MUNI
LAW

Certifikace podle CSA a CRA (a jak to bude fungovat?)

Mgr. Jakub Vostoupal, Ph.D.

Zde prezentované názory jsou pohledem jednotlivce a nejedná se o vyjádření oficiálních pozic žádných organizací.

MUNI LAW

Proč se hodí řešit certifikace?

- *§ 13 odst. 2 nZoKB*
  - *„Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření podle § 14 v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.“*

- Příloha I., CRA
  - Na základě posouzení kybernetického bezpečnostního rizika musí být produkty s digitálními prvky dodávány:
    - *dodávány na trh bez známých zneužitelných zranitelností,*
    - *zajišťují ochranu před neoprávněným přístupem **vhodnými kontrolními mechanismy**, mimo jiné na základě systémů správy ověřování, identity nebo přístupu, a podávají zprávy o možném neoprávněném přístupu,*
    - *jsou navrženy, vyvinuty a vyrobeny tak, aby omezily prostory k útoku, včetně vnějších rozhraní,*
    - *chrání důvěrnost uchovávaných, předávaných nebo jinak zpracovávaných údajů, ať již osobních či jiných, například šifrováním příslušných uložených nebo přenášených údajů prostřednictvím nejmodernějších mechanismů a za pomoci jiných technických prostředků*
    - *jsou navrženy, vyvinuty a vyrobeny tak, aby se snížil dopad incidentu použitím vhodných mechanismů a technik zmírňujících zneužití*
    - *chrání dostupnost základních a klíčových funkcí, a to i po incidentu, prostřednictvím opatření ke zvýšení odolnosti vůči útokům, jejichž důsledkem je odepření služby, a opatření ke zmírňování těchto útoků,*

MUNI LAW

Performativní pravidla

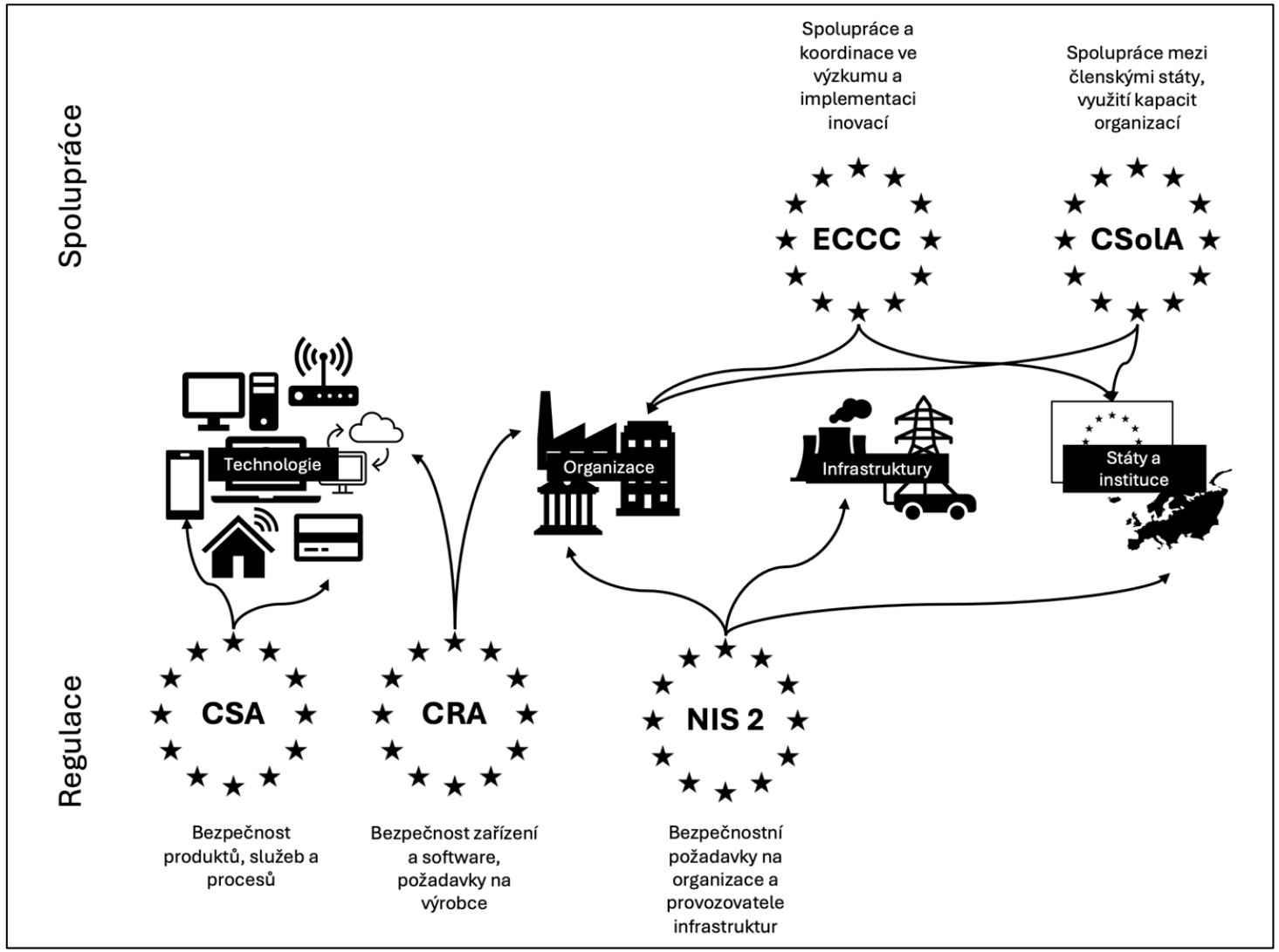
- Spolu s chytrými pravidly tradiční regulačním modelem pro oblast kybernetické bezpečnosti

- Stanovení cíle → adresát normy je sám svým normotvůrcem
  - Dokumentace nezbytná (transparentnost, kontrola)

- Výhody: Flexibilita, Risk-based approach
- Nevýhody: Nejistota (právní i podnikatelská), administrativní zátěž (zejména pro SME)

Compliance procedury

- *Compliance*
  - Moment posuzování
  - Podnikatelské riziko → náklady na dosažení compliance nesmí převýšit případné pokuty
- Complience procedury
  - Sebe-posouzení
  - Certifikace
- Standardizace
  - Dobrovolné standardy, roztříštěný trh (a komplikující se regulace)


Spolupráce
Regulace
Spolupráce a koordinace ve výzkumu a implementaci inovací
Spolupráce mezi členskými státy, využití kapacit organizací
ECCC
CSolA
Technologie
Organizace
Infrastruktury
Státy a instituce
CSA
CRA
NIS 2
Bezpečnost produktů, služeb a procesů
Bezpečnost zařízení a software, požadavky na výrobce
Bezpečnostní požadavky na organizace a provozovatele infrastruktur

MUNI LAW

Certifikace podle CSA

- Certifikační schéma specifikuje konkrétní pravidla a požadavky pro určitý okruh produktů/služeb/procesů.
  - Schémata připravuje ENISA (v součinnosti s pracovními skupinami expertů) na základě požadavku od Evropské komise či European Cybersecurity Certification Group (ECCG).
  - Komise schéma formálně **přijme formou prováděcího aktu**, čímž se stane závazným evropským schématem.
  - Každé schéma vymezuje **předmět a rozsah** (typy ICT produktů/služeb pokryté schématem), **bezpečnostní požadavky** (často odkazem na existující technické normy), metodiku hodnocení a **úrovně záruky** (assurance levels)
  - **Národní autority certifikace** – v ČR NÚKIB
  - Vlastní *certifikaci* provádějí **akreditované a oznámené *Conformity Assessment Bodies* (či autorizované u vysoké úrovně) / akreditované laboratoře** (ITSEF), které testují produkty a vydávají certifikáty.
  - **Platnost certifikátu** je časově omezená (např. EUCC certifikát platí max. 5 let) a může být pozastaven či zrušen, pokud produkt přestane splňovat požadavky (např. neopravené zranitelnosti). Držitel certifikátu musí udržovat procesy pro *management zranitelností* a hlásit vážné objevené chyby příslušnému orgánu

Úrovně záruky certifikace

- CSA definuje tři úrovně – *základní, významná, vysoká.* Ty odrážejí, jak důkladně a proti jak pokročilým hrozbám byl produkt posouzen.
  - **Základní** (basic) – poskytuje **základní míru jistoty**, že produkt/služba splňuje stanovené bezpečnostní požadavky. Hodnocení je nejméně přísné: zahrnuje *kontrolu dokumentace* a základní testy, cílem je eliminovat známá triviální rizika. Výstupem může být **EU prohlášení o shodě** vydané samotným výrobcem (forma **samocertifikace**), pokud to dané schéma dovolí.
  - **Významná** (substantial) – zajišťuje vyšší úroveň jistoty; produkt musí odolávat běžným kybernetickým útokům aktérů s omezenými zdroji. Hodnocení zahrnuje **testování** bezpečnostních funkcí a ověření, že neobsahuje *žádné veřejně známé zranitelnosti.* Certifikát na této úrovni již musí vydat akreditovaný certifikační orgán, *samohodnocení zde nestačí*.
  - **Vysoká** (high) – nejpřísnější úroveň, určená pro produkty vystavené vysokým rizikům (např. kritická infrastruktura). Poskytuje **důvěru, že odolá sofistikovaným útokům státních či dobře financovaných aktérů.** Hodnocení zahrnuje hloubkovou analýzu, *penetrační testy* a další formy ověření odolnosti. Certifikát opět vydává nezávislý posuzovatel.
- S rostoucí úrovní záruky se zvyšuje i **náročnost a cena** certifikace. Organizace tak mohou zvolit úroveň přiměřenou rizikům použití daného produktu

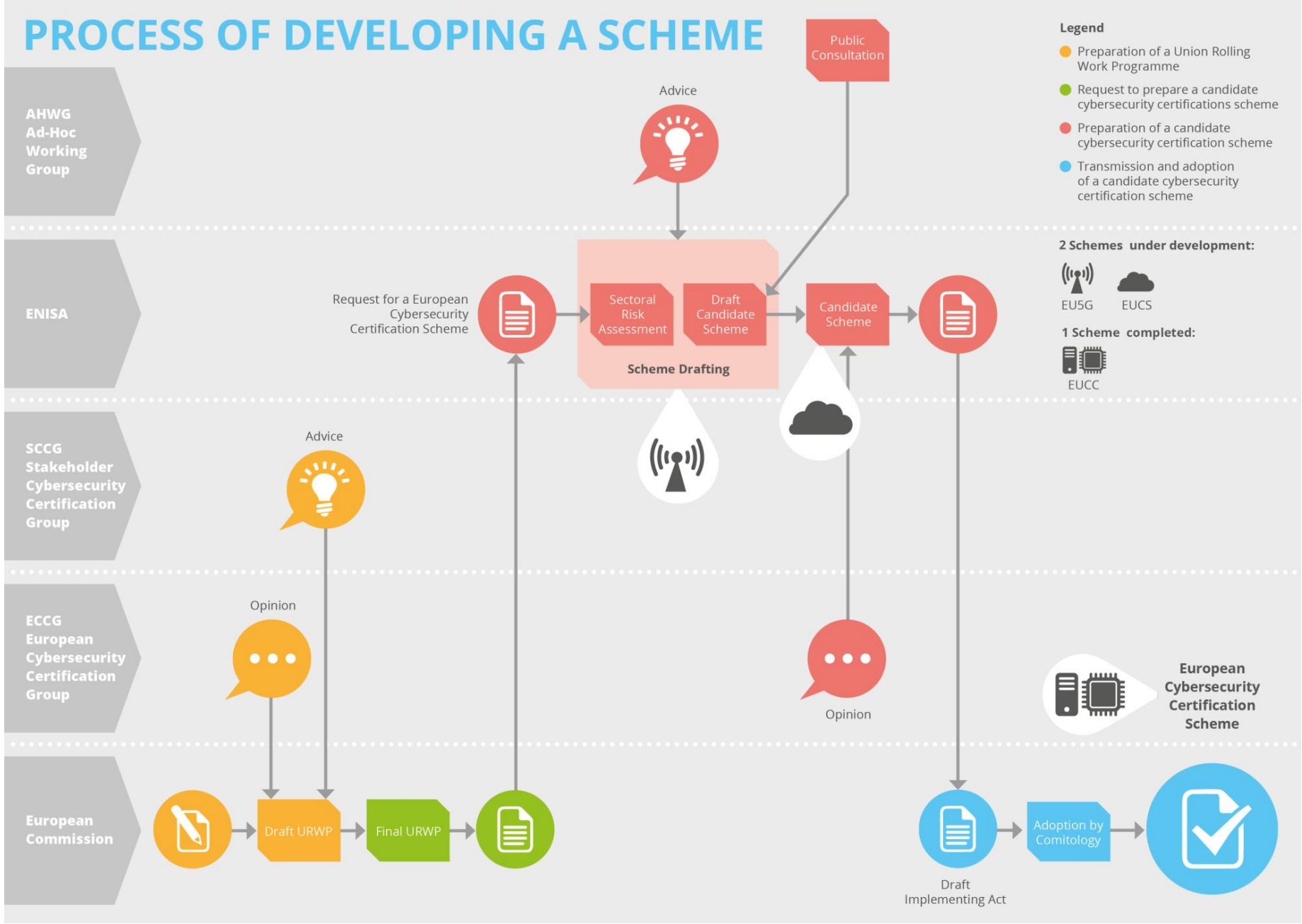
Dobrovolná vs. povinná certifikace

- Certifikace v rámci CSA jsou zatím **dobrovolné** – firmy *nemusí* získat certifikát, pokud zákon nestanoví jinak. CSA však *vytvořil podmínky* pro to, aby jiné právní předpisy nebo rozhodnutí EU mohly **certifikaci učinit povinnou** v určitých případech.
  - CRA
  - Sektorové předpisy (elektroměry apod.)
  - NIS2: I když směrnice NIS2 přímo neukládá povinnost mít certifikát, organizace v regulovaných odvětvích mohou **v rámci řízení dodavatelských rizik** požadovat po svých dodavatelích certifikované produkty. Tím se *nepřímo tržně prosadí* certifikace – produkt bez certifikátu může být znevýhodněn ve veřejných zakázkách či u náročných zákazníků.

Připravená/Připravovaná schémata

- **EUCC (Common Criteria)** – První schéma EU, zveřejněné v únoru 2024, vychází z mezinárodní normy Common Criteria (ISO/IEC 15408). **EUCC umožňuje certifikaci širokého spektra ICT produktů** (HW, SW, komponenty) na úrovni významná nebo vysoká. Certifikace je *dobrovolná*, ale může být konkurenční výhodou a způsobem, jak prokázat zabezpečení např. dle požadavků NIS2, DORA či CRA. **Od února 2025 mohou výrobci žádat o EUCC certifikáty** a členské státy (skrze své NCCA/CAB) je mohou vydávat. Např. výrobce může certifikovat router, čip nebo software, a po získání EUCC označit výrobek evropskou známkou kybernetické certifikace.
- EUCS, EU5G, EUDI Wallets atd.
- **LES/FTE?**

MUNI LAW


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
Advice
Opinion
Opinion
Draft URWP
Final URWP
Draft Implementing Act
Adoption by Comitology
European Cybersecurity Certification 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
2 Schemes under development:
EU5G
EUCS
1 Scheme completed:
EUCC

MUNI LAW

EUCC

- Vydávání EUCC certifikátů plně zahájeno
- Národní CC schémata přestávají přijímat nové žádosti
- Stávající národní certifikáty platné ještě 5 let
- První certifikáty
  - **GMV GNSS Cryptographic Module** (červenec 2025) - DEKRA Španělsko, Významná úroveň
  - **STMicroelectronics ST54J/ST54K** (duben 2025) - ANSSI Francie, mikrokontroler pro smart karty
  - **Thales Smart Tachograph G2** (duben 2025) - ANSSI Francie
- Založeno na CC procesu

EUCC - Proces

- Příprava (2-6 měsíců)
  - Definice rozsahu certifikace (Target of Evaluation - TOE)
  - Vypracování Security Target dokumentu
    Bezpečnostní cíle (buď definované výrobcem/žadatelem o certifikaci, nebo s odkazem na existující Protection Profile, ať už certifikovaný pod EUCC nebo ne)
    Definice funkčních požadavků na bezpečnost (*Security Functional Requirements* - CC, část druhá)
    Definice požadavků na zajištění bezpečnosti (*Security Assurance Requirements* – včetně AVA_VAN úrovně, tedy úrovně hodnocení bezpečnosti)
  - Výběr certifikační autority
- Evaluace (6-18 měsíců)
  - Významná úroveň (AVA_VAN.1-2): 6-12 měsíců
  - Vysoká úroveň (AVA_VAN.3-5): 12-24 měsíců

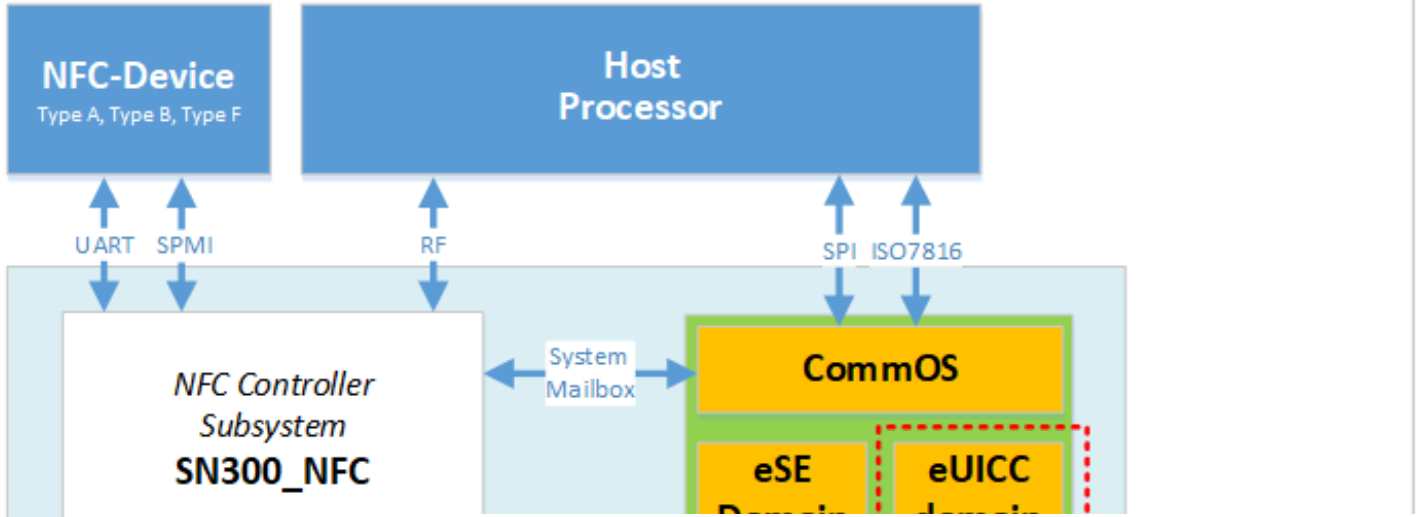


Figure 1. Place in the System

The following list contains the main features of the TOE:

- hardware to perform computations on multiprecision integers, which are suitable for public-key cryptography
- hardware to calculate the Data Encryption Standard with up to three keys
- hardware to calculate the Advanced Encryption Standard (AES) with different key lengths
- hardware to support Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Counter (CTR) modes of operation for symmetric-key cryptographic block ciphers
- hardware to support Galois/Counter Mode (GCM) of operation for symmetric-key cryptographic block ciphers
- hardware to calculate Cyclic Redundancy Checks (CRC)
- hardware to serve with True Random Numbers
- hardware to control access to memories and hardware components

In addition, the hardware embeds sensors, which ensure proper operating conditions of the device. Integrity protection of data and code involves error correction and error detection codes, EMFI detector, light sensing and other security functionality. Memory encryption and masking mechanisms are implemented to preserve confidentiality of data. The IC hardware is shielded against physical attacks. And the lockstep (redundant) CPU ensures protection against faults in the CPU.

5 Security Objectives

5.1 Security Objectives for the TOE

5.1.1 Security Objectives for Java Card System

5.1.1.1 Identification

OT.SID	**Subject Identification** The TOE shall uniquely identify every subject (applet, or CAP file) before granting it access to any service.

5.1.1.2 Execution

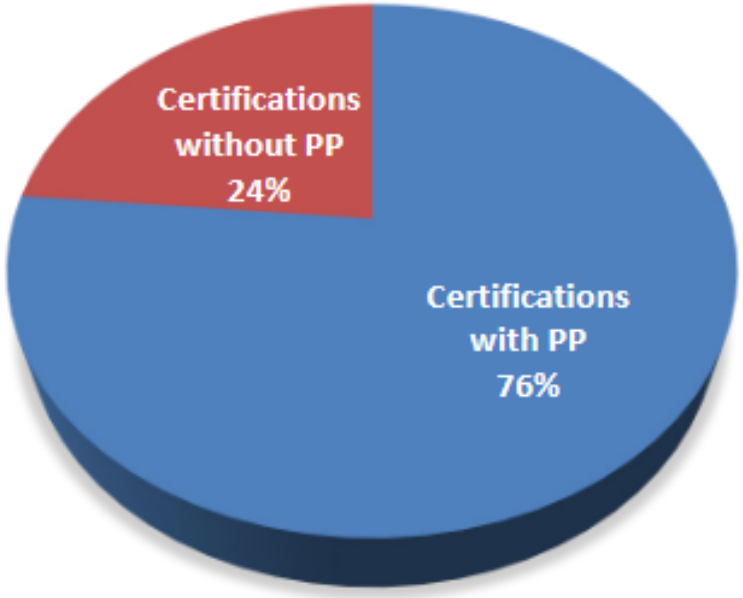
OT.FIREWALL	**Firewall** The TOE shall ensure controlled sharing of data containers owned by applets of different CAP files or the JCRE and between applets and the TSFs. See SA.FIREWALL for details.
OT.GLOBAL_ARRAYS_CONFID	**Confidentiality of Global Arrays** The TOE shall ensure that the APDU buffer that is shared by all applications is always cleaned upon applet selection. The TOE shall ensure that the global byte array used for the invocation of the install method of the selected applet is always cleaned after the return from the install method.
OT.GLOBAL_ARRAYS_INTEG	**Integrity of Global Arrays** The TOE shall ensure that only the currently selected applications may have a write access to the APDU buffer and the global byte array used for the invocation of the install method of the selected applet.

Protection profiles

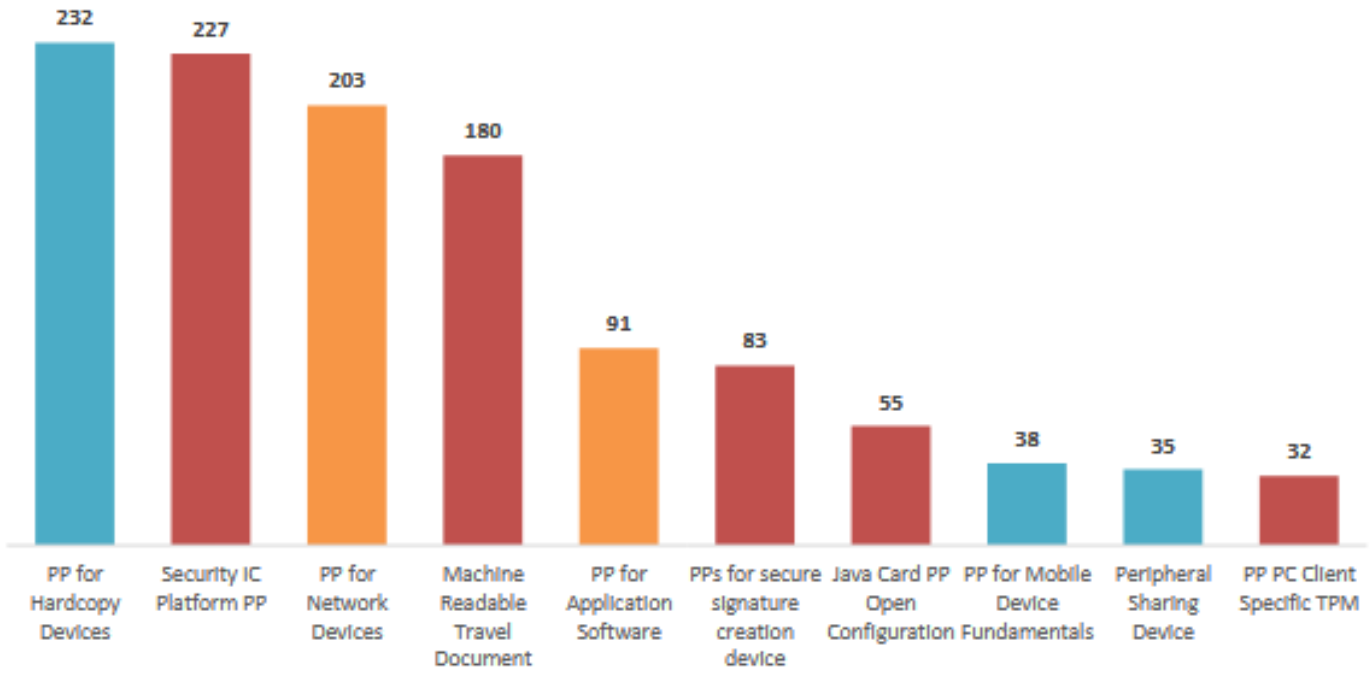
- **Protection Profiles** jsou opakovaně použitelné soubory bezpečnostních požadavků pro specifické kategorie produktů.
- Pro AVA_VAN.4 - 5 je existující PP nutný.
  - Ve výjimečných případech, kdy technická doména nebo PP není uvedena, je certifikace na těchto úrovních možná po důkladném odůvodnění a schválení národními certifikačními orgány pro kybernetickou bezpečnost (NCCA) a Evropskou skupinou pro certifikaci kybernetické bezpečnosti.
- Momentální verze: CC:2022, Security targets v souladu s touto verzí budou akceptován do konce roku 2027

Use of Protection Profiles in CC Industry

CC CERTIFICATIONS (2020 – Oct. 2024)



Top PPs 2020-2024 (October)



- ✓ **Market dominated by Protection Profiles**
- ✓ **Top-10 PPs are used to certify:**
  - **CRA Critical products: 50%**
  - **CRA Important products: 28%**
  - **CRA non-critical, non-important: 22%**

Source: jtsec CC statistics

MUNI LAW

EUCC - Evaluace

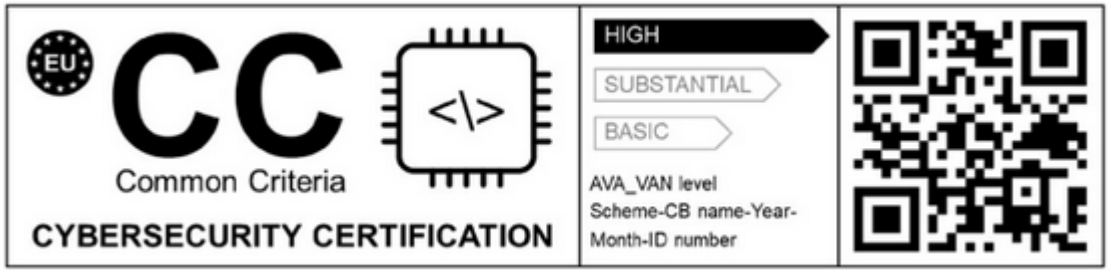
- Přezkum dokumentace (design, development, lifecycle)
- Funkční testování
- Analýza zranitelnosti (AVA_VAN):
  - AVA_VAN.1: Základní vyhledávání známých zranitelností
  - AVA_VAN.2: Detailnější analýza, odolnost vůči začátečníkům
  - AVA_VAN.3: Systematická analýza, odolnost vůči zkušeným útočníkům
  - AVA_VAN.4: Rigorózní analýza včetně covert channels
  - AVA_VAN.5: Nejvyšší úroveň, odolnost vůči expertům

EUCC – Certifikace

- ITSEF vypracuje Evaluation Technical Report
- CB přezkoumá a vystaví certifikát
- Zveřejnění v ENISA databázi

- Průběžně po certifikaci
  - Monitoring každé 2 roky
  - Vulnerability management
  - Platnost certifikátu: až 5 let

- ČR: SGS (ITSEF)



MUNI LAW

Finanční náročnost (odhad)

Úroveň záruky	Malý produkt	Střední produkt	Komplexní produkt
Substantial (AVA_VAN.1-2)	€75,000 - €120,000	€100,000 - €150,000	€120,000 - €200,000
High (AVA_VAN.3)	€138,000 - €180,000	€160,000 - €220,000	€200,000 - €260,000
High (AVA_VAN.4-5)	€200,000+	€250,000+	€300,000+

MUNI LAW

Časové odhady

Úroveň	Příprava	Evaluace	Celkem
Substantial (AVA_VAN.1)	2-4 měsíce	6-8 měsíců	8-12 měsíců
Substantial (AVA_VAN.2)	3-5 měsíců	8-10 měsíců	11-15 měsíců
High (AVA_VAN.3)	4-6 měsíců	10-14 měsíců	14-20 měsíců
High (AVA_VAN.4-5)	6-8 měsíců	14-18 měsíců	20-26 měsíců

Akt o kybernetické odolnosti

MUNI
LAW

Co nás čeká a nemine

- Konec roku 2027 může být relativně krátká doba.
- CRA se vztahuje na **všechny "produkty s digitálními prvky"** dodávané na trh EU. Tím se rozumí **hardware nebo software** a jejich vzdálené datové řešení, včetně samostatně dodávaných komponent, **jejichž zamýšlené nebo rozumně předvídatelné použití zahrnuje datové připojení k zařízení či síti.**
  - Laicky řečeno sem spadá drtivá většina *chytrých a propojených zařízení a aplikací*.
  - Chytré telefony, počítače, IoT zařízení, operační systémy, databázové servery, mikročipy, inteligentní senzory aj.
- Kategorie produktů (příspěvek od Martina Hurycha)
  - CRA zavádí **rizikové rozdělení produktů do kategorií**, podle kterého se odvíjí přísnost hodnocení ("conformity assessment")

MUNI LAW

Klasifikace produktů

- **Ostatní (“default”) produkty:** Sem patří všechny produkty s digitálními prvky, které **nejsou** zařazeny na seznamy významných ani kritických. Tvoří většinu (~90%) trhu.
- **Důležité produkty třídy I a II:** Jde o produkty, u nichž selhání může mít vážnější dopady, a plní důležité bezpečnostní funkce. **Příloha III CRA** obsahuje seznam *důležitých produktů* rozdělený na **třídu I a II** podle míry kritičnosti.
  - *Příklady:* Třída I může zahrnovat identity management systémy, VPN software, SIEM nástroje, operační systémy aj. Třída II pak např. firewally, IDS/IPS systémy, hypervisory, bezpečnostní čipy apod.
- **Kritické produkty (“Critical – Příloha IV”):** Nejužší kategorie pro produkty, jejichž kompromitace by měla **zásadní dopad na bezpečnost**. **Příloha IV CRA** vypočítává konkrétní kritické produkty, např. *hardwarová zařízení pro zabezpečené operace (HSM moduly), chytré měřiče a brány, smartkarty a podobné bezpečnostní prvky.* Tyto produkty jsou považovány za tak důležité, že vyžadují nejpřísnější postup posouzení shody.

Posouzení shody dle klasifikace

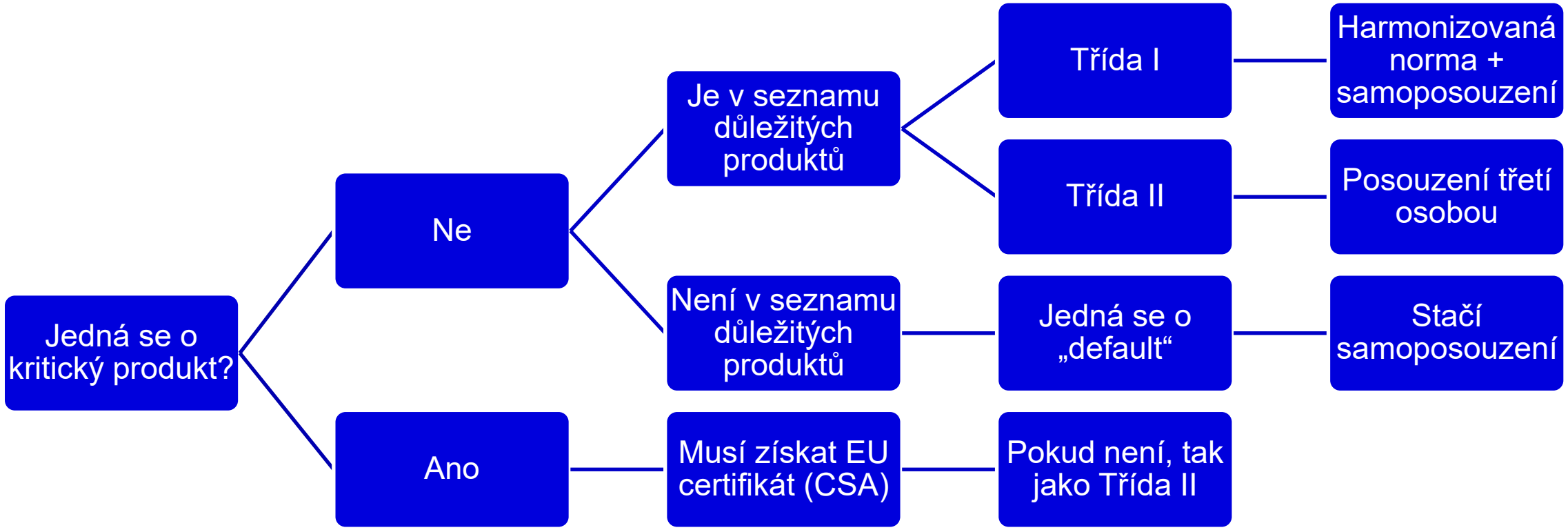
- **Posouzení shody:** Každý výrobek musí před uvedením na trh projít procesem posouzení shody s požadavky CRA.
  - **“Default” (ostatní) produkty:** *Vlastní posouzení výrobcem* – výrobce provede **interní hodnocení rizik a splnění** všech tzv. *essential requirements* CRA a vydá **EU prohlášení o shodě**. Není vyžadována účast nezávislé třetí strany. To uleví méně rizikovým produktům, avšak výrobce plně odpovídá za správnost.
  - **Důležité produkty – Třída I:** Zde se počítá s možností **použít harmonizované normy** – pokud EU vydá harmonizované standardy pokrývající požadavky CRA pro daný typ produktu a výrobce je aplikuje, může *opět stačit interní postup*. Pokud ale takové standardy **nejsou k dispozici nebo výrobek nesplňuje úplně normu**, **nastupuje třetí strana** (notifikovaný subjekt) stejně jako u třídy II.

Posouzení shody dle klasifikace

- **Posouzení shody:** Každý výrobek musí před uvedením na trh projít procesem posouzení shody s požadavky CRA.
  - **Důležité produkty – Třída II:** *Povinné zapojení notifikované osoby.* Výrobce musí oslovit akreditovaný orgán (notified body), který provede **nezávislé hodnocení**. Typicky se využije buď **EU přezkoušení typu (modul B + C přílohy VIII CRA)**, nebo **posuzování shody založené na komplexním zabezpečování kvality (modul H přílohy VIII CRA)** známé z rámce posuzování shody. Tato třetí strana ověří splnění požadavků a vydá certifikát či schválení.

  - **Kritické produkty:** *Nejpřísnější režim.* Pokud pro daný produkt existuje relevantní **evropské certifikační schéma kyberbezpečnosti (CSA)**, **musí** výrobce získat certifikát podle tohoto schématu (alespoň na úrovni významné). Pokud není schéma, postupuje se jako u důležitých produktů ve II. třídě.
- Po úspěšném posouzení shody (ať interním či s pomocí třetí strany) výrobce **vydá EU prohlášení o shodě a opatří produkt označením CE**. CE značka tak nově bude indikovat i splnění kyberbezpečnostních požadavků. Spotřebitelé a zákazníci by díky tomu měli snadno rozpoznat bezpečné produkty

CRA – posouzení shody



MUNI LAW

CRA – základní povinnosti výrobců a dodavatelů

- Security by Design – Navrhnout, vyvíjet a vyrábět bezpečně (na základě analýzy rizik)
- Zajistit aktualizace a podporu (v rámci „support period“)
- Mít technickou dokumentaci s výsledky analýzy rizik
- EU prohlášení o shodě a CE označení
- Monitoring zranitelností a incidentů (mj. CVD)

- *Výrobce chytrých žárovek může mít ISO 9001 a 27001 pro kvalitu a bezpečnost řízení. Podle CRA však musí zajistit konkrétně, že žárovka nebude mít defaultní heslo pro Wi-Fi modul, bude podporovat bezpečné šifrování komunikace a že výrobce poskytne aktualizace firmwaru. To možná částečně dělal, ale nyní to bude muset* ***formálně doložit*** *a zohlednit při návrhu každé nové verze produktu – nutná GAP analýza.*

Předpoklad shody

- K čemu je certifikát dle CSA v CRA (mimo kritické produkty)?
  - **“Presumpce shody” a zjednodušení posuzování:** Pokud je produkt **certifikován podle evropského schématu** (např. EUCC, EUCS) na odpovídající úrovni, **předpokládá se**, že produkty s digitálními prvky jsou ve shodě s CRA.
  - **Je ale nutná věcná souvislost!**

  - V únoru 2025 vydala ENISA studii navrhující, jak uznat **EUCC certifikaci jako doklad plnění CRA** (což by znamenalo, že např. certifikovaný produkt by automaticky splňoval příslušné *essential requirements* podle Přílohy I CRA).
    Toto propojení je výhodné pro výrobce – **jedno důkladné testování může pokrýt více povinností**.

  - **V technických požadavcích není plný překryv!! Např. cloud-based řešení jsou pro EUCC obecně problematické, mj. kvůli specifikaci TOE. EUCC nepokrývá všechny bezpečnostní požadavky CRA.**

MUNI LAW

Soulad CAB podle CSA i pro CRA

- Mezi požadavky CSA a CRA na CAB (notifikované subjekty) je extenzivní překryv.
  - Právní status a nezávislost
  - Nestrannost a odpovědnost
  - Technická způsobilost a postupy
  - Důvěrnost a transparentnost
- ENISA shledala, že pouze s relativně malými úpravami mohou obě role být zastávány jedním subjektem.
- V zásadě by takový krok byl vítaný. Takový subjekt jednoduše zvládne kontrolovat překryvy/mezery mezi CSA a CRA.

Praktické problémy

- Dostupnost harmonizovaných norem včas – pokud nebudou, bude nutné volit notifikované osoby (zkušenosti z CSA), což bude dražší a potenciálně problematické pro SME
- Kapacity CAB a ITSEF (i notifikovaných osob) – administrativní překážky, opět problematické pro SME
- Byrokratická zátěž
- Ohrožení trhu certifikačními magnáty
  - 24 CAB, primárně Francie, Německo, Španělsko a Švédsko
- Flexibilita CRA v kontextu vývoje (vs. CSA)
- Kontrola – dohled nad CSA i CRA má NÚKIB. Trh je veliký, NIS2 též

Otázky?

MUNI
LAW

MUNI
LAW

Děkuji za pozornost!

Jakub.vostoupal@law.muni.cz