

LOCAL
Adversary must be in the proximity of the device.

REMOTE
Adversary can be anywhere. And also mount remote- physical attacks.

ATTACK LANDSCAPE EMBEDDED & IOT

- Published attacks shows the relevance of hardware and software attacks
- Static analysis and fuzzing dominant in the SW sphere
- A lot of glitching attacks in the HW area
- Both areas skew towards cheaper tooling and low-cost attacks

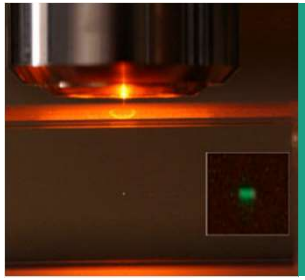


*Publications/Conferences surveilled by CCCS and selected on impact to NXP product portfolio and general quality (no network security threats considered)

ATTACK ARE ALSO EVOLVING

ML assisted attacks

- ❑ ***Side-Channel analysis***
  - Identification of regions of interest
  - Leakage analysis and exploit testing
- ❑ ***Fuzzing***
  - Automated search optimization and exploit building
- ❑ ***Reverse Engineering***
  - Cell and Trace identification in invasive hardware reverse engineering
  - OP-code identification via side-channel signal



New Tools and Methods

- ❑ ***Two-Photon Laser Fault Injection***
- ❑ ***Multi-Shot Electromagnetic Fault Injection***
- ❑ ***Statistical Ineffective Fault Analysis***
- ❑ ***Combined HW attacks***

Micro-Architectural Attacks

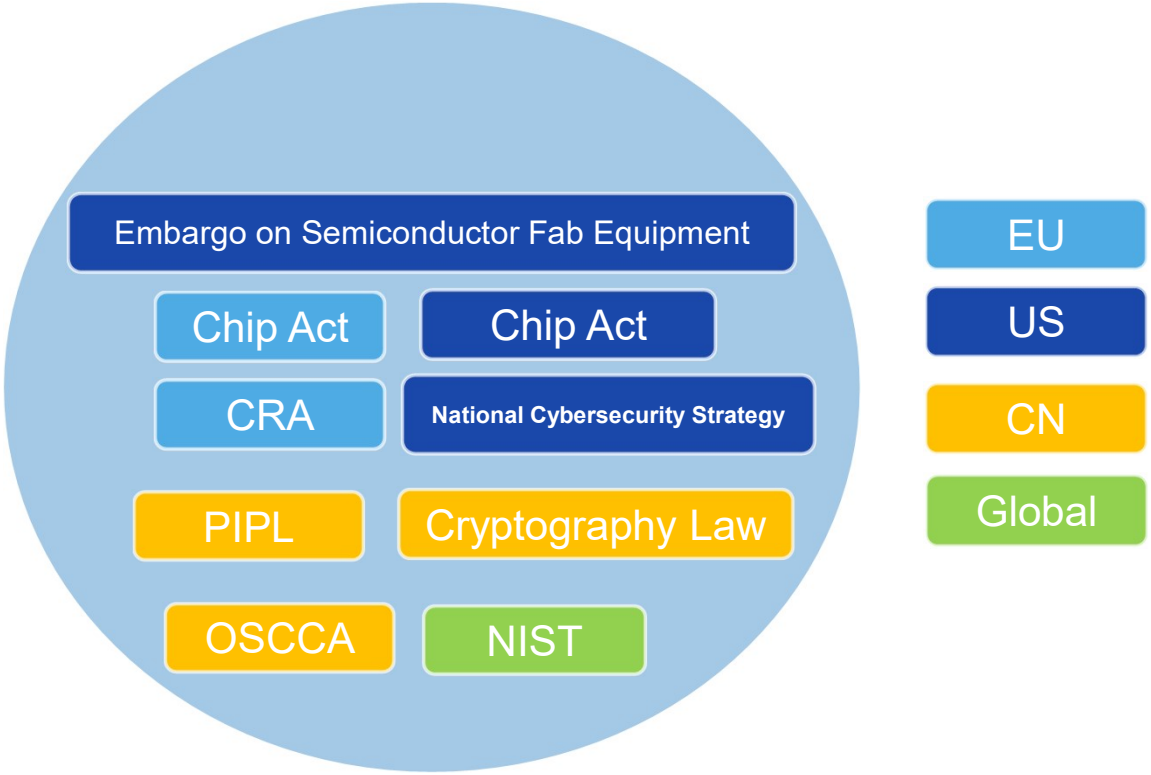
- ❑ ***Often used combinations are V-Glitch → Reverse Engineering → Logical attack***
- ❑ ***Reverse engineering can be replaced by ML / Fuzz tools making the exploit chain more automated***

Legislation and Regulations

SECURE CONNECTIONS
FOR A SMARTER WORLD

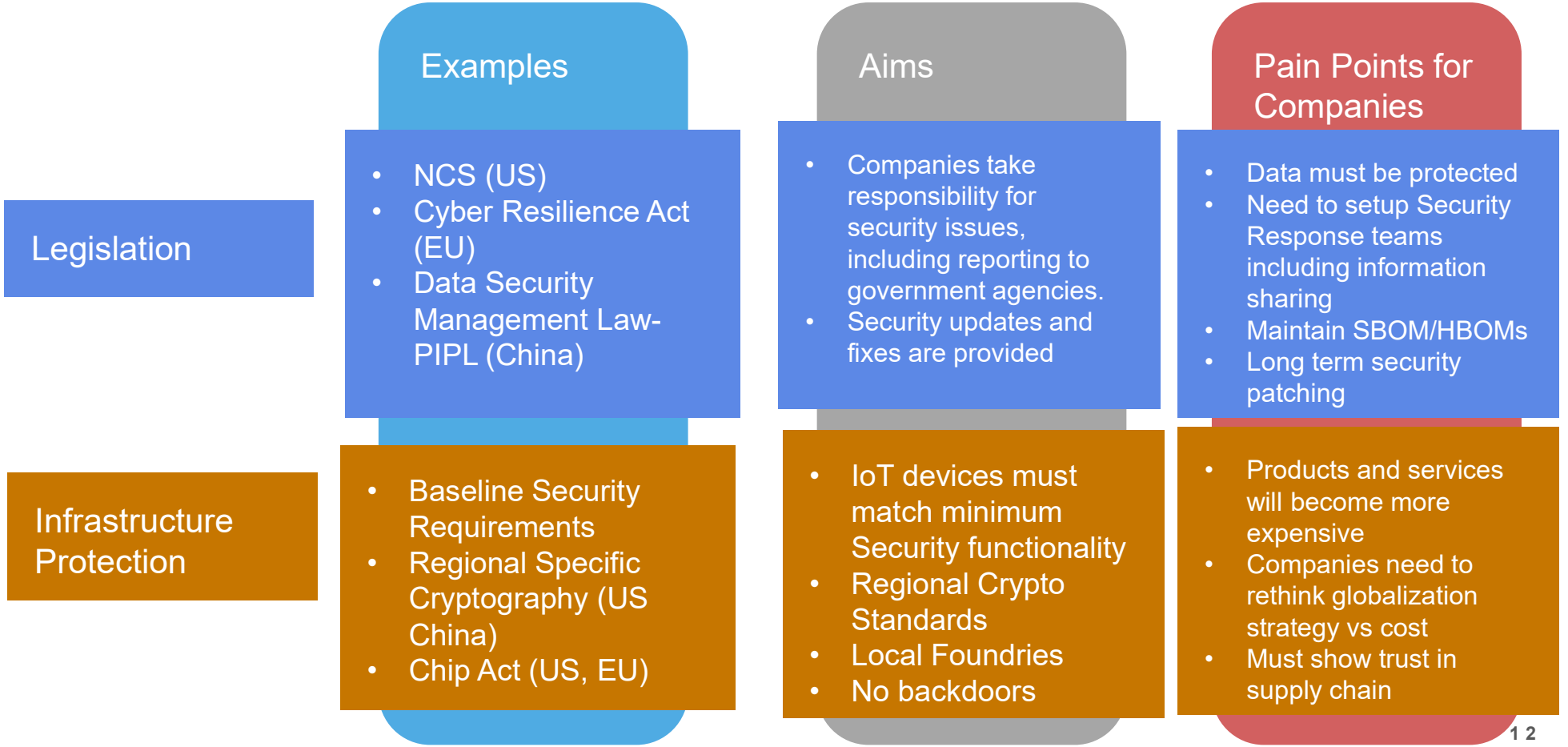
GEOPOLITICAL LANDSCAPE AND LEGISLATION SEMICONDUCTOR VIEW

- COVID caused issues with supply chains
- Chips became a strategic asset (Chip Act)
- Also global tensions led to a rise in cyber attacks (CRA, NCS)
- Local Legislation was written to enhance cyber resilience (CRA, NCS, NIS)
- Mandatory local standards lead to complexity and trade barriers (NIST, OSCCA)
- In US and EU mandatory certifications are being put in place (CSA, IoT Labelling, etc.)

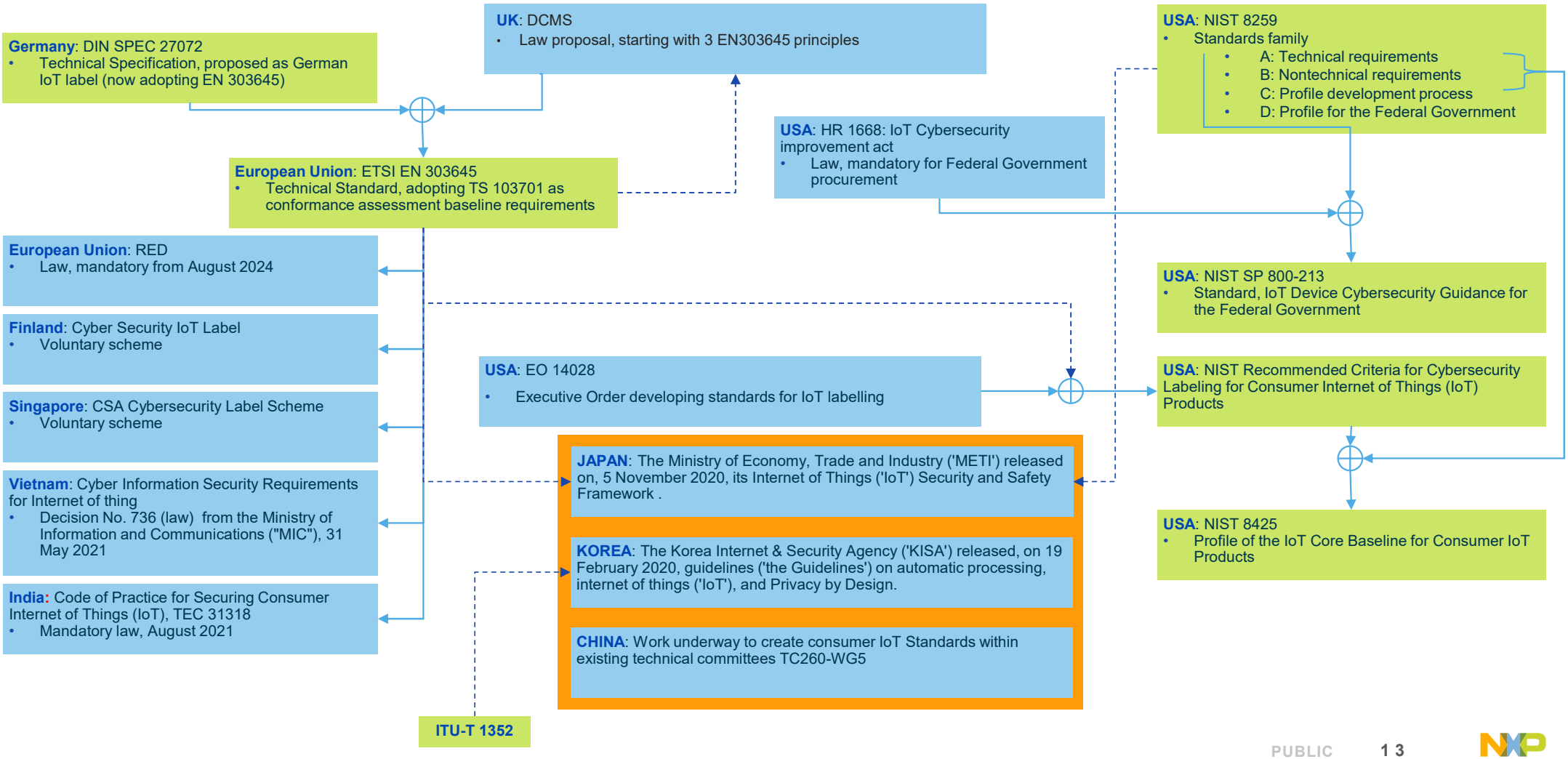


LEGISLATION

- Legislation is rapidly being put in place- there is though commonality



IMAGINE YOU ARE A CONSUMER IOT DEVELOPER – THIS IS THE COMPLEXITY



NXP Certification Strategy

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP IS RECOGNIZED FOR SECURITY ACROSS MANY MARKETS

PRODUCTS
Discrete and integrated solutions to meet customer needs

SUPPORT
NXP and partner ecosystem support for end-to-end security

PROCESS
Security-by-design is integral to how we operate

COMPLIANCE
Products designed to meet relevant industry standards

WHAT IS OUR CERTIFICATION MISSION

Mission: To ensure that we have all the certifications required to match our product markets:

- Compliance to sectorial standards
- Compliance to geographical regulations
- Proof of trusted solutions and services
- Differentiation on security features and innovation

Benefit of Certification

- Proof that NXP is a trusted supplier
- Proof that NXP follows Security by design principles

Trusted Supply Chains

Security by Design

THE NXP HOLISTIC CERTIFICATION STRATEGY – PROVIDING PROOF OF TRUST

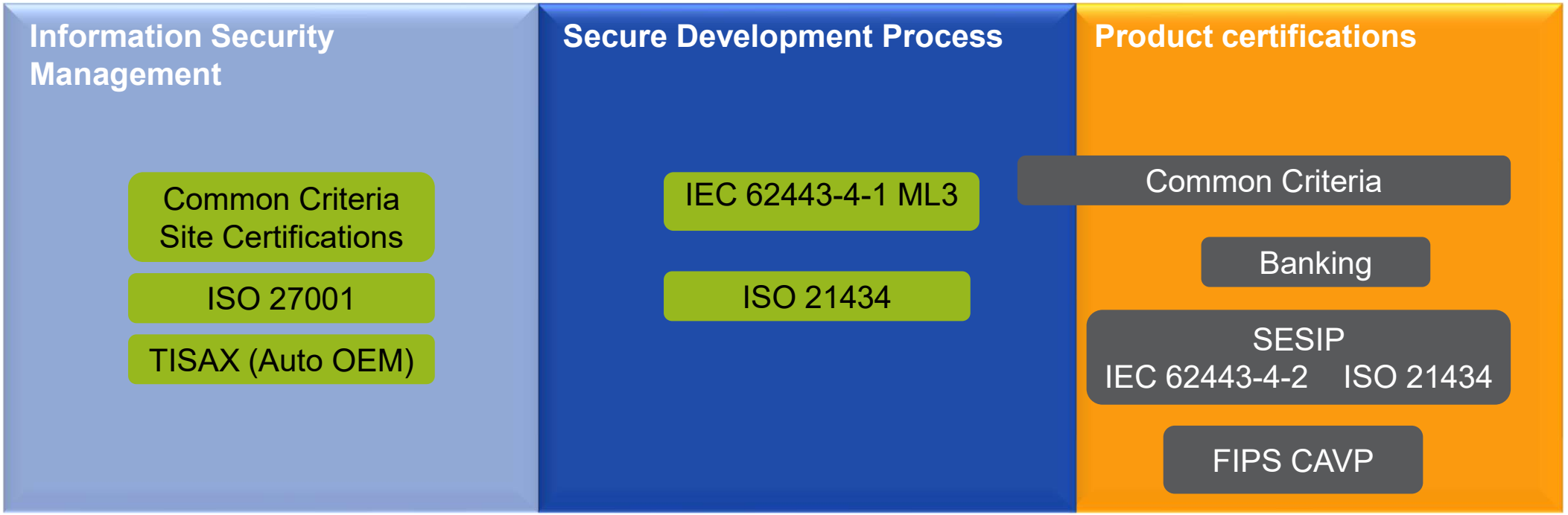
Information Security Management	Secure Development Process	Product Certifications
Certify the Security philosophy of the company how we protect IP and data (both NXP and Customer), deal with security incidents, etc.	Ensure that we develop security products with a focus on security embracing concepts like security by design, ensure development process controls and security audits are in place.	Security testing and conformity testing of our end products.
Concept • Security mindset	Concept • Security focused processes and procedures	Concept • Secure solutions

Trusted Supply Chains

Security by Design

We drive a holistic approach and cover all 3 types of certifications providing proof points for customers and stakeholders

USING GLOBAL STANDARDS



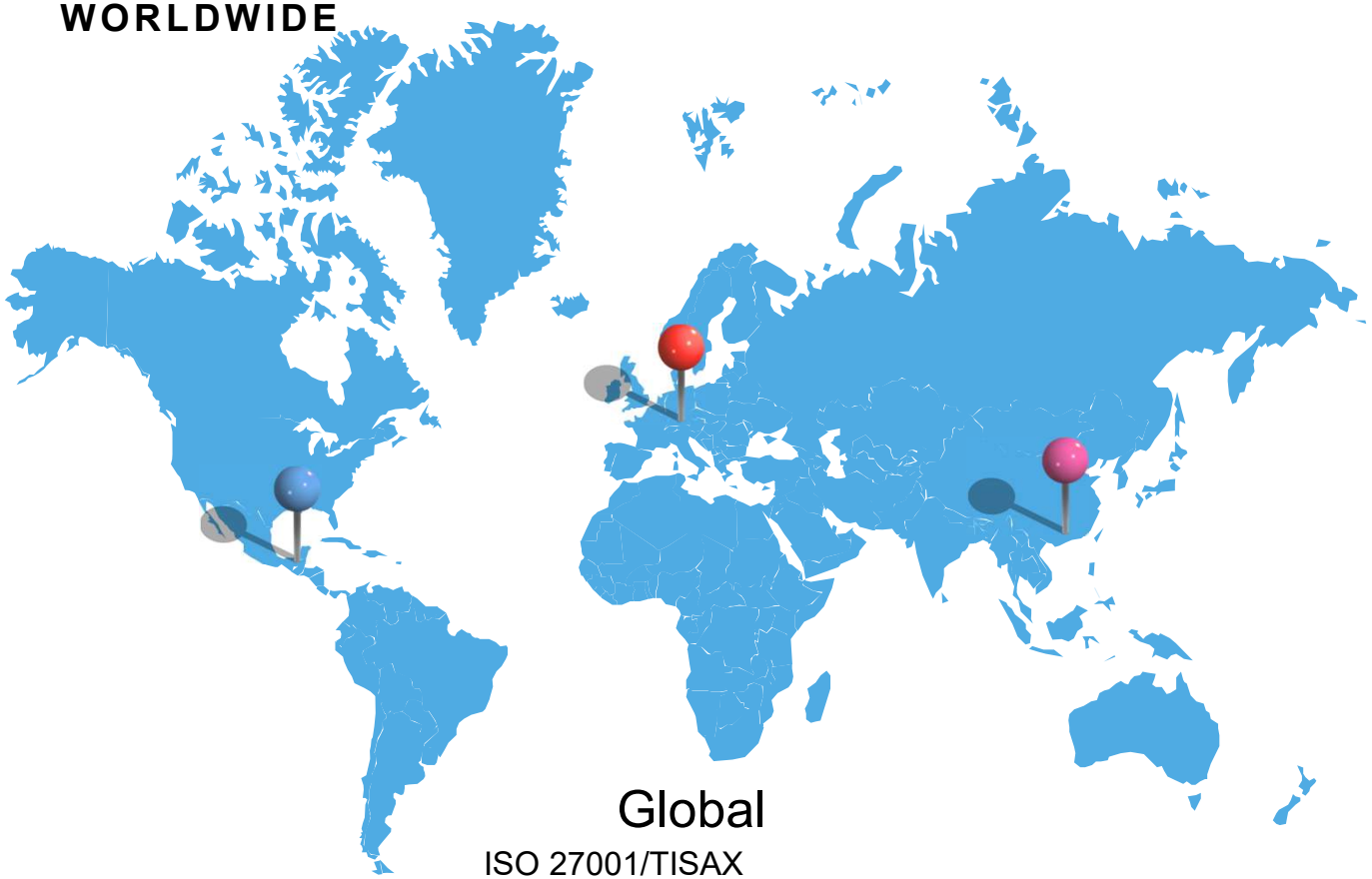
300+ product certifications per year

All NXP locations covered + key external supply chain partners

Security Development Process deployed and used

Certification linked to EdgeLock classification

NXP CERTIFIES WORLDWIDE – AND SUPPORTS LEGISLATION WORLDWIDE



Global

ISO 27001/TISAX
ISO 21434
Common Criteria (Government/Commercial)
EMVCo (Banking)
SESIP (EN-17927)
GSMA (Telecoms)
Global Platform (Standardization)

Americas

FIPS 140-2 (USA/Canada) (Government)
CAVP (USA/Canada) (Government)
SESIP (EN-17927)
Mastercard/Amex/Visa/Interac etc. (Banking)
ICP (Brazil) (Government)

EMEA

Common Criteria (ISO15408) (Government/Commercial)
EMVCo
IEC 62443
ARM PSA
SESIP (EN-17927)
MiFare

APAC

OSCCA (Government/Commercial)
Japan Banking
Malaysian Banking
NFTC (China Mobile Banking)
PBOC/CUP (Banking)
MOT (Ministry of Transport china)
TAF (Telecoms China)
FeliCa Networks (Japan)

NXP and Composition

SECURE CONNECTIONS
FOR A SMARTER WORLD

IoT Application
Sensors, data analysis, …

IoT Platform

Other Software
OS, drivers and connectivity, …

Security Services
TF-M, Services, …

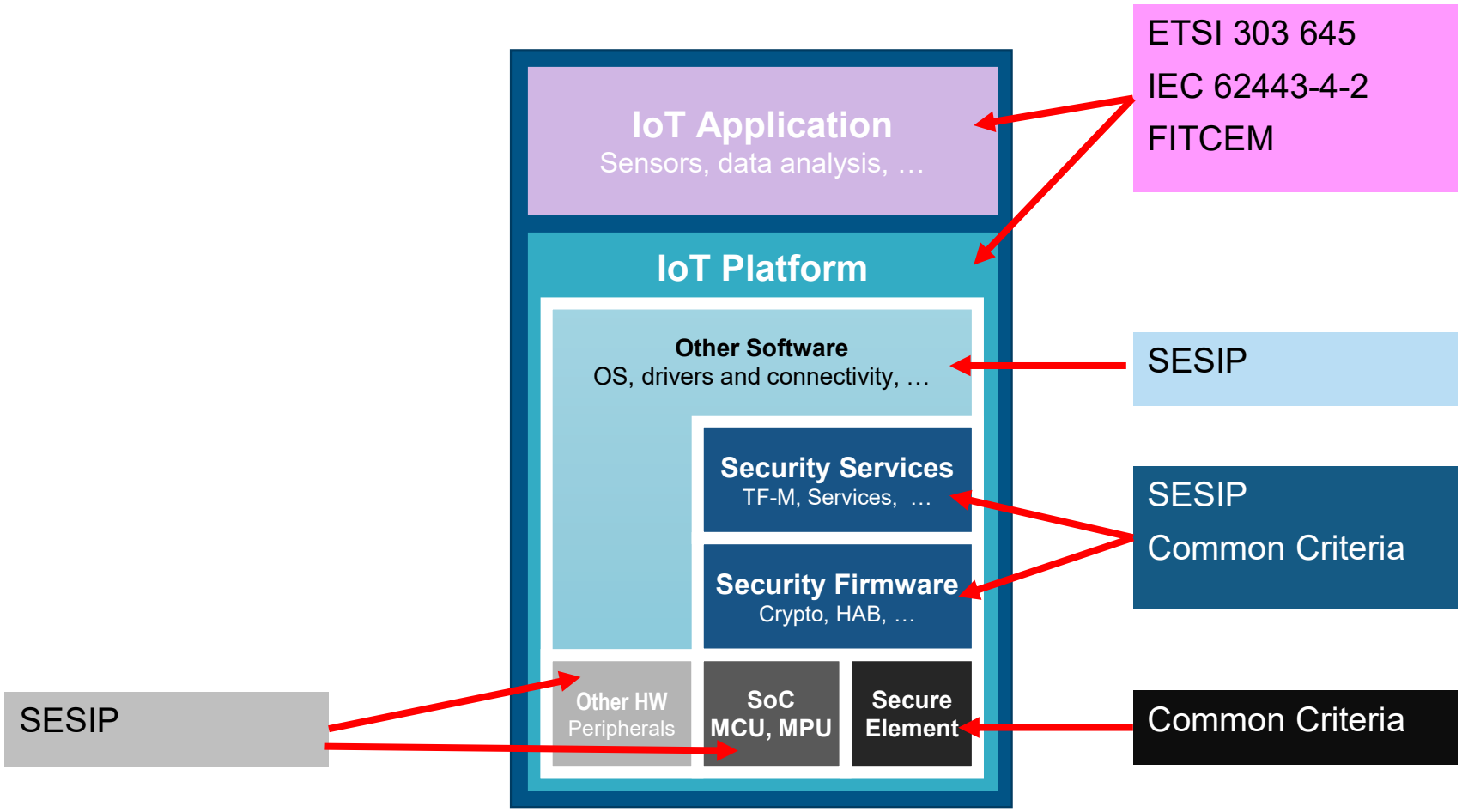
Security Firmware
Crypto, HAB, …

Other HW
Peripherals

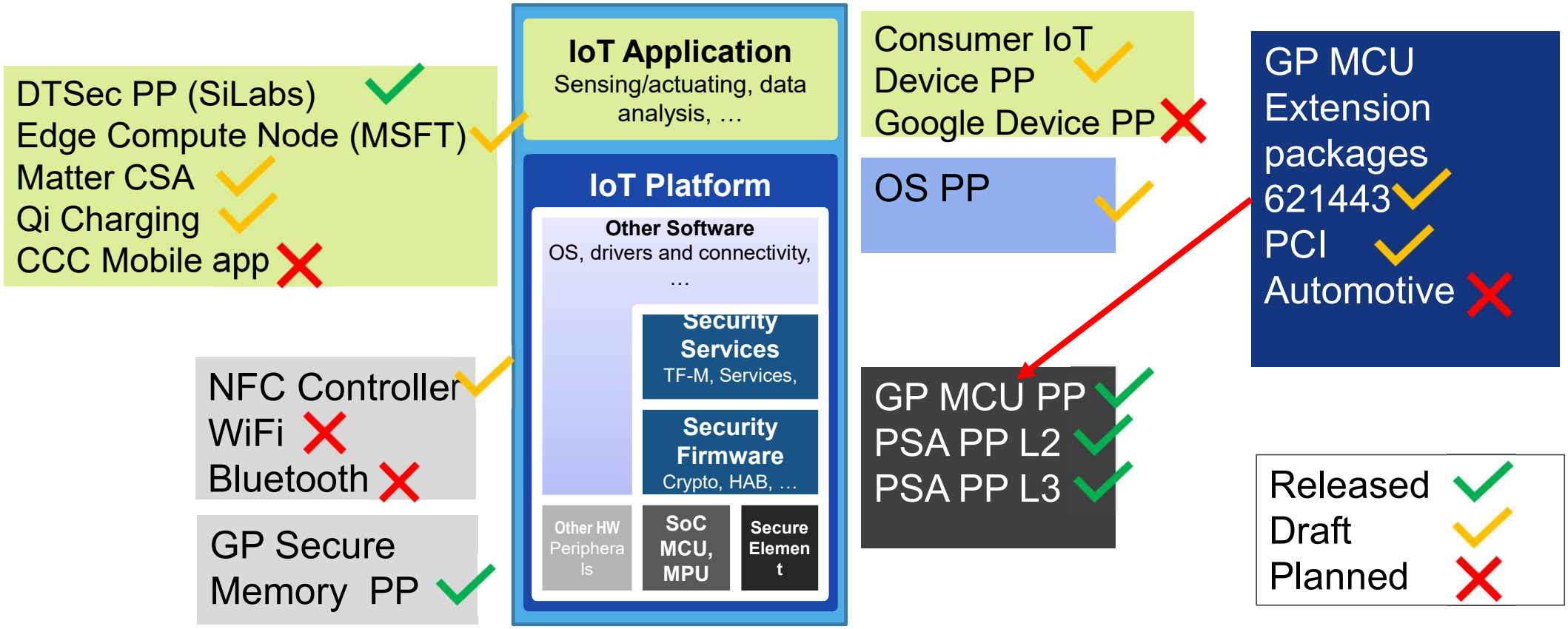
SoC
MCU, MPU

Secure
Element

CERTIFYING AN IOT PRODUCT USING VARIOUS STANDARDS



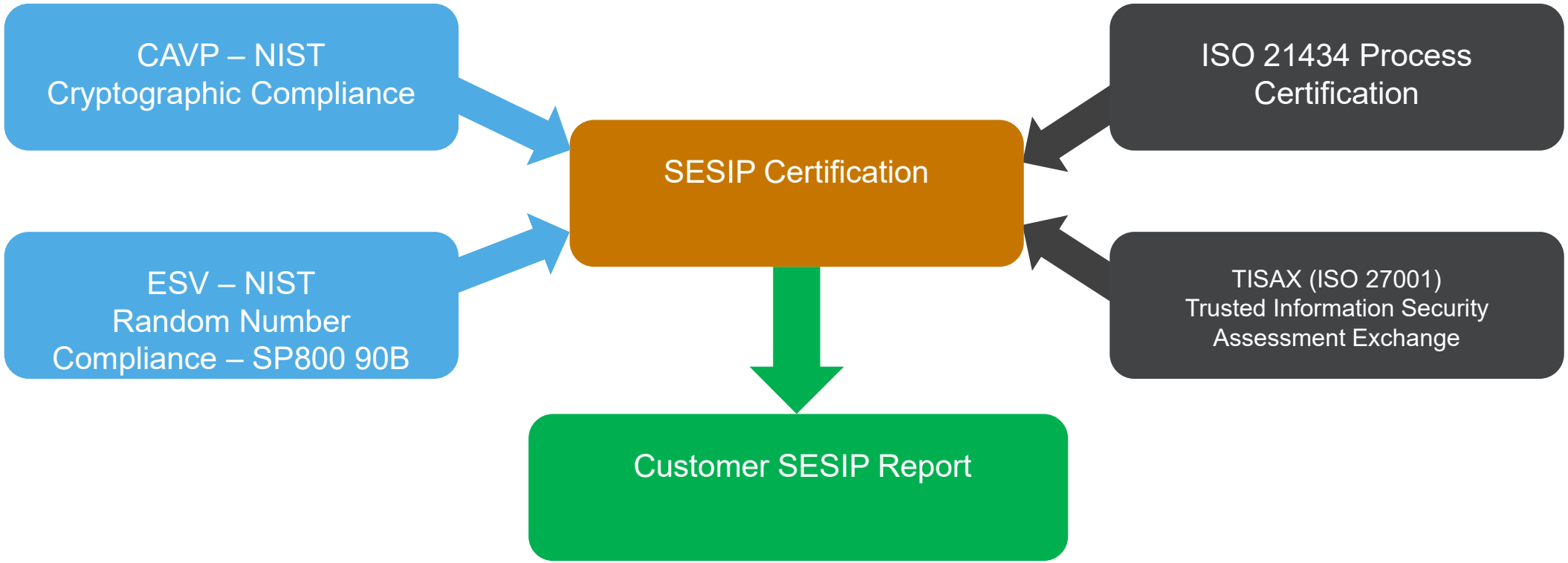
SESIP (EN 17927) PROTECTION PROFILES



Automotive Chip using EN 17927 (SESIP)

SECURE CONNECTIONS
FOR A SMARTER WORLD

AUTOMOTIVE NXP CERTIFICATIONS –SESIP PROVIDES A PROOF POINT FOR THE OTHER CERTIFICATION STANDARDS



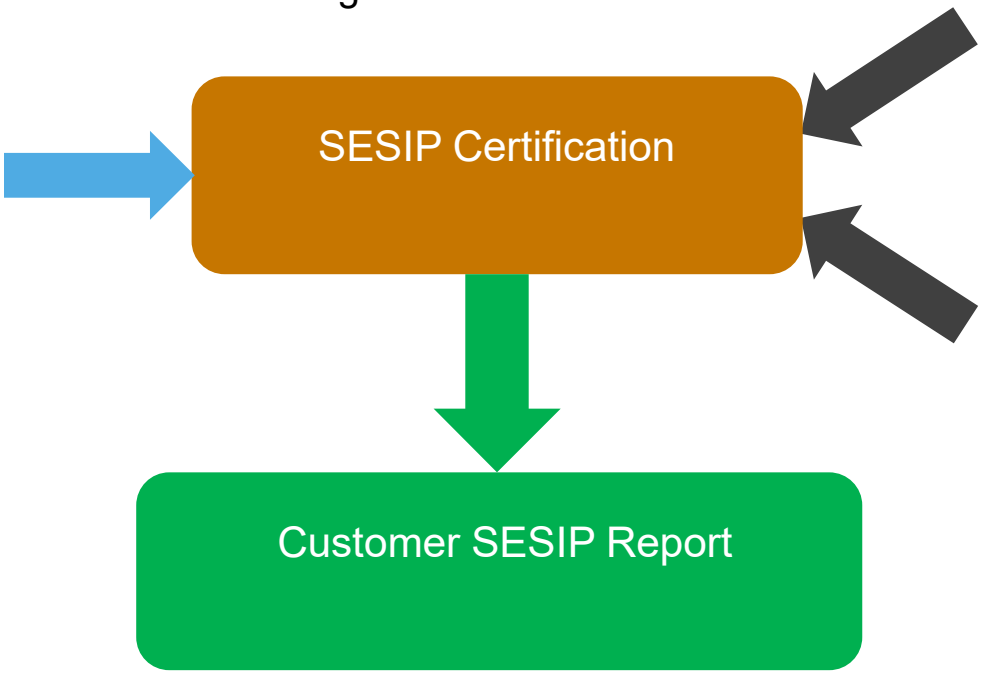
AUTOMOTIVE NXP CERTIFICATIONS – WHAT THE SESIP CERTIFICATE COVERS

Certificates proving that the Cryptography is implemented correctly

Proof that the random number generator complies to a industry standard

Certificates provided by US Government

The Device has been defined using a common threat model detail how it mitigates these threats.

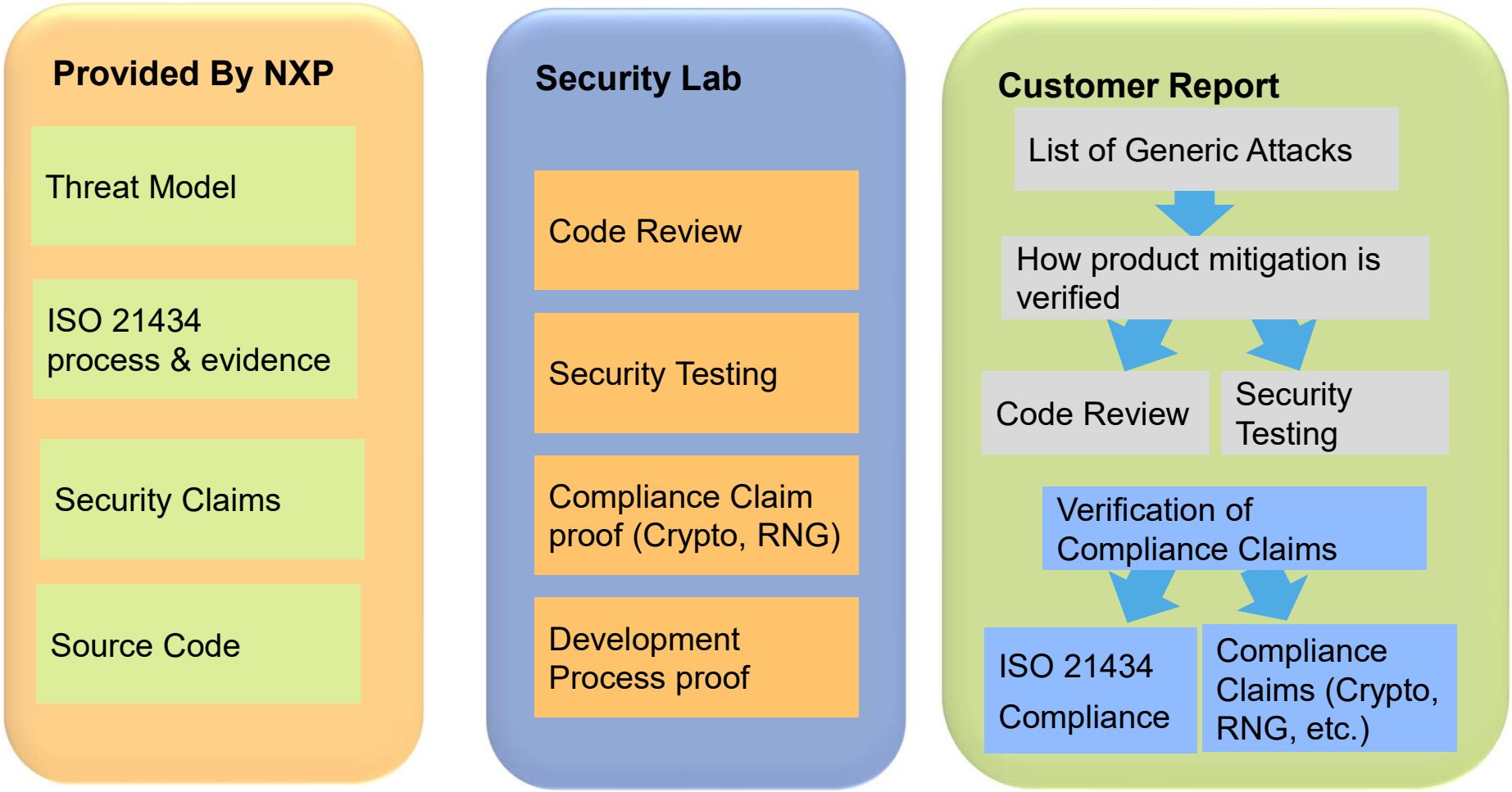


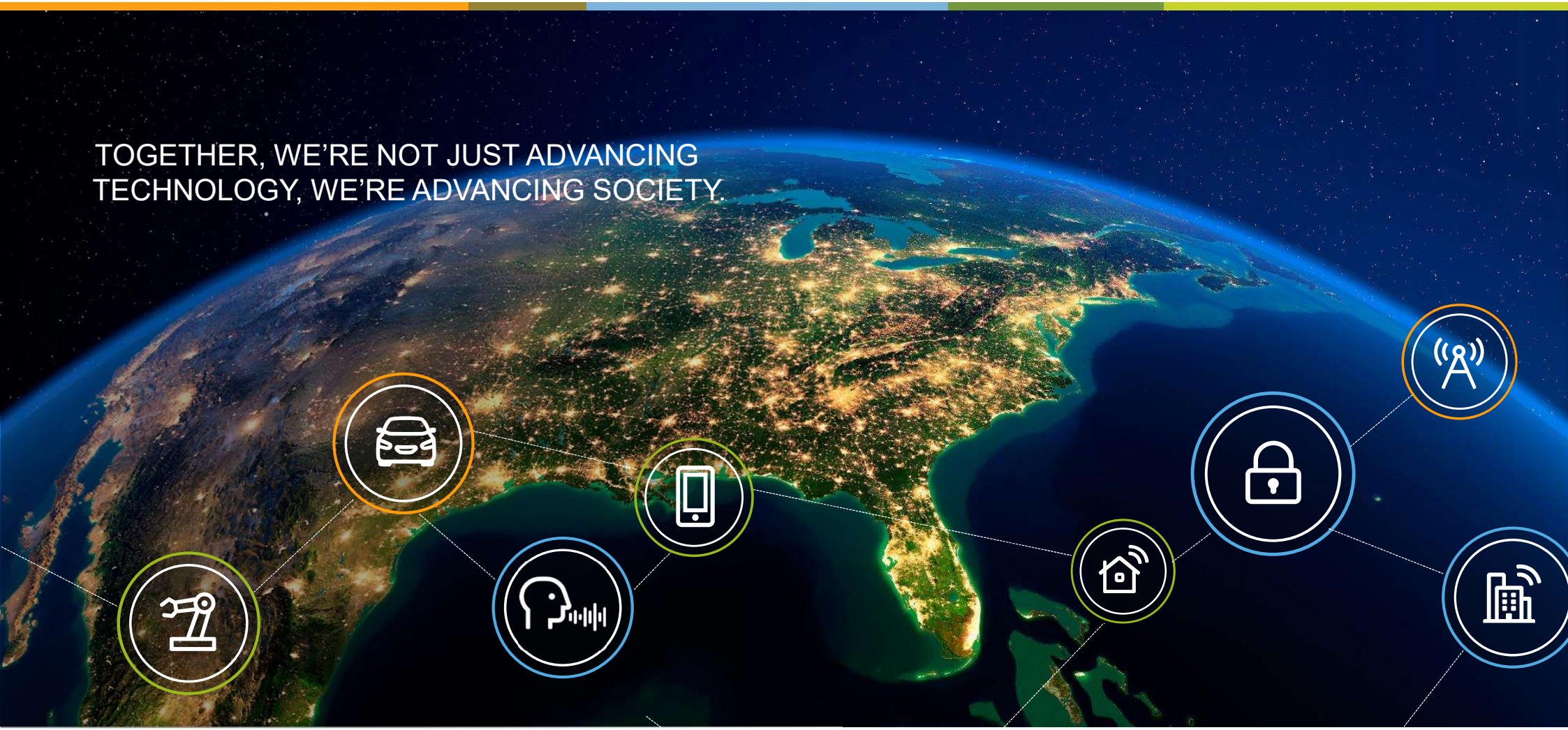
Proof that the ISO 21434 certified processes and procedures were followed during devlopment

Elements of the way that security sensitive information is handled within NXP

Proof that the Device is covered by NXP Product Security Response Incident Team (PSIRT)

WHAT NXP PROVIDE TO A CUSTOMER





NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP

Q&A

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Evropské certifikace kybernetické bezpečnosti

CERTIFIKÁCIA KYBERBEZPEČNOSTI PODĽA EURÓPSKYCH SCHÉM V PODMIENKACH SR

MARTIN SENČÁK

riaditeľ orgánu bezpečnostnej certifikácie
Národný bezpečnostný úrad

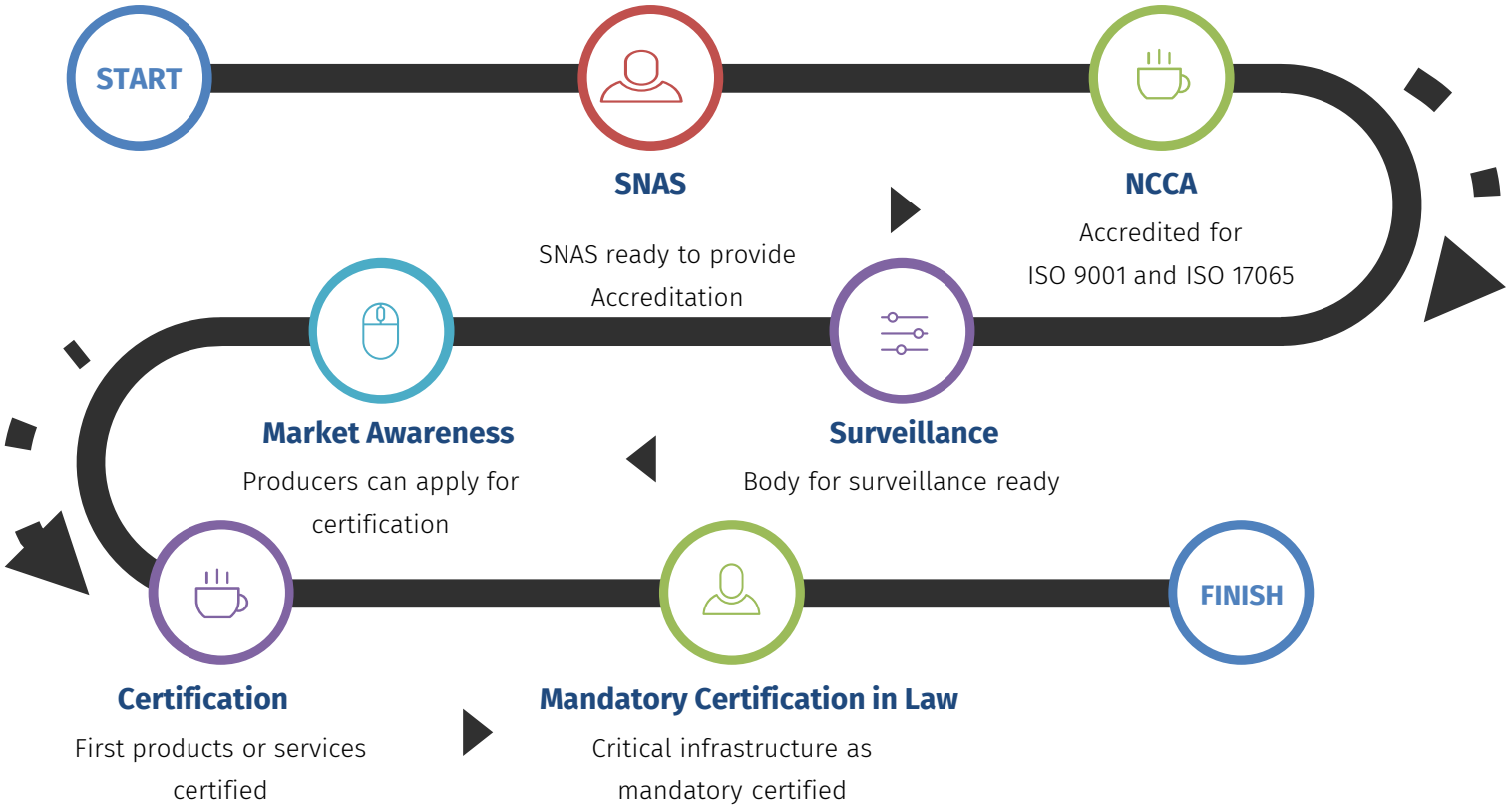
Digitální Česko

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Certifikácia kyberbezpečnosti podľa európskych schém v podmienkach SR

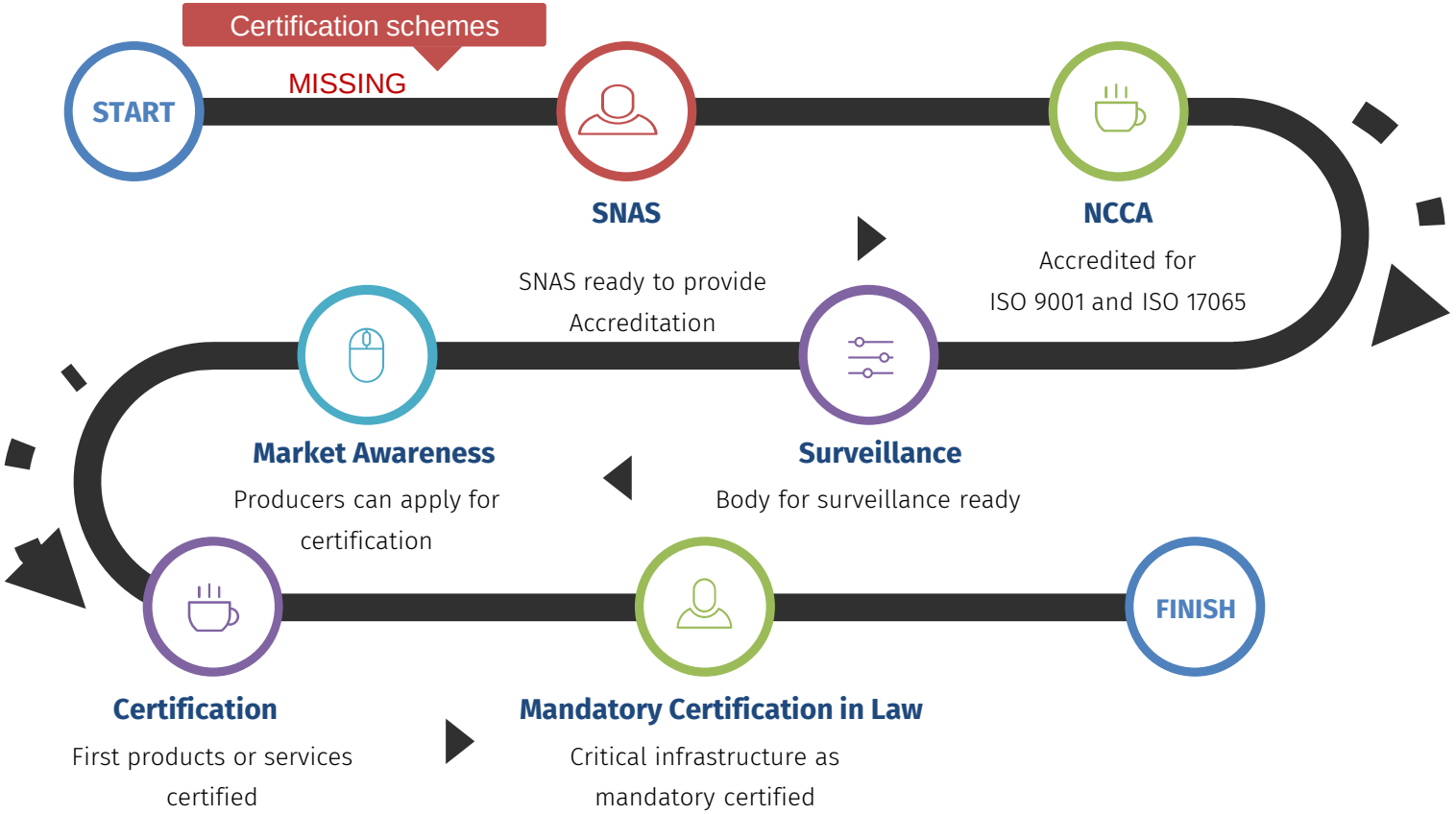
por Mgr. Martin Senčák
Riaditeľ orgánu bezpečnostnej certifikácie
National Cybersecurity Certification Authority
NBÚ

ORIGINAL IMPLEMENTATION PLAN – pôvodný plán implementácie



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

ORIGINAL IMPLEMENTATION PLAN – pôvodný plán implementácie



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Realita 2023

Certifikačné schémy trvajú dlho, bez garancie termínov z EK

Chýbajúce schémy brzdia akreditáciu od SNAS, prípravu posudzovateľov/ audítorov

Príprava čerpania zdrojov z EÚ projektu - časovo senzitívne

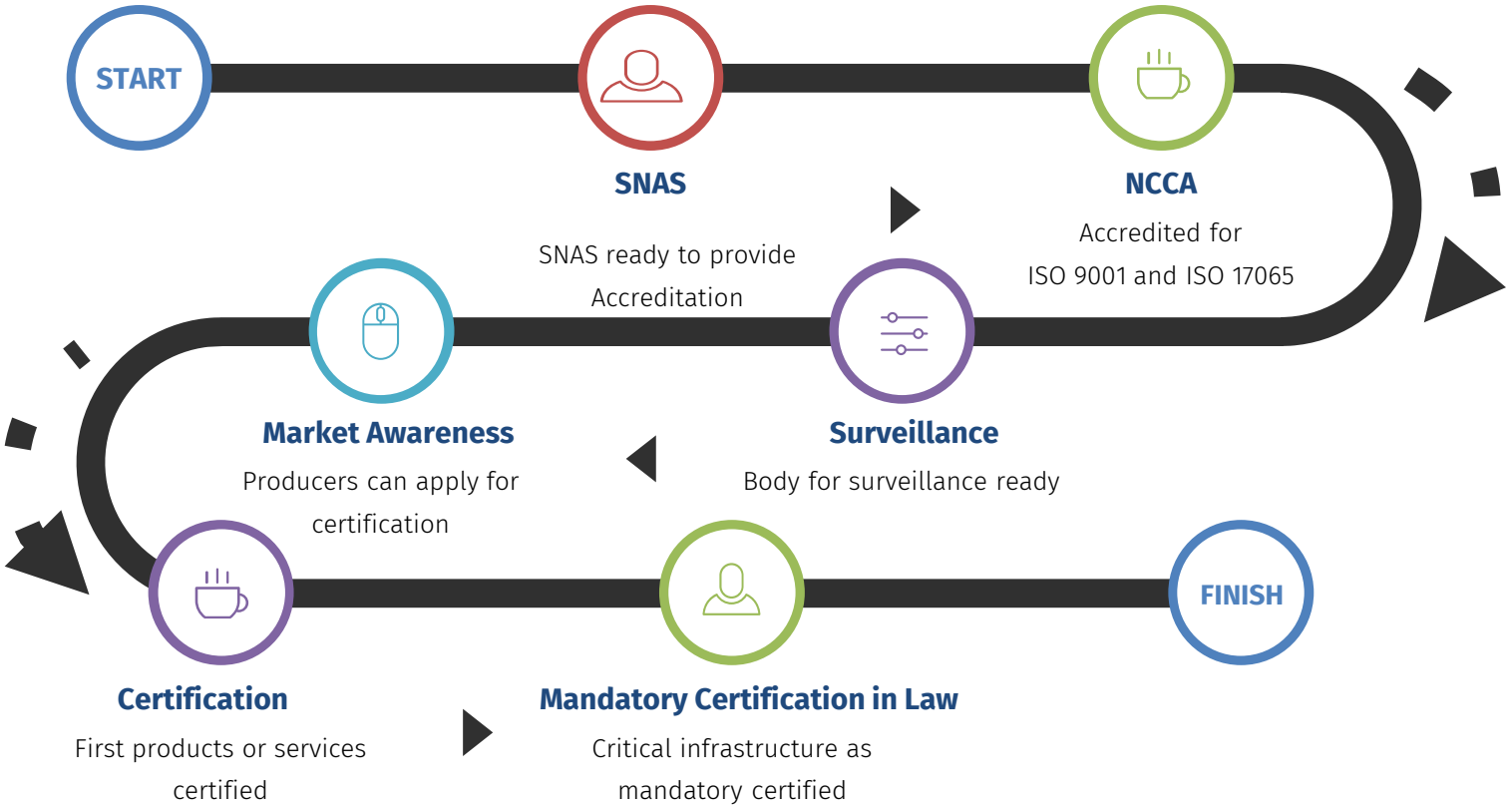
Vníme, že aktéri sú nepripravení, je potrebné im dať jednoznačné informácie

Certifikácie budú znamenať náklady pre prevádzkovateľov, ktorí musia porozumieť, čo ich čaká a dať si to do rozpočtov, preškoliť si pracovníkov

Bez certifikačných schém sme zastali hneď na štarte dlhoročného procesu.

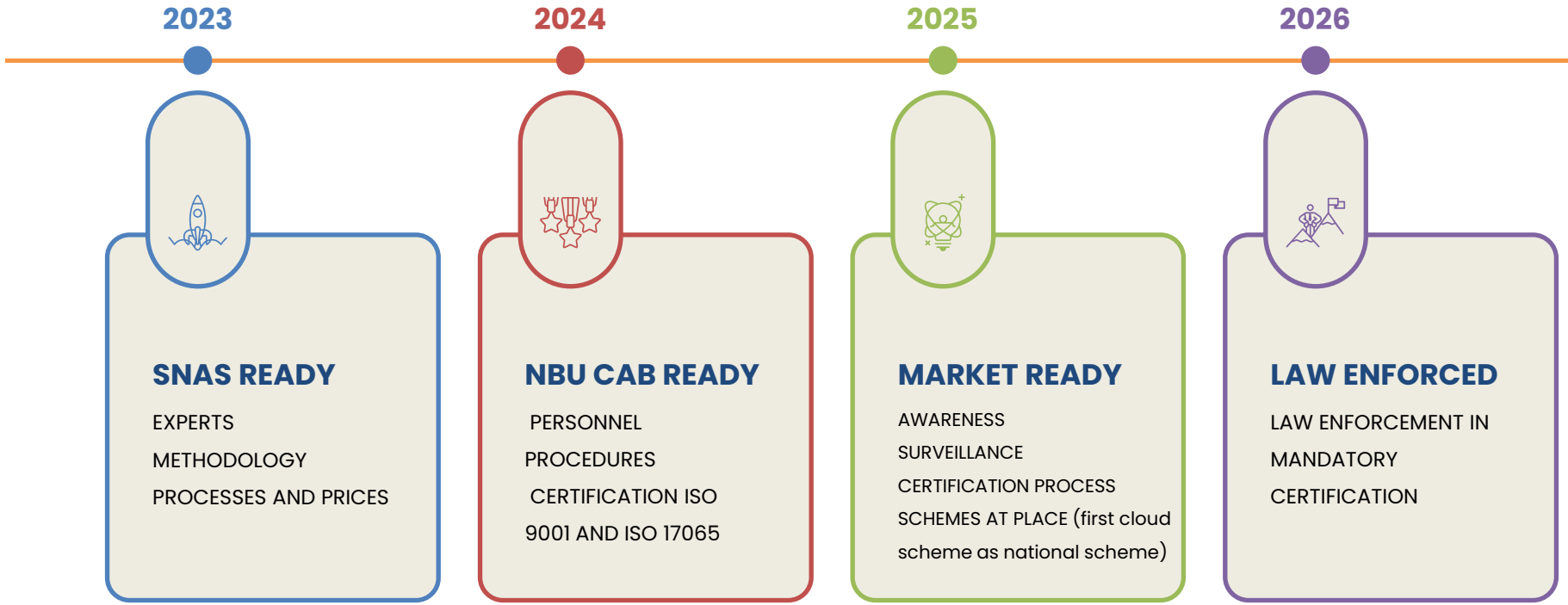
2023 IMPLEMENTATION PLAN – plán implementácie 2023

Slovenská národná schéma =
preklad EU CS k 06/2023

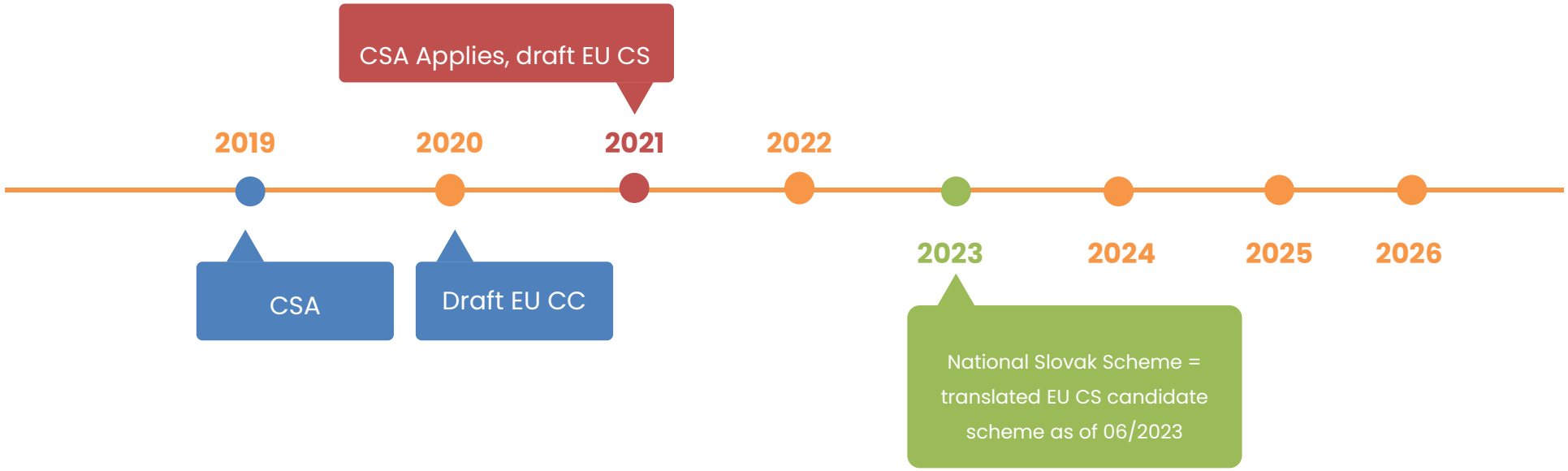


NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

EXPECTED MILESTONES in EU schemes – očakávané míľniky pre EU schémy



SCHEME DEVELOPMENT TIMELINE



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Plánované aktivity 2023-2027

Trojročný projekt na podporu implementácie:

Medzinárodná výmena skúseností

Príprava databázy expertov/ posudzovateľov/ audítorov

Príprava SNAS, NCCA (NBÚ), akreditácia CAB

Mediálna kampaň a eventy pre výrobcov a poskytovateľov služieb

Vzdelávanie všetkých aktérov (schémy, požiadavky, implementácia)

Finančná podpora pre výrobcov a poskytovateľov služieb (napr. Audit KB)

ĎAKUJEM ZA POZORNOSŤ

NÁVRH AKTU O KYBERNETICKÉ ODOLNOSTI

ADAM BOTEK

vedoucí oddělení multilaterální spolupráce I
Národní úřad pro kybernetickou a informační bezpečnost

Návrh Aktu o kybernetické odolnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

13. června 2023

Adam Botek

CRA teaser

- Povinné kyberbezpečnostní požadavky pro všechny produkty s digitálním prvkem na EU trhu
- Zajištění kybernetické bezpečnosti v průběhu celého životního cyklu produktů
- Zvýšení informovanosti uživatelů

Dva hlavní cíle návrhu

1) Zmenšit počet zranitelností digitálních produktů
2) Zlepšit informovanost uživatelů

Základ v novém legislativním rámci

Horizontální působnost

- Interakce s legislativou k AI, strojním výrobkům, NIS2, RED DA

Působnost

- **Produkty s digitálním prvkem**
  - Veškerý hardware i software, který je možno připojit k jinému zařízení nebo k síti

  - HW: Laptopy, smartphony, routery, senzory, průmyslové řídící systémy
  - SW: operační systémy, mobilní aplikace, video hry
  - Komponenty: CPU, softwarové knihovny

- **Kritické produkty**
  - Podle funkcionalit nebo zamýšleného použití
  - Zabezpečené kryptoprocesory, firewally a routery pro průmyslové použití

Hospodářské subjekty a jejich povinnosti

- **Hospodářské subjekty** = výrobci, dovozci, distributoři

- **Povinnosti** (dopadají zejména na výrobce)

  - Plnění základních požadavků na kybernetickou bezpečnost
  - Informování a instruktáž uživatelů
  - Příprava technické dokumentace
  - Hlášení **aktivně zneužívaných** zranitelností a kybernetických incidentů
  - Umístění CE označení

Základní požadavky

- **Požadavky vztahující se k vlastnostem produktů**
  - Dodávání produktů bez známých zranitelností

  + Na základě zhodnocení rizik:
  - Zajištění ochrany dat šifrováním, ochrany dostupnosti základních funkcí
  - Zajištění možnosti provádět bezpečnostní aktualizace
  - …

- **Požadavky na zvládání zranitelností** (po umístění produktu na trh)
  - Identifikace a dokumentace zranitelností
  - Pravidelné testování bezpečnosti produktů
  - Zvládání zranitelností
  - Zveřejňování opravených zranitelností
  - …

Harmonizované normy

- K upřesnění základních požadavků

- Připravovány evropskými standardizačními organizacemi (CEN, CENELEC, ETSI)

- **Pravomoc Komise**
- Určit certifikační schémata podle CSA, které lze použít k prokázání shody se základními požadavky nebo jejich částmi
- Vydávat obecné specifikace v případě absence nebo nedostatků harmonizovaných norem

Posuzování shody

- **„Nekritické“ produkty** (90 % produktů)
  - sebehodnocení (modul A)

- **Kritické produkty**
  - I. úrovně: při sebeposouzení navíc aplikace harmonizovaných norem, příp. společných specifikací nebo certifikačního systému podle CSA / hodnocení třetí stranou
  - II. úrovně: hodnocení třetí stranou
  - Vysoce kritické produkty: povinné využití certifikačních schémat podle CSA

- **Pravomoc Komise**
  - vydávat *společné specifikace* v případě absence nebo nedostatků harmonizovaných norem

Dozor nad trhem

- **Procedura vztahující se k produktům představující významné kyberbezpečnostní riziko**
  - na národní úrovni
  - na unijní úrovni

- **Opatření**
  - Nařízení nápravy
  - Stažení výrobku z trhu

  - Při neplnění povinností podle Aktu, možnost pokuty

Adam Botek

E-mail: adam.botek@nukib.cz

PŘEDSTAVENÍ ČINNOSTÍ NÁRODNÍHO KOORDINAČNÍHO CENTRA A MOŽNOSTI FINANCOVÁNÍ Z PROGRAMU DEP KYBERBEZPEČNOST

NIKOLA CHVÁTALOVÁ

zástupce vedoucího oddělení vědy, výzkumu a inovací
Národní úřad pro kybernetickou a informační bezpečnost

NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

PŘEDSTAVENÍ ČINNOSTÍ NÁRODNÍHO KOORDINAČNÍHO CENTRA A MOŽNOSTI FINANCOVÁNÍ Z PROGRAMU DEP KYBERBEZPEČNOST

Mgr. Nikola Chvátalová I Oddělení vědy, výzkumu a inovací NÚKIB I NCC-CZ

OBSAH PREZENTACE

Představení NKC a jeho činností

- vymezení a úkoly NKC
- Komunita kompetencí pro kybernetickou bezpečnost

Možnosti financování z programu Digitální Evropa

- vymezení DEP
- aktuálně řešené projekty
- otevřené výzvy

Závěr (dotazy, kontakt)

PŘEDSTAVENÍ NKC A JEHO ČINNOSTÍ

VYMEZENÍ NKC

- vzniká na základě Nařízení Evropského parlamentu a Rady (EU) **2021/887** ze dne 20. května 2021, kterým se zřizuje **Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost** a **síť národních koordinačních center**
- v ČR činnosti NKC zajišťuje **NÚKIB** ve spolupráci s **CSH**

NÚKIB

CyberSecurityHub.cz

KONTEXT

Evropské kompetenční centrum (ECCC)

- posiluje vedoucí postavení a strategickou autonomii EU v oblasti KB
- přispívá ke zlepšení VaV v KB a k rozvoji průmyslových, technologických a výzkumných kapacit a schopností v této oblasti

Síť Národních koordinačních center (NKC)

- je tvořena jednotlivými NKC, které podporují ECCC při plnění poslání a cílů

Komunita kompetencí pro KB (Komunita)

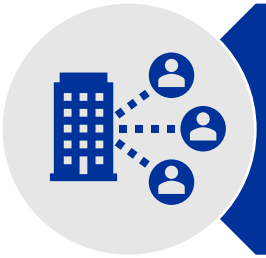
- je rozsáhlá, otevřená, interdisciplinární a různorodá skupina evropských zúčastněných stran zapojených do technologií kybernetické bezpečnosti

ÚKOLY NKC

- působit jako **kontaktní místo na vnitrostátní úrovni pro Komunitu** na podporu ECCC
- propagovat, podněcovat a usnadňovat **účast v přeshraničních projektech a akcích financovaných EU**
- poskytovat **podporu ve fázi podávání žádostí** o projekty
- poskytovat **finanční podporu** třetím stranám

VYMEZENÍ KOMUNITY

rozsáhlá, otevřená a různorodá skupina stakeholderů v oblasti kybernetické bezpečnosti



podporuje ECCC při plnění jeho poslání a cílů a úzce spolupracuje s ECCC a NKC

poskytuje strategické poradenství ECCC

PODMÍNKY ČLENSTVÍ V KOMUNITĚ

Členy Komunity se mohou stát pouze subjekty, které:

- mají **sídlo v ČS EU**
- mohou přispívat k **plnění poslání** a mají **odborné znalosti** v oblasti KB v alespoň jedné z těchto oblastí:
  - akademická oblast, výzkum nebo inovace;
  - průmyslový vývoj nebo vývoj produktů;
  - odborná příprava a vzdělávání;
  - bezpečnost informací nebo reakce na incidenty;
  - etika;
  - formální a technická normalizace a specifikace
- splní **národní bezpečnostní kritéria**

MOŽNOSTI FINANCOVÁNÍ Z PROGRAMU DIGITÁLNÍ EVROPA (DEP)

VYMEZENÍ DEP

- cílem DEP je **podpora digitální transformace** v EU prostřednictvím investic do špičkových technologií
- má 5 specifických cílů:
  - Vysoce výkonná výpočetní technika (HPC)
  - Umělá inteligence (AI)
  - **Kybernetická bezpečnost a důvěra**
  - Pokročilé digitální dovednosti
  - Zavedení, co nejlepší využívání digitální kapacity a interoperabilita

AKTUÁLNĚ ŘEŠENÉ PROJEKTY: NCC-CZ

NÁZEV:	National Coordination Centre – The Czech Republic
CÍL:	zajistit vznik a fungování NKC v ČR a plnění úkolů vyplývajících z nařízení 2021/887
ZAČÁTEK:	v závislosti na podpisu GA
TRVÁNÍ:	2 roky
PLÁNOVANÉ AKTIVITY:	▪ aktivizace národní R&D komunity, podpora spolupráce a zapojování do projektů ▪ poskytování podpory směrem ke Komunitě a ECCC ▪ poskytování finanční podpory třetím stranám ▪ aktivity v oblasti awareness raising
FSTP:	▪ rozpočet 150 000 EUR ▪ bez nutnosti kofinancování ▪ finanční podpora ze strany NKC cca 40 000 EUR

AKTUÁLNĚ ŘEŠENÉ PROJEKTY: TEST-CERT-CZ

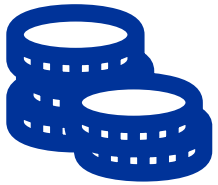
NÁZEV:	Building Testing and Certification Capabilities in the Czech Republic
CÍL:	finančně podpořit subjekty v oblasti certifikací KB (budování schopností, zlepšení kyberbezpečnosti SMEs, podpora standardizace)
ZAČÁTEK:	v závislosti na podpisu GA
TRVÁNÍ:	3 roky
PLÁNOVANÉ AKTIVITY:	▪ nastavení mechanismu poskytování finanční podpory ▪ poskytování informací a podpory ohledně chystaných výzev (WS) ▪ spuštění výzev, výběr projektů a poskytnutí finanční podpory ▪ prezentace podpořených projektů a výstupů (závěrečná akce)
FSTP:	▪ rozpočet 500 000 EUR ▪ 50 % kofinancování ze strany subjektu ▪ finanční podpora ze strany NKC cca 50 000 EUR

TYPES OF ACTIVITY:

- capacity building including for threat-based penetration testing, e.g. for the acquisition of certification testbeds; exchange of best practices and staff trainings; deploy innovative evaluation methods for specific ICT products or components; support standardisation actions;
- testing and certifying ICT products, ICT services or ICT process;
- auditing infrastructures in term of cybersecurity resilience;
- standardization actions (e.g., creation of protection profiles or adoption/improvement of standards used in certification schemes), considering activities by European and international standardisation organisations as appropriate;
- cyber-security and interoperability testing capabilities on 5G disaggregated and open solutions.

TARGETED STAKEHOLDERS:

- (future) conformity assessment bodies (CABs)
- accrediation bodies
- SMEs (manufactures/providers, ICT equipment users)



OTEVŘENÉ VÝZVY DEP KYBEREZPEČNOST

TÉMA	DEADLINE
EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges	6/7/23
Capacity Building of Security Operation Centres	6/7/23
Uptake of Innovative Cybersecurity Solutions	6/7/23
Preparedness Support and Mutual Assistance	26/9/23
Coordination Between the Cybersecurity Civilian and Defence Spheres	26/9/23
Standardisation in the area of Cybersecurity	**26/9/23**
Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies	**26/9/23**

STANDARDISATION IN THE AREA OF CYBERSECURITY

DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION

OBJECTIVES	podpora standardizace v oblasti KB zejména s ohledem na implementaci CRA
SCOPE	zajistit širokou účast stakeholderů ve standardizačních aktivitách (např. skrze setkání, WS, společné aktivity se zapojením soukromého i veřejného sektoru)
OUTCOMES	organizace akcí, WS, konzultací, white papery, podpora účasti expertů na akcích
TARGETED STAKEHOLDERS	stakeholdeři v oblasti standardizace v KB (evropské standardizační organizace, CABs, průmyslové subjekty, SMEs a start-upy, aktéři hrající roli ve standardizačním procesu a v implementaci CRA a CSA) mezinárodní konsorcia nejsou podmínkou, ale pozitivně ovlivní impakt projektu
TYPE OF ACTION	coordination and support action grant (100 % funding rate)
HARMONOGRAM	otevření 25. 5. 2023 – deadline 26. 9. 2023
TRVÁNÍ	36 měsíců
ROZPOČET	celková alokace 3 mil EUR, až 3 mil EUR per project

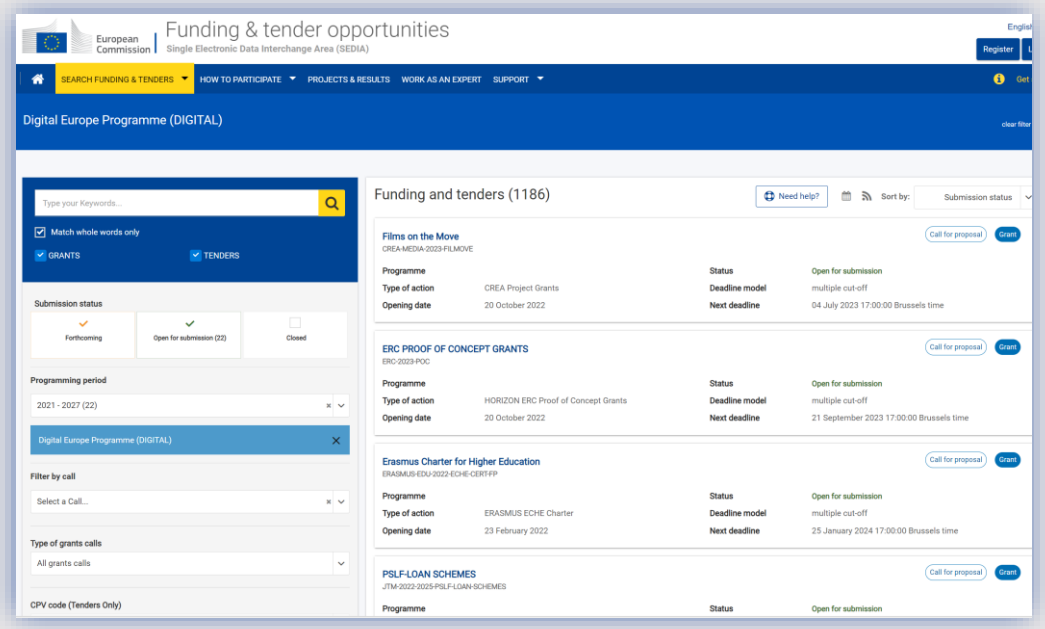
SUPPORT FOR IMPLEMENTATION OF EU LEGISLATION ON CYBERSECURITY AND NATIONAL CYBERSECURITY STRATEGIES

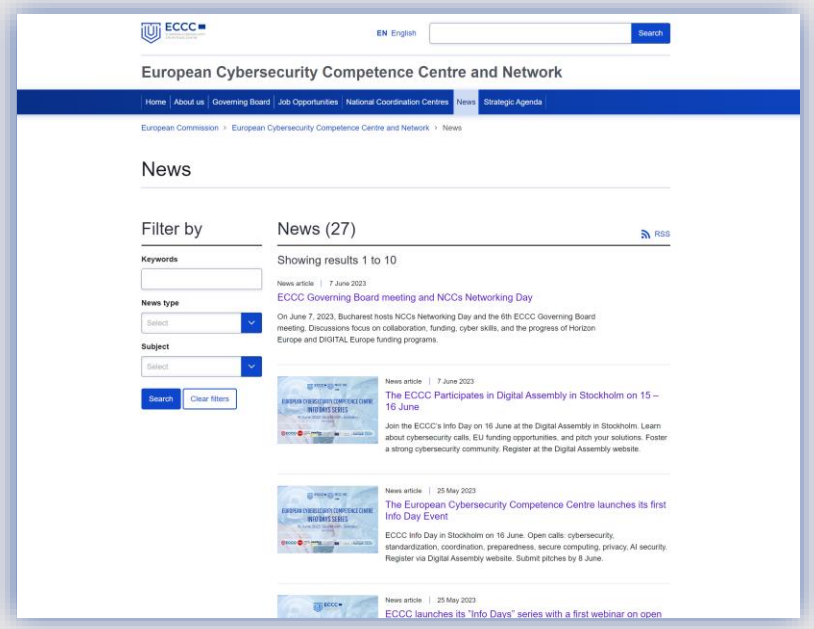
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION

OBJECTIVES	podpora implementace EU legislativy (NIS2, CSA, CRA, směrnice 2013/40), podpora připravenosti průmyslu a trhu na legislativní požadavky pro produkty s digitálními prvky
SCOPE	implementace NIS2; zlepšení bezpečnosti produktů; podpora certifikace KB směrem k vnitrostátním orgánům a stakeholderům (SMEs)
OUTCOMES	lepší soulad s NIS2; organizace akcí a WS; posílení spolupráce a KB odolnosti EU; podpora akcí v oblasti certifikace
TARGETED STAKEHOLDERS	aktéři v rozsahu legislativy výše, průmysloví aktéři vč. SMEs a start-upů v rozsahu CRA, NIS2 a kteří mohou těžit z certifikačních schémat, národní autority implementující NIS2, CSIRTs, SOCs, OES, DSP, ISACs, aktéři hrající roli v implementaci CRA vč. certifikačních těles mezinárodní konsorcia nejsou podmínkou, ale pozitivně ovlivní impakt projektu
TYPE OF ACTION	simple grant (50 % funding rate)
HARMONOGRAM	otevření 25. 5. 2023 – deadline 26. 9. 2023
TRVÁNÍ	36 měsíců
ROZPOČET	celková alokace 30 mil EUR, 1-5 mil EUR per project

CO DOPORUČUJEME SLEDOVAT

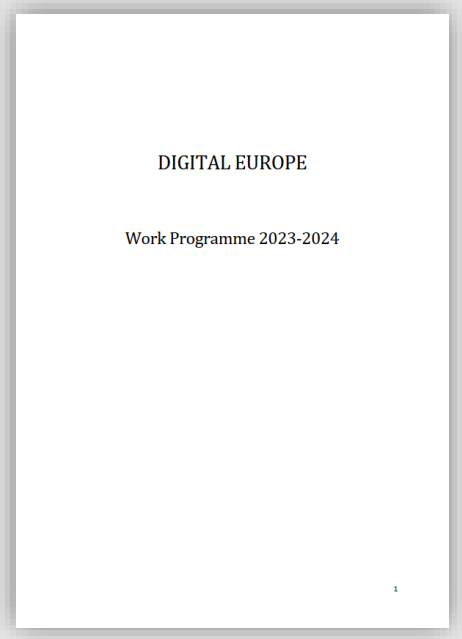
- Funding & Tender Opportunities Portal
- Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti
- webové stránky ECCC



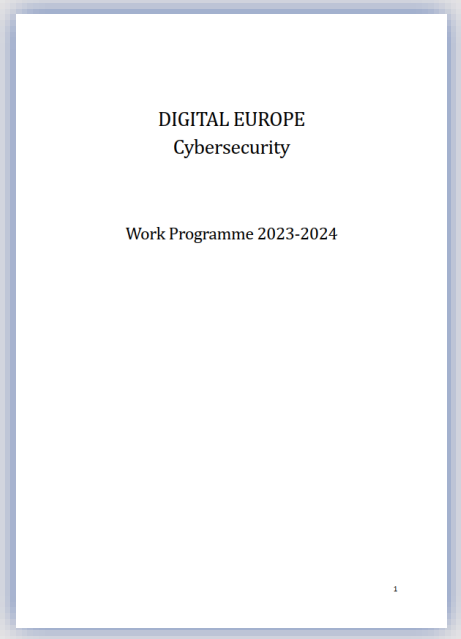


DŮLEŽITÉ DOKUMENTY

OBECNÝ WP DEP 2023-2024



WP DEP KYBERBEZPEČNOST 2023-2024



CALL DOKUMENT CYBER-B-03

CALL DOKUMENT CYBER-04

DOTAZY A KONTAKT

Oddělení vědy, výzkumu a inovací NÚKIB I **vyzkum@nukib.cz**

Národní koordinační centrum I **ncc@nukib.cz**

Evropské certifikace kybernetické bezpečnosti

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Digitální Česko

NETWORKING

(prostor pro navázání kontaktů volnou formou)

Pracovní skupina evropské certifikace

www.eucertifikace.nukib.cz

ncca@nukib.cz

Markéta Šilhavá
Email: marketa.silhava@nukib.cz
Telefon: +420 702 160 590

Jiří Procházka
Email: jiri.prochazka@nukib.cz
Telefon: +420 601 069 970