

EU certifikace KB

29. 5. 2024

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Simona Vyšatová
odbor regulace



CSA

Akt o kybernetické bezpečnosti

L 151/15

(Text s významem pro EHP)

vzhledem k těmto důvodům:



CRA

Akt o kybernetické odolnosti

- **průlomová unijní legislativu na poli kybernetické bezpečnosti** s doposud nevídaným dopadem na unijní trh a uživatele
- **nařízení** – je přímo účinné – nevyžaduje transpozici či přijetí na národní úrovni
- za cíl zavést **povinné požadavky na kybernetickou bezpečnost softwarových a hardwarových produktů**, kterými se podmíní jejich vstup na vnitřní trh a které bude nutné naplňovat po dobu jejich životního cyklu.
- vytváří kategorii tzv. **produktů s digitálními prvky**
- dalším cílem je **snížit počet zranitelností** v produktech a **zlepšit informovanost uživatelů** v otázkách kybernetické bezpečnosti produktů



CRA bude vstupovat v účinnost natřikrát:

- 18 a 21 měsíců po vstupu v platnost, kdy začnou platit některá ustanovení,
- 36 měsíců po vstupu v platnost, kdy začne platit nařízení jako celek,
- předpokládaný vstup v účinnost celého nařízení je Q3/Q4 2027.

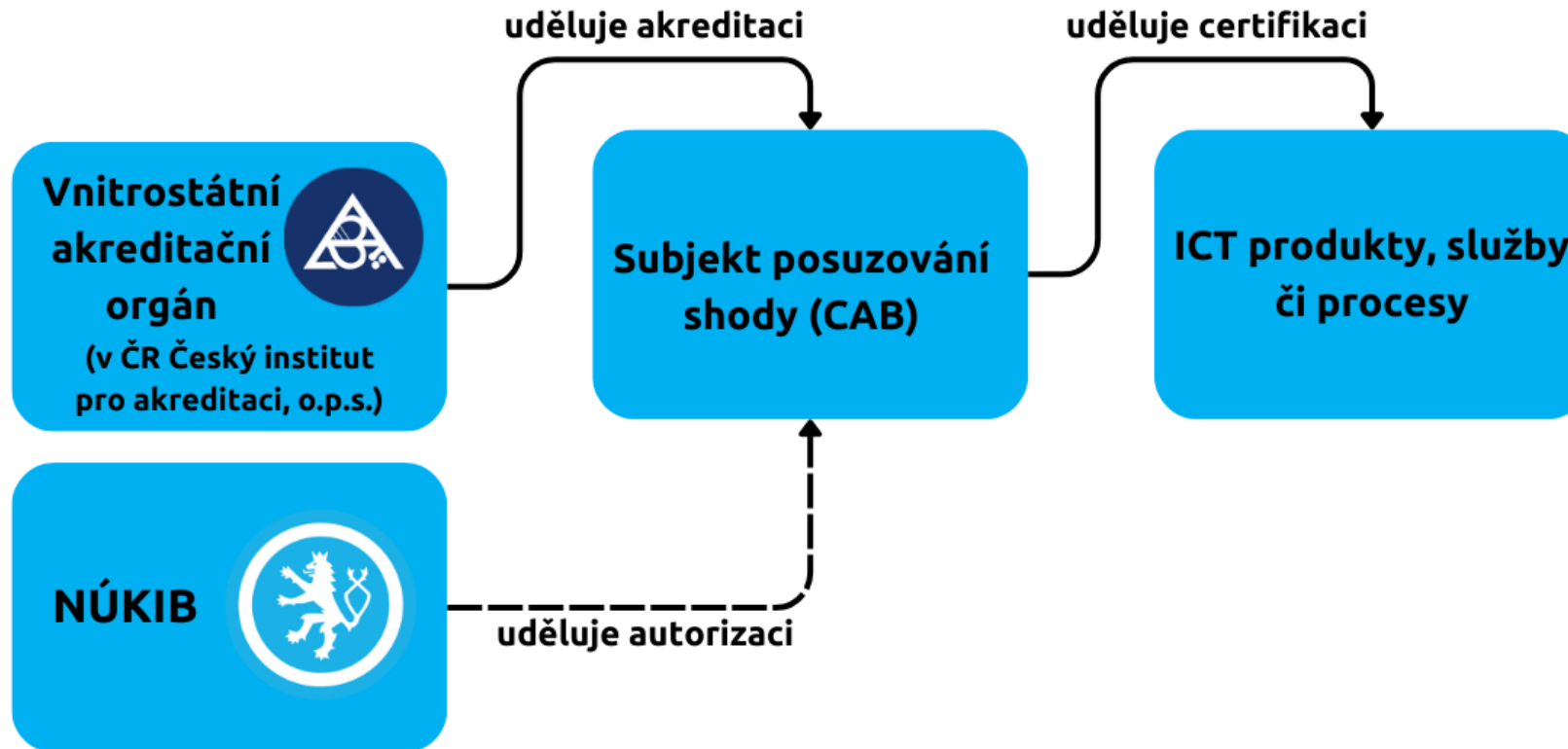


- **dopadají na všechny produkty s digitálním prvkem s cílem zaručit jeho kybernetickou bezpečnost po celou dobu životního cyklu**
- **přináší základní bezpečnostní požadavky pro výrobce produktů s digitálním prvkem, které podmíní vstup takového produktu na unijní trh**
 - výrobci např. budou povinni zajistit, že produkt je na trh uveden bez známých zneužitelných zranitelností a je možné na něm defaultně automaticky instalovat bezpečnostní aktualizace
 - výrobce bude taktéž povinen provést posouzení kyberbezpečnostních rizik spojených s daným produktem.



Úvod do světa certifikací:

rozdíl mezi certifikací, akreditací a autorizací, role NÚKIB a dalších orgánů





- existuje mnoho druhů certifikačních schémat
- mezinárodní uznání certifikací se liší, což vytváří složitost v oblasti standardizace

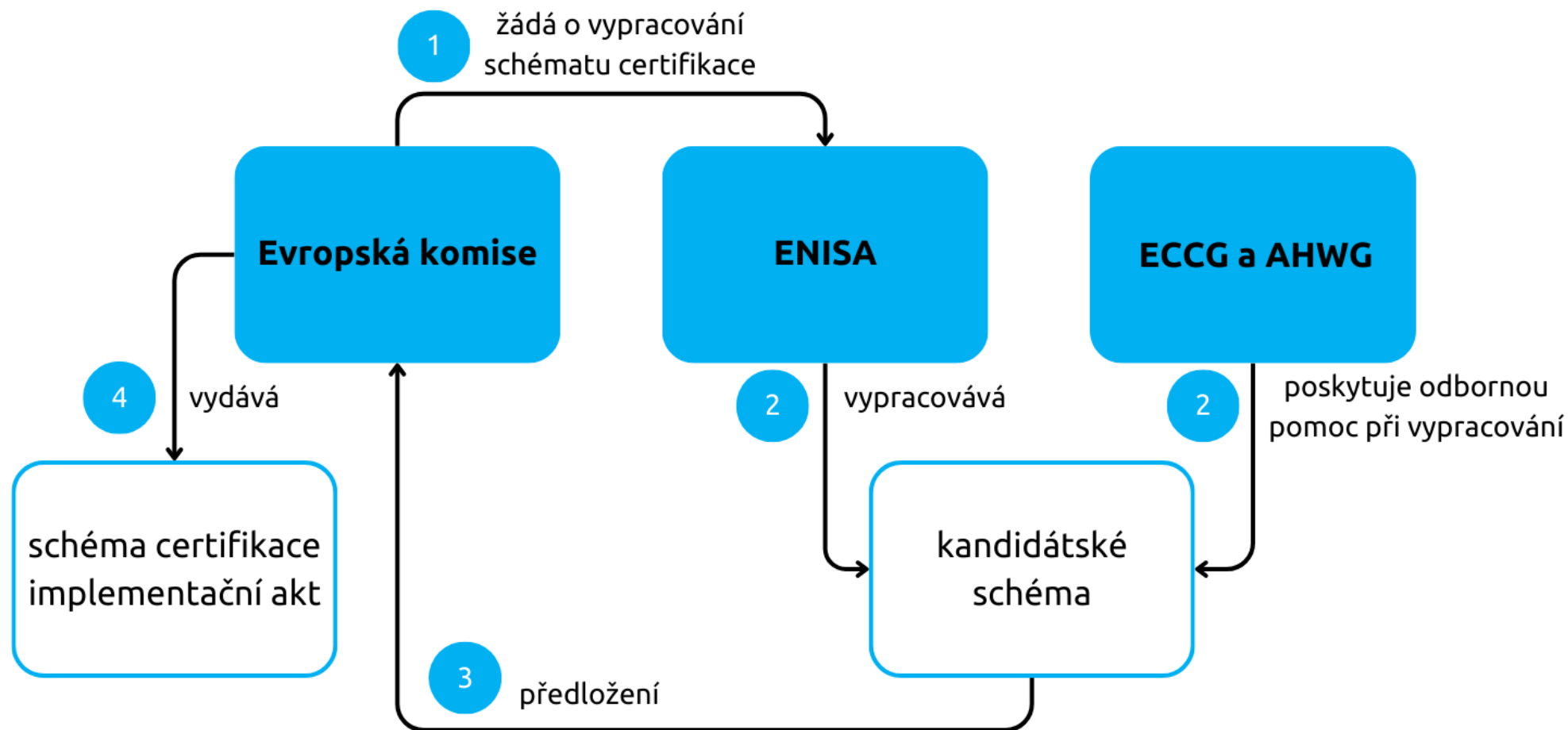
Snahy Evropské unie:

- vytvoření jednotného certifikačního rámce
- harmonizace pro vybrané ICT produkty, procesy a služby
- zvýšení kybernetické bezpečnosti ICT produktů, procesů a služeb
- nastolení důvěry v ICT produkty





- **Akt o kybernetické bezpečnosti (CSA)**
- **Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.)**
 - role NÚKIB jako orgán certifikace kybernetické bezpečnosti (§ 22 písm. y), autorizace (§ 22b)
- **Nový legislativní rámec (NLF)**
 - zákon o technických požadavcích na výrobky (č. 22/1997 Sb.)
 - zákon o posuzování shody stanovených výrobků při jejich dodávání na trh (č. 90/2016 Sb.)





Současná schémata:

- **EUCC** (Common Criteria)
- **EUCS** (Cloud Services)
- **EU5G** (5G)

Schémata, o kterých se uvažuje, že by mohla být vydána:

- Certifikace digitálních peněženek
- Certifikace řízených bezpečnostních služeb (managed security services)

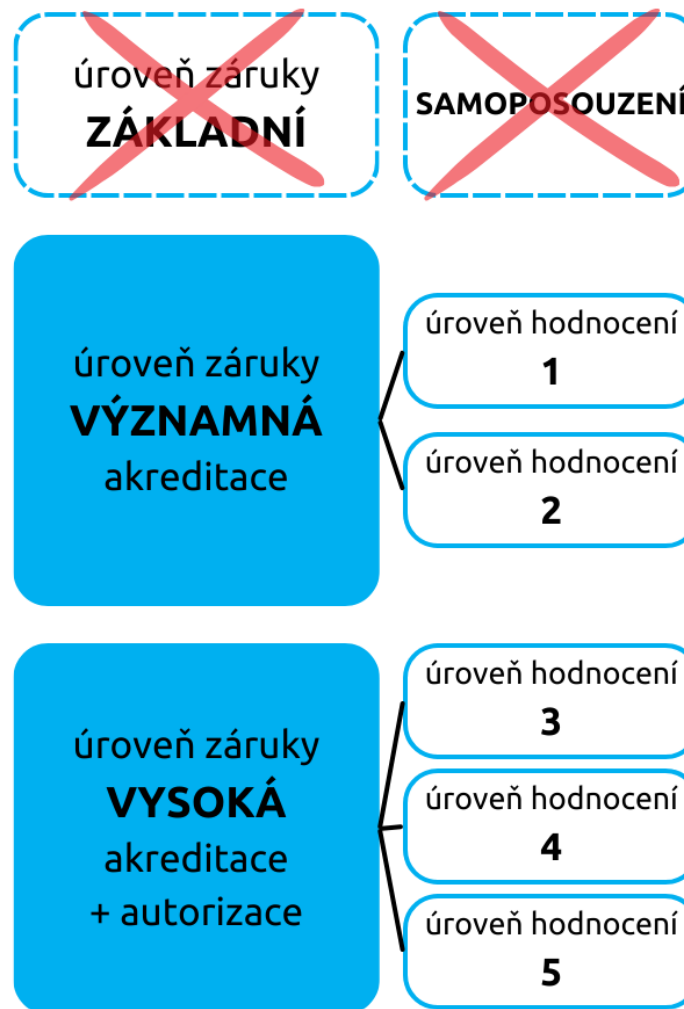
31. 1. 2024 byl zveřejněn implementační akt (vč. příloh) pro EUCC

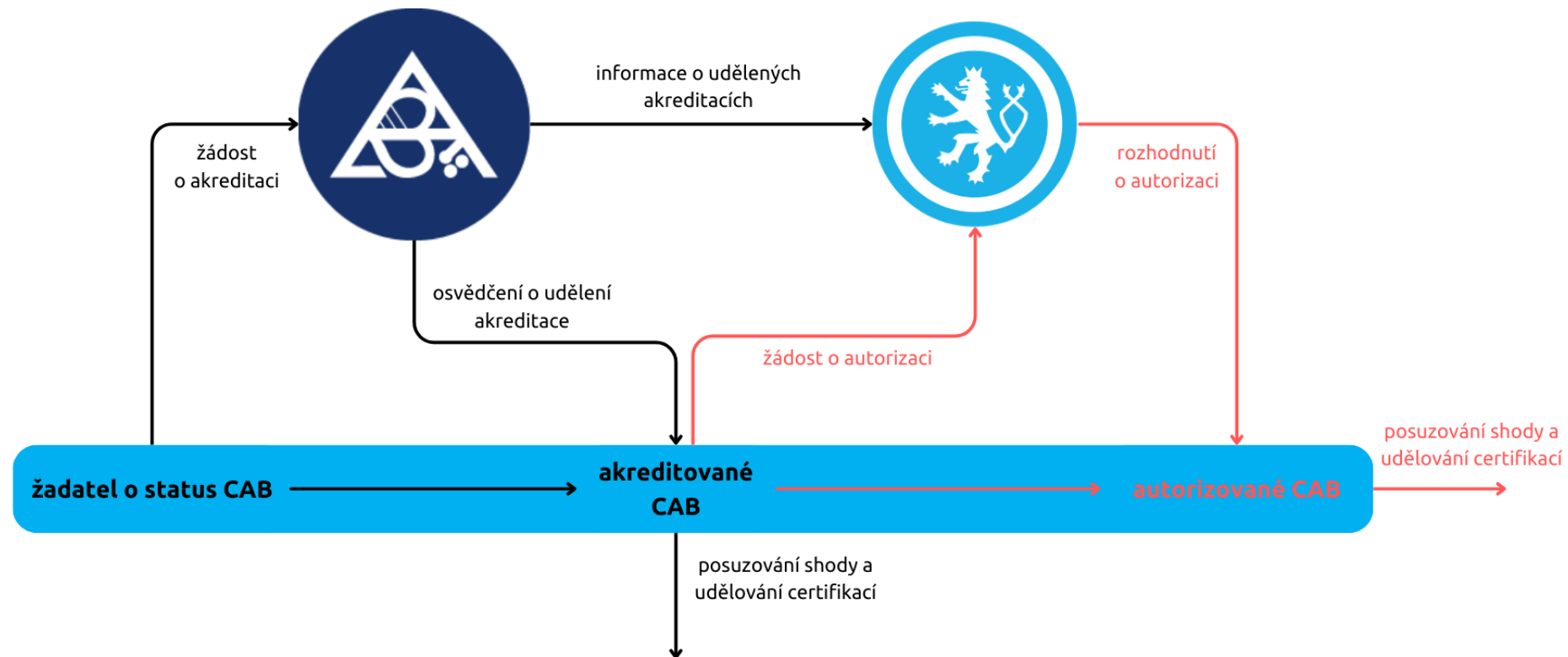
- hlavní cíl = sjednotit a upřesnit pravidla, povinnosti a strukturu evropského systému certifikace kybernetické bezpečnosti založeného na „společných kritériích“ (EUCC), např.:
 - Podmínky pro vydání certifikátu EUCC a doba platnosti, dodatečné požadavky pro autorizaci, hodnocení a zapojení laboratoří, notifikace a monitoring.
- přílohy: State of the Art document, technické požadavky, ochranné profily, obsah certifikátu, vyobrazení označení
- udělování akreditací od **27. 2. 2024** (vydávání certifikátů od **27. 2. 2025**)



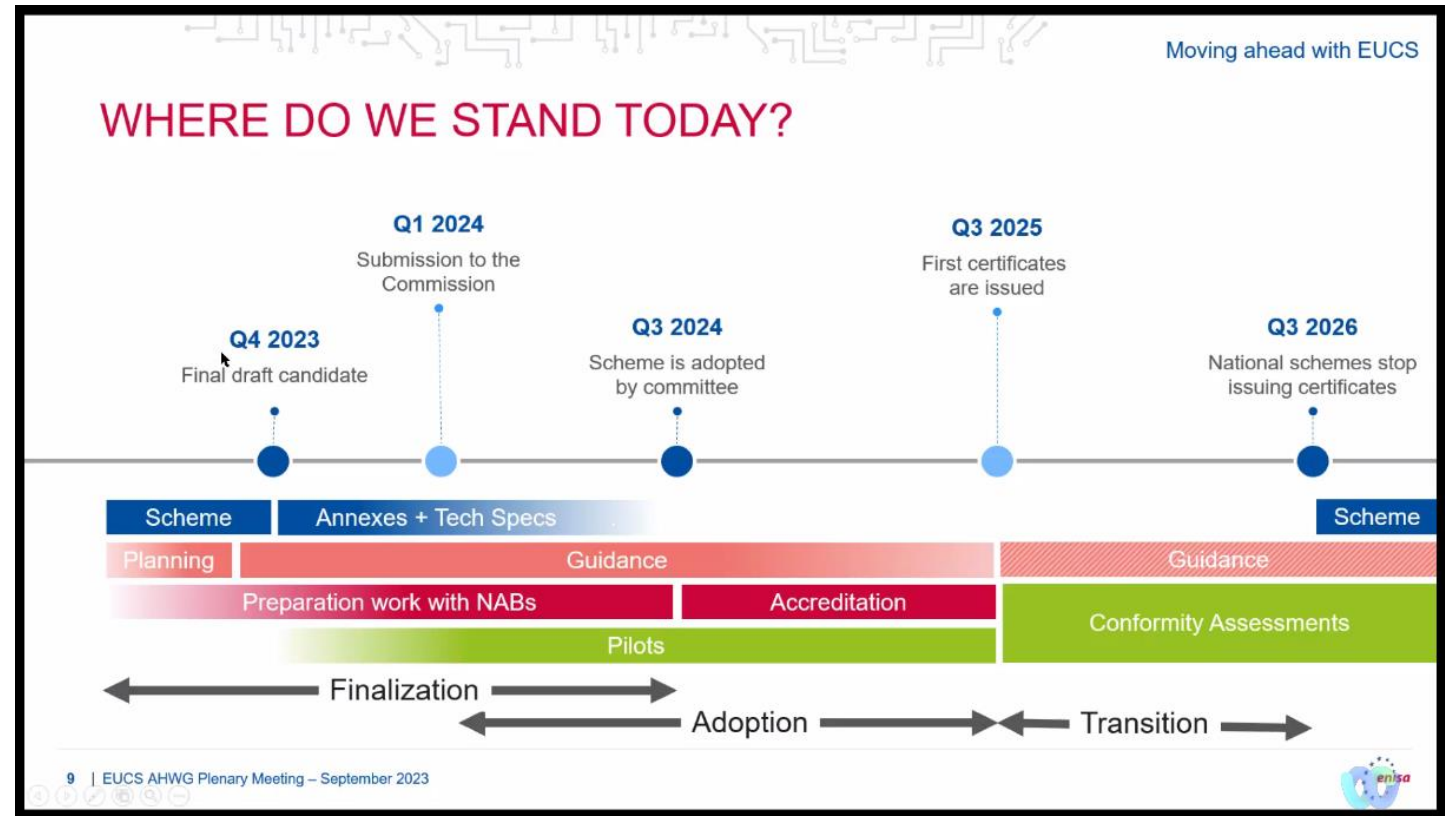
- dobrovolné certifikační schéma
- platnost certifikace je maximálně 5 let
- certifikace ICT produktů (technologické komponenty, hardware, software)
- stanovuje 2 úrovně záruky a vylučuje samoposouzení
 - **významná** – akreditace
 - **vysoká** – akreditace & autorizace

Proces akreditace a autorizace pro EUCC





EUCS – Evropská certifikace cloudových služeb





- Cílem systému EUCS je **zlepšit podmínky na vnitřním trhu a zvýšit úroveň zabezpečení široké škály cloudových služeb** a cloudových schopností, které implementují (schopností aplikací, infrastruktury a platforem).
- Systém EUCS je **technický nástroj určený k poskytování informací zákazníkům** a umožnění jim **činit informovaná rozhodnutí**.
- Poslední neveřejný draft z března 2024, aktuální (a velmi ambiciózní) cíl Komise je v září mít EUCS vydané včetně prováděcího aktu



EU5G – aktuality

- pro vybrané aspekty/komponenty 5G, čerpá se z 5G toolboxu, GSMA dokumentů (NESAS a SAS schémat), plánuje se také znovuvyužití některých postupů z EUCC a EUCS
 - přípravy jsou zpomaleny a prioritu dostala jiná certifikační schémata
 - představení návrhu od agentury ENISA s veřejným připomínkováním je plánováno na duben 2024 (Spring Cyber Security Certification Week 2024 v Bruselu)



- vydán 7. února 2024
- odkazuje na legislativní vývoj a přináší strategické priority
- odkaz zde:

[Union Rolling Work Programme for European cybersecurity certification | Shaping Europe's digital future \(europa.eu\)](https://europa.eu/european-council/en/press-releases/stories/2024/02/european-cybersecurity-certification-shaping-europe-digital-future_240207)





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:	1. prosince 2023
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



Typy aktivit:

- budování kapacit
- testování a certifikace ICT produktů, ICT služeb nebo ICT procesů
- audit infrastruktury
- standardizační aktivity

Cílové skupiny:

- (budoucí) subjekty pro posuzování shody (CAB – certifikační orgány, laboratoře)
- akreditační orgány
- SME (výrobci/dodavatelé, uživatelé ICT zařízení)



nkc.nukib.gov.cz





eucertifikace.nukib.gov.cz

EU certifikace kybernetické bezpečnosti

Autorem a garantem obsahu je:

NÚKIB 

SAVE THE DATE – 14. listopadu 2024: konference NÚKIB k EU certifikacím



certification.enisa.europa.eu

EU Cybersecurity Certification

Brings trust to the market of ICT products,
services and processes across the Union and
beyond.





NÚKIB

Vnitrostátní orgán certifikace kybernetické bezpečnosti – ncca@nukib.gov.cz

- možnost zasílání novinek
- změna kontaktní osoby – simona.vysatova@nukib.gov.cz, +420 702 146 354

ČIA

Národní akreditační orgán

- Ing. Milan Svoboda, svobodam@cai.cz (certifikační orgány certifikující produkty)
- Ing. Jan Velíšek, velisekj@cai.cz (zkušební a kalibrační laboratoře)
- Ing. Gor Petrosjan petrosjang@cai.cz (zkušební laboratoře technické)

PROSTOR NA DOTAZY

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost