



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



M U N I



Název projektu: Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI

Identifikační kód: VJ02010010

## Odborná zpráva - Etapa 3

Období: 01/2022 - 06/2022

Příjemce: Vysoké učení technické v Brně  
Antonínská 548/1  
Brno 60190

Jméno hlavního řešitele: doc. Ing. Jan Hajný, Ph.D.  
Tel.: +420541146961  
Email: hajny@vut.cz

Další účastník 1: Masarykova univerzita  
Žerotínskovo náměstí 617/9  
Brno 602 00

Jméno řešitele: doc. RNDr. Petr Švenda, Ph.D.  
Tel.: +420549491878  
Email: xsvenda@fi.muni.cz

Další účastník 2: České vysoké učení technické v Praze  
Jugoslávských partyzánů 1580/3  
Praha 160 00

Jméno řešitele: Ing. Martin Novotný, Ph.D.  
Tel.: +420224358715  
Email: martin.novotny@fit.cvut.cz



---

## Obsah

<b>1</b>	<b>Úvod</b>	<b>2</b>
<b>2</b>	<b>Analýza stávajících certifikačních reportů schémat Common Criteria a FIPS 140-2/3</b>	<b>4</b>
2.1	Scénáře využití při možnosti automatické analýzy dat . . . . .	4
2.2	Analýza proveditelnosti automatického zpracování dokumentů . . . . .	5
2.2.1	Kategorie dat extrahovatelných z certifikačních artefaktů . . . . .	5
2.3	Reference mezi certifikáty . . . . .	7
2.3.1	Formát identifikace certifikátu . . . . .	7
2.3.2	Typy referencí mezi certifikáty . . . . .	7
2.4	Identifikované problémy pro automatizované zpracování . . . . .	8
2.5	Sumář relevantních prací z Masarykovy univerzity . . . . .	11
2.5.1	“Data analysis of the Common Criteria certificates”, Jiří Michalík . . . . .	11
2.5.2	“Analysis of NIST FIPS 140-2 security certificates”, Stanislav Boboň . . . . .	13
2.5.3	“Analysis of Common Criteria Protection Profiles”, Martin Friant . . . . .	13
<b>3</b>	<b>Závěr</b>	<b>14</b>



Číslo a název aktivity: Etapa 3	
Období řešení:	01/2022 - 06/2022
Cíl aktivity:	Analýza stávajících certifikačních reportů schémat Common Criteria a NIST FIPS 140-2/3.
Krátký popis řešení:	Analýza proveditelnosti automatizovaného zpracování a vyhodnocení obsahu bezpečnostních certifikátů vydaných dle schémat Common Criteria a NIST FIPS140/2-3. Identifikace problémů. Identifikace scénářů využití.
Řešitel zodpovědný za realizaci:	Petr Švenda (Masarykova univerzita).
Stav plnění aktivity:	Splněno
Výstupy:	1x shrnující zpráva, 3x přílohy popisující provedené analýzy (bp/mgr práce, EN), 1x rozšířena implementace nástroje seccerts ( <a href="https://github.com/crocs-muni/sec-certs">https://github.com/crocs-muni/sec-certs</a> ).
Výsledky:	Odborná zpráva
Doložení splnění aktivity:	Odborná zpráva – Etapa 3
Shrnutí:	Všechny podmínky pro přechod do další aktivity byly splněny.



---

## 1 Úvod

Tato zpráva se zabývá analýzou stávajících schémat Common Criteria a NIST FIPS 140-2/3 používaných pro certifikaci bezpečnostních produktů na celosvětové (Common Criteria) a národní úrovni s celosvětovým přesahem (USA, NIST FIPS 140-2/3). Obě tato schémata jsou výrazně relevantní pro projekt VJ02010010 „Nástroje pro verifikaci bezpečnosti kryptografických zařízení s využitím AI“ – zhruba 35% všech certifikovaných produktů v rámci Common Criteria je z kategorie kryptografického hardware (“ICs, Smart Cards and Smart Card-Related Devices and Systems”) a schéma NIST FIPS 140-2/3 je přímo zaměřeno na certifikaci kryptografických modulů a jejich implementací (“Security Requirements for Cryptographic Modules”). Cílem zprávy je popsat možnosti automatické analýzy již vydaných certifikátů a souvisejících dokumentů a jejich následné využití pro získání vhledu do dlouhodobých certifikačních trendů, podpora uživatele certifikovaného zařízení pro včasné notifikaci o potenciálních zranitelnostech a analýza vlivu dílčích částí certifikačního procesu na výslednou bezpečnost certifikovaných produktů.

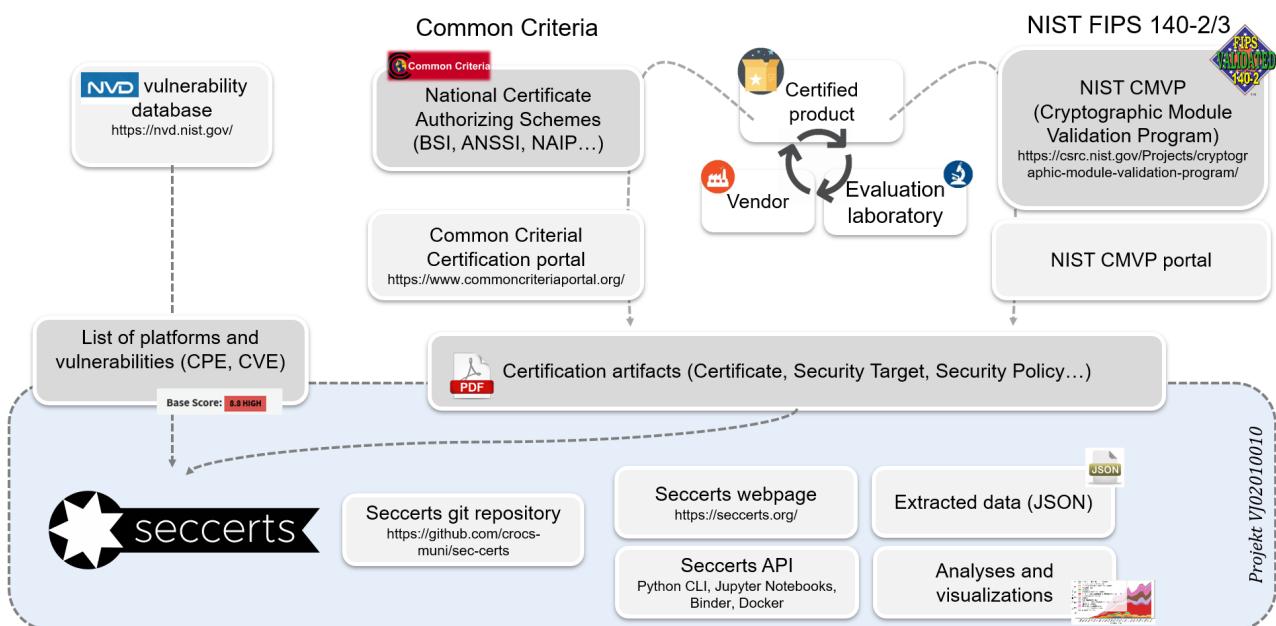
Nejprve poskytujeme přehled identifikovaných scénářů využití automatizované analýzy, souhrn dostupných certifikačních artefaktů, kategorie extrahovaných dat a typy identifikovaných referencí. Dále detailně popisujeme identifikované problémy pro automatizované zpracování a poskytujeme ukázky výstupů provedených analýz.

Pro vývoj nástroje *seccerts* [1] pro analýzu certifikátů jsme zvolili metodu častých iterací konzultovaných s aplikačním garantem. Nástroj je tedy průběžně rozšiřován dle aktuálních potřeb a zpětné vazby od aplikačního garanta a dalších uživatelů. Prototypová verze nástroje pro analýzu s iniciální funkčností vznikala již před formálním započetím projektu (typicky bakalářské, magisterské a postgraduální práce vedené na FI MUNI) a bylo tak možné v omezeném čase prvních šesti měsíců běhu projektu provést i kvantitativní vyhodnocení nad reálnými certifikačními daty, demonstrovat základní funkčnost aplikačnímu garantovi a navrhnout další potřebné rozšíření funkčnosti. Celkové schéma řešené problematiky je zachyceno obrázku 1.

Zpracované výstupy jsou dostupné na stránce <https://seccerts.org> [8].

Výsledky byly prezentovány aplikačnímu garantovi (NUKIB) v těchto termínech:

- **28.4.2022, Praha.** Prezentace stávajících možností nástroje *seccerts*, diskuze oblastí využití a dalších rozšíření.
- **22.6.2022, Brno.** Zaškolení pracovníka NUKIB do použití Python programovací rozhraní API nástroje *seccerts*. Diskuze možností analýzy neveřejných dokumentů pomocí dodatečné lokace souborů a párování. Důležitost možností filtrování na omezenou sadu produktů.
- **1.7.2022, Praha.** Prezentace nových rozšíření, mapování na NIST NVD databázi.



Obrázek 1: Celkové schéma řešené problematiky. Zpracovávané datové artefakty (certifikáty, popisy produktů) jsou vytvářeny v rámci certifikačních schémat Common Criteria a NIST FIPS 140-2/3. Používané popisy platform (CPE) a publikované zranitelnosti (CVE) jsou získávány z NIST National Vulnerability Database. Projekt *seccerts* tyto vstupní data automaticky zpracovává a poskytuje možnost jejich analýzy, vyhledávání dle produktů i zranitelností či notifikaci nově objevené relevantní zranitelnosti. Zpracované výstupy lze nalézt na webu <https://seccerts.org>, nebo je vygenerovat lokálně s využitím otevřeného nástroje *seccerts*.



## 2 Analýza stávajících certifikačních reportů schémat Common Criteria a FIPS 140-2/3

V rámci této kapitoly se zabýváme identifikací postupů pro analýzu artefaktů vznikajících během certifikační procesu dle Common Criteria a FIPS140-2/3, možností jejich automatického zpracování, možného využití a seznamu zjištěných problémů. Základní schéma celého procesu je zachyceno na Obrázku 2.

Cílem tohoto textu není poskytnout detailní popis fungování certifikačního procesu, ale shrnout nové informace ohledně datového zpracování certifikátů zjištěných během této fáze projektu. Zájemce o detaily fungování certifikačních schémat odkazujeme na existující literaturu, implementační doporučení a příslušné standardy [7; 9].

### 2.1 Scénáře využití při možnosti automatické analýzy dat

Analýza certifikačních dokumentů může poskytnout celou řadu využití. V současné době se zaměřujeme na tyto scénáře:

1. **Vhled do trendů v celém certifikačním ekosystému** včetně jejich kontinuální aktualizace v čase, například typ a bezpečnostní úroveň vydaných certifikátů, výskyty zájmových klíčových slov, doba platnosti certifikátů a další. Obrázky 7 (vývoj počtu certifikátů pro danou kategorii vydaných v konkrétním roce), 8 (vývoje zastoupení výrobců produktů v letech) a 9 (vývoj zastoupení kryptografických algoritmů v čase) zachycují ukázku extrahovaných charakteristik certifikačního procesu.
2. **Notifikace uživatelů certifikovaných produktů při výskytu nové relevantní potenciální zranitelnosti.** Vyžaduje mapování certifikátů na identifikaci platformy v databází zranitelností (např. Common Platform Enumeration, CPE, v NIST NVD databázi) a vytvoření grafu referencí mezi jednotlivými certifikáty pro zachycení vzájemných vztahů (kompozitní produkty, částečná aktualizace existujícího produktu...). Obrázek 6 zachycuje ukázku webové stránky automaticky generované z extrahovaných dat pro vybraný certifikát.
3. **Iniciální posouzení rozsahu dopadů nově nalezené zranitelnosti.** Bezpečnostní výzkumník může provést zjištění, které další produkty by mohly být zasaženy a bylo by vhodné provést např. oznámení chyby (responsible disclosure). Lze využít vyhledávání dle přímých a nepřímých referencí prokazatelně zranitelného produktu či výskytu klíčových slov. Koncový uživatel může zjistit, zda je ovlivněn zranitelností v souvisejícím produktu.
4. **Proaktivní sledování komponent ovlivňujících bezpečnost používaných produktů** pro zachycení potenciální zranitelnosti. Ukázka takového grafu je zachycena na Obrázku 5.
5. **Možnost navázání dodatečných datových zdrojů k certifikovaným produktům**, např. parametry provedených laboratorních testů a jejich výsledky pro možnost jejich nezávislé replikace.



## 2.2 Analýza proveditelnosti automatického zpracování dokumentů

V rámci analýzy schématu Common Criteria jsme identifikovali tyto veřejně dostupné a analyzovatelné dokumenty:

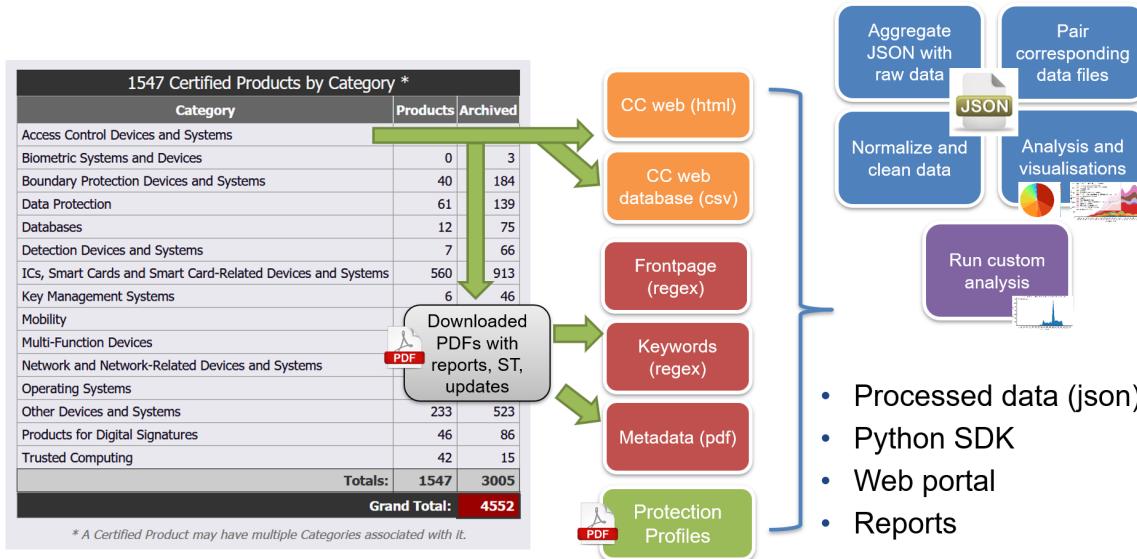
- **Security Target**, dokument poskytnutý výrobcem evaluační laboratoři. Obsahuje technický popis a hranice certifikovaného produktu.
- **Certification Report** vydaný certifikační autoritou, v případě Common Criteria tzv. Certificate Authorization Member (např. French ANSSI) na základě kontroly provedené akreditovanou evaluační laboratoří. Příklad úvodní strany dokumentu certifikátu je uveden na Obrázku 3.
- **Maintenance Report, Monitoring report**, dokumenty obsahující úpravy certifikovaného produktu drobného charakteru, které nevyžadují kompletní recertifikaci, případně jen prodloužení doby platnosti certifikátu.
- **Protection Profile**. Dokumenty popisující ochranný profil -- šablonu pro specifickou certifikovatelnou funkčnost.
- **CSV/HTML stránky** s dodatečnými informacemi poskytující metadata, sumáře, datové rozšíření atp. generované např. commoncriteriaproduct.org, Certificate Authorizing Members atp.
- **Webová stránky** s průběžným stavem certifikačního procesu. Rozdílné mezi jednotlivými vydavateli certifikátů (např. BSI nebo ANSSI).
- **(Dodatečné) neveřejné dokumenty** sdílené typicky mezi laboratoří a výrobcem.

V rámci analýzy schématu NIST FIPS 140-2/3 jsme identifikovali tyto veřejně dostupné a analyzovatelné dokumenty:

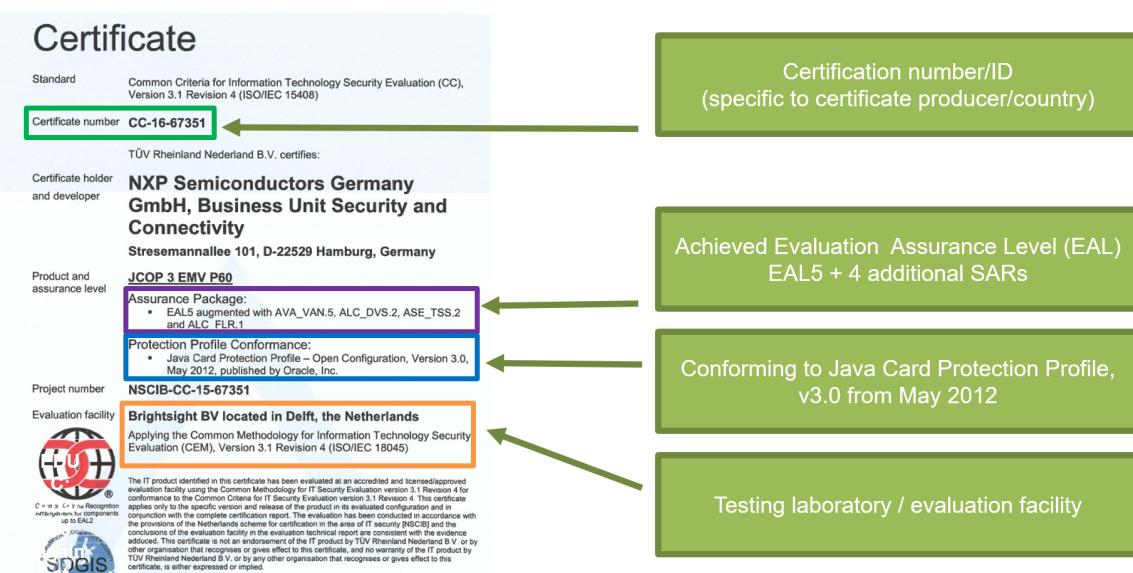
- **Security Policy**, dokument poskytnutý výrobcem evaluační laboratoři. Obsahuje technický popis a hranice certifikovaného kryptografického modulu a obsažené implementace algoritmů.
- **Webová stránka s certifikátem modulu a algoritmu/algoritmů**, vydaná NISTem na základě kontroly provedené akreditovanou evaluační laboratoří. Obsahuje metada provazující modul a jeho používané algoritmy.
- **Webová stránky** s průběžným stavem certifikačního procesu.

### 2.2.1 Kategorie dat extrahovatelných z certifikačních artefaktů

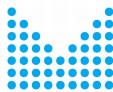
- **Metadata:** Výrobce, Název produktu, Období platnosti, Categorie, certifikační schéma, použitý Protection Profile, výsledná celková úroveň certifikace.
- **Klíčová slova zachytitelná regulárními výrazy:** Cryptographic algorithms, Cryptographic libraries, Security Assurance Requirements, Security Functional Requirement, Evaluation facility, Vulnerability identifier.
- **Strojové učení pro napojení na jiné datové sady:** Certificate identifier, Common Platform Enumeration (CPE) a napojené zranitelnosti (CVE).



Obrázek 2: Schéma analýzy certifikačních artefaktů v rámci nástroje *secctools*. Zobrazené statistiky a stahovaná data pocházejí z <https://commoncriteriaportal.org> [4].



Obrázek 3: Ukázka přední stránky běžného certifikátu [3] se zvýrazněním vybraných položek relevantních z hlediska analýzy certifikátů. Pouze malá část z uvedených údajů je poskytována ve strojově zpracovatelné podobě.



## 2.3 Reference mezi certifikáty

Pro stanovení mapy závislosti v rámci všech certifikovaných produktech je třeba v textu dokumentu identifikovat výskyt reference, určit referencovaný dokument i typ provedené reference. Taková mapa v současnosti není od organizací zastínující certifikační schémata dostupná, automatická analýza dokumentů však nabízí potenciál jejího vytvoření. Obrázek 4 zachycuje část mapy referencí mezi certifikáty vydanými dle Common Criteria a FIPS 140-2/3 extrahované pomocí nástroje *seccerts*. Obrázek 5 vizualizuje vybranou podkomponentu grafu s certifikáty přímo či nepřímo ovlivňující certifikát ANSSI-CC-2020/44 (Electronic passport eTravel v2.2).

### 2.3.1 Formát identifikace certifikátu

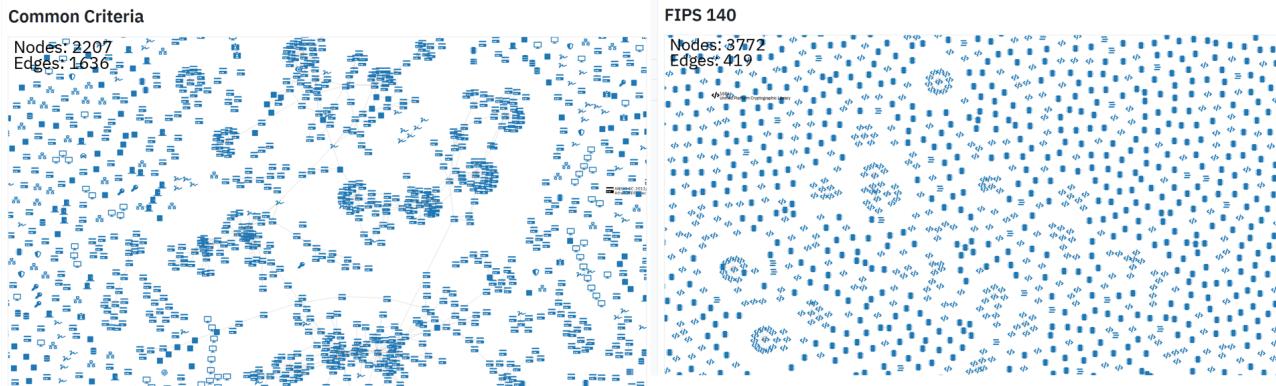
Výchozím krokem analýzy bylo vytvoření sady regulárních výrazů pro všechny používané formáty identifikace certifikátů jednotlivými (národními) autoritami. Následně byly tyto identifikátory v jednotlivých souborech automatizovaně vyhledávány a manuálně rozšiřovány o další tak, aby došlo k pokrytí téměř všech vydaných certifikátů. Celkově se jedná o více než 30 regulárních výrazů, které zachycují více jak 60 různých formátů a došlo k pokrytí více jak 97% všech certifikátů.

### 2.3.2 Typy referencí mezi certifikáty

Druhou fází bylo přiřazení čísla certifikátu konkrétnímu certifikovanému produktu (ne vždy je toto přiřazení dostupné přímo v rámci dat poskytovaných [commoncriteriaprofile.org](http://commoncriteriaprofile.org) [4]) a detekci všech referencí v daném dokumentu na ostatní certifikáty.

Na základě ruční analýzy náhodně vybraných certifikátů jsme identifikovali tyto typy používaných referencí mezi certifikáty:

- **Recertifikace na základě dříve certifikovaného produktu:** Příklad: "This is a re-certification based on BSI-DSZ-CC-322-2005 and BSI-DSZ-CC-338-2005." Re-certifikace je pro upravený produkt založený na jiném, již certifikovaném, například s vyměněnou základní platformou integrovaných obvodů.
- **Podobné jako již certifikovaný produkt, ale odlišný:** Příklad: „Re-use has been made of evaluation results of a very similar TOE on another hardware platform under certification ID CC-13-37078.“. Podobné recertifikaci, ale certifikaci obou produktů může probíhat paralelně s využitím sdílené evaluace shodných částí.
- **Na základě, nebo s použitím, již certifikované komponenty.** Příklad: "The TOE is a composite product. For development and production sites regarding the platform please refer to the certification report ANSSI-CC-2017/61." Evaluace využívá již existující certifikované komponenty a věnuje se dodatečným rozšíření a způsobu začlenění.
- **Nahrazující již certifikovanou komponentu.** Dříve certifikovaný produkt je nahrazen novějším s předpokladem delší doby platnosti certifikátu. Produkty mohou sdílet část kódu nebo výrobních postupů.
- **Část produktu je pokryta separátní certifikací:** Příklad: "The further security mechanism Basic Access Control (BAC)) is subject of the separate evaluation process BSI-DSZ-CC-1074-2019". ToE neobsahuje některé části (BAC – Basic Access Control v tomto



Obrázek 4: Celkový pohled na extrahovaný graf referencí pro produkty certifikované v rámci Common Criteria (vlevo) a NIST FIPS 140-2/3 (vpravo). Produkty v rámci Common Criteria obsahují výrazně větší množství vzájemných referencí než FIPS 140, zároveň významná část produktů nereferencuje žádný jiný certifikát.

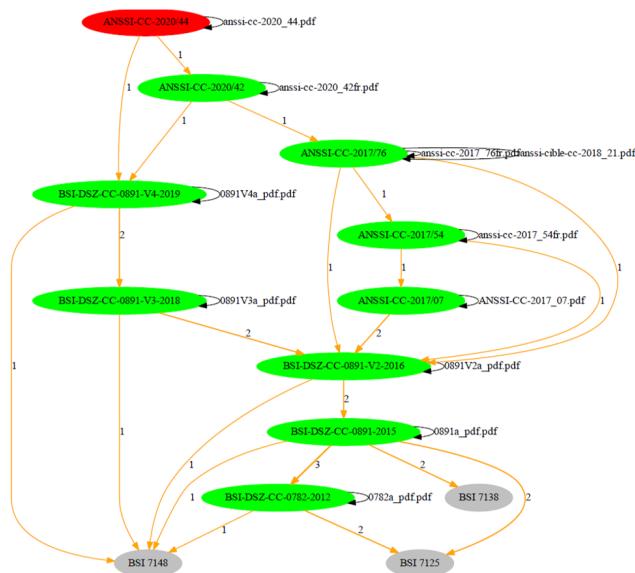
příkladu), ale tyto části jsou certifikovány samostatně. Jedná se defacto o kompozitní produkt, ale není jako kompozitní certifikován. Pokud je referencovaný produkt zranitelný, referencující produkt může být také zranitelný.

- **Jiný typ reference.** Jiný typ reference, například zmínka o typickém příkladu určité třídy produktů nebo blíže neurčená reference. Certifikáty a popisy certifikovaných produktů všeobecně používají reference na jiné certifikáty jen v odůvodněných případech a proto reference jiného typu nejsou příliš časté.

## 2.4 Identifikované problémy pro automatizované zpracování

Hlavním důvodem pro identifikované problémy při automatickém zpracování je fakt, že certifikační dokumenty připravují lidé s primárním určením pro lidského čtenáře, nikoli pro automatický nástroj. Jednotlivé standardy nepožadují striktní jednotnou formu ani standardizovaná metadata.

- **Chybějící standardní unikátní identifikace dokumentu.** Jednotlivé (národní) schémata pro autorizaci certifikátů (např. německé BSI, francouzské ANSSI, americký NIAP atp.) používají vlastní (a odlišný) způsob přidělování unikátních identifikátorů. Mezi jednotlivými formáty existují velké rozdíly, které zároveň ovlivňují úspěšnost a přesnost jejich automatické detekce. Například BSI nebo ANSSI používají formáty s dobře definovanou strukturou ("BSI-DSZ-CC-322-2005") a lze jej relativně snadno detektovat. Naopak např. NIST FIPS 140 používá pouze inkrementální čísla -- a to jak pro certifikované moduly (modules), tak pro algoritmy (algorithms). Inkrementální číslo je předcházeno znakem #, ale jen v některých případech a jeho odlišení od jiných výskytů čísel v dokumentech je tedy obtížný a kontextově závislý problém. Kanadské schéma se přesunulo od obecně lépe strukturovaného identifikátoru ("383-4-138-CR") na obecně hůře detekovatelný ("516-LS").
- **Certifikační dokumenty a další artefakty jsou v různých národních jazycích,** což vyžaduje nejprve (automatický) překlad a tím zvyšuje riziko nepřesnosti.



Obrázek 5: Ukázka závislostí relevantních pro bezpečnost certifikátu s identifikátorem ANSSI-CC-2020/44 (Electronic passport eTravel v2.2 platform, Gemalto, EAL5+). Díky znalosti grafu referencí jsou zobrazeny všechny certifikáty, které jsou přímo nebo transitivně referencovány certifikátem ANSSI-CC-2020/44.

[seccerts](#) CSV Report Security target Heuristics References Updates Raw data Search

[Home](#) / Common Criteria / 36ed04f4b45e3ab9

# NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3

**⚠ This certificate has known related [CVEs](#), which means that the certified product may have security vulnerabilities.**

## CSV information [?](#)

Status: archived Valid from: 06.04.2011 Valid until: 01.09.2019 Scheme: Manufacturer: NXP Semiconductors Germany GmbH Business Line Identification Category: ICs, Smart Cards and Smart Card-Related Devices and Systems Security level: ALC\_DVS2, AVA\_VAN.S, EAL5+

[Certification report](#) PDF TXT [Security target](#) PDF TXT

## Heuristics [?](#)

Certificate ID: BSI-DSZ-CC-0675-2011  
**CPE matches**

- cpe:2.3:h:nxp:j3a081:.\*:.\*:.\*
- cpe:2.3:h:nxp:j2a081:.\*:.\*:.\*
- cpe:2.3:h:nxp:j3a041:.\*:.\*:.\*

## Related CVEs

ID	Links	Severity	CVSS Score	Published on		
ID	Links	Severity	Base	Exploitability	Impact	Published on
CVE-2021-3011	<a href="#">C</a> <a href="#">M</a> <a href="#">N</a>	<span>MEDIUM</span>	4.2	3.6	07.01.2021 16:15	

## References [?](#)

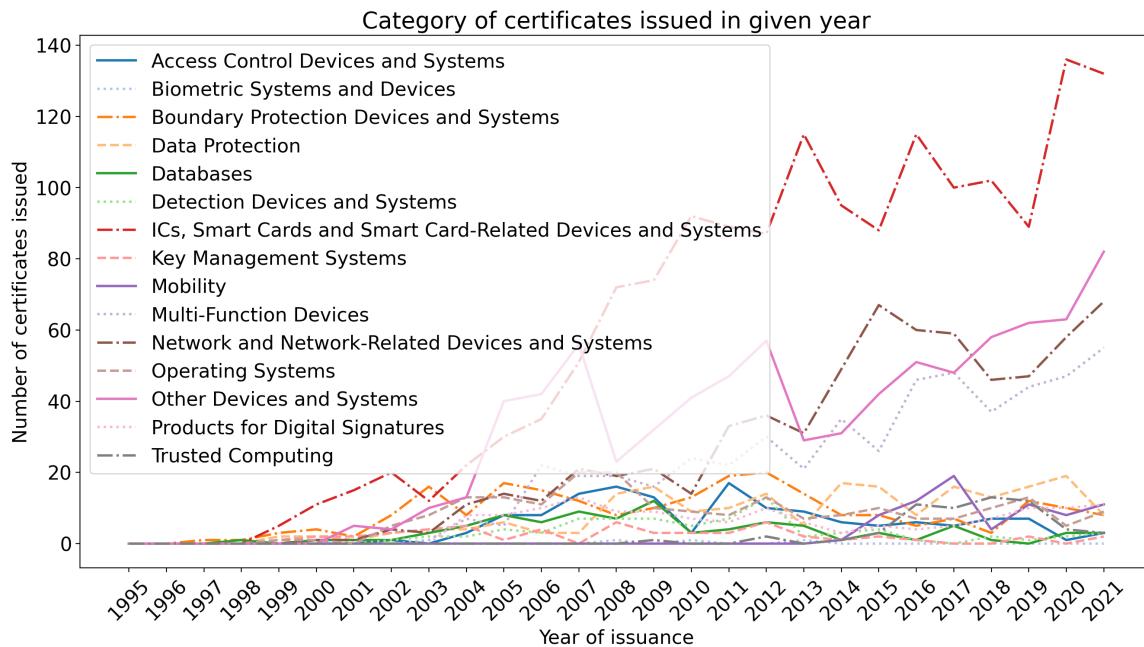
Nodes: 683 Edges: 1146



Obrázek 6: Ukázka automatizovaně generované stránky na portálu seccerts.org obsahující vybrané, automaticky extrahované data o vybraném produktu. Díky mapování na databázi zranitelností NIST NVD jsou zvýrazněny nalezené zranitelnosti dle CVE (zde jedna známá zranitelnost).



- **Dokumenty obsahují velké množství překlepů**, a to včetně klíčových položek jako název certifikovaného produktu nebo jeho identifikace, např. "BSI-DSZ-CC-404-2007" vs. "BSI-DSZ-CC-0404-2007" (chybějící 0 v inkrementální části formátu) nebo vynechání některé podčásti (např. roku).
- **Dostupné dodatečné certifikační artefakty nemají validní strukturu.** Například CSV soubor se základní údaji o certifikovaných produktech poskytovaný portálem com-moncriteriaporta.org používá jako oddělovač čárku, která se ale zároveň vyskytuje ve jménech certifikovaných produktů. Výsledný poskytnutý CSV soubor tak nemá validní strukturu a je nutné provádět jeho heuristickou, nejednoznačnou opravu.
- **Ochranné profily (Protection Profiles, PP) nemají jednoznačný identifikátor** a díky tomu jsou nejednoznačně referencovány z certifikačních dokumentů. Dodatečný problém vzniká u těch PP, které mají sami několik možných konfigurací a referencující dokument tak musí specifikovat korektně i konkrétní konfiguraci.
- **Veřejně dostupné dokumenty neobsahují dostatečné zdůvodnění pro vydání údržbových certifikátů (Maintainance Report).** V některých případech je zmíněna adresace existujících zranitelností, jejich seznam je ale vynechán či je přítomný pouze v neveřejných dokumentech (Impact Analysis) připravovaných výrobcem certifikovaného produktu.
- **Certifikační dokumenty neobsahují dostatek podkladů pro nezávislou replikaci evaluačních kroků** provedených v průběhu certifikace evaluační laboratoří. Koncový uživatel tak nemůže posoudit míru a rozsah provedené bezpečností evaluace, ani identifikovat vůči kterým konkrétním útokům byl produkt testován. Aby mohl koncový uživatel nezávisle replikovat (v ideálním případě) všechny certifikační kroky, je potřebné mít kompletní seznam použitých hardwarových i softwarových nástrojů jejich konfigurace a laboratoř obdržené výsledky i mít tyto nástroje k dispozici (ideálně open-source). V praxi je nezávislá replikace jen velmi obtížně proveditelné, neboť provedené testy jsou většinou považované za duševní vlastnictví dané laboratoře, chybí přesný popis konfigurací a získaných výsledků.
- **Certifikované produkty nemají přiřazenou unikátní identifikaci v rámci veřejných databází známých zranitelností** (např. NIST National Vulnerability Database, NVD). V případě nalezení nové zranitelnosti tak i při jejím propojení se zranitelnou platformou (záznam CPE v případě databáze NVD) nedochází k automatickému propojení na certifikovaný produkt a možné automatické notifikace koncového uživatele. Řešením by bylo proaktivně přiřazovat certifikovaným produktům CPE záznam pro případ budoucích zranitelností.
- **Kompositní certifikované produkty nemají jasně specifikovanou a automaticky zpracovatelnou interní komponentní strukturu**, čímž se zvyšuje obtížnost nalezení všech zranitelných produktů v případě nalezení chyby v dílčí komponentě. Možným řešením by bylo provést standardní specifikaci produktu obdobně jako v případě tzv. Bill of Material (BoM) používaný pro hardwarové komponenty.
- **Certifikace většinou nepokrývá celý produkt, ale pouze jeho vybranou podčást,** definované scénáře použití a vybrané konfigurace (tzv. Target of Evaluation, ToE). Specifikace ToE a jeho hranice jsou ale provedeny pouze textovou formou bez standardizované



Obrázek 7: Ukázka analýzy vývoje certifikačního ekosystému v čase na základě datové analýzy certifikátů pomocí nástroje *seccerts*. Zachycuje počet certifikátů vydaných pro danou certifikační kategorii v rámci Common Criteria.

struktury a může tak být pro koncového uživatele obtížné určit, zda je nasazený produkt provozován v certifikované konfiguraci. Automatická extrakce hranic ToE je velmi obtížná a může tak dojít k situaci identifikace zranitelnosti v produktu, ale mimo jeho certifikované hranice.

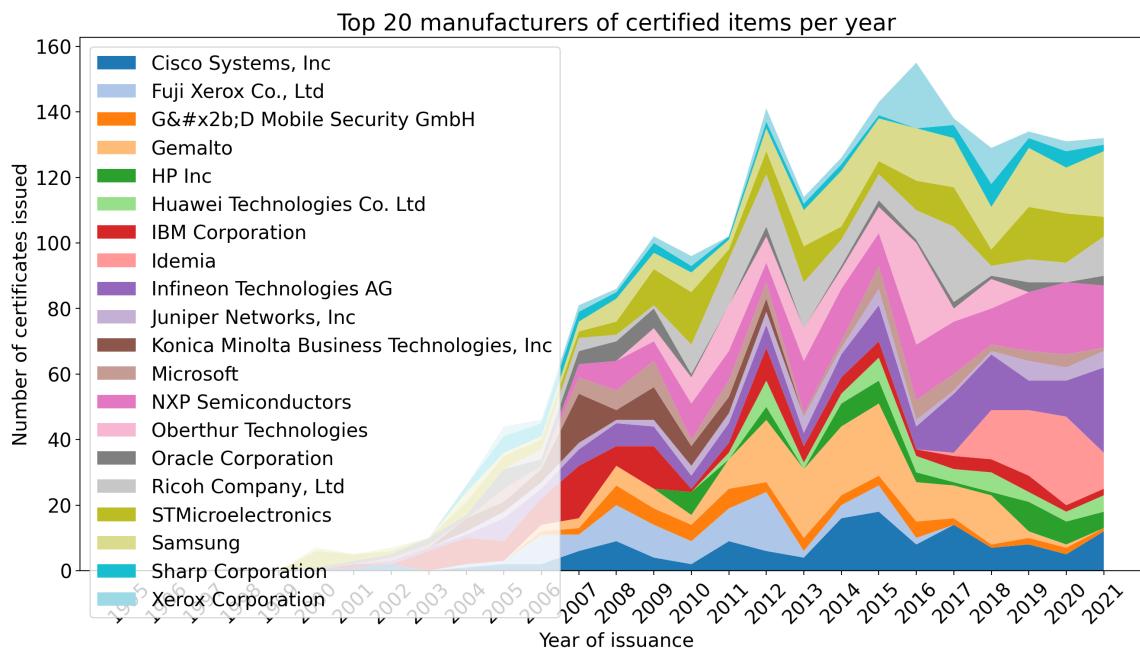
- **Některé dokumenty jsou nedostupné, nebo v chybném formátu.** Při pokusu o přístup k certifikačnímu artefaktu dojde k http chybě 408 (client request timed out) nebo 404 (page not found), případně jsou uvedeny v jiném formátu, než naznačuje přípona dokumentu.
- **Dokument je dostupný pouze jako obrazový scan,** nikoli v textové podobě, případně je šifrovaný. Před analýzou dokumentu je potřeba provést optické rozpoznání textu (OCR), což dále zvyšuje riziko zanesení textové chyby.

## 2.5 Sumář relevantních prací z Masarykovy univerzity

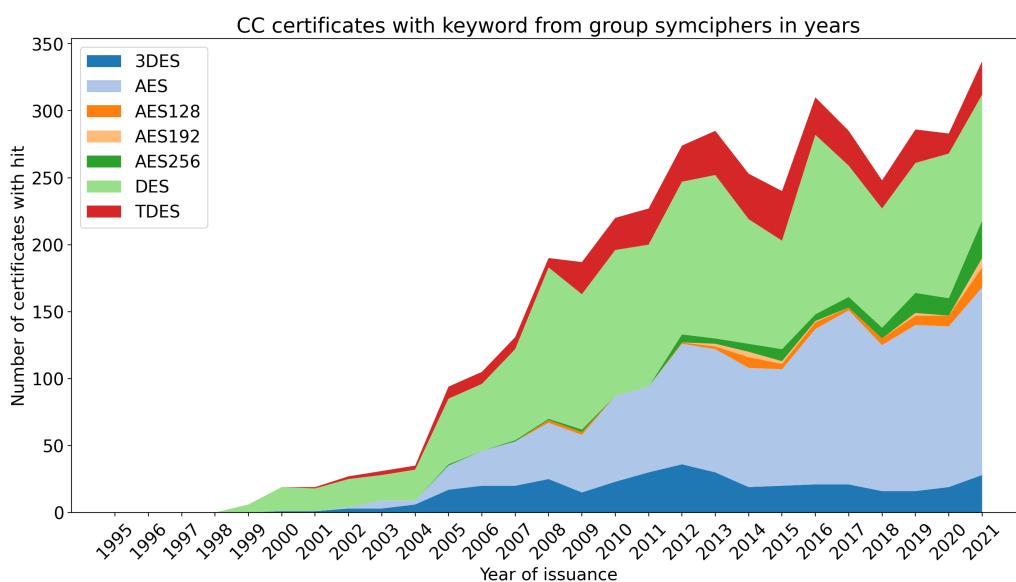
V rámci vývoje nástroje *seccerts* a následně v průběhu řešení tohoto projektu vzniklo několik implementačních a analytických prací, které řeší dílčí problém při zpracování certifikátů. Níže poskytujeme krátké shrnutí jejich obsahu, jejich kompletní text je součástí příloh.

### 2.5.1 “Data analysis of the Common Criteria certificates”, Jiří Michalík

Práce Jiřího Michalíka [7] obhájená v roce 2022 pokrývá rozšíření nástroje o vylepšenou extrakci identifikátorů certifikátů. S využitím extraovaných identifikátorů analyzuje stav certifikačního



Obrázek 8: Ukázka analýzy vývoje počtu počtu certifikátů vydaných nejvýznamějším výrobcům vytvořeným automatizovaně pomocí nástroje *seccerts*.



Obrázek 9: Ukázka analýzy vývoje výskytu klíčových slov odpovídajících algoritmu symetrické kryptografie v certifikovaných produktech v čase vytvořeným automatizovaně pomocí nástroje *seccerts*.



---

ekosystému Common Criteria z hlediska používání referencí. Kromé základních statistik popisujících detekované typy referencí dokládá na rozdílnou kulturu v odkazování na jiné certifikáty v rámci národních schémat, tzv. Certificate Authorizing Schemes (certifikáty vydané francouzským ANSSI často referencují německé BSI certifikáty, ale naopak to neplatí; německé BSI certifikáty často referencují jiné německé certifikáty; certifikáty vydané americkým NIAPem prakticky nereferencují žádný jiný certifikát), poměr certifikací vzhledem k úrovni certifikátu (certifikáty typicky referencují jiné certifikáty na stejně nebo vyšší úrovni). Dále analyzuje výskyt zranitelností u certifikovaných produktů.

### **2.5.2 “Analysis of NIST FIPS 140-2 security certificates”, Stanislav Boboň**

Práce Stanislava Boboně [2] obhájená v roce 2021 navrhuje a implementuje extrakci referencí na moduly a algoritmy v rámci certifikátů vydaných dle NIST FIPS 140-2/3. Věnuje se vyhodnocení úspěšnosti extrakce (díky použití prostého inkrementálního čísla pro moduly i algoritmy je zatížena potenciálně velkou chybovostí). Dále analyzuje celkovou frekvenci referencování v rámci FIPS 140 (je obecně nízká) a identifikuje často používané implementace algoritmů.

### **2.5.3 “Analysis of Common Criteria Protection Profiles”, Martin Friant**

Převažující část v současnosti vydávaných certifikátů produktů je evaluována vzhledem k tzv. ochrannému profilu (Protection Profile, PP). Práce [6] se věnuje problematice automatizované analýzy dokumentace popisující PP a jejich párování s certifikáty produktů. Provádí diskuzi metodiky detekce referencí použitého PP, převodu do kanonického tvaru a extrakci relevantních metadat z dokumentů popisujících PP a implementuje nástroj pro automatizaci těchto kroků. Dále poskytuje vyhodnocení frekvence použití konkrétních PP v čase (často používané vs. velmi málo používané PP) a relevantních dat extrahovaných z dokumentů PP. Identifikuje také komplikace s analýzou dat — především chybějící jednotnou strukturu dokumentů, nejednoznačnou identifikaci použitého PP (speciálně v případě více možných konfigurací u jednoho PP) a nekonzistence mezi údaji poskytovanými prostřednictvím commoncriteriaprofile.org a údaji dostupnými přímo v certifikačních dokumentech.



### 3 Závěr

Veškeré plánované činnosti v rámci Etapy 3 byly úspěšně dokončeny a proběhla prezentace výsledků aplikačnímu garantovi v rámci tří workshopů a školení (duben, červen a červenec 2022).

V rámci této etapy proběhla iniciální analýza artefaktů vytvářených v rámci bezpečnostních schémat Common Criteria a NIST FIPS140-2/3, identifikace problémů a scénářů využití získaných metadat. Tato zpráva shrnuje zjištěné problémy a spolu s přílohami poskytuje základní vhled do certifikačního ekosystému s využitím datové analytiky.

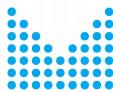
V rámci této zprávy jsme poskytli shrnutí počáteční analýzy možností automatizovaného zpracování certifikačních artefaktů vytvářených během bezpečnostní certifikace produktů v rámci schémat Common Criteria a FIPS140-2/3. Přehled existující literatury a vlastní analýza provedená s pomocí prototypového nástroje *seccerts* [1] identifikovala řadu problémů znesnadňujících automatickou analýzu, jejich použití a interpretaci výsledků. Část problémů lze řešit vhodnou heuristikou, případě s využitím expertních pravidel, v případě ostatních jsou vyžadovány změny v samotném certifikačním procesu. Vznikající doporučení jsou průběžně předávána aplikačnímu garantovi i relevantním výzvám k připomínkám k novým verzím certifikačního procesu, např. odlehčenému certifikačnímu procesu EUCC připravovanému evropskou agenturou ENISA [5]. Další plánované iterace nástroje *seccerts* postupně rozšíří pokrytí začleněním dalších analyzačních technik se zaměřením na oblast kryptografických zařízení a posouzení jejich bezpečnosti dle konzultací s aplikačním garantem projektu.



---

## Reference

- [1] ADAM JANOVSKÝ, Jan Jančák Jiří Michalík Stanislav Boboň Leo Vansimay Martin Friant, Petr Švenda. *sec-certs: Tool for analysis of security certificates (Common Criteria, NIST FIPS140-2/3)*. <https://github.com/crocs-muni/sec-certs>.
- [2] BOBOŇ, Stanislav. *Analysis of NIST FIPS 140-2 security certificates*. bachelor thesis, Masaryk University, 2021. <https://is.muni.cz/auth/th/wftuc/>.
- [3] B.V., TÜV Rheinland Nederland. *JCOP 3 EMV P60 Certification Report*. [https://www.commoncriteriaportal.org/files/epfiles/\[CR\]%20NSCIB-CC-15-67351-CR.pdf](https://www.commoncriteriaportal.org/files/epfiles/[CR]%20NSCIB-CC-15-67351-CR.pdf).
- [4] CRITERIA, Common. *Common Criteria Portal*. <https://www.commoncriteriaportal.org>.
- [5] ENISA. *Cybersecurity Certification: Candidate EUCC Scheme*. 2020. <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>.
- [6] FRIAN, Martin. *Analysis of Common Criteria Protection Profiles*. diploma thesis, Masaryk University, 2020. <https://is.muni.cz/auth/th/hf0kp>.
- [7] MICHALÍK, Jiří. *Data analysis of the Common Criteria certificates*. bachelor thesis, 2022. <https://is.muni.cz/auth/th/sust6/>.
- [8] MU, CRoCS. *seccerts.org web, analysis of security certificates (Common Criteria, NIST FIPS140-2/3)*. <https://seccerts.org>.
- [9] TIERNEY, John and BOSWELL, Tony. Common Criteria: Origins and Overview, pp. 193–216. Cham: Springer International Publishing, 2017. ISBN 978-3-319-50500-8. doi:10.1007/978-3-319-50500-8\_8.  
URL [https://doi.org/10.1007/978-3-319-50500-8\\_8](https://doi.org/10.1007/978-3-319-50500-8_8)



## Příloha: Analýza rizik

Tabulka 1: Analýza rizik relevantních k Etapě 3.

Riziko	Možný dopad rizika	Skutečný dopad rizika	Datum rizika	Opatření pro minimalizaci/eliminaci
Omezení přístupnosti zdrojových certifikačních artefaktů	Bez zdrojových artefaktů není možné provádět jejich automatizovanou analýzu a extrakci	V průběhu řešení etapy nebylo pozorováno zádmerné omezení dostupnosti, pouze krátkodobé výpadky.	-	Nástroj provádějící automatizované stahování zdrojových dokumentů se pokouší stahovat dokumenty automatizovaně každý den a dočasné výpadky jsou tedy opraveny při obnovení dostupnosti dokumentů.
Nemožnost veřejného vyštavení výstupů datových analýz	Nedostupné zpracované výstupy	Nutnost provést zpracování u každého odběratele	-	Nástroj seccerts lze spouštět u každého uživatele samostatně s výstupy pouze pro vlastní potřebu