

ROZUMÍTE CERTIFIKACÍM?

ZATÍM NE



FESTIVAL BEZPEČNÉHO INTERNETU

Úvod do evropských certifikací kybernetické bezpečnosti

26.10.2022

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost



PROGRAM:

- ORGANIZAČNÍ POKYNY A ÚVOD
- 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
- SHRUTÍ
- KONTAKTY, ZDROJE INFORMACÍ



ORGANIZAČNÍ POKYNY

- Prosím, vypněte si mikrofony a kamery
- V průběhu a na závěr setkání bude prostor pro otázky a odpovědi.
Pro interaktivní komunikaci bude využito webové aplikace SLICO.COM pod #FBI-CSA.
Pokud nebudou otázky zodpovězeny na tomto setkání, budou odpovědi zaslány emailem na všechny zúčastněné
- Pokud bude v průběhu prezentace uváděn odkaz na nějakou dokumentovanou informaci dostupnou na webových stránkách, je link připraven v seznamu odkazů ve SLIDO pod #FBI-CSA
- S ohledem na plánovanou délku trvání tohoto setkání neplánujeme přestávku
- UPOZORNĚNÍ: PREZENTACE JE NAHRÁVÁNA

slido



**Join at slido.com
#FBI-CSA**

① Start presenting to display the joining instructions on this slide.



**JAK BYSTE OHODNOTILI SVOJE ZNALOSTI
V OBLASTI EVROPSKÝCH CERTIFIKACÍ
KYBERNETICKÉ BEZPEČNOSTI?**

① Start presenting to display the poll results on this slide.



ÚVOD - NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

- Ústřední správní orgán, který vznikl 1. srpna 2017

Poslání NÚKIB

- Posilujeme bezpečnost a odolnost České republiky v kyberprostoru

Vize NÚKIB

- Jsme profesionální a důvěryhodnou autoritou a lídrem v informační a kybernetické bezpečnosti doma i v zahraničí
- Neustále se učíme a adaptujeme, chceme být připraveni i na to, co teprve přijde
- Inspirujeme, vedeme a podporujeme společné úsilí v budování bezpečné informační společnosti
- Jsme tým, ve kterém chtějí lidé pracovat



ÚVOD - Evropské certifikace kybernetické bezpečnosti

Akt o kybernetické bezpečnosti:

- 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



PROČ A CO?





PROČ A CO?



shutterstock.com · 2114637353



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 od zástupců členských států



PROČ A CO?

Když používáme IC T produkty

Co chceme?

Co potřebujeme?

Co očekáváme?

Bezpečnost

Kybernetickou bezpečnost



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



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



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



PROČ A CO?

RŮZNÉ POUŽITÍ – RŮZNÁ ÚROVEŇ RIZIKA

RŮZNÉ ÚROVNĚ ZÁRUKY

- Základní
- Významná
- Vysoká

SPECIFIKACE POŽADAVKŮ NA ICT PRODUKTY, PROCESY NEBO SLUŽBY



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



JAK TO VŠECHNO VZNIKNE A KDO TO VYMYSLÍ?

Vznik schématu posuzování shody:

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



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





Standards and Certification

▸ Standards

▾ Certification

▸ EU Cybersecurity Certification
- FAQ

▸ Public Consultation on
Cybersecurity Schemes

▸ Ad-hoc Working Groups calls

▸ ENISA survey on the EU
Cybersecurity Market

EU Cybersecurity Certification Framework

Securing network and information systems in the European Union has been deemed as a key objective in an effort to keep the EU online economy functional and secure; it is evident that failure to do so could have far reaching consequences for European citizens and threatens to impact the trust of citizens, the industry and public administration alike. As the role of ENISA has been further bolstered by means of Regulation (EU) 2019/881 (Cybersecurity Act), the important task of cybersecurity certification calls for appropriate stakeholders' involvement and support.

The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to establish and maintain trust and security on cybersecurity products, services and processes. Drawing up cybersecurity certification schemes at the EU level aims at providing criteria to carry out conformity assessments to establish the degree of adherence of products, services and processes against specific requirements. Users and service providers alike, need to be able to determine the level of security assurance of the products, services and processes they procure, make available or use.

Cybersecurity certification requires the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance; as such cybersecurity certification plays a key role in increasing trust and security in products, services and processes. Cybersecurity certification in the EU serves the purpose of providing notice and assurance to users about the level of conformity against stated requirements. EU cybersecurity certification schemes serve as the vehicle to convey such requirements from the EU policy level to the industry service provision level and further to the users and conformity assessment bodies.

As set out in Regulation (EU) 2019/881, the EU cybersecurity certification framework lays down the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more level(s) of assurance (basic, substantial or high), based on the level of risk associated with the envisioned use of the product, service or process.

Mission of ENISA

The mission of ENISA in the area of the EU cybersecurity certification framework is outlined as



Recommended publications

EU Cybersecurity Market Analysis - IoT in Distribution Grid

This report analyses demand and supply of IoT cybersecurity in distribution grids. It provides detailed indications on how this market might further...

Published on April 08, 2022



ENISA Cybersecurity Market Analysis Framework (ECMAF)

Published on April 08, 2022

Methodology for Sectoral Cybersecurity Assessments

Published on September 13, 2021

Public Consultation on the draft Candidate EUCC Scheme

Published on May 26, 2021

Recommended news

Cybersecurity Market Analysis in support of Informed...

The European Union Agency for Cybersecurity (ENISA) introduces a framework to perform cybersecurity market analyses and dives into the market of the...

Published on April 08, 2022

slido



**Join at slido.com
#FBI-CSA**

① Start presenting to display the joining instructions on this slide.

slido



Audience Q&A Session

① Start presenting to display the audience questions on this slide.



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



KDO BUDE PROVÁDĚT CERTIFIKACE?

ČSN EN ISO/IEC 17011:

- Orgán (subjekt) posuzování shody
 - Certifikační orgán
- Akreditace
 - Národní akreditační orgán – Český institut pro akreditaci, o.p.s.

Případně také u vysokého rizika:

- Autorizace
 - Vnitrostátní orgán certifikace kybernetické bezpečnosti - NÚKIB

FBI: Úvod do EU certifikací KB



TUT
TACI, O.P.S.

O NÁS · AKREDITACE · MEZINÁRODNÍ SPOLUPRÁCE · KONTAKTY ·

V DATABÁZI AKREDITOVANÝCH SUBJEKTŮ

Databáze akreditovaných subjektů

VYBRAT KATEGORII SUBJEKTŮ: VŠECHNY

Potřebujete pomoci s vyhledáváním v databázi subjektů? Klikněte ZDE

Vyhledávání

Název subjektu

Číslo akreditovaného objektu

Číslo osvědčení o akreditaci

ČSN EN ISO/IEC 17065:2013

Údaje subjektu (adresa, IČ,...)*

Fulltext přílohy OA*

HLEDAT

HYMAZAT FILTRY

KOPÍROVAT DOTAZ

Řazení

DLE ČÍSLA

DLE NÁZVU

DLE ČÍSLA OSVĚDČENÍ

DLE NORMY

Vzestupně

Sestupně



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 certifikujících 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

janaki@cai.cz

[seznam_certifikacnich_schemat-2022-8-24](#)

[Stáhnout](#)

Informační dopisy

Dokumenty ke stažení



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 právníckými osobami v



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



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



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 schémata
- sledovat vývoj v oblasti
- účastnit se vzájemného hodnocení za účelem harmonizace postupů vnitrostátních orgánů certifikace KB



JAKÉ JSOU POVINNOSTI NÚKIB?

Přestupky:

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

Pokuty do:

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



MOŽNOST FINANCOVÁNÍ

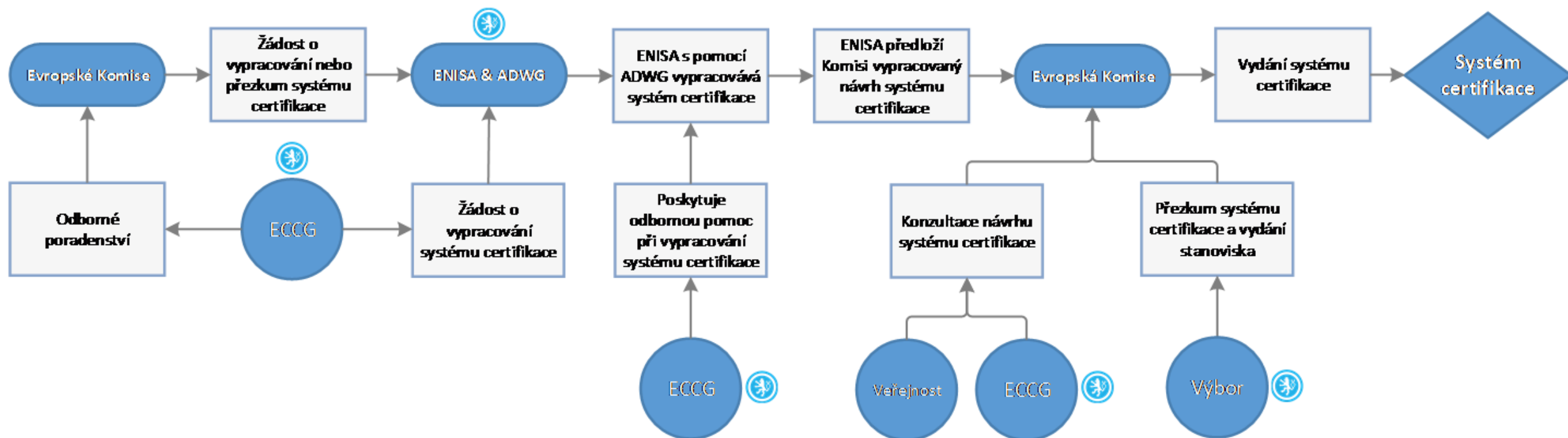
Digital Europe Programme (DIGITAL)

- Work programme part: Digital Europe Work Programme 2021-2022
- Call: Cybersecurity and Trust (DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILITIES - Testing and Certification Capabilities)
- Planned opening date: 15 November 2022
- Deadline date: 15 February 2023 17:00:00 Brussels time
- Grants for Financial Support — 100% funding rate
- Total: 5 000 000 EUR

[Funding & tenders \(europea.eu\)](https://europea.eu)

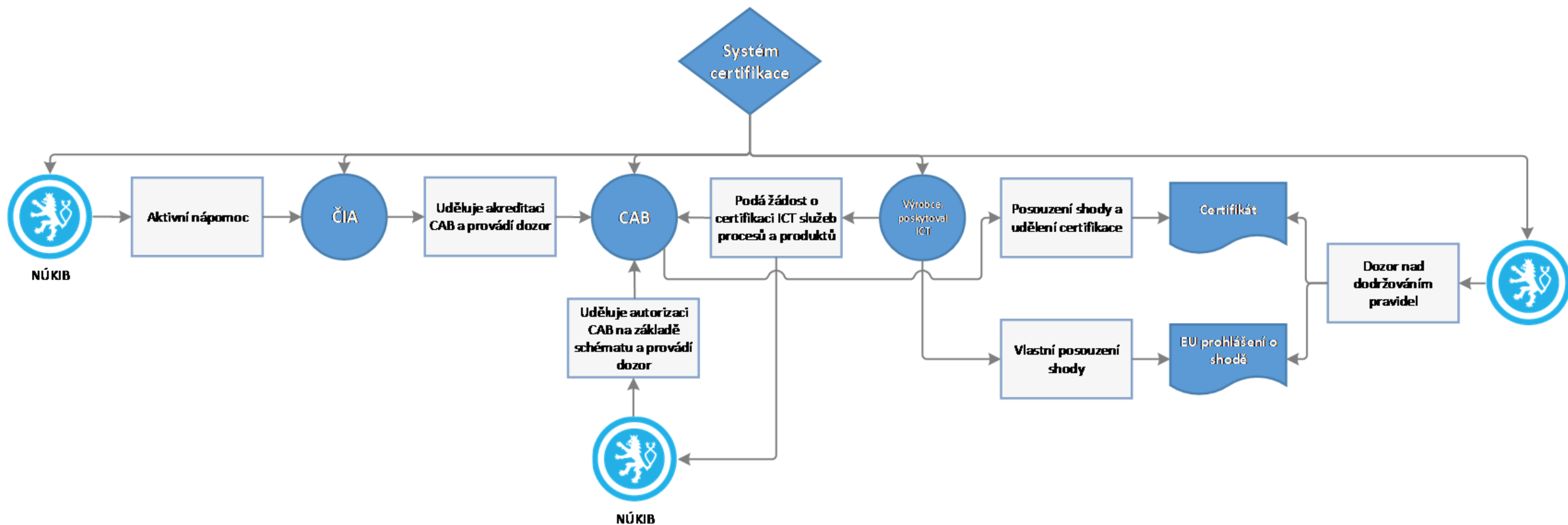


SHRNUTÍ





SHRNUTÍ





SHRNUTÍ - European Cybersecurity Certification - All you need to know





KONTAKTY, ZDROJE INFORMACÍ

NÚKIB

- Osvětové akce, odborná setkání, novinky emailem
- Vnitrostátní orgán certifikace kybernetické bezpečnosti – ncca@nukib.cz
- Ing. Markéta Šilhavá, +420 702 160 590, m.silhava@nukib.cz
- Bc. František Grossmann, +420 720 061 890, f.grossmann@nukib.cz

Český institut pro akreditaci, o.p.s.

- Ing. Milan Svoboda, +420 724 797 777, svobodam@cai.cz



KONTAKTY, ZDROJE INFORMACÍ

[EUR-Lex - 32019R0881 - CS - EUR-Lex \(europa.eu\)](#)

[Kybernetická bezpečnost: jak EU řeší kybernetické hrozby - Consilium \(europa.eu\)](#)

[The European Cybersecurity Certification Group | Shaping Europe's digital future \(europa.eu\)](#)

[ENISA \(europa.eu\)](#)

[Certification — ENISA \(europa.eu\)](#)

[ENISAvideos - YouTube](#)

slido



**Join at slido.com
#FBI-CSA**

① Start presenting to display the joining instructions on this slide.

slido



Audience Q&A Session

① Start presenting to display the audience questions on this slide.

slide
**JAK BYSTE NYNÍ OHODNOTILI
SVOJE ZNALOSTI V OBLASTI
EVROPSKÝCH CERTIFIKACÍ
KYBERNETICKÉ BEZPEČNOSTI?**



DĚKUJI ZA POZORNOST
Ing. Markéta Šilhavá
m.silhava@nukib.cz
+420 702 160 590
ncca@nukib.cz

ⓘ Start presenting to display the poll results on this slide.



DĚKUJI ZA POZORNOST
A PŘEJI VÁM KRÁSNÝ DEN

Ing. Markéta Šilhavá
m.silhava@nukib.cz
+420 702 160 590
ncca@nukib.cz