



# ISO8583 MESSAGE FORMAT SPECIFICATION



September 21, 2005  
Version 3.0

## Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>A98 Overview .....</b>	<b>3</b>
<b>ISO8583 Messages between the Host and the A98.....</b>	<b>3</b>
<b>ISO8583 Message Format for A98 to Host Connection .....</b>	<b>3</b>
General Messaging Format .....	3
General Field Definitions.....	3
Message Flow Protocol .....	3
A98 System to Host Sign-On .....	3
Receiving the Response from the Host .....	3
A98 System to Host Sign-Off.....	3
Receiving the Response from the Host .....	3
A98 to System Echo .....	3
Receiving the Response from the Host .....	3
Sending the Key to the Host from the A98 .....	3
Receiving the Response from the Host.....	3

## A98 Overview

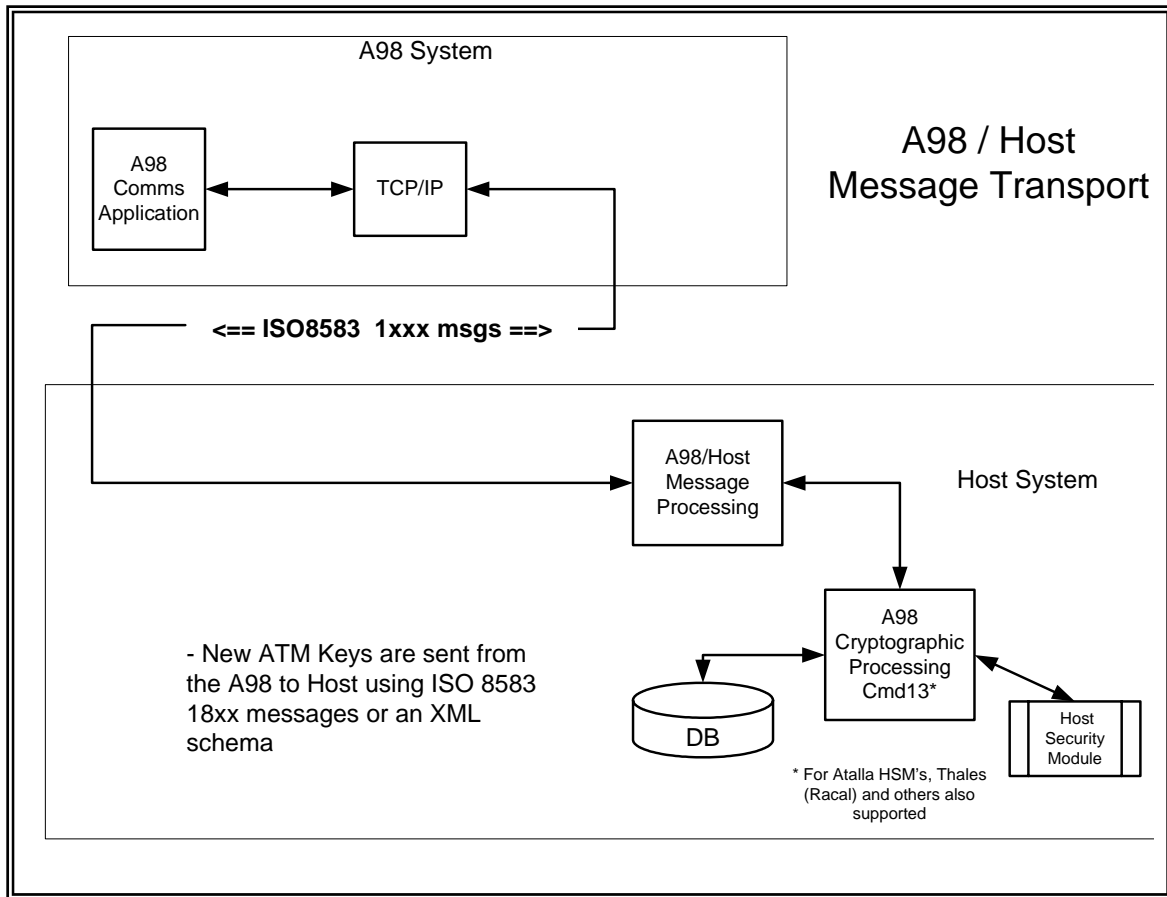
Trusted Security Solutions, Inc. is offering the A98 ATM Initial Key Establishment System to institutions that manage the cryptographic keys for ATMs. A98 works with all ATMs, requires no hardware or programming changes to the ATMs and avoids the cumbersome requirements normally associated with compliant key management. Service personnel communicate with the A98 system via a touch-tone telephone to establish the initial ATM keys in a manner which is fully compliant with the applicable ANSI standards and network operating rules. Once established, the initial keys are securely communicated to the host computer that drives the ATMs. All activity and events are securely logged and detailed reports provide concise audit trail information.

This document explains the A98 Comvelope Solution ISO8583 Host Message format.

The A98-R Remote Key Solution communicates with the Host using XML format which is documented in the A98-R Remote Listener Configuration Guide.

**ISO8583 Messages between the Host and the A98**

The A98 Initial ATM Key Establishment System and the A98 to which it is attached, communicate using an ISO-8583<sup>1</sup> messaging protocol as shown below in Figure 1. The newly established ATM key is sent from the A98 to the host using 18xx message formats. The message containing the new ATM key also contains additional information to minimize any errors from being propagated. Key check values are provided to permit the Host to verify the correct information is being sent.



**Figure 1 - A98 to Host Connection**

<sup>1</sup> ISO-8583 – 1993 – Financial transaction card originated messages – Interchange message specifications

## ISO8583 Message Format for A98 to Host Connection

The A98 implements an ISO-8583 like messaging protocol. Only the fields defined in this specification are permitted. Deviation from the message formats in this specification may cause unexpected results.

### General Messaging Format

The general message format is shown below. The messages consist of predefined fields. The presence or absence of a field is indicated by the presence or absence of the corresponding bit in the primary (fields 1-64) or secondary (fields 65-129) bit maps. Fixed length fields are easy. The variable length fields are resolved via a length parameter carried at the beginning of those fields. All non-binary fields are of type ASCII chars while Binary fields are of type unsigned char. For example the message number 1804 is sent as 0x31, 0x38, 0x30, 0x34 while the binary field of 803001 is sent as 0x38, 0x30, 0x33, 0x30, 0x30, 0x31 etc. Binary Fields MUST be a multiple of 8 Bits. The VERY general 18xx message layout is:

Off	Len	Type	Bit	Name	Description	Comments
0	4	n4	xxx	Msg. Num.	ISO Message Number	18xx
4	16	b8	xxx	Primary Bit Map	Fields 1-64	First bit -> Sec. Map
20	16	b8	xxx	Secondary Bit Map	Fields 65-129	First bit -> Ter. Map
36	6	n6	P11	System Audit	Message Trace Number	
42	12	n12	P12	Date Time Local	YYMMDDhhmmss	
54	3	n3	P24	Function Code	801=Sign on 802=Signoff 803=Target Sys Unavail 805=Special 811=Key Change	n
57	3	n3	P39	Action Code	880-899=available - private	A98 assigned
60	var	n..999	P59	Transport Data	The Key Information plus User Defined Authentication Data	A98 Data
63+ var	11	n..11	S93	Transp. Destination	Message destination ID	BIN + DEST-ID
76+ var	11	n..11	s94	Transp. Origin	Message Origin ID	BIN + ORG-ID

### General Field Definitions

Field	Description
P11	6 numeric digit trace number assigned by A98 or Host depending on message direction
P12	12 numeric digits for the message date and time in the format of YYMMDDhhmmss
P24	3 numeric digit code indicating function to be performed
P39	3 numeric digit code indicating the result of performing the requested function
P59	Variable length field that carries information specific to the requested function
S93	Variable length field with length fixed at 11 that specifies the destination for this message. It is in the form of BIN + Destination ID (nnnnnndddd)
S94	Variable length field with length fixed at 11 that specifies the origin of this message. It is in the form of BIN + Origin ID (nnnnnnooooo)

## Message Flow Protocol

Each 1804 or 1805 message sent requires an 1814 response message to be sent from the message receiver.

Msg#	A98 Host	Function Code	Action Code	Translation
1804	→	801		"Please Sign Me ON"
1804	→	802		"Please Sign Me OFF"
1804	→	803		"The A98 is not currently available"
1804	→	811		"Here's the new A and B keys for ATM-ID so and so"
1805	→	811		"Here's the new A and B keys for ATM-ID so and so. Repeat of prior message"
1814	←		800	"Successful Completion" – e.g. - "Logon Successful" - or - "New ATM Keys were accepted"
1814	←		880	"Host System Currently Unavailable"
1814	←		881-889	"These are reserved"
1814	←		890	"Please re-send the message"
1814	←		891	"Terminal ID Not Found"
1814	←		892	"KEK ID Not Found"
1814	←		893	"KEK Key Check Value Error"
1814	←		894	"ATMA Key Check Value Error"
1814	←		895	"ATMB Key Check Value Error"
1814	←		896	"Checksum did not check"
1814	←		897	"Short Message received"
1814	←		898	"Long Message received"
1814	←		899	"Undefined Error Occurred"

## A98 System to Host Sign-On

An ISO-8583 1804 message is used to sign-on to the Host System. The command is carried in p24 (primary bit field). An 1814 message is expected in response from the host. If required or requested, the information is resent as an 1805 message, which is identical to the 1804 – except for the number of course.

User defined Authentication Data is transmitted in P59. If no Authentication is used set P59 to Nulls.

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1804
4	16	b8	xxx	Primary Bit Map	8030 0100 0000 0020
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss
54	3	n3	P24	Function Code	801 – Sign-On 803 – System Unavailable
57	16	n...999	P59	Transport Data	16 digits of Authentication Data - TBD
76	11	n..11	S93	Transp. Destination	BIN+SYS-ID
89	11	n..11	S94	Transp. Origin	BIN+A98-ID

## Receiving the Response from the Host

An ISO-8583 1814 message is used to send the results of Host processing of the corresponding 1804 Sign-on message

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1814
4	16	b8	xxx	Primary Bit Map	8030 0000 0200 0000
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss – remains unchanged
54	3	n3	P39	Action Code	800 - Sign-On Successful 880 – Unsuccessful. Host Unavailable
57	11	n..11	S93	Transp. Destination	BIN+SYS-ID
70	11	n..11	S94	Transp. Origin	BIN+A98-ID

## A98 System to Host Sign-Off

An ISO-8583 1804 message is used to sign-off from the Host System. The command is carried in p24 (primary bit field). An 1814 message is expected in response from the host. If required or requested, the information is resent as an 1805 message, which is identical to the 1804 – except for the number of course.

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1804
4	16	b8	xxx	Primary Bit Map	8030 0100 0000 0000
29	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss
54	3	n3	P24	Function Code	802 - Sign-Off 803 – System Unavailable
57	11	n..11	S93	Transp. Destination	BIN+SYS-ID
70	11	n..11	S94	Transp. Origin	BIN+A98-ID

## Receiving the Response from the Host

An ISO-8583 1814 message is used to send the results of Host processing of the corresponding 1804 Sign-on message

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1814
4	16	b8	xxx	Primary Bit Map	8030 0000 0200 0000
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss – remains unchanged
54	3	n3	P39	Action Code	800 - Sign-On Successful 880 – Unsuccessful. Host Unavailable
57	11	n..11	S93	Transp. Destination	BIN+SYS-ID
70	11	n..11	S94	Transp. Origin	BIN+A98-ID

## A98 to System Echo

An ISO-8583 1804 message is used to poll the host system to verify the status of the connection. The command is carried in p24 (primary bit field). An 1814 message is expected in response from the host.

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1804
4	16	b8	xxx	Primary Bit Map	8030 0100 0000 0000
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss
54	3	n3	P24	Function Code	831 - Login
57	11	n..11	S93	Transp. Destination	BIN+SYS-ID
68	11	n..11	S94	Transp. Origin	BIN+A98-ID

## Receiving the Response from the Host

An ISO-8583 1814 message is used to send the results of Host processing of the corresponding 1804 Echo message

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1814
4	16	b8	xxx	Primary Bit Map	8030 0000 0200 0000
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss – remains unchanged
54	3	n3	P39	Action Code	800 – Echo Successful
57	11	n..11	S93	Transp. Destination	BIN+SYS-ID
68	11	n..11	S94	Transp. Origin	BIN+A98-ID

Below is an example 1804 echo message from the A98 to the Host.

```
Buffer Size: 81           Length Indicator: &h4F &h0
>1804803001000000000000000000000000000000000000000000000000000000050901182704831$LOCALHOST$$A98<
```

Below is an example 1814 response from the Host to the A98.

```
Buffer Size: 81           Length Indicator: &h4F &h0
>1814803000000200000000000000000000000000000000000000000000000000050901182704800$LOCALHOST$$A98<
```

## Sending the Key to the Host from the A98

An ISO-8583 1804 message is used to send the newly established ATMB and ATMA keys to the host system. The command is carried in p39 (primary bit field) and the keying information is carried in p59. An 1814 message is expected in response from the host. If required or requested, the information is resent as an 1805 message, which is identical to the 1804 – except for the number of course.

Off	Len	Type	Bit	Name	Value																								
0	4	n4	xxx	Msg. Num.	1804																								
4	16	b8	xxx	Primary Bit Map	8030 0100 0000 0020																								
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000																								
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged																								
42	12	n12	P12	Date Time Local	YYMMDDhhmmss																								
54	3	n3	P24	Function Code	811																								
57	134	n...999	P59	Transport Data	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Len</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>134 &lt;Length of p59&gt;</td> </tr> <tr> <td>16</td> <td>Terminal ID</td> </tr> <tr> <td>32</td> <td>KEK ID</td> </tr> <tr> <td>6</td> <td>KCV for KEK</td> </tr> <tr> <td>1</td> <td>ATMB Length<sup>2</sup></td> </tr> <tr> <td>32</td> <td>eKEK(ATMB)</td> </tr> <tr> <td>1</td> <td>ATMA Length<sup>3</sup></td> </tr> <tr> <td>6</td> <td>KCV for ATMB</td> </tr> <tr> <td>32</td> <td>eKEK(ATMA)</td> </tr> <tr> <td>6</td> <td>KCV for ATMA</td> </tr> <tr> <td>2</td> <td>xor of all bytes in field p59</td> </tr> </tbody> </table>	Len	Description	3	134 <Length of p59>	16	Terminal ID	32	KEK ID	6	KCV for KEK	1	ATMB Length <sup>2</sup>	32	eKEK(ATMB)	1	ATMA Length <sup>3</sup>	6	KCV for ATMB	32	eKEK(ATMA)	6	KCV for ATMA	2	xor of all bytes in field p59
Len	Description																												
3	134 <Length of p59>																												
16	Terminal ID																												
32	KEK ID																												
6	KCV for KEK																												
1	ATMB Length <sup>2</sup>																												
32	eKEK(ATMB)																												
1	ATMA Length <sup>3</sup>																												
6	KCV for ATMB																												
32	eKEK(ATMA)																												
6	KCV for ATMA																												
2	xor of all bytes in field p59																												
194	11	n..11	S93	Transp. Destination	BIN+SYSID																								
207	11	n..11	S94	Transp. Origin	BIN+A98-ID																								

Prior to the release 2.5, the message length (p59) was included in the xor, checksum calculation. With release 2.5, you can include or exclude the message length in the checksum calculation. By default, the A98 does not include the message length in the checksum calculation. Refer to the A98 Users guide to change the default setting.

<sup>2</sup> 1=Single-Length Key, 2= Double Length Key

<sup>3</sup> 1=Single-Length Key, 2= Double Length Key

## Receiving the Response from the Host

An ISO-8583 1814 message is used to send the results of Host processing of the corresponding 1804 message.

Off	Len	Type	Bit	Name	Value
0	4	n4	xxx	Msg. Num.	1814
4	16	b8	xxx	Primary Bit Map	8030 0000 0200 0020
20	16	b8	xxx	Secondary Bit Map	0000 000C 0000 0000
36	6	n6	P11	System Audit Numb	NNNNNN – remains unchanged
42	12	n12	P12	Date Time Local	YYMMDDhhmmss – remains unchanged
54	3	n3	P39	Action Code	8xx -response codes as defined above
57	var	n...99 9	P59	Transport Data	Response code dependent information
57+var	11	n..11	S93	Transp. Destination	BIN+SYS-ID
68+var	11	n..11	S94	Transp. Origin	BIN+A98-ID