Laboratorium Programowania Kart Elektronicznych

Global Platform – Secure Communication

Marek Gosławski

GP – Secure Communication

- Przygotowanie do zajęć
  - otrzymane od prowadzącego karta JavaCard
- Potrzebne wiadomości
  - język angielski w stopniu pozwalającym na czytanie dokumentacji technicznej
  - APDU
  - arytmetyka szesnastkowa
  - kryptografia

GP – Secure Communication

- Oprogramowanie
  - Application Loader
  - EasyReader
  - BP-Tools (EFTLab)
  - SmartCardSuite
    - http://sourceforge.net/projects/smartcardsuite/
    - mile widziane wszelkie informacje o błędach, pomysły

Słowniczek

- **Secure communication**
  - Secure Channel
  - Secure Messaging
- **SCP 01 / SCP 02 / SCP 03**
  - Secure Channel Protocol
- **MAC**
  - Message Authentication Code
    - operacje kryptograficzne zapewniające uwierzytelnienie i integralność

Słowniczek

- **Dywersyfikacja**
  - przekształcenie kryptograficzne pozwalające na otrzymanie z jednej wartości klucza (klucza „matki”) wartości kluczy statycznych/sesyjnych indywidualnych dla karty
  - rodzaje
    - Card Serial
    - tag ’CF’

Słowniczek

- **KMC**
  - DES Master Key, klucz „matka”
- **K_{ENC}, K_{MAC}, K_{DEK}**
  - K-ENC, K-MAC, K-DEK
  - klucze statyczne
- **S_{ENC}, S_{MAC}, S_{DEK}**
  - S-ENC, S-MAC, S-DEK
  - klucze sesyjne

Dokumentacja

- GlobalPlatform Card Specification 2.1.1 [GP211]
  - Card Spec v2.1.1 v0303.pdf
- EMV Card Personalization Specification [EMVCPS11]
  - EMV_CPS_v1.1_20111123125920236.pdf
- EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 Security and Key Management
  - EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

GP – Secure Communication

- Zadania
  - Zadanie 1: host/card challenge & cryptogram
  - Zadanie 2: K-ENC, K-MAC, K-DEC
  - Zadanie 3: S-ENC, S-MAC, S-DEC, MAC
- Przesłanie na adres:
  - marek.goslawski@put.poznan.pl

GP – Secure Communication

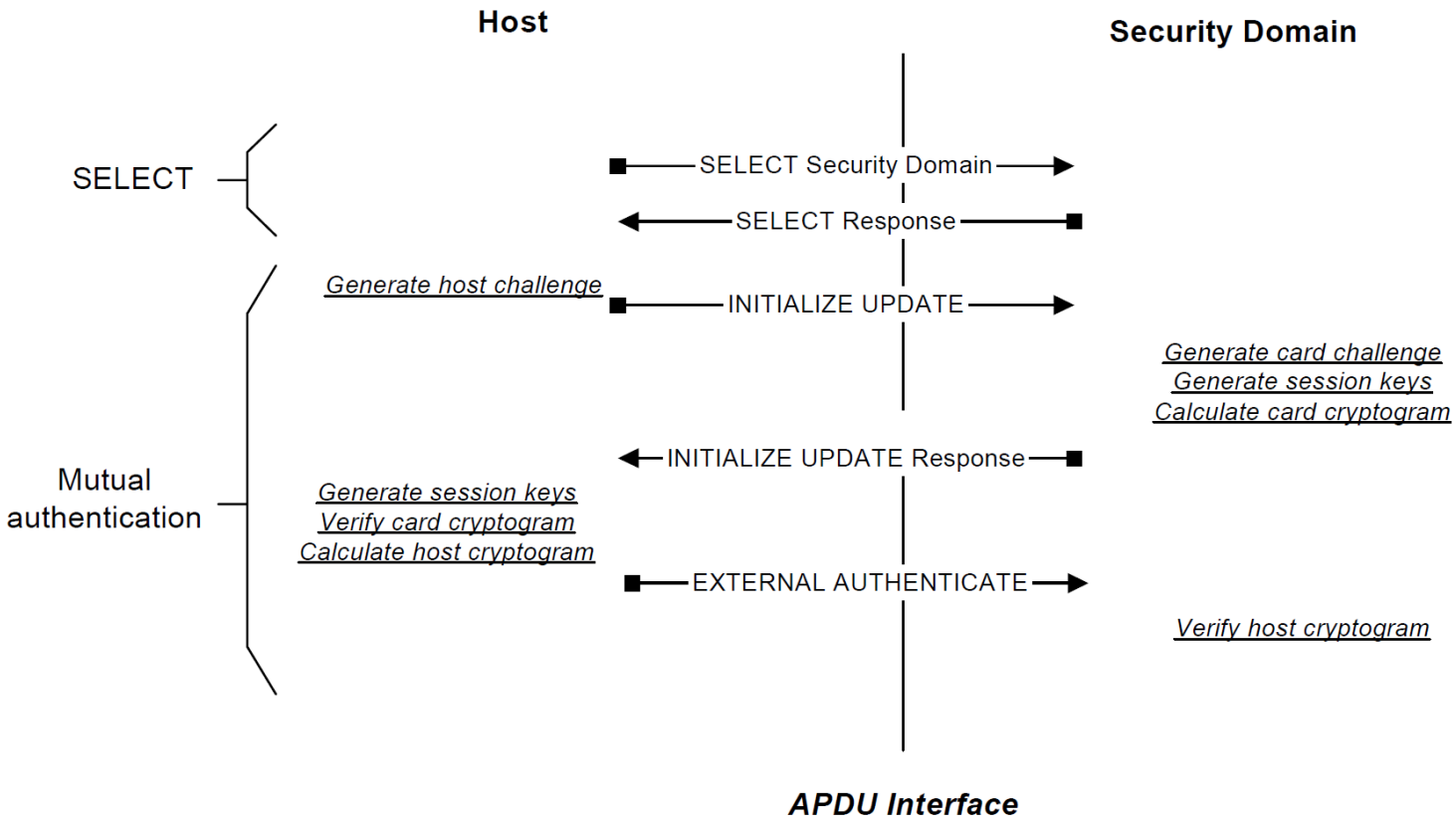


Figure D-1: Mutual Authentication Flow (Security Domain)

GP – Secure Communication

- Select CM
  - 00 A4 04 00 XX <CM AID>
    - 00 A4 04 00 **08** **A0 00 00 00 03 00 00 00**

- Select CM Response
  - 90 00 - Conditions of use not satisfied

GP – Secure Communication

- GET STATUS
  - 80 F2 **80** 00 00
    - 0x80 – Issuer Security Domain only
    - 0x40 – Applications and Security Domains only
    - 0x20 – Executable Load Files only
    - 0x10 – Executable Load Files and their Executable Modules only
- GET STATUS Response (1)
  - 69 85 - Conditions of use not satisfied

GP – Secure Communication

- INITIALIZE UPDATE
  - 80 50 00 00 08
    01 02 03 04 05 06 07 08 00
  - Host challenge
    - **01 02 03 04 05 06 07 08**

Code	Value	Meaning
CLA	'80'	
INS	'50'	INITIALIZE UPDATE
P1	'xx'	Key Version Number
P2	'xx'	Key Identifier
Lc	'08'	Length of host challenge
Data	'xx xx…'	Host challenge
Le	'00'	

Table D-4: INITIALIZE UPDATE Command Message

GP – Secure Communication

- INITIALIZE UPDATE Response
  - **63 61 20 49 4C 4D 31 39 34 32**
    01 01
    61 C9 F8 E1 D3 D7 02 84
    4F 1B 2A DF C4 1A 92 17

Name	Length
Key diversification data	10 bytes
Key information	2 bytes
Card challenge	8 bytes
Card cryptogram	8 bytes

Table D-5: INITIALIZE UPDATE Response Message

GP – Secure Communication

- Klucz „matka”, dane dywersyfikacyjne

- Klucze statyczne
  - K-ENC, K-MAC, K-DEK

- Klucze sesyjne
  - S-ENC, S-MAC, S-DEK

GP – Secure Communication

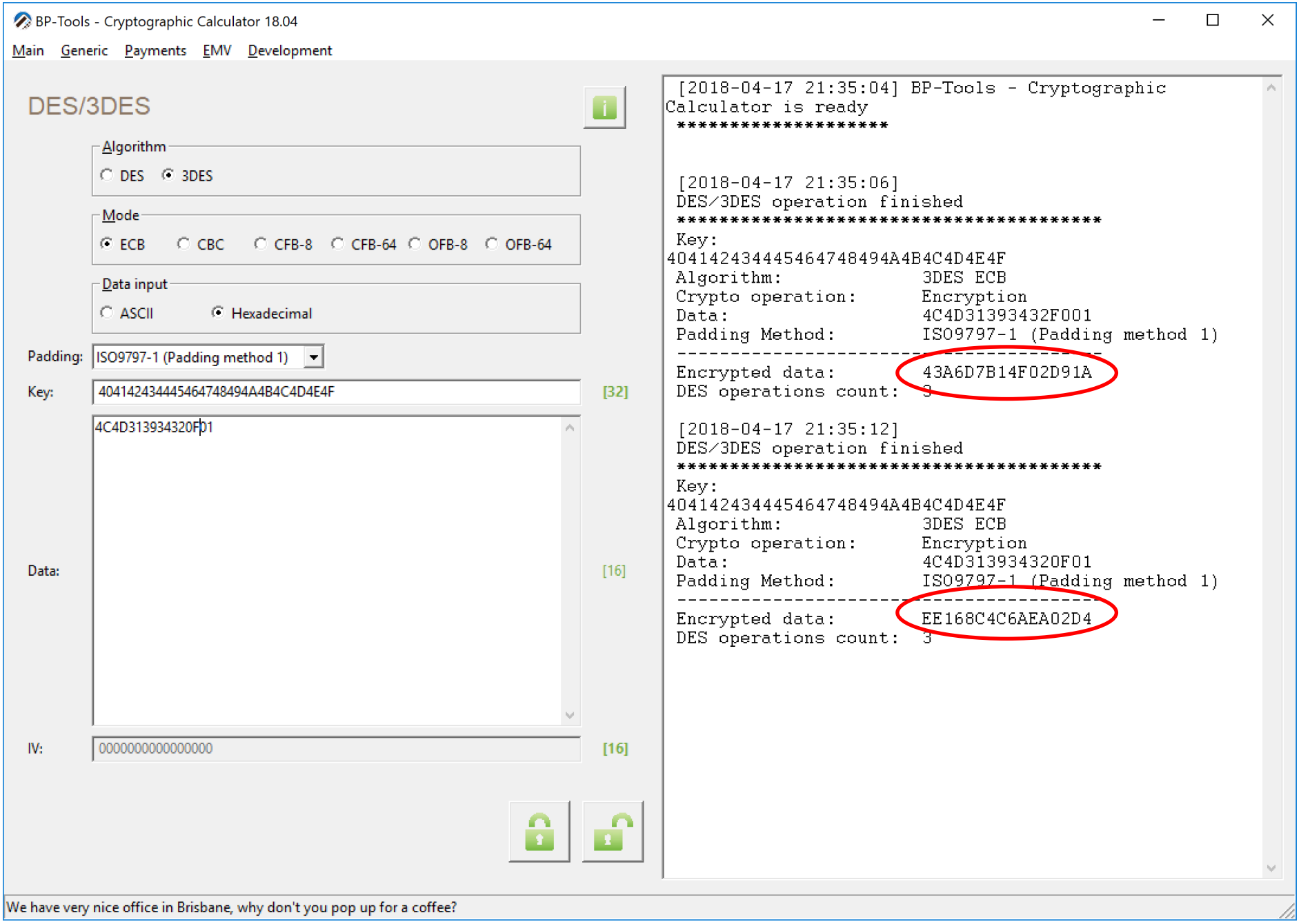
- Klucze statyczne
  - KMC (klucz „matka”)
    - **40 41 42 43 44 45 … 4A 4B 4C 4D 4E 4F**
  - KEYDATA = tag ’CF’
    - **63 61 20 49 4C 4D 31 39 34 32**
  - Dywersyfikacja tag ’CF’

GP – Secure Communication

- Klucze statyczne [EMVCPS11]
  - K_{ENC} :=
    DES3(KMC)[Six least significant bytes of the KEYDATA || ’F0’ || ‘01’] ||
    DES3(KMC)[Six least significant bytes of the KEYDATA || ‘0F’ || ‘01’]

GP – Secure Communication

- Klucze statyczne
  - KEYDATA = TagCF = Key diversification data
    - **63 61 20 49 4C 4D 31 39 34 32**
  - K_{ENC} :=
    DES3(KMC)[4C 4D 31 39 34 32 || ’F0’ || ‘01’] ||
    DES3(KMC)[4C 4D 31 39 34 32 || ‘0F’ || ‘01’]
  - K_{ENC}
    - **43 A6 D7 B1 4F 02 D9 1A ||**
      EE 16 8C 4C 6A EA 02 D4


BP-Tools - Cryptographic Calculator 18.04
Main Generic Payments EMV Development
DES/3DES
Algorithm
DES 3DES
Mode
ECB CBC CFB-8 CFB-64 OFB-8 OFB-64
Data input
ASCII Hexadecimal
Padding: ISO9797-1 (Padding method 1)
Key: 40414243444546474849 4A4B4C4D4E4F [32]
4C4D313934320F01
Data: [16]
IV: 0000000000000000 [16]
[2018-04-17 21:35:04] BP-Tools - Cryptographic Calculator is ready
****
[2018-04-17 21:35:06]
DES/3DES operation finished
****
Key:
40414243444546474849 4A4B4C4D4E4F
Algorithm: 3DES ECB
Crypto operation: Encryption
Data: 4C4D31393432F001
Padding Method: ISO9797-1 (Padding method 1)
Encrypted data: 43A6D7B14F02D91A
DES operations count: 3
[2018-04-17 21:35:12]
DES/3DES operation finished
****
Key:
40414243444546474849 4A4B4C4D4E4F
Algorithm: 3DES ECB
Crypto operation: Encryption
Data: 4C4D313934320F01
Padding Method: ISO9797-1 (Padding method 1)
Encrypted data: EE168C4C6AEA02D4
DES operations count: 3
We have very nice office in Brisbane, why don't you pop up for a coffee?

GP – Secure Communication

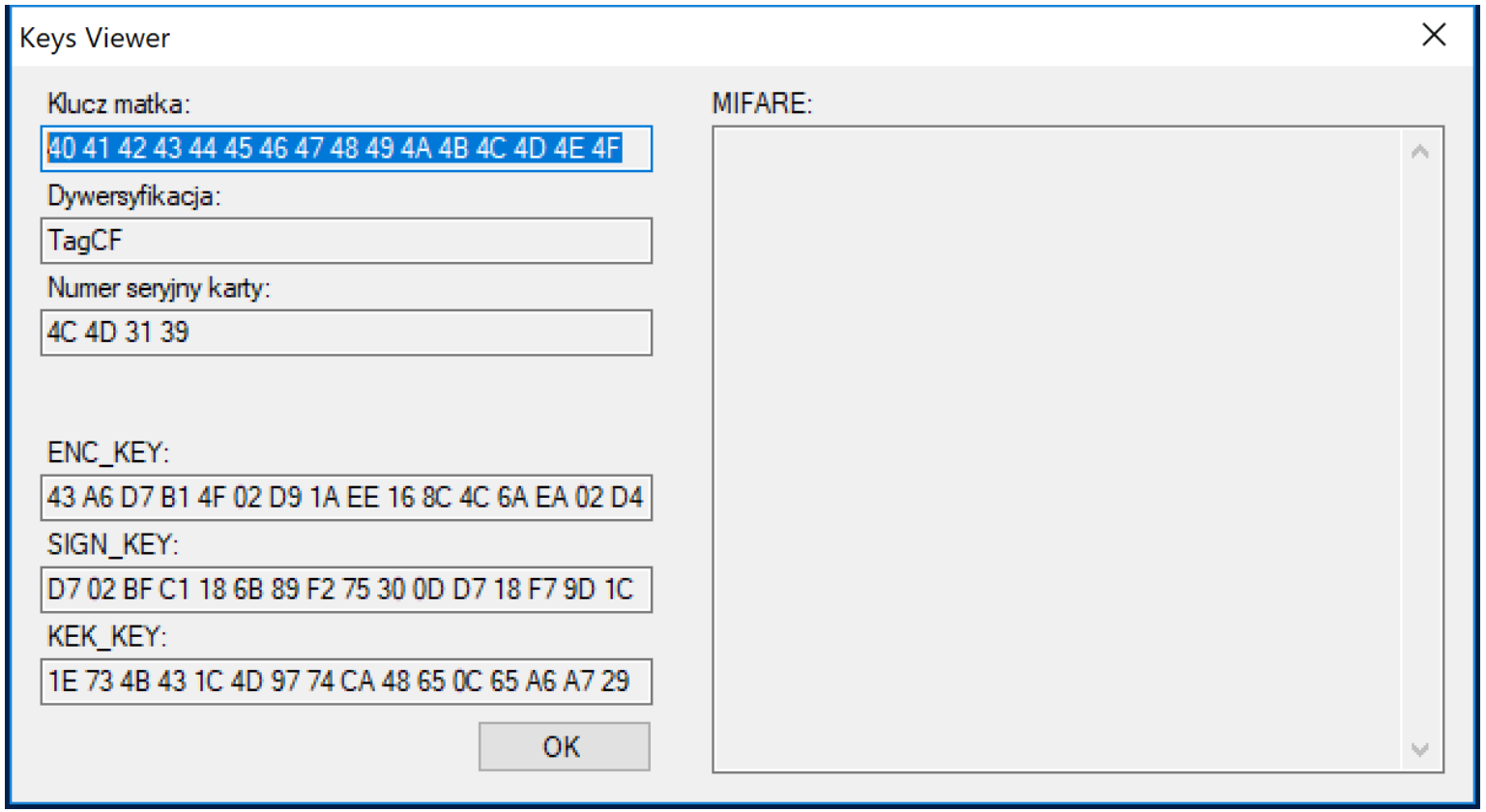
- Klucze statyczne
  - K_{MAC} :=
    DES3(KMC)[Six least significant bytes of the KEYDATA || ’F0’ || ‘02’] ||
    DES3(KMC)[Six least significant bytes of the KEYDATA || ‘0F’ || ‘02’]
  - K_{MAC}
    - **D7 02 BF C1 18 6B 89 F2 ||**
      75 30 0D D7 18 F7 9D 1C

GP – Secure Communication

- Klucze statyczne
  - K_{DEK} :=
    DES3(KMC)[Six least significant bytes of the KEYDATA || ’F0’ || ‘03’] ||
    DES3(KMC)[Six least significant bytes of the KEYDATA || ‘0F’ || ‘03’]
  - K_{DEK}
    - **1E 73 4B 43 1C 4D 97 74 ||**
      CA 48 65 0C 65 A6 A7 29

GP – Secure Communication

- Klucze statyczne



GP – Secure Communication

- Klucze sesyjne [GP211, s.203]
  - S_{ENC}, S-ENC – bezpieczny kanał i szyfrowanie
  - S_{MAC}, S-MAC – weryfikacja MAC
  - S_{DEK}, DEK – szyfrowanie wrażliwych danych

  - przynajmniej jeden zestaw obowiązkowy

Key	Usage	Length	Remark
Secure Channel Encryption Key (S-ENC)	Secure Channel Authentication & Encryption (DES)	16 bytes	Mandatory
Secure Channel Message Authentication Code Key (S-MAC)	Secure Channel MAC Verification (DES)	16 bytes	Mandatory
Data Encryption Key (DEK)	Sensitive Data Decryption (DES)	16 bytes	Mandatory

Table D-1: Security Domain Secure Channel Keys

GP – Secure Communication

- Klucze sesyjne – generowanie
  - Krok 1 – przygotowanie „key derivation data”
  - Krok 2 – obliczenie S_{ENC}
  - Krok 3 – obliczenie S_{MAC}

  - Algorytm 3DES w trybie ECB

GP – Secure Communication

- Klucze sesyjne – generowanie
  - Krok 1 – przygotowanie „key derivation data”

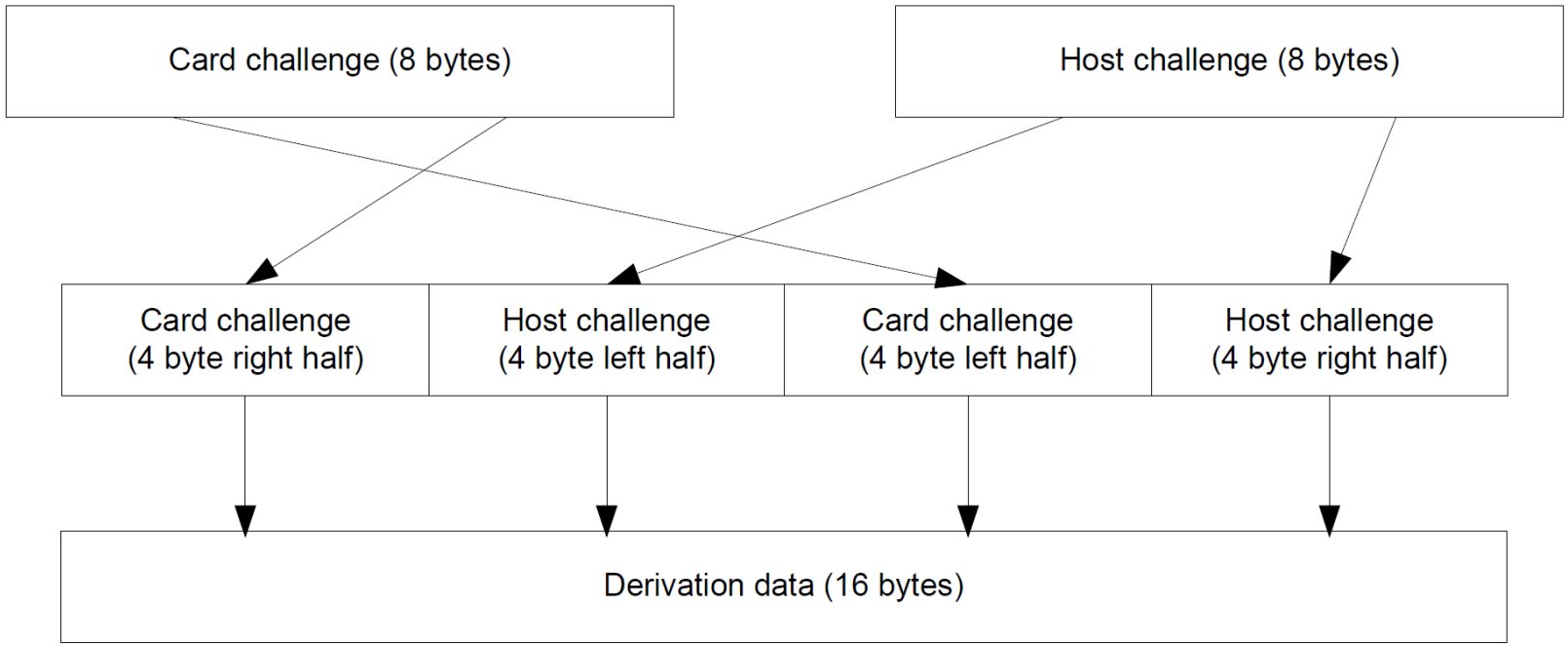


Figure D-3: Session Key - Step 1 - Generate Derivation data

GP – Secure Communication

- Klucze sesyjne – generowanie

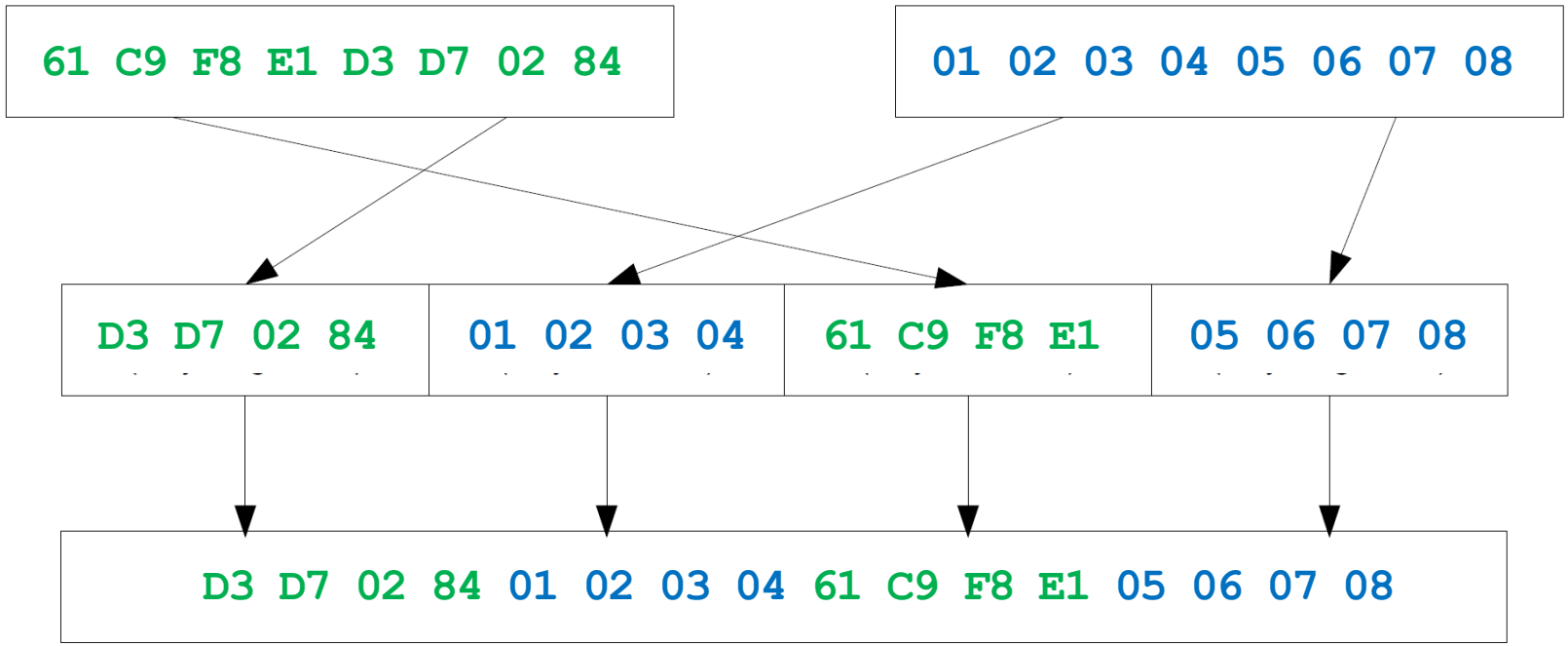


Figure D-3: Session Key - Step 1 - Generate Derivation data

GP – Secure Communication

- Klucze sesyjne – generowanie
  - Krok 2 – obliczanie S_{ENC}

D3 D7 02 84 01 02 03 04 61 C9 F8 E1 05 06 07 08

43 A6 D7 B1 4F 02 D9 1A EE 16 8C 4C 6A EA 02 D4

39 8F 20 0C 2F 62 16 AE C7 F4 2B 96 B9 03 14 D0

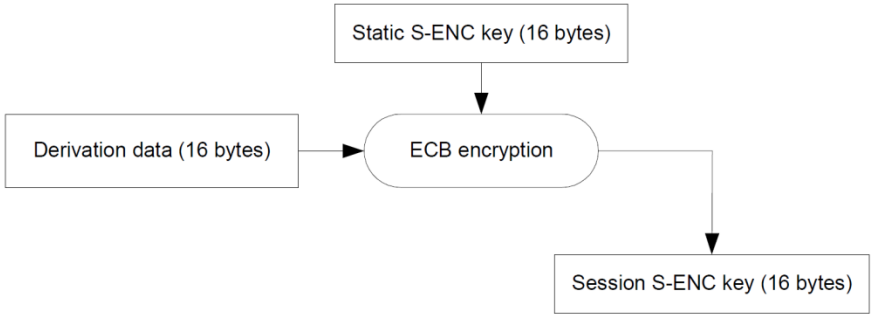


Figure D-4: Session Key - Step 2 - Create S-ENC Session Key

GP – Secure Communication

- Klucze sesyjne – generowanie
  - Krok 3 – obliczanie S_{MAC}

```
D3 D7 02 84 01 02 03 04 61 C9 F8 E1 05 06 07 08
D7 02 BF C1 18 6B 89 F2 75 30 0D D7 18 F7 9D 1C
```

```
48 D0 23 C3 F7 09 C9 8F E5 A2 11 94 05 78 64 1C
```

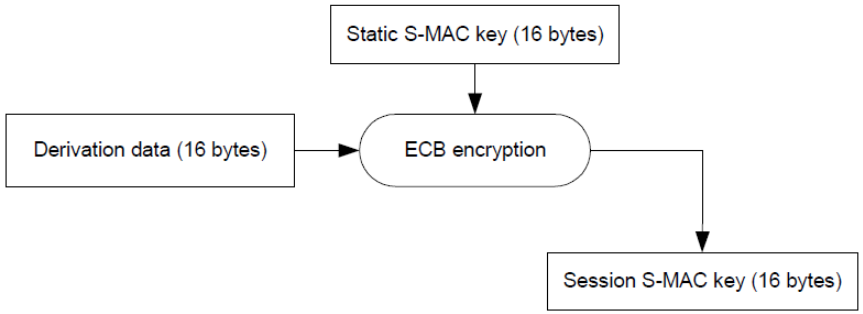
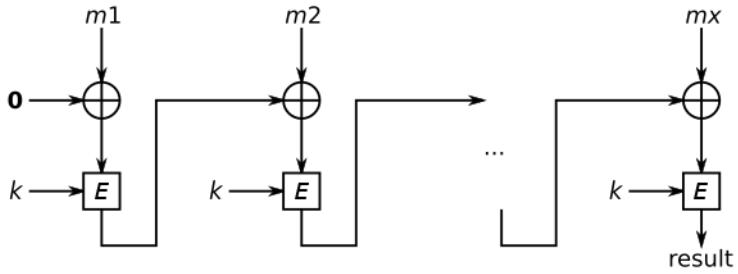


Figure D-5: Session Key – Step 3 - Create S-MAC Session Key

GP – Secure Communication

- Weryfikacja kryptogramu karty [GP211, s. 205]
  - Host challenge ||
    Card challenge ||
    80 00 00 00 00 00 00 00

    `01 02 03 04 05 06 07 08`
    `61 C9 F8 E1 D3 D7 02 84`
    `80 00 00 00 00 00 00 00`
  - S_{ENC}, ICV=0…0
  - MAC Algorithm 1 with output transformation 1, without truncation (CBC-MAC)



https://en.wikipedia.org/wiki/CBC-MAC

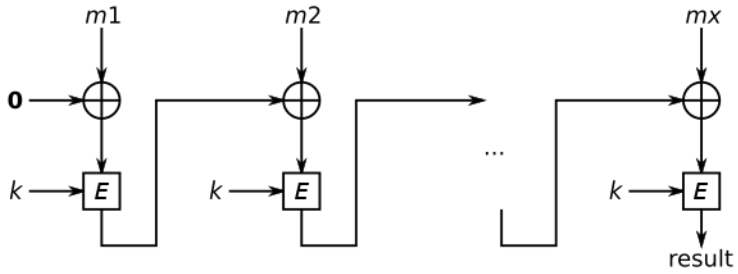
GP – Secure Communication

- Weryfikacja kryptogramu karty [GP211, s. 205]
  1. **DES3(S-ENC)[01 02 03 04 05 06 07 08]**
     = 3B B6 73 43 FC 7E A4 31
  2. **xor 61 C9 F8 E1 D3 D7 02 84**
     = 5A 7F 8B A2 2F A9 A6 B5
  3. **DES3(S-ENC)[**5A 7F 8B A2 2F A9 A6 B5**]**
     = 84 14 E6 AF A8 74 71 66
  4. **xor 80 00 00 00 00 00 00 00**
     = 04 14 E6 AF A8 74 71 66
  5. **DES3(S-ENC)[**04 14 E6 AF A8 74 71 66**]**
     = **4F 1B 2A DF C4 1A 92 17**

GP – Secure Communication

- Obliczenie kryptogramu hosta [GP211, s. 205]
  - Card challenge ||
    Host challenge ||
    80 00 00 00 00 00 00 00

    61 C9 F8 E1 D3 D7 02 84
    01 02 03 04 05 06 07 08
    80 00 00 00 00 00 00 00
  - S_{ENC}, ICV=0…0
  - MAC Algorithm 1 with output transformation 1, without truncation (CBC-MAC)



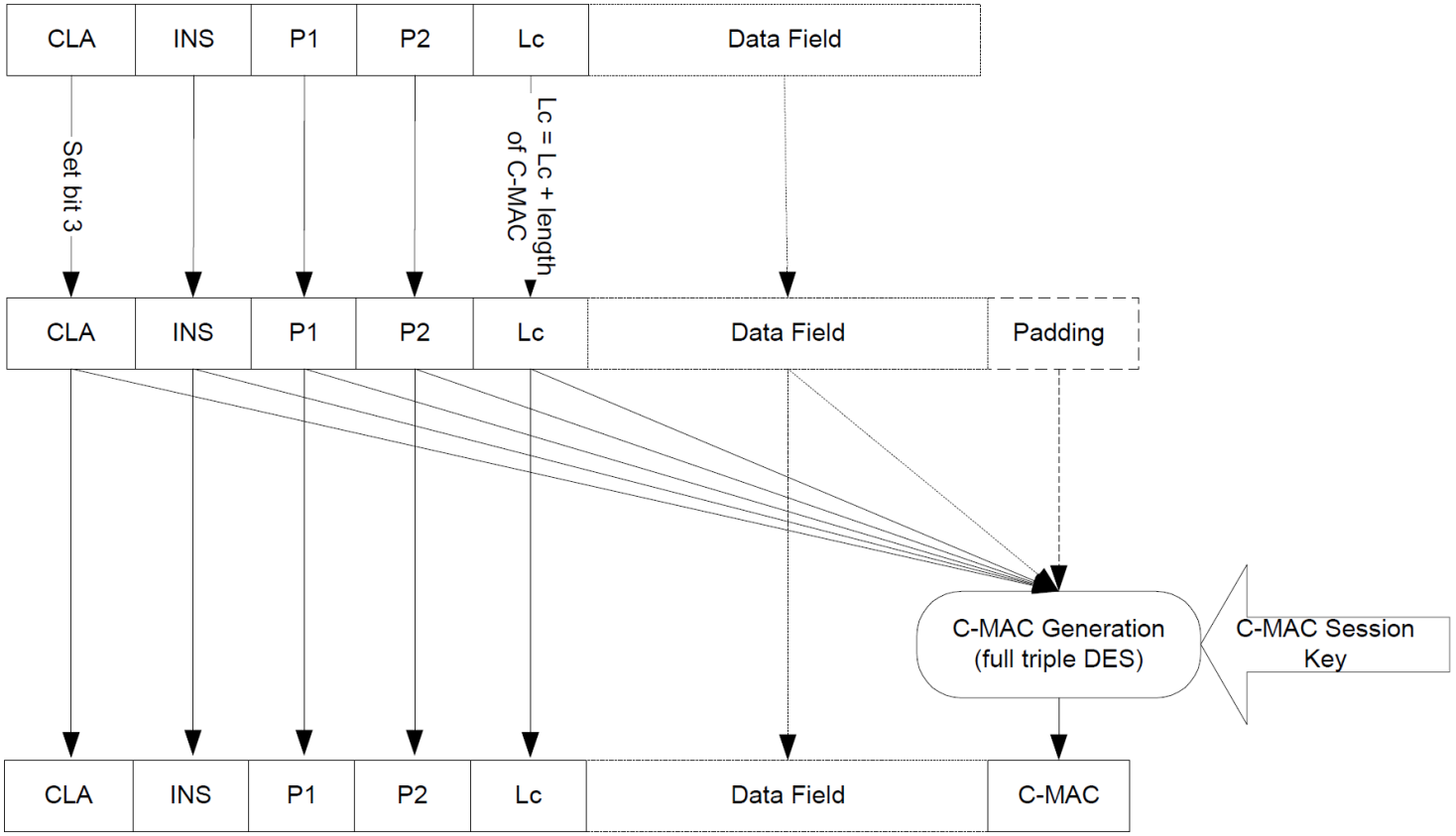
https://en.wikipedia.org/wiki/CBC-MAC

GP – Secure Communication

- Obliczenie kryptogramu hosta [GP211, s. 205]
  1. **DES3(S-ENC)[61 C9 F8 E1 D3 D7 02 84]**
     = 3D D0 28 24 C5 A6 29 31
  2. **xor 01 02 03 04 05 06 07 08**
     = 3C D2 2B 20 C0 A0 2E 39
  3. **DES3(S-ENC)[**3C D2 2B 20 C0 A0 2E 39**]**
     = 29 D4 FC 97 EB 06 FE C8
  4. **xor 80 00 00 00 00 00 00 00**
     = A9 D4 FC 97 EB 06 FE C8
  5. **DES3(S-ENC)[**A9 D4 FC 97 EB 06 FE C8**]**
     = **33 32 61 AB 11 05 1E A6**

GP – Secure Communication

- Obliczenie MAC [GP211, s. 206]



GP – Secure Communication

- Obliczenie MAC [GP211, s. 206]

1. APDU: 84 82 00 00 10
   33 32 61 AB 11 05 1E A6
   80 00 00 (Padding)

84 82 00 00 10 33 32 61
AB 11 05 1E A6 80 00 00

1. **DES3(S-MAC)**[**84 82 00 00 10 33 32 61**]
   = 4C 1A 6B D6 AD 5A 1D 77
2. **xor AB 11 05 1E A6 80 00 00**
   = E7 0B 6E C8 0B DA 1D 77
3. **DES3(S-MAC)**[E7 0B 6E C8 0B DA 1D 77]
   = **3C B9 C7 C5 48 9D 8C 11**

GP – Secure Communication

- EXTERNAL AUTHENTICATE
  - 84 82 00 00 10
    33 32 61 AB 11 05 1E A6 ; host cryptogram
    3C B9 C7 C5 48 9D 8C 11 ; MAC

Code	Value	Meaning
CLA	'84'	
INS	'82'	EXTERNAL AUTHENTICATE
P1	'xx'	Security level
P2	'00'	Reference control parameter P2
Lc	'10'	Length of host cryptogram and MAC
Data	'xx xx…'	Host cryptogram and MAC
Le		Not present

Table D-7: EXTERNAL AUTHENTICATE Command Message

GP – Secure Communication

- EXTERNAL AUTHENTICATE Response
  - `90 00` ☺
  - `63 00` ☹ „Authentication of host cryptogram failed”

Zadanie 1: host/card challenge & cryptogram
Zadanie 2: K-ENC, K-MAC, K-DEC
Zadanie 3: S-ENC, S-MAC, S-DEC, MAC

wysłać na adres:
marek.goslawski@put.poznan.pl

GP – Secure Communication

- GET STATUS
  - 80 F2 **80** 00 00
    - 0x80 – Issuer Security Domain only
    - 0x40 – Applications and Security Domains only
    - 0x20 – Executable Load Files only
    - 0x10 – Executable Load Files and their Executable Modules only

Code	Value	Meaning
CLA	'80' or '84'	
INS	'F2'	GET STATUS
P1	'xx'	Reference control parameter P1
P2	'xx'	Reference control parameter P2
Lc	'xx'	Search criteria (and MAC if present)
Le	'00'	

Table 9-20: GET STATUS Command Message

GP – Secure Communication

- GET STATUS Response [GP211, s. 107]
  - 08 A0 00 00 00 03 00 00 00 07 9A
    - **0x08** – length of AID
    - **0xA0 00 00 00 03 00 00 00** – AID
    - **0x07** – Life Cycle State (0x07 = SELECTABLE)
    - **0x9A** – Application privileges
      0b**1**00**11**0**1**0
      0b**1**0000000 = Security Domain
      0b000**1**0000 = Card Lock
      0b0000**1**000 = Card Terminate
      0b0000000**1** = CVM (Cardholder Verification Method) management

Zadanie 1: host/card challenge & cryptogram
Zadanie 2: K-ENC, K-MAC, K-DEC
Zadanie 3: S-ENC, S-MAC, S-DEC, MAC

wysłać na adres:
marek.goslawski@put.poznan.pl

- marek.goslawski@put.poznan.pl
- +48 61 665 3680
- +48 694 949 750
- pl. Marii Skłodowskiej-Curie 5 (Wilda)
  Budynek B1 (Rektorat), pok. 405

- http://mcp.poznan.pl/