Company INTERNAL

CRYPTO 2022

24. března 2022

Pavel Vondruška
Historie a současnost kryptografie

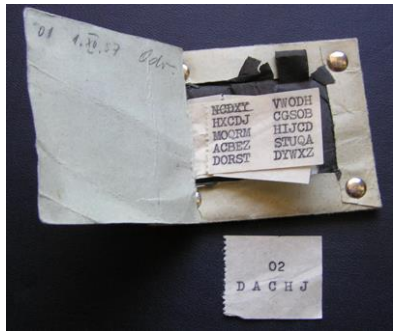
v konferenčním sále společnosti MICROSOFT

Vývoj kryptografických zařízení v ČS(S)R

Pavel Vondruška

Mikulášská kryptobesídka 2009

- ŠTOLBA
- MAGDA
- Slepé uličky (ŠTOLBA-2, KAREL, BOBA, ERA, ELA, VĚRA a HEDA)
- Použití trofejních šifrových strojů (ENIGMA, ANNA, KRYHA, C-36)
- Vznik Zvláštní správy ministerstva vnitra
- ŠD-1
- ŠD-2
- ŠD-3
- HPS-2
- …
- Varšavská smlouva FIALKA (M125)



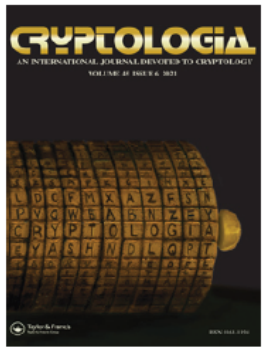
MAGDA

Po druhé světové válce bylo pro potřeby československé armády započato s vývojem polního šifrátoru MAGDA

První známý šifrátor československé výroby byl vyroben roku 1930 odborníkem na mechanické konstrukce plk. Ing. Josefem Štolbou (Sieber).
Použití armáda, ministerstva, prokazatelně využíval i Dr. E.Beneš).

Mechanický šifrátor s vlastní tvorbou hesla.
Přenos „signálu“ z klávesnice přes šifrová kola až po tiskový mechanismus byl řešen zcela specifickým způsobem a to **pneumatickým převodem**.

1945 – 1955 byl používán v československé armádě k výrobě hesla..

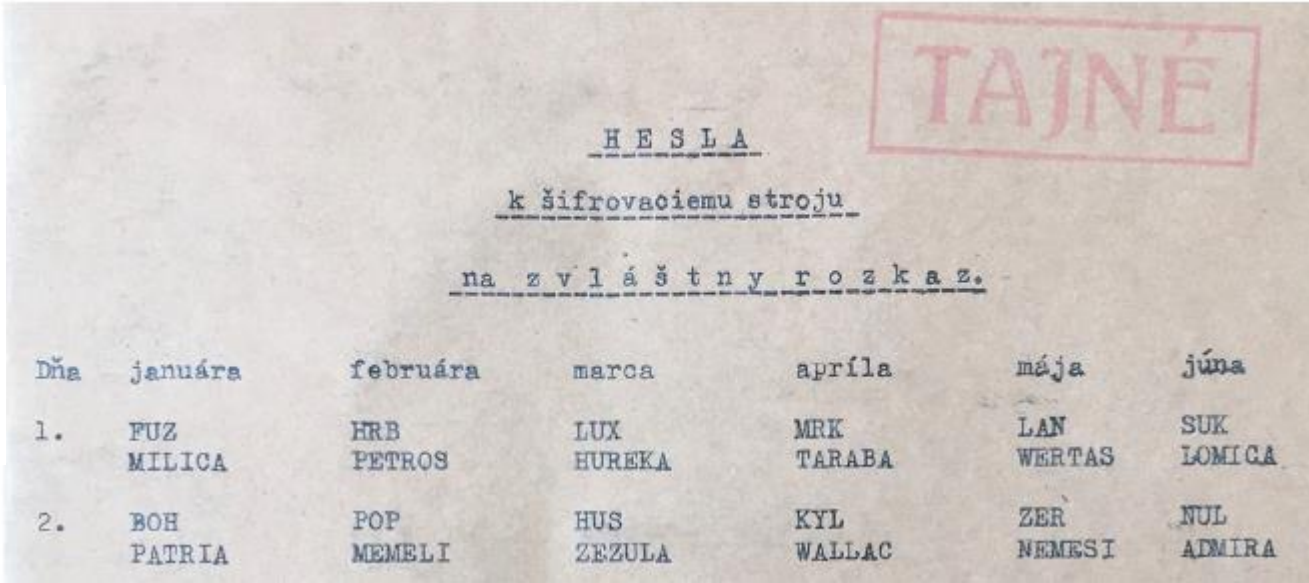


Cryptologia

The first Czechoslovak cipher machine

Eugen Antal & Pavol Zajac

Cryptologia, DOI: 10.1080/01611194.2021.1998809



TAJNÉ

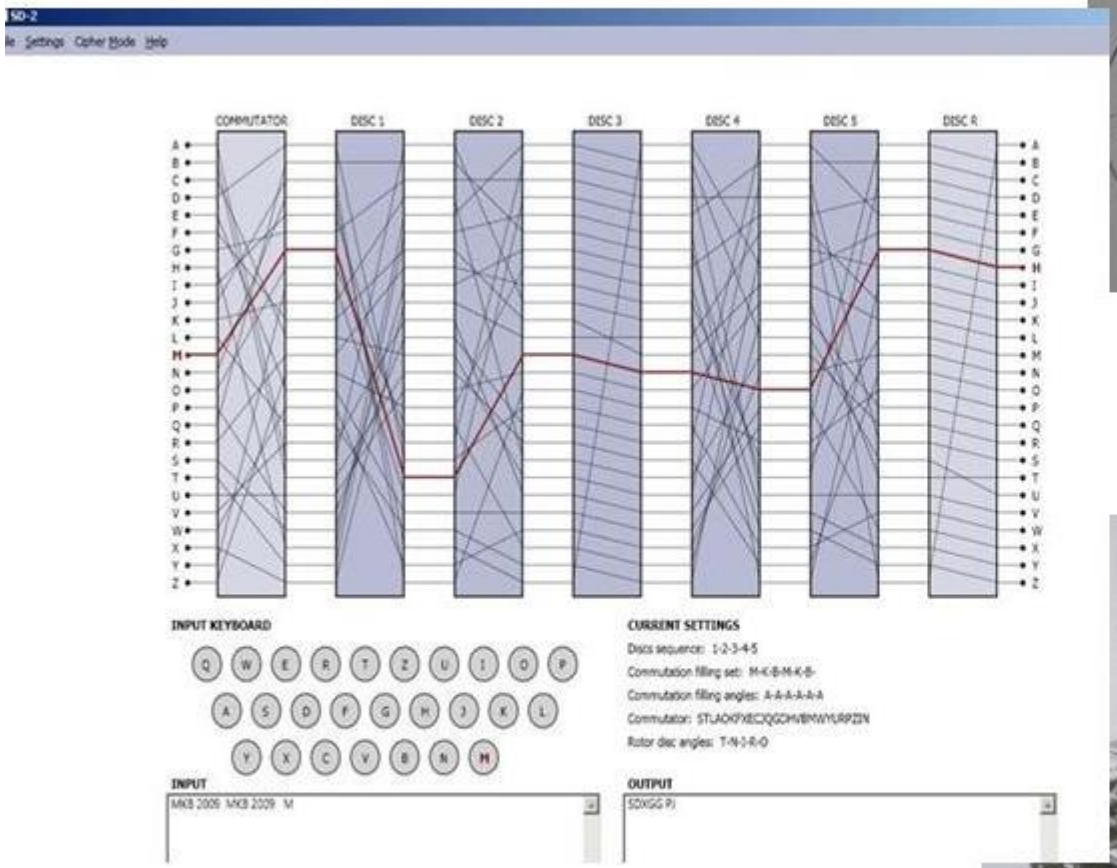
H E S L A

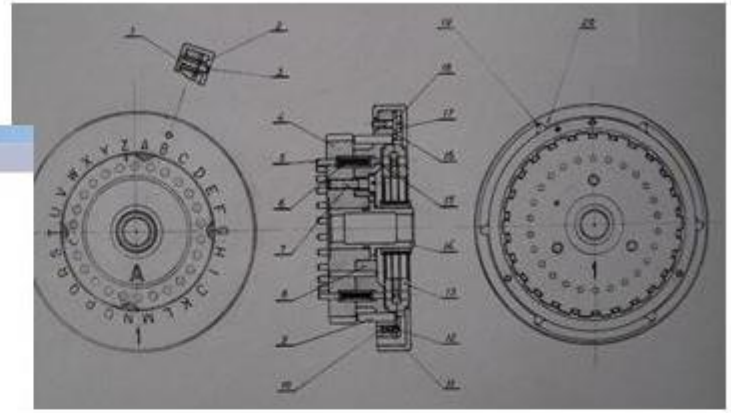
k šifrovaciemu stroju

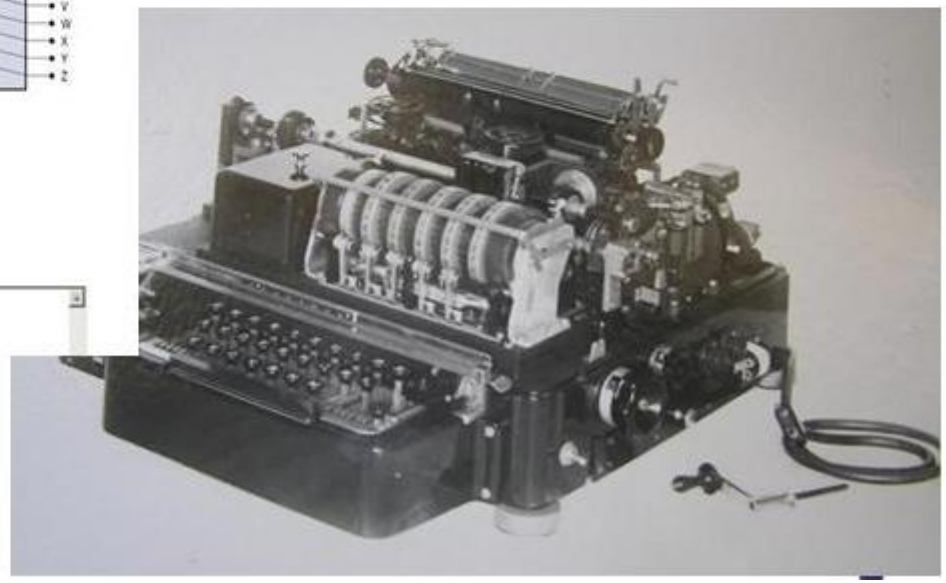
na z v l á š t n y r o z k a z.

Dňa	januára	februára	marca	apríla	mája	júna
1.	FUZ MILICA	HRB PETROS	LUX HUREKA	MRK TARABA	LAN WERTAS	SUK LOMICA
2.	BOH PATRIA	POP MEMELI	HUS ZEZULA	KYL WALLAC	ZER NEMESI	NUL ADMIRA

ŠD-2 / CM-1



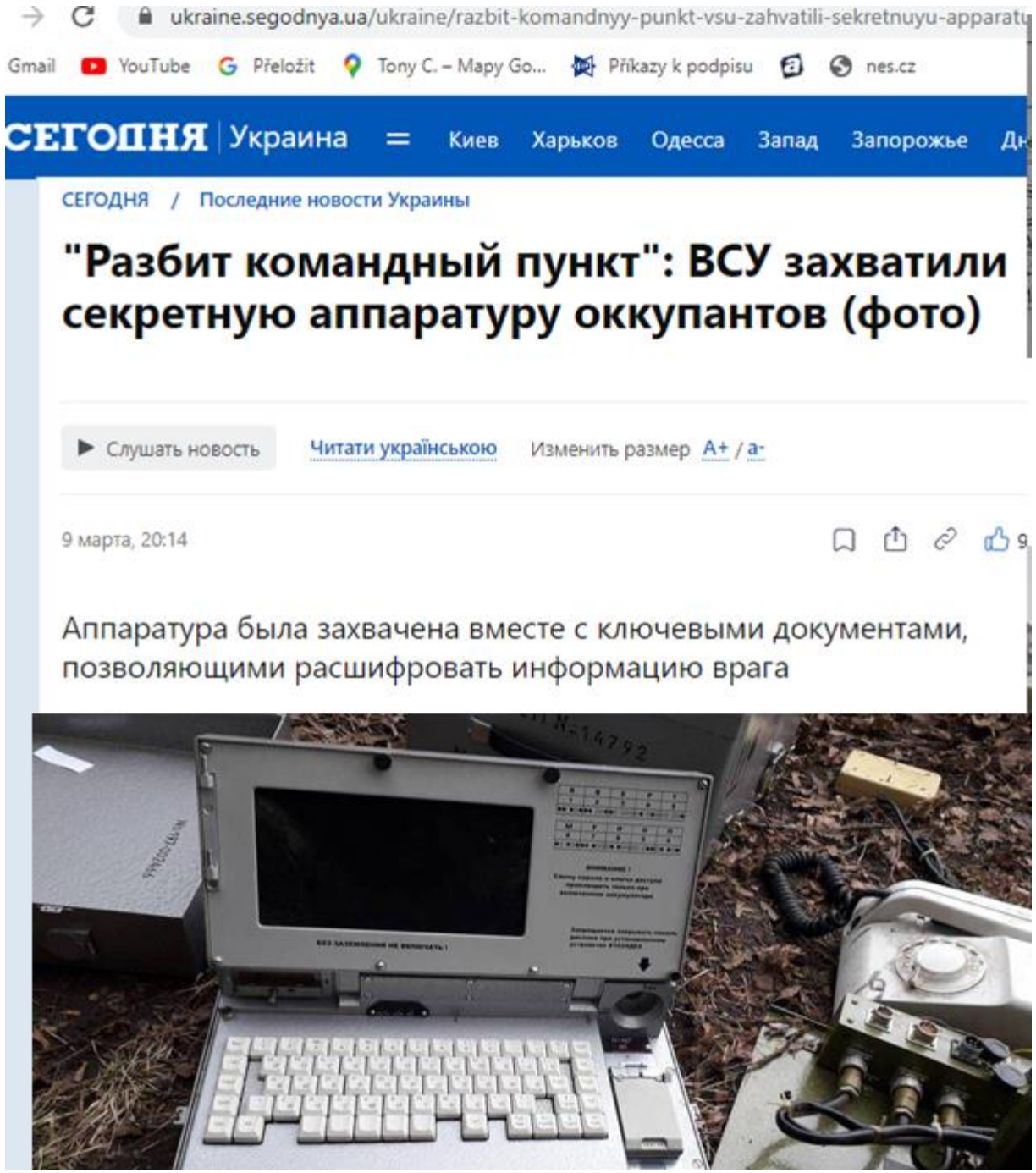




Vojtěch Brtník, 2009, bakalářská práce, MFF UK Praha

ŠD-3

Dálnopisný stroj D-302 „Dalibor"
vyráběný ve Zbrojovce Brno



9. března 2022 se na internetu objevily fotografie **M-427** s tiskárnou M-211, údajně zabavené ukrajinskými silami z ruského velitelského stanoviště poblíž Kyjeva (Ukrajina). Není jasné, zda tomu tak skutečně je, nebo jde o dezinformaci, ale možné to určitě je.
Zařízení jako M-427 se mohou zdát v éře internetu a osobních počítačů (PC) jako zastaralé a archaické, ale mají mnoho výhod oproti komerčním běžným commercial off-the-shelf (COTS) zařízením. Nelze je hacknout a jsou odolnější proti útokům elektromagnetickým pulsem (EMP).

M-427, kódové označení DERVISH (rusky: ДЕРВИШ), je online/offline šifrovací zařízení pro textové zprávy, vyvinuté kolem roku 2000 v Rusku. Zařízení umožňuje bezpečnou komunikaci přes pevné sítě, jako jsou analogové telefonní linky PSTN a ad-hoc vojenské polní linky, stejně jako mobilní radiokomunikační sítě. Šifrovací algoritmus RAZBEG (РАЗБЕГ) používá 512bitový klíč, který je uložen v zařízení pro ukládání klíčů K1634DK4 (К1634ДК4) vyrobeném společností Data Key v USA.

https://cryptomuseum.com/crypto/ru/m427/

Zlomová léta 1990-2000

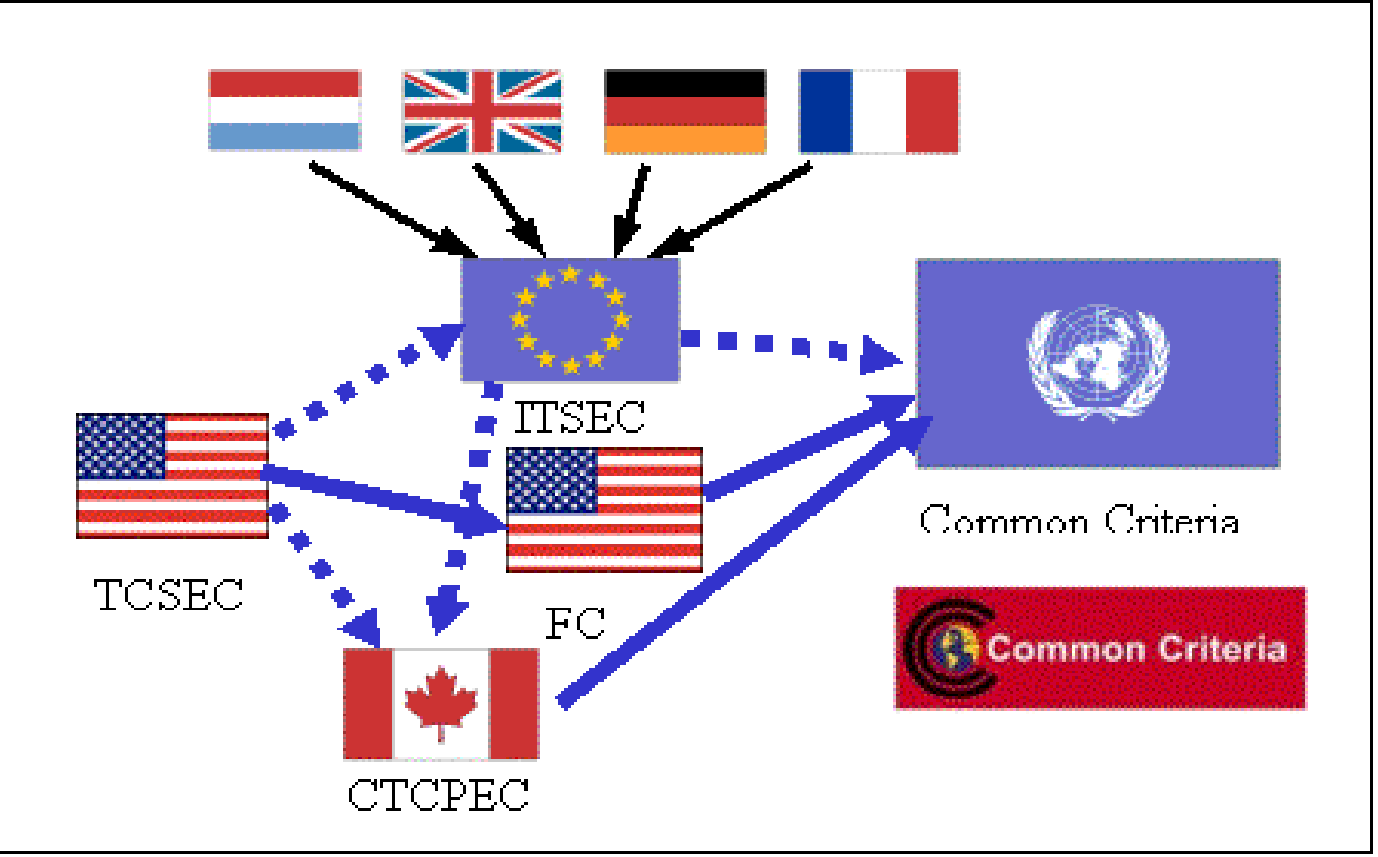
- pád železné opony
- rozvoj PC …… „náhrada za dedikované *HW* šifrátory“
- hledání vhodných šifer pro „PC“
- vstup akademické sféry do oblasti kryptografie (Crypto, Eurocrypt)
- **standardizace , včetně standardů hodnocení bezpečnosti**
- hledání silných šifer ve veřejných soutěžích (AES, SHA3, …)
- ukončení zákazu vývozu silné kryptografie
- legislativa upravující různé oblasti, které se dotýkají informační bezpečnosti

x zapojení ..„stopa“ ČR

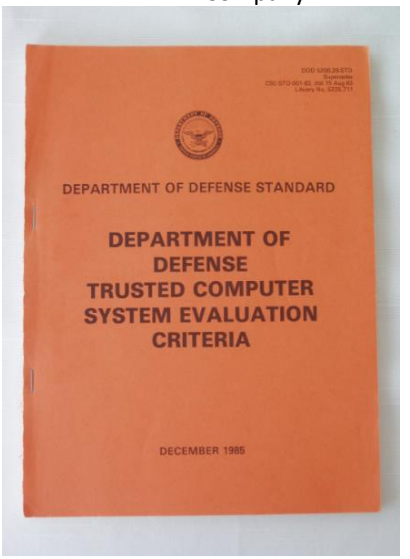
1883
Holandský kryptolog Auguste Kerckhoffs (1835-1903) vydal knihu La Cryptographie Militaire (Vojenská kryptografie).

Autor v knize uvádí řadu požadavků, které by měl vojenský šifrovací systém splňovat. Tyto požadavky jsou známy jako tzv. Kerckhoffsovy principy.

Snad nejdůležitější zásadou, kterou lze z těchto principů snadno odvodit, je, že systém musí odolat i za předpokladu, kdy protivník zná šifrovací systém a nezná pouze šifrovací klíče.



1985: Trusted Computer System Evaluation Criteria (TCSEC)



1990: Information Technology Security Evaluation Criteria (ITSEC)

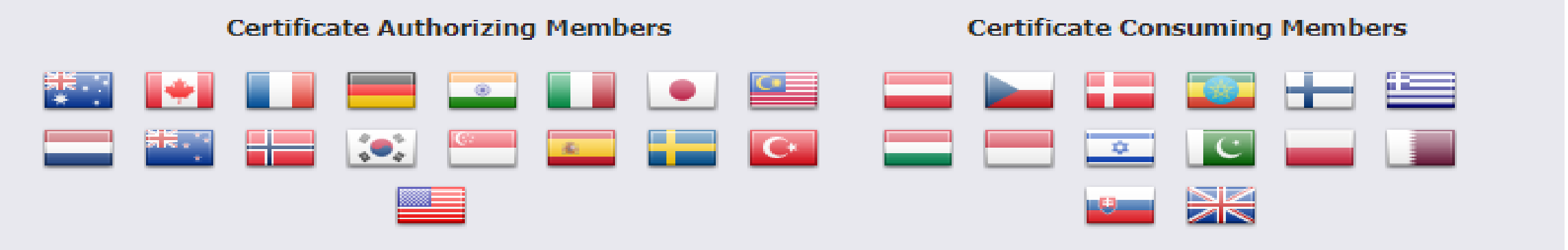
Harmonizovaná verze národních „evropských“ kritérií přijatých ve Francii, Německu, Anglii a Nizozemí, byla předložena v září 1990 v Bruselu k připomínkám a diskusi, které se zúčastnily i USA. Po úpravách byla vydána Úřadem pro oficiální publikace Evropského společenství v červnu 1991 (materiál byl označen jako prozatímní materiál k dvouletému ověření). **Schválena jako doporučení byla v dubnu 1995.**

TCSEC	ITSEC	
-	E0	
D (min. ochrana)	-	
C1 (výb. přístup)	E1	F-C1
C2 (řízený přístup)	E2	F-C2
B1(ochrana návěštím)	E3	F-B1
-	-	
-	-	
B2 (strukt. ochrana)	E4	F-B2
B3 (bezp. domény)	E5	F-B3
A1 (verif. návrh)	E6	

Common Criteria

CC vznikla na základě již dříve používaných kritérií hodnocení, zejména amerických **TCSEC** a Federal Criteria, **evropských ITSEC** a kanadských CTCPEC. Na vývoji CC se podílely **národní organizace** šesti států světa, působící v oblasti bezpečnosti a standardizace, jmenovitě *Kanady, Francie, Německa, Holandska, Velké Británie a Spojených států amerických* a jsou posledním výsledkem úsilí o vytvoření společného standardu v oblasti hodnocení bezpečnosti informačních technologií.

Jako formální základ pro **vzájemné uznávání hodnocení** uzavřely Kanada, Francie, Německo, Velká Británie a Spojené státy americké v roce **1998** dohodu "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security", zkráceně nazývanou **CCRA (CC Recognition Arrangement**).



Česká republika se připojila k dohodě v září roku 2004 **jako certifikáty využívající účastník.**

V současné době již k této smlouvě **celkem 31 členů** (Certificate **Authorizing** Members – **je 17)** Certificate **Consuming** Members – je **14**).

Hodnocení podle CC

V dubnu 2017 byla vydána zatím poslední verze: **CC v3.1. Rele**

Byla vyvinuta společná metodologie pro provádění hodnocení podle CC - **Common Evaluation Methodology (CEM)**. CEM zahrnuje hodnocení na úrovních EAL1 až EAL4 včetně. V důsledku toho je uznávání hodnocení v rámci CCRA prozatím **omezeno na tyto prvé čtyři úrovně záruk**. Oficiální verzí CEM je od 4/2017 verze 3.1, R.5.
http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

Seznam licencovaných laboratoří se neustále rozšiřuje. Naposledy se významně rozšířil o řadu laboratoří v Asii. Aktuální přehled těchto laboratoří je k dispozici zde:
Licensed Laboratories : CC Portal (commoncriteriaportal.org)
(EU: Francie, Německo, Itálie, Holandsko, Norsko, Španělsko, Švédsko, Turecko)

TCSEC	ITSEC		CTCPEC	FC	CC
-	E0		-	-	-
D minimální ochrana	-		-	-	EAL 1 funkčně testovaný HP (TOE)
C1 výběrový přístup	E1	F-C1	-	-	EAL 2 strukturálně testovaný HP (TOE)
C2 řízený přístup	E2	F-C2	T-1	T1	EAL 3 metodicky testovaný a kontrolovaný HP (TOE)
B1 ochrana návěštím	E3 detailní návrh a zdrojové texty programů bezpečnostních funkcí	F-B1	T-2	T2	EAL 4 metodicky navržený, testovaný a přezkoumaný HP (TOE)
-	-	-	T-3	T3	-
-	-	-	-	T4	-
B2 strukturální ochrana	E4	F-B2	T-4	T5	EAL 5 polo-formálně navržený a testovaný HP (TOE)
B3 bezpečnostní domény	E5	F-B3	T-5	T6	EAL 6 polo-formálně navržený s polo-formálně ověřeným návrhem a testovaný HP (TOE)
A1 verifikovaný návrh	E6	-	T-6	T7	EAL 7 formálně navržený s formálně ověřeným návrhem a testovaný HP (TOE)

SOGIS - Senior Oficials Group Information Systems Security

Dohoda SOG-IS vznikla v reakci na rozhodnutí Rady EU ze dne 31. března 1992 (92/242/EHS) v oblasti bezpečnosti informačních systémů a následné doporučení Rady ze 7. dubna (1995/144/ES) o společná kritéria hodnocení bezpečnosti informačních technologií.

Smlouva byla z důvodu zastarání, a především z důvodu požadavku na jednotný přístup hodnocení bezpečnosti vycházející ze standardu **CC** aktualizována v lednu **2010.**

Účastníky této dohody jsou vládní organizace nebo vládní agentury ze zemí Evropské unie nebo EFTA (Evropské sdružení volného obchodu), které zastupují svou zemi nebo země. Od června **2017** jsou národní orgány účastnící se dohody:

- Austria, Bundeskanzleramt
- Belgium, Centre for Cyber Security Belgium
- Croatia, Information Systems Security Bureau
- Denmark, CFCS - Center for Cyber Security
- Estonia, RIA - Riigi Infosüsteemi Amet
- Finland, FICORA - Finnish Communications Regulatory Authority
- France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik
- Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica
- The Netherlands, NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- Luxembourg, ANSSI.lu - Agence Nationale de la SÃŠcurite des SystÃ¨mes d'Information Luxembourg
- Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- Poland, NASK - Naukowa i Akademicka Siec Komputerowa
- Slovakia, NBÚ - Národný bezpečnostný úrad
- Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- Sweden, FMV - Försvarets Materielverk
- United Kingdom, NCSC - National Cyber Security Centre

ENISA European Agency for Cybersecurity

- Dne 17. dubna 2019 bylo schváleno *Nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013* („akt o kybernetické bezpečnosti“), které zavádí nový jednotný certifikační rámec společný pro celou Unii.

- Jedná se o první akt svého druhu a rozsahu – zatím žádný mezinárodně uznávaný certifikační systém na světě totiž nebyl založen na veřejnoprávní bázi a neintegroval certifikaci jak produktů (např. router, čipová karta, …), tak **služeb a procesů**.

- Pravděpodobně největším a nejúspěšnějším předchůdcem tohoto systému byla Common Criteria, ta se však soustředila (a aplikovala) pouze na certifikaci produktů.

- Pro EU je v tomto ohledu důležitá zejména spolupráce SOG-IS (Senior Officials Group Information Systems Security). Užší spolupráce několika evropských členů Common Criteria, kteří jsou svázáni hlubší důvěrou a ve vzájemné spolupráci tvoří nová schémata a uznávají si certifikáty vyšší bezpečnostní úrovně než ostatní členové), neboť první schéma ENISA, které je v současné době ve schvalovacím procesu, je právě schéma nahrazující SOG-IS, tedy v podstatě EU implementace Common Criteria. Jde o návrh schématu pro certifikaci produktů.

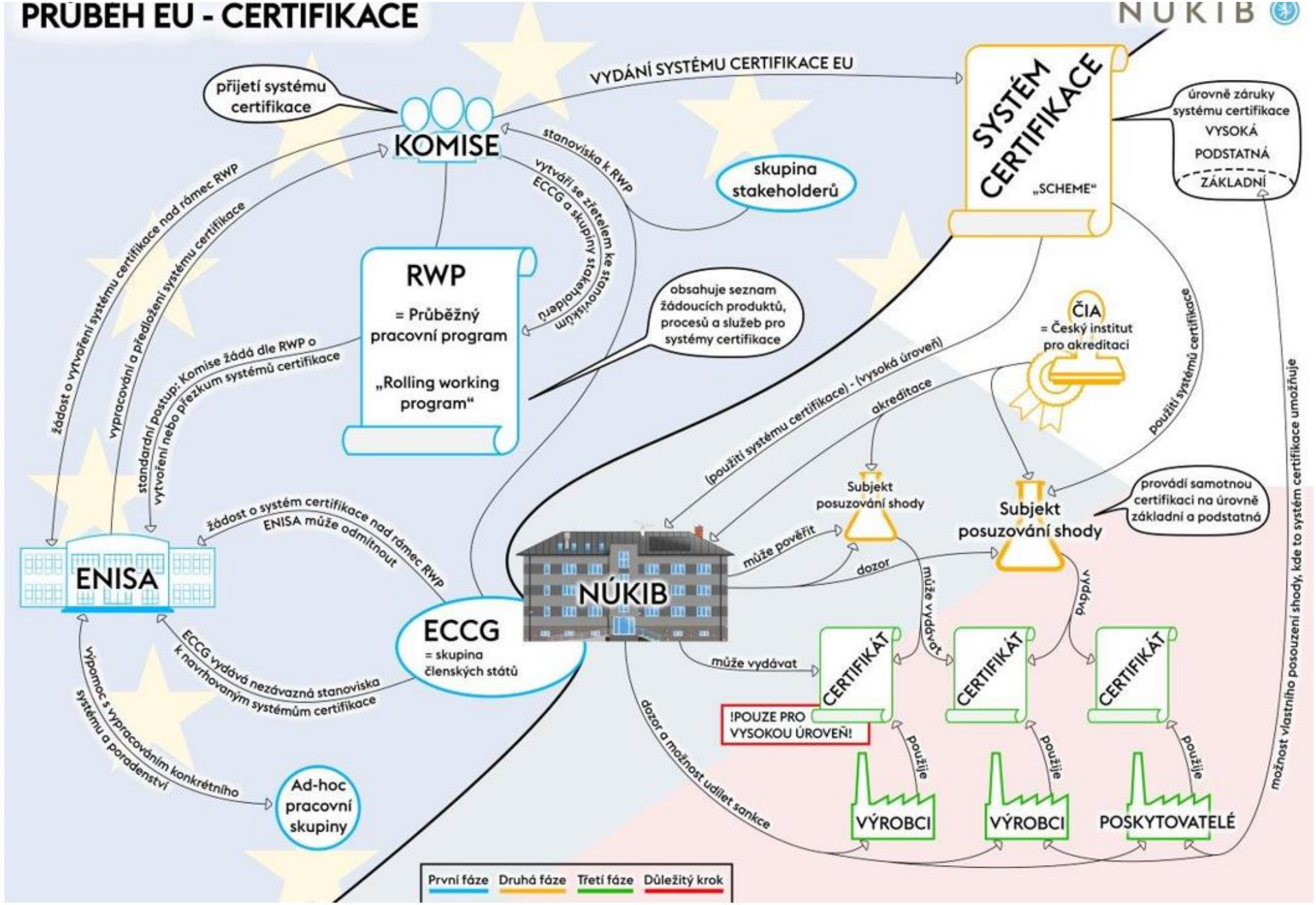
CAB

- Subjekty, označované jako Conformity Assessment Bodies (CAB) jsou faktickými vykonavateli certifikace, přičemž CAB pracují ve spojení s testovacími laboratořemi.
- K výkonu hodnocení musí splnit vcelku náročné podmínky, které Akt stanovuje ve své Příloze. Jenom takové CAB mohou být akreditovány akreditačním orgánem (v českém prostředí se jedná o Český institut pro akreditaci, o.p.s.) a jenom akreditované CAB mohou provozovat certifikaci.
- Jako subjekt posuzování shody může (a měl by) být akreditován i certifikační orgán, který je součástí NCCA, neboť je v některých případech vyžadováno, aby byla certifikace prováděna přímo NCCA. Pokud evropské certifikační schéma stanoví speciální požadavky na CAB, provádět certifikaci podle takového schématu může jen takový CAB, který byl pro naplnění speciálních podmínek k takové certifikaci autorizován od NCCA. U každého takového schématu musí NCCA zpravit Komisi o všech autorizovaných subjektech posuzování shody.

Podmínky provozu CAB jsou natolik přísné, že je možné, že by v některých státech CAB vůbec nevznikly nebo vznikly až s odstupem více let.

Příloha č.1 - Čtyři úrovně certifikace definované v IACS

Figure 11 Four levels of certification in IACS


PRŮBĚH EU - CERTIFIKACE
NÚKIB
přijetí systému certifikace
KOMISE
VYDÁNÍ SYSTÉMU CERTIFIKACE EU
SYSTÉM CERTIFIKACE
„SCHEME"
úrovně záruky systému certifikace
VYSOKÁ
PODSTATNÁ
ZÁKLADNÍ
stanoviska k RWP
skupina stakeholderů
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
výpomoc s vypracováním konkrétního systému a poradenství
Ad-hoc pracovní skupiny
CERTIFIKÁT
CERTIFIKÁT
CERTIFIKÁT
!POUZE PRO VYSOKOU ÚROVEŇ!
použije
použije
použije
dozor a možnost udílet sankce
VÝROBCI
VÝROBCI
POSKYTOVATELÉ
možnost vlastního posouzení shody, kde to systém certifikace umožňuje
První fáze
Druhá fáze
Třetí fáze
Důležitý krok

- Děkuji za pozornost

Pavel Vondruška
pavel.vondruska@crypto-world.info
pavel.vondruska@matfyz.cz a
pavel.vondruska@cetin.cz