ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Martin Fritzl

BEZPEČNOSTNÍ ASPEKTY ODBAVOVACÍCH SYSTÉMŮ V DOPRAVĚ

Diplomová práce

2015

Zadání

PROHLÁŠENÍ

Já Martin Fritzl tímto prohlašuji, že jsem předloženou diplomovou práci vypracoval výhradně samostatně. Veškeré použité zdroje, z kterých je čerpáno v této práci, jsou uvedeny v seznamu užité literatury.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změnách některých zákonů (autorský zákon).

V Praze dne 25. 5. 2015 Podpis: …….

PODĚKOVÁNÍ

Chtěl bych vyjádřit díky všem, kteří mi poskytli odborné rady důležité k vypracování tohoto materiálu. Mimořádné poděkování patří především Ing. Marku Kalikovi, Ph.D za odbornou informační podporu a Ing. Radku Holému za vedení mojí práce. V neposlední řadě patří velké poděkování mé rodině a blízkým za morální podporu, které mi bylo dopřáno po celou dobu mého akademického studia.

ABSTRAKT

Název: **Bezpečnostní aspekty odbavovacích systémů v dopravě**

Autor: Bc. Martin Fritzl

Obor: Inženýrská informatika v dopravě a spojích

Druh práce: Diplomová práce

Vedoucí práce: Ing. Radek Holý

Ústav aplikované informatiky v dopravě, K614

Fakulta dopravní, ČVUT v Praze

Rok vydání: Praha 2015

Diplomová práce je zaměřena na problematiku čipových karet v oblastech vyžadující vysoký stupeň zabezpečeného přístupu. Práce podrobně rozebírá systém čipových identifikátorů a bezpečnostní aspekty jeho komunikační struktury. Hlavním cílem této práce je analýza současného stavu karetního přístupového systému na univerzitě ČVUT a návrh nové bezpečnostní nadstavby pro současný systém.

Klíčová slova:

RFID, čipová karta, DESFire, SAM, kryptografie, čtečka karet, šifrování

ABSTRACT

Title: **Security of fare control systems**

Author: Bc. Martin Fritzl

Branch: Informatics in Transportation and Telecommunications

Document type: Master's thesis

Thesis advisor: Ing. Radek Holý

Department of applied informatics in transportation sciences, K614

Faculty of transportation sciences, CTU Prague

Year of release: Prague 2015

Master's thesis is focused on smart card problematics in areas requiring a high level of secure access. Text details a chip identifier system and safety aspects of its communications structure. The main objective of this paper is to analyze the current state of the card access system at the Czech Technical University in Prague and to design new safety upgrades upon the current system.

Key words:

RFID, chip card, smart card, DESFire, SAM, cryptography, card reader, ciphering

SEZNAM POUŽITÝCH ZKRATEK

PICC	Proximity integrated circuit card
PCD	Proximity coupling device
RFID	Radio Frequency identification
SAM	Secure Access Module
HSM	Hardware Security Module
LF	Low frequency
HF	High frequency
UHF	Ultra high frequency
RO	Read Only
WORM	Write Once Read Many
RW	Read Write
DES	Data encryption standard
3DES	Triple DES
3K3DES	Triple key 3DES
AES	Advanced encryption standard
EAL	Evaluation Assurance Level
AID	Application identifier
UID	Unique IDentifier
MAD	Mifare Application Directory
MAC	Message Authentication Code
CMAC	Cipher-based Message Authentication Code
ATR	Answer to reset
RAM	Random-access Memory
EEPROM	Electrically Erasable Programmable Read-only Memory
ROM	Read-only Memory
CRC	Cyclical Redundancy Check

CBC	Cipher Block Chaining
APDU	Application Protocol Data Unit
RSA	Rivest, Shamir, Adleman cipher
SPA	Simple Power Analysis
DPA	Differential Power Analysis
SEMA	Simple Electromagnetic Analysis
DEMA	Differential Electromagnetic Analysis
TZS	Transakční zúčtovací systém
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization

Obsah

SEZNAM POUŽITÝCH ZKRATEK 6
1 ÚVOD 11
2 RFID 12
2.1 Historie 12
2.2 RFID systém 12
2.3 Dělení RFID tagů 13
2.3.1 Dle zdroje napájení 13
2.3.2 Dle frekvence nosné vlny 13
2.3.3 Dle typu paměti 13
2.3.4 Dle použití 14
3 MIFARE DESFire technologie 15
3.1 Technické specifikace Mifare DESFire EV1 15
3.2 Přístup do paměti a její organizace 16
3.2.1 Identifikátor aplikace AID 16
4 Kryptografické algoritmy 18
4.1 Blokové šifry 18
4.1.1 DES 18
4.1.2 3DES 20
4.1.3 AES 20
5 Princip zabezpečení DESFire 23
5.1 Autentizace 23
5.1.1 Relační klíč 25
6 Operace s daty na kartě DESFire 26
6.1 Základní příkazy pro komunikaci a operaci s daty 27
6.1.1 Blokové schéma 28

7 SAM 29
7.1 Obecná charakteristika 29
7.2 Přenos a komunikace 30
7.3 Kryptografie a přenos klíčů 32
7.3.1 Klíče DES a 3DES 32
7.3.2 Klíče AES 33
7.3.3 Klíče MIFARE 33
7.3.4 Zvýšení bezpečnosti – CMAC 34
7.4 Úložiště klíčů 34
7.4.1 Atributy charakterů 35
7.5 Diverzifikace klíčů 37
7.6 SAM Command SET 38
7.6.1 SAM_SelectApplication 38
7.6.2 Příkaz SAM_AuthenticateHost 40
8 Útoky na smart card 43
8.1 Útoky na fyzické úrovni – přímé 43
8.2 Nepřímé útoky 44
8.3 Polopřímé útoky 45
8.4 Útoky postranními kanály 45
8.4.1 Časová analýza 46
8.4.2 Napěťově proudová analýza 46
8.4.3 Elektromagnetická analýza 48
8.4.4 Zanesení chyby 48
9 Návrh technologie 50
9.1 Současný stav 50
9.1.1 Oblast systémového pozadí 50
9.1.2 Oblast PICC 52
9.1.3 Oblast PCD 53
9.2 Standardy FIPS 54

9.2.1 Stupně bezpečnosti 55
9.2.2 Seznam požadavků pro kryptografický modul 56
9.2.3 Management kryptografických klíčů 56
9.2.4 Vazba na univerzitní prostředí ČVUT 57
10 Experimentální realizace DESFire SAM 58
10.1 DESFire SAM – hardware 58
10.2 Místa vhodné implementace technologie SAM 60
10.2.1 Prostory VIC ČVUT 60
10.2.2 Laboratoř sítí a elektronických komunikací na FEL ČVUT 61
10.3 Komunikace SAM s čipovou kartou 62
10.3.1 Blok 1 63
10.3.2 2. Blok 2 63
10.3.3 Blok 3 64
10.4 SAM_AuthenticatePICC 64
10.4.1 Ostatní příkazy SAM Command SET 66
11 Závěr 67
Literatura 69
Seznam obrázků 72
Seznam tabulek 73

1 ÚVOD

Informační technologie jsou trendem dnešní doby, v dopravě toto platí dvojnásob. Dopravní systémy jsou integrovány do stále větších celků a to ruku v ruce nese čím dál zvětšující se nároky na přenos, řízení a především skladování vygenerovaných informací. Historicky se v dopravě přenášely informace v tzv. „papírové“ formě, tedy veškeré dokumenty byly fyzicky vystaveny a cestující nebo jedinec využívající systém je musel mít při sobě. Konec 20. století, ale především začátek 21. století přinesl v tomto odvětví revoluci. Dopravci začaly integrovat do svých odbavovacích systémů technologie čipových karet, které v určitých aplikacích začaly postupně nahrazovat klasické jízdenky.

Technologie čipových karet ovšem přináší i nová rizika. V některých případech jednodušší způsoby odcizení osobních a mnohdy i jiných velmi citlivých informací. V poslední době je tedy kladen velký důraz na zvýšení zabezpečení proti všem možným, dosud popsaným útokům a to vedeným buďto proti samotným čipovým kartám nebo odbavovacím systémům obecně.

Velký důraz byl brán již od poloviny dvacátého století kladen na vývoj a zdokonalování šifer a šifrování komunikace. V této pionýrské době byl veškerý vývoj kryptografických metod určen především pro vládní a vojenské účely. Tento základ dal nicméně podnět k masovému rozšíření kryptografie do dalších oblastí průmyslu a v průběhu let byl postupně implementován i v oblasti čipových karet.

Text je rozdělen do čtyř na sebe navazujících celků. V úvodu je podrobně rozebrána problematika a principy technologie RFID. Na tuto část koncepčně navazuje rozbor technologie Mifare DESFire a popis kryptografických metod, které jsou touto karetní technologií využívány. Hlavním celkem je třetí část. Ta nejdříve teoreticky popisuje modul SAM, včetně konkrétních příkazů, které vystupují v zabezpečené komunikaci. Následně na praktických příkladech demonstruje aktuální možnosti nasazení modulů SAM na ČVUT. V závěru, který je poslední částí této práce, jsou diskutovány zjištěné poznatky a doporučení.

Cílem a hlavním jádrem této práce je návrh nového bezpečnostního řešení, které by bylo možné nasadit v místech univerzitního prostředí ČVUT. Požadavkem je zaručení nadstavbového stupně zabezpečení v extrémně střežených prostorách. Protože žádné rozšířené zabezpečení nebylo dosud na půdě univerzity implementováno, v textu je podrobně popsáno praktické nasazení konkrétního modulu SAM, včetně komunikační struktury a příkazových služeb. Po úspěšném pilotním testování na půdě ČVUT je potom možné tuto technologii rozšířit i do dalších odvětví dopravních aplikací, především tedy v oblasti odbavovacích resp. přístupových systémů.

2 RFID

Technologie RFID, anglicky Radio Frequency identification, je přímým pokračovatelem technologie čárových kódů. Spadá do rodiny identifikátorů, která stejně jako čárové kódy pracuje na bezkontaktní komunikaci na krátkou vzdálenost. Zásadním způsobem se ovšem odlišuje v tom, že není nutná přímá viditelnost identifikovatelného objektu. Masivně se využívá pro bezkontaktní identifikaci např. v logistice, obchodu, autentizace osob atd. Všechny přenášené informace jsou přitom uloženy na čipu, neboli tagu, a jsou vyráběny v provedení pro čtení nebo pro čtení a zápis. Čipy pracují na několika různých frekvencích, které především závisí na regionu, kde jsou užívány. Vlastní komunikace potom probíhá na předávání informace mezi tagem a terminálem. Tag přitom musí být fyzicky upevněn na identifikovaném objektu, např. kontejneru a terminál potom získává potřebné informace přímo z tagu. Základní princip fungování je jednoduchý. RFID vysílač vyšle signál do tagu, který se tím aktivuje.

Rozeznáváme dva základní typy tagů. Pasivní a aktivní RFID tag. Popis obou těchto zařízení je shrnut v kapitole 2.3 – Dělení RFID tagů. [22]

- **Pasivní tag**
- **Aktivní tag**

2.1 Historie

Pionýrské aplikace RFID jsou datovány do období II. světové války. V této době docházelo k nasazování radiolokačních systému, nicméně operátoři mohli zjistit pouze polohu letadla. Nebylo možné získat žádné další informace o letounech. Němci přitom experimentováním zjistili, že při natočení draku letadla o jistý úhel se změní odrážený signál a operátoři tak mohli zjistit, že se jedná o domácí letadlo. Tímto způsobem bylo prvně v praxi užito pasivní RFID. Aktivní RFID bylo následně vyvinuto pod dohledem Roberta A. Watsona – Watta v britském tajném programu IFF. Jednalo se o systém aktivní identifikace, kdy letouny britského letectva byly opatřeny vysílačem. Když vysílač zaznamenal přijetí signálu z domovského radaru, začal okamžitě vysílat zpět signál a hlásil se jako přátelské letadlo. [6]

2.2 RFID systém

Samotný systém je složen ze tří základních zařízení. **Transpondér (tag)** a slouží jako identifikační jednotka. Sestává z RFID čipu a rezonančního obvodu (kondenzátor paralelně s cívkou, která je zároveň anténou). **Terminál (čtečka)**, která je tvořena vysílacím,

přijímacím a vyhodnocovacím obvodem. **Nadřazený systém**, který pracuje s vyhodnocenými daty přenesenými z tagu do terminálu.

2.3 Dělení RFID tagů

RFID tagy je možné dělit dle několika pravidel. Jako základní dělení se uvádí zejména dělení dle zdroje **napájení**, **frekvence nosné vlny**, **typu paměti**, **typu kódování**.[4]

2.3.1 Dle zdroje napájení

Popis obou těchto zařízení je shrnut úvodu této kapitoly, proto ho nem

- **Pasivní RFID tagy –** není nutné napájet žádným externím zdrojem, energii čerpá z RF pole, v kterém se tag nachází a tu následně využívá k vysílání odpovědi do čtečky. Princip čerpání energie je přitom jednoduchý – v oblasti kolem čipu karty je umístěn obvod s cívkou a ten je nabit pomocí elektromagnetické indukce. Pokud se ovšem pasivní tag nenachází v RF poli, je tzv. mrtvý a není schopný komunikace. Pasivní tagy jsou velmi trvanlivé a vyznačují se vysokou životností.
- **Aktivní RFID tagy –** oproti pasivnímu dražší a složitější, protože v sobě integruje jak čip a obvod vysílající informace zpět do čtečky, tak obsahuje vlastní zdroj energie a může tedy po jistou dobu pracovat nezávisle na RF v poli. Aktivní tagy se ovšem v praxi vyskytují v daleko menší míře než pasivní.

2.3.2 Dle frekvence nosné vlny

- **Nízkofrekvenční systémy (LF)** mají dosah řádově desítky centimetrů. Používaná frekvence je pro tuto oblast nastavena jako LF = 125 kHz
- **Vysokofrekvenční systémy (HF a UHF)** mají dosah i několik desítek metrů. Používaná frekvence má hodnota HF = 13,5 MHz. V některých státech se v systémech RFID používá rovněž frekvence s hodnotou UHF = 800 MHz. Tyto frekvence jsou obecně popsány normou ISO 1443 a ISO 15693.

2.3.3 Dle typu paměti

- **Read-Only (RO)** – jsou to tagy, které jsou určeny pouze ke čtení. Paměť je naplněna daty již při výrobě a je dále již nepřepisovatelná, tedy zůstává po celou dobu životnosti tagu neměnná.
- **Write Once Read Many (WORM)** – stejně jako RO tagy jsou určeny pouze pro čtení. Do tagu ovšem nejsou data vložena už při výrobě, ale data jsou na tag zapsána až u prodejce. Dále jsou data opět znovu nepřepsatelná a dále neměnná.

- **Read Write (RW)** – Použitá paměť je typu EEPROM a je snadno adresovatelná a přepisovatelná. Data zapsaná do tagu je možné za pomoci speciální čtečky přepisovat zhruba 1000 cykly.

2.3.4 Dle použití

S masivním rozvojem technologie RFID jsou tagy nasazovány v mnoha odvětvích od potravinářství přes lehký a těžký průmysl až po dopravní aplikace. Při nákupu potravin v hypermarketu se zákazník může setkat s RFID tagy nalepenými na zboží. Na přepravovaných bednách v logistických řetězcích můžeme pozorovat nasazení systémů sledující přepravované zboží, na skládkách lze sledovat množství a druh přiváženého odpadu.

Z tohoto praktického nasazení rozlišujeme tagy ve formě nálepky. Těmito nálepkami opatřené předměty jsou základně chráněné proti odcizení v hypermarketech, kdy při průchodu branou (např. u východu), vyzařující el. mag. pole, dojde k inicializaci tagu systémem a je spuštěn výstražný poplach. Odolnější tagy jsou zapouzdřeny v obalu, obvykle plastovém. Takový tag je možné uschovat uvnitř nebo připevnit vně výrobku. V logistických aplikacích jsou těmito tagy vybaveny přepravované bedny nebo další zboží. V poslední době se jednoduché RFID tagy používají také ve sportovním odvětví, kdy je sportovcům na dres nebo jinou výbavu připevněn pasivní tag a při průběhu kolem čtečky je tento tag aktivován a vyšle informaci o průběhu RF branou.

3 MIFARE DESFire technologie

Karetní technologie MIFARE byla na trh uvedena společností NXP v roce 1992. Nejdříve ve variantě MIFARE Classic, následně MIFARE DESFire. V průběhu let společnost NXP uvedla několik evolučních změn této technologie – následující text se bude výhradně zabývat technologií MIFARE DESFire a to hlavně z důvodu celkově lepšího zabezpečení oproti MIFARE Classic.

Mifare DESFire ve verzi EV1 je bezkontaktní čipová karta vyhovující standardu ISO/IEC 14443A-4, jedná se o typ karet s větší podporou kryptografických a bezpečnostních funkcí než Mifare Classic. Tento text popisuje evoluční variantu EV1, avšak v dnešní době se na trhu vyskytuje již varianta varianty EV2 s dalšími technologickými vylepšeními.

Karta je nabízena ve více variantách, s různou velikostí paměti. Čip používá operační systém "DESFire operating system". Technologie DESFire se vyznačuje vysokým stupněm zabezpečení, který využívá jak starších DES algoritmů, tak především dostatečně bezpečného 3DES nebo AES hardwarového šifrování. Taktéž poskytuje vysoké rychlostí inicializace a čtení a celkově vysokou integritou souborového systému.

Technologie MIFARE DESFire je využívána v mnoha odvětvích dopravních systémů, další možnosti využití jsou především instalace v oblastech docházkových systémů, identifikátorů osob atd. Významné komerční nasazení u nás je v podobě In-Karty Českých drah nebo karetní systém ČVUT pro zaměstnance a studenty univerzity.

3.1 Technické specifikace Mifare DESFire EV1

Čipová karta Mifare DESFire je charakterizována těmito základními vlastnostmi [16]:

Obecné:

- Bezkontaktní přenos dat na základě technologie RFID
- Komunikační frekvence 13,56 MHz
- Několik rychlostí přenosu dat: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s
- 7 - bitový jedinečný identifikátor
- Kompatibilní s ISO/IEC 14443-4

Paměť:

- 2 kB, 4 kB nebo 8 kB
- Retence zapsaných dat je zhruba 10 let
- Možnost zápisu současně až 28 aplikací na jedné kartě

Zabezpečení:

- Certifikační kritéria EAL4+
- Unikátní 7 bytový sériový klíč pro každou kartu
- APDU podléhající standardu ISO/IEC 7816-4
- 1 hlavní klíč, 14 dalších klíčů pro každou aplikaci
- Zabezpečení pomocí DES/AES pomocí 56/112/168 bitového klíče

Jednotlivé varianty DESFire karet jsou shrnuty v tabulce 1:

	MF3IC40	MF3IC21–EV1	MF3IC41-EV1	MF3IC81-EV1
Memory Size	4k	2k	4k	8k
Free Space	4096 bytes	2272 bytes	4832 bytes	7936 bytes
Max. Applications	28	28	28	28
Max. Files per application	16	32	32	32
Crypto	DES, TDES	DES, TDES, 3KTDES, AES	DES, TDES, 3KTDES, AES	DES, TDES, 3KTDES, AES
Support for ISO 7816 Cmds	Very limited	YES	YES	YES

Tab. 1 – specifikace DESFire [16]

3.2 Přístup do paměti a její organizace

DESFire implementuje 8kbyte flexibilní využívání paměti při nahrávání jednotlivých aplikací na kartu. Podporuje až 28 různých aplikací, každá taková aplikace nahraná na kartu potom figuruje jako samostatný subjekt a může do ní být uloženo až 32 různých datových struktur. [16]

3.2.1 Identifikátor aplikace AID

Každé nové aplikaci zaznamenané na kartu je přiřazen jednoznačný unikatní identifikátor AID. Struktura MIFARE DESFire je odlišená od původní Mifare Classic, která má paměť jednoduše rozdělenou jen na bloky a sektory. AID je u MIFARE DESFire přiřazováno dynamicky a hodnoty těcto AIDs mohou nabývat následujících hodnot: 4011h, 4012h a 4013h. Samotný AID identifikátor je tří bytový, struktura přiřazení AID při každém novém vstupu je znázorněna v tabulce 2.

DESFire AID byte 1		DESFire AID byte 2		DESFire AID byte 3	
Nibble 0	Nibble 1	Nibble 2	Nibble 3	Nibble 4	Nibble 5
F	Mifare Classic AID				0 - F

Tab. 2 – AID identifikátor [16]

Jednotlivé hodnoty AIDs 4011h, 4012h a 4013h potom generují 48 samotných DESFire AIDs. Samostatná čísla AIDs jsou potom rozdělena a využívána následovně:

F40110	Service Directry Applications
F40111	CCDA Applications
F40112 - F4012F	Service Applications
F40130 - F4013F	RFU

Tab. 3 – využití AIDs na kartě [16]

4 Kryptografické algoritmy

K celkovému pochopení problematiky v následujících kapitolách je nutné popsat základní problematiku šifrování. Jelikož technologie DESFire využívá převážně šifrování pomocí DES, 3DES a AES, budou rozebrány především tyto šifrovací techniky.

Šifry DES, 3DES a AES spadají do oboru **symetrického šifrování**. Význam tohoto pojmu je takový, že při šifrování a dešifrování informace se používá stejného klíče. Odesílatel a příjemce (v našem případě čtečka a karta) musí tedy být držiteli stejného klíče. Výhodou takového schématu je především to, že takové kryptografické systémy se vyznačují menší početní náročností a jsou tedy rychlejší. Dalším velmi důležitým faktorem je zajištění vysoké informační zabezpečenosti. Teorie symetrického šifrování je charakteristická dvěma typy šifer – proudové šifry a blokové šifry. Protože jak DES a 3DES tak AES spadají do typu blokových šifer, pro naše účely a obsah práce podrobněji popíšeme pouze šifry typu „blokové“. [22]

4.1 Blokové šifry

Blokové šifry pracují na principu zpracování dat po blocích, které jsou předem jasně definované délky. Nejzásadnější vlastností potom je, že všechny bloky jsou šifrované toutéž transformací a všechny zašifrované bloky jsou dešifrované stejnou transformací. Velikost, resp. délka bloků je u každého typu šifrování různá. DES a 3DES pracuje s bloky délky 64 bit, nicméně v současné době je tendence přechodu na bloky větší délky. Tak je tomu např. u AES, kde je délka bloků 128 bitů.

Jako ochrana proti prolomení této šifrovací metody je zaveden do procesu šifrace nový vstup, tzv. operační módy. Ty zaručí, že se jednotlivé bloky na výstupu budou chovat jako náhodný tok a šifrovaný text nebude identický. Pokud by to tak nebylo, útočník by mohl při odchycení dostatečného počtu bloků sestavit jistou podobnost, na základě které by mohl sestavit tajný klíč obou entit (odesílatel, příjemce) a tím celý systém efektivně (za poměrně krátkou dobu) prolomit.

4.1.1 DES

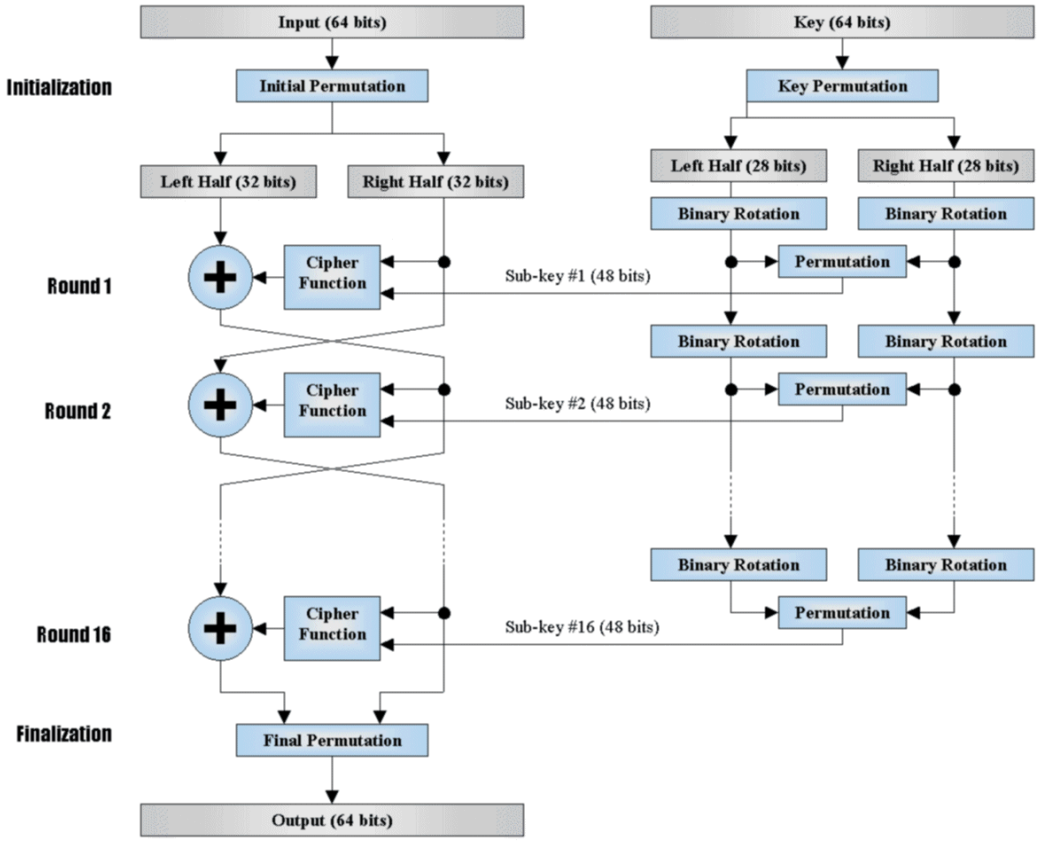
Potom co jsou požadovaná data k zašifrování rozdělena do pevně daných bloků (viz. 3.1), každý blok je rozdělen na dvě stejně velké části (po 32 bitech). Tyto části jsou potom v tzv. „rundách“ kombinovány s šifrovacím klíčem. Samotný šifrovací klíč má délku 56 bit, nicméně je interpretován jako délky 64 bit (každý 8. bit je bit parity). Tento klíč je na počátku, v tzv. inicializační fázi, rozdělen na subklíče (rundovní), ty jsou uloženy v řetězci délky 48 bit.

Algoritmus šifrování

Na samém počátku běhu algoritmu je provedena tzv. „počáteční permutace. Po ní je blok rozdělen na dvě poloviny po 32 bit. Potom každá z 16 rund transformuje tuto polovinu na novou hodnotu. To je zaručeno použitím vždy nového rundovního klíče. Princip běhu algoritmu je zachycen na schématu.

Bezpečnost algoritmu DES

V důsledku rapidního vývoje výpočetní techniky a nárůstu výpočetního výkonu samotných procesorů je nutné konstatovat, že šifrování DES není již v této době bezpečné. V současnosti je možné tuto šifru prolomit hrubou silou a to v „rozumném“ čase. Od 70. let 20. století je teoreticky deklarována prolomitelnost této šifry – teoretický útok hrubou silou byl stanoven na průměrnou dobu úspěšného luštění rámcově na 12 hodin. Stroj, který tuto šifru teoreticky luštil, byl osazen 10^6 čipy. V 90. letech byla tato doba luštění zkrácena na zhruba 3,5 hodiny. V minulosti proběhly i tzv. DES Challenges, které měly za cíl nalézt klíč metodou hrubé síly a ukázat veřejnosti, že šifrování DES neposkytuje vysoké zabezpečení prolomitelnosti. [22]



Obr. 1 – schéma šifrování DES [23]

4.1.2 3DES

Algoritmus byl vyvinut na základě deklarované teoretické (a následně praktické) prolomitelnosti šifry DES. Na rozdíl od klasického DESu k šifrování používá klíč dvojnásobné nebo trojnásobné délky. Díky této skutečnosti je 3DES znatelněji rezistentní proti prolomení. Znatelná nevýhoda 3DES je její výpočetní náročnost a algoritmus je tedy pomalejší než např. novější AES.

Algoritmus šifrování

3DES obecně pracuje s třemi různými klíči DES v módu EDE. Běh algoritmu je potom takový, že pomocí prvního klíče K_1 data zašifrujeme (D), pomocí druhého klíče K_2 dešifrujeme a následně pomocí třetího klíče K_3 zašifrujeme. 3DES potom sestává z klíče trojnásobné délky (192 bit).

Možná je i takzvané šifrování 3DES za pomoci dvou klíčů DES. V takovém případě šifrujeme pomocí K_1, potom dešifrujeme za pomoci K_2 a ve finále opět šifrujeme pomocí klíče K_1. Samotný 3DES klíč má potom délku 112 bit.

Bezpečnost algoritmu 3DES

Délka jednoho šifrovacího klíče (K_n) je v případě 3DES identická jako pro klasický DES – tedy 56 bit. Zvýšený stupeň zabezpečení, v případě 3DES, ovšem zaručuje trojnásobná aplikace klíče tohoto klíče a lze tedy dosáhnout délky klíče až 192 bit, která v současné době, za využití současné počítačové techniky je hrubou silou neprolomitelná.

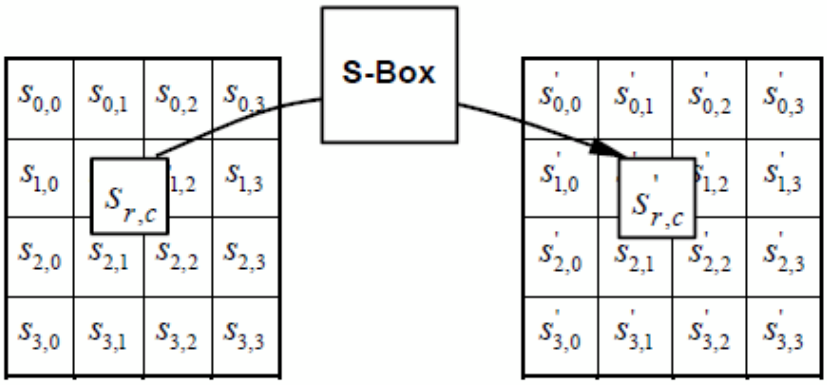
4.1.3 AES

Stejně jako DES a 3DES spadá AES do kategorie symetrického šifrování a blokových šifer. Využívá variabilní délku klíče, která je před samotným šifrováním definována a může být délky 128, 192 nebo 256 bit. Klíč je aplikován na bloky délky 128, 192 nebo 256 bit. Vztah mezi délkou klíče a délkou bloku není definován, klíč je tedy na velikosti bloku nezávislý. [24]

Algoritmus šifrování

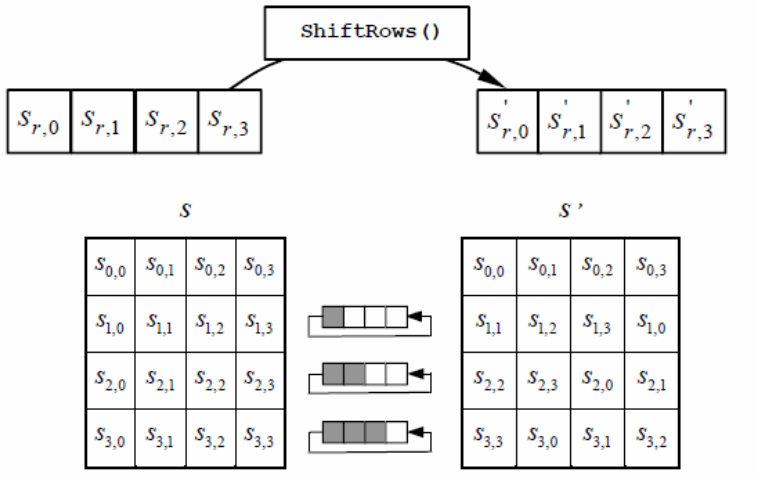
Nejdříve jsou vstupní data rozdělena do předem definovaných bloků, které jsou reprezentovány polem. Tak např. blok o velikosti 128 bit je reprezentován polem 4x4. Potom je šifrovací klíč expandován na rozšířený klíč. Části rozšířeného klíče jsou potom aplikovány pro šifrování bloku v jednotlivých rundách. Determinování počtu rund je závislé na délce klíče a délce bloku. Obvykle bývá v intervalu 10 – 14 rund. Samotná šifrace sestává z kroků, které jsou vždy stejné pro každou rundu až na poslední (FinalRound):

- **ByteSub:** Jednotlivé slabiky (byty) v aktuálním bloku jsou nahrazeny jejich ekvivalenty z nelineární převodní tabulky – tím je zaručena nelineárnost operace.



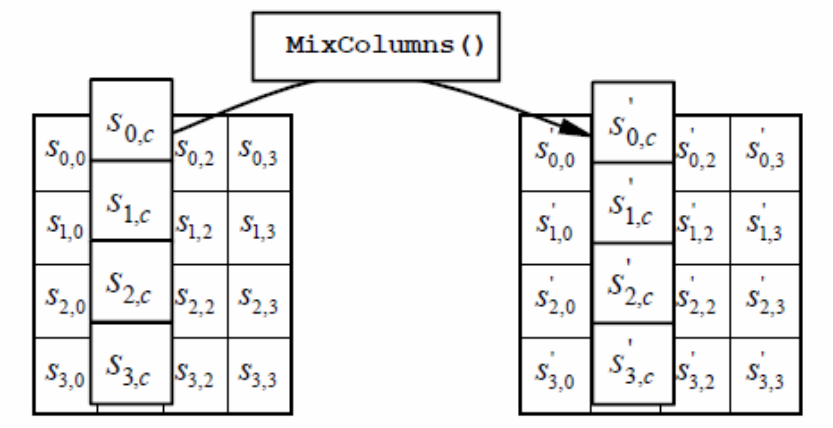
Obr. 2 – princip ByteSub [24]

- **ShiftRow:** Skupiny slabik bloku jsou podrobeny cyklickému posunu. Velikost samotného posunu záleží na velikosti bloku.



Obr. 3 - princip cyklického posunu [24]

- **MixColumn:** Dochází k prohození sloupců a zároveň je každý sloupec (skupina 4 bytů) vynásobena definovanou maticí.



Obr. 4 – princip prohození sloupců [24]

- **AddRoundKey:** Na celý blok je aplikována operace XOR s klíčem (RoundKey) pro aktuální rundu získaného z rozšířeného klíče (ExpandedKey). Tímto získáme požadovanou finální šifru.

Bezpečnost algoritmu AES

Délka klíčů AES a struktura algoritmu zaručuje, že pokud bychom chtěli prolomit AES klíč hrubou silou, při výpočetním výkonu současných počítačů by nám celá operace zabrala několik miliard let. Nicméně v minulosti byly deklarovány metody, jak prolomit dílčí části klíče. Do této doby nebyla zatím popsána žádná metoda, jak úspěšně prolomit kompletní klíč AES.

Počet možných kombinací pro jednotlivé délky klíčů:

- **128 bit:** $2^{128} = 3.4 * 10^{38}$ kombinací
- **192 bit:** $2^{192} = 6.2 * 10^{57}$ kombinací
- **256 bit:** $2^{256} = 1.1 * 10^{77}$ kombinací

5 Princip zabezpečení DESFire

Ještě před samotným zahájením komunikace mezi čtečkou (PCD) a DESFire kartou (PICC) je provedena tří stupňová autentizace a to právě mezi PCD a PICC. Tato autentizace je vykonána bezprostředně potom, co je karta zavedena do el. mag. pole čtečky a je vždy iniciována čtečkou. Součástí autentizace je také nastavení určitého stupně zabezpečení, na kterém je samotná autentizace a přenos dat uskutečňován. Rozlišujeme tyto tři stupně zabezpečení:

1) **Přenos dat bez šifrování**
2) **Přenos dat bez šifrování s MAC**
3) **Šifrovaný přenos dat**

5.1 Autentizace

Před samotným přenosem dat mezi PCD a PICC je vždy provedena tří stupňová autentizace. Jakým způsobem je tato autentizace provedena, záleží vždy na nastavení v jakém módu zabezpečení PCD a PICC pracují. Autentizaci je tedy možné realizovat buď v 56 bit DES, 112 bit DES (triple DES, 2K3DES), 168 bit DES (3 key triple DES, 3K3DES) nebo AES. Po úspěšném procesu autentizace je možné konstatovat, že obojí PCD a PICC jsou držiteli společného tajemství. Ve finále je navázán šifrovaný kanál mezi oběma subjekty procesu. Tabulka podrobně shrnuje celý proces tří stupňové autentizace.

Krok	PCD	Vyměněná data	PICC
1	Čtečka, jakožto iniciátor komunikace začíná proces autentizace. To se děje při vstupu PICC do pole čtečky, která vysílá první příkaz "Autentizuj se". Jako parametr je vysláno číslo klíče do PICC za účelem vybrání jednoho z klíčů uložených v paměti na kartě. Pokud číslo klíče neodpovídá číslu klíče na kartě, PICC odešle chybovou hlášku. Potom záleží právě na vybrané AID, která má předem nastavenou proceduru autentizace a podle ní je následně realizován proces autentizace na předem vybraném stupni zabezpečení.	Číslo klíče ➡	

2		8 nebo 16 bytové $ek_{(keyno)}(RndB)$ ⬅	Jakmile je vybrán klíč, PICC vygeneruje 8 bytové (DES, 2K3DES) nebo 16 bytové (3K3DES/AES) náhodné číslo RndB. Toto číslo je zašifrováno pomocí vybraného klíče, označeno jednoznačným číslem ek(keyno) a odesláno do PCD.
3	PCD zahájí dešifraci obdrženého $ek_{keyNo}(RndB)$ a takto získá původní číslo *RndB*.V dalším kroku je číslo *RndB* zrotováno doleva o 8 bitů (první byte je posunut na konec) a tím se vytvoří *RndB'*. Následně na začátku určeném způsobu autentizace (jednoduché/složité šifrování) PCD vygeneruje náhodné číslo *RndA* . Toto číslo je sloučeno společně s *RndB'* a zašifrováno pomocí vybraného klíče. Takto vytvořený token je odeslán do PICC.	16 nebo 32 bytové ek_{keyNo}(RndA + RndB') ➡	
4		8 nebo 16 bytové $ek_{keyNo}(RndA')$ ⬅	Karta zahájí dešifraci obdrženého tokenu a získá *RndA*+*RndB'*. PICC v tomto okamžiku může porovnat obdržený *RndB'* tím, že původní *RndB* zrotuje také o 8 bitů doleva. Po této úspěšné verifikaci je dokázáno, že čtečka a karta jsou držiteli společného klíče. Pokud je verifikace neúspěšná, karta přeruší proces autentizace a odešle chybovou hlášku. Ve finále karta provede na *RndA* rotaci o 8 bitů doleva a tím vytvoří *RndA'*. Tato hodnota je opět zašifrována, čím vznikne token $ek_{(keyno)}(RndA')$. Ten je odeslán do čtečky.
5	PCD provede dešifraci obdrženého tokenu a tím získá RndA', který porovná s dříve PCD vytvořeným a zrotovaným		

	RndA'. Pokud je verifikace těchto dvou hodnot neúspěšná, PCD ukončí proces autentizace a může zablokovat přístup PICC do systému.		
6			PICC vybere autentizační stupeň pro právě vybranou aplikaci na kartě, podle kterého je vytvořen relační klíč.
7	Pokud během procesu nedošlo k žádné chybě ve verifikaci vyměněných dat mezi PCD a PICC, je vytvořen 8 - 24 bytový klíč pro aktuální relaci. Tento relační klíč je vytvořen kombinací *RndA* a *RndB* a to podle pravidel, která jsou individuální vždy pro dané šifrování.		

Tab. 4 – autentizace mezi PCD a PICC [16]

5.1.1 Relační klíč

Vygenerování relačního klíče je různé pro právě zvolenou kryptografickou operaci. Relační klíč je potom vytvořen dle následujícího vzorce:

DES relační klíč = $RndA_{1.\ polovina} + RndB_{1.\ polovina}$

2K3DES relační klíč = $RndA_{1.\ polovina} + RndB_{1.\ polovina} + RndA_{2.\ polovina} + RndB_{2.\ polovina}$

3K3DES relační klíč = RndA byte 0…3 + RndB byte 0…3 + RndA byte 6…9 + RndB byte 6…9 + RndA byte 12…15 + RndB byte 12…15

AES relační klíč = RndA byte 0…3 + RndB byte 0…3 + RndA byte 12…15 + RndB byte 12…15

6 Operace s daty na kartě DESFire

Data, ze kterých je složena každá aplikace se dále dělí na tyto typy:

- Standardní datové soubory (kódovány jako 0x00)
- Záložní datové soubory (kódovány jako 0x01)
- Záložní datové soubory s určitou hodnotou (kódovány jako 0x02)
- Záložní lineární záznamové soubory (kódovány jako 0x03)
- Záložní cyklické záznamové soubory (kódovány jako 0x04)

Pro přístup k datům zaznamenaným na kartě či pro samotnou komunikaci s kartou technologie MIFARE DESFire využívá čtyř základních typů operací:

- Čtení
- Zápis
- Čtení a zápis
- Změna přístupových práv

Každé z přístupových práv je kódováno 4 bity, což je jeden nibble. Každý nibble potom reprezentuje odkaz k jednomu z klíčů, který je uložen uvnitř aplikace a na nějž přímo odkazuje. Každý nibble dovoluje zakódovat 16 různých hodnot.

Pokud je vybrána hodnota klíče v rozmezí hodnot od 0 do 13 (maximum je 14), potom je indikováno, že taková hodnota odkazuje právě na klíč uložený uvnitř aplikace.

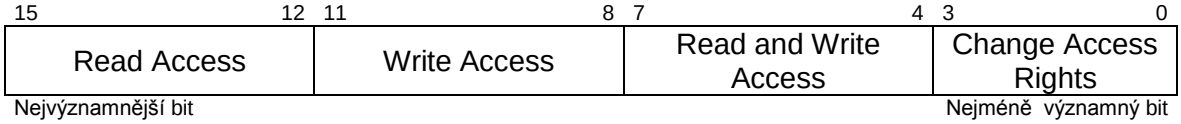
Pokud je hodnota klíče kódována jako 14 (0xE), znamená to volný přístup. To znamená, že přístup je umožněn okamžitě, bez předchozí autentizace, přímo po vybrání požadované aplikace.

Jestliže je hodnota 15, je vyvolán opak hodnoty 14 – tedy zamítnutí přístupu.

Jak již bylo řečeno, pro všechna čtyři přístupová práva jsou vyhrazeny 2 byty pro každou aplikaci. Ty jsou potom dle významnosti dále děleny po 4 bitech následovně.

- Nejvýznamnější 4 bity referují číslo klíče pro práva na čtení (Read Access).
- Další 4 bity odpovídají číslu klíče pro práva na zápis (Write Access).
- Horní nibble pro spodní byte obsahuje informaci pro číslo klíče pro práva na čtení a zápis (Read and Write Access)
- Poslední nibble obsahuje informace o číslu klíče, který je nutný pro autentizaci při změně vlastních přístupových práv k celému souboru a k odkazování přístupových práv na jednotlivá čísla klíčů.

Přístupová práva jsou vždy zabalena do 2 bytů dle tohoto schématu:



Obr. 5 – struktura přístupových práv [16]

Čtení je potom možné pouze při současně garantovaném Read Access a Read and Write Access. Zapisování je potom možné pouze při současně garantovaném Write Access a Read and Write.

Pakliže je k souboru přistupováno bez autentizace, ale volný přístup (0xE) je realizován alespoň jedním přístupovým právem, komunikace je potom nastavena jako nešifrovaná. V případě, že jeden z klíčů Read/Write a Read and Write Access je nastaven jako volný přístup (0xE) a druhý klíč je jiný než 0xE, komunikace je realizována pomocí MAC nebo šifrována. [16]

6.1 Základní příkazy pro komunikaci a operaci s daty

Pro komunikaci mezi PCD a PICC je implementován soubor příkazů, tzv. „command sets“. Existuje jich celá řada, pro potřeby této práce blíže přiblížím ty nejzákladnější, které slouží pro samotnou autentizaci a pro základní operace s daty na kartě.

Každý command má přiřazený svůj vlastní unikátní hexový kód, kterým je volán. Celá operace funguje tak, že čtečka (PCD), vyšle požadovaný command a karta (PICC) na něj odpoví, resp. vykoná požadovanou operaci.

PŘÍKAZY PRO OPERACE AUTENTIZACE

Kód Hex	Příkaz (Command)	Popis
0x0A	Authenticate	Čtečka i karta figurují v tomto procesu jako entity komunikující po šifrované cestě. Vystupují jako subjekty držící stejné „tajemství“, tedy stejný klíč. Tato procedura negarantuje, že obě zařízení mohou provádět vzájemné operace, ale také vytváří relační klíč. Ten garantuje, že kdykoliv v budoucnu bude komunikace realizována právě v rámci této relace a bude šifrována. Relační klíč na konci komunikace mezi PCD a PCII zaniká a při každé nové autentizaci je vytvořen nový.
0x1A	AuthenticateISO	Stejná pravidla jako pro 0x0A
0xAA	AuthenticateAES	Stejná pravidla jako pro 0x0A
0x54	Change KeySettings	Změna hlavního klíče (master key) na kartě a pro jednotlivé aplikace

Tab. 5 – příkazy pro operace autentizace [16]

PŘÍKAZY PRO OPERACE NA ÚROVNI PICC

Kód Hex	Příkaz (Command)	Popis
0xCA	Create Application	Vytvoří novou aplikaci na PICC
0xDA	Delete Application	Permanentně deaktivuje aplikaci na PICC
0x6A	Get Application IDs	Vrátí IDs všech aplikací na PICC
0x6E	Free Memory	Vrátí dostupnou volnou paměť na PICC
0x6D	GetDFNames	Vrátí DF názvy
0x45	Get KeySettings	Získá informace o nastavení PICC master key. Pokud je požadováno, vrátí informaci o maximálním počtu klíčů, které jsou nastaveny pro vybranou aplikaci
0x5A	Select Application	Vybere jednu konkrétní aplikaci, do které je požadován přístup
0xFC	FormatPICC	Vymaže všechny aplikace a zformátuje PICC
0x60	Get Version	Vrátí informace o verzi kartě a další hodnoty z výroby
0x51	GetCardUID	Vrátí UID

Tab. 6 – příkazy pro operace PICC [16]

6.1.1 Blokové schéma

Pro lepší názornost struktury „command sets“ na úrovni jednotlivých bitů a jejich výměny mezi čtečkou a kartou jsou uvedena základní bloková schémata.

7 SAM

Jako bezpečnostní nadstavba DESFIRE se pro komunikaci mezi kartou a terminálem používá modulu SAM (Secure Access Module). Je kompatibilní se smartcards, které podléhají standardu ISO/IEC 7816 třídy A, třídy B a třídy C. Samotný modul SAM je schopný ovládat relevantní terminál, příkazy jsou kódovány dle ISO/IEC 7816-4. [9]

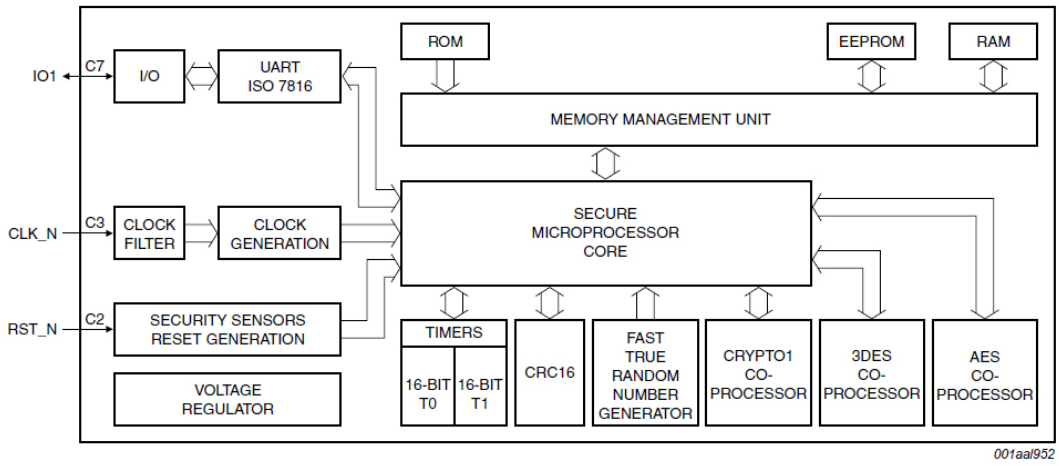
7.1 Obecná charakteristika

SAM module je hardwarový prvek, který dokáže bezpečně uchovávat symetrické a asymetrické klíče. Samotný hardware potom poskytuje ochranu proti útokům postranními kanály. Díky této vlastnosti samotný SAM poskytuje daleko vyšší ochranu zabezpečení než samotné čtečky, v kterých je nainstalován.

DESFire SAM je plně kompatibilní se standardy ISO/IEC třídy A, třídy B a třídy C pro oblast smartcard. Transportní protokol odpovídá standardům ISO/IEC 7816-3. Příkazy instrukcí podléhají standardům ISO/IEC 7816-4.

DESFire SAM mimo klasické funkce bezpečného úložiště klíčů, také nabízí možnost ovládat bezkontaktní čtečky a terminály a to za pomocí nativních příkazů, které jsou definovány dle norem společnosti NXP.

Jako příklad zabezpečení komunikace v praxi je instalování této technologie americkou vládou pro samotné pasy, kdy je využita technologie SAM ve čtečkách na kontrolních stanovištích. Blokové schéma na obr. 7 potom znázorňuje hardwarovou implementaci.



Obr. 6 – blokové schéma SAM [2]

Dle schématu (obr. 6) je názorné, že veškerá komunikace probíhá s modulem „Secure microprocessor core“. Jakékoliv kryptografické operace probíhají stejným způsobem, výměna klíčů potom probíhá právě po zvolené kryptografické větvi.

7.2 Přenos a komunikace

DESFIRE SAM podporuje dva operační módy, v kterých může pracovat, a které jsou rozlišeny podle ATR (Answer To Reset). Prvním je mód, v kterém je vybírán bit rate přenosu a je nastaven podle žádosti PPS. Druhý je specifický mód, který je charakteristický tím, že je nastavena nejvyšší možná rychlost přenosu. Dále jsou rozlišovány dva různé módy ATR – cold reset a warm reset.

Princip komunikace funguje následovně. Po vykonání cold reset karta odpoví na ATR. Po tomto úkonu se nachází v negotiable módu a čeká na další PPS příkazy. Pokud je vykonán warm *reset*, DESFIRE SAM změní operační mód, aplikuje nový mód a vyšle ATR pro warm reset. [22]

Cold a Warm reset

Cold a Warm reset jsou obecné pojmy, které se vztahují obecně k výpočetní technice. Zjednodušeně se rozlišují tak, že Cold reset je vykonán kompletním restartem systému odpojením jednotky od zdroje elektrického proudu a novým bootem. Warm reset je vykonán kompletním restartem a bootem, ovšem při běhu jednotky bez odpojení od elektrického proudu. Proto také v našem systému je možné Warm reset uskutečnit až po prvním Cold resetu.

Answer to reset (ATR)

Následuje bezprostředně po vykonání Cold nebo Warm resetu a podléhá standardům ISO/IEC. Pomocí ATR potom SAM identifikuje, v jakém stavu se karta nachází a nastaví další kroky, na základě kterých je potom uskutečňována samotná komunikace. ATR bývá často užívána jako ukazatel, že je karta v operativním režimu a je jí možné podrobit dalším krokům komunikace se SAMem. Jako příklad je uvedena struktura ATR po cold resetu.

ATR je uskutečňováno v několika krocích:

- Počáteční znak – TS
- Formátovací byte – T0
- Byty rozhraní – TA_i, TB_i, TC_i, TD_i
- Byty historie - T_i
- Kontrolní byty – TCK

Znak	Hodnota	Hodnota	Význam
TS	3Bh	Počáteční znak, nastavení úvodních pravidel	Pořadí bitů
T0	DEh	TA(1), TC(1), TD(1) jsou obsaženy, počet znaků historie je 14	Počet vyvolaných T(i)
TA(1)	18h	F = 372, D = 12	Natavení maximální frekvence (F) a bit rate (D)
TC(1)	FFh	N = 255	Zpoždění mezi jednotlivými byty, které je vyžadováno kartou
TD(1)	81h	TD(2) je vyvoláno, T = 1	První přenosový protokol
TD(2)	F1h	TA(3), TB(3), TC(3), TD(3) je vyvoláno, T = 1	Podporovaný protokol a další globální parametry
TA(3)	FEh	Velikost přijatého bloku kartou = 254	Maximální velikost bloku informace, kterou může karta přijmout
TB(3)	43h	BWT indikátor = 4, CWT indikátor = 3	Maximální zpoždění mezi znaky
TC(3)	00h	Detekování chyby, kód = LRC	Typ použitého kódu při detekci chyby
TD(3)	3Fh	TA a TB jsou vyvolány, T = 15 protokol	Podporovaný protokol včetně globálních parametrů
TA(T = 15)	07h	Zastavení hodin není povoleno	-
TB(T = 15)	83h	Proprietární užití C6	-
Byty historie	44h…58h	ASCII hodnoty DESFIRE SAM	-
TCK	17h	Kontrolní znaky	-

Tab. 7 – struktura ATR [2]

Dle ISO/IEC 7816 – 3 DESFIRE SAM podporuje přenosový protokol T = 1 a to jako jediný možný a žádný jiný není podporován. Protokol T = 1 je na rozdíl od protokolu T = 0 bytově orientovaný. T = 0 je orientovaný blokově.

Application Protocol Data Unit (APDU)

Je popsán v ISO/IEC 7816-4. Pro oblast smartcard je to komunikační protokol, který je používán při komunikaci mezi terminálem a PICC. Dle standardu je rozlišován tzv. Command APDU, což jsou data, které vyšle PCD při první iniciaci s PICC, do PICC. Následně karta (PICC) odešle odpověď „Response APDU“ zpět do terminálu.

Command APDU obsahuje povinnou 4 bytovou hlavičku, která je následována daty o velikosti od 0 do 255 bytů. Response APDU sestává z 2 povinných bytů, které obsahují

informaci o stavu karty a dále obsahuje data o velikosti od 0 do 65 536 bytů. Strukturu obou typů APDU vystihují následující tabulky.

Jméno pole	Popis	Počet bytů
CLA	Třída instrukce – určuje typ příkazu např. obecná, uzavřená atd.	1
INS	Kód instrukce – určuje specifický příkaz např. zapiš data	1
P1 – P2	Parametr příkazu – např. specifikace offsetu pro zápis	2
Lc	Kódování počtu (Nc) bytů příkazových dat, které mají následovat	0,1 nebo 3
Příkazová data	Nc bytů dat	Nc
Le	Kódování maximálního počtu (N_e) bytů odpovědi, která je očekávána	0,1,2 nebo 3

Tab. 8 – příkaz APDU [2]

Jméno pole	Popis	Počet bytů
Data odpovědi	Data odpovědi	Nr ; převážně Ne
SW1 – SW2 response trailer	Status, v jakém se aktuálně nachází příkaz, který odeslala PCD. Např. 90 000 (hexadecimálně) znamená „úspěch“.	2

Tab. 9 – odpověď APDU [2]

7.3 Kryptografie a přenos klíčů

Klíče DES, 3DES a AES se především liší svou strukturou a délkou v bytech. DES, resp. 3DES, se od AES odlišují především svou délkou. Další odlišnosti je možné nalézt ve složení samotných řetězců, do kterých jsou tyto klíče ukládány. Klíče MIFARE jsou oproti předešlým nejjednodušší, avšak jsou ukládány do stejného úložiště jako DES (3DES) nebo AES. [2]

7.3.1 Klíče DES a 3DES

Oboje DES a 3DES klíče, které jsou délky 112 bitů, jsou uloženy v řetězcích po 16 bytech. Klíče typu 3DES délky 168 bitů jsou uchovávány v řetězcích délky 24 bytů. Pro rozlišení DES a 3DES klíčů potom platí následující pravidlo:

- Pokud **je** druhá polovina řetězce, ve kterém je uchován klíč, **rovna** první polovině, PICC a SAM identifikuje tento klič jako typ DES.

- Pokud **není** druhá polovina řetězce, ve kterém je uchován klíč, **rovna** první polovině, PICC a SAM identifikuje tento klíč jako typ 3DES.

Toto první rozlišení klíče je nejdůležitější v procesu následné komunikace a zabezpečení. Na základě typu klíče jsou potom provedeny další operace s kartou – autentizace, MACing, šifrování atd. DES a 3DES pracují tzv. v 8 bytovém režimu. Datový tok je tedy vždy rozdělen do kontejnerů právě o délce 8 bytů.

Cipher Block Chaining mode (CBC)

Všechny kryptografické operace jsou uskutečňovány právě v tomto módu. Ten je definován tak, že výsledek předešlé operace je počátečním šifrujícím vektorem (init vector) nadcházející kryptografické operace. CBC je možné využít jak při módu odeslání, tak při módu přijímání.

Init vector je resetován po každém kryptografickém příkazu. Po tomto resetu jsou všechny byty nulové, dle defaultního nastavení.

7.3.2 Klíče AES

AES klíče jsou uchovávány v řetězcích o délce 16 bytů nebo 24 bytů. Opět záleží, jestli je AES klíč délky 128 bitů nebo 192 bitů. Podobně jako u DES a 3DES jsou data rozdělena do kontejnerů, případě AES jsou kontejnery délky 16 bytů. Šifrovaná data jsou následně formátována do následné podoby:

- CRC32 (dle Ethernetových standardů) je přidáno k datům
- Pro jakékoliv AES operace musí být délka dat rovna n*16 bytů, tedy naplněna do bloků po n*16 bytech s 00h (ekvivalent pro bloky v hexadecimální interpretaci)
- Každý z bloků je dešifrován/šifrován v módu CBC
- Délka výsledných dat je tedy vždy n*16 bytů

Na konci procesu při dešifraci je kontrolována CRC a jednotlivé bytové bloky, jestli jsou stále validní a nedošlo při procesu dešifrace/šifrace k jejich poškození.

7.3.3 Klíče MIFARE

Klíče MIFARE jsou ukládány do stejného úložiště jako klíče AES a 3DES. Pro ukládané klíče MIFARE platí tato obecná pravidla:

- MIFARE standardní klíč A je uložen v rozmezí bytů 0 – 5 v 16 bytovém poli kontejneru.
- Číslo klíče MIFARE standardního klíče rozlišení pro MIFARE klíč A je uložen v bytu 6 v 16 bytovém poli kontejneru.

- Verze klíče MIFARE standardního klíče rozlišení pro MIFARE klíč A je uložen v bytu 7 v 16 bytovém poli kontejneru.
- MIFARE standardní klíč B je uložen v rozmezí bytů 8 – 13 v 16 bytovém poli kontejneru.
- Číslo klíče MIFARE standardního klíče rozlišení pro MIFARE klíč B je uložen v bytu 14 v 16 bytovém poli kontejneru.
- Verze klíče MIFARE standardního klíče rozlišení pro MIFARE klíč B je uložen v bytu 15 v 16 bytovém poli kontejneru.

7.3.4 Zvýšení bezpečnosti – CMAC

DESFIRE SAM nabízí možnost odeslat každý příkaz se zvýšeným stupněm zabezpečením a to aplikováním CMAC. Pokud je tato možnost vybrána, SAM vytvoří logický kanál, ve kterém se host autentizuje, nicméně při této autentizaci a při každém budoucím odeslání jakéhokoliv příkazu je nutná CMAC kalkulace. SAM přitom využívá relační klíč tohoto logického kanálu pro výpočet MAC. Je nutné poznamenat, že při využívání CMAC zabezpečení, MAC musí být vypočítán na celém APDU příkazu předtím, než je APDU odesláno do SAMu. MAC nemusí být připojen a odeslán do SAMu, nicméně musí být vypočítán z důvodu vytvoření init vectoru pro další kryptografickou operaci (viz CBC).

SAM samostatně vypočítá MAC kvůli vygenerování vlastního init vectoru. Ten musí být bezpodmínečně stejný. Po tom, co je vykonán požadovaný příkaz, je vygenerován další MAC, pomocí kterého je získán nový init vector. Ten je připojen k odpovědi, kterou vyšle SAM.

Poslední vlastností tohoto módu zabezpečení je blokace některých příkazů, s kterými samotný SAM pracuje. Je to především z důvodu udržení bezpečnostní integrity celého procesu a některé z uvedených příkazů z manuálu pro SAM tuto podmínku nezaručují.

7.4 Úložiště klíčů

Toto je jedna z největších výhod DESFIRE SAM, protože na rozdíl od klasické čtečky tento hardware nabízí dramaticky vyšší bezpečnost uložení klíčů, které jsou v něm uchovávány.

DESFIRE SAM používá k ukládání jednotlivých klíčů tzv. Key Storage Table (KST). Do této tabulky jsou ukládány informace o těchto uložených klíčích, ale KST také nabízí budoucí správu a editaci uložených klíčů.

Kapacita KST je maximálně 128 uložených záznamů. Každý záznam potom umožňuje uložit tři 3DES klíče, dva 3key3DES klíče, tři AES128, dva AES192 nebo šest MIFARE

standardních klíčů současně s jejich atributy. Každý uložený záznam klíče je později identifikován podle jednoznačně definovaného indexu, tzv. KeyNo.

Strukturu jednoho záznamu klíče v KST znázorňuje tabulka:

Forma	Charakter	Popis	Délka [byte]
Unsigned byte	KeyNo	Referenční číslo klíče	-
String	KeyVa	Klíč – verze a	16 (24)
String	KeyVb	Klíč – verze b	16 (24)
String	KeyVc	Klíč – verze c	16 (-)
Unsigned 24-bit	DF_AID	Odpovídající DESFIRE AID	3
Unsigned byte	DF_KeyNo	Odpovídající DESFIRE číslo klíče (vztahující se k jeho AID)	1
Unsigned byte	KeyNoCEK	Referenční číslo klíče nutné pro příkaz změny záznamu klíče v SAMu	1
Unsigned byte	KeyVCEK	Verze klíče odkazující na klíč pro změnu záznamu klíče v SAMu	1
Unsigned byte	RefNoKUC	Počítadlo četnosti užití klíče	1
Bit mask	SET	Konfigurační nastavení záznam klíče	2
Unsigned byte	Va	Verze klíče A	1
Unsigned byte	Vb	Verze klíče B	1
Unsigned byte	Vc	Verze klíče C	1 (-)

Tab. 10 – struktura záznamu klíče v KST [2]

7.4.1 Atributy charakterů

Z tab. je patrná struktura jednotlivých záznamů v KST, není ovšem patrný podrobnější obsah jednotlivých charakterů. Je nutné poznamenat, že tyto vlastnosti jsou stěžejní pro celou teorii hospodářství a nakládání s klíči v DESFIRE SAM.

Referenční číslo klíče (KeyNo)

KeyNo je index záznamu v KST a může nabývat hodnot 00h nebo 7Fh (hexadecimálně). KeyNo 00H je definován jako SAM master key.

Klíč – verze A (KeyVa)

Je zde uložen jednoduchý DES klíč, dvojitý 3DES klíč, 128-bit AES klíč nebo MIFARE standardní set klíčů (klíč A a klíč B). Tyto klíče jsou ukládány do 16-byte pole. Klíče typu trojitý 3DES klíč nebo 192-bit AES jsou ukládány do 24-byte pole.

Pokud je záznam klíče určen pro ukládání klíče typu 24-byte, první polovina tohoto klíče (verze B) je určena pro ukládání dodatečných dat.

Klíč – verze B (KeyVb)

Je zde uložen jednoduchý DES klíč, dvojitý 3DES klíč, 128-bit AES klíč nebo MIFARE standardní set klíčů (klíč A a klíč B). Tyto klíče jsou ukládány do 16-byte pole. Klíče typu trojitý 3DES klíč nebo 192-bit AES jsou ukládány do 24-byte pole.

Pokud je záznam klíče určen pro ukládání klíče typu 24-byte, první polovina tohoto klíče (verze C) je určena pro ukládání dodatečných dat.

Klíč – verze C (KeyVc)

Je zde uložen jednoduchý DES klíč, dvojitý 3DES klíč, 128-bit AES klíč nebo MIFARE standardní set klíčů (klíč A a klíč B). Tyto klíče jsou ukládány do 16-byte pole.

Odpovídající DESFire AID (DF_AID)

Tento 24-bite unsigned integer obsahuje informaci o tom, kterému záznamu klíče odpovídá daný DESFire AID. Pole DF_AID je potom použito příkazem SAM_SelectApplication pro předběžný výběr klíčů k tří krokové autentizaci (viz. DESFire autentizace).

Odpovídající DESFire číslo klíče (DF_KeyNo)

DF_KeyNo je definováno v rozmezí hodnot 00h až 0Dh. DF_KeyNo je použito při vyvolání příkazu SAM_SelectApplication a to z důvodu vytvoření tabulky validních klíčů pro jednotlivé DF_AID.

Referenční číslo klíče nutné pro příkaz změny záznamu klíče v SAMu (KeyNoCEK)

Číslo klíče, které je nutné pro autentizaci při volání příkazu SAM_ChangeKeyEntry.

Verze klíče odkazující na klíč pro změnu záznamu klíče v SAMu (KeyVCEK)

Tato položka obsahuje informaci o verzi klíče v celém záznamu klíče.

Počítadlo četnosti užití klíče (RefNoKUC)

Tato hodnota určuje, kolikrát byl aktuální klíč využit pro autentizaci. Tato hodnota je automaticky zvýšena o jedno při každé další autentizaci. Defaultně je pro všechny

záznamy klíčů v celém DESFire SAM nastavena hodnota FFh. Tato hodnota musí být také nastavena, pokud se pro daný klíč nepoužívá počítadlo četnosti.

Konfigurační nastavení pro záznam klíče (SET)

Jednotlivá nastavení správy klíčů v SAMu. Pro další zaměření této práce není nutné tuto položku dále rozebírat.

Verze klíče A

Obsahuje data s verzí klíče, která je relevantní pro první klíč. (KeyVa)

Verze klíče B

Obsahuje data s verzí klíče, která je relevantní pro druhý klíč. (KeyVb)

Verze klíče C

Obsahuje data s verzí klíče, která je relevantní pro třetí klíč. (KeyVc)

7.5 Diverzifikace klíčů

Diverzifikace klíčů je proces vytvoření jednoho nebo více vedlejších klíčů z hlavního klíče (master key). Následně je každé kartě zaregistrované do systému přiřazen tento unikátní, diverzifikovaný klíč, a pokud by došlo k prolomení tohoto dílčího klíče, nedošlo by k ohrožení integrity celého systému (zabezpečení všech karet v systému), protože z diverzifikovaného klíče nelze sestavit hlavní klíč.

Diverzifikované klíče jsou vygenerovány a přiřazeny každé kartě při personalizačním procesu, tudíž všechny karty v systému získají unikátní klíč. DESFire SAM je proto ideálním prostředkem k diverzifikování klíčů, jelikož hlavní (master) klíč je bezpečně uložen uvnitř jednotky SAM a může být právě použit ke generování diverzifikovaných klíčů.

Vlastní proces diverzifikace je obdobný jak pro klíč 3DES a jeho varianty tak pro klíče AES. Liší se pouze v délce vstupních diverzifikačních dat a v délce vstupního hlavního klíče. Na výstupu procesu je vždy diverzifikovaný klíč odpovídající délce kryptografické metody (3DES, AES).

Např. pro klíč AES délky 192-bit jsou hodnoty vstupu a výstupu následující:

Vstup:

- Diverzifikační data pro vstup – délky 1 až 31 byte
- 24 byte AES 192 bit hlavní (master) klíč

Výstup:

- 24 byte AES 192 bit diverzifikovaný klíč

Algoritmus pro diverzifikaci využívá metody CMAC výpočtu a čtenář ho může nalézt v dokumentaci viz [2].

7.6 SAM Command SET

Stejně jako v případě klasické DESFire karetní technologie, i technologie DESFire SAM umožňuje implementaci souboru příkazů, kterými je možné ovládat komunikaci s kartou. Od klasického DESFire se liší svojí strukturou a proto jsou uvedeny dva charakteristické příkazy.

Teoretický popis Command SETs, tzv. příkazových setů, pro technologie MIFARE DESFire byl uveden v kap. 6. Technologie DESFire SAM umožňuje implementaci souboru příkazů, kterými je možné ovládat komunikaci s kartou. Zásadní odlišností, od klasického DESFire, při samotné komunikaci s kartou MIFARE DESFire, je skutečnost, že autentizační MIFARE klíč musí být uložen uvnitř SAM a je jednoznačně rozlišen vlastním číslem.

Veškerá komunikace směřující z karty do SAM jednotky musí být kompatibilní dle APDU struktury. V tabulkovém popise následujících příkazů je proto vždy uvedena nejdříve struktura příkazu a následně odpovědi na něj a to vždy v bytové struktuře dle APDU. Všechny možné odpovědi na volaný příkaz jsou reprezentované tzv. operačními stavy SW1 a SW2. Tyto stavy mohou nabývat předem definovaných bytových hodnot a jsou plně kompatibilní se standardem ISO/IEC 7816-4.

7.6.1 SAM_SelectApplication

Po úspěšném přečtení bloků karty je vyslán příkaz SAM_SelectApplication. Je to ekvivalentní příkaz jako pro klasický DESFire příkaz SelectApplication a umožňuje vybrat konkrétní aplikaci z karty. Tento příkaz je především důležitý pro následné spuštění autentizačního procesu a pro získání přístupu k vybrané aplikaci a k jejímu následnému použití v komunikaci mezi PICC a SAM. [2]

Potom co je tento příkaz uskutečněn, SAM vygeneruje seznam dostupných klíčů, které odkazují na ID vybrané aplikace. Samotné ID je uloženo v záznamu klíčů pod položkou „DF_AID“.

Princip generování tohoto seznamu je následující:

- SAM vygeneruje seznam dostupných klíčů pro jednotlivá DESFire AID a DESFire čísla klíčů.

- Pro každé číslo klíče může být v tomto seznamu uloženo maximálně 6 verzí klíče. Tzn., že podle struktury úložiště klíčů (KST), mohou být v seznamu uloženy maximálně dva záznamy a to jak pro DESFire AID a DESFire číslo klíče.
- Pokud KST obsahuje více než 6 záznamů verzí klíče, v seznamu bude uvedeno prvních 6 uložených verzí tohoto klíče.

Dle struktury APDU jsou postupně uvedeny všechny kroky komunikace, které se uskuteční v průběhu vykonání příkazu SAM_SelectApplication. Významy výrazů v jednotlivých buňkách jsou vysvětleny v kap. 7.2. Hodnoty bytů, kterých příkaz nabývá, jsou definovány v hexadecimální soustavě.

Příkaz SAM_SelectApplication

CLA	INS	P1	P2	Lc	Data	Le
80h	5Ah	00h	00h	03h	DF_AID	-

Tab. 11 – příkaz SAM_SelectApplication [2]

Význam a hodnoty jednotlivých bytů shrnuje následující tabulka. V případě bytů P1 a P2 je přípustná hodnota, kterou může toto pole nabývat, pouze 00h. Jakákoliv jiná hodnota má za následek chybový výstup.

Byte	Data	Popis
P1	00h	RFU a nastaveno na hodnotu 00h
P2	00h	RFU a nastaveno na hodnotu 00h
L_c	délka dat	03h
Data	DF_AID	DESFire AID

Tab. 12 – přípustné byte hodnoty pro SAM_SelectApplication [2]

Odpověď APDU:

Odpověď dle struktury APDU může nabývat dvou stavových hodnot SW1 a SW2. V našem případě je uvedena pouze odpověď pro úspěšně provedený příkaz. Vypsání všech hodnot, kterých mohou byty SW1 a SW2 nabývat, je pro účely této práce zbytečné.

Data	SW1	SW2	Funkce
-	90h	00h	Operace úspěšně provedena

Tab. 13 – odpověď APDU pro SAM_SelectApplication [2]

7.6.2 Příkaz SAM_AuthenticateHost

Příkaz SAM_AuthenticateHost je obvykle uskutečněn okamžitě po úspěšném vykonání příkazu SAM_SelectApplication. Tento příkaz iniciuje 3-stupňovou autentizaci, která je popsána v kap. 5.1 a je identická s autentizací karty DESFire terminálem. Následkem této autentizace je možné prohlásit, že oboje entity vystupující v autentizačním procesu (SAM a PICC), jsou držitelem stejného tajemství (klíče). Ty mohou být verze DES, 3DES nebo AES a v závislosti na jednom z těchto klíčů (který je dopředu selektován) vygeneruje relační klíč pro další kryptografické operace. [2]

Na základě úspěšného provedení autentizace je vytvořen relační klíč, který je následně využíván při zabezpečené komunikaci mezi SAM a PICC. Zároveň je deklarováno, že SAM a PICC na sobě vzájemně mohou uskutečňovat další příkazy a operace.

Příkaz SAM_AuthenticateHost rovněž umožňuje diversifikování klíčů určených k autentizaci. Diversifikační vstup může být buďto 8 bytový (DES) nebo 16 bytový (AES).

První část příkazu SAM_AuthenticateHost

CLA	INS	P1	P2	Lc	Data	Le
80h	A4h	Auth mode	00h	02h	KeyNo || KeyV	00h
				0Ah	KeyNo || KeyV || DivInp → 3DES	
				12h	KeyNo || KeyV || DivInp → AES	

Tab. 14 – první část SAM_AuthenticateHost [2]

V závislosti na volbě typu klíče (DES, 3DES, AES) a dalších možností jako např. diverzifikace klíčů apod., mohou jednotlivé bytové pole nabývat různé bitové hodnoty. Následující tabulka shrnuje tyto možnosti:

Byte	Data	Popis
P1	Auth mode	bit 0: - “0”: žádná diversifikace klíče - “1”: klíče diversifikovány s 8 nebo 16 byty DivInp
		bit 1: - “0”: není používán logický kanál pro CMAC - “1”: logický kanál pro CMAC je používán
		bit 2: - “0”: generování session klíče z autentizačního procesu - “1”: použij tajný klíč pro šifrování
		bit 3: 3DES klíč: - “0”: diversifikace užitím dvou šifrovacích rund - “1”: diversifikace užitím jedné šifrovací rundy 3key3DES, AES klíč: - “0”: RFU
		bit 4 - 7: - “0”: RFU
P2	00h	RFU
L_c	délka dat	02h; 0Ah; 12h
Data	KeyNo	Referenční číslo klíče z KST
	KeyV	Verze čísla klíče
	DivInp	8 (DES) nebo 16 (AES) bytový vstup pro diversifikaci klíče

Tab. 15 – byte hodnoty pro první část SAM_AuthenticateHost [2]

Odpověď APDU:

Struktura odpovědi APDU je obdobná jako v případě příkazu SAM_SelectApplication. Dle struktury APDU odpověď obsahuje data o provedeném příkazu a zároveň dva stavové byty, které charakterizují stav odpovědi po provedení příkazu.

Data	SW1	SW2	Funkce
ekNo(RndB)	90h	AFh	Úspěšně provedený příkaz, zašifrované náhodné číslo B

Tab. 16 – odpověď APDU pro první část SAM_AuthenticateHost [2]

Druhá část příkazu SAM_AuthenticateHost

Po obdržení informace o úspěšně provedené první části autentizace je okamžitě provedena druhá část autentizace. V tomto kroku již figurují obě náhodná čísla RndA a RndB‘. Tak jako v případě autentizace mezi PCD a PICC v klasickém DESFire je i zde číslo RndB‘ zrotováno o 8 bitů.

CLA	INS	P1	P2	Lc	Data	Le
80h	A4h	00h	00h	10h	ekNo(Rnd A + RndB‘) → 3DES	00h
				20h	ekNo(Rnd A + RndB‘) → 3keyDES, AES	

Tab. 17 – druhá část SAM_AuthenticateHost [2]

Stejně jako v první části, následující tabulka shrnuje významy jednotlivých bytů a jakých hodnot tyto byty nabývají.

Byte	Data	Popis
P1	RFU	00h
P2	RFU	00h
L_c	délka dat	10h, 20h
Data	ekNo(RndA + RndB‘)	Zašifrováno (náhodné číslo A || náhodné číslo B, zrotované o 1 byte)

Tab. 18 – byte hodnoty pro druhou část SAM_AuthenticateHost [2]

Odpověď APDU:

Po obdržení odpovědi o úspěšném vykonání druhé části autentizačního procesu je deklarováno, že příkaz SAM_AuthenticateHost byl proveden korektně, je vytvořen relační klíč, na základě kterého je vytvořena relace a kanál, po kterém je uskutečňována další komunikace. SAM je okamžitě schopen provádět další operace.

Data	SW1	SW2	Funkce
ekNo(RndA‘)	90h	00h	Operace úspěšně provedena (zašifrované náhodné číslo A, zrotováno vlevo o 1 byte

Tab. 19 – odpověď APDU pro druhou část SAM_AuthenticateHost [2]

8 Útoky na smart card

V současné době je popsána a identifikována řada útoků na smart card. Obecně je nutné konstatovat, že žádný systém není dokonalý a při určité znalosti technologie a systému a při dostatku času útočníka není žádný systém stoprocentně bezpečný. Klasifikace útoků je také různá z hlediska typu útoku, kým je útok prováděn atd. [14]

Obecně je dělení následující.

Typy útoků na čipové karty:

- Fyzická úroveň – útok na přímé zařízení (čip, karta, obvod)
- Logická úroveň – útok na kryptografický protokol, pomocí výpočtu
- Sociální úroveň – útok na pracovníky a vývojáře, kteří mají přístup ke kartě buď při výrobě nebo manipulaci s kartou. Spadají sem i lidé z širšího okolí, kteří disponují nějakou inteligencí a know-how fungování interních procesů karty.

Dle časování útoku:

- Při vývoji
- Při výrobě
- Při používání karty

8.1 Útoky na fyzické úrovni – přímé

K útokům tohoto typu je nutné vlastnit poměrně rozsáhlé informace o struktuře čipu, paměti a čtecích senzorech. Taktéž je nutné vlastnit dobře vybavenou laboratoř nebo podobné pracoviště, kde by byla karta podrobena tomuto typu útoku. Čip a karta samotná je při útoku na fyzické úrovni značně poškozena nebo zničena úplně. Útočník především extrahuje čip z úložiště v kartě, současně se využívá reverzního inženýrství. Pro tento útok je také nutné vlastnictví mikroskopu a ostatních měřících zařízení. Při reverzním inženýrství je pozorována struktura čipu na úrovni tranzistorů, kdy jsou zkoumány jednotlivá propojení a struktura uložení tranzistorů. Tyto vědomosti jsou potom použity při dalších útocích. Při použití laserové řezačky lze po detailní analýze elektronovým mikroskopem přerušit nebo naopak vytvořit nové obvodové smyčky a tím změnit strukturu a fungování čipu karty.

Ochrana proti těmto typům útoků je dělena na prvky aktivní a pasivní. Do oblasti pasivní ochrany spadá samotná výroba polovodičů – s ochranou proti fyzickým útokům je již kalkulováno při samotné výrobě. Do oblasti aktivní ochrany spadá aplikace mikro senzorů, které jsou instalovány na čip karty. Při detekování potenciálního útoku tímto senzorem (světelný, tepelný…) dojde k formátování čipu a paměti a tím ke ztrátě dat. Je nutné

konstatovat, že v současné době nejsou fyzické útoky využívány na přímé prolomení ochrany, ale pouze jako doprovodné analýzy pro získání dostatečných vědomostí při vedení útoku k prolomení na jiné úrovni. Je tomu především kvůli tomu, že systémy ochrany a zabezpečení na fyzické úrovni jsou čím dál dokonalejší.

Útok na pasivní úrovni:

- Elektronový mikroskop – sledování struktury čipu, tzn. struktury tranzistorů a obvodů na čipu
- Mikroskopické sondy – jsou osazeny mikro jehlami, které jsou přiloženy na čip a umožňují sledovat průběh signálu
- Spodní rentgenování – mapování tranzistorů zespodu čipu

Útok na aktivní úrovni:

- Suché leptání čipu – je možné docílit oklamání senzorů na čipu – tedy aktivní ochrany
- Laserový nůž – za jeho pomoci je možné přerušit nebo naopak vytvořit nové obvody na úrovni tranzistorů a tím získat přístup k čipu. Při tomto útoku dochází ke změně struktury samotné karty.
- Iontový paprsek – podobný princip jako laserový nůž, avšak útok probíhá v jiném fyzikálním prostředí.

8.2 Nepřímé útoky

V případě nepřímých útoků nedochází k fyzickým změnám struktury karty ani čipu. Narušitel provádí útoky pozorováním okolí karty, tedy jakým způsobem karta komunikuje s okolím (čtečkou atd.), jak se chová v elektromagnetickém poli čtečky a využívá softwarových chyb, které nebyly odladěny ve fázi vývoje. Útočník při takovém ataku nepotřebuje natolik nákladné zařízení, jako v případě útoku fyzického, nicméně potřebuje znát strukturu karty, na kterou útočí. Proto jsou tyto útoky doprovázeny útoky fyzickými nebo alespoň špionáží ve výrobě, která mohou útočníkovi poskytnout náležité informace. Při tomto typu ataku je jeho samotná detekce velmi obtížná a to právě z jeho charakteru vedení.

Dělení nepřímých útoků je různé, v našem případě zvolíme následující:

Softwarové chyby

Útoky jsou vedeny na úrovni zkoumání bezpečnostních děr, tedy již při vývoji softwaru, ale také již během samotného provozu. Útočník se snaží nalézt rozličné typy chyb – ať už na úrovni transportních protokolů, ale také hledá chyby v kryptografických algoritmech. Jak již bylo řečeno v kapitolách o kryptografii, např. na slabý algoritmus DES útočník může

aplikovat ataky hrubou silou. V pokročilých kryptografických algoritmech jsou tyto útoky nicméně prakticky neúspěšné.

Analýza chování

Tento typ útoků je kombinován s útoky fyzickými. Při těchto atacích jsou získávány data o chování čipu karty a dalších veličinách. Obecně se sleduje napětí a hodinový signál čipu. Do tohoto oboru spadá časová analýza, odběrová analýza a chybová analýza. Po náležitém pozorování chování karty dochází k manipulaci s napětím, hodinovým signálem atd.

8.3 Polopřímé útoky

U těchto ataků je bezpodmínečně nutný přístup k čipu, nicméně nedochází k samotnému poškození karty nebo obvodu s čipem. Je to historicky nejnovější typ útoku, který je oproti útoku fyzickému ekonomicky a časově méně náročný, avšak může být minimálně stejně efektivní. Při těchto útocích se využívá různých typů záření (elektromagnetické, laserové, iontové, UV), které zasahují bezpečnostní pojistky paměti karty a vyřadí je z provozu. Útočník potom získá snazší přístup ke struktuře čipu a následné manipulaci s ním.

8.4 Útoky postranními kanály

Útoky tohoto typu jsou charakteristické tím, že jsou založeny na analýze a odchytu informací při běhu čipu, tedy při chodu, kdy zařízení vykonává operace. Útoky postranními kanály potom využívají skutečnosti, že čip je při vykonávání výpočtů a při běhu algoritmu ovlivňován vnějšími vlivy a je možné získat informace o činnosti procesoru měřením a vnějším pozorováním.

Obecně jsou definovány čtyři nejrozšířenější útoky postranními kanály. Každý z nich je jinak nákladný a také náročný na čas. Nicméně je možné konstatovat, že v prvopočátku se útoky věnovaly analýze na výpočetní čas. Toto ovšem není ojedinělá aplikace, postupem času se začaly objevovat nové praktiky, ty jsou popsány v další části této kapitoly.

Postranní kanál je tedy nutné chápat jako nežádoucí únik informací, které jsou emitovány PICC do jejího okolí, tedy např. při komunikaci s čtečkou, ale není to podmínkou. Ve většině případů je reprezentován fyzikální veličinou. Díky těmto pozorováním, které jsou charakteristické přímo pro operace prováděné kartou, může útočník získat přístup k jednotlivým strukturám karty.

Konkrétně budou v následujícím textu popsány tyto nejvíce používané útoky:

- Časová analýza
- Napěťově proudová analýza
- Elektromagnetická analýza
- Zanesení chyby

8.4.1 Časová analýza

Časová analýza je založena na skutečnosti, že při postupném běhu kryptografických procesů je doba výpočtu pro každý kryptografický proces různá. Z této skutečnosti je možné při čerpání informací na výstupu o dobách běhu procesu sestavit tajný klíč, protože doba je na tomto klíči přímo závislá. Samotná analýza zkoumá dobu, která uplynula od zadání příkazu čtečkou a odpovědí PICC. Pomocí časových analýz je možné prolomit RSA šifru.

Moderní karty typu MIFARE DESFire ovšem užívají takové šifrovací algoritmy, kde šifrovací a dešifrovací algoritmus negeneruje stejné časové hodnoty, tedy časová analýza je v tomto případě méně úspěšná či úplně selhává.

8.4.2 Napěťově proudová analýza

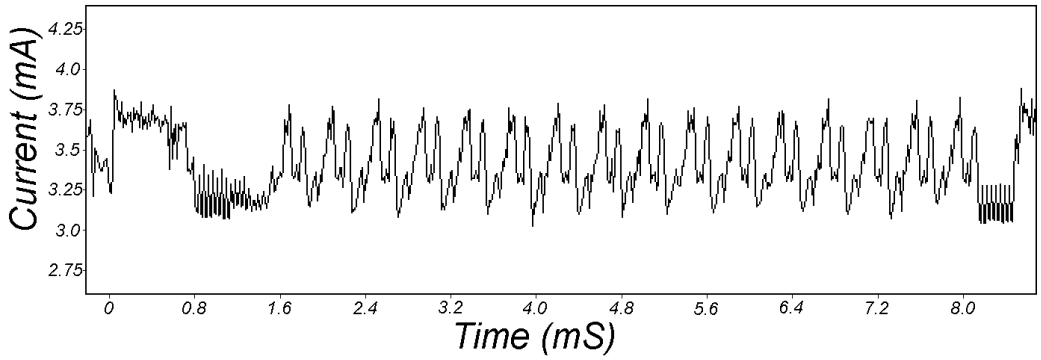
V současnosti je to dobře popsaný útok, který není nikterak náročný na vybavení a realizaci. Využívá skutečnosti, že PICC nemá vlastní zdroj energie – k běhu a vlastnímu napájení využívá energie elektromagnetického pole v okolí čtečky, kterou je nabíjen. Karta samotná tuto energii spotřebovává při vykonávání kryptografických operací. Pokud je na čtečku nainstalováno zařízení, které dokáže detekovat tuto spotřebovanou energii, útočník může získat poměrně věrný obraz celého kryptografického procesu. Pokud je totiž provedena analýza získaných dat spotřebované energie, je možné sestavit posloupnost jednotlivých kryptografických operací. Tento typ útoků je velmi obávaný, protože z jeho charakteru je velmi těžké se proti němu bránit a zjistit ho. Podrobněji je útok pomocí napěťově proudové analýzy dělen na jednoduchou napěťově proudovou analýzu a na diferenciální napěťově proudovou analýzu**.** [12]

Jednoduchá napěťově proudová analýza (SPA)

Jednoduchá napěťově proudová analýza je přímé zjišťování aktuální spotřeby elektrické energie při vykonávání kryptografických operací v průběhu času. Pokud známe kryptografický algoritmus, podle kterého je komunikace šifrována, může útočník sestavit obraz operací na kartě a tím získat potřebné znalosti k prolomení zabezpečení. Tento typ útoku není nijak časově náročný, sběr dat probíhá v řádu vteřin. Pro úspěšné provedení SPA je ovšem nutná expertní analýza zkušeného kryptografa.

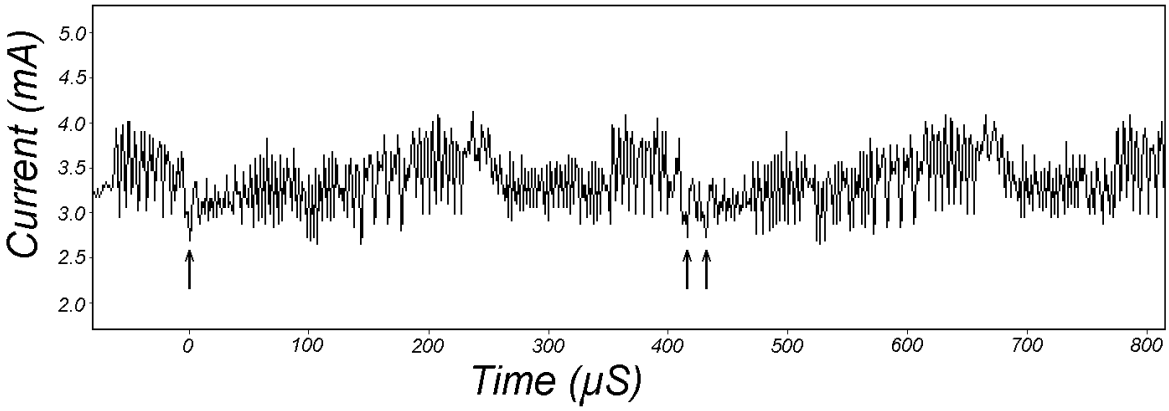
Obzvláště nebezpečná je tato analýza v oblasti blokových šifer. Je totiž možné identifikovat jednotlivé operace permutací a posuvu bytů. Každé takové operaci můžeme totiž přiřadit charakteristický tvar křivky v grafu závislosti odběru proudu na čase. Na obr. je znázorněn tento graf s charakteristickými tvary křivek.

Na obr. 7 je vidět analýza SPA průběhu amplitudy proudu (osa y) v závislosti na čase (osa x). Samotný průběh odpovídá analýze PSA na kompletním šifrování pomocí single DES (16 rund).



Obr. 7 – SPA na kryptografii DES [10]

Na obr. 8 křivka znázorňuje detailní analýzu PSA na druhé a třetí rundě šifrování single DES.



Obr. 8 – SPA na druhé třetí rundě single DES [10]

Diferenciální napěťově proudová analýza (DPA)

Diferenciální napěťově proudová analýza je komplexnější než SPA. Útočník totiž nemusí znát přesnou strukturu systému a k úspěšnému prolomení kryptografického klíče užívá matematického aparátu, resp. statistických analýz. Rozeznávání charakteristických křivek v průběhu je potom možné zautomatizovat. Proces DPA je oproti SPA časově náročnější

(řádově hodiny), protože je nutné shromáždit větší množství vzorků pro statistickou analýzu. Oproti SPA zde ovšem odpadá faktor expertní analýzy kryptografa.

8.4.3 Elektromagnetická analýza

Elektromagnetická analýza zkoumá elektromagnetické pole kolem čipu karty. Toto pole je vytvářeno jako vedlejší produkt na CMOS logice čipu a to tak, že pokud se změní stav z logické 0 na logickou 1 a naopak, je emitován krátký elektrický impulz jako doprovodný jev. Pokud útočník změří tyto elektrické impulzy kolem čipu impulzní sondou, může potom jako v případě SPA nebo DPA analyzovat změny signálu při běhu kryptografických operací. Oproti napěťově proudové analýze tato metoda dosahuje přesnějších výsledků a to díky většímu poměru signálu k šumu. Proto je tato metoda efektivnější vzhledem k času, protože k úspěšnému prolomení tajného klíče postačuje daleko menší čas – není nutný sběr tolika vzorků.

Stejně jako u napěťově proudové analýzy rozlišujeme elektromagnetickou analýzu na jednoduchou (SEMA) a diferenciální (DEMA). Princip sběru dat a jejich vyhodnocení je obdobné. [15]

8.4.4 Zanesení chyby

Tento typ útoků úmyslně zanáší chybu do zařízení vykonávající kryptografické operace. Následná analýza těchto chyb útočníkem může odhalit důležité informace vedoucí k prolomení systémového zabezpečení. Pro zanesení chyby přitom stačí do kryptografického procesu zanést pouze jediný chybový bit.

Útok je obecně dělen na typ, kdy není zařízení při zanesení chyby trvale poškozeno, jen po určitou dobu provádí chybné operace. Druhý typ útoku je takový, že zařízení již není schopné dále vykonávat svou původní funkci a je trvale poškozeno. Samotný útok je dělen na dvě části a to takové, že v první části je provedeno zanesení chyby do systému, v druhé části útoku je tato chyba analyzována a útočník se snaží načerpané informace zneužít k prolomení ochrany (např. tajného klíče). [3]

Způsoby zanesení chyb jsou rozličného charakteru, nejtypičtější jsou následující:

- **Chyba při zvýšení napětí –** Pokud se útočníkovi povede manipulovat s vlastním čtecím zařízením (tedy PCD), může také manipulovat s velikostí napětí, kterým je karta buzena. Ta je navržena na hodnoty napětí okolo 5V, při vyšších (nebo nižších) hodnotách ovšem není zaručena její původní funkčnost a může zde docházet k chybám ve výpočtu a k vyřazení vlastní ochrany hardware proti ostatním útokům (viz. začátek této kapitoly). Obecně je tento typ útoku realizován tak, že útočník

provede krátké a intenzivní výkyvy (nahoru nebo dolů) napětí. Ty potom vedou k vložení vlastní chyby do struktury kryptografické operace.

- **Chyba při kolísání frekvence –** Protože je karta buzena externím zdrojem (pole PCD) a pokud získáme přístup k této čtečce, můžeme stejně jako v případě manipulace s napětím, upravovat hodinový signál čipu. Hodnota této frekvence je stejně jako v předešlém případě definována normou a pokud dojde k překročení této prahové hodnoty (ať už v horní nebo spodní mezi), může dojít k nestabilitě v systému a útočník může zavést chybu.
- **Chyba při variaci teplot –** Jelikož má PICC dle standardů přesně definován rozsah teplot, při kterých pracuje správně, je možné docílit zanesení chyby při zvýšení teplot. Stejný princip platí i pro snížení teplot. Pro co nejlepší efekt musí být změna teploty extrémně rychlá.
- **Chyba při ozařování –** Chybu je možné také zanést, pokud PICC ozařujeme α, β nebo rentgenovým zářením. Jistým problémem je v tomto případě pro útočníka fakt, že částice alfa a beta nemají dostatečnou energii na proniknutí ochranným obalem karty. Pro úspěšné zanesení chyby tedy útočník buďto musí odstranit vrchní obal karty nebo může využít rentgenového záření, jehož částice mají dostatečně vysokou energii na to, aby pronikly obalem. Částice, která potom pronikne obalem, může změnit hodnotu jediného bitu v kryptografické operaci, čímž vznikne chyba.
- **Chyba při ozařování kosmickým paprskem –** Uváděna jako poslední a v tuto chvíli spíše laboratorní pokus o narušení ochrany PICC a zavedení chybového bitu do procesu kryptografie. Kosmické záření je druh vysoko-energetického paprsku, nicméně v praxi těžko použitelné, protože paprsek samotný trpí velkou nepřesností útoku a také zařízení generující tento druh paprsku je obtížně dostupné.

9 Návrh technologie

Návrh rozšířeného systémového zabezpečení vychází ze skutečnosti, že univerzitní kartové hospodářství ČVUT je postaveno. Součástí této práce je připravit podklad a samotnou realizaci nasazení SAM na vybraných čtečkách, které již jsou na ČVUT nasazeny v reálném provozu. V prvním běhu dojde k osazení terminálu modulem SAM na předem vytipovaných místech, především to jsou experimentální laboratoře nebo místa s technologiemi, které vyžadují zvýšený stupeň zabezpečení proti neoprávněnému přístupu.

9.1 Současný stav

V univerzitním prostředí je již řadu let nasazen karetní systém, spravující jak studentské, tak zaměstnanecké, popř. ve speciálních případech návštěvnické karty.

V případě studentských karet je nabízeno vydání čipové karty ve formě studentské přístupové karty do systémů ČVUT současně s dodatkem programu ISIC nebo je možné vydat pouze tzv. kartu ČVUT, která neobsahuje prvky a design ISIC. Technologicky jsou tyto karty identické.

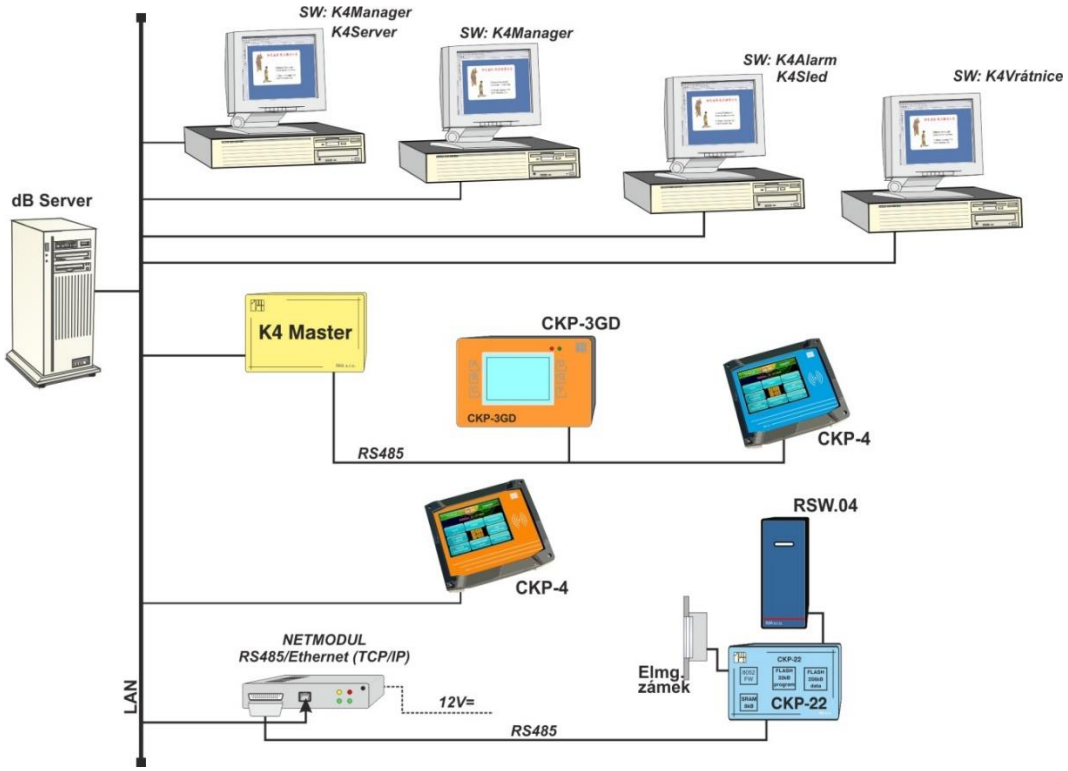
Zaměstnancům ČVUT je vydávána tzv. zaměstnanecká karta, která oproti studentské obsahuje kontaktní čip umožňující se uživateli identifikovat elektronickým podpisem. Ve speciálních případech je možné vydat kartu bez tohoto kontaktního čipu. Zároveň je v hlavním karetním systému implementováno několik subsystémů, které jsou umístěny na serverech VIC ČVUT. Jedná se především o podpůrné informační systémy, ale také je umožněno studentům a zaměstnancům využívat Transakčního zúčtovacího systému (TZS). Uživatel si může nabít kredit na svojí kartu a tím potom platit na místech pro tento typ plateb určených. Dobíjení funguje na principu vložení osobní karty do automatu, kde si uživatel manuálně kredit dobije, nicméně je možné dobíjení převodem přímo na uživatelský účet a stejně tak si uživatel může dobít kredit ve Vydavatelství průkazů ČVUT.

V oblasti hardwarového vybavení jsou místa vyžadující uživatelskou autentizaci vybavena čtečkami karet (viz. 9.1.3) nebo terminály, které mohou být i na vyžádání koncipovány jako docházkové. Tato část je shrnuta v dalším textu.

9.1.1 Oblast systémového pozadí

Protože je čtečku možné v širším pohledu chápat jako pouhou vysílací jednotku, která v sobě nemá implementovánu žádnou výpočetní inteligenci, tento prvek musí být integrován do jednotky, který tyto čtečky obsluhuje. Za tímto prvkem jsou další zařízení, tvořící celý systém, který může servisovat nejenom přístupu uživatelů. Obecně lze jmenovat tyto prvky

tvořící přístupový systém na ČVUT – čtečky karet, terminály, master jednotky a databázový server. Komunikace v síti je realizována technologií ethernet a RS-485 a probíhá v režimu half-duplex. Základní problematiku znázorňuje obr. 9



Obr. 9 – schéma přístupového systému K4

Čtečky karet – rozebrány v další části textu viz kapitola 9.1.3

Terminály – prvek v síti spojující čtečku (PCD) a master jednotkou. Se čtečkou je spojen pomocí linky wiegand, pomocí které získává data, která načte PCD z přiložené karty. Komunikace je tedy realizována pouze jednosměrně, a to ze směru od čtečky do terminálu. Samotný terminál potom na základě načtených dat rozhodne, jestli odemkne el. mag. zámek na dveřích, u kterých uživatel požaduje vstup. Terminál tedy přímo obsluhuje zámky na dveřích a zároveň je napojen přímo do master jednotky.

Master jednotka – Je určen k řízení poloduplexnímu provozu na čtyřech linkách RS485 a je možné ho připojit do datové sítě ethernet. Tím je přímo připojen do DB Serveru. Tato jednotka z DB Serveru čerpá identifikační údaje uživatelů, které dále posílá do terminálu. Master jednotka může pracovat autonomně, ale je ji nutné po určitém časovém intervalu synchronizovat s DB serverem, který spravuje přístupové matriční hodnoty uživatelů. Potom co master jednotka obdrží tyto údaje, uloží je v paměti a využívá je následně pro proces

autentizace, když uživatel přiloží kartu ke čtečce. Master jednotka také odesílá informace zpět do DB databázového serveru. Jsou to záznamy o přístupech do systému, kdy se uživatel autentizuje na čtečce, ale odesílají se taktéž servisní informace, kterých je velké množství. Ve speciálních případech je možné master jednotku provozovat jako autonomní entitu poskytující přístup i několik měsíců (teoreticky roků), avšak takový systém není aktualizovaný právě o nové přístupy a práva uživatelů.

Databázový server – Entita fungující jako hlavní správce v systému, udržující aktuální databázi uživatelů a jejich přístupových práv, kterými se tito uživatelé prokazují při vstupech. DB Server průběžně komunikuje jak se softwarem K4Manager atp., pomocí kterého se ukládají právě uživatelské údaje do systému a také zároveň tyto informace průběžně předává do master jednotky, která je přímo užívá pro poskytnutí nebo zamítnutí přístupu uživatele na čtečce. Databázový server pracuje především na linuxovém jádře.

Jak je z obrázku patrné, čtečka samotná je v tomto systému koncipována jako koncové zařízení se základní inteligencí obsluhující prvotní inicializaci karty a autentizaci. Je ovšem možné realizovat čtečku s pamětí a pokročilou inteligencí, do které je možné ukládat určité množství dat. Cena je ovšem proti klasické čtečce bez paměti řádově vyšší, nasazení takových čteček je tedy spíše specializované.

9.1.2 Oblast PICC

V dřívější době se na univerzitě k identifikaci využívalo karet MIFARE Classic s velikostí 4 byty. Na kartu nebylo možné nahrávat žádné aplikace, pouze se realizovalo jednoduché ověření uživatele na terminálu za použití UID karty.

Tato technologie byla později nahrazena variantou MIFARE DESFire, která oproti Classic nabízí rozšířené možnosti zabezpečení a navíc disponuje větší pamětí. Byla zvolena varianta MIFARE DESFire EV1 8k. Ta je navíc, jako všechny identifikátory z rodiny DESFire, kompatibilní s technologií DESFIRE SAM (viz kap. 7). Karta primárně slouží jako identifikační prostředek pro vstup do výukových prostor školy. Zaměstnanci a studenti navíc mohou využívat doplňkových aplikací, které jsou defaultně nahrány na kartu při jejím vydání ve Vydavatelství průkazů ČVUT.

Navíc je ještě rozlišena karta studenta a zaměstnance. Karta studenta je vydávána ve verzi ISIC nebo ČVUT, technologická verze obou karet je identická. Karta zaměstnance může navíc být vybavena kontaktním čipem, dotyčná osoba disponující kartou je vybavena osobním certifikátem a PINem, může se tedy prokazovat elektronickým podpisem.

Obr. 10 - zaměstnanecká karta ČVUT s kontaktním čipem [19]

9.1.3 Oblast PCD

V univerzitním prostředí ČVUT jsou prostory vyžadující autentizaci vstupující osoby osazeny čtečkami několika druhů. Čtečka splňuje parametry pro bezkontaktní komunikaci s kartou MIFARE, DESFire a iClass – podléhá standardům ISO 14443A/B a ISO 15693. V některých prostorách jsou rovněž instalovány přístupové terminály. V současné době jsou klasickými čtečkami osazeny prakticky všechny vstupy univerzitních prostor, učeben a dalších servisních zařízení.

Nově mohou být ve vlastní přístupové síti využity tyto jednotky jako samostatné entity, do kterých je možné implementovat modul SAM. Dle podrobné analýzy, nebyla nikde v rámci univerzity, v praxi nasazena čtečka či terminál vybavený modulem SAM.

Obr. 11 - Čtečka karet DESFire

Příklad terminálu, který může být nasazen i ve verzi „docházkový“. Oproti čtečce je tento systém rozšířen o další uživatelské možnosti, výhodou ve struktuře systémové implementace je, že terminál funguje jako autonomní jednotka, která může být připojena přímo do master jednotky. Klasická čtečka tuto možnost nenabízí a musí být napojena do terminálové jednotky.

Obr. 12 – terminál verze ČVUT

9.2 Standardy FIPS

Soubor standardů Federal Information Processing Standards (FIPS) je dokument, který vydává National Institute of Standards and Technology (NIST), což je organizace spravující bezpečnostní standardy ve Spojených státech amerických. Tento soubor pravidel zásadně definuje stupně bezpečnosti, které musí jakékoliv kryptografické zařízení splňovat, aby mohlo být jednoznačně řečeno, že je bezpečné. Všeobecně těmto standardům musí vyhovovat všechny zařízení, které jsou implementovány ve státních institucích celosvětově, ale velmi často se objevují i v soukromé sféře.

Důvodem k vytvoření tohoto souboru pravidel bylo vyvinout všeobecný standard, podle kterého budou navrhována všechna zařízení, která budou operovat nebo vykonávat kryptografické operace. Tato zařízení mohou být jakéhokoliv druhu, tedy od čtečky, terminálu, SAMu nebo daleko sofistikovanějších systémů. FIPS obecně definují požadavky na tato zařízení a to jak v oblasti hardwaru tak softwaru. Tyto standardy nedefinují

požadavky pouze na samotná zařízení, ale také na doplňující oblasti, jakými jsou např. technická dokumentace nebo různé druhy komentářů, které může obsahovat zdrojový kód softwaru takového zařízení. Organizace využívající zařízení podléhající standardům FIPS musí tuto skutečnost jednoznačně deklarovat certifikátem k takovému zařízení, kde je uvedeno jméno zařízení, hardware, software, firmware a/nebo verzi appletu. [5]

9.2.1 Stupně bezpečnosti

Dle požadavků klientů a společností, které vyrábějí kryptografická zařízení, byly navrženy čtyři vrstvy bezpečnosti. Ty pokrývají velkou škálu kritérií a jsou odstupňovány dle aktuálně žádaného zabezpečení pro konkrétní aplikační nasazení. Pro příklad, nižší stupeň zabezpečení budou vyžadovat systémy spravující data běžného denního chodu firmy a logicky vyšší stupeň zabezpečení budou vyžadovat bankovní systémy nebo systémy schraňující matriční data uživatelů.

1. stupeň bezpečnosti

Jedná se o nejnižší možný stupeň zabezpečení. Pro kryptografický modul jsou vyžadovány pouze základní prvky zabezpečení a nejsou vyžadovány žádné fyzické prvky zabezpečení samotného modulu. Implementace alespoň jednoho kryptografického algoritmu je vyžadována pro kryptografické operace. Šifrovací jednotka v osobním počítači je příklad zařízení podléhajícímu 1. stupni zabezpečení.

2. stupeň bezpečnosti

Implementuje fyzické zabezpečení kryptografického modulu. Do systému jsou zavedeny prvky mechanických zámků, plomb nebo dalších bezpečnostních prvků ochraňujících zařízení proti fyzickému přístupu. Tento stupeň bezpečnosti také zavádí základní formu autentizace, kdy kryptografický modul autentizuje uživatele vstupující do systému pomocí předem implementovaného algoritmu. U tohoto stupně bezpečnosti je také zavedena funkce operátora, jako osoby, která má speciální práva na provádění rozšířených operací v systému.

3. stupeň bezpečnosti

Integruje veškeré prvky stupňů 1 a 2, navíc ještě přidává ochranný prvek, kdy při detekci útoku na kryptografický modul je paměť zařízení vynulována.

4. stupeň bezpečnosti

Reprezentuje nejvyšší stupeň zabezpečení. Zařízení podléhající tomuto stupni zabezpečení mají kompletní ochranu proti všem možným útokům na fyzické úrovni. Jakýkoliv útok

na tomto stupni zabezpečení má velmi vysokou pravděpodobnost odhalení. Ostatní parametry jsou stejné jako v předešlých stupních.

Dle kap. 9.2.2 je potom pro každý individuální požadavek, dle stupňů bezpečnosti, definována jasná architektura kryptografického modulu a jaké požadavky musí splňovat.

9.2.2 Seznam požadavků pro kryptografický modul

Standardy FIPS definují 11 hlavních pravidel, které jsou dále škálovány dle jednotlivých stupňů bezpečnosti:

- Specifikace kryptografického modulu
- Porty a interface kryptografického modulu
- Role, služby a autentizace
- Konečný stavový model
- Bezpečnost na fyzické úrovni
- Operační prostředí
- Management kryptografických klíčů
- EMI/EMC
- Vlastní testování
- Dokumentace
- Ochrana proti novým útokům

Pro účely této práce jsou rozebrány především oblasti pravidel vztahující se k zabezpečení a správě kryptografických klíčů.

9.2.3 Management kryptografických klíčů

Bezpečnostní požadavky spadající do této kapitoly shrnují kompletní správu klíče – jeho životní cyklus – od vlastního vygenerování takového klíče až po jeho skartaci. Taktéž definuje jeho strukturu, jakým způsobem je generován a jasně definuje povolené metody vygenerování kryptografického klíče.

Náhodný generátor čísel

Kryptografický modul může být vybaven generátorem náhodných čísel. Pokud modul takový generátor obsahuje, všechna vygenerovaná čísla musí být otestována schváleným testovacím algoritmem, testována jsou na jejich správnost.

Vkládání klíčů

Kryptografické klíče mohou být vloženy do modulu buďto manuálně (např. klávesnice) nebo elektronicky (např. karta DESFire). Klíče mohou také být vloženy automatizovanou

metodou a to např. při strojovém generování. Před jakoukoliv manipulací s klíči (při jejich vkládání nebo extrakci) musí být provedeno jejich zašifrování pomocí předem definovaných šifrujících pravidel.

Vkládání kryptografických klíčů na úrovni 3 nebo 4 potom definuje další rozšiřující pravidla. Z nich jsou důležitá především tato pravidla:

- Kryptografický modul musí umožňovat administrátorovi individuální přístup ke kryptografickým klíčům při jejich vkládání nebo vyjímání. Tento přístup musí být systémově odlišen od běžného přístupu.
- Při rekonstrukci kryptografického klíče musí být třeba nejméně dva komponenty subklíče, z kterých je tento originální klíč zpětně složen.

9.2.4 Vazba na univerzitní prostředí ČVUT

Technologie, která je v současné době nasazena v prostředí univerzity, je plně kompatibilní se standardy FIPS. Bezpečnostní nadstavba karetní technologie DESFire ve formě DESFire SAM nicméně implementuje další bezpečnostní prvky, které původní technologie nemá. Především je to právě v oblasti managementu kryptografických klíčů, kdy zabezpečené ukládání klíčů a jejich uchování poskytuje rozšířené možnosti nasazení této technologie v oblastech, které vyžadují vyšší stupeň ochrany při autentizace uživatelů.

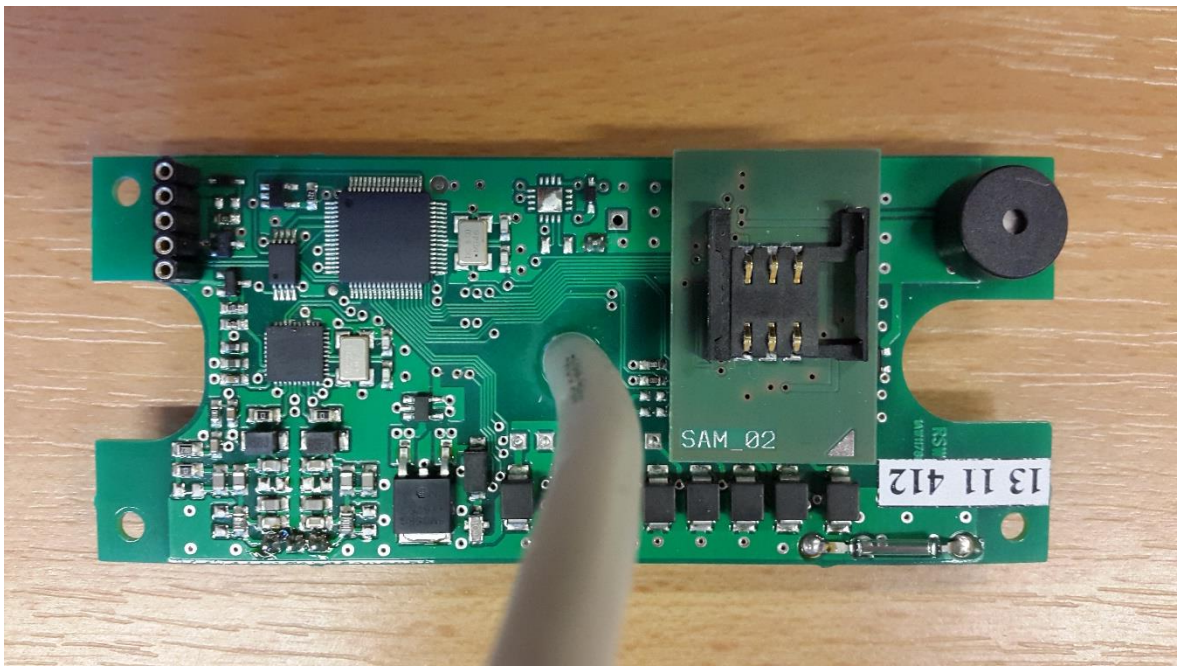
10 Experimentální realizace DESFire SAM

Pro účely pilotního provozu bylo zvoleno experimentální zařízení vyvinuté na půdě společnosti IMA. Z hlediska systémové implementace je plánováno nasazení kompletní SAM čtečky a to v místech, kde je klíčová zvýšená bezpečnost a zaručení náležitého stupně zabezpečení.

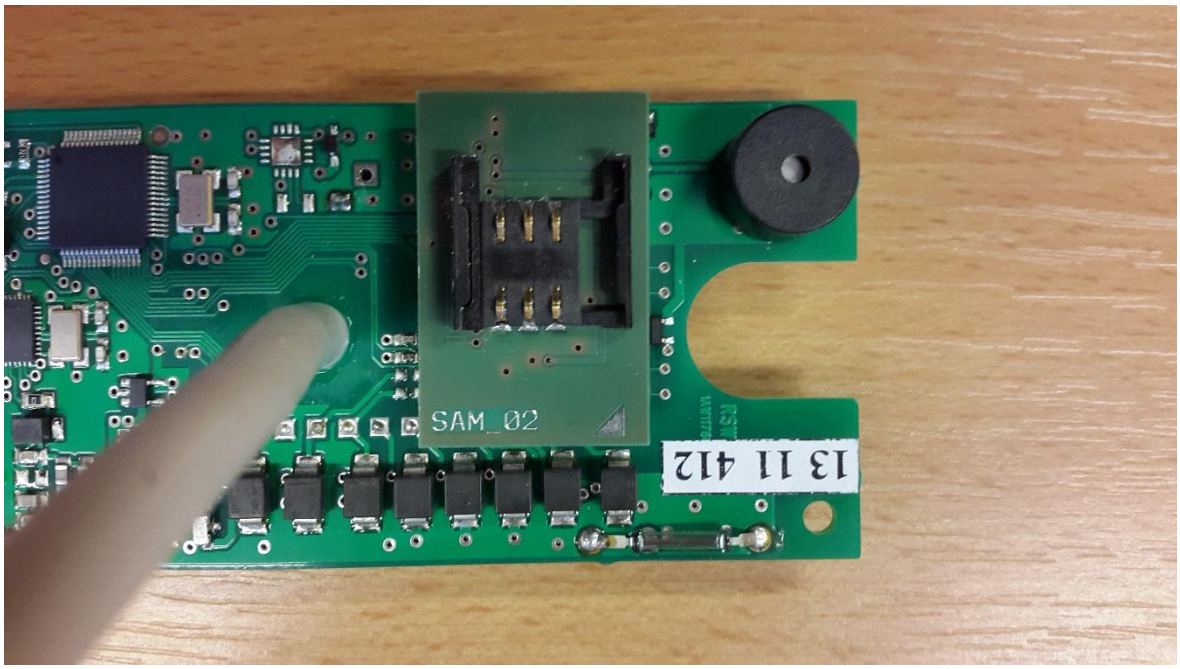
10.1 DESFire SAM – hardware

Jak již bylo řečeno v úvodu této kapitoly, zařízení již existuje v experimentální formě. Samotný hardware je realizován jako čtečka doplněná o modul SAM. Jako další možná realizace, která je v praxi nasazována, je realizace SAMu ve formě integrovaného obvodu. Obr. znázorňuje čtečku společně se SAMem, na obr. je v detailu samotný slot pro SAM modul.

Obecně čtečka karet doplněná o SAM modul musí splňovat standardy ISO 14443 A/B. Čtečka tedy pracuje na definované frekvenci 13.56 MHz a jak je již ze specifikace zřejmé, podporuje karty všech typů z rodiny MIFARE DESFire.



Obr. 13 – čtečka se slotem pro modul SAM



Obr. 14 – slot pro modul SAM

Modul SAM je ve formě čipu dodáván individuálně. Čip je poté oddělen z plastového prefabrikátu a vložen do zařízení při instalaci.

Obr. 15 – modul SAM

10.2 Místa vhodné implementace technologie SAM

V rámci univerzity ČVUT se nachází prostory, které vyžadují nejvyšší stupeň zabezpečeného přístupu. Obecně to jsou místa, kde je nutné garantovat extrémní ochranu proti neoprávněnému přístupu – technologie spravující uživatelské účty, specializovaná pracoviště a laboratoře a místa jako např. síťové uzly, zaručující bezproblémový běh informačních technologií pro celou univerzitu.

Protože jednotka SAM je plně kompatibilní se standardy FIPS a tento vysoký stupeň zabezpečení poskytuje, v pilotním nasazení je počítáno s nasazením na dvou místech:

- VIC ČVUT a to v prostorech, kde jsou instalovány technologie spravující uživatelské účty
- Laboratoř sítí a telekomunikací na FEL ČVUT

10.2.1 Prostory VIC ČVUT

První implementace experimentálního zařízení je předpokládána v prostorách VIC ČVUT, a sice v místech, kde jsou instalovány servery obsluhující uživatelské účty a to v celouniverzitním měřítku. Jedná se tedy o integrální část přístupového systému na všech fakultách a pracovištích ČVUT. Na těchto serverech jsou navíc uloženy všechny matriční údaje jak studentů, tak všech zaměstnanců. Navíc jsou tyto údaje spárovány s číslem karty, kterou uživatel disponuje (ISIC, ČVUT, zaměstnanecká atd.).

Druhá technologie instalovaná v těchto prostorách je jednotka HSM, v které jsou uloženy veškeré přístupové klíče a hlavní (master) klíče ke všem kartám na univerzitě. Pokud by došlo k prolomení ochrany tohoto systému a ke zcizení přístupových klíčů, okamžitě by došlo k rapidnímu snížení bezpečnostní integrity všech čipových karet. Všechny přístupové klíče by totiž bylo možné replikovat z těchto zcizených kryptogramů a útočník by teoreticky získal práva na přístup do jakýchkoliv prostor, kde je autentizace uživatele při vstupu ověřována jen přiložením čipové karty ke čtečce.

Obr. 16 – serverovna VIC ČVUT

Jak je patrné z přiložené fotodokumentace (obr. 17), prostory jsou zabezpečeny bezpečnostní mříží, která splňuje nejvyšší standard zabezpečení. Uživatel bránu otevře přiložením karty ke čtečce umístěné v blízkosti mříže. Vstup do místnosti je navíc osazen další klasickou čtečkou, kde je rovněž vyžadována autentizace uživatele čipovou kartou.

10.2.2 Laboratoř sítí a elektronických komunikací na FEL ČVUT

Druhý příklad praktického nasazení je předpokládán v prostorách Katedry telekomunikační techniky na FEL ČVUT. V laboratoři se nacházejí přístroje značné finanční hodnoty, proto je nutné navýšit bezpečnost proti neoprávněnému přístupu potencionálních útočníků.

Přístup do laboratoře je vybaven pouze bezpečnostním zámkem na dveřích a klasickou DESFire čtečkou. Opět je uvažováno nasazení čtečky vybavené SAM modulem.

Obr. 17 – laboratoř sítí a elektronických komunikací FEL ČVUT

10.3 Komunikace SAM s čipovou kartou

Ve formě pseudo kódu je v této kapitole shrnuta ukázka komunikace mezi kartou, terminálem a modulem SAM.

Samotnou komunikaci PICC a PCD s integrovaným SAM modulem lze v kódu roztřídit do několika pomyslných bloků. Ty lze členit následovně.

- **1. blok**: Zde probíhá samotné navázání komunikace mezi PICC a PCD. Proběhne select vybrané aplikace.
- **2. blok**: Spuštění autentizačního procesu. Na konci tohoto bloku dochází k vytvoření session klíče a vyčtení dat na kartě.
- **3**. **blok**: Odeslání dat na komunikační linku wiegand, mezi čtečkou a terminálem. Na konci bloku dochází k terminování komunikace mezi PICC a PCD.

Důležité je poznamenat, že elektronika čtečky a tedy čtečka samotná figuruje v celém procesu komunikace mezi SAM a PICC pouze jako obyčejný zprostředkovatel komunikace. Inteligence pro autentizaci a ukládání klíčů je přesunuta do modulu SAM.

Příkazy jsou uváděny pomocí pseudo kódu, avšak integrovaný algoritmus ve čtecím zařízení a SAMu je implementován pomocí jazyku C.

10.3.1 Blok 1

První blok slouží jako inicializační a obsahuje pouze jeden příkaz a to k výběru konkrétní aplikace na kartě. Na základě výběru této aplikace jsou nastaveny další autentizační kroky (nastavení šifrování a další).

Vyslání příkazu pro výběr konkrétní aplikace

SEND_SELECTAPP,
RESPONSE_SELECTAPP_WAIT,

10.3.2 2. Blok 2

Po úspěšném vykonání první operace, algoritmus přechází do druhé fáze, kde dochází k autentizaci a v případě úspěšného provedení této operace SAM vytvoří session klíče ze vstupních autentizačních hodnot

Vlastní provedení první části autentizace. Potom co karta vygeneruje náhodné číslo a to odešle do SAMu, čeká se na jeho odpověď. Ta je ve formě vypočteného kryptogramu.

SEND_AUTH_1,
RESPONSE_AUTH_1_WAIT,
SEND_SAM_AUTH_PICC_1,
RESPONSE_SAM_AUTH_PICC_1_WAIT,

Karta vyšle druhou odpověď na autentizaci do SAMu. Na základě těchto dat je vytvořen session klíč, který je v SAMu uložen.

SEND_AUTH_2,
RESPONSE_AUTH_2_WAIT,
SEND_SAM_AUTH_PICC_2,
RESPONSE_SAM_AUTH_PICC_2_WAIT,

Vyslání příkazu na čtení souboru.

SEND_READFILE,

RESPONSE_READFILE_WAIT,

Potom co jsou přečteny data z karty, do SAMu jsou odeslána data s příkazem pro jejích dešifrování. SAM tyto dešifrovaná data odešle zpět.

SEND_SAM_DECRYPT,

RESPONSE_SAM_DECRYPT_WAIT,

10.3.3 Blok 3

V této poslední fázi dochází k odeslání do wiegandu (viz. kap. 9.1.1) a k ukončení komunikace mezi SAMem a kartou. Další komunikace se již neuskutečňuje, pokud by ji uživatel chtěl obnovit, musí projít celý proces od počátku.

Odeslání dat do wiegandu

SEND_TO_WIEGAND,

Dojde k vyslání příkazu pro ukončení

SEND_POWER_DOWN_COMMAND,

RESPONSE_POWER_DOWN_COMMAND,

10.4 SAM_AuthenticatePICC

V kap. 10.3 je naznačena komunikace mezi SAM a PICC, v našem případě kartou DESFire. Pro detailní pochopení této problematiky je v této kapitole rozebrána struktura příkazu **SAM_AuthenticatePICC**, který implementuje autentizační proces mezi SAM jednotkou a PICC.

V případě autentizačního procesu PICC a SAM disponují stejným tajemstvím – stejným tajným klíčem. Stejně jako v případě autentizace klasického DESFire mezi PCD a PICC i zde tento příkaz deklaruje, že zařízení mohou na sobě navzájem provádět následné operace. Pomocí tohoto procesu je také generován session klíč umožňující budoucí komunikaci. [2]

Pro autentizační proces je nutné specifikování čísla klíče, na základě kterého je tato operace uskutečňována. To je možné realizovat pomocí těchto možností:

- Pokud je příkaz SAM_SelectApplication uskutečněn ještě před vlastním SAM_AuthentitacePICC, číslo klíče pro vybranou aplikaci je možné použít jako hodnota tohoto klíče.
- Pokud nebyl dříve užit příkaz SAM_SelectApplication, SAM_AuthentitacePICC vyžaduje vybrání čísla klíče ze záznamu klíčů.

V rámci tohoto příkazu je také možné provést operaci diverzifikování klíčů, kdy diverzifikační vstup může být aplikován pouze na klíče, které aktuálně vstupují do procesu autentizace. Podmínkou pouze je délka diverzifikačního vstupu, který může být definované délky 8 (DES) nebo 16 (AES) byte.

Tabulky 20 a 21 shrnují nejpodstatnější první a druhou část autentizačního procesu, včetně hodnot, které mohou jednotlivé byty nabývat. Obě rovněž odpovídají struktuře APDU.

První část příkazu SAM_AuthenticatePICC

CLA	INS	P1	P2	Lc	Data	Le
80h	A4h	Auth mode	00h	0Ah	KeyNo || KeyV || ekNo(RndB) → DES	00h
				12h	KeyNo || KeyV || ekNo(RndB) → 3keyDES, AES	
				12h	KeyNo || KeyV || ekNo(RndB) || DivInp → 3DES	
				1Ah	KeyNo || KeyV || ekNo(RndB) || DivInp → 3keyDES	
				22h	KeyNo || KeyV || ekNo(RndB) || DivInp → AES	

Tab. 20 – první část příkazu SAM_AuthenticatePICC [2]

Jak je z tabulky 20 patrné, v oblasti datové výměny je naznačeno, kdy do procesu autentizace je možné zavést proces diverzifikování klíčů.

Druhá část příkazu SAM_AuthenticatePICC

CLA	INS	P1	P2	Lc	Data	Le
80h	0Ah	00h	00h	08h	ekNo(RndA') → 3DES	-
				10h	ekNo(RndA') → 3keyDES, AES	

Tab. 21 - druhá část příkazu SAM_AuthenticatePICC [2]

Po uskutečnění druhé části příkazu SAM_AuthenticatePICC dochází k odpovědi ve struktuře APDU, která má obecně několik variant. Právě po APDU odpovědi o úspěšném provedení autentizačního procesu dochází ke generování session klíče.

10.4.1 Ostatní příkazy SAM Command SET

Strukturu dalších příkazů SAM Command SET není pro účely této práce nutné uvádět. Pro čtenáře byl uveden především stěžejní příkaz SAM_AuthenticatePICC, který je jediný relevantní pro vykonání úspěšné první inicializace při kontaktu karty se SAM.

Rozdělení ostatních příkazů lze shrnout do těchto oborů. Škálování je provedeno na základně oboru vykonávané operace [2]:

- SAM konfigurační příkazy
- SAM příkazy pro manipulaci s klíči
- SAM příkazy zabepezpečení
- SAM příkazy pro zpracování dat
- SAM obecné příkazy
- SAM příkazy pro mód spánku
- Příkazy pro ovládání MFRC52X
- Příkazy pro ovládání rádiové frekvence
- Příkazy ISO
- MIFARE příkazy

Tyto sady příkazů mohou být implementovány konkrétním výrobcem SAMu a jejich úplná znění jsou vždy individuální pro konkrétní modul a implementaci v systému.

11 Závěr

Hlavním cílem této práce je analýza a praktický návrh nového bezpečnostního řešení, které je postaveno na současné struktuře karetního přístupového systému, v rámci univerzity ČVUT, a které je následně možné integrovat v dopravních systémech a aplikacích. Z toho důvodu bylo nutné popsat strukturu a možnosti současného řešení a jeho bezpečnostní vlastnosti. Na těchto poznatcích je potom postaven nový návrh.

Z toho důvodu je diplomová práce dělena do jednotlivých celků, které na sebe postupně navazují. Teoreticky jsou zpracovány současné možnosti technologie DESFire a postupně jsou diskutovány obecné vlastnosti a bezpečnostní hranice, kterých toto řešení dosahuje. Prakticky je potom popsáno nové bezpečnostní řešení, které do systému zavádí čtecí jednotku vybavenou modulem SAM.

První část této práce popisuje základní prvky bezkontaktní technologie RFID, teoretickou komunikační strukturu a technické specifikace. Rovněž je v této úvodní části shrnuta problematika RFID tagů, jakožto identifikačních prvků figurujících v dopravních aplikacích.

Druhá část hovoří o technologii Mifare DESFire EV1 a její implementaci v rámci přístupového sytému na univerzitě ČVUT. Nejdříve přibližuje základní vlastnosti, poté popisuje komunikační řešení mezi čtečkou a čipovou kartou. Jedním ze základních pilířů této technologie je obor kryptografie, kterému je věnována samostatná kapitola. V té jsou postupně diskutovány tři základní šifrovací algoritmy – DES, 3DES a AES. U těchto algoritmů je především nutné charakterizovat jejich míru odolnosti proti vnějším útokům ve snaze získat šifrované tajemství. Proto je jako kryptografický algoritmus v celém přístupovém systému na ČVUT implementován algoritmus 3DES. Ten je díky znatelně silnějšímu šifrování, oproti klasickém DES, stále dostatečně bezpečný. Ještě o něco lepších výsledků v tomto ohledu dosahuje šifrovací algoritmus AES, který má odlišnou strukturu šifrování a je v současné době poskytuje největší ochranu proti prolomení.

Z analýz kryptografických algoritmů a zabezpečení modulu SAM, zpracovaných v diplomové práci, plyne doporučení, že i v rámci přístupového systému ČVUT by v budoucnu mělo dojít k nahrazení šifrovacího algoritmu 3DES právě modernějším algoritmem AES.

V z tohoto důvodu jsou v práci také popsány metody prolamování zabezpečení čipových karet a to především poměrně efektivní útoky postranními kanály. Tato forma prolamování zabezpečení čipových karet je v dnešní době zřejmě nejefektivnější metodou, jak může získat útočník neoprávněný přístup do systému.

V třetí části práce je následně rozebrána implementace modulu SAM, který poskytuje rapidně vyšší bezpečnostní nadstavbu v porovnání s klasickým autentizačním procesem

mezi čtecí jednotkou a k ní přiloženou čipovou kartou. Modul SAM dokáže uvnitř své paměťové struktury uchovávat master klíče, na základě kterých jsou uživateli přiřazovány dílčí klíče využívané při autentizacích mezi čtecí jednotkou a kartou. SAM dokáže také pomocí nativních příkazů samostatně ovládat čtecí jednotku a tím komunikovat s přiloženou kartou v elektromagnetickém poli čtečky. Zatím není deklarováno, že autentizační klíče uložené v modulu SAM je možné za pomoci současné techniky zcizit, a tedy systém vybavený tímto zařízením je oproti klasické koncepci znatelně více odolný proti případným snahám o prolomení ochrany.

Ve spolupráci se společností IMA s.r.o. bylo vlastní čtecí zařízení včetně modulu SAM v experimentální podobě poskytnuto k testování. Vzhledem k charakteru zařízení byl úkol zmapovat případné prostory, kde by bylo možné tuto technologii experimentálně testovat a zjistit případné nedostatky před jeho širším nasazením v prostředí univerzity. Takové prostory byly nalezeny a to v rámci VIC ČVUT a laboratoří FEL ČVUT. Důležitým faktorem pro výběr instalace této technologie bylo nalezení prostor, které mají extrémní nároky na zabezpečení proti neoprávněným přístupům. Jsou to především místa, kde jsou instalována strategická zařízení zajišťující bezproblémový běh informačních systémů, výzkumná pracoviště kde jsou instalována zařízení značných finančních hodnot atd. V rámci analýzy byly také zjištěny bezpečnostní hranice samotného modulu SAM a jeho technologické možnosti uchovávání kryptografických klíčů.

Hlavním přínosem této práce je především ověření, že samotná technologie přístupového systému doplněného o modul SAM, zaručuje daleko vyšší integritu zabezpečení než aktuálně instalovaný systém na půdě ČVUT. Potenciál tohoto zařízení je obrovský. Po dalším náležitém testování a odladění je možné tuto technologie bez větších problémů v širokém měřítku instalovat jako nadstavbu současného systému. Jako velké pozitivum je také fakt, že samotná implementace není časově ani finančně náročná. Díky tomu je možné tuto technologii postupně rozšiřovat do všech odvětví dopravy, kde je vyžadována vysoká míra zabezpečení v přístupových, resp. odbavovacích systémech. Obrovský přínos tohoto zařízení tkví také v tom, že je kompatibilní s drtivou většinou současných přístupových systémů. Moduly SAM v nich je tedy možné instalovat za minimální časové, finanční a materiální náročnosti.

Literatura

[1] ALTMAN, T.: *Analýza čipových karet pomocí přípravku Proxmark III*. Praha: FEL ČVUT, 2012. 90 s. Diplomová práce. Vedoucí práce: Ing. Jiří Buček

[2] *DESFire8 SAM-X – Mifare Secure Application Module*. NXP B V., 2008. 126 s.

[3] EGRT, L.: *Útoky zanesením chyby aplikované na čipové karty*. Brno: Fakulta informatiky Masarykova univerzita, 2011. 38 s. Bakalářská práce. Vedoucí práce: RNDr. Jiří Kůr

[4] FINKENZELLER, K., MÜLLER D.: RFID Handbook: *Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. New York: John Wiley & Sons, 2010. 478 s. ISBN: 978-0470695067

[5] *FIPS Publication (všechny části).* 2002.

[6] *Historie RFID* [online]. 2014. Dostupné z: http://www.rfid-epc.cz/co-je-rfid/historie-rfid/

[7] *ISO 14443 – Identification cards – Integrated circuit cards – Proximity cards (všechny části).* 2007.

[8] *ISO 15693 – Identification cards – Integrated circuit cards – Vicinity cards (všechny části).* 2009.

[9] *ISO 7816 – Identification cards – Integrated circuit cards (všechny části).* 2006.

[10] KOCHER P., JAFFE J., JUN B.: *Differential Power Analysis* [online]. 1999. Dostupné z: http://www.cryptography.com/public/pdf/DPA.pdf

[11] KOCHER, P., JAFFE, J., JUN, B, ROHATGI, P..: *Introduction to Differential Power Analysis* [online]. 2011. Dostupné z: http://ftp.cryptography.com/public/pdf/IntroToDPA.pdf

[12] KOCHER, P., JAFFE, J., JUN, B.: *Introduction to Differential Power Analysis and Related Attacks* [online]. 2011. Dostupné z: http://www.cryptography.com/public/pdf/DPATechInfo.pdf

[13] KOPECKÝ M.: *Úvod do kryptologie* [online]. 2012 [cit. 2015-03-15]. Dostupné z: https://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/leto2012/DES_Kopecky.pdf

[14] MATĚJKA, J.: *Útoky postranními kanály na čipové karty*. Brno: FEKT VUT v Brně, 2010. 88 s. Diplomová práce. Vedoucí práce: Ing. Zdeněk Martinásek.

[15] MATTHEWS, A.: *Low cost attacks on smart cards The electromagnetic Side-Channel*. 2006 [cit. 2015-02-06]. Dostupné z: https://www.nccgroup.trust/media/18514/low_cost_attacks_on_smart_cards_the_electromagnetic_side_channel.pdf

[16] *Mifare DESFire EV1, Full Product Data Sheet*. NXP B.V., 2011. 114 s.

[17] *Mifare DESFire, Full Product Specification*. Koninklijke Philips Electronics, 2002. 37 s.

[18] MOLLIN, A., R.: *An Introduction to Cryptography*. New York: Taylor and Francis group, 2006. 413 s. ISBN 978-1584886181.

[19] *Průkaz typu osobní* [online]. Obrázek ve formátu jpeg. Dostupné z: http://intranet.cvut.cz/informace-pro-studenty/prukazy/osobni

[20] *R10 iClass čtečka* [online]. Obrázek ve formátu jpeg. Dostupné z: http://www.hidglobal.com/products/readers/iclass/r10

[21] RANKL, W., COX K.: *Smart Card Application: Design models for using and programming smartcards.* John Wiley & Sons, 2007. 217s. ISBN: 978-0-470-05882-4.

[22] RANKL, W., RANKL, E.: *Smart Card Handbook, 4th edition*. New York: John Wiley & Sons, 2010. 1088 s. ISBN: 978-0-470-74367-6

[23] RUDOLF, D.: *Development and Analysis of Block Ciphers and the DES System* [online]. 2000 [cit. 2015-05-02]. Dostupné z: http://homepage.usask.ca/~dtr467/400/

[24] SIA, A.: *Advanced Encryption Standard* [online]. 2007 [cit. 2015-04-09]. Dostupné z: http://imps.mcmaster.ca/courses/SE-4C03-7/wiki/siaa/se4c03_aes_wiki(7).html

Seznam obrázků

Obr. 1 – schéma šifrování DES 19
Obr. 2 – princip ByteSub 21
Obr. 3 - princip cyklického posunu 21
Obr. 4 – princip prohození sloupců 22
Obr. 5 – struktura přístupových práv 27
Obr. 6 – blokové schéma SAM 29
Obr. 7 – SPA na kryptografii DES 47
Obr. 8 – SPA na druhé třetí rundě single DES 47
Obr. 9 – schéma přístupového systému K4 51
Obr. 10 - zaměstnanecká karta ČVUT s kontaktním čipem 53
Obr. 11 - Čtečka karet DESFire 53
Obr. 12 – terminál verze ČVUT 54
Obr. 13 – čtečka se slotem pro modul SAM 58
Obr. 14 – slot pro modul SAM 59
Obr. 15 – modul SAM 59
Obr. 16 – serverovna VIC ČVUT 61
Obr. 17 – laboratoř sití a elektronických komunikací FEL ČVUT 62

Seznam tabulek

Tab. 1 – specifikace DESFire 16
Tab. 2 – AID identifikátor 17
Tab. 3 – využití AIDs na kartě 17
Tab. 4 – autentizace mezi PCD a PICC 25
Tab. 5 – příkazy pro operace autentizace 27
Tab. 6 – příkazy pro operace PICC 28
Tab. 7 – struktura ATR 31
Tab. 8 – příkaz APDU 32
Tab. 9 – odpověď APDU 32
Tab. 10 – struktura záznamu klíče v KST 35
Tab. 11 – příkaz SAM_SelectApplication 39
Tab. 12 – přípustné byte hodnoty pro SAM_SelectApplication 39
Tab. 13 – odpověď APDU pro SAM_SelectApplication 39
Tab. 14 – první část SAM_AuthenticateHost 40
Tab. 15 – byte hodnoty pro první část SAM_AuthenticateHost 41
Tab. 16 – odpověď APDU pro první část SAM_AuthenticateHost 41
Tab. 17 – druhá část SAM_AuthenticateHost 41
Tab. 18 – byte hodnoty pro druhou část SAM_AuthenticateHost 42
Tab. 19 – odpověď APDU pro druhou část SAM_AuthenticateHost 42
Tab. 20 – první část příkazu SAM_AuthenticatePICC 65
Tab. 21 - druhá část příkazu SAM_AuthenticatePICC 65