

Document Number: NMSAC-TWIC-Card Feb 07

TWIC Smart Card Application Specification DRAFT v 1.0

Feb. 16, 2007

Sponsor

National Maritime Security Advisory Committee TWIC Working Group

Abstract: The document describes the data model and application requirements for smart card based Transportation Worker Identification Credential (TWIC). This credential is used to access secure areas and information in transportation facilities according to a facility's security plan control requirements.

Keywords: TWIC, smart card, biometric, fingerprint.

1 Summary

1.1 Contacts

Lisa Himber, Vice-Chair, National Maritime Security Advisory Committee
(NMSAC)
Maritime Exchange for the Delaware River and Bay
Tel: (215) 925-2615
Email: lisa.himber@maritimedelriv.com

Basil Maher, President & Chief Operating Officer
Maher Terminals, Inc.
Tel: (908) 665-2100
Email: basil@maherterminals.com

Table of contents

1	Summary	ii
1.1	Contacts	ii
1.2	Change history	Error! Bookmark not defined.
2	Overview	5
2.1	Scope and purpose	5
2.2	References	6
3	TWIC Card-application.....	7
3.1	Card-application Identifier	7
3.2	Key Reference(s).....	7
3.3	Data Model	8
3.4	TWIC card-application command set:.....	10
3.4.1	SELECT card command	10
3.4.2	GET DATA card command	11
4	Annexure A (Informative).....	12
4.1	Sample Data	12
4.1.1	Transportation Worker Unique Information Data Object (0xDFC100) ...	14
4.1.2	TWIC Privacy key Data Object (0xDFC101).....	14
4.1.3	Card Holder Unique Identifier Data Object (0x5FC102)	15
4.1.4	Cardholder Fingerprints Data Object (0xDFC103)	16
4.1.5	Security Object Data Object (0xDFC10F).....	17

2 Overview

2.1 Scope and purpose

This document specifies the requirements for smart card-application for the Transportation Worker Identification Credential (TWIC). The mission of the TWIC program is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation's transportation system and their associated information systems. In its development, the TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document. This specification enables varying levels of control in support of threat level risk mitigation plans.

This specification has been developed by the National Maritime Security Advisory Committee (NMSAC) in response to a request from the Transportation Security Administration (TSA) and the U.S. Coast Guard. The NMSAC TWIC Working Group is comprised of members of the maritime industry with support from representatives from the security technology industry who are affiliated with such organizations as the International Biometric Industry Association (IBIA), the Security Industry Association (SIA) and the Smart Card Alliance.

2.2 References

- [R1] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)
- [R2] FIPS 201 Errata FIPS 201-1 Change Notice
(<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)
- [R3] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2
- [R4] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.3
- [R5] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers
- [R6] ANSI/INCITS 378-2004, Information Technology – Finger Minutiae Format for Data Interchange
- [R7] ANSI/INCITS 358-2002, Information Technology – BioAPI Specification
- [R8] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)
- [R9] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts
- [R10] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards
- [R11] FIPS 197, Advanced Encryption Standard
- [R12] FIPS 140-2, Security Requirements for Cryptographic Modules
- [R13] PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1
- [R14] Global Platform Messaging Specification, Version 1.0, Nov. 2003 (Provides a definition of all the roles and responsibilities for all the actors (systems) in a multi application smart card infrastructure and defines reference standard on information exchange (message) between actors)
- [R15] UL 294, Standard for Safety of Access Control System Units
- [R16] TSA Guidance Package – Biometrics for Airport Access Control (30 September 2005)
- [R17] ANSI/SIA OSIPS ACOV-01:200x (Under Development). The OSIPS (Open, Systems Integration and Performance Standards) data models are defining interoperability between components in traditional access control systems.

3 TWIC Card-application

3.1 Card-application Identifier

TWIC card-application AID		
RID	PIX	State
A0 00 00 xx xx	00 00 10 00 00 01	Default Selected

3.2 Key Reference(s)

Algorithm Identifier*	Key Reference	Key Name	Authenticatable Entity	Security Status	Retry Reset Value	Number of Unlocks
08	'Kp'	TWIC card-application Privacy key	TWIC Card-application Biometric data and Cardholder	Application	N/A	N/A

* Reference FIPS 201-1

3.3 Data Model

Buffer Description	Data Object (BER-TLV tag)	Maximum Length	Access Rule	Contact/Contactless	M/O
Transportation Worker Unique Information	0xDFC100 (0x2000)**	32	Always Read	Contact and Contactless	M
TWIC Privacy key Buffer	0xDFC101 (0x2001)**	64	Always Read	Contact (and Magstripe also)	M
			Never	Contactless	
Card Holder Unique Identifier	0x5FC102 (0x3000)**	3000	Always Read	Contact and Contactless	M
Card Holder Fingerprints	0xDFC103 (0x2003)**	896	Always Read	Contact and Contactless	M
Security Object	0xDFC10F (0x9000)**	920	Always Read	Contact and Contactless	M

** for Security Object DG mapping use only

Note: All the Data Objects in the TWIC card-application data model are elementary data objects with 3-byte ASN.1 BER-TLV encoded tags. Please be aware that individual tags inside these data objects may not be subjected to follow ASN.1 coding rules in the interest of keeping backward compatibility with PIV data model.

Transportation Worker Unique Information		0xDFC100			
Data Element (TLV)	Tag	M/O	Type	Max Bytes	
FASC-N	0x30	M	Fixed Text	25	
Expiration Date	0x35	M	Date (YYYYMMDD)	8	

TWIC Privacy Key Buffer		0xDFC101			
Data Element (TLV)	Tag	M/O	Type	Max Bytes	
TWIC Privacy Key (Kp)	0xC0	M	Variable	32	
Algorithm Identifier	0xC1	M	Fixed Text	01	
Key Index	0xC2	M	Fixed Text (00 = RFU)	01	

Card Holder Unique Identifier		0x5FC102			
Data Element (TLV)	Tag	M/O	Type	Max Bytes	
FASC-N	0x30	M	Fixed Text	25	
GUID	0x34	M	Fixed Numeric	16	
Expiration Date	0x35	M	Date (YYYYMMDD)	8	
Issuer Asymmetric Signature	0x3E	M	Variable	2816	
Error Detection Code	0xFE	M	LRC	0	

Card Holder Fingerprints		0xDFC103		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Encrypted Fingerprint template (2 fingers)	0xBC	M	Fixed	862

Note: Tag 0xBC shall contain the encrypted data (CBEFF header and bio templates). The data should be encrypted by TWIC card-application Privacy key (Kp).

Security Object		0xDFC10F		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Mapping of DG to Data Objects	0xBA	M	Variable	10
Security Object	0xBB	M	Variable	900
Error Detection Code	0xFE	M	LRC	0

Note: The security object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1. [8] Tag “0xBA” is used to map the Data Objects in the TWIC data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD). This enables the security object to be fully compliant for future activities with identity documents.

The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object. The signature field of the security object shall omit the issuer's certificate, since it is included in the CHUID. Card Issuer's Digital Signature is in accordance with FIPS 201-1.

The calculation of hashes of the individual data objects, which are then to be used for creation of Security Object shall be based on the contents of Data Objects as stored in the TWIC card-application.

3.4 TWIC card-application command set:

- SELECT
- Get Data

3.4.1 SELECT card command

Command Syntax

CLA	'00'
INS	'A4'
P1	'04'
P2	'00'
Lc	'0B'
Data Field	TWIC AID (= TWIC RID TWIC PIX)
Le	Length of TWIC card-application property template

Card-application Property Template

Upon selection, the TWIC card-application shall return the application property template described below.

Data Objects in the TWIC Card-application Property Template (Tag '61')

Application identifier of application	'4F'	M	The PIX of the AID includes the encoding of the version of the TWIC card-application.
Coexistent tag allocation authority	'79'	M	Coexistent tag allocation authority template. See Sec 3.1.

Response Syntax

Data Field	Card-application property template
SW1-SW2	Status Word

SW1	SW2	Description
'6A'	'82'	Card-Application not found
'90'	'00'	Successful execution

3.4.2 GET DATA card command

Command Syntax

CLA	'00'
INS	'CB'
P1	'3F'
P2	'FF'
Lc	'05'
Data Field	'See table A
Le	Number of data content bytes to be retrieved

Table A: Data Field

Name	Tag	M/O	Comment
Tag List	5C	M	BER-TLV tag of the data object to be retrieved in clear or encrypted

Response Syntax

Data Field	BER-TLV with the tag '53' containing in the value field the requested data object
SW1-SW2	Status Word

SW1	SW2	Description
'61'	'XX'	Successful execution where SW2 encodes the number of response data bytes still available
'69'	'82'	Security status not satisfied
'6A'	'82'	Data Object not found
'90'	'00'	Successful execution



4 Annexure A (Informative)

4.1 Sample Data

Advisory: The data below is for reference purposes only, The contents of the individual tags have not been verified.

FASC-N (0x30): D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32 48 43 E2

Expiration Date (0x35): 32 30 31 31 30 34 31 30

TWIC Privacy key - Kp (0xC0): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Algorithm Identifier (0xC1): 08

Key Index (0xC2): 00

GUID (0x34): 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30

Fingerprints data:

03 0D 00 00 02 48 00 00 00 1B 02 01 14 06 01 05 0E 1D 00 5A 14 06 04 0A 0D 30 25
5A 14 0B 04 0A 0D 30 25 5A 00 00 08 80 FE 4E 49 53 54 20 43 72 65 61 74 6F 72 00
00 00 00 00 00 D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32
48 43 E2 00 00 00 00 46 4D 52 00 20 32 30 00 02 48 00 00 00 00 00 00 02 00 01 E0
00 C5 00 C5 02 00 07 00 32 29 41 35 00 51 04 00 41 21 00 7A 04 00 40 C2 00 7B 6D
00 41 3C 00 80 5B 00 41 2D 00 90 01 00 80 D1 00 A5 0B 00 41 6B 00 B0 4D 00 41 21
00 BF 62 00 40 EB 00 C6 10 00 40 FB 00 DF 0B 00 41 33 00 E5 AD 00 40 A8 00 E8
73 00 81 57 00 EB 98 00 81 00 00 F1 07 00 81 16 00 F2 62 00 81 4C 00 F3 4C 00 41
20 00 F7 68 00 41 02 00 F9 6B 00 81 43 00 FD 56 00 81 68 01 09 A3 00 81 7C 01 0F
49 00 80 B8 01 2F 1D 00 40 9E 01 49 1D 00 41 25 01 51 82 00 80 A9 01 53 66 00 80
9C 01 54 6B 00 80 C0 01 5B 1A 00 41 3B 01 61 9C 00 81 12 01 69 22 00 41 14 01 76
1A 00 41 27 01 79 AC 00 80 B3 01 7F 12 00 81 3B 01 82 53 00 81 65 01 86 4C 00 80
E1 01 90 11 00 80 E0 01 9E 0B 00 41 65 01 A5 51 00 40 C3 01 B0 08 00 40 F6 01 BB
04 00 80 EC 01 C7 01 00 41 38 01 C8 58 00 00 00 02 10 32 32 41 31 00 15 A4 00 80
EF 00 1F AD 00 41 3C 00 39 4A 00 41 56 00 39 47 00 81 01 00 40 AD 00 81 17 00 4D
51 00 41 4B 00 4D 9C 00 41 59 00 64 44 00 81 4F 00 70 9E 00 40 BA 00 81 06 00 80
AE 00 8A 04 00 80 B1 00 97 5A 00 41 6A 00 9A 41 00 41 19 00 A1 4C 00 81 41 00 A5
9D 00 40 A3 00 AD 02 00 40 B5 00 B9 68 00 41 46 00 BA 42 00 40 B2 00 C1 0B 00 40
E3 00 C7 01 00 40 C9 00 C9 0B 00 40 A7 00 D3 06 00 81 03 01 0D 9B 00 80 FA 01 1B
3F 00 81 30 01 1F 79 00 41 11 01 2B 1D 00 81 1D 01 2F 1A 00 41 41 01 31 36 00 81
2D 01 35 0F 00 81 3F 01 3A 59 00 81 1E 01 3F 09 00 81 43 01 46 5A 00 81 32 01 4B
00 00 40 FF 01 4F 0F 00 41 61 01 52 A1 00 81 4D 01 57 A8 00 81 1D 01 59 62 00 41
7E 01 5A 44 00 41 66 01 5D 4C 00 41 69 01 5E 9B 00 80 CB 01 61 0F 00 81 00 01 63
0A 00 81 5F 01 67 4D 00 81 2B 01 6E 5F 00 80 C0 01 79 0E 00 81 7F 01 7A 45 00 81
70 01 81 4D 00 81 35 01 87 62 00 81 18 01 98 05 00 81 2A 01 9B 5E 00 00 00

Encrypted (under Key Kp) Fingerprints template data:

CC B2 1C 99 0A 63 19 31 B3 05 68 81 3E D9 F2 DF 97 87 7D 48 85 42 52 9C 7E 6E
20 F6 39 57 56 31 51 08 5C 9C 8D D8 54 D2 76 2F DB AB D7 AD D4 42 90 BF 71 A9
38 CC DB 8B 63 76 A0 51 C1 7F 5F CD 33 EA 7B 65 3C B5 D9 87 25 EA 20 9A F9 EA
C5 9C 08 82 01 0B 32 E4 69 43 3F 16 1B F3 B6 4B D8 78 29 3C 50 05 0B 60 66 F3 0A
B5 CC AF EE 74 49 D9 B1 36 C3 2E 02 B3 4B C4 69 65 9E 9B 1C 24 F7 0A 82 84 DB
03 F0 82 BD 51 39 27 AF BE 99 76 38 58 5E 34 A9 49 0D 38 3B EB C7 73 BA 70 DC
42 3F 83 C5 D7 FF 2A 94 A5 93 F5 8F 0E 2B CA 5F 3C CC D9 4C 82 A2 39 4B 1A AA
D6 91 EB 6A D1 C8 C5 AE 9D 67 B6 A7 A3 2E 2F 79 A3 A0 80 32 83 F7 90 31 37 0F
1F 0F 66 AC 4F 06 3E E0 9F 05 7E 64 3A 3E D9 C1 D4 97 6B F4 5B BE 67 EB 0D C9
E1 5F E5 3A 9C E4 61 54 22 E8 E4 D0 B9 D5 44 90 7B DD 39 9C A4 2D FB 66 3B 8D
7C 10 77 95 D0 B4 26 5B A7 FE 1A 70 30 5C C1 A4 AE F0 6B D8 EA A5 2E F5 BC 52
B9 AF 5C 1C 1E 39 11 BF D2 F6 66 79 12 32 0D CF 61 19 3A 54 B4 78 D6 4B 2F CF
89 B2 87 D9 D0 C6 93 BD 2B 84 C7 E7 63 A5 CF D5 76 B0 F5 87 FB BD E9 38 E2 84
C1 B7 ED 5E 31 5E E2 BD F7 8A 08 AE BF 16 B3 2F 30 F2 55 B4 74 BA 8D 93 02 3A
13 8B 94 34 F6 2B B7 20 FB 89 EA 5E E6 04 DA 4A 8C 95 F1 C7 3F 0C 9E 9D 3C 01
99 C4 30 B3 71 C7 F1 8B E6 F1 79 48 31 5F AA 0C 96 14 7E 03 52 20 33 38 10 0F 8E
F2 7B 62 1B 6D A8 20 5F C5 0A 79 D9 05 4E E0 C3 28 56 D3 9A 66 D4 8D 77 D6 D3
07 9C 32 E3 22 2D 0E 68 51 B1 3F 6C 2C E0 7D AC 5B DB E6 8E 6A 74 38 55 C5 E8
47 BF F2 85 6C ED 64 66 CF 33 72 7A 50 15 3B FF 8D AD CD 50 89 1E 07 10 23 27
A6 59 22 02 82 2C 0B 92 91 18 57 02 78 26 F4 6A 42 08 F4 6F F4 24 BA AF DA 57 3A
C8 EF 27 B6 8A 90 83 5C 33 7B 90 7D 85 B8 68 69 8F 64 E8 F0 FF B6 5C 21 18 F7 34
E5 01 60 81 44 43 F4 4F BD 59 6E 72 5D F8 7D A4 1F 65 E0 E0 B4 ED 45 B2 6E 59
CB B3 56 F7 F4 58 BB 6F BA D1 EA C0 D7 C3 1E D1 E2 8C 74 E6 4F 2D 85 51 2D 96
EE 46 E1 0B 6C 61 7F 40 37 45 EE 5B 5C AC 06 FF DB 88 B8 B5 CF 74 56 50 2B BB
93 80 04 BC 0E 99 DF 79 F6 87 14 BB 70 FE BA 61 CD EC 24 D1 31 1B B4 7A 75 76
99 74 7D 59 89 2A 94 41 A5 0A FA E7 A6 42 08 F7 17 33

4.1.1 Transportation Worker Unique Information Data Object (0xDFC100)

30 19 D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32 48 43 E2
35 08 32 30 31 31 30 34 31 30

4.1.2 TWIC Privacy key Data Object (0xDFC101)

C0 10 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F C1 01 08 C2 01 00

4.1.4 Cardholder Fingerprints Data Object (0xDFC103)

BC 82 02 A0 CC B2 1C 99 0A 63 19 31 B3 05 68 81 3E D9 F2 DF 97 87 7D 48 85 42
52 9C 7E 6E 20 F6 39 57 56 31 51 08 5C 9C 8D D8 54 D2 76 2F DB AB D7 AD D4 42
90 BF 71 A9 38 CC DB 8B 63 76 A0 51 C1 7F 5F CD 33 EA 7B 65 3C B5 D9 87 25 EA
20 9A F9 EA C5 9C 08 82 01 0B 32 E4 69 43 3F 16 1B F3 B6 4B D8 78 29 3C 50 05
0B 60 66 F3 0A B5 CC AF EE 74 49 D9 B1 36 C3 2E 02 B3 4B C4 69 65 9E 9B 1C 24
F7 0A 82 84 DB 03 F0 82 BD 51 39 27 AF BE 99 76 38 58 5E 34 A9 49 0D 38 3B EB
C7 73 BA 70 DC 42 3F 83 C5 D7 FF 2A 94 A5 93 F5 8F 0E 2B CA 5F 3C CC D9 4C 82
A2 39 4B 1A AA D6 91 EB 6A D1 C8 C5 AE 9D 67 B6 A7 A3 2E 2F 79 A3 A0 80 32 83
F7 90 31 37 0F 1F 0F 66 AC 4F 06 3E E0 9F 05 7E 64 3A 3E D9 C1 D4 97 6B F4 5B
BE 67 EB 0D C9 E1 5F E5 3A 9C E4 61 54 22 E8 E4 D0 B9 D5 44 90 7B DD 39 9C A4
2D FB 66 3B 8D 7C 10 77 95 D0 B4 26 5B A7 FE 1A 70 30 5C C1 A4 AE F0 6B D8 EA
A5 2E F5 BC 52 B9 AF 5C 1C 1E 39 11 BF D2 F6 66 79 12 32 0D CF 61 19 3A 54 B4
78 D6 4B 2F CF 89 B2 87 D9 D0 C6 93 BD 2B 84 C7 E7 63 A5 CF D5 76 B0 F5 87 FB
BD E9 38 E2 84 C1 B7 ED 5E 31 5E E2 BD F7 8A 08 AE BF 16 B3 2F 30 F2 55 B4 74
BA 8D 93 02 3A 13 8B 94 34 F6 2B B7 20 FB 89 EA 5E E6 04 DA 4A 8C 95 F1 C7 3F
0C 9E 9D 3C 01 99 C4 30 B3 71 C7 F1 8B E6 F1 79 48 31 5F AA 0C 96 14 7E 03 52
20 33 38 10 0F 8E F2 7B 62 1B 6D A8 20 5F C5 0A 79 D9 05 4E E0 C3 28 56 D3 9A
66 D4 8D 77 D6 D3 07 9C 32 E3 22 2D 0E 68 51 B1 3F 6C 2C E0 7D AC 5B DB E6 8E
6A 74 38 55 C5 E8 47 BF F2 85 6C ED 64 66 CF 33 72 7A 50 15 3B FF 8D AD CD 50
89 1E 07 10 23 27 A6 59 22 02 82 2C 0B 92 91 18 57 02 78 26 F4 6A 42 08 F4 6F F4
24 BA AF DA 57 3A C8 EF 27 B6 8A 90 83 5C 33 7B 90 7D 85 B8 68 69 8F 64 E8 F0
FF B6 5C 21 18 F7 34 E5 01 60 81 44 43 F4 4F BD 59 6E 72 5D F8 7D A4 1F 65 E0
E0 B4 ED 45 B2 6E 59 CB B3 56 F7 F4 58 BB 6F BA D1 EA C0 D7 C3 1E D1 E2 8C 74
E6 4F 2D 85 51 2D 96 EE 46 E1 0B 6C 61 7F 40 37 45 EE 5B 5C AC 06 FF DB 88 B8
B5 CF 74 56 50 2B BB 93 80 04 BC 0E 99 DF 79 F6 87 14 BB 70 FE BA 61 CD EC 24
D1 31 1B B4 7A 75 76 99 74 7D 59 89 2A 94 41 A5 0A FA E7 A6 42 08 F7 17 33

4.1.5 Security Object Data Object (0xDFC10F)

BA 0C 01 20 00 02 20 01 03 30 00 04 20 03 BB 82 02 15 30 82 02 11 06 09 2A 86 48
86 F7 0D 01 07 02 A0 82 02 02 30 82 01 FE 02 01 03 31 0B 30 09 06 05 2B 0E 03 02
1A 05 00 30 81 B1 06 06 67 81 08 01 01 01 A0 81 A6 04 81 A3 30 81 A0 02 01 00 30
09 06 05 2B 0E 03 02 1A 05 00 30 81 8F 30 19 02 01 01 04 14 1D 63 83 1D CF 5C 23
EB B6 76 B9 9C 48 57 87 C4 44 6D C3 EC 30 19 02 01 02 04 14 AC 5A EB 84 03 8C
39 03 5A 0A D2 0B 6C 75 68 0B 95 EC 23 52 30 19 02 01 03 04 14 D0 CF D0 B6 5B
72 CD 99 55 24 A1 DF 3E D5 34 3C 3F A8 E2 3130 19 02 01 04 04 14 AD C6 BD B6
40 BD D7 ED 17 81 16 59 19 A2 08 D9 0F 57 B6 98 30 05 02 01 06 04 00 30 05 02 01
07 04 00 30 05 02 01 08 04 00 30 05 02 01 09 04 00 30 05 02 01 0A 04 00 31 82 01
36 30 82 01 32 02 01 01 30 34 30 2F 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0D
30 0B 06 03 55 04 0A 13 04 4E 49 53 54 31 11 30 0F 06 03 55 04 03 13 08 46 41 53
43 4E 20 43 41 02 01 01 30 09 06 05 2B 0E 03 02 1A 05 00 A0 5A 30 15 06 09 2A 86
48 86 F7 0D 01 09 03 31 08 06 06 67 81 08 01 01 01 30 1C 06 09 2A 86 48 86 F7 0D
01 09 05 31 0F 17 0D 30 37 30 32 31 36 30 33 30 33 33 38 5A 30 23 06 09 2A 86 48
86 F7 0D 01 09 04 31 16 04 14 C9 7C 5E 9C 3D 5C A5 9D AA 8B 9B D0 0A F3 E1 7F
8C F3 14 B5 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 04 81 80 21 CB 42 CA 32
AE E1 46 2D CC 37 B6 F2 1C 84 91 AB CB B2 44 43 3E EC 5F 8F 88 01 21 01 95 C5
C4 0B AD EB B1 00 EB 2C 3A 84 85 29 FF 71 36 E7 91 60 2B 82 41 C1 96 83 4C BD
53 D5 74 DA A3 C6 3C 4E 92 B9 27 E3 28 FB 56 BC E3 CA B8 7D 49 C2 46 6E 7D 4A
52 75 B1 EA 26 FD AB F0 9C 57 12 01 7F 2C C7 AD AA 32 62 C0 CB 43 57 9F 3F 34
32 6C E6 13 5B 0C AD 7C A9 2B A1 8A 5D E5 29 27 B8 4B C7 FE 00



5 Annexure B

TWIC AID Structure (Draft)

This section presents how the TIWC Application Identifier is defined and how it should be used in the TWIC applications developed in readers and terminals.

The AID used for the TWIC application will consist of a 5 bytes RID and a 6 bytes long PIX.

RID Current Status:

TSA has applied for a Registered Identifier (RID) according to ISO/IEC 7816-5 which will be communicated to the group as soon as it is available. This RID is, for the time being, represented by the string "A0 00 00 0x xx" in this document. It is also called the TSA RID.

In the mean time, until the final TSA RID is known, the following temporary RID can be used for tests: 'F0 54 57 49 43' (The value 'Fx' indicates a non registered value for the RID and last four bytes are ACSII for 'TWIC').

PIX Structure:

All TSA applications using the RID "A0 00 00 0x xx" will have a similar structure.

The first two bytes of the PIX are used to define the group to which the application belongs. The values '00 00' and 'FF FF' are not defined for now and reserved. The following group values are defined:

- applications used by TSA employees or contractors: group = '10 00'
- applications used by non TSA employees or contractors: group = '20 00'

The following two bytes of the PIX are used to identify the application within a group. The values '00 00' and 'FF FF' are not defined for now and reserved. The following applications are allocated:

- Group '20 00'
- TWIC application number '00 01'

The following byte of the PIX is used to identify the release of the specification as well as the nature of the card. If the first most right bit of this byte is set to one ('1') it indicates the card is a test card. If the rightmost bit is set to zero it is a normal application card. This allows the terminal to set itself in diagnostic mode and execute some more testing/diagnostic functions (when not disabled) when a test card is presented. The current release is defined as release '1'.

The following and last byte of the PIX is used by the card to indicate the version of the specification. The values '00' and 'FF' are so far reserved for future use and not defined. The current TWIC card specification is version '01'.

Bytes of the AID	Symbol	Value	Comment
1 to 5	RID	A0 00 00 0x xx	TSA RID
		F0 54 57 49 43	Temporary TSA RID for test purpose
6 & 7	Grp	00 00 & FF FF	Reserved values
		10 00	TSA employees & contractor group
		20 00	non TSA employees or contractors group
8 & 9	App	00 00 & FF FF	Reserved values
		00 01	TWIC application in group 20 00
10	Release	00 & 7F	Reserved values
		1xxx xxxx	If bit on indicates test card
		01 & 81	TWIC specification release 1
11	Version	00 & FF	Reserved values
		01	TWIC application version 01

The current possible AIDs for a TWIC card are:

A0 00 00 0x xx 20 00 00 01 01 01 Normal TWIC Card
A0 00 00 0x xx 20 00 00 01 81 01 Test TWIC card

F0 54 57 49 43 20 00 00 01 01 01 Temporary AID TWIC Card
F0 54 57 49 43 20 00 00 01 81 01 Temporary AID Test TWIC card

Only one TWIC AID (using the same RID) per card will ever exist but a given card may have a different TWIC application version than another card.

Application cards issued for normal use should not use the temporary RID.

Note:

The terminal looking for the TWIC application should use a partial select command and ask for the partial AID on the first 9 bytes.

The card will respond with the full AID of the TWIC application it has (including release and version as well as the test bit indicator) and the terminal will have to verify it can work with the version in the card. Specifications expect to be upward compatible. In case a new TWIC application specification cannot be made upward compatible, (thus creating a potential problem for existing terminals) a new application will have to be used (App bytes of the PIX).