



ECHO SSL Gateway Developer's User Guide

Electronic Clearing House, Inc.
(800) 233-0406
www.echo-inc.com

Notice of Proprietary Information

The information in this user's guide is confidential and proprietary to Electronic Clearing House, Inc. (*ECHO*). No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written permission of Electronic Clearing House, Inc. Any unauthorized duplication is in violation of U.S. copyright and other laws, and can result in severe monetary and criminal damages.

ECHO proprietary and confidential information exempt from public disclosure under the Freedom of Information Act [5 USC 552 (b) (4)], The ARMS Export Control Act [22 USC 2778 (e)], the Export Administration Act [50 USC APP. 2411 (c)] and the Trade Secrets Act [18 USC 1905].

Copyright Notice

©2005 Electronic Clearing House, Inc (*ECHO*). All rights reserved.

Registered Trademarks and Proprietary Names

The following are copyrights of their respective companies or organizations:

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

ECHO[®], *MerchantAmerica*SM, *NCN*[®] and *XPRESSCHEX*[®] are all property of Electronic Clearing House, Inc. (*ECHO*).

Table of Contents

List of Figures	iv
List of Tables	iv
Introduction	1
<i>References</i>	1
<i>Revision History</i>	1
ECHO SSL Gateway	1
<i>Description</i>	1
<i>Gateway Services</i>	1
Secure Socket Layer	2
SPKT Protocol.....	4
<i>Transaction Packet Format</i>	4
<i>Client/Server Data Flow</i>	4
ECHK and ECHK Simulator Protocols.....	4
<i>Transaction Packet Format</i>	5
<i>Client/Server Data Flow</i>	5
<i>Using the ECHK Simulator</i>	5
Check Image Upload Protocol	6
<i>Client/Server Data Flow</i>	6
<i>Transaction Packet Format</i>	6
<i>Image Repository</i>	6
Appendix A – ECHK Simulator Responses	7
Appendix B – Troubleshooting Q & A	9

List of Figures

<i>Figure 1, SSL Session Handshake.....</i>	<i>3</i>
---	----------

List of Tables

<i>Table 1, SSL Gateway Server</i>	<i>1</i>
<i>Table 2, List of Supported Services.....</i>	<i>2</i>
<i>Table 3, Transaction Processing Flow.....</i>	<i>4</i>
<i>Table 4, Transaction Processing Flow.....</i>	<i>5</i>
<i>Table 5, Check Image Upload Processing Flow.....</i>	<i>6</i>

Introduction

This document is intended to provide a developer with the information needed to send and receive ECHK and SPKT transaction packets to the *ECHO* SSL Gateway.

References

The following resources are referenced in this document.

- NCN ECHK Host Protocol
- NCN SPKT Host Protocol
- Stunnel: <http://www.stunnel.org/>
- OpenSSL: <http://www.openssl.org/>

Revision History

Revision	Date	Author(s)	Comments
1.0	10/03/2005	M. Swann	This document combines the ECHK and SPKT SSL Gateway User Guides into a single user guide.

ECHO SSL Gateway

Description

The *ECHO* SSL Gateway server uses OpenSSL to provide a secure tunnel (see Stunnel reference) to multiple services. OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.

Gateway Services

The *ECHO* SSL Gateway server can be reached at IP address 12.35.204.158. Ports 9000 through 9005 are allocated for use by the SSL Gateway for SSL encryption services. These assignments are described as follows.

IP Address	Port	Service Provided
12.35.204.158	9000	Credit/Debit (future)
	9001	Check Image Upload
	9002	ISO 8583 Translation (future)
	9003	ECHK Simulated Transactions
	9004	ECHK
	9005	SPKT

Table 1, SSL Gateway Server

All the supported services are listed below.

Service	Description
SPKT	This service provides a secure tunnel directly to the SPKT host.
ECHK	This service provides a secure tunnel directly to the ECHK Batch host.
ECHK Simulator	This service provides a secure tunnel to the ECHK simulator.
Check Image Upload	Single-image upload for check images.

Table 2, List of Supported Services

Secure Socket Layer

The *ECHO* SSL Gateway is set up for server validation only. This means that the terminal does not need to maintain a client certificate and does not need to present one during the SSL session handshake.

The following diagram shows the SSL handshake activity followed by the encrypted transaction data exchange and the exchange of close notifications.

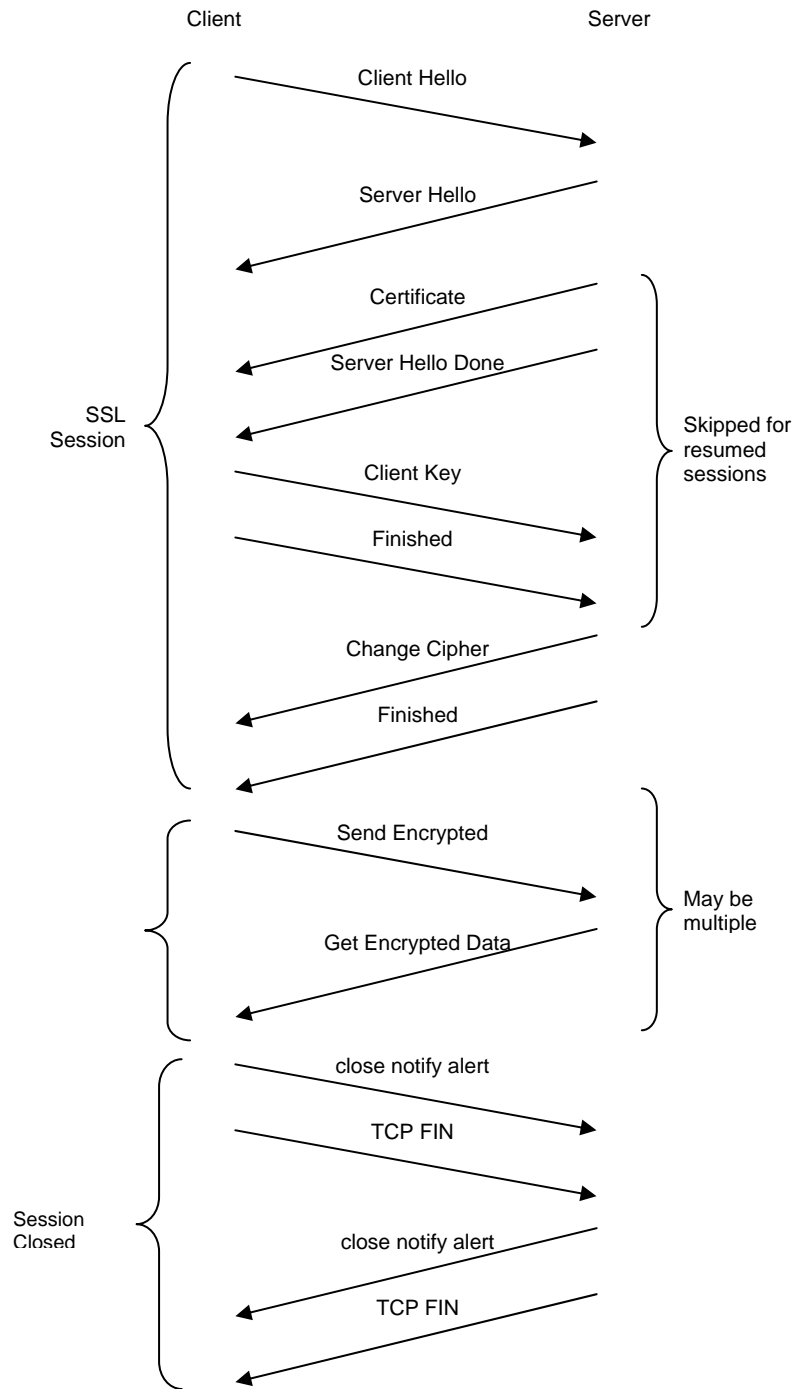


Figure 1, SSL Session Handshake

The *ECHO* SSL Gateway server maintains session information in a session certificate cache for up to one hour. If the terminal makes another connection within the one-hour period, the previous SSL session will be resumed and part of the initial SSL handshake will be bypassed. This will noticeably improve the connection time for terminals that have a large transaction rate.

SPKT Protocol

Refer to document **NCN SPKT Host Protocol, Rev1.0** for a description of the contents of the SPKT transaction packet.

Transaction Packet Format

The client <msg> shown in Table 3, step 2 below, is of the form:

<STX><request packet¹><ETX>

The host <reply> to the <msg> (step 3 below) is of the form:

<STX><response packet><ETX>

This differs only slightly from the dialup transaction packet format. The trailing <LRC> is not required and should not be included.

Client/Server Data Flow

The following table describes the interaction between the terminal and the SSL Server.

Step	Client	SSL Server	Description
1	SSL Session Handshake		Client and Server negotiate a secure socket session GOTO Step 2
2	<msg>		Terminal sends encrypted <msg> to Host. GOTO Step 3
3		<reply>	Host sends encrypted <reply> to terminal GOTO Step 4
4	Session Close		Client initiates SSL session close with Server.

Table 3, Transaction Processing Flow

ECHK and ECHK Simulator Protocols

The ECHK and ECHK Simulator service protocols are the same so both will be described here. The two services only differ in their functionality. The ECHK Simulator:

- Cannot move money, and
- Cannot simulate a host batch retrieval.
- Simulates NCN responses and does not access or impact velocity on the NCN production system.

¹ See the NCN SPKT Host Protocol document.

Transaction Packet Format

The client <msg> shown in Table 4, step 2, is of the form:

<STX><request packet²><ETX>

The host <reply> to the <msg> (step 3) is of the form:

<STX><response packet><ETX>

This differs only slightly from the dialup transaction packet format. The trailing <LRC> is not required and should not be included.

Client/Server Data Flow

The following table describes the interaction between the terminal and the SSL Server.

Step	Client	SSL Server	Description
1	SSL Session Handshake		Client and Server negotiate a secure socket session GOTO Step 2
2	<msg>		Terminal sends encrypted <msg> to Host. GOTO Step 3
3		<reply>	Host sends encrypted <reply> to terminal If (Not last client transaction) THEN Client sends next request GOTO Step 2 ELSE Client closes communication session GOTO Step 4 ENDIF
4	Session Close		Client initiates SSL session close with Server.

Table 4, Transaction Processing Flow

Single and multiple transactions are supported. The terminal does not need to do anything special to indicate that this is a single or multi-transaction session beyond initiating an SSL session close after the last transaction.

Using the ECHK Simulator

Application developers should first use the ECHK Simulator on port 9003 before using the live ECHK service on port 9004. The ECHK Simulator is mainly useful for testing how well your application handles all the different host responses. It does not, however, perform the full transaction validation that the ECHK service does on port 9004.

Refer to the ECHK Simulator Responses in Appendix A to see the responses that the simulator can send. To select a response, send a transaction with a dollar amount

² See the NCN ECHK Host Protocol document.

(tag "A") that corresponds with the **Index** column in the table, i.e., send an amount of \$67.00 to receive the host response "AUTH NUM 123-999".

Check Image Upload Protocol

Client/Server Data Flow

The following table describes the interaction between the terminal and the SSL Server.

Step	Client	SSL Server	Description
1	SSL Session Handshake		Client and Server negotiate a secure socket session GOTO Step 1
2	<image>		Terminal sends encrypted <image> to Host. No host response is expected. GOTO Step 3
3	Session Close		Client initiates SSL session close with Server.

Table 5, Check Image Upload Processing Flow

Transaction Packet Format

The client sends the check <image> data to the ECHO SSL Gateway using the following format.

<image-size><image-data>

Where <image-size> is the size of <image-data> formatted into a 4-byte binary word with big-endian byte order. The following diagram should clarify this further.

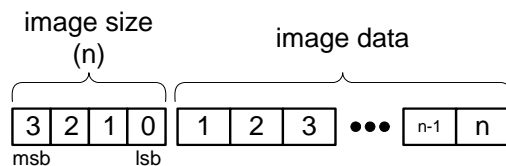


Image Repository

Images uploaded to the ECHO SSL Gateway server are retained locally in a temporary holding area. The images will be forwarded to image repository drop zone within 2 to 3 minutes. The Image Repository system will process the images, which will be made available for viewing approximately 15 minutes later.

Appendix A – ECHK Simulator Responses

Index	Host response
000	AUTH NUM 123-000
001	DECLINE CHECK 1 UNPAIDS (ALL) UNPAID AMT= 140PHN 800-947- 2954 XACT!
002	RE-PRESENTED CHKAUTH NUM 123- 001
003	NO ACH AUTH NUM 123-002
004	VOID ACCEPTED
005	RECORD NOT FOUND
006	MANAGER NEEDED OUT OF AREA
007	MANAGER NEEDED BANK STOP
008	DECLINE CHECK ACCOUNT CLOSED
009	DECLINE CHECK STLN/FRGD
010	DECLINE CHECK ID IS FLAGGED
011	DECLINE CHECK DUPLICATE CHECK
012	MANAGER NEEDED DAY LOC/NCHK=2
013	MANAGER NEEDED DAY GRP/NCHK=2
014	MANAGER NEEDED DAY ALL/NCHK=2
015	MANAGER NEEDED WIN LOC/NCHK=2
016	MANAGER NEEDED WIN GRP/NCHK=2
017	MANAGER NEEDED WIN ALL/NCHK=2
018	MANAGER NEEDED DAY LOC/AMT=50
019	MANAGER NEEDED DAY GRP/AMT=50
020	MANAGER NEEDED DAY ALL/AMT=50
021	MANAGER NEEDED WIN LOC/AMT=50
022	MANAGER NEEDED WIN GRP/AMT=50
023	MANAGER NEEDED WIN ALL/AMT=50
024	MANAGER NEEDED DAY LOC/CASH=30
025	MANAGER NEEDED DAY GRP/CASH=30
026	MANAGER NEEDED DAY ALL/CASH=30
027	MANAGER NEEDED WIN LOC/CASH=30
028	MANAGER NEEDED WIN GRP/CASH=30
029	MANAGER NEEDED WIN ALL/CASH=30
030	MANAGER NEEDED NUM PAYCHKS= 2
031	MANAGER NEEDED AMT PAYCHKS=1001

Index	Host response
032	MANAGER NEEDED CHECK TOO LARGE
033	MANAGER NEEDED TOO MUCH CASH
034	MANAGER NEEDED PAY CHK TOO BIG
035	ID IS NEEDED
036	ERROR IN ID
037	ERROR IN MICR
038	NO MICR
039	NO CANADIAN
050	BAD TERMINAL ID
051	UNDEF RULE SET
052	AGENCY DATA ERR
053	SERVICE CUT OFF
054	SYS ERR
055	SYS BUSY
056	PACKET ERROR
057	DECLINE CHECK YOUNG ACCOUNT 2 UNPAIDS (ALL) UNPAID AMT= 140ID IS FLAGGED PHN 800-947-2954 XACT! PHN 800-296-4430 OGDEN CHECK
058	DECLINE CHECK YOUNG ACCOUNT ID IS FLAGGED PHN 800-947-2954 XACT! PHN 800-296-4430 OGDEN CHECK PHN 888-481- 0757GLOBAL E TELECOMPHN 800- 230-5931MTNLAND COLLECTN
059	MANAGER NEEDED YOUNG ACCOUNT CHECK TOO LARGE DAY LOC/AMT=425 DAY LOC/CASH=316WIN LOC/AMT=425 WIN LOC/CASH=316
060	DECLINE CHECK CUSTOMER STOP
061	DECLINE CHECK STORE STOP
062	DECLINE CHECK AGENCY STOP
063	DECLINE CHECK CHECK STOP
064	NO SUCH ISSUER
065	ISSUER UNAVAIL
066	ROUTING ERROR
067	AUTH NUM 123-999
068	AUTH NUM 123- 999KEEP CHECK
069	ACCEPTED
070	BATCH CLOSED
071	BATCH NOT AVAIL
072	NO ACH 123-456

Index	Host response
073	NO ACH
074	ABA IS NON-ACH
075	UNKNOWN TERMINAL
076	PACKET ERROR ABA IS NON-ACH
077	PACKET ERROR RROR IN MICR
078	SYSTEM ERROR PACKET TYPE ERR
100	<warn/decl msg> ACCOUNT CLOSED
101	<warn/decl msg> AMT PAYCHKS
102	<warn/decl msg> CHECK TOO LARGE
103	<warn/decl msg> DAY ALL/AMT
104	<warn/decl msg> DAY ALL/CASH
105	<warn/decl msg> DAY ALL/NCHK=2
106	<warn/decl msg> DAY GRP/AMT
107	<warn/decl msg> DAY GRP/CASH
108	<warn/decl msg> DAY GRP/NCHK=2
109	<warn/decl msg> DAY LOC/AMT
110	<warn/decl msg> DAY LOC/CASH
111	<warn/decl msg> DAY LOC/NCHK=2
112	<warn/decl msg> HAS STOP PAY
113	<warn/decl msg> ID IS FLAGGED
114	<warn/decl msg> NUM PAYCHKS
115	<warn/decl msg> OUT OF AREA
116	<warn/decl msg> PAY CHK TOO BIG
117	<warn/decl msg> STLN/FRGD
118	<warn/decl msg> TOO MUCH CASH
119	<warn/decl msg> WIN ALL/AMT
120	<warn/decl msg> WIN ALL/CASH
121	<warn/decl msg> WIN ALL/NCHK=2
122	<warn/decl msg> WIN GRP/AMT
123	<warn/decl msg> WIN GRP/CASH
124	<warn/decl msg> WIN GRP/NCHK=2
125	<warn/decl msg> WIN LOC/AMT
126	<warn/decl msg> WIN LOC/CASH
127	<warn/decl msg> WIN LOC/NCHK=2

Index	Host response
128	ABA IS NON-ACH
129	ACCEPTED
130	ACCOUNT AUTHED
131	ACCOUNT MISMATCH
132	ACCOUNT PROBLEM
133	AGENCY DATA ERR
134	AGENCY PROBLEM
135	AGENCY UNKNOWN
136	AMOUNT MISMATCH
137	AUTH NUM 123-003
138	AUTH NUM 123-004
139	AUTH NUM 123-005
140	AUTH NUM 123-006KEEP CHECK
141	BATCH CLOSED
142	BATCH NOT AVAIL
143	DECLINE CHECK
144	DECLINE CHECK ACCOUNT CLOSED SC
145	DECLINE CHECK CUM AMT TOO MUCH
146	DECLINE CHECK DUPLICATE CHECK
147	DECLINE CHECK INVALID ACCOUNT
148	DECLINE CHECK NO CANADIAN
149	DECLINE CHECK NON SUFF FUNDS
150	DECLINE CHECK TOO MANY CHECKS
151	DECLINE CHECK UNPAID CHECKS
152	DUP TRANSACTION
153	END OF BATCH
154	FS CARD ERROR
155	ID AUTHORIZED
156	ID IS NEEDED
157	ID-NO PAYRL AUTH
158	INVALID PACKET
159	INVALID PASSWORD
160	INVALID REVERSAL
161	INVALID SERVICE
162	INVALID TRANSACT
163	ISSUER UNAVAIL
164	MANAGER NEEDED RE-PRESENTED CHK
165	NCIS NOT AVAIL
166	NO ACH SC
167	NO ACK AUTO-REV
168	NO CONNECT V3PY
169	NO CONNECT VACQ
170	NO MICR
171	NO PAYROLL
172	NO ROOM FOR AUTH
173	NO SUCH ISSUER
174	NOT PAYROLL ACCT
175	ON NEW BATCH
176	PACKET ERROR
177	PACKET ERROR ABA IS NON-ACH
178	PACKET ERROR BAD TERM LOC FLD
179	PACKET ERROR ERROR IN MICR

Index	Host response
180	PACKET ERROR INVALID FOR ACH
181	PACKET ERROR INVALID TERM ID
182	PACKET ERROR NO ACCT NUMBER
183	PACKET ERROR NO CHECK NUMBER
184	PACKET ERROR NO ECHO FIELD
185	PACKET ERROR NO RAW MICR
186	PACKET ERROR NOT ECHK PACKET
187	PAYROLL NEEDS ID
188	RECORD NOT FOUND
189	ROUTING ERROR
190	SCHK NOT AVAIL
191	SERVICE CUT OFF
192	SITE NOT SETUP
193	SYS BUSY
194	SYS ERR
195	SYSTEM ERROR
196	SYSTEM ERROR INVALID RESPONSE
197	SYSTEM ERROR INVALID SITE NUM
198	SYSTEM ERROR INVALID TERM ID
199	SYSTEM ERROR NO ECHO FIELD
200	SYSTEM ERROR PACKET TYPE ERR
201	SYSTEM ERROR SITE NOT SETUP
202	TIMED OUT
203	TIMED OUT RETRY
204	UNASKED REVERSAL
205	UNDEF RULE SET
206	UNKNOWN ACQUIRER
207	UNKNOWN MERCH
208	UNKNOWN RESPONSE
209	UNKNOWN SERVICE
210	UNKNOWN TERMINAL
211	UNPAIDS ON ACCT
212	VISA NOT AVAIL
213	VOID REFUSED
214	DECLINE CHECK
215	DECLINE CHECK OUT OF AREA
216	DECLINE CHECK HAS STOP PAY
217	DECLINE CHECK ACCOUNT CLOSED sc
218	DECLINE CHECK SC
219	INVALID PACKET
220	ACQ PROC SAYS NO RAW MICR
221	ACQ PROC SAYS ERROR IN MICR
222	ACQ PROC SAYS NO CHECK NUMBER
223	ACQ PROC SAYS NO ACCT NUMBER

Index	Host response
224	ACQ PROC SAYS ABA IS NON-ACH
225	ACQ PROC SAYS BAD TERM LOC FLD
226	SYSTEM BUSY
227	ACQ PROC SAYS NO ECHO FIELD
228	ACQ PROC SAYS INVALID TERM ID
229	ACQ PROC SAYS INVALID SITE NUM
230	ACQ PROC SAYS SITE NOT SETUP
231	SYSTEM ERROR PACKET TYPE ERR
232	ACQ PROC SAYS INVALID RESPONSE
233	UNKNOWN ACQUIRER
234	UNKNOWN MERCH
235	AGENCY UNKNOWN
236	NO SUCH ISSUER
237	ISSUER UNAVAIL
238	ROUTING ERROR
239	SYSTEM ERROR

Appendix B – Troubleshooting Q & A

The following Q&A is based on actual events.

- Q:** I put <STX> and <ETX> around the packet data. Why isn't it working?
- A:** This has actually happened. A developer not familiar with ASCII control codes literally inserted "<", "S", "T", "X", ">", and "<", "E", "T", "X", ">" into the transaction data. <STX> and <ETX> are ASCII control codes. <STX> is <start of text>, which is 0x02 (hex) or simply a decimal 2. <ETX> is <end of text>, which is 0x03 (hex) or a decimal 3. In C string notation, the packet would look like "\002...request packet...\003".
- Q:** (version 1) I'm getting a good host response, but you say that the transaction log on the host side doesn't look right.
- A:** Yes. The transaction log shows that you are sending in a trailing <LRC> character. Please reread the appropriate section on how to format the transaction properly (see SPKT Protocol and ECHK and ECHK Simulator Protocols).
- Q:** (version 2) I'm getting a good host response, but you say that the transaction log on the host side doesn't look right.
- A:** Yes. The transaction log shows that you are sending what appears to be a carriage return character (0x0D, 13₁₀) after the trailing <ETX>. I know from our previous conversations that you are using C# (.NET). You are probably using the **WriteLine** member function to send transaction data. **WriteLine** sends a line-end character at the end of the transaction data. Instead, use **Write**, which will not send a line-end character.
- Q:** Using the ECHK simulator, I've sent several transactions and all are getting the same response. Some of them should have been rejected by the host. What is wrong?
- A:** If you want a different response from the from the ECHK simulator, you will need to vary the dollar amount of the transactions. See Appendix A – ECHK Simulator Responses. The ECHK simulator performs minimal validation on the transaction packet and is really only useful for testing how your application responds to the different responses that the real host will send.