



National Check Network

Technical Documents Overview

730 Paseo Camarillo
Camarillo, CA 93010
(800)-280-7677

www.NationalCheckNetwork.net

Division of



Table of Contents

INTRODUCTION.....	2
NOTICE OF PROPRIETARY INFORMATION	2
INTERNET TRANSACTIONS OVERVIEW.....	3
INETGATEWAY METHOD.....	3
SSL GATEWAY METHOD	3
FRAME RELAY TRANSACTIONS OVERVIEW.....	3
TECHNICAL DOCUMENTS.....	3
NCN SPKT HOST PROTOCOL.....	3
SECURENCIS.EXE	4
SECURENCIS PROGRAM OVERVIEW	4
DEVELOPERS REGISTRATION FORM.....	4
ECHO SSL GATEWAY DEVELOPER’S USER GUIDE.....	4
NCN COMPLIANCE TEST SUITE.....	4
NCN ECHK HOST PROTOCOL.....	4
NEGFILE SPECIFICATION.....	4
NCN TLOG GUIDE FOR ECC	5
CHECK CONVERSION TERMINAL SPECIFICATIONS (CM3000 TERMINAL).....	5

INTRODUCTION

This document gives a brief description of each of the documents and programs listed on the [Technical Documentation for Developers](http://www.NationalCheckNetwork.net) page on the www.NationalCheckNetwork.net website.

Notice of Proprietary Information

Information contained herein is subject to change without notice and does not constitute a commitment on the part of Electronic Clearing House, Inc. (**ECHO**). Except for use by customers for obtaining **ECHO** products and services, 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 **ECHO**. 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].

©2006 Electronic Clearing House, Inc (**ECHO**). All rights reserved.

The following are copyrights of their respective companies or organizations:
ECHO[®], **MerchantAmerica**SM, **NCN**[®] and **XpressCheX**[®] are all property of Electronic Clearing House, Inc. (**ECHO**).

INTERNET TRANSACTIONS OVERVIEW

Several of the following documents detail the formats required to conduct transactions with the NCN verification system via an Internet connection. There are two methods that can be used to send transactions over the Internet to NCN using the SPKT protocol. Each method uses a different gateway application at NCN for handling the transactions with different encryption methods and connection requirements. The two methods/gateways are the **Inetgateway** and the newer **SSL Gateway**.

Inetgateway Method

The Inetgateway is a gateway service that NCN will be made obsolete in the near future. No new connections to this gateway should be developed. The Inetgateway was NCN's original Internet transaction method. It uses Blowfish encryption, a method that uses passphrases. In order to connect to NCN through the Inetgateway, NCN requires a static IP address of the computer attempting to connect to NCN. NCN will issue port numbers that a program can use to open a socket connection to the Internet Gateway machine at NCN. Each port issued will accept transactions for a specific Site number coming from one specific IP address. Therefore, more than one port may be required for conducting transactions on multiple Sites or for connecting to NCN from multiple IP addresses. All Internet transactions must be encrypted using our Blowfish encryption logic by using either our **SecureNCIS.exe** program or by embedding the same encryption logic into the programs that connect to NCN.

SSL Gateway Method

The SSL Gateway is designed to be a simpler and more standardized method for connecting to NCN using open SSL encryption. This gateway does not require static IP addresses or dedicated ports. As long as the packet conforms to the SPKT protocol and connection using open SSL, any device or program can communicate and send transactions to NCN. For more information on this gateway, refer to the *ECHO SSL Gateway Developer's User Guide*.

FRAME RELAY TRANSACTIONS OVERVIEW

Like Internet transactions, Frame Relay using TCP/IP protocols may be used for sending transactions to the NCN verification system. Unlike Internet transactions, Frame Relay does not require encryption. Several of the following documents detail the formats required to conduct transactions. NCN maintains connections with several carriers such as AT&T, Sprint, Qwest, MCI, and Touch America.

TECHNICAL DOCUMENTS

NCN SPKT Host Protocol

In order to conduct a check verification transaction, a point-of-sale (POS) device must send information to the NCN verification system in a single packet of information called a **request packet**. The NCN system evaluates the **request packets** and then composes and sends a single packet of information back to the point of sale in a **response packet**. This document details the formats of these request and response packets based on a proprietary format developed by NCN called the **SPKT** protocol. The **SPKT** protocol gets its name from the fact that all of these request packets have a field in them containing the letters **SPKT** and was originally given the name "Single Packet Transactions".

This document details all of the packet formats necessary to conduct various forms of check **verification** and **Electronic Check Conversion (ECC)** type transactions in this **SPKT** format. The **SPKT** format is the same for all transactions regardless of the communication method used. Internet, dial-up, and Frame Relay use the same **SPKT** formats described in this document. There is another more involved specification to conduct **ECC** type transactions called the **ECHK** protocol which provides host-based batching and additional services such as the VISA POS Check Service which is detailed below in another Document.

SecureNCIS.exe

The SecureNCIS.exe program is a proxy server that provides two types of services for NCN clients: Encryption and Multiplexing. This program can be used to satisfy the requirement of encrypting all Internet transactions with the NCN System via the Inetgateway method. *The Inetgateway is a gateway service that NCN will sunset in the near future. No new connections to this gateway using the SecureNCIS program should be developed.*

SecureNCIS Program Overview

This document gives a brief overview of how the SecureNCIS program works in providing encryption and multiplexing capabilities for Internet transaction to the NCN using the Inetgateway method. *The Inetgateway is a gateway service that NCN will sunset in the near future. No new connections to this gateway using SecureNCIS should be developed.*

Developers Registration Form

This document is the starting point for all developers wishing to certify an application on the NCN System. This form starts the process and allows NCN to begin the paperwork needed for a formal certification.

ECHO SSL Gateway Developer's User Guide

This document provides information on how to connect to the ECHO open SSL Server to provide a secure tunnel for transactions coming across the Internet. The SSL gateway provides support for both SPKT and ECHK formatted transactions as well as Image Transfer for Electronic Check Conversion (POP) transactions.

NCN Compliance Test Suite

This document is list of all the testing required to certify a Verification and/or an ECC application with the NCN System using the SPKT or ECHK protocols.

NCN ECHK Host Protocol

This document explains the new **ECHK** protocol that is an enhancement to the **SPKT** protocol for ECC transactions. The **ECHK** protocol was originally designed for the Visa POS Check Service. These packets can be used for ECC transactions without participating in the VISA Check program as well as for the verification-only service. These transactions work very similarly to conventional **ECC SPKT** transactions with additional safeguards and features. **ECHK** transactions have several new features and fields specifically designed to enhance electronic check processing.

Negfile Specification

This document explains the format of the data file called the “**Negfile**.” The **Negfile** is the data file sent to the NCN verification system containing details on each returned check from the check recovery or collection system maintained by the contributing agency/customer. This file contains multiple records, with each record representing an individual check. Each record also includes a control command, dictating the action (addition or deletion) to be taken. A file may contain any number of individual records.

NCN Tlog Guide for ECC

NCN Transaction Logs (Tlogs) contain transactional information on check verification, electronic check conversion (ECC), batch results, and other requests from the POS device. This document describes the TLOG format available from NCN and identifies best practices for using these logs. The TLOG format is used to record all transaction requests arriving at NCN in the SPKT format and their responses.

Transactions processed using the ECHK Host Protocol also generate TLogs, but not all of the information that is part of the ECHK protocol is passed into the TLogs. The TLogs are generally referred to as the “Transaction Log.”

Check Conversion Terminal Specifications (CM3000 Terminal)

This document describes the functionality of the first ECC program written by NCN (formerly known as RMRS-Rocky Mountain Retail Systems) in SPKT format for the IVI CheckManager 3000 Terminal. It is provided as an educational tool to enable others to create a check conversion program on any point of sale device which functions in substantially the same way as the application initially developed by NCN for the CheckManager CM3000 Terminal. The specification emphasizes the basic functions required for Check Conversion, and includes minimal specific implementation details. This document does not serve as an instruction manual for exactly how an ECC application should perform as this document was written in 1998. However, it does provide a basic framework for the functionality initially developed on a POS device when implementing the **SPKT** protocol for ECC transactions.