Úvod do evropských certifikací kybernetické bezpečnosti

Ing. Markéta Šilhavá,
odbor regulace

12.04.2023

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

PROGRAM:

- PROČ A CO ?
- JAK TO VŠECHNO VZNIKNE A KDO TO VYMYSLÍ?
- CO TO ZNAMENÁ PRO VÝROBCE?
- KDO BUDE PROVÁDĚT CERTIFIKACE?
- JAKÉ JSOU POVINNOSTI NÚKIB?
- MOŽNOSTI FINANCOVÁNÍ
- SHRNUTÍ

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

Akt o kybernetické bezpečnosti (nařízení č. 2019/881):

- Agentura ENISA
- Evropský rámec pro certifikaci kybernetické bezpečnosti

ČSN EN ISO/IEC 17000:

- Posuzování shody
- Vlastní posuzování shody / certifikace
- Schéma posuzování shody
- Systém posuzování shody

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

PROČ A CO?

Jaké ICT produkty, procesy nebo služby?

- Evropská komise
- Strategické priority

Průběžný pracovní program Unie:

a) existující pravidla pro certifikace konkrétní skupiny ICT produktů
b) relevantní politika nebo právo Unie či členského státu
c) tržní poptávka
d) vývoj v oblasti kybernetických hrozeb
e) žádost o vypracování konkrétního návrhu systému ze strany Evropské skupiny pro certifikaci kybernetické bezpečnosti (ECCG)

Úvod do EU certifikací KB

PROČ A CO?

Co pro nás kybernetická bezpečnost vlastně znamená?
Bezpečnostní cíle

a) chránit proti náhodnému nebo neoprávněnému ukládání, zpracování, přístupu nebo sdělování

b) chránit údaje proti náhodnému nebo neoprávněnému zničení, ztrátě nebo změně nebo proti nedostupnosti

c) zajistit přístup pouze k údajům, službám nebo funkcím, jichž se týkají jejich přístupová práva

Úvod do EU certifikací KB

PROČ A CO?

Čeho chceme dosáhnout?
Bezpečnostní cíle

d) identifikovat a zdokumentovat známé případy závislosti a známé zranitelnosti
e) zaznamenat přístup, použití nebo jiné zpracování, kdy k tomu došlo a kdo tak učinil
f) kontrolovat přístup, použití nebo jiné zpracování, kdy k tomu došlo a kdo tak učinil
g) ověřit, že produkty, služby a procesy IKT neobsahují žádné známé zranitelnosti

Úvod do EU certifikací KB

PROČ A CO?

Čeho chceme dosáhnout?
Bezpečnostní cíle

h) včas obnovit dostupnost a přístup k nim v případě fyzických nebo technických incidentů

i) zajistit zabezpečení na úrovni standardního nastavení a výchozího návrhu

j) zajistit poskytování s aktualizovaným softwarem a hardwarem, které neobsahují veřejně známé zranitelnosti, a aby obsahovaly mechanismy pro bezpečné aktualizace

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

PROČ A CO?

RŮZNÉ POUŽITÍ – RŮZNÁ ÚROVEŇ RIZIKA

RŮZNÉ ÚROVNĚ ZÁRUKY

- Základní
- Významná
- Vysoká

SPECIFIKACE POŽADAVKŮ NA ICT PRODUKTY, PROCESY NEBO SLUŽBY

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

JAK TO VŠECHNO VZNIKNE A KDO TO VYMYSLÍ?

Vznik schématu posuzování shody:

- Žádost o návrh
- Návrh - ENISA
- Konzultace/ připomínkování
- Předložení Komisi
- Zpracování návrhu právního předpisu se schématem

Úvod do EU certifikací KB

JAK TO VŠECHNO VZNIKNE A KDO TO VYMYSLÍ?

Vznik schématu posuzování shody:

- Připomínkování – veřejnost, ECCG
- Zapracování připomínek
- Hlasování
- Stanovení
- Platnost
- Účinnost

Úvod do EU certifikací KB

JAK TO VŠECHNO VZNIKNE A KDO TO VYMYSLÍ?

Připravovaná schémata:

- EUCC – evropské schéma založené na Common critériích
- EUCS – evropské schéma pro cloudové služby
- EU5G – evropské schéma pro 5G sítě

Více info:
https://www.enisa.europa.eu/topics/certification
https://certification.enisa.europa.eu/

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

CO TO ZNAMENÁ PRO VÝROBCE?

Dobrovolné certifikace = možnost posouzení shody UZNÁVANÉ V CELÉ EU

Nízké riziko – úroveň záruky základní
Vlastní posouzení shody
EU prohlášení o shodě

Posouzení shody = certifikace
Posouzení certifikačním orgánem
Certifikát

Úvod do EU certifikací KB

KDO BUDE PROVÁDĚT CERTIFIKACE?

ČSN EN ISO/IEC 17011:

- Orgán (subjekt) posuzování shody
  - Certifikační orgán

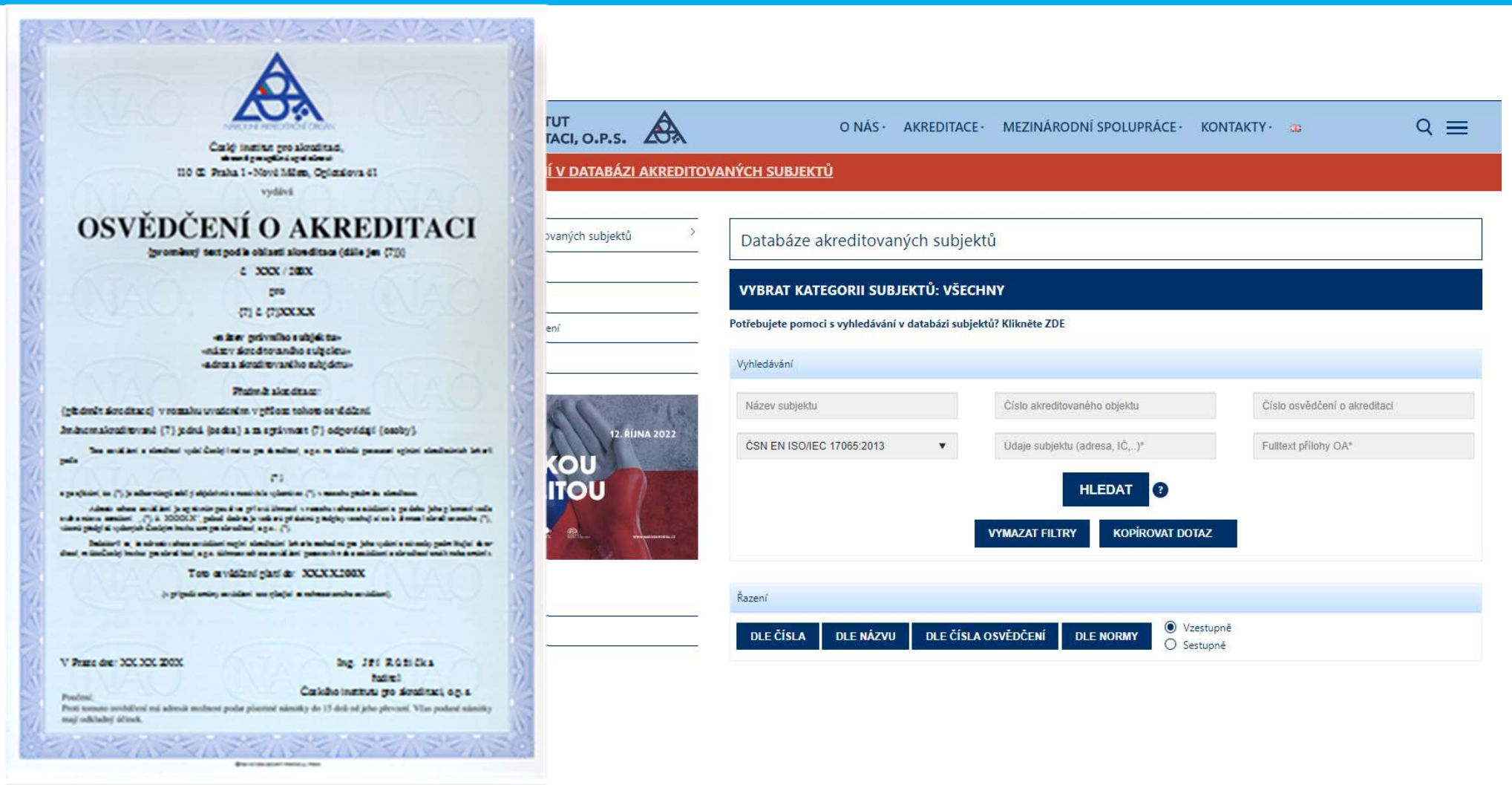
- Akreditace (nařízení č. 765/2008)
  - Národní akreditační orgán – Český institut pro akreditaci, o.p.s.

Případně také u specifických případů:

- Autorizace
  - Vnitrostátní orgán certifikace kybernetické bezpečnosti - NÚKIB

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost



Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

ČESKÝ INSTITUT PRO AKREDITACI, O.P.S.

O NÁS · AKREDITACE · MEZINÁRODNÍ SPOLUPRÁCE · KONTAKTY ·

VYHLEDÁVÁNÍ V DATABÁZI AKREDITOVANÝCH SUBJEKTŮ

- Databáze akreditovaných subjektů
- Aktuality
- Semináře ČIA
- Dokumenty ke stažení
- Časté dotazy

- Laboratoře
- Inspekční orgány
- Certifikační orgány
- Ověřovací a validační orgány
- Poskytovatelé PT
- Výrobci referenčních materiálů

Certifikační orgány certifikující produkty

„Akreditací se rozumí oficiální uznání (reprezentované vydáním Osvědčení o akreditaci), že certifikační orgán je způsobilý provádět certifikaci produktů"

Akreditace certifikačních orgánů certifikujících produkty se řídí požadavky normy ČSN EN ISO/IEC 17065:2013 (Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby) a MPA 40-01-..

*Produkt je termín zahrnující i proces a službu ve smyslu normy ČSN EN ISO/IEC 17065:2013, čl. 3.4.

Garant pro oblast certifikačních orgánů certifikujících produkty:		
Ing. Milan Svoboda	272 096 208, 724 797 777	svobodam@cai.cz
Zástupce garanta pro oblast certifikačních orgánů certifikujících produkty:		
Ing. Jaroslav Janák	272 096 204, 724 695 677	janakj@cai.cz

seznam_certifikacnich_schemat-2022-8-24 Stáhnout

Informační dopisy

Dokumenty ke stažení

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost

O NÚKIB | INFOSERVIS | ÚŘEDNÍ DESKA | KYBERNETICKÁ BEZPEČNOST | OCHRANA UI V ICT | GALILEO PRS | KONTAKTY | CS / EN

- Národní výzkum a vývoj
- Mezinárodní výzkum a vývoj
- EU certifikace kybernetické bezpečnosti
- Publikace
- Kontakty

NÚKIB › Kybernetická bezpečnost › Výzkum › EU certifikace kybernetické bezpečnosti

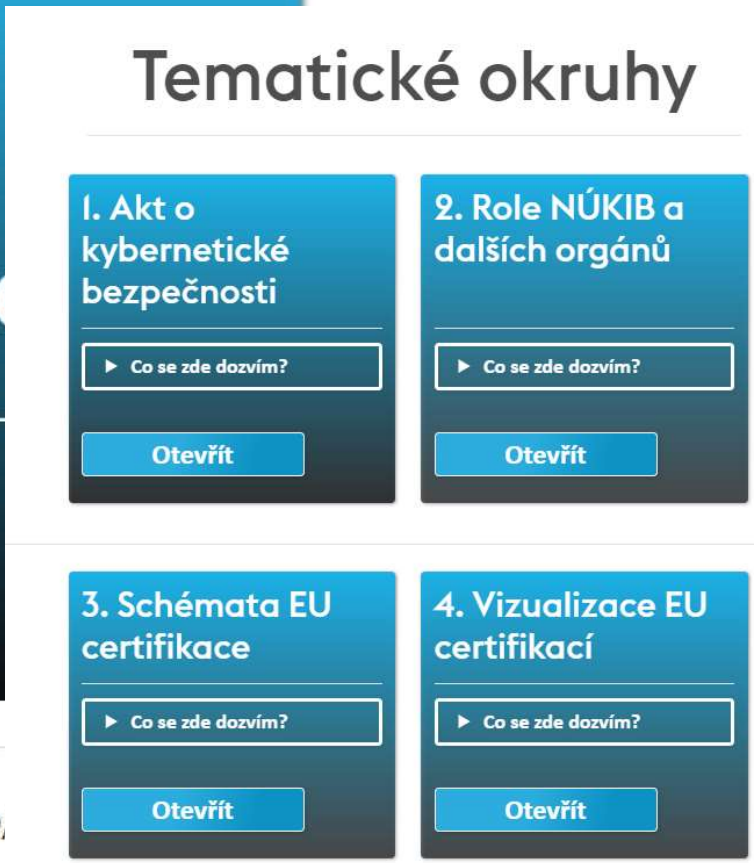
EU certifikace kybernetické bezpečnosti

Smyslem EU certifikace kybernetické bezpečnosti, která je upravena přímo nařízením Evropského Parlamentu a Rady (EU) 2019/881 („Akt o kybernetické bezpečnosti"), je zvyšování důvěry v produkty, služby a procesy v oblasti informačních a komunikačních technologií skrze jejich bezpečnost. Certifikací se osvědčí, že produkty, služby a procesy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, důvěrnosti a integrity.

V rámci evropského rámce certifikace kybernetické bezpečnosti bude NÚKIB dohlížet na pravidla zahrnutá v evropských systémech certifikace kybernetické bezpečnosti a tato pravidla vymáhat, napomáhat Českému institutu pro akreditaci, o.p.s. při monitorování činnosti subjektů posuzování shody, v příslušných případech autorizovat subjekty posuzování shody, delegovat vydávání certifikátů na úrovni záruky vysoká a řešit stížnosti podané fyzickými nebo právnickými osobami v

Úvod do EU certifikací KB

Národní úřad pro kybernetickou a informační bezpečnost



V červnu 2019 vstoupilo v platnost nařízení Evropského parlamentu a Rady (EU) 2019/

„**akt o kybernetické bezpečnosti**“, „Akt“), které zavádí **evropský rámec pro certifikaci kybernetické bezpečnost produktů, služeb a procesů informačních a komunikačních technologií (ICT)**. Cílem

Úvod do EU certifikací KB

JAKÉ JSOU POVINNOSTI NÚKIB?

NÚKIB zastupuje ČR v ECCG a ve Výboru pro komitologii

NÚKIB = vnitrostátní orgán certifikace KB může:

- Provádět certifikace pro úroveň záruky vysoká
- Delegovat provádění certifikací pro úroveň záruky vysoká
- Zastupovat ČR v pracovních skupinách ENISA pro návrh certifikačních schémat

Úvod do EU certifikací KB

JAKÉ JSOU POVINNOSTI NÚKIB?

NÚKIB = vnitrostátní orgán certifikace KB musí:

- autorizovat subjekty posuzování shody pro určitá schémata, dále na základě kontrol omezovat, pozastavovat nebo odebírat autorizace
- provádět dohled nad produkty, procesy a službami ve shodě s CSA (posouzení subjektem posuzování shody nebo vlastní provedené výrobcem/poskytovatelem)
- provádět dohled nad subjekty posuzování shody veřejnými a spolupracovat s ČIA dohledu nad akreditovanými

Úvod do EU certifikací KB

JAKÉ JSOU POVINNOSTI NÚKIB?

NÚKIB = vnitrostátní orgán certifikace KB musí:

- řešit stížnosti
- předkládat výroční zprávu agentuře ENISA a ECCG; účastnit se jednání ECCG;
- sdílet informace o možných případech nesouladu s požadavky CSA nebo jednotlivých schémat
- sledovat vývoj v oblasti
- účastnit se vzájemného hodnocení za účelem harmonizace postupů vnitrostátních orgánů certifikace KB

Úvod do EU certifikací KB

JAKÉ JSOU POVINNOSTI NÚKIB?

Přestupky:

- **Výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající EU prohlášení o shodě**
- **Držitel evropského certifikátu kybernetické bezpečnosti**
- **Právnická nebo podnikající fyzická osoba**

Pokuty do (aktuálně):

- **5 000 000 Kč**
- **1 000 000 Kč**
- **100 000 Kč**

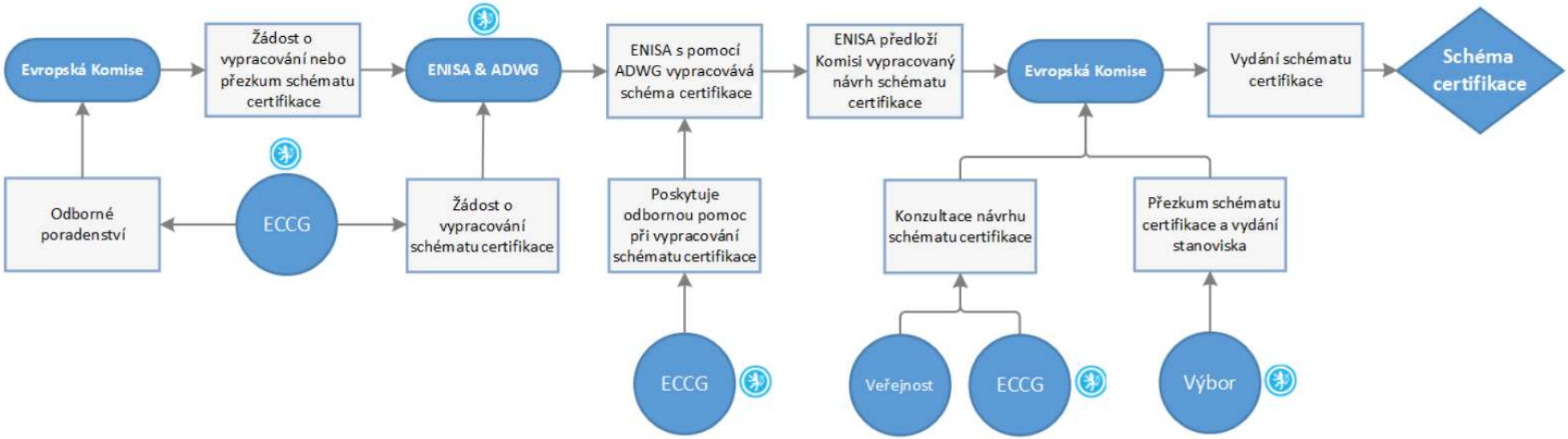
MOŽNOST FINANCOVÁNÍ

Digital Europe Programme (DIGITAL)

- Work programme: Cybersecurity Work Programme 2023-2024
  1. 5 Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies
- Planned opening date: Q3-2023 / Q2-2024
- Deadline date: Q1-2024 / Q3-2024
- Simple grant
- Indicative budget EUR 30 million / ?
- Indicative duration of the action 36 months / ?
- Indicative budget per grant (EU contribution) EUR 1 - 2 million / ?
- Implementation ECCC (Národní koordinační centrum, NÚKIB – ncc@nukib.cz)

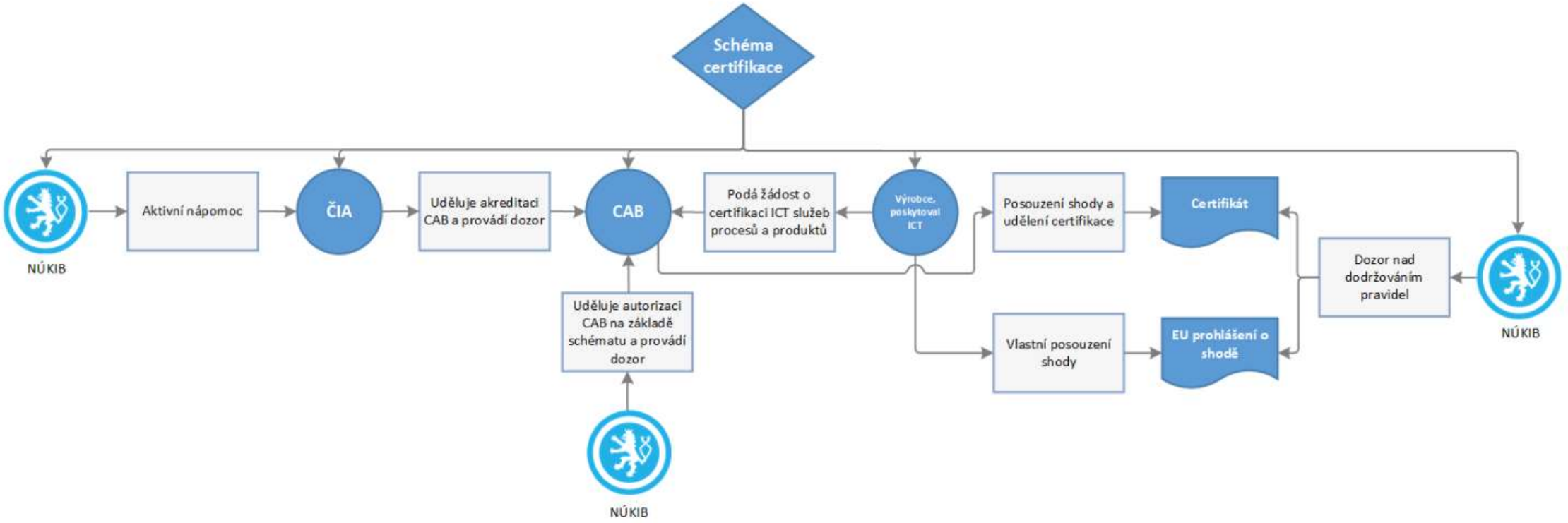
Úvod do EU certifikací KB

SHRNUTÍ



Úvod do EU certifikací KB

SHRNUTÍ



Národní úřad
pro kybernetickou
a informační bezpečnost

OTÁZKY A ODPOVĚDI

Národní úřad
pro kybernetickou
a informační bezpečnost

DĚKUJI ZA POZORNOST
A PŘEJI VÁM KRÁSNÝ DEN

Ing. Markéta Šilhavá
702 160 590
m.silhava@nukib.cz / ncca@nukib.cz