This document was developed by the Smart Card Alliance Physical Access Council to respond to requests for sample Wiegand message formats that will handle the additional fields of the Federal Agency Smart Credential Number (FASC-N) for programs that use Credential Series fields and Individual Credential Issue to identify credential holders. In addition there is a need to define device status messages to log field device activity. Additional Wiegand formats are defined to support this enhanced messaging along with the extra fields of the FASC-N.

The guidance below is not intended to be normative (or mandated) since some physical access control systems are not able to handle expanded message formats. It was developed to provide industry recommendations on how the Wiegand message format can be extended so that different implementations can proceed forward with guidance that industry has agreed upon.

The Smart Card Alliance Physical Access Council is providing this guidance to the Transportation Security Administration (TSA) for consideration in the Transportation Worker Identification Credential (TWIC) program and to the Department of Defense (DoD) for their Common Access Card (CAC) program, and will be submitting it to the Physical Access Interagency Interoperability Working Group (PAIIWG) for further government/industry discussion.

Reader and system manufactures are not precluded from transmitting and using more or all the fields for the FASC-N. The following two formats meet the minimum number of fields needed to uniquely identify card holders in the TSA - TWIC and DOD CAC programs.

TWIC / CAC Wiegand 58 bit format. When the credential is registered with the physical access control system (PACS), the expiration date will be set equal to or less than the expiration date on the credential.

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14

Credential Code	30-49	20
Credential Series	50-53	4
Individual Series Issue	54-57	4
Parity Bit P2	58	1

58-bit Example:
Agency+System+Credential+Series+Issue
0001000101011 1+0010001010111 0+0101000101100001010 1+0100+0101

Split in half to calculate parity
0001000101011100100010101110 0101000101100001010101000101

Begin parity is Even and starts at bit 2 for 28 bits = 0
End Parity is Odd and starts at bit 30 for 28 = 0

Final output = 0000100010101110010001010111001010001011000010101010001010

TWIC / CAC Wiegand 64-bit format (BCD). When the credential is registered with the PACS, the expiration date will be set equal to or less than the expiration date on the credential.

Description	Position	Length
Agency Code	1-16	16
System Code	17-32	16
Credential Code	33-56	24
Credential Series	57-60	4
Individual Series Issue	61-64	4

64-bit Example (BCD):
Agency+System+Credential+Series+Issue
0001000100010001+0010001000100010+0011001100110011001100110011+0100+0101
No parity
Final output =
0001000100010001001000100010001000110011001100110011001101000101

TWIC / CAC Wiegand 83-bit format. This card format adds the Credential Series and Individual Series Issue fields to the 75 bit format used by the General Services Administration (GSA) Personal Identity Verification (PIV) Evaluation Program test labs.

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Credential Series	50-53	4
Individual Series Issue	54-57	4
Expiration Date	58-82	25
Parity Bit P2	83	1

83-bit Example:
Agency+System+Credential+Series+Issue+Expiration
00010001010111+00100010101110+01010001011000010101+0100+0101+0101110111
101110111001010

Split in half with a one bit overlap to calculate parity
000100010101110010001010111001010001011 0
0010101010001010101110111101110111001010

Begin parity is Even and starts at bit 2 for 41 bits = 1
End Parity is Odd and starts at bit 42 for 41 bits = 1

Final output =
100010001010111001000101011100101000101100001010101000101010111011110111
01110010101

Transaction Status Messages are designed to provide enhanced feedback about the authentication(s) that takes place between device interfacing with the card and the card holder or changes in status of the device configuration. This is a one-byte (8 bits) message where message numbers 0-100 (binary 0000 0000 thru 0110 0100) are accept messages and messages numbers 101 -200 (binary 0110 0101 thru 1100 1000) are reject messages. When the device has a status change, it will transmit all 9s for the card number and expiration date. The device status message numbers are 201-255 (binary 1100 0101

thru 1111 1111). Below are two formats. These messages are optional for card device and system manufacturers. These messages can be transmitted by any communications protocol including Serial (RS-232, RS-422, & RS-485), Ethernet, Wiegand, etc.

TWIC / CAC Wiegand 58-bit format with Transaction Status Messages (total of 66 bits). When the credential is registered with the PACS, the expiration date will be set equal to or less than the expiration date on the credential.

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Credential Series	50-53	4
Individual Series Issue	54-57	4
Transaction Status Messages	58-65	8
Parity Bit P2	66	1

TWIC / CAC Wiegand 56-bit format(without parity) with Transaction Status Messages (total of 64 bits). This format is for manufacturers with legacy panels that cannot handle more than 64 bits. The parity bits can be omitted to create the following format:

Description	Position	Length
Agency Code	1-14	14
System Code	15-28	14
Credential Code	29-48	20
Credential Series	49-52	4
Individual Series Issue	53-56	4

Transaction Status Messages	58-64	8

TWIC / CAC Wiegand 83-bit format with Transaction Status Messages (total of 91 bits). This card format adds the Credential Series and Individual Series Issue fields to the 75-bit format use by the GSA test labs.

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Credential Series	50-53	4
Individual Series Issue	54-57	4
Expiration Date	58-82	25
Transaction Status Messages	83-90	8
Parity Bit P2	91	1

Message Definitions

	Message number (decimal)	**Message**
Accept Messages 0 – 100	0	All verifications passed
	1	Biometric match passed. CHUID and Biometric signatures passed.
	2	Biometric match passed. CHUID and Biometric signatures passed. CAK challenge and response passed. PIN challenge to the card passed.
	3	Biometric match success – similarity score is above the threshold value.
	4	Personal Identification Number (PIN) match. PIN challenge to the card passed.
	5	Card Holder Unique Identifier (CHUID) signature passed.
	6	Card Authentication Key (CAK) challenge and response passed.
	7	PIV challenge and response passed.
	8	Biometric signature passed.
	9	CAK challenge and response passed and certificate is valid.
	10	PIV challenge and response passed and certificate is valid.
	11-100	Reserved for future use.
Reject Messages 101 - 200	101	Biometric match failure – similarity score is below the threshold value.
	102	Failure to acquire – biometric capture did not result in a usable information data set.
	103	Biometric retries limit reached.
	104	PIN mismatch – PIN challenge to the card failed.
	105	CHUID signature failed.
	106	CAK challenge and response failed.
	107	PIV challenge and response failed.
	108	Biometric signature failed.
	109	TWIC Privacy Key (TPK) decryption failure.
	110	No TKP for card holder in the device.
	111	No TKP available from TPK server.
	112	Card's CHUID Expired.
	113	Card's PIV certificate expired.
	114	Card's CAK certificate expired.
	115	Card on Hot list.
	116	Card's PIV certificate revoked.
	117	Card's CAK certificate revoked.
	120	CHUID expired.
	121	Card locked.
	122	PIN retries limit reached.
	123-200	Reserved for future use.

Device Status Messages 201-255	201	Device in card-only mode.
	202	Device in PIN-to-system-only mode.
	203	Device in card or PIN-to-system-only (one factor).
	204	Device in biometric-only mode.
	205	Device in card + PIN-to-system mode.
	206	Device in card + PIN-to-card mode.
	207	Device in card + biometric mode.
	208	Device in car + PIN + biometric mode.
	209	Device in multimode biometric mode - biometric A or Biometric B only
	210	Device in multimode biometric mode - biometric A and Biometric B only.
	211	Device in multimode biometric mode - biometric A or Biometric B + card.
	212	Device in multimode biometric mode - biometric A and Biometric B + card.
	213	Two cards in the reader field.
	214	Less than 1 second between card presentations.
	215-254	Reserved for future use.
	255	Device not capable of supporting Transaction Status Messages.

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating the widespread acceptance, usage, and application of smart card technology for physical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the physical access industry and that will address key issues that end user organizations have in deploying new physical access system technology.

The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software and reader vendors; physical access control systems vendors; and integration service providers. Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.