



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

EURÓPSKA CERTIFIKAČNÁ SCHÉMA PRE CERTIFIKÁCIU CLOUDOVÝCH SLUŽIEB

Konferencia eFocus:
Riadenie rizík v informatickom a kybernetickom prostredí
14. 9. 2021, Ivan Makatura



NA ÚVOD...

- Certifikácia je najformálnejšou, ale zároveň aj najdôveryhodnejšou v rade metód posudzovania súladu
- Certifikácia výrobkov procesov a služieb (súhrnne len „produktov“) v kybernetickej bezpečnosti je postup, ktorým akreditovaný orgán posudzovania zhody poskytuje písomné ubezpečenie, že objekt posudzovania je v zhode so špecifickými požiadavkami
- Na základe mandátu daného Nariadením EÚ č. 2019/881 ENISA zriadila ad-hoc pracovnú skupinu, ktorá pracuje na príprave kandidátskej schémy pre cloudové služby EUCS (European Cybersecurity Certification Scheme for Cloud Services), ako súčasť európskeho rámca certifikácie kybernetickej bezpečnosti



VŠEOBECNÝ ÚČEL OVEROVANIA ÚROVNE BEZPEČNOSTI

Získať objektívnu informáciu o stave ochrany informačných aktív, najmä:

- zhodnotiť súlad aktuálneho stavu kybernetickej bezpečnosti so stanovenými bezpečnostnými cieľmi
- posúdiť:
 - zhodu prijatých opatrení so stanoveným rozsahom opatrení
 - účinnosť implementovaných bezpečnostných opatrení
 - bezpečnostnú architektúru (security by design)
 - bezpečnosť aplikácií (security by default)
 - vyspelosť procesu riadenia bezpečnosti
- identifikovať zraniteľnosti a hrozby
- stanoviť úrovne rizík
- **atestovať spôsobilosti a súlad v oblasti kybernetickej bezpečnosti**

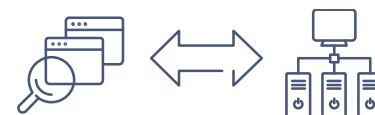


METÓDY OVEROVANIA ÚROVNE BEZPEČNOSTI

Overované entity a prvky sú v procese overovania úrovne bezpečnosti všeobecne nazývané ako „**objekty posúdenia**“ (z angl. „assessment objects“)

- Štyri základné prístupy ako sa môže subjekt uistiť o požadovanej úrovni KB:

1. **Posúdenie** - Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania



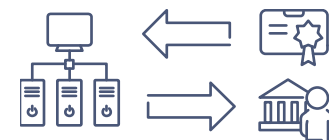
2. **Testovanie** - Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky



3. **Audit** - Systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky



4. **Certifikácia** (Posudzovanie zhody) - Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania



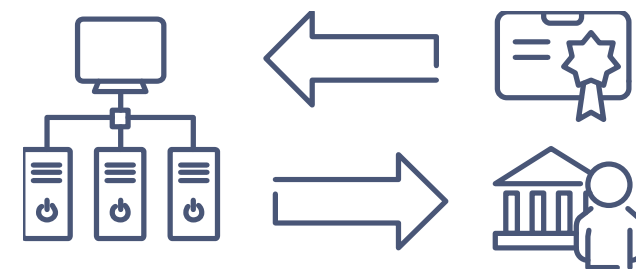


CERTIFIKÁCIA BEZPEČNOSTI

Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania

Typický proces:

1. **Žiadosť** o posúdenie zhody
2. **Vyhodnotenie** (overenie, že objekt spĺňa kvalifikačné kritériá)
3. **Atestácia** (rozhodnutie o splnení kvalifikačných kritérií)
4. **Dohľad** (priebežné posudzovanie, že objekt naďalej spĺňa kritériá)



Primárny účel:

- Deklarácia primeranej úrovne kybernetickej bezpečnosti výrobkov, služieb a procesov
- Posilnenie transparentnosti posudzovania a dôvery v bezpečnosť výrobkov, služieb a procesov

Pre certifikáciu je typická požiadavka na akreditáciu a dohľad



POROVNANIE METÓD OVEROVANIA ÚROVNE BEZPEČNOSTI

Metóda	Určený nástroj	Opakovateľný postup	Formálna špecifikácia	Nestrannosť	Dôkazy	Certifikovaná osoba	Akreditácia	Dohľad
Posudzovanie	✗	✗	✗	✗	✗	✗	✗	✗
Testovanie	✓	✓	✓	✗	✗	✗	✗	✗
Audit	✓	✓	✓	✓	✓	✓	✗	✗
Certifikácia	✓	✓	✓	✓	✓	✓	✓	✓



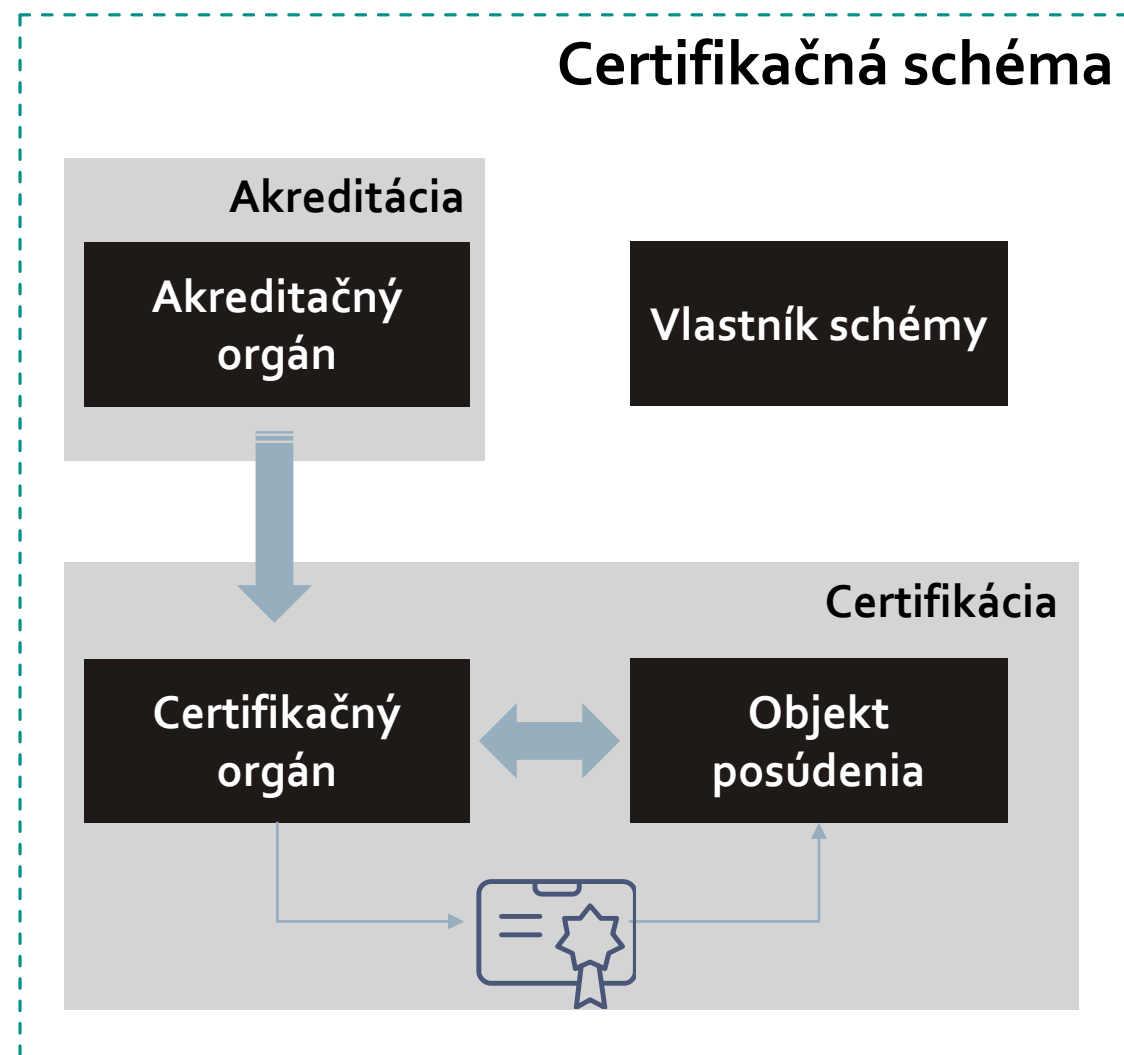
Certifikačné schémy

EURÓPSKA CERTIFIKAČNÁ SCHÉMA PRE CERTIFIKÁCIU CLOUDOVÝCH SLUŽIEB



PROCES AKREDITÁCIE PRE POSUDZOVANIE ZHODY

- **Akreditačný orgán:** autoritatívny orgán, ktorý vykonáva akreditáciu. (V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba – SNAS)
(STN EN ISO/IEC 17000: 2005, čl. 2.6)
- **Certifikačný orgán:** orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy
(ISO/IEC 17065: 2012, čl. 3.12)
- **Akreditácia** - atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody
(STN EN ISO/IEC 17000: 2005, čl. 5.6)
- **Certifikácia:** atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb.
(STN EN ISO/IEC 17000: 2005, čl. 5.5)





CERTIFIKAČNÁ SCHÉMA



- **Certifikačná schéma:** systém certifikácie, ktorý sa vzťahuje na určené produkty, na ktoré sa aplikujú rovnaké určené požiadavky, osobitné pravidlá a postupy. (ISO/IEC 17065: 2012, čl. 3.9)



- **Vlastník schémy:** osoba alebo organizácia zodpovedná za rozvoj a udržiavanie konkrétnej certifikačnej schémy (ISO/IEC 17065: 2005, čl. 3.11)

Certifikačné schémy obsahujú dva kľúčové prvky:

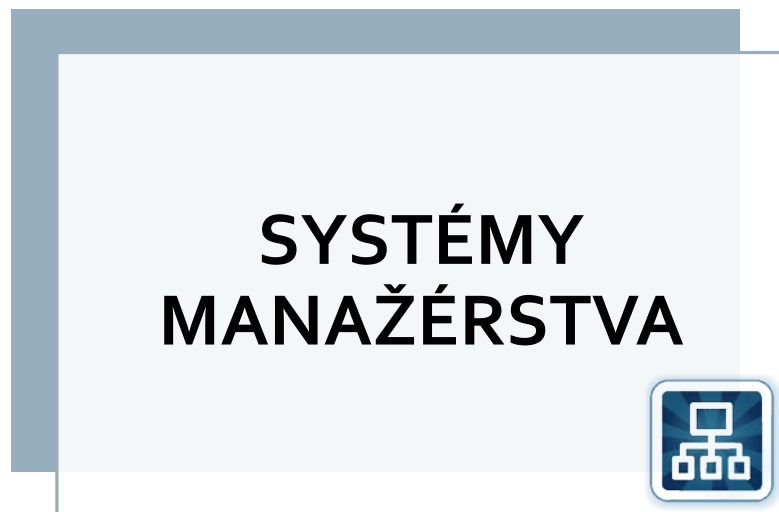
1. Kritériá stanovujúce konkrétne certifikačné požiadavky na posúdenie (tieto tvoria špecifikáciu, podľa ktorej sa posudzuje zhoda)
2. Metodiku posudzovania ktorú aplikuje certifikačný orgán na vykonanie posúdenia zhody



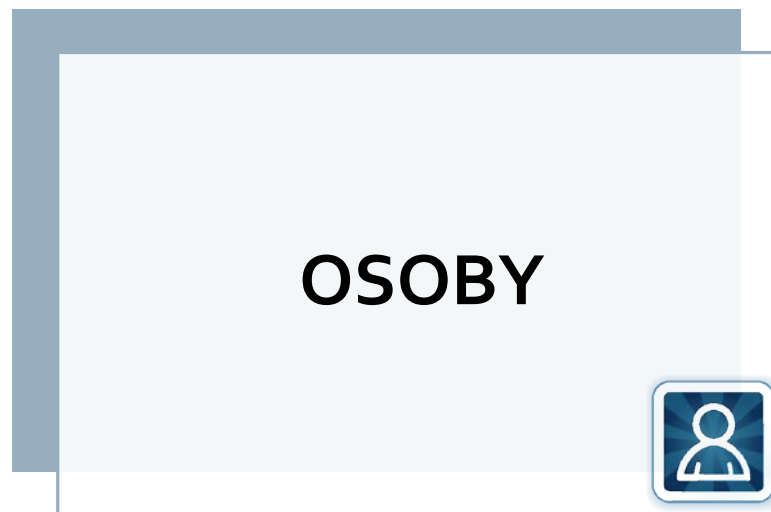


OBJEKTY POSUDZOVANIA ZHODY V OBLASTI BEZPEČNOSTI

(ISO/IEC 17021-1: 2015)



(ISO/IEC 17024: 2012)



(ISO/IEC 17065: 2012)



Schéma podľa Nariadenia 2008/765



OBJEKTY POSUDZOVANIA ZHODY V OBLASTI BEZPEČNOSTI

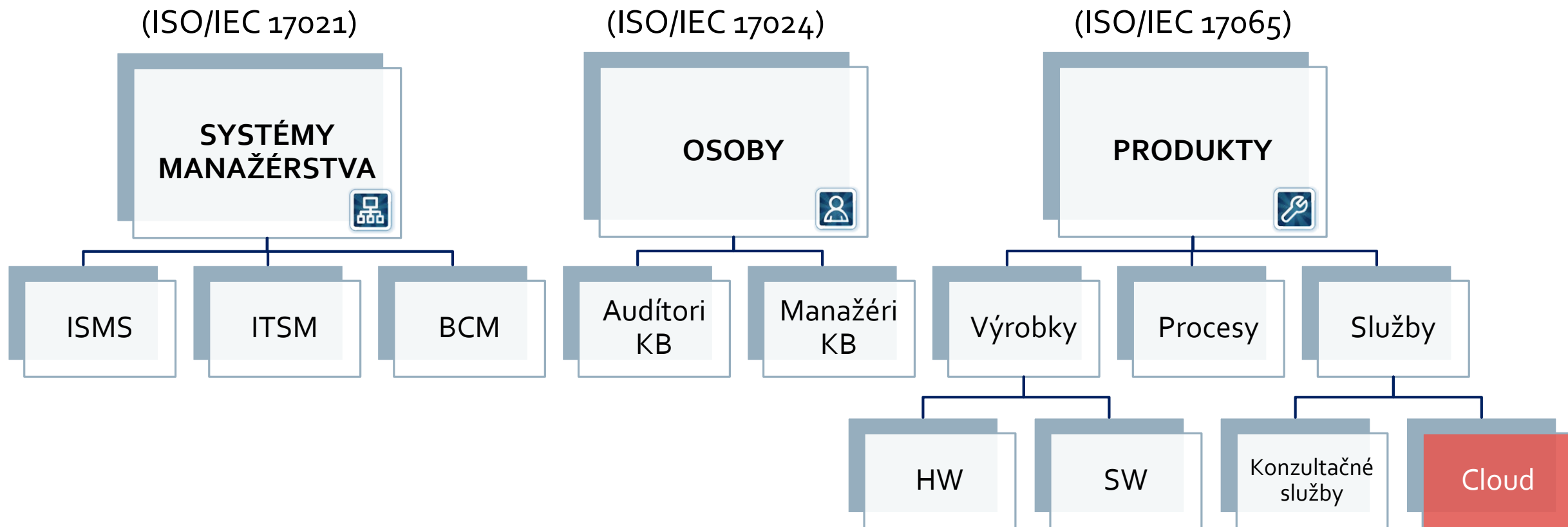


Schéma podľa Nariadenia 2008/765



Certifikačná schéma na posudzovanie cloudových služieb

EURÓPSKA CERTIFIKAČNÁ SCHÉMA PRE CERTIFIKÁCIU CLOUDOVÝCH SLUŽIEB



PRÁVNÝ ZÁKLAD CERTIFIKÁCIE CLOUDOVÝCH SLUŽIEB



- Nariadenie (EÚ) 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Nariadenie (EÚ) 765/2008 ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh
- Zákon č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu
- Zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody
- Nariadenie (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (Všeobecné nariadenie o ochrane údajov)
- Nariadenie (EÚ) 2018/1807 o rámci pre voľný tok iných ako osobných údajov v Európskej únii



STUPNE DÔVERYHODNOSTI VÝROBKU, PROCESU, ALEBO SLUŽBY PODĽA NARIADENIA EÚ 881

Základná

- Spĺňa stanovené bezpečnostné požiadavky
- Obsahuje požadované bezpečnostné funkcie
- Hodnotený na úrovni:
 - známych **základných rizík**
- Hodnotiace činnosti zahŕňajú aspoň:
 - Preskúmanie **technickej dokumentácie**
- Možné je **vlastné posúdenie** (self-assessment)

Pokročilá

- Hodnotený na úrovni:
 - Známych rizík,
 - Rizík incidentov, ktoré vykonávajú **subjekty s obmedzenými zručnosťami** a zdrojmi
- Hodnotiace činnosti zahŕňajú aspoň:
 - Vylúčenie **verejne známych zraniteľností**
 - **Test** ktorý preukazuje, že výrobky, procesy alebo služby IKT správne plnia **potrebné bezpečnostné funkcie**

Vysoká

- Hodnotený na úrovni:
 - Rizika najpokročilejších kybernetických útokov, ktoré vykonávajú **subjekty so značnými zručnosťami** a zdrojmi
- Hodnotiace činnosti zahŕňajú:
 - Vylúčenie **verejne známych zraniteľností**
 - Preukázanie, že výrobky, procesy alebo služby IKT správne plnia **najpokročilejšie potrebné bezpečnostné funkcie**
 - posúdenie ich odolnosti proti zručným útočníkom prostredníctvom **penetračného testovania**



POSUDZOVANIE PODĽA COMMON CRITERIA

Stupne dôveryhodnosti

EAL ₁	Funkčne otestované
EAL ₂	Štruktúrálné testované
EAL ₃	Metodicky testované a kontrolované
EAL ₄	Metodicky navrhnuté, testované a preskúmané
EAL ₅	Poloformálne navrhnuté, testované
EAL ₆	Poloformálne overené, navrhnuté a testované
EAL ₇	Formálne overené, navrhnuté a testované

Funkčné požiadavky

1. FAU	Bezpečnostný audit
2. FCO	Komunikácia
3. FCS	Kryptografická podpora
4. FDP	Ochrana používateľských údajov
5. FIA	Identifikácia a autentizácia
6. FMT	Riadenie bezpečnosti
7. FPR	Súkromie
8. FPT	Ochrana funkcií objektu posúdenia
9. FRU	Využitie zdrojov
10. FTA	Prístup k objektu posúdenia
11. FTP	Dôveryhodná trasa



OBSAH EURÓPSKEJ CERTIFIKAČNEJ SCHÉMY

1. Schéma pre cloudové služby
 2. Predmet a rozsah úpravy
 3. Účel schémy
 4. Použitie štandardov
 5. Úrovne dôveryhodnosti
 6. Samohodnotenie
 7. Špecifické požiadavky na orgány posudzovania zhody
 8. Metódy a kritériá hodnotenia
 9. Informácie potrebné na certifikáciu
 10. Certifikačné značky a označenia
 11. Dohľad
 12. Správa certifikátov
 13. Spôsob ošetrenia nesúlady
 14. Nové zraniteľnosti
 15. Uchovávanie záznamov
 16. Súvisiace schémy
 17. Formát certifikátu
 18. Dostupnosť informácií
 19. Platnosť certifikátu
 20. Zásady zverejnenia
 21. Vzájomné uznávanie certifikátov
 22. Posudzovanie treťou stranou
 23. Záverečné informácie
 24. Doplnujúce témy
 25. Ďalšie odporúčania
 26. Referencie
- Príloha A:** Bezpečnostné ciele a požiadavky na cloudové služby
- Príloha B:** Meta-prístup k posudzovaniu cloudových služieb
- Príloha C:** Posudzovanie pokročilých a vysokých úrovní dôveryhodnosti
- Príloha D:** Posudzovanie základnej úrovne dôveryhodnosti
- Príloha E:** Požiadavky na spôsobilosť orgánov posudzovania zhody
- Príloha F:** Požiadavky na obsah dokumentu certifikačnej schémy
- Príloha G:** Životný cyklus certifikácie a trvalá záruka
- Príloha H:** Posudzovanie treťou stranou
- Príloha I:** Použitá terminológia



VÝHODY EURÓPSKEJ CERTIFIKAČNEJ SCHÉMY

Pre poskytovateľov cloudových služieb (CSP)



- dve metodiky hodnotenia prispôsobené stupňom dôveryhodnosti navrhnuté tak, aby sa zjednodušila ich integrácia s inými zavedenými metodikami (napr. [ISO17021] alebo [ISAE3402])
- súbor cieľov a požiadaviek inšpirovaných existujúcimi schémami a mapovaných na tri stupne dôveryhodnosti
- možnosť použiť kompozíciu na zjednodušenie certifikácie cloudových služieb, ktoré sa opierajú o iné, už certifikované cloudové služby
- certifikát, ktorý je možné použiť na preukázanie, že ich cloudové služby spĺňajú požiadavky certifikačnej schémy

Pre zákazníkov cloudových služieb (CSC)



- požiadavky zaručujúce transparentné rozdelenie zodpovednosti za kybernetickú bezpečnosť medzi CSC a CSP
- požiadavky zaručujúce transparentnosť umiestnenia spracúvania a uchovávaní údajov podľa príslušných zákonov
- možnosť použiť kompozíciu na certifikáciu vlastnej cloudovej služby v prípade potreby

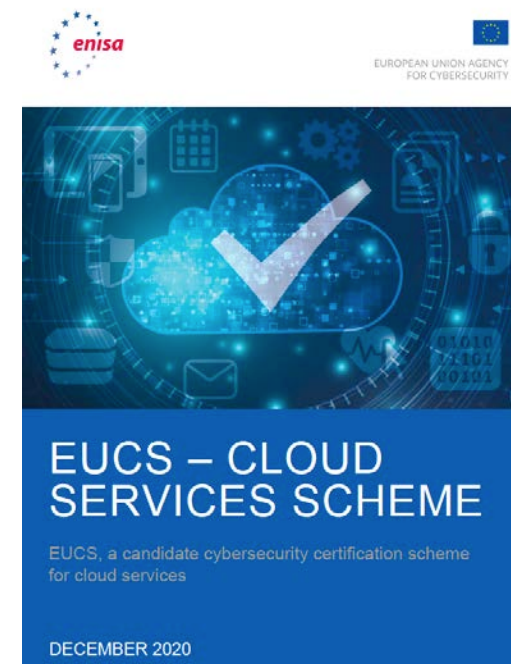
Pre poskytovateľov aj zákazníkov cloudových služieb

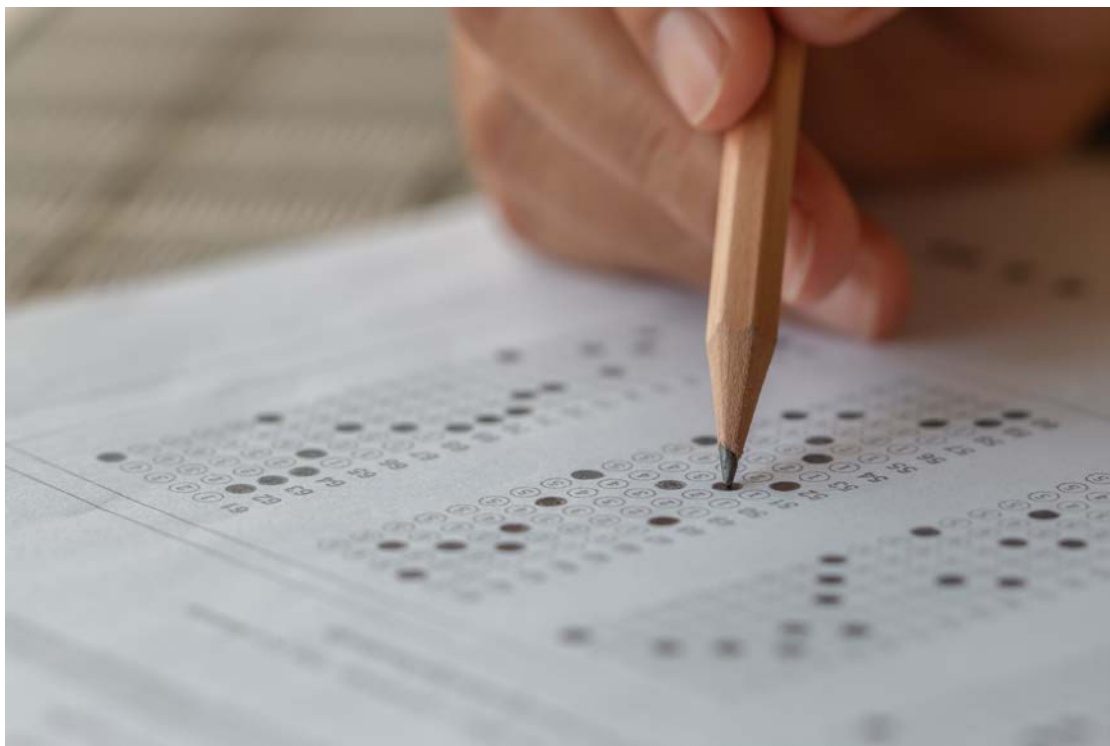
- jednotný certifikačný systém uznávaný v celej Európskej únii
- tri stupne dôveryhodnosti zodpovedajúce rôznym potrebám a rôznym prípadom použitia



ZÁVER

- Certifikácia produktov v kybernetickej bezpečnosti je ošetrená nariadením (EÚ) 2019/881 o kybernetickej bezpečnosti
- Orgán posudzovania zhody, ktorý má ambíciu certifikovať cloudové služby musí byť akreditovaný podľa *STN EN ISO/IEC 17065 Posudzovanie zhody - požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb*
- Podmienkou žiadosti o akreditáciu je existencia certifikačnej schémy
- Európska certifikačná schéma musí byť „adoptovaná“ do národnej sústavy prostredníctvom NCCA (NBÚ)
- Využívanie európskej certifikácie kybernetickej bezpečnosti by malo ostať dobrovoľné
- Členským štátom je však umožnené prijať vnútroštátne predpisy, ktorými stanovia povinnú certifikáciu podľa európskeho systému certifikácie kybernetickej bezpečnosti v súlade so smernicou (EÚ) 2015/1535





Ochrana vlastnických práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastnických a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



@CybercenterSk