KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Technická normalizácia a certifikácia

Meno a priezvisko

XX.XX.XXXX

KCKB UPJS CSIRT UPJS

Technické normy a certifikácia

- **technické normy a certifikácia** - jeden z najdôležitejších prvkov pre preukazovaní súladu s požiadavkami kybernetickej bezpečnosti.

Zdroj: https://www.enisa.europa.eu/sites/default/files/publications/ENISA_candidate%20scheme_EUCC.pdf

Technická norma (I.)

- **Norma (**ISO/IEC Guide 2: 2004)
  - je dokument vytvorený na základe dohody a schválený uznaným orgánom, ktorý poskytuje na všeobecné a opakované použitie pravidlá, pokyny, charakteristiky alebo výsledky činností a zameriava sa na dosiahnutie optimálneho stupňa poriadku v danej súvislosti

- **Dokument technickej normy:**
  - je kodifikovanou najlepšou praxou a obsahuje všeobecne uznávané technické riešenia, ktoré sú k dispozícii všetkým zainteresovaným stranám,
  - je návodom na efektívne ošetrovanie rizík,
  - je nástrojom konkurencieschopnosti pre výrobcov, predajcov a dovozcov,
  - prispieva k ochrane spotrebiteľov a
  - uľahčuje medzinárodný obchod.

Zdroj: https://www.epi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm

Technická norma (II.)

- **Norma** (čl. 2 ods. 1 Nariadenia (EÚ) č. 1025/2012 o európskej normalizácii):
  - je technická špecifikácia prijatá uznaným normalizačným orgánom na opakované alebo nepretržité používanie

  - súlad s ňou nie je povinný a je jednou z nasledujúcich technických špecifikácií:
    - a) **medzinárodná norma** - je norma prijatá medzinárodným normalizačným orgánom
    - b) **európska norma** - je norma prijatá jednou z európskych normalizačných organizácií;
    - c) **harmonizovaná norma** - je európska norma, ktorá bola prijatá na základe požiadavky Komisie na uplatňovanie harmonizovaných právnych predpisov Únie;
    - d) **národná norma** - je norma prijatá národným normalizačným orgánom;

Právna úprava technickej normalizácie

- **Právna úprava technickej normalizácie:**
  - Nariadenie (EÚ) č. 1025/2012 o európskej normalizácii,
  - zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu v znení neskorších predpisov,
  - zákon č. 55/2018 Z. z. o poskytovaní informácií o technickom predpise a o prekážkach voľného pohybu tovaru v znení neskorších predpisov,
  - zákon č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

Normalizačné organizácie (I.)

- **Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky („ÚNMS SR“)**
  - je ústredným orgánom štátnej správy, ktorý plní kľúčové úlohy v oblasti sprístupňovania technických noriem, metodickej činnosti, skúšania výrobkov, merania a kvality na trhu s technickými výrobkami. ÚNMS SR zároveň zastupuje Slovenskú republiku v medzinárodných organizáciách ISO/CEN.

- **Slovenská národná akreditačná služba (SNAS)**
  - je verejnoprávna inštitúcia zriadená zákonom č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody., jediným vnútroštátnym akreditačným orgánom v SR, ktorý vykonáva akreditáciu orgánov posudzovania zhody.. Posudzovanie zhody je založené na existencii certifikačných schém a tieto sa väčšinou opierajú o technické normy a technické normalizačné informácie.

- **Medzinárodná organizácia pre normalizáciu (International Organization for Standardization)**
  - je medzinárodný normalizačný orgán zložený zo zástupcov rôznych národných normalizačných organizácií. ISO koordinuje technickú normalizáciu v medzinárodnom meradle.

- **Medzinárodná elektrotechnická komisia (International Electrotechnical Commission - IEC)**

Normalizačné organizácie (II.)

CEN/CENELEC

- **CEN** - Európsky výbor pre normalizáciu (z francúzskeho „Comité Européen de Normalisation“)
- **CENELEC** - Európsky výbor pre normalizáciu v elektrotechnike (z francúzskeho „Comité Européen de Normalisation Électrotechnique“)

- opiera sa o štruktúru technických komisií
- CEN-CLC/JTC 13 - technická komisia pre „Kybernetická bezpečnosť a ochrana údajov“
  - prevziať príslušné medzinárodné normy najmä z technickej komisie ISO/IEC JTC 1 SC 27**10)** a
  - vyvinúť vlastné európske normy (EN) na podporu právnych aktov EÚ (napr. GDPR, CSA, CRA, DORA, ePrivacy, DSA, DMA, RED, Chips Act, AI Act, eIDAS, eIDAS2, NIS, NIS2 a mnohých iných).

ETSI - E**urópsky inštitút pre telekomunikačné normy** (European Telecommunications Standards Institute)

ITU - Medzinárodná telekomunikačná únia (International Telecommunication Union)

Tvorba technických noriem

- **Pôvodné slovenské technické normy (STN)** - ch tvorba prebieha na národnej úrovni v rámci národných technických komisií
- **Európske normy (EN)** - preberajú sa do sústavy slovenských technických noriem najneskôr do 6 mesiacov od ich sprístupnenia európskymi normalizačnými orgánmi (CEN a CENELEC)
- **Harmonizované normy** – európske normy, ktoré sa stávajú harmonizovanými vtedy, keď ich európske normalizačné organizácie oficiálne predložia Európskej Komisii a Európska Komisia ich vyhlási v Úradnom vestníku Európskej únie
- **Medzinárodné normy (ISO, IEC, ISO/IEC)** – sú prijímané do sústavy slovenských technických noriem na základe podnetov odbornej verejnosti, resp. odborových združení, podnikateľských subjektov či orgánov štátnej správy.

Zdroj: https://www.epi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm

Záväznosť technických noriem (I.)

- technická norma je dokument vo všeobecnosti určený na dobrovoľné používanie
- plnenie požiadaviek technických noriem na rozdiel od požiadaviek všeobecne záväzných právnych predpisov nie je povinné.
- § 3 ods. 14 zákona č. 60/2018 Z. z. o technickej normalizácii
- Orgán štátnej správy môže uviesť odkaz na slovenskú technickú normu alebo technickú normalizačnú informáciu v texte návrhu všeobecne záväzného právneho predpisu.
- Podmienky: predkladateľ návrh zákona nesie výdavky na každé poskytnutie slovenskej technickej normy, vopred musí oboznámiť ÚNMS SR, technická norma je alebo bude prevzatá do sústavy STN

Záväznosť technických noriem (II.)

- V zmysle legislatívnych pravidiel vlády SR platí, že ak je to potrebné vzhľadom na technický charakter právneho predpisu alebo ak ide o právny predpis, ktorým sa do právneho poriadku Slovenskej republiky preberá právne záväzný akt Európskej únie, ktorý odkazuje na technické normy, **odkazovať sa na ne možno iba v poznámke pod čiarou**. **Podmienkou takejto citácie medzinárodnej alebo európskej technickej normy je, že norma je prevzatá do sústavy STN**.

- **Technické normy sa môžu stať záväznými aj v rámci zmluvných vzťahov**, napríklad v obchodných zmluvách medzi dodávateľom a odberateľom alebo v dohodách o úrovni služieb (SLA).

(EU) harmonizované normy (I.)

- **(EU) harmonizovaná norma (HN)**
  - je európska norma, ktorá bola prijatá na základe požiadavky Komisie na uplatňovanie harmonizovaných právnych predpisov Únie
  - životný cyklus tvorby a prijatia HN sa začína a končí v Európskej komisii
  - len Európska komisia rozhodne, či v Úradnom vestníku EÚ uverejní, neuverejní alebo uverejní s obmedzením odkazy na príslušnú harmonizovanú normu

Zdroj: https://european-standards.com/compliance-guides/harmonised-standards/

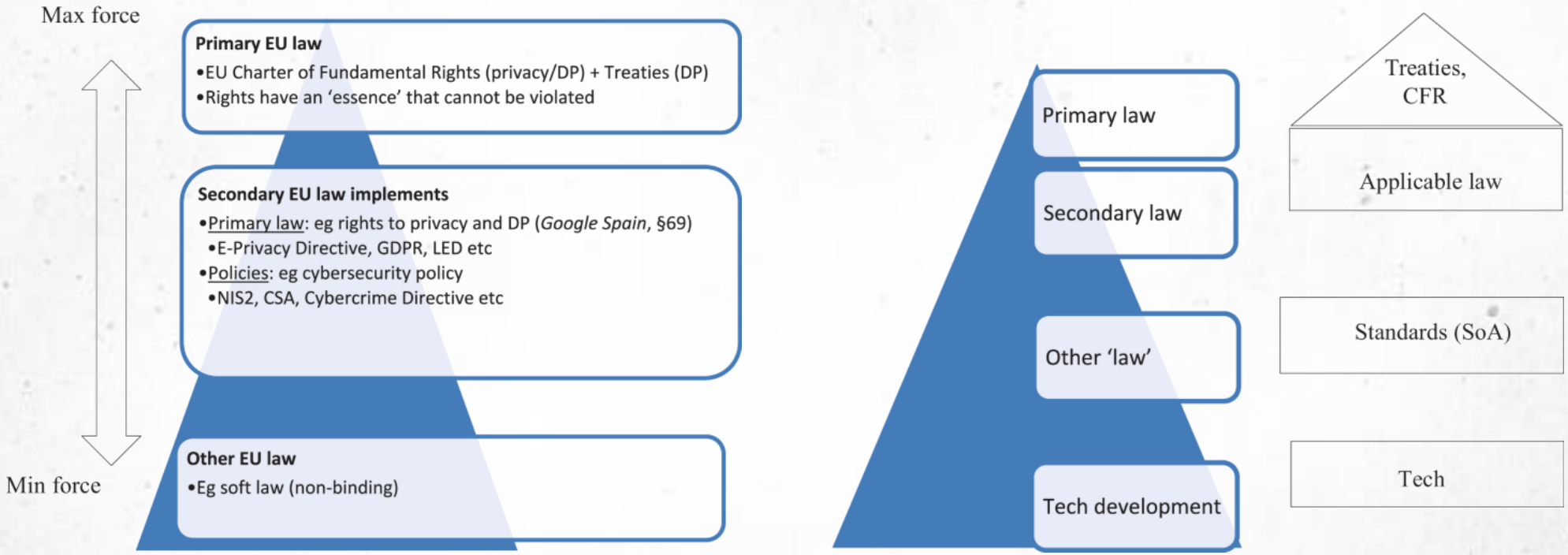
(EU) harmonizované normy (II.)

Charakteristika	Harmonizovaná norma (HN)	Európska norma (EN)
Iniciátor	Európska komisia (na základe mandátu)	Priemysel / národné normalizačné orgány
Právny status	Predpoklad zhody (Presumption of Conformity)	Dobrovoľná najlepšia prax
Citácia v Úradnom vestníku EÚ (OJEU)	Áno (povinná pre právne účinky)	Nie
Prílohy (Annex Z / ZA / ZB)	Áno (mapovanie požiadaviek normy na právne predpisy EÚ)	Nie

Zdroj: https://european-standards.com/compliance-guides/harmonised-standards/

Juridifikácia technických noriem (I.)

- právo EÚ často nedokáže priamo ovplyvniť technický dizajn, pretože medzi právnymi princípmi, štandardizáciou a samotným vývojom technológií chýba účinné prepojenie.
- technologická neutralita a trhové určovanie štandardov vedú k tomu, že konkrétne technické riešenia a „state of the art“ v praxi neurčuje právo, ale najmä trh a štandardizačné procesy.



Zdroj: Porcedda, M. G. (2023). The Effacement of Information Technology from EU Law: The Need for Collaborative Approaches to Redesign the EU's Regulatory Architecture. In IFIP International Summer School on Privacy and Identity Management (pp. 20-28). Cham: Springer Nature Switzerland.

Juridifikácia technických noriem (II.)

- **„We live in a world of standards“** (Brunsson, N., & Jacobsson, B. (2002). *A world of standards*. Oxford University Press).

- Prelomové rozhodnutia Súdneho dvora EÚ:
  - **C-171/11 Fra.bo** - právny význam HN vzrástol natoľko, že predpisy nie je možné plne pochopiť bez príslušných noriem, čím sa HN stávajú de facto záväznými
  - **C-613/14 James Elliott** - HN sú vzhľadom na svoje právne účinky súčasťou práva Únie, keďže práve odkazmi na ustanovenia takejto normy je určené, či domnienka [súladu] uvedená v [uvedenej smernici] platí alebo neplatí pre daný výrobok
  - **C-160/20 Stichting Rookpreventie Jeugd** - prístup a použitie ISO noriem
    - technické normy vypracované normalizačným orgánom, akým je Medzinárodná organizácia pre normalizáciu (ISO), a vyhlásené za záväzné legislatívnym aktom Únie, uplatňovať voči jednotlivcom vo všeobecnosti len vtedy, ak tieto normy boli uverejnené v Úradnom vestníku Európskej únie.
    - problém so zásadou právnej istoty

Juridifikácia technických noriem (III.)

- **Pojem "juridifikácia"**
  - Schapel, H. (2013). The new approach to the new approach: The juridification of harmonized standards in EU law. *Maastricht Journal of European and Comparative Law*, *20*(4), 521-533.

- Kto sa snaží účinne tento predpoklad vyvrátiť, musí preukázať, že tento výrobok alebo služba nespĺňa túto normu, alebo alternatívne, že uvedená norma je chybná (C-588/21 Public.Resource.Org)

Certifikácia v kybernetickej bezpečnosti (I.)

- **certifikácia** je nástroj, ktorý umožňuje dodávateľom produktov a služieb preukázať a komunikovať úroveň kybernetickej bezpečnosti ich riešení
- Cieľom EÚ je harmonizovať hodnotenie kybernetickej bezpečnosti ICT riešení naprieč členskými štátmi
- Certifikácia je dobrovoľná, no prispieva k rozvoju jednotného digitálneho trhu

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (**akt o kybernetickej bezpečnosti - CSA**)
- **Európskym rámcom certifikácie kybernetickej bezpečnosti** sa zabezpečuje mechanizmus zavádzania európskych systémov certifikácie kybernetickej bezpečnosti a osvedčovania, že **produkty IKT, služby IKT a procesy IKT** vyhodnotené v súlade s týmito systémami spĺňajú špecifikované bezpečnostné požiadavky s cieľom chrániť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo funkcií či služieb, ktoré tieto produkty, služby a procesy poskytujú alebo sprístupňujú, a to počas ich celého životného cyklu. (**Čl. 46 ods. 2 CSA)**

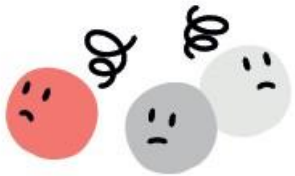
EU CYBERSECURITY CERTIFICATION

WHAT YOU SHOULD **KNOW** ABOUT IT!

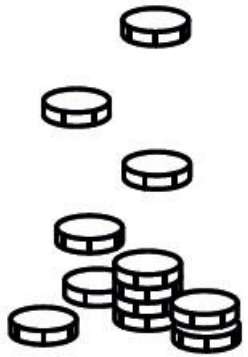
IN TODAY'S ICT MARKET, HOW IS IT POSSIBLE TO COMPARE THE LEVEL OF SECURITY OF SOLUTIONS?

SOME OF THESE SOLUTIONS CALL THEMSELVES CYBER SECURE AND TRUSTWORTHY, WHILE OTHERS CARRY VARIOUS LABELS.

THIS LEAVES ICT CONSUMERS WITH **COMPLICATED** CHOICES.



DEVELOPERS AND **SERVICE PROVIDERS** ENTERING NEW MARKETS NEED TO COMPLY WITH NUMEROUS SECURITY REQUIREMENTS.



THIS LACK OF HARMONISATION RESULTS IN **HIGH COSTS**.

TO ADDRESS THIS CHALLENGE, THE EUROPEAN UNION IS DEVELOPING **EU CYBERSECURITY CERTIFICATION** TO PROVE COMPLIANCE TO A GIVEN LEVEL OF

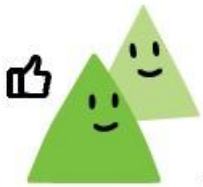
TRUST

EACH NEW CERTIFICATION SCHEME IS ALSO **TESTED** BY DEVELOPERS, SERVICE PROVIDERS, AUDITORS, EVALUATORS AND NATIONAL AUTHORITIES, TO MAKE SURE THAT IT IS ACCURATE.

ENISA, THE EUROPEAN UNION AGENCY FOR CYBERSECURITY, IS WORKING ON SCHEMES FOR **ICT PRODUCTS, CLOUD SERVICES, 5G,... AND MORE TO COME!**

ONCE IN FORCE, EACH EU COUNTRY WILL BE ABLE TO ISSUE CYBERSECURITY CERTIFICATES RECOGNISED IN A HARMONISED WAY ACROSS THE UNION.

HARMONISATION



CONSUMERS WILL EASILY BENCHMARK ICT SOLUTIONS BASED ON THEIR TRUSTWORTHINESS AND SECURITY.

DEVELOPERS AND **SERVICE PROVIDERS** WILL ONLY NEED A **SINGLE CERTIFICATION** FOR A MARKET OF 500 MILLION EU CITIZENS.

ENISA IS WORKING ON **GUIDANCE DOCUMENTS** TO HELP THE **CERTIFICATION ECOSYSTEM**.

FOLLOW ENISA!

enisaeuagency | european-union-agency-for-cybersecurity-enisa | @enisa_eu

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Zdroj: https://ncca.nbu.gov.sk/certifikacia/?csrt=840454988934603762

Certifikácia v kybernetickej bezpečnosti (III.)

- Certifikácia:
  - produkt IKT
  - služba IKT
  - proces IKT

- Novela Aktu o kybernetickej bezpečnosti (CSA) - Nariadenie(EÚ) 2025/37
  - ***riadené bezpečnostné služby***
  - je služba poskytovaná tretej strane pri riadení rizika kybernetickej bezpečnosti alebo poskytovanie pomoci pri týchto činnostiach, ako je **riešenie incidentu, penetračné testovanie, bezpečnostné audity a konzultácie vrátane odborného poradenstva súvisiaceho s technickou podporou**

- Recitál 69: Európske systémy certifikácie kybernetickej bezpečnosti by mali byť nediskriminačné a založené na európskych alebo medzinárodných normách.

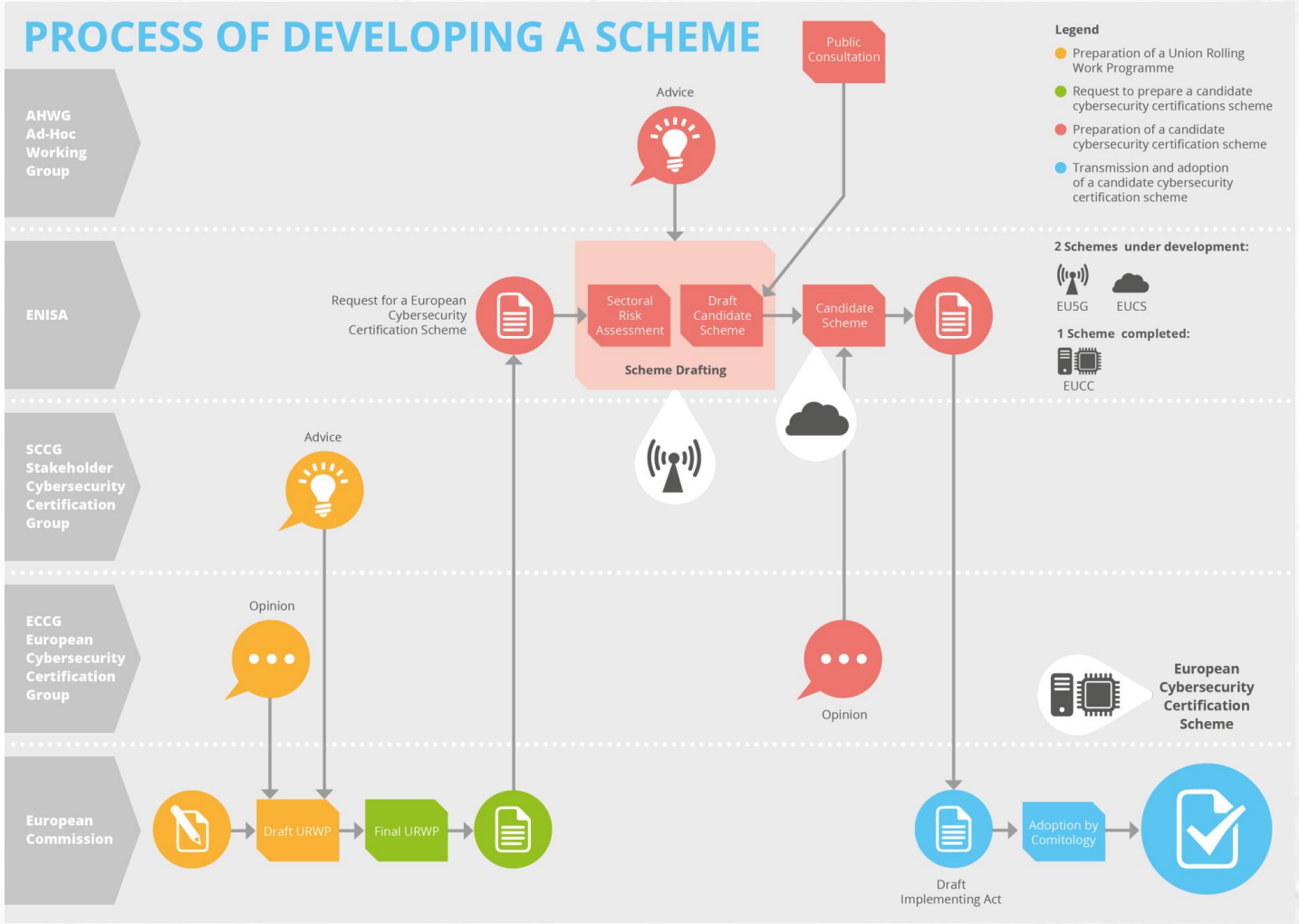
- Článok 52 ods. 4: Certifikát alebo EÚ vyhlásenie o zhode odkazujú na súvisiace technické špecifikácie, normy a postupy vrátane technických kontrol, ktorých účelom je znížiť riziko kybernetických bezpečnostných incidentov alebo týmto incidentom predísť.

Certifikácia v kybernetickej bezpečnosti (IV.)

- Článok 52 CSA - **Stupne dôveryhodnosti európskych systémov certifikácie kybernetickej bezpečnosti -** Európsky systém certifikácie kybernetickej bezpečnosti môže uvádzať jeden alebo viacero z týchto stupňov dôveryhodnosti pre produkty IKT, služby IKT a procesy IKT:
  - **„základný“, „pokročilý“ alebo „vysoký“.**
  - stupeň dôveryhodnosti zodpovedá úrovni rizika spojeného s plánovaným využívaním daného produktu IKT, služby IKT alebo procesu IKT z hľadiska pravdepodobnosti a vplyvu incidentu.

Certifikácia v kybernetickej bezpečnosti (V.)

- Agentúra ENISA
- Európske systémy certifikácie kybernetickej bezpečnosti



Zdroj: https://certification.enisa.europa.eu/about-eu-cyber-certification/developing-certification-schemes_en

EUCC schéma (I.)

- **Európska schéma certifikácie kybernetickej bezpečnosti založená na spoločných kritériách (EUCC)**
- Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC).
  - účinnosť **27.2.2025**

- „objekt hodnotenia“ je produkt IKT alebo jeho časť alebo ochranný profil ako súčasť procesu IKT, ktoré sú predmetom hodnotenia kybernetickej bezpečnosti s cieľom získať certifikáciu EUCC

Zdroj: https://certification.enisa.europa.eu/certificates_en

EUCC schéma (II.)

- európska schéma certifikácie kybernetickej bezpečnosti založený na spoločných kritériách (ďalej len „EUCC“).

- https://ncca.nbu.gov.sk/data/files/99_vykonavacie-nariadenie-komisie-2024_482-eucc_konsolidovane-znenie.pdf?csrt=16822680954098228l0

- spoločné kritériá“ sú spoločné kritériá hodnotenia bezpečnosti informačných technológií stanovené v normách:
- ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408- 3:2022, ISO/IEC 15408-4:2022 alebo ISO/IEC 15408-5:2022 alebo stanovené v spoločných kritériách hodnotenia bezpečnosti informačných technológií, verzii CC:2022, častiach 1 až 5, ktoré uverejnili účastníci dohody o uznávaní certifikátov spoločných kritérií v oblasti hodnotenia bezpečnosti informačných technológií;

Certifikáty (I.)

EU Cybersecurity Certificates

18 February 2026

EUCC-3090-2026-01

The evaluated product is a "smart card" type device that can be used in two modes: contact and contactless. It is intended for use as a secure signature creation device (SSCD).

Certification Scheme

EUCC

18 February 2026

EUCC-3090-2026-03

The evaluated product is a "smart card" type device that can be used in two modes: contact and contactless. It is intended for use as a secure signature creation device (SSCD).

Certification Scheme

EUCC

18 February 2026

EUCC-3090-2026-04

The evaluated product is a "smart card" type device that can be used in two modes: contact and contactless. It is intended for use as a secure signature creation device (SSCD).

Certification Scheme

EUCC

18 February 2026

EUCC-3090-2026-05

The evaluated product is a "smart card" type device that can be used in two modes: contact and contactless.
It implements electronic travel document functions in accordance with the specifications of the International Civil Aviation Organization (ICAO).
This product is designed to verify the authent

Certification Scheme

EUCC

18 February 2026

EUCC-3090-2026-05

The evaluated product is a "smart card" type device that can be used in two modes: contact and contactless.
It implements electronic travel document functions in accordance with the specifications of the International Civil Aviation Organization (ICAO).

Certification Scheme

EUCC

18 February 2026

EUCC-3090-2026-12

This product is a TPM (Trusted Platform Module). It is designed to guarantee the hardware and software integrity of trusted platforms (servers, computers, etc.) in accordance with TPM2.0 functional specifications.

Certification Scheme

EUCC

Zdroj: https://certification.enisa.europa.eu/certificates_en

Certifikáty (II.)

CERTIFICATE EUCC-3110-2025-11-2500051-01

14 NOVEMBER 2025

Certification Scheme EUCC

Huawei ATN Series Routers

The TOE is a series of network infrastructure routers including both hardware and software.

It is defined as the software running on the hardware corresponding to the following routers: ATN 910C-M, ATN 910C-K and ATN 910D-B. These routers consist of both hardware and software.

Details of the Certificate

Certificate ID	CERTIFICATE EUCC-3110-2025-11-2500051-01
Name of Product	Huawei ATN Series Routers
Type of Product	Generic software and network products
Version of Product	version V800R022C00SPC600
Name of the Holder	Huawei Technologies Co., Ltd
Address of the Holder	Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, People's Republic of China

Zdroj: https://certification.enisa.europa.eu/certificates/eucc-3110-2025-11-2500051-01_en

Certifikáty (III.)

CERTIFICATE EUCC-3090-2025-10-0006

The product evaluated is the family of micro-controlers «S3D384C/S3D352C/S3D300C/S3D264C/S3D232C/S3K384C, S3D384C_20250630 » developed by SAMSUNG ELECTRONICS CO. LTD.

10 DECEMBER 2025

Certification Scheme EUCC

ST31P450

The microcontroller, by itself, is not a standalone product that can be used in its current state. It is designed to host one or more applications and may be embedded in a plastic support to form a smart card. This card has multiple uses (secure identity documents, banking applications, subscription television, transport, health, etc.) depending on the application software embedded in it.

Details of the Certificate

Certificate ID	CERTIFICATE EUCC-3090-2025-10-0006
Name of Product	S3D384C/S3D352C/S3D300C/S3D264C/S3D232C/S3K384C
Type of Product	*smart card and similar device*
Version of Product	*S3D384C_20250630*
Name of the Holder	*SAMSUNG ELECTRONICS CO*

Zdroj: https://certification.enisa.europa.eu/certificates/eucc-3090-2025-10-0006_en

Common Criteria (I.)

- Common Criteria je medzinárodný štandard pre hodnotenie bezpečnosti IT produktov
- publikovaný ako ISO/IEC 15408:2022 (očakávaná zmena ISO/IEC 15408:2026)
- používa sa na certifikáciu rôznych systémov – od smart kariet po sieťové zariadenia.
- poskytuje spoločný jazyk medzi vývojármi, zákazníkmi a hodnotiteľmi.

Common Criteria (II.)

- CC vznikol, pretože každá krajina mala vlastný štandard (napr. USA – TCSEC, Európa – ITSEC).
- Cieľ: zjednotiť metodiku a umožniť vzájomné uznávanie certifikátov.
- Výsledok: organizácie si môžu vybrať produkty certifikované podľa CC a mať istotu, že spĺňajú definované bezpečnostné požiadavky.

- 1999 – prvé vydanie CC.
- 2017 – verzia 3.1 R5 (dlho používaná).
- 2022 – nové vydanie (CC:2022 a CEM:2022).

Common Criteria (III.)

Štruktúra CC:2022

- **Časť 1, Úvod a všeobecný model** je úvodom do CC. Definuje všeobecné koncepty a princípy hodnotenia bezpečnosti IT a predstavuje všeobecný model hodnotenia.
- **Časť 2, Funkčné bezpečnostné komponenty** stanovuje súbor funkčných komponentov, ktoré slúžia ako štandardné šablóny, na ktorých sú založené funkčné bezpečnostné požiadavky (SFR) pre TOE.
- **Časť 3, Komponenty bezpečnostnej istoty** stanovuje súbor komponentov istoty, ktoré slúžia ako štandardné šablóny, na ktorých sú založené požiadavky na bezpečnostnú istotu pre TOE.
- **Časť 4, Rámec pre špecifikáciu hodnotiacich metód a aktivít** poskytuje štandardizovaný rámec pre špecifikáciu metód a aktivít hodnotenia, ktoré môžu byť zahrnuté do PP, ST a akýchkoľvek podporných dokumentov
- **Časť 5, Preddefinované balíky bezpečnostných požiadaviek** poskytuje balíky požiadaviek na bezpečnostnú istotu a SFR, ktoré boli identifikované ako užitočné pre bežné použitie zainteresovanými stranami.

Predmet hodnotenia (I.)

Predmet hodnotenia (Targent of Evaluation, TOE)

- Definuje: hranice, komponenty, konfigurácie, prostredie.
- Príklad:
  - TOE = firewall, prostredie = sieťová infraštruktúra, kde je nasadený.
- **Predmet hodnotenia pre operačný systém**

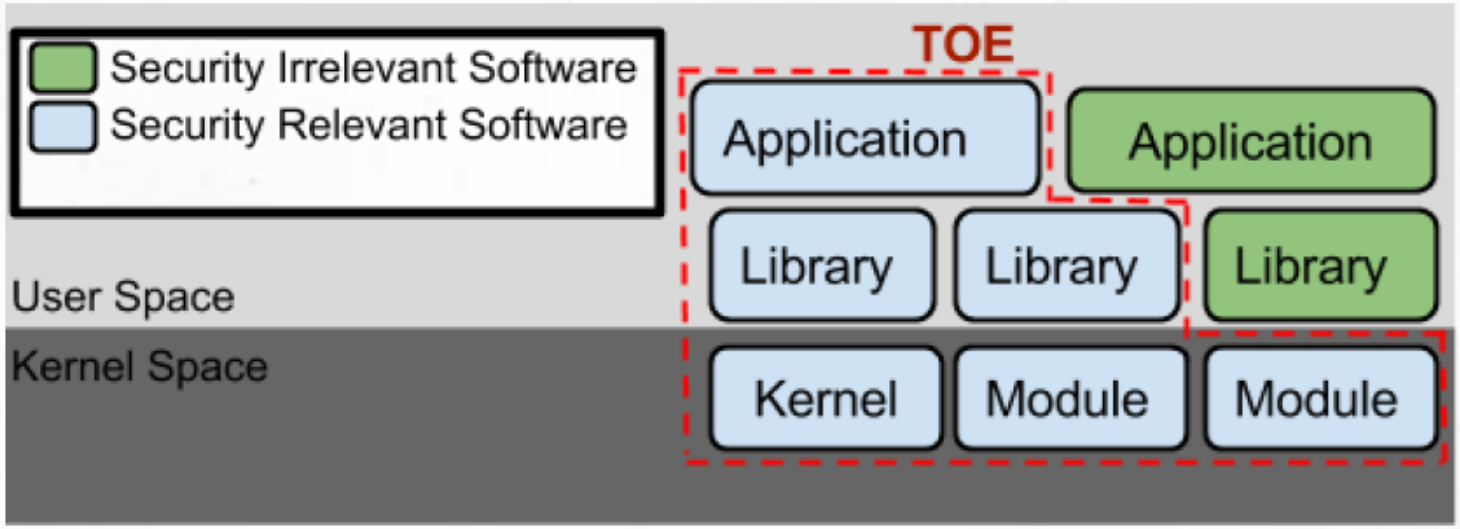


Figure 1: General TOE

Zdroj: National Information Assurance Partnership - Protection Profile for General Purpose Operating Systems, Version: 4.2.1, 2019-04-22

Predmet hodnotenia (II.)

- **Predmet hodnotenia pre operačný systém**

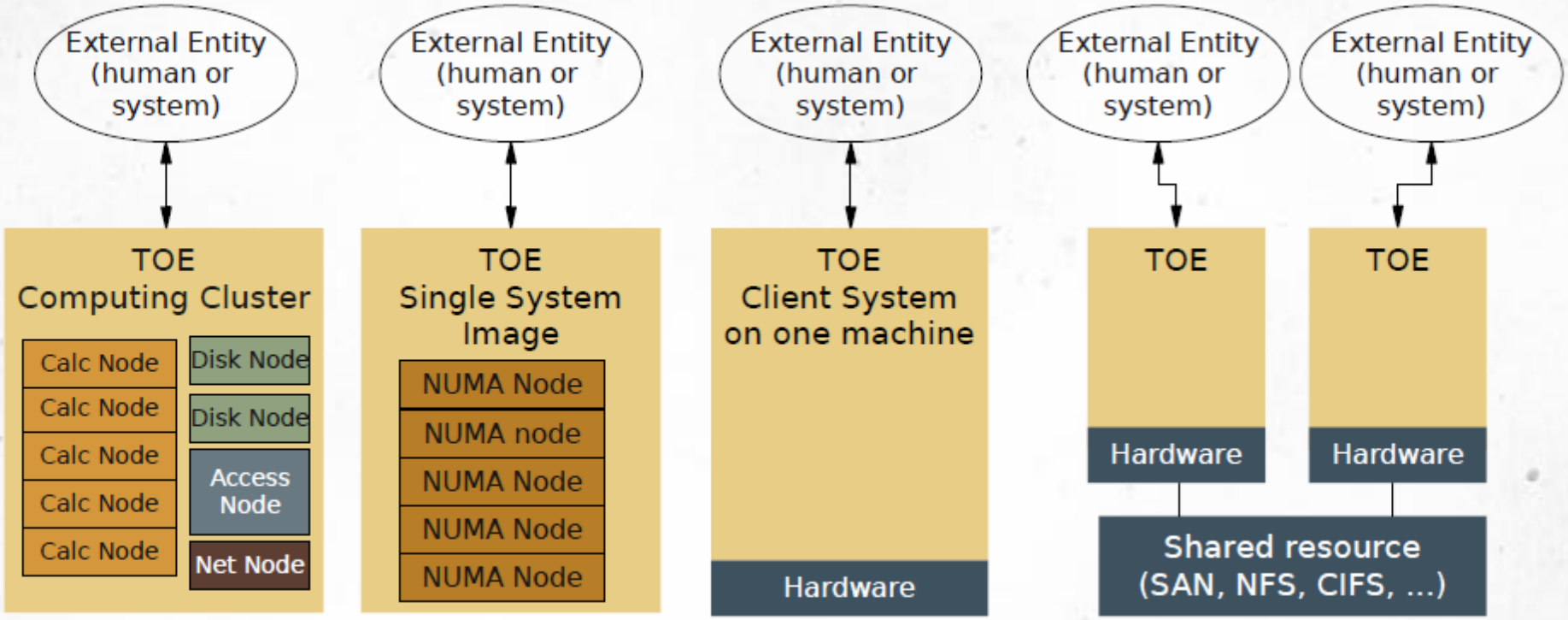


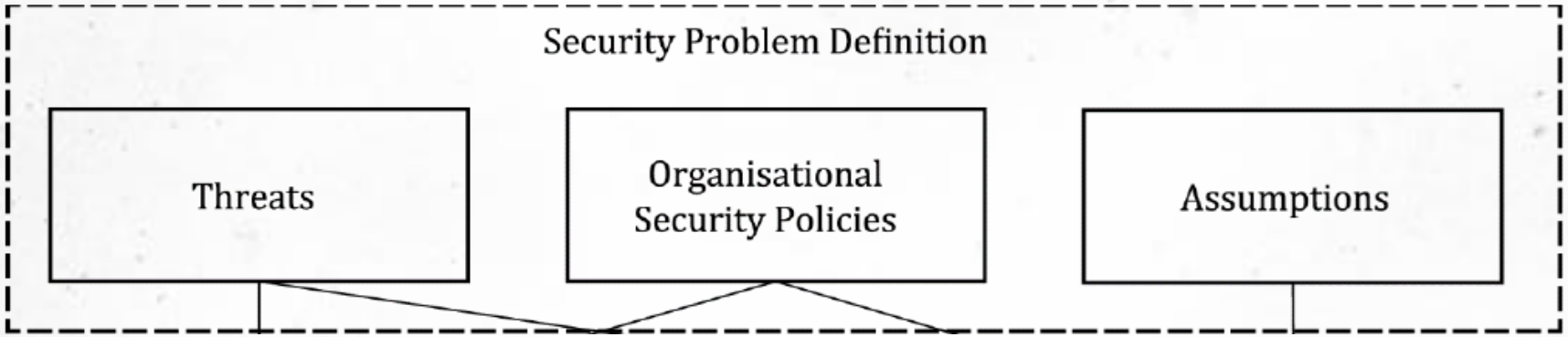
Illustration 1: Types of TOE instances and their boundaries

Zdroj: Protection Profile - Operating System Protection Profile, Common Criteria, BSI-CC-PP-0067, Version 2.0

Definícia bezpečnostného problému (I.)

Definícia bezpečnostného problému (Security problem definition, SPD) obsahuje:

- **Hrozby** (napr. neoprávnený prístup).
- **OSPs (organizational security policies)** – povinné pravidlá (napr. logovanie všetkých udalostí).
- **Predpoklady** – čo musí zabezpečiť prostredie (napr. fyzická ochrana serverovne).



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Definícia bezpečnostného problému (II.)

- **Definícia bezpečnostného problému pre operačné systémy**
- TSF = TOE security function

5.1.3 Threats countered by the TOE

T.ACCESS.TSFDATA	A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.
T.ACCESS.USERDATA	A threat agent might gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy.
T.ACCESS.TSFFUNC	A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.

5.2 Organizational Security Policies

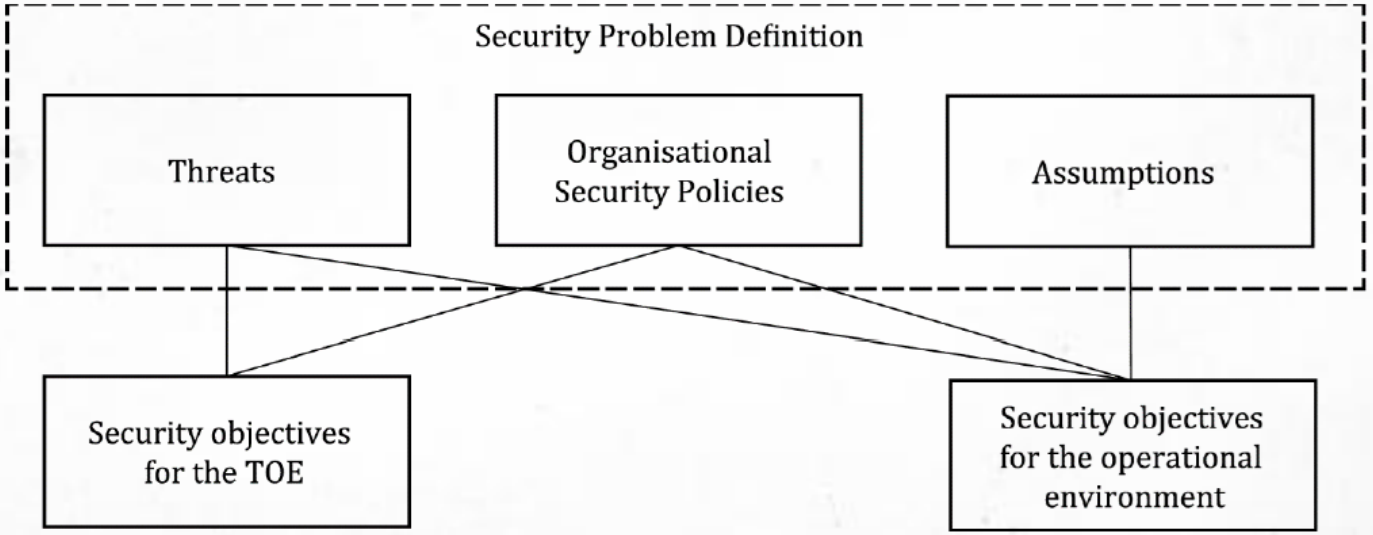
The following organizational security policies are addressed by PP-conformant TOEs:

P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

Zdroj: Protection Profile - Operating System Protection Profile, Common Criteria, BSI-CC-PP-0067, Version 2.0

Bezpečnostné ciele (I.)

- **bezpečnostné ciele (Security Objectives)** sú odpoveďou na SPD
  - rozdelenie:
    - **Pre TOE** (napr. autentifikácia používateľa) – O (objective for system)
    - **Pre prostredie** (napr. administrátori musia byť dôveryhodní) **OE** (objective for environment).
  - každý cieľ sa musí trasovať späť na konkrétnu hrozbu alebo politiku.



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Bezpečnostné ciele (II.)

- **Bezpečnostné ciele pre operačné systémy**

6.1 Security Objectives for the TOE

The following objectives are defined for the TOE.

O.AUDITING	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.CRYPTO.NET	The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.
O.DISCRETIONARY.ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.NETWORK.FLOW	The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.

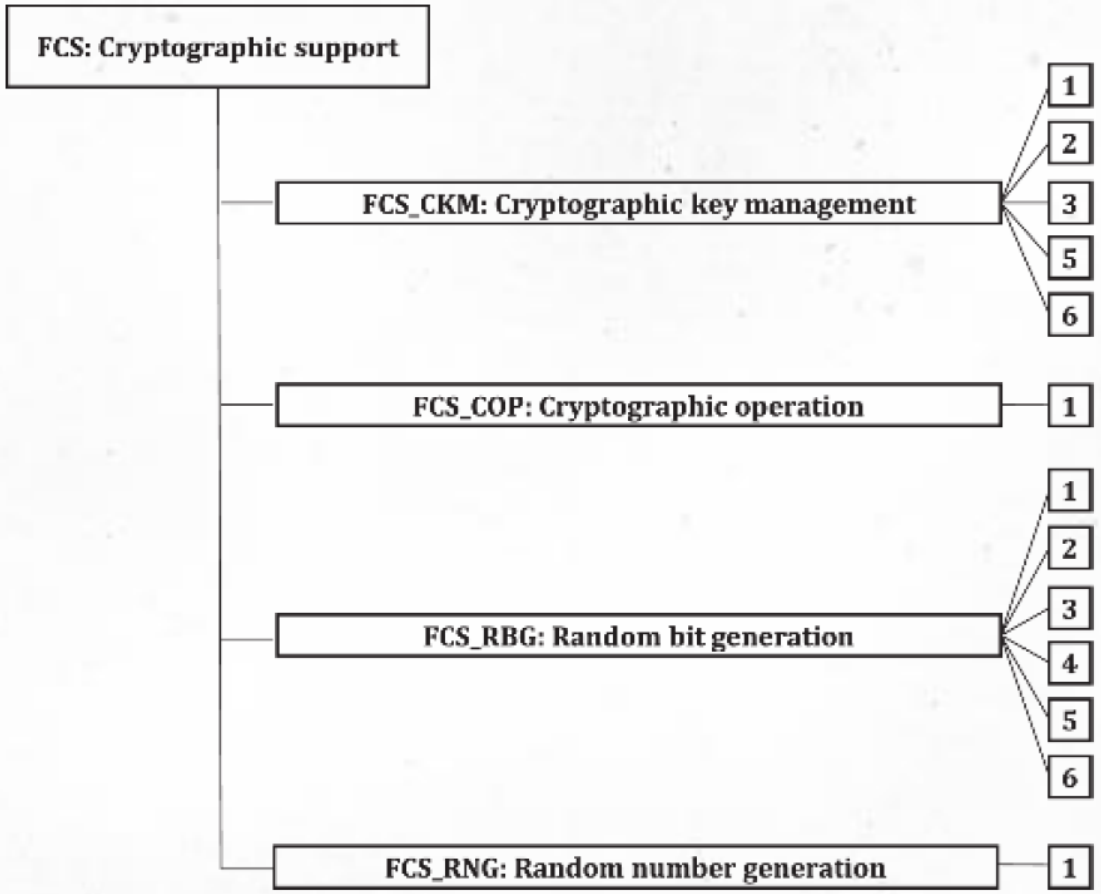
Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Bezpečnostné požiadavky (I.)

- **SFR (Security Functional Requirements):** určujú, aké bezpečnostné funkcie musí TOE implementovať (napr. šifrovanie dát).
  - triedy komponentov:
    - **FAU:** audit (logovanie, alarmy).
    - **FCS:** kryptografia (šifry, generovanie kľúčov).
    - **FDP:** ochrana dát (prístupové práva).
    - **FCO:** komunikácia (nepopierateľnosť).
  - príklad: FAU_GEN.1 – TOE musí generovať auditné záznamy.

Bezpečnostné požiadavky (II.)

- **SFR (Security Functional Requirements):** určujú, aké bezpečnostné funkcie musí TOE implementovať (napr. šifrovanie dát).



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC: 2022

Bezpečnostné požiadavky (III.)

- **Ukážka SFR (Security Functional Requirements) pre operačné systémy:**

8.2.2 FAU_GEN.2 User identity association

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

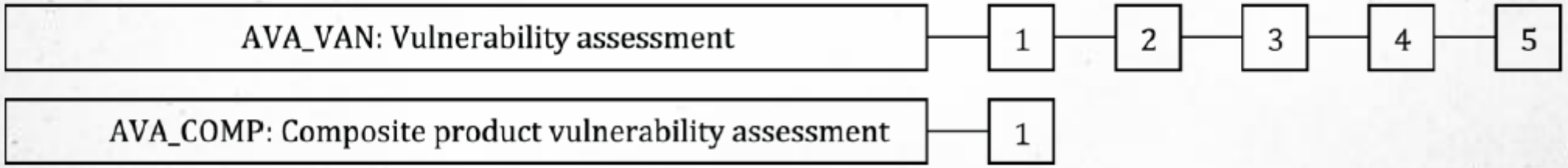
8.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1	The TSF shall provide **[assignment: the authorised identified roles, or users that satisfy the following rules: [assignment: rules that define when a user is allowed to override the default values]]**[4] with the capability to read [assignment: list of audit information] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Zdroj: Protection Profile - Operating System Protection Profile, Common Criteria, BSI-CC-PP-0067, Version 2.0

Bezpečnostné požiadavky (IV.)

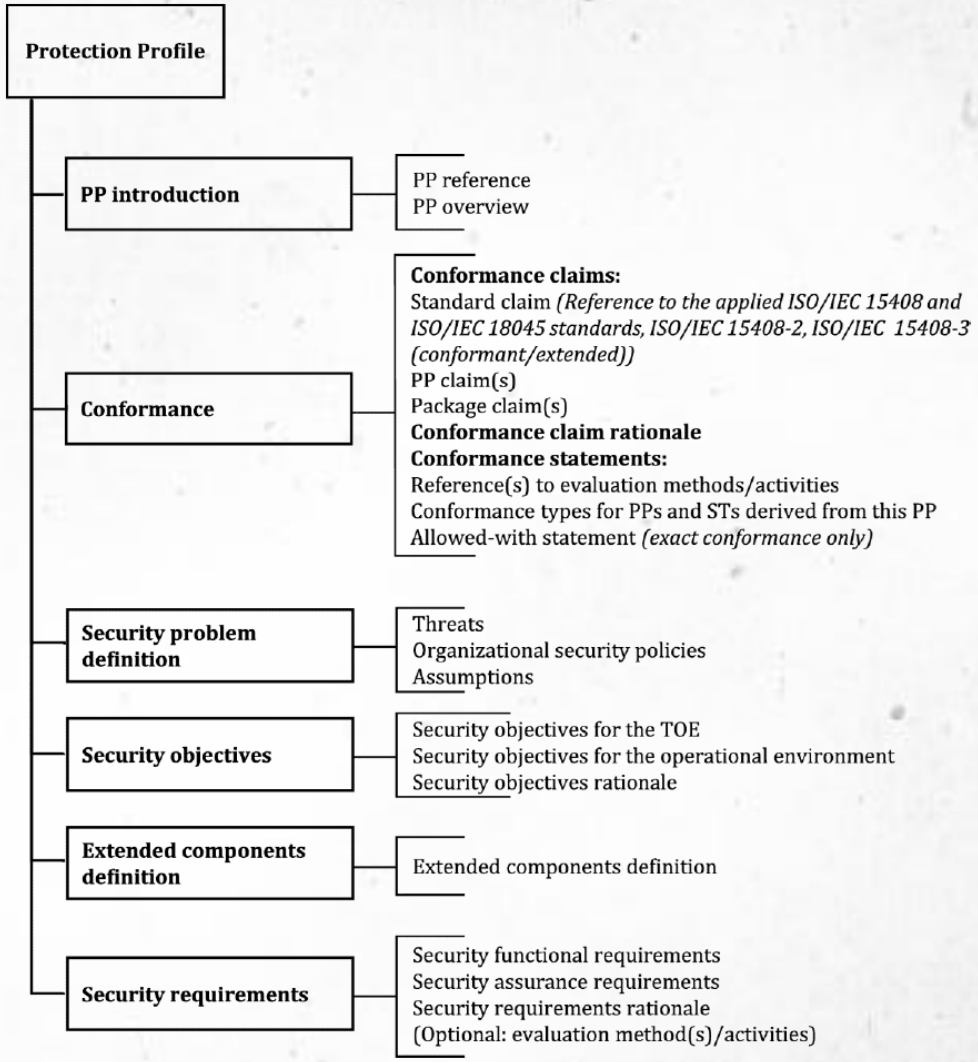
- **SAR (Security Assurance Requirements):** určujú, aké dôkazy musí výrobca poskytnúť (napr. dokumentácia, testy).
  - Triedy:
    - **APE:** Protection Profile evaluation.
    - **ASE:** Security Target evaluation.
    - **ADV:** Development evidence.
    - **ATE:** Testing.
    - **AVA:** Vulnerability assessment.
  - Cieľ: poskytnúť dôveru, že TOE funguje správne a bezpečne.



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC: 2022

Bezpečnostný profil (I.)

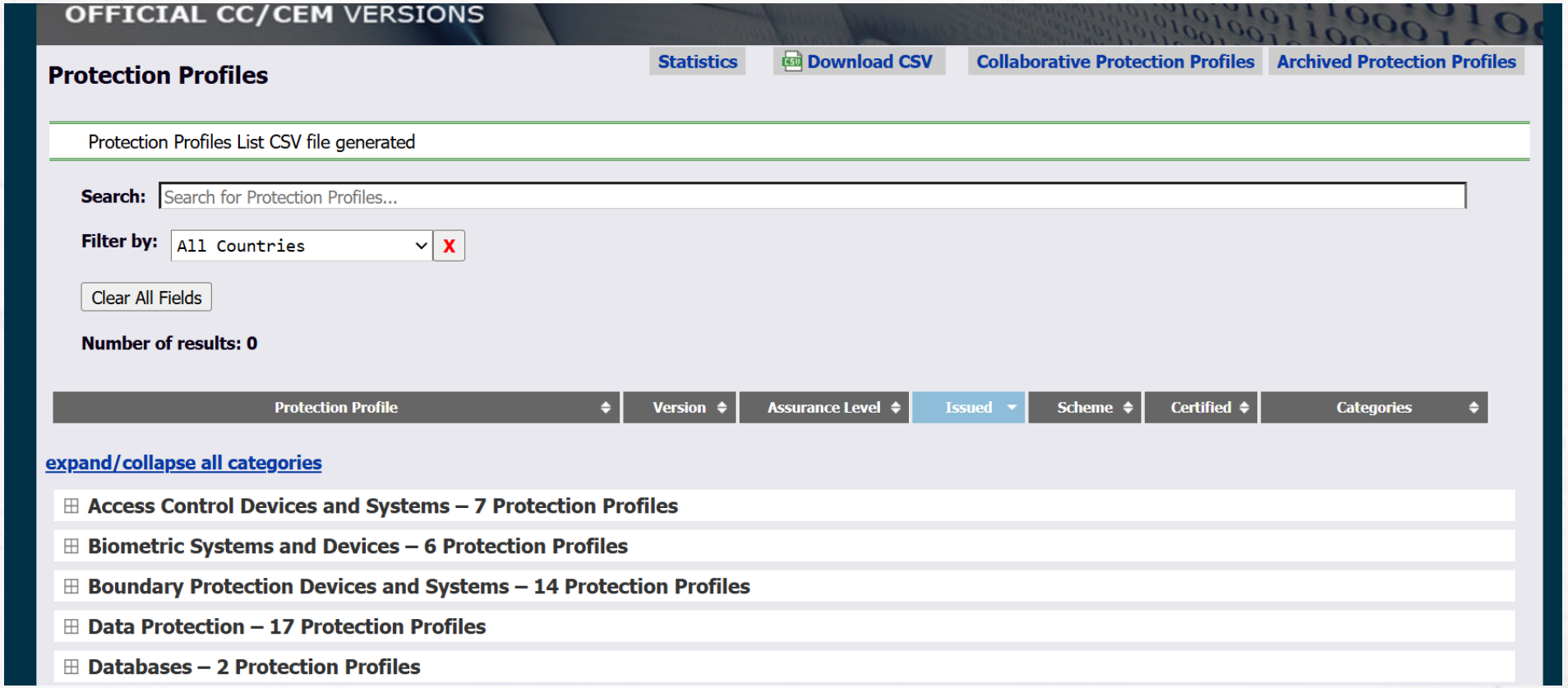
- **protection profile (PP)** - šablóna bezpečnostných požiadaviek pre určitú triedu produktov.
- **príklad:** PP pre inteligentné karty alebo firewally.
- konformita:
  - **Strict** – musí byť presne podľa PP.
  - **Demonstrable** – musí byť preukázateľne rovnako bezpečné.
  - **Exact** – nesmie sa odchýliť ani doplniť.



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Bezpečnostný profil (II.)

- **Zoznam: https://www.commoncriteriaportal.org/pps/index.cfm**

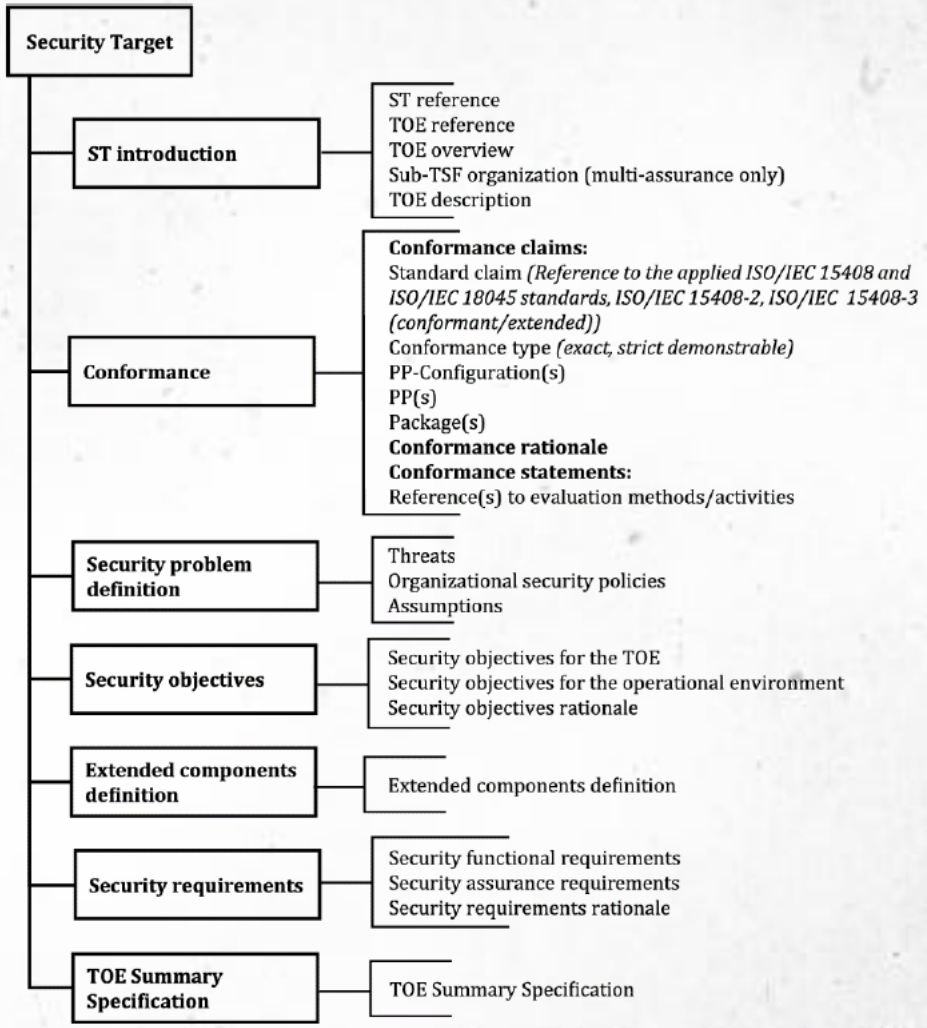


Zdroj: https://www.commoncriteriaportal.org/pps/index.cfm

Bezpečnostný cieľ (I.)

Bezpečnostný cieľ (Security target)

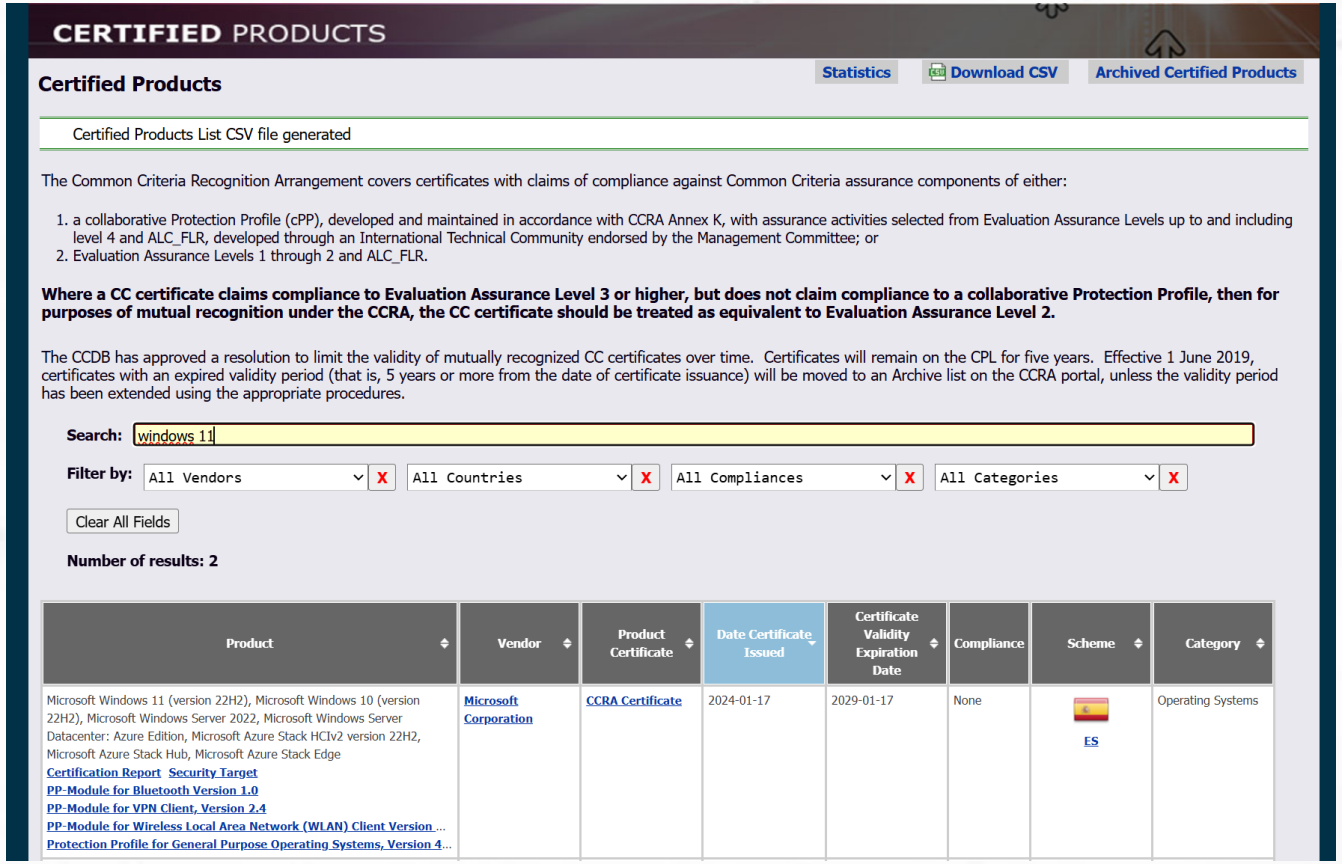
- dokument špecifický pre konkrétny produkt.
- popisuje: TOE, ciele, požiadavky a implementáciu.
- slúži ako základ pre certifikáciu.
- väzba: security target sa často odvoláva na protection profile



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Bezpečnostný cieľ (II.)

- Zoznam: https://commoncriteriaportal.org/products/index.cfm



CERTIFIED PRODUCTS

Certified Products

Statistics | Download CSV | Archived Certified Products

Certified Products List CSV file generated

The Common Criteria Recognition Arrangement covers certificates with claims of compliance against Common Criteria assurance components of either:

1. a collaborative Protection Profile (cPP), developed and maintained in accordance with CCRA Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an International Technical Community endorsed by the Management Committee; or
2. Evaluation Assurance Levels 1 through 2 and ALC_FLR.

Where a CC certificate claims compliance to Evaluation Assurance Level 3 or higher, but does not claim compliance to a collaborative Protection Profile, then for purposes of mutual recognition under the CCRA, the CC certificate should be treated as equivalent to Evaluation Assurance Level 2.

The CCDB has approved a resolution to limit the validity of mutually recognized CC certificates over time. Certificates will remain on the CPL for five years. Effective 1 June 2019, certificates with an expired validity period (that is, 5 years or more from the date of certificate issuance) will be moved to an Archive list on the CCRA portal, unless the validity period has been extended using the appropriate procedures.

Search: windows 11

Filter by: All Vendors | All Countries | All Compliances | All Categories

Clear All Fields

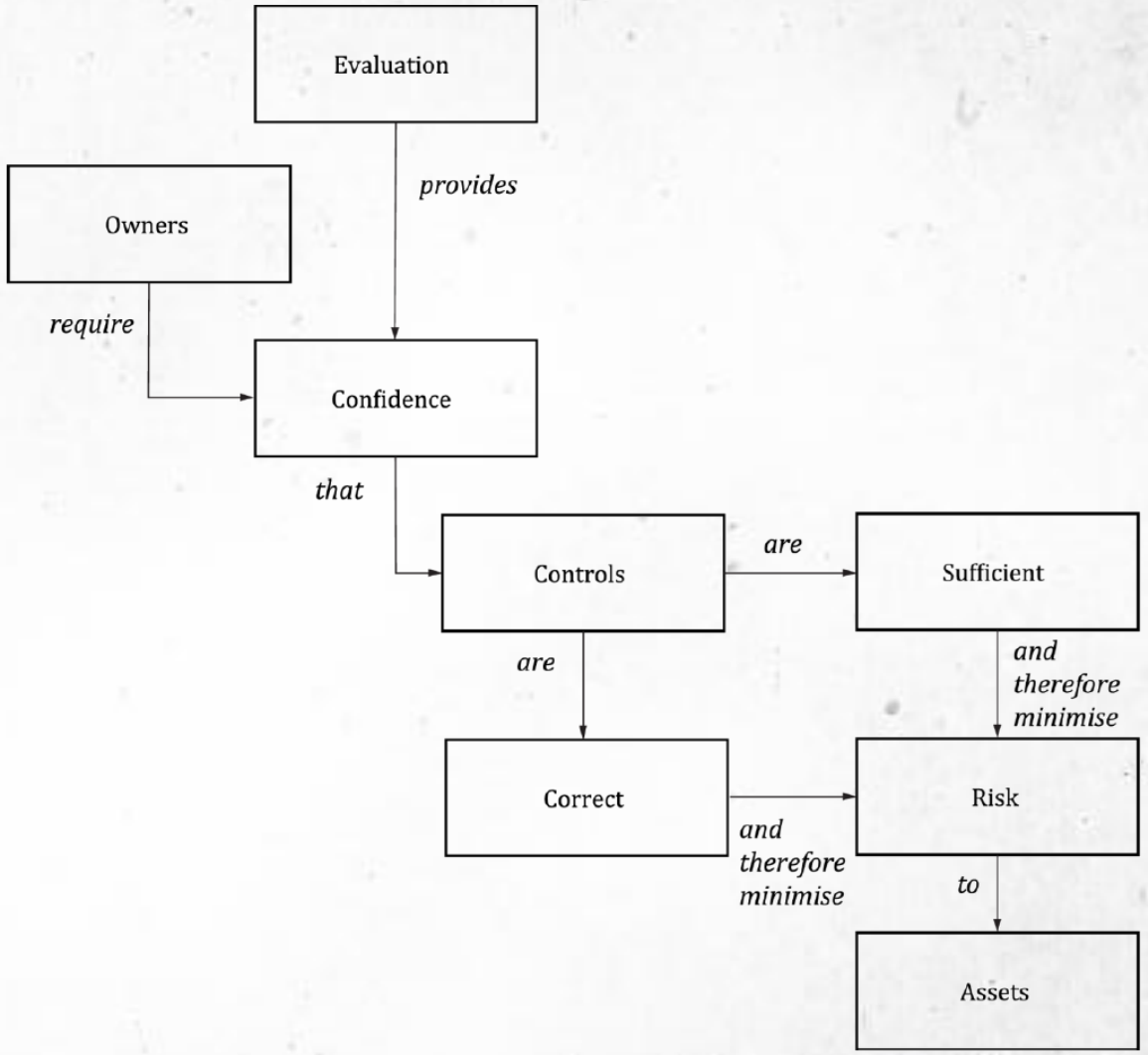
Number of results: 2

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Scheme	Category
Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub, Microsoft Azure Stack Edge Certification Report Security Target PP-Module for Bluetooth Version 1.0 PP-Module for VPN Client, Version 2.4 PP-Module for Wireless Local Area Network (WLAN) Client Version ... Protection Profile for General Purpose Operating Systems, Version 4...	Microsoft Corporation	CCRA Certificate	2024-01-17	2029-01-17	None	ES	Operating Systems

Zdroj: https://commoncriteriaportal.org/products/index.cfm

Metodológia hodnotenia (I.)

- **Metodológia hodnotenia (CEM:2022)**
- Proces:
  - **Vstupy:** ST, dokumentácia, TOE.
  - **Činnosti:** analýza, testovanie, overenie.
  - **Výstupy:** správa hodnotenia (Evaluation Technical Report).
- Účastníci: výrobca, hodnotiteľ, certifikačný orgán.



Zdroj: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022

Metodológia hodnotenia (II.)

Evaluation Assurance Levels (EAL1–EAL7)

- čím vyššia úroveň, tým väčšia dôvera, ale aj náklady.

- **EAL1 – Funkčne testovaný:** základné overenie funkčnosti podľa špecifikácie. *(napr. malá aplikácia na správu hesiel)*
- **EAL2 – Štruktúrne testovaný:** doplnené o dokumentáciu architektúry a nezávislé testy. *(napr. podniková databázová aplikácia)*
- **EAL3 – Metodicky testovaný a kontrolovaný:** hodnotenie návrhu a procesov vývoja s detailnejšími testami. *(napr. sieťové zariadenie pre vládne použitie)*

Metodológia hodnotenia (III.)

- **EAL4 – Metodicky navrhnutý, testovaný a revidovaný:** detailná dokumentácia a systematické testovanie, najpoužívanejšia úroveň. *(napr. firewall, VPN brána)*
- **EAL5 – Semi-formálne verifikovaný dizajn a testovaný:** vyžaduje semi-formálne modely a presné zdokumentovanie. *(napr. bezpečnostný modul pre banky)*
- **EAL6 – Semi-formálne verifikovaný (rozšírený):** prísnejšia analýza a hlbšie testovanie pre vysoko rizikové prostredia. *(napr. riadiace systémy v energetike)*
- **EAL7 – Formálne verifikovaný dizajn a testovaný:** matematicky dokázaná správnosť návrhu, extrémne nákladné. *(napr. vojenské šifrovacie zariadenie)*

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

pavol.sokol@upjs.sk

https://cyberawareness.sk