III. odborné setkání – implementace nařízení EU o certifikaci kybernetické bezpečnosti IKT

24.02.2021

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

III. odborné setkání k CSA

Organizační pokyny

- Prosím, vypněte si kamery a mikrofony, pokud nemluvíte k účastníkům.

- Na závěr setkání budou otázky a odpovědi.
  Po každé části bude prostor na krátké otázky a odpovědi k jednotlivým tématům.
  Pro interaktivní komunikaci bude využito webové aplikace SLICO.COM pod #3CSA.
  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 #3CSA.

- S ohledem na plánovanou délku trvání tohoto setkání neplánujeme přestávku.

slido

Přidejte se na

slido.com

#3CSA

Úvodní slovo

Ing. Jaroslav Šmíd
Náměstek ředitele, Sekce informační bezpečnosti

III. odborné setkání k CSA

Program:

1. Úvodní slovo
2. Kybernetický balíček EK – Evropská strategie a velká revize směrnice NIS
3. Finanční program Evropské unie Digital Europe programme (DEP)
4. Cloudy:
   a) Návrh EU systému certifikace EUCS – Cloud Services Scheme
   b) Regulace cloudu v ČR a její vztah k evropské certifikaci cloudu (EUCS)
5. Další informace z NÚKIB a Evropské skupiny pro certifikace kybernetické bezpečnosti
6. *Informace z Agentury ČAS k vývoji standardizační činnosti v oblasti CSA*
7. Informace z ČIA a Evropské organizace pro spolupráci v oblasti akreditace
8. Q&A
9. Závěr

Kybernetický balíček EK – Evropská strategie a velká revize směrnice NIS

Jakub Otčenášek
Cyber attaché, Brusel

III. odborné setkání k CSA

Směrnice NIS

- Kybernetický balíček 16. 12. 2020
- Nový návrh NIS (NIS2) v některých ohledech připomíná spíše národní legislativu, které byla původní NIS předlohou.
- Dvě nové kategorie: tzv. *essential entities* (základní subjekty) a *important entities* (důležité subjekty)
- Nové sektory a určování na základě velikosti
- **NIS2 poskytuje právní základ pro povinné užití certifikačních systémů pro naplnění některých bezpečnostních požadavků této směrnice.**

Článek 21

Použití evropských systémů certifikace kybernetické bezpečnosti

1. K prokázání splnění některých požadavků článku 18 mohou členské státy požadovat, aby základní a důležité subjekty certifikovaly některé produkty IKT, služby IKT a procesy IKT podle zvláštních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881. Produkty, služby a procesy podléhající certifikaci mohou být vyvinuty základním nebo důležitým subjektem nebo pořízeny od třetích stran.

2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci upřesňující, které kategorie základních subjektů budou povinny obstarat si certifikát a podle kterých konkrétních evropských systémů certifikace kybernetické bezpečnosti podle odstavce 1. Akty v přenesené pravomoci se přijímají v souladu s článkem 36.

3. Komise může požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2, připravila návrh systému podle čl. 48 odst. 2 nařízení (EU) 2019/881.

III. odborné setkání k CSA

Evropská strategie kybernetické bezpečnosti (ESKB)

- ESKB odkazuje na certifikaci v bodu 1.5, Internet zabezpečených věcí.
- Evropská komise obecně vnímá potřebu zajistit kybernetickou bezpečnost produktů, které mohou komunikovat přes internet
- K této problematice aktuálně probíhá studie proveditelnosti

1.5 Internet zabezpečených věcí

Každý předmět připojený k internetu obsahuje chyby zabezpečení, které lze zneužít s potenciálně rozsáhlými následky. Pravidla vnitřního trhu zahrnují záruky proti nezabezpečeným výrobkům a službám. Komise již pracuje na zajištění transparentních bezpečnostních řešení a certifikace podle aktu o kybernetické bezpečnosti a na podpoře bezpečných produktů a služeb, aniž by byla ohrožena výkonnost.
V prvním čtvrtletí roku 2021 přijme svůj první průběžný pracovní program Unie (bude aktualizován nejméně jednou za tři roky), který umožní, aby se průmysl, vnitrostátní orgány a normalizační orgány mohly předem připravit na budoucí evropské systémy certifikace kybernetické bezpečnosti. Jak se internet věcí rozrůstá, vynutitelná pravidla vyžadují posílení, a to jak k zajištění celkové odolnosti, tak k podpoře kybernetické bezpečnosti.

slido

Přidejte se na

slido.com

#3CSA

Finanční program Evropské unie
Digital Europe programme (DEP)

Mgr. Luboš Fendrych
Ředitel Odboru vzdělávání, výzkumu a projektů

III. odborné setkání k CSA

Program Digitální Evropa (DEP)

- Podpora digitální transformace EU a nasazení nových technologií v praxi, nikoliv výzkum a vývoj (Horizont Evropa)
- Programové období 2021 – 2027
- Podpora pěti oblastí:
  - vývoj vysoce výkonné výpočetní techniky
  - umělá inteligence
  - kybernetická bezpečnost
  - pokročilé digitální dovednosti
  - a zajištění rozsáhlého využívání digitálních technologií v celém hospodářství i společnosti.
- Celková alokace: 7,5 mld. euro

III. odborné setkání k CSA

DEP - cybersecurity – výzva „Testing and certification capabilities“

- **Cíl**: budování kapacit a certifikačních testbedů, výměna zkušeností, zvyšování kvalifikace pracovníků, podpora SMEs provádět certifikace a testování produktů a služeb, včetně realizace auditů
- **Dopad**: posílení testovacích kapacit, snadnější zavádění certifikačních systému v členských zemích EU, posílení vnitřního trhu EU prostřednictvím certifikovaných produktů a služeb
- **Oprávnění žadatelé**: vnitrostátní orgány certifikace kybernetické bezpečnosti, subjekty posuzování shody, vnitrostátní akreditační orgány, SMEs

III. odborné setkání k CSA

DEP - cybersecurity – výzva „Testing and certification capabilities“

- **Alokace**: ~ 15 – 20 milonů eur, 1 – 2 miliony eur na jeden projekt
- **Granty** (50% spolufinancování, v případě SMEs až 75%)
- Výzva vyhlášena pravděpodobně **v roce 2021**
- **Více informací na** Europe investing in digital: the Digital Europe Programme | Shaping Europe’s digital future (europa.eu)

slido

Přidejte se na

slido.com

#3CSA

Návrh EU systému certifikace EUCS – Cloud Services Scheme

Ing. Markéta Šilhavá
Oddělení výzkumu a evropské spolupráce

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

EUCS – Cloud Services Scheme — ENISA (europa.eu)
Zveřejněno 22.12.2020

Stručné informace o schématu byly agenturou ENISA prezentovány dne 11.01.2021 na Webinar - Certification of Cloud Services — ENISA (europa.eu)
K dispozici jsou záznam i prezentace.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- 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**.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Systém EUCS proto **nevymáhá žádná omezení** týkající se zeměpisného umístění údajů nebo jejich zpracování. Vyžaduje však, aby CSP (poskytovatel cloudových služeb) byl ohledně těchto informací **transparentní**, a aby tyto **informace byly veřejně dostupné a srozumitelné** jako součást informací poskytovaných s certifikátem.
- Systém EUCS uznává, že **odpovědnost** za bezpečnost cloudové služby je **rozdělena mezi poskytovatele cloudových služeb** (CSP) a **zákazníka cloudové služby** (CSC), a jeho cílem je ověřit, že toto rozdělení odpovědnosti je výslovně a veřejně dokumentováno CSP.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

Úroveň záruky základní

- známá základní rizika incidenty a kybernetické útoky;
- **nekritická data a systémy**;
- útočníkem jedna osoba s omezenými schopnostmi opakující známé útoky s omezenými zdroji.

Úroveň záruky významná

- známá rizika kybernetické bezpečnosti a rizika incidentů a kyber. útoků prováděných aktéry s omezenými dovednostmi a zdroji;
- **obchodně kritická data a systémy**;
- útočníkem malá skupina osob se schopností útoků a přístupu k širokému rozpětí známých útočných technik s omezenými zdroji.

Úroveň záruky vysoká

- rizika nejmodernějších kyber. útoků prováděných aktéry se značnými dovednostmi a zdroji;
- **mission-critical data a systémy**;
- útočníky jsou vysoce kvalifikované osoby s přístupem k významným zdrojům, které jim umožňují navrhovat a provádět útoky, získat přístup zasvěcených osob, objevit nebo koupit přístup k dříve neznámým zranitelnostem.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Schéma je horizontální aplikující **všechna kritéria pro všechny cloudové služby. Požadavky** na certifikaci definované v příloze A jsou rozděleny do 20 kategorií a významně čerpají **z německého schématu C5**, ale také z **francouzského** systému **SecNumCloud**, z návrhů ve zprávě CSP-CERT a z principů v jiných systémech používaných v Evropě.

- Mapping mezi bezpečnostními cíli podle čl. 51 CSA a kategoriemi požadavků je k dispozici v tab. 3.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Speciální pozornost je věnována **dodavatelům** a posouzení požadavků, které jsou naplňovány za využití těchto dodavatelů.

- V průběhu hodnocení se podporuje **znovupoužití závěrů a důkazů již certifikovaných ICT produktů, procesů a služeb**.

- **Upřesnění detailů** pro jednotlivé požadavky má být uvedeno **v návodech**, které mají být zpracovány.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Pro metody hodnocení je zvažováno využití auditních metod podle **ISO/IEC 17021 a ISO/IEC 27006 nebo** podle auditních standardů **ISAE3402 a ISAE3000**.

- Pro **záznamy** vznikající při certifikaci byly/budou stanoveny **vzory**.

- **Požadavky na CABy** navrženy nejsou. Pro úroveň záruky vysoká lze očekávat povinnost **autorizace**.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Pro **úroveň záruky základní** je zaveden tzv. **limited assurance engagement**, vizte příloha B.1, resp. D.1 EUCS – navrženo podle ISAE3000.

- Posuzování shody na úrovni záruky základní je značně zjednodušeno a **spoléhá se pouze na důkazy poskytnuté CSP**. Tyto **důkazy a poskytnutou dokumentaci ke cloudové službě auditor** certifikačního orgánu **posoudí**, vyhodnotí **neexistenci neshody** a doporučí certifikačnímu orgánu rozhodnutí o (ne)udělení certifikace. V případě potřeby může certifikační orgán vznést explicitní požadavek na další důkazy.

III. odborné setkání k CSA

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Pro **úroveň záruky významné a vysoké** je naplánovanou metodou hodnocení audit.
- Aktuálně není jasné, zda tyto audity budou prováděny **podle ISO/IEC 17021 anebo podle ISAE3402 a ISAE3000**.
- Aktuálně např. není plánováno stanovení doby trvání auditu.
- **Součástí auditu** má být penetrační **testování**, které provádí auditor.

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Detailně je zpracován **postup pro vzájemné hodnocení CABů** provádějících certifikaci pro úroveň záruky vysoká.

- Navrženo zavedení tzv. **bezpečnostních profilů** – mohou zvyšovat požadavky schématu. Mají být schvalovány ECCG a publikovány na webových stránkách ENISA.

- Navrženo je ošetření tzv. **vyšší moci**, která by neumožnila realizaci dozorů/recertifikací.

slido

Přidejte se na

slido.com

#3CSA

REGULACE CLOUDU V ČR

A JEJÍ VZTAH K EVROPSKÉ CERTIFIKACI CLOUDU (EUCS)

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Martin Klumpar
Oddělení regulace cloud computingu
Odbor regulace

24. února 2021, Brno
TLP: WHITE

REGULACE CLOUDU V ČR

Legislativní rámec

- Hlava VI zákona č. 365/2000 Sb., o **informačních systémech veřejné správy**, ve znění sněmovního tisku č. 756/4 = ZoISVS, aktuálně 3. čtení v Poslanecké sněmovně ČR.

- § 4 odst. 5, § 6 písm. e) zákona č. 181/2014 Sb., o **kybernetické bezpečnosti,** ve znění sněmovního tisku č. 756/4 = ZKB.

Na základě výše uvedeného NÚKIB vydá cloudové vyhlášky:

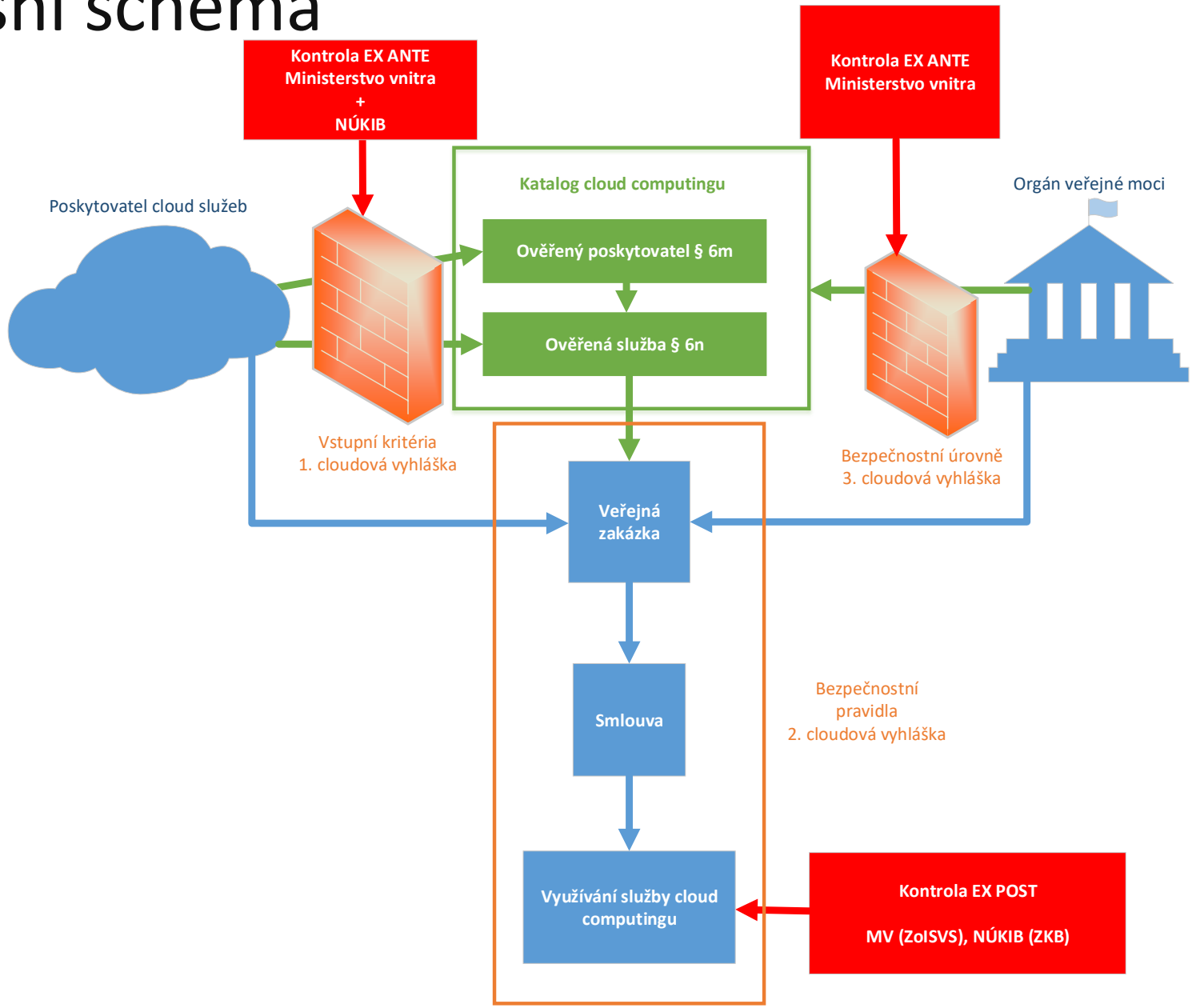
- Požadavky na poskytovatele cloud computingu a samotnou službu cloud computingu (§ 12 odst. 2 ZoISVS) = **VSTUPNÍ KRITÉRIA** – po meziresortním připomínkovacím řízení

- Bezpečnostní pravidla pro orgány veřejné moci využívající služby poskytovatelů cloud computingu [§ 6 písm. e) ZKB] = **BEZPEČNOSTNÍ PRAVIDLA** – v procesu tvorby, , vychází z německého schématu C5.

- Bezpečnostní úrovně pro využívání služeb cloud computingu [§ 6 písm. e) ZKB] = **BEZPEČNOSTNÍ ÚROVNĚ** – před meziresortním připomínkovacím řízení

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

Procesní schéma



NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Hlavní body regulace

- Prověření poskytovatele cloud computingové služby z hlediska **veřejného pořádku, bezpečnosti a dodržování práv třetích osob**.

- Rozdělení nabízených služeb cloud computingu do bezpečnostních úrovní – dle rozhodnutí poskytovatele – musí splnit odpovídající **VSTUPNÍ KRITÉRIA** pro zápis.

- Zařazení informačního systému veřejné správy do bezpečnostní úrovně – **BEZPEČNOSTNÍ ÚROVNĚ**.

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

Hlavní body regulace

- Podmínkou vypsání veřejné zakázky na službu cloud computingu je, že bezp. úroveň služby cloud computingu = bezp. úroveň inf. syst. veřejné správy.

- Orgán veřejné moci zajistí splnění **BEZPEČNOSTNÍCH PRAVIDEL** při nákupu, uzavírání smlouvy a využívání služby cloud computingu.

- Transparentnost ve zpracování dat (kde, proč, jak dlouho) – mimo EU pouze v nezbytných případech.

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

Vstupní kritéria

- 35 kritérií, členěno dle bezpečnostních úrovní a distribučního modelu (IaaS, PaaS, SaaS)
- Požadavky na certifikaci dle ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018
- Splnění některých kritérií lze dokládat pomocí auditních zpráv SOC 2® Type 2, ISO/IEC 20000-1 nebo ISO 22301
- Kritéria týkající se:
  - místa uložení a zpracování dat,
  - šifrování dat,
  - odolnosti datacenter,
  - žádostí cizozemských orgánů o vydání dat,
  - penetračních testů.
- Splnění podstatné části kritérií lze doložit čestným prohlášením poskytovatele = nízká úroveň záruky

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

VZTAH REGULACE CLOUDU V ČR A EUCS

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Výhrady NÚKIB k draftu EUCS

- EUCS neřeší **nezbytnost zpracování dat v EU** – pouze požadavek na transparentnost, ať zákazník ví, kde se data zpracovávají. Národní regulace zdůrazňuje, že zpracování mimo EU je možné pouze v nezbytných případech a v nezbytném rozsahu (vyjma specifikované cloudové služby).

- EUCS řeší posuzování **cloudové služby a nikoli jejího poskytovatele z pohledu zajištění veřejného pořádku, bezpečnosti a dodržování práv třetích osob**.

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Vztah regulace cloudu v ČR a EUCS

- **Po zavedení EUCS** a vyřešení výše uvedených výhrad bude možné přizpůsobit národní regulaci EUCS:

  - **úprava VSTUPNÍCH KRITÉRIÍ**
    (umožnění předložení EUCS certifikátu + dodatečné požadavky k místu zpracování dat a prověření poskytovatele cloudové služby)

  - **úprava BEZPEČNOSTNÍCH PRAVIDEL**
    (sjednocení znění bezpečnostních pravidel s požadavky na poskytovatele cloudových služeb v EUCS + požadavky týkající se výhradně orgánu veřejné moci).

Zde může být vložena nějaká poznámka ke slidu nebo nějaký jiný vhodný text.

Martin Klumpar

Vedoucí Oddělení regulace cloud computingu
Email: regulace@nukib.cz
Telefon: +420 541 110 560

slido

Přidejte se na

slido.com

#3CSA

III. odborné setkání k CSA

Návrh Cybersecurity Certification Scheme for Cloud Services (EUCS)
Public Consultations on Cybersecurity Candidate Schemes — ENISA (europa.eu)
Proběhla do 7.2.2021

Dále jsou uvedeny informace prezentované agenturou ENISA na jednání ECCG pořádaného dne 22.02.2021.

Do konzultace se zapojilo:
75 respondentů z řad veřejnosti (2 subjekty z ČR, jedním z nich ČIA)
17 respondentů z řad SCCG
7 respondentů z řad ECCG

Takřka ¾ **respondentů** uvedlo, že certifikace podle EUCS bude mít **pozitivní dopad na jednotný EU trh.**

III. odborné setkání k CSA

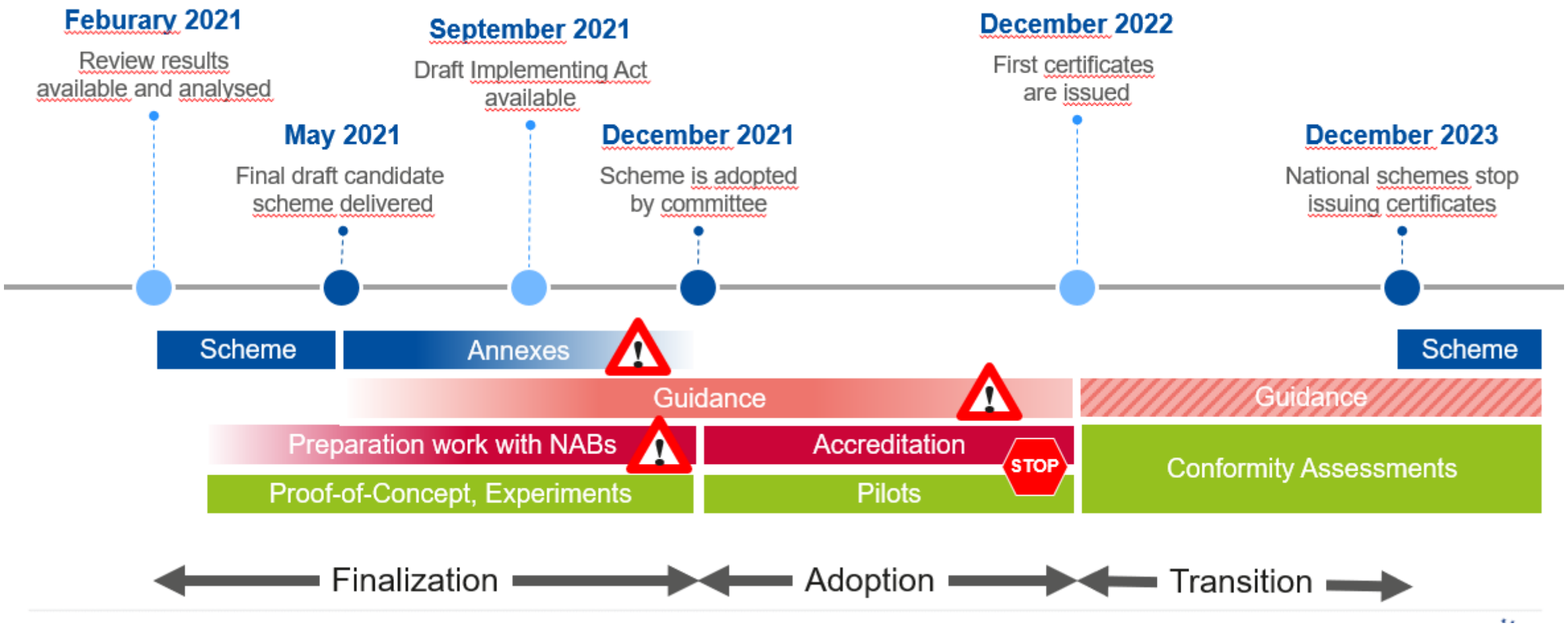
Nastavení požadavků pro jednotlivé úrovně bylo hodnoceno převáženě jako vyhovující. Pro AL základní však také jako příliš vysoké a pro AL vysokou jako nízké. Specifická pozornost bude věnována vybraným skupinám požadavků.

Jako preferovaná **kombinace s jinými schématy** byla nejčastěji zvolena EUCS se schématem ISMS podle ISO/IEC 27001 a dále přechod z národního schématu.

Pro adopci/přechod na EUCS bylo nejčastěji voleno období **delší než 18 měsíců**.

Následovat bude upřesnění, dopracování a „zlepšení“ **definic úrovní záruk**, jednotlivých **příloh**, detailů k **penetračnímu testování, zmapování ISO/IEC 17065,** práce na **požadavcích na CABy a na akreditaci vs. autorizaci**.

III. odborné setkání k CSA



III. odborné setkání k CSA

Další informace z NÚKIB a ECCG

K návrhu EUCC probíhá **:**

- zpracování prováděcího předpisu k EUCC
- jednání k dohodě o vzájemném uznávání certifikátů (EUCC a SOGIS/CC, ale také příprava koncepce pro všechna další schémata obecně)
- návrh návodů pro všechny tři strany (výrobce, CAB, NAB/NCCA)
- diskuze k adaptaci / přechodu z CC

III. odborné setkání k CSA

Další informace z NÚKIB a ECCG

Evropská komise požádala agenturu ENISA o **zpracování návrhu EU systému certifikace pro 5G sítě** Securing EU's Vision on 5G: Cybersecurity Certification — ENISA (europa.eu). Tento krok navazuje na soubor EU toolbox for 5G security a očekává se, že dále zvýší kybernetickou bezpečnost sítí 5G, protože přispěje k řešení určitých rizik v rámci širší strategie zmírňování rizik.

Za tímto účelem bude systém certifikace kybernetické bezpečnosti pro 5G založen na ustanoveních, která jsou již k dispozici prostřednictvím stávajících systémů certifikace kybernetické bezpečnosti, a zkušeností již získaných od doby, kdy se agentura začala zabývat certifikací kybernetické bezpečnosti.

Odborníci na 5G budou vyzváni, aby se zapojili prostřednictvím práce v ad-hoc pracovní skupiny, kterou ENISA založí pro vznik systému. Výzva bude zveřejněna na webových stránkách agentury ENISA Ad-hoc Working Groups calls — ENISA (europa.eu)

III. odborné setkání k CSA

Další informace z NÚKIB a ECCG
ENISA-ERA Conference: Cybersecurity in Railways — ENISA (europa.eu)
Proběhne online ve dnech 16.-17.03.2021 v čase 10:00-13:00

Agentura ENISA a ERA, Agentura EU pro železnice, spojily své síly a uspořádaly **virtuální konferenci o kybernetické bezpečnosti na železnici**.

Konference je rozdělena do **čtyř sekcí**, kde budou účastníci diskutovat na různá témata:

- Vývoj politiky;
- Normy a certifikace pro železniční sektor;
- Výsledky výzkumu a inovací;
- Způsoby sdílení informací a způsob spolupráce v zájmu kyber-bezpečnějšího železničního sektoru v EU.

Cílem konference je posílit dialog mezi železničními organizacemi, tvůrci politik, průmyslem, výzkumem, standardizačními a certifikačními organizacemi.

III. odborné setkání k CSA

Další informace z NÚKIB a ECCG
Highlights of the Cybersecurity Standardisation Conference — ENISA (europa.eu)
Proběhla online ve dnech 02.-04.02.2021

Hlavní témata:

- Požadavky na kybernetickou bezpečnost a standardizační činnosti v oblasti působnosti směrnice o rádiových zařízeních (RED), budoucí most mezi NLF a CSA
  Nový legislativní rámec – ÚNMZ (unmz.cz)
  EUROPA - European Commission - Growth - Regulatory policy – NANDO
  RED: Commission Expert Group on Radio Equipment (po 26.02.2021)
- Standardizace pro podporu CSA
- Vývoj ve standardizaci v oblasti spotřebitelského IoT;
- Standardizace v oblasti sítí 5G, další plánované kroky.

slido

Přidejte se na

slido.com

#3CSA

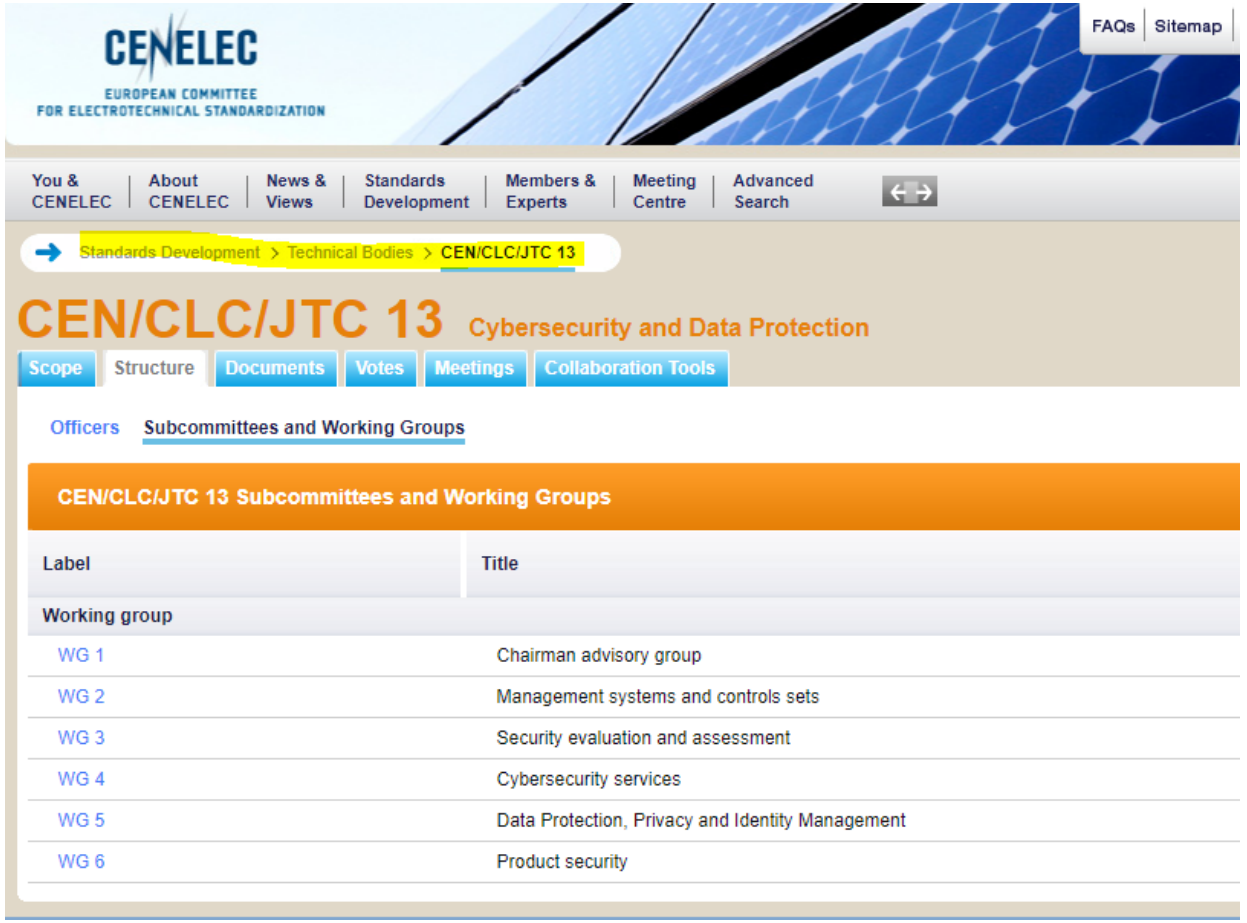
ČESKÁ AGENTURA PRO STANDARDIZACI

5G sítě, IoT, kybernetická bezpečnost ve standardizaci

Zdena Slaná | 24. 2. 2021

Cybersecurity

CEN/CLC/JTC 13 Cybersecurity and data protection



Cybersecurity

ČESKÁ AGENTURA PRO STANDARDIZACI

CEN/CLC/JTC 13 Cybersecurity and data protection

ISO/IEC JTC 1/SC 27 Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí

návrh na EN ISO/IEC 24760-1:2019	IT security and privacy - A framework for identity management - Part 1: Terminology and concepts Bezpečnost IT a soukromí - Rámec pro řízení identity - Část 1: Terminologie a pojmy
návrh na EN ISO/IEC 24760-2:2015	Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements
návrh na EN ISO/IEC 24760-3:2016	Information technology - Security techniques - A framework for identity management - Part 3: Practice
návrh na EN ISO/IEC 29101:2018	Information technology - Security techniques - Privacy architecture framework Informační technologie - Bezpečnostní techniky - Rámec architektury soukromí
návrh na EN ISO/IEC 29151:2017	Information technology - Security techniques - Code of practice for personally identifiable information protection Informační technologie - Bezpečnostní techniky - Soubor postupů na ochranu osobně identifikovatelných informací
návrh na EN ISO/IEC 39794-16/CD	Information technology - Extensible biometric data interchange formats - Part 16: Full body image data
návrh na EN ISO/IEC TS 19608:2018	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

prEN ISO/IEC 27007 ISO/IEC 27007:2020	Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí - Směrnice pro audit systémů řízení bezpečnosti informací
prEN ISO/IEC 27010 ISO/IEC 27010:2015	Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi
prEN ISO/IEC 27701 ISO/IEC 27701:2019	Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines

Cybersecurity

CEN/CLC/JTC 13 Cybersecurity and data protection

(TNK 20 Informační technologie; TNK 750 Koordinační skupina pro kybernetickou bezpečnost)

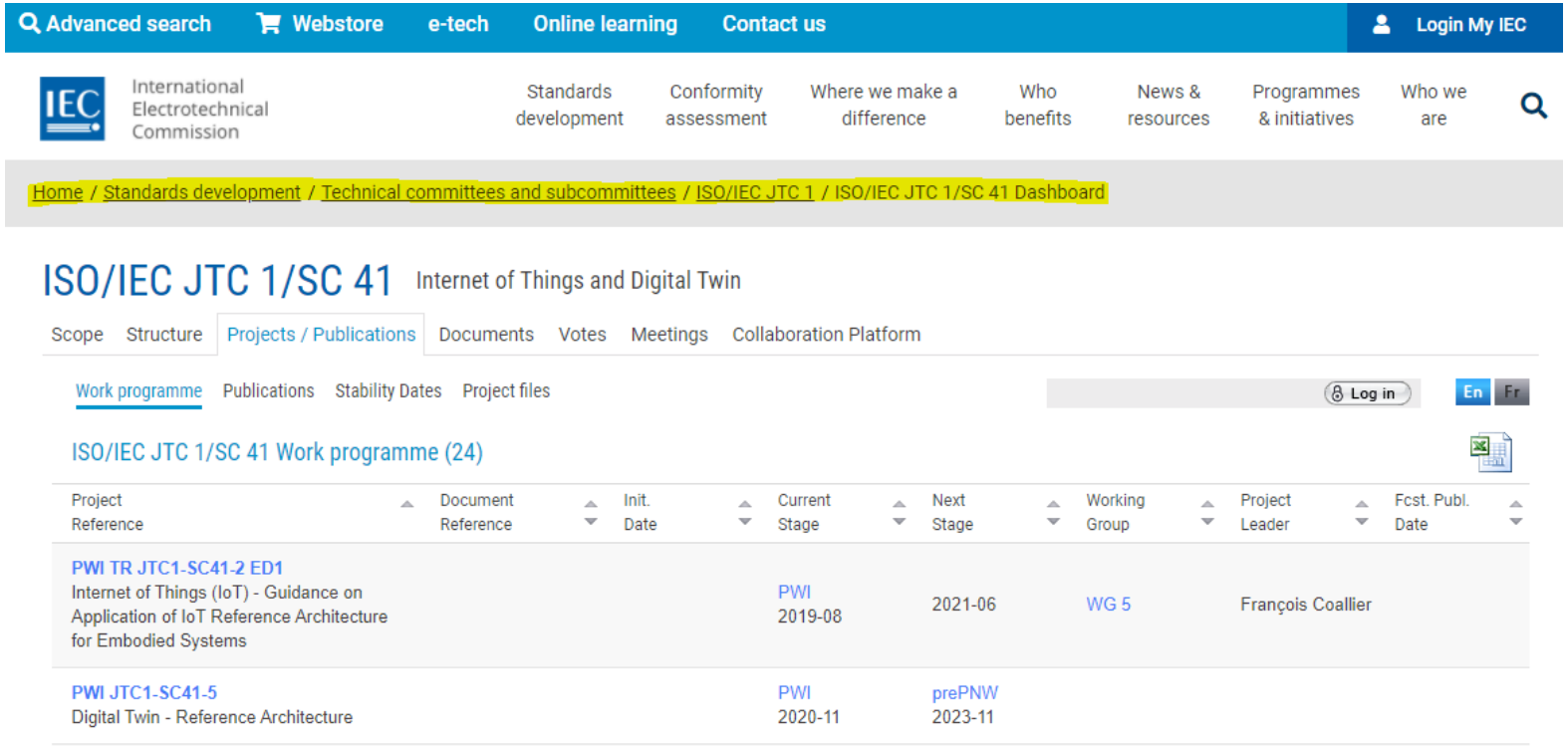
EN 17640 *Fixed time cybersecurity evaluation methodology for ICT products*

- plánované vydání 08/ 2022 s povinností implementace do národních soustav do 2023-02-01
- 2020-11-19 byl distribuován první pracovní návrh
- 2021-02-17 byl schválen k veřejnému projednávání (Acceptance of ENQ draft)
- plán veřejného projednávání od 2021-05-06.

- s podobným změřením: EN ISO/IEC 18045:2020 *Information technology - Security techniques - Methodology for IT security evaluation;* zavedena jako ČSN EN ISO/IEC 18045 *Informační technologie - Bezpečnostní techniky - Metodika pro hodnocení bezpečnost IT* (v angličtině)

ISO/IEC JTC 1/SC 41 Internet of things and digital twin

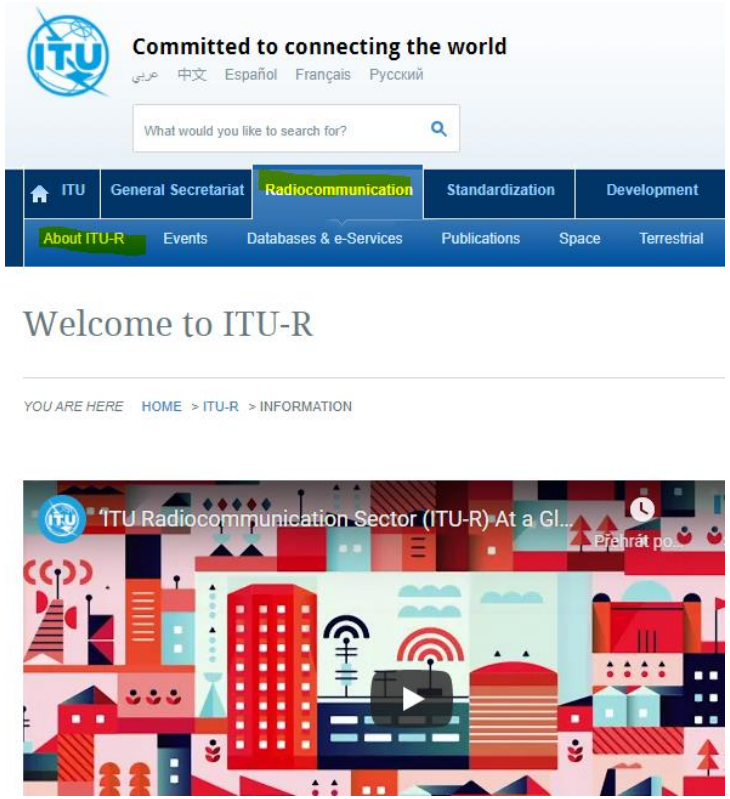
- ČSN ISO/IEC 20924:2019 - Internet věcí (IoT) - Slovník
- ČSN ISO/IEC 21823-1:2020 - Internet věcí (IoT) - Interoperabilita systémů IoT - Část 1: Struktura
- ČSN ISO/IEC 30141:2019 - Internet věcí (IoT) - Referenční architektura

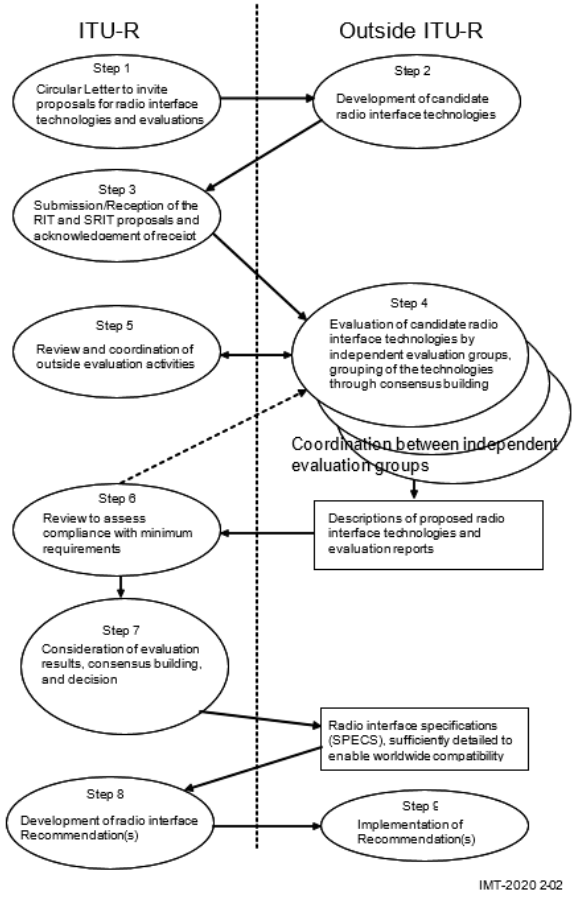


ITU Radiocommunication Sector

- projekt

International Mobile Telecommunications-2020

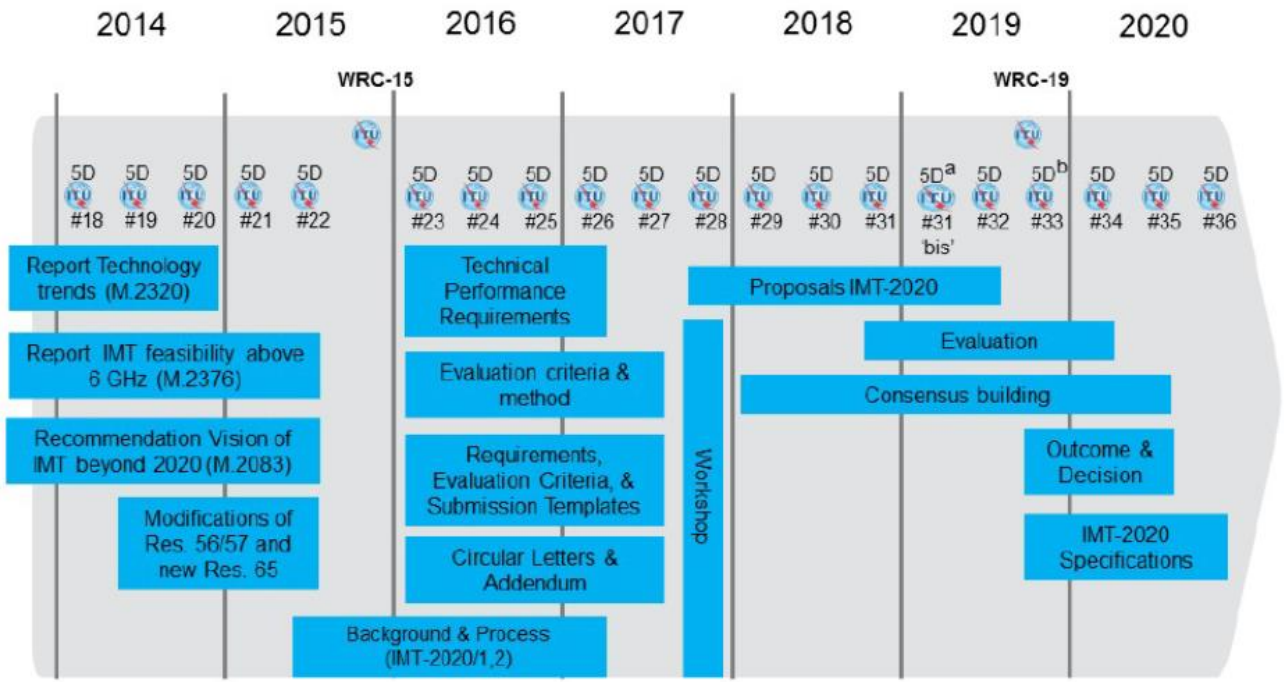




ČESKÁ AGENTURA PRO STANDARDIZACI

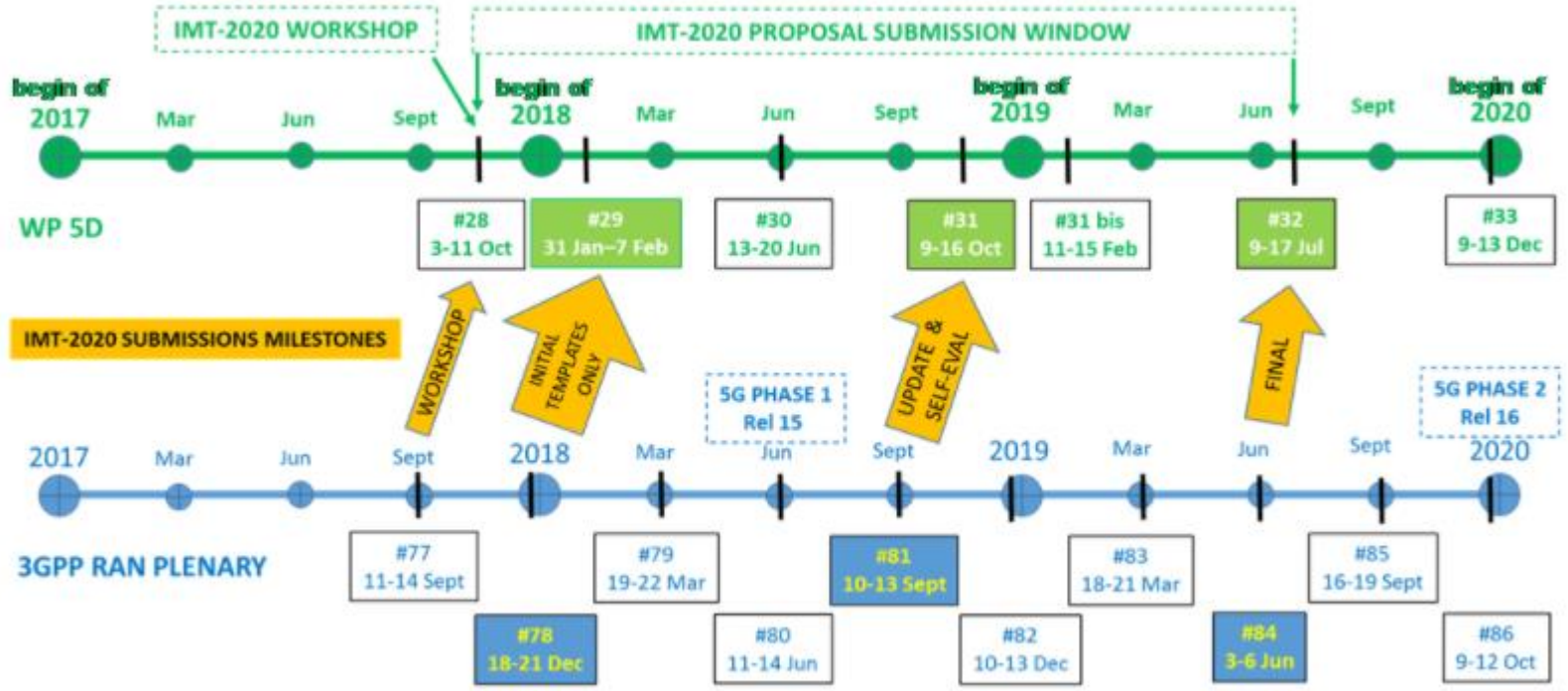
ITU Radiocommunication Sector

- projekt International Mobile Telecommunications-2020



ISO/IEC JTC 1/SC 41 Internet of things and digital twin

- ČSN ISO/IEC 20924:2019 - Internet věcí (IoT) - Slovník
- ČSN ISO/IEC 21823-1:2020 - Internet věcí (IoT) - Interoperabilita systémů IoT - Část 1: Struktura
- ČSN ISO/IEC 30141:2019 - Internet věcí (IoT) - Referenční architektura



5G sítě, IoT, kybernetická bezpečnost

European Multi Stakeholder Platform on ICT Standardisation:

"Rolling plan for ICT standardisation 2021“

https://ec.europa.eu/digital-single-market/en/rolling-plan-ict-standardisation

3GPP, ITU, ETSI NFV

The 3rd Generation Partnership Project (3GPP): 7 telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC)

ITU: International Telecommunication Union

ETSI NFV: Industry Specification Group (ISG) Network Functions Virtualisation (NFV)

ČESKÁ AGENTURA PRO STANDARDIZACI

DĚKUJEME!

Kontakt:

Zdena Slaná

slana@ agentura-cas.cz

tel. +420 222 333 444

slido

Přidejte se na

slido.com

#3CSA

ČESKÝ INSTITUT
PRO AKREDITACI, O.P.S.

Využití akreditace – certifikace podle ISO/IEC 27001 a tvorba „vlastních“ certifikačních schémat

Ing. Milan Svoboda

Akreditace pro provádění certifikace ISMS podle ISO/IEC 27001

Využití akreditace pro účely certifikace systémů managementu bezpečnosti informací (ISMS)

- další možnosti využití akreditace - kromě ČSN EN ISO/IEC 17025:2018 a ČSN EN ISO/IEC 17065:2013 u subjektů posuzování shody (CSA)

- využití akreditace pro účely certifikace systémů managementu bezpečnosti informací (**ISMS**)

- akreditace podle **ČSN EN ISO/IEC 17021-1:2016** Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu ve spojení s **ČSN ISO/IEC 27006:2016** (ISO/IEC 27006:2015) – Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Akreditace pro provádění certifikace ISMS podle ISO/IEC 27001

ČSN ISO/IEC 27006:2016 (ISO/IEC 27006:2015) – Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

- v současnosti probíhá „**dvouleté přechodné období**“ - ISO/IEC 27006:2015, AMD 1:2020
  - **IAF – rezoluce 2020-18** ze dne 5.11.2020 – **2 leté přechodné období** od posledního dne měsíce publikace, tedy **do 31.3.2022**
- převedení ISO/IEC 27006:2015, AMD 1:2020 **do soustavy českých norem** jako **ČSN** EN ISO/IEC 27006:202**1** – **odhad: 5/2021**
- **vlastní proces akreditace** – obdobný ostatním oblastem akreditace – **MPA 50-01-..**
- norma určená k posuzování shody (certifikační norma) **ČSN EN ISO/IEC 27001:2014** Informační technologie – Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

Akreditace pro provádění certifikace ISMS podle ISO/IEC 27001

ISO/IEC 27006:2015, AMD 1

změna se týká následujících částí:

7.2.1.1 – nově je vyžadováno, aby auditor ve výcviku provedl pod dohledem alespoň jeden audit typu úvodní či recertifikační audit a alespoň jeden dozorový audit. Zároveň je doplněna kompetence auditování ISMS podle ISO/IEC 27001

8.2.1 – nové znění připouští, že na certifikátech mohou být odkazy na jiné národní či mezinárodní normy. V souvislosti s touto možností se objevují snahy, aby certifikační orgány, které jsou akreditované pro ISO/IEC 27001 přestaly vydávat certifikace podle dalších ISO a preferovaly využití této možnosti. Jinými slovy by akreditované certifikační orgány měly využít této možnosti namísto vydávání neakreditovaných certifikátu ISO/IEC 27017, ISO/IEC 27018 …

Akreditace pro provádění certifikace ISMS podle ISO/IEC 27001

ISO/IEC 27006:2015, AMD 1

změna se týká následujících částí:

9.3.1.1 – doplněn text, že přezkoumání kompetence auditního týmu po fázi 1 může provést vedoucí auditor

B.2.1 – upraven text tak, že celkový počet pracovníků se nevztahuje k organizaci, ale k rozsahu certifikace

B.3.6 – zpřesnění textu, co je součástí off-site auditu

B.6 – upravení výpočtu pro více lokalit, aby to odpovídalo rizikovému přístupu – povinnost COSM zaznamenat důvody pro rozložení času auditu

Nařízení EP a Rady (EU) 2019/881 (CSA) - schémata

Certifikace podle vlastního schématu

- obecné pravidlo – certifikace (ověření planí stanovených požadavků) je prováděna vždy na základě určitého „schématu/certifikačního schématu - „CS““
- certifikační schéma
  - dokumentovaný a veřejně dostupný soubor požadavků, které stanoví:
  - předmět posuzování shody, tj. produkt, proces, služba, systém, osoba, jejichž shoda má být posouzena;
  - požadavky podle kterých se shoda posuzuje;
  - mechanismus, podle kterého je shoda stanovena, např. zkoušení, inspekce nebo audit
  - všechny další podpůrné činnosti pro zajištění shody;
  - požadavky kladené SO na CABs/AO a jakékoli konkrétní použití jejich výklady, pokud připadají v úvahu
- kdo může být tvůrcem/vlastníkem CS
  - „kdokoli“ (orgán státní správy, právní subjekt, ….) – existuje jediná výjimka – akreditační orgán, ten pouze posoudí schéma z pohledu EA 1/22

Nařízení EP a Rady (EU) 2019/881 (CSA) - schémata

Pravidla a požadavky na CS

- **Dokument EA 1/22 -** Postup a kritéria pro hodnocení schémat posuzování shody akreditačními orgány - členy EA (aktuální verze **EA-1/22 A-AB:2020)**

- **ČSN EN ISO/IEC 17067 -** Posuzování shody - Základní principy certifikace produktu a směrnice pro certifikační schémata

17067 - přehled tabulka.JPG

Nařízení EP a Rady (EU) 2019/881 (CSA) - schémata

Další využitelné standardy pro tvorbu CS

- **ISO/IEC TR 17026:2015 –** Posuzování shody – Příklad certifikačního schématu pro hmotné produkty (typ 5 dle EN ISO/IEC 17067)

- **ISO/IEC TR 17028:2017 –** Posuzování shody – Návod a příklady pro certifikační schémata pro služby

Pozn.: Jsou dostupné v ČSN on-line, část TNI

V návaznosti na zavádění „CSA“ připravuje ČIA seminář

- plánovaný termín: **6.4.2021**
- zaměření: potenciální subjekty posuzování shody podle požadavků CSA (COV, ZL)
- forma semináře: „online“ – s využitím **platformy ZOOM**
- cena semináře: 2000,- Kč

- základní témata:
  - proces akreditace – základní kroky
  - požadavky ČSN EN ISO/IEC 17025:2018 a nejčastější/typické problémy při její aplikaci (ZL)
  - požadavky ČSN EN ISO/IEC 17065:2013 a nejčastější/typické problémy při její aplikaci (COV)
  - aktuální informace o vývoji v oblasti CSA (zástupce NÚKIB)

slido

Přidejte se na

slido.com

#3CSA

III. odborné setkání k CSA

Questions & Answers

SLIDO.COM
#3CSA

slido

Přidejte se na

slido.com

#3CSA

Závěr

Ing. Jaroslav Šmíd
Náměstek ředitele, Sekce informační bezpečnosti

slido

Přidejte se na

slido.com

#3CSA

Národní úřad
pro kybernetickou
a informační bezpečnost

DĚKUJEME ZA POZORNOST
A PŘEJEME VÁM KRÁSNÝ DEN