MUNI
LAW

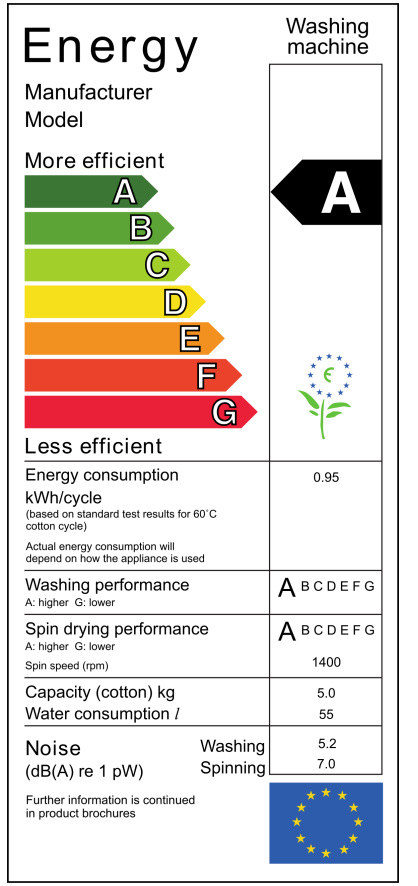
Certifikace dle Aktu o kybernetické bezpečnosti

Václav Stupka

MUNI
LAW

Proč certifikace?

Prokázání compliance



MUNI LAW

Certifikace v kybernetické bezpečnosti

- Rodina standardů ISO/IEC 27K
- Common criteria - ISO/IEC 15408
  - Jde o rámec – Targets of Evaluation (TOE); Protection Profiles (PP); Securit targets (ST)
  - Více úrovní ochrany (EAL)
  - Mutual recognition agreements uzavřené uznávajícími státy
  - SOG-IS MRA (producenti a konzumenti certifikace) – tvorba vlastních PPs
- V některých členských státech národní a sektorové certifikační mechanismy
  - (Německo, Nizozemsko, Itálie, Francie Finsko, UK)

MUNI LAW

Motivace

- Posílení jednotného digitálního trhu
- Performativní charakter regulace
- Nedostatečné povědomí spotřebitelů a podniků
- Rozdíly v přístupu jednotlivých členských států
- Dosažení vyšší úrovně bezpečnosti produktů, služeb a procesů (není ale očekávána garance)
- Směřování ke standardům security by design & default

MUNI
LAW

Kyberbezpečnostní certifikace EU

EU rámec pro kyberbezpečnostní certifikace

- Upraven v hlavě III Aktu o kybernetické bezpečnosti
- Stanovuje jen rámec (zásady, cíle, charakter, procesy, institucionální zajištění)
- Harmonizovaný přístup
  - Zvýšení úrovně bezpečnosti v rámci celé EU
- Certifikace produktů, služeb a procesů postavená na analýze rizik
- Výstupem jsou:
  - EU kyberbezpečnostní certifikáty
  - EU prohlášení o shodě

MUNI LAW

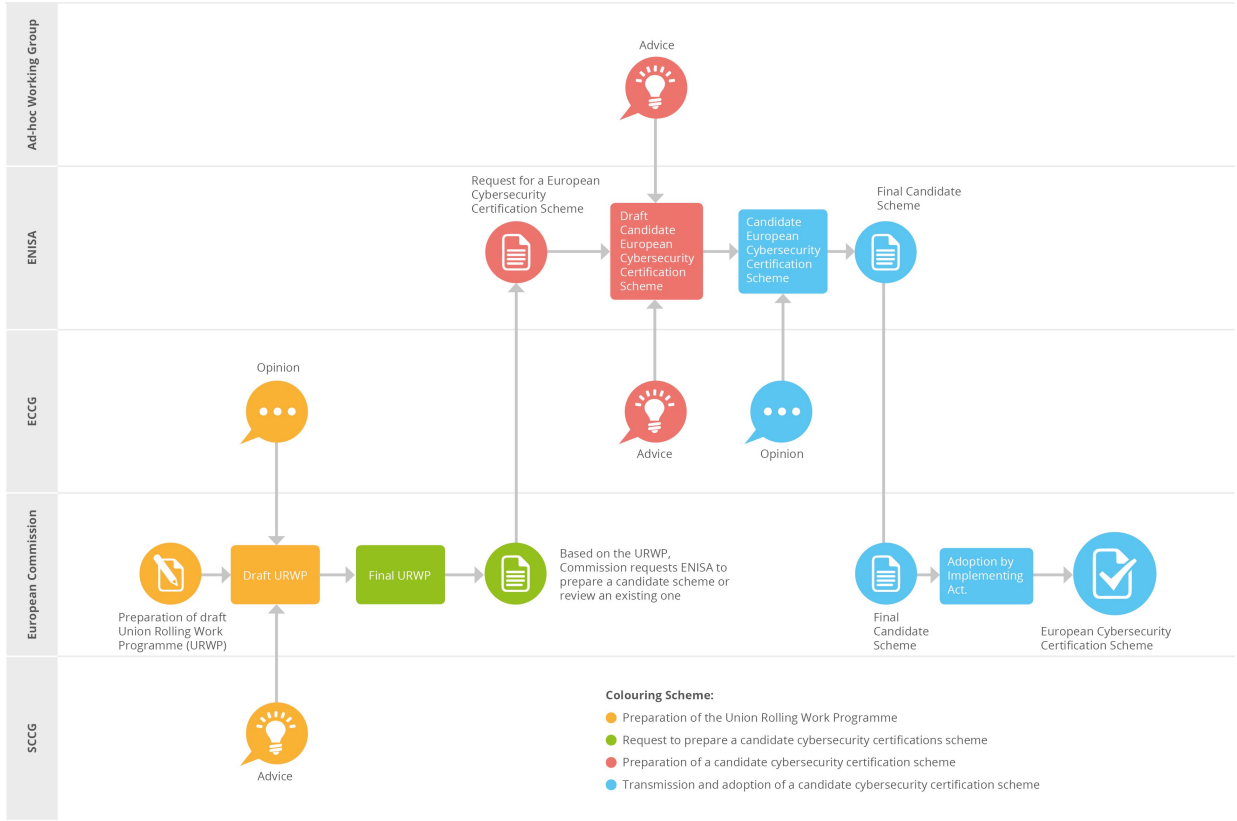
Certifikační schémata/systémy

- Hlavní nástroj certifikace
- Mají obsahovat alespoň:
  - Kategorie krytých produktů/služeb/procesů
  - Kyberbezpečnostní požadavky (standardy, technické specifikace)
  - Způsob posouzení shody (self-assessment, third party)
  - Úrovně záruky
- Může navazovat akreditační schéma definující požadavky na CAB, nebo certifikační laboratoře

Úrovně záruky

- Vyjadřuje, jak náročnými testy produkt/služba/proces prošel a jakým hrozbám by měl být schopen čelit
- Tři úrovně:
  - **Základní**
    dosažení bezpečnostních požadavků minimalizujících známá základní rizika incident;
    zpravidla jen přezkum dokumentace
  - **Významná**
    známá základní rizika a útoky prováděné subjekty s omezenými dovednostmi a zdroji;
    přezkum neexistence známých zranitelností a zkouška bezpečnostních funkcionalit
  - **Vysoká**
    minimalizace rizik sofistikovaných kybernetických útoků prováděných subjekty s významnými dovednostmi a zdroji;
    vyloučení známých zranitelností, zkouška nejnovějších bezpečnostních funkcionalit, penetrační testování
- Každé schéma/systém může zahrnovat jednu nebo více úrovní

Příprava certifikačních schémat/systémů



MUNI LAW

Vnitrostátní certifikáty

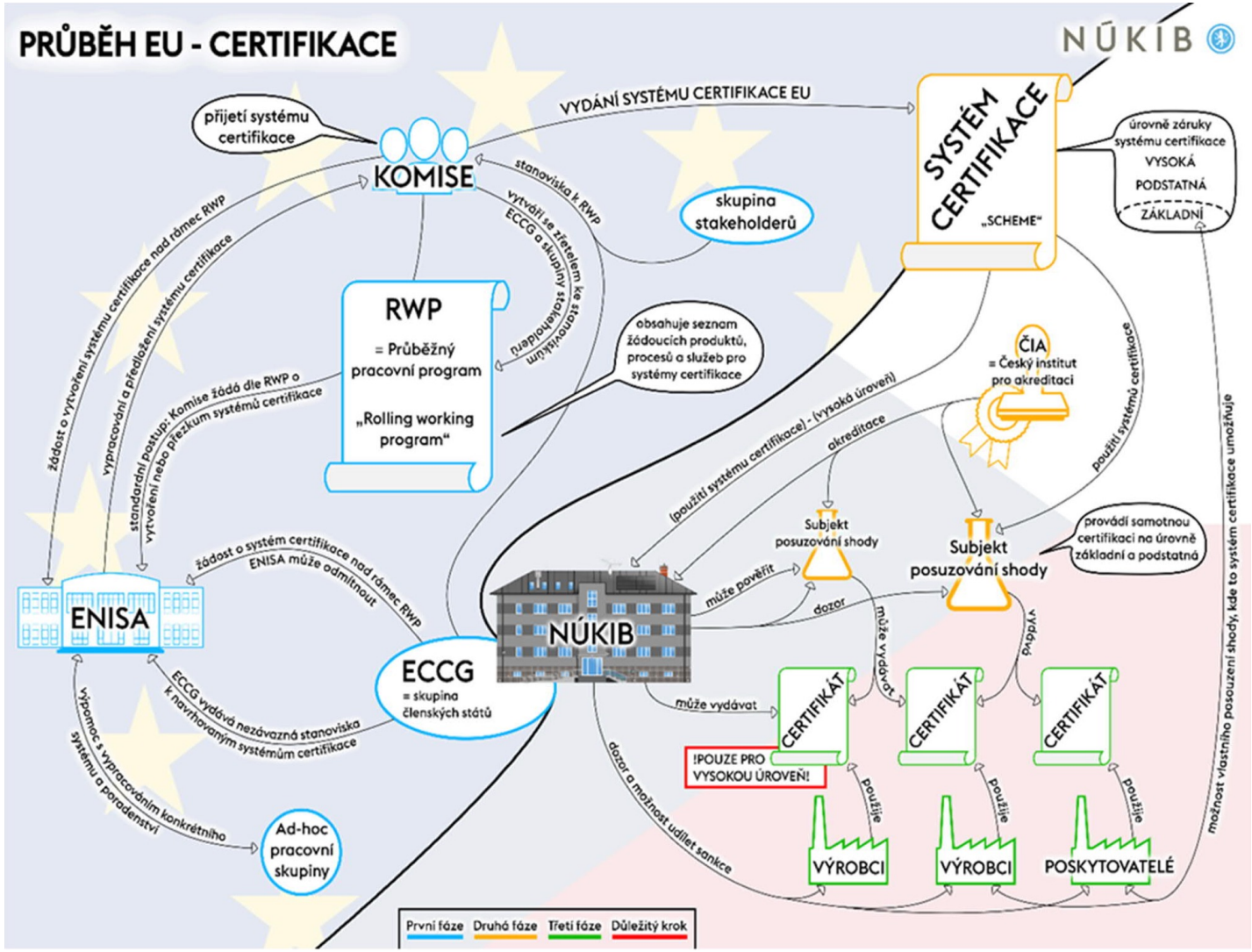
- Členské státy mohou vytvářet vlastní certifikační schémata/systémy
- Jen tam, kde neexistují evropská
- Povinnost notifikovat Komisi a ECCG
- Stávající systémy platné do konce platnosti I když jsou konkurenční

MUNI LAW

Certifikace/posuzování shody

- Není povinné (není-li stanoveno jinak!)
- Vlastní hodnocení (self-assessment) -> prohlášení o shodě
  - Sám výrobce ověří a deklaruje soulad s požadavky certifikačního schématu
  - Možné jen u základní úrovně
- Certifikace –> certifikát
  - Provádí v závislosti na úrovni CAB/orgán certifikace
  - Na žádost výrobce – ten volí z dostupných úrovní
  - Ověřování ve spolupráci s certifikační laboratoří
- Konkrétní průběh a parametry určuje schéma/systém

MUNI LAW


PRŮBĚH EU - CERTIFIKACE
NÚKIB
přijetí systému certifikace
KOMISE
VYDÁNÍ SYSTÉMU CERTIFIKACE EU
SYSTÉM CERTIFIKACE
„SCHEME"
úrovně záruky systému certifikace
VYSOKÁ
PODSTATNÁ
ZÁKLADNÍ
skupina stakeholderů
stanoviska k RWP
vytváří se zřetelem ke stanoviskům ECCG a skupiny stakeholderů
RWP
= Průběžný pracovní program
„Rolling working program"
obsahuje seznam žádoucích produktů, procesů a služeb pro systémy certifikace
žádost o vytvoření systému certifikace nad rámec RWP
vypracování a předložení systému certifikace
standardní postup: Komise žádá dle RWP o vytvoření nebo přezkum systémů certifikace
ČIA
= Český institut pro akreditaci
(použití systému certifikace) - (vysoká úroveň)
akreditace
použití systémů certifikace
Subjekt posuzování shody
Subjekt posuzování shody
provádí samotnou certifikaci na úrovně základní a podstatná
žádost o systém certifikace nad rámec RWP
ENISA může odmítnout
ENISA
NÚKIB
může pověřit
dozor
může vydávat
vydává
ECCG
= skupina členských států
ECCG vydává nezávazná stanoviska k navrhovaným systémům certifikace
CERTIFIKÁT
CERTIFIKÁT
CERTIFIKÁT
!POUZE PRO VYSOKOU ÚROVEŇ!
může vydávat
použije
použije
použije
VÝROBCI
VÝROBCI
POSKYTOVATELÉ
dozor a možnost udělit sankce
možnost vlastního posouzení shody, kde to systém certifikace umožňuje
výpomoc s vypracováním konkrétního systému a poradenství
Ad-hoc pracovní skupiny
První fáze
Druhá fáze
Třetí fáze
Důležitý krok

MUNI LAW

Novela ZoKB (?)

- Vnitrostátním orgánem podle aktu NÚKIB
- Možnost uzavření veřejnoprávní smlouvy – pro vysokou úroveň
- Sankce (certifikované subjekty, CAB, držitelé certifikátu)

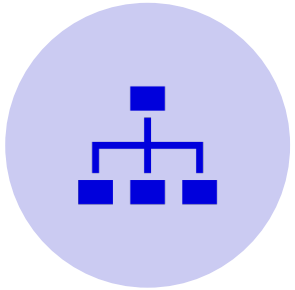
MUNI
LAW

Institucionální zajištění

ENISA (EU)

Zajišťuje tvorbu certifikačních schémat/systémů (podle URWP nebo na žádost komise)

Monitoruje hrozby, stav techniky, standardy –> zohledňuje při tvorbě schémat/systémů



Vyhodnocuje, případně reviduje stávající schémata/systémy

Poskytuje odbornou a metodickou podporu

Komise (EU)

Připravuje URWP

Zadává přípravu schémat/systémů ENISA

Přijímá schémata/systémy formou implementačních aktů

Hodnotí fungování rámce i jednotlivých schémat v EU trhu

Uzavírá smlouvy s třetími státy o uznávání certifikátů

ECCG, SCCG a pracovní skupiny (EU)

- **ECCG**
  - Zástupci členských států (od nás NÚKIB)
  - Zasahují do tvorby URWP a přípravy schémat/systémů
- **SCCG**
  - Zástupci standardizačních organizací, průmyslu, sdružení
  - Zasahuje do tvroby URWP, konzultační role
- **Ad-hoc pracovní skupiny**
  - Zástupci odborné veřejnosti
  - Sestavuje ENISA pro potřeby přípravy jednotlivých schémat

MUNI LAW

Národní autorita pro certifikace (ČS)

- Orgán veřejné moci (u nás NÚKIB)
- Úkoly:
  - Dohled a kontrola nad certifikacemi (CAB, self-assessment, laboratoře)
  - Provádění certifikací v úrovni vysoká – nebo delegace této povinnosti
  - Přijímání stížností z certifikačního procesu
  - Ukládání sankcí
- Peer-review mechanismus

Subjekty posuzování shody (ČS)

- Provádí ověřování shody a vydává certifikáty
- Musí být akreditovány podle ISO/IEC 17065 (ČIA), případně na specifické požadavky schémat
- Mohou vykonávat posuzování shody jen pro vybraná schémata
- Vnitrostátní subjekt, musí prokázat nezávislost
- Musí disponovat potřebným technickým a personálním zázemím

Certifikační laboratoř

- Provádí zkoušky a testování v rozsahu svojí odbornosti
- Nutná akreditace podle ISO/IEC17025 - ČIA
- Nejsou blíže stanovené požadavky na charakter provozovatele

MUNI
LAW

Certifikační systémy/schémata

EUCC – EU Common criteria

- Postaveno na principech Common Criteria, není sektorově ani technologicky specifické
- Využije dostavadní infrastrukturu SOG-IS
- Univerzální schéma postavené na uplatnění Protection profiles
- Zaměřeno na certifikaci produktů
- V současnosti publikované v podobě Candidate scheme
- Nepočítá se s umožněním self-assessmentu

EUCS – EU Cloud Services scheme

- Certifikace cloudových služeb (plánováno v návrhu URWP)
- Všechny stupně záruky
- Nepočítá se se self assessmentem
- V současnosti publikovaný draft schématu

EU5GS – EU 5G scheme

- Příprava mimo URWP na žádost Komise
- Postaveno na 5G toolboxu
- Uvažované typy schémat:
  - Certifikace kritických síťových komponent a funkcí 5G sítí
  - Certifikace dodavatelských vývojových, developerských, dodavatelských a udržovacích procesů
- Sestavena pracovní skupina, zatím nepublikován žádný návrh

MUNI

LAW