Alfa & Ariss
Network Security Solutions

SIP2 Extensions for A-Select

The Netherlands Public Library Association has started the pilot “Landelijk Lenen”. Within this pilot A-Select is used as authentication middleware.

This document describes how A-Select uses SIP2 messages and how they are interpreted.
To be sure to offer compatibility with A-Select, SIP2 back-end suppliers should verify that the used SIP2 messages are interpreted the same way. This, because SIP2 is not that closed and it offers too many possibilities to define a ‘dialect’ within SIP2.

Besides the standard SIP2 messages used by A-Select, there is a wish to use the SIP2 back-end as a user database for A-Select. A-Select is able to connect with most popular databases and has therefore defined a database layout for these databases.
Because SIP2 does not meet the requirements set by A-Select to use it as an interface to the database, an extension to the SIP2 protocol is defined in this document.
SIP2 back-end suppliers should implement this extension to be able to offer a compatible SIP2 back-end as user database for A-Select.

Author: Alfa & Ariss bv
Version: 1.1
Date: 8/26/2004 10:46 AM
Classification: PUBLIC

Revision history

Version	Change	Responsible	Date
V1.0	Initial release	Alfa & Ariss	6/17/2004
V1.1	- Chapter 2.1.2 The critical field description of the patron status field was updated. - Chapter 3.1 The layout table of the user database did refer to the 'aselect<authentication name>Enabled' item. This is not correct and therefore changed to 'aselect<authentication name>Registered'.	Alfa & Ariss	8/26/2004

Introduction

The intent of this document is to provide software developers with information required to develop and test an interface between an A-Select system and a so-called Automated Circulation System (ASC). The interface protocol required is 3M SIP V2.00 (SIP2). SIP is a standard that is defined in [Ref SIP2 descr] and [Ref SIP2 dev].

Within this document the ASC is from now on referred to as SIP2 Server.

A SIP interface is required between an A-Select system and SIP2 Server to provide the exchange of valuable information about authentication and database records.

This document provides insight into what software needs to be implemented in the SIP2 Server to be compliant with A-Select. This document does not make any statements about how SIP2 works. It is the responsibility of the software engineer to have knowledge about SIP2.

Table of Contents

Table of Figures

1. Overview of A-Select

This chapter gives you an overview about the A-Select system. It is recommended to read this chapter because you will be able to understand better why and how SIP2 messages are used by A-Select.

The A-Select Authentication System (in short A-Select) is a single sign-on system for authentication of users in a Web environment. A-Select is a framework where users can be authenticated by several means with Authentication Service Providers (AuthSP's).
Several AuthSP's have been implemented already. Among them, very strong AuthSP's like ABN AMRO Internet Banking, Rabobank Internet banking and Mobile Phone authentication are available. But also more commonly used AuthSP's are available like username/password for RADIUS and LDAP back-ends.

Figure 1 gives a schematic overview how A-Select works and the components used within A-Select.

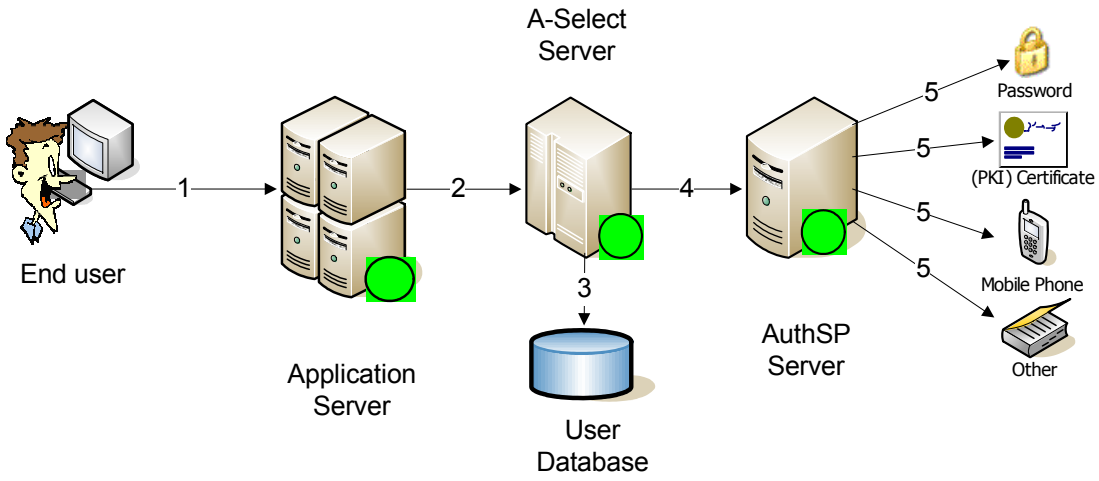

Figure 1: A-Select overview

1. End users will browse to an URL for accessing an application. The application is secured with A-Select and needs authentication.
2. The application concludes there is no valid authentication session. Therefore the user's browser is redirected to the URL of the A-Select Server for authentication of the user.
3. The user enters his/her user-id in a form presented by the A-Select Server. Now the A-Select Server checks its user database to verify that this is a known user.

Besides that, the user database provides information about the authentication methods the user is allowed to use.

4. Based on the data retrieved from the user database, the user is presented a selection form from which it may choose an authentication method he/she wishes to use. Based on the chosen authentication method, the user's browser is redirected to an AuthSP Server.
   The AuthSP Server presents a form (if needed for that authentication method) to gather user specific information needed for authentication.
5. All information needed is offered to the authentication back-end to verify the users identity. The authentication back-end sends its results tot the AuthSP Server that will pass the results back to the A-Select Server. If authentication was successful, the user is redirected back to the application.

More information regarding A-Select can be found in [Ref A-Select].

2. Authentication with SIP2

A-Select is built up of modules to be able to serve all different types of infrastructures. To be able to integrate with authentication back-ends already in use within organizations, A-Select has modules for widely used authentication back-ends.
The Netherlands Public Library Association uses however different authentication back-ends. Most of these back-ends support the use of the SIP2 protocol. Because this module was not available yet in A-Select, the SIP2 connector is recently added to A-Select.

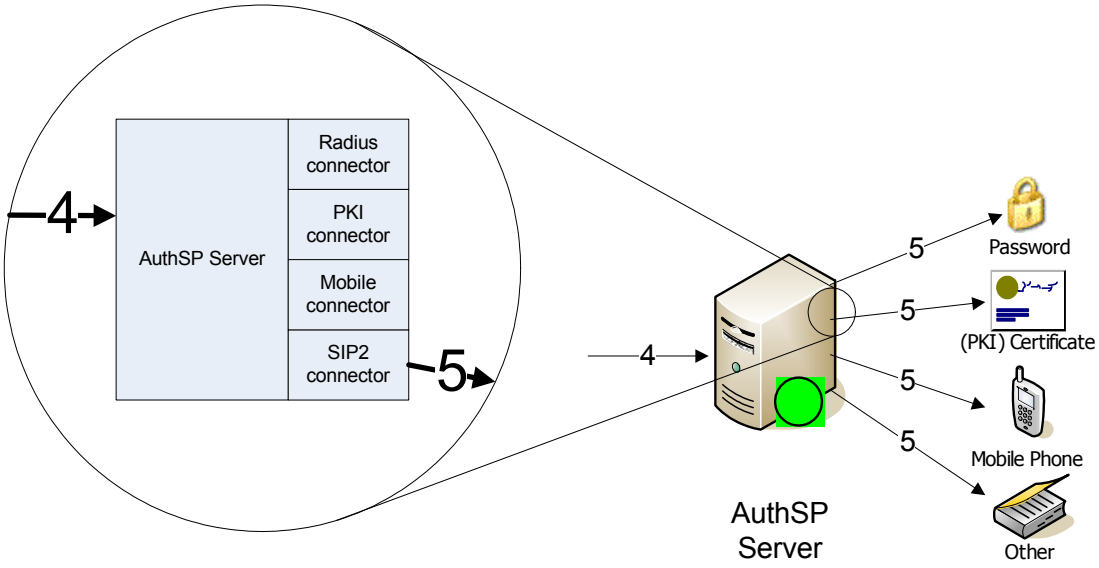

Figure 2: SIP2 authentication

The implementation of the A-Select SIP2 connector is based on the standard 'Patron Status request, Message 23' and 'Patron Status Response, Message 24'.
This chapter describes only how 'Patron Status" messages are interpreted. The initial connection setup between A-Select and SIP2 Server is described in chapter 4.

2.1. Message definition

This section describes the SIP2 messages that are sent from the AuthSP Server to the SIP2 Server. Additional information pertaining to error detection, checksums and sequence numbers are described in chapter 5.

2.1.1. Patron Status Request, Message 23

This command message is initiated by the AuthSP Server when it requires information about a patron's authenticity from the SIP2 Server. The SIP2 Server must respond to this command with a Patron Status Response, Message 24.

23<language><transaction date><institution id><patron identifier><terminal password><patron password>

Field	ID	Format
Language		3-char, fixed length required field
transaction date		18-char, fixed length required field: YYYYMMDDZZZZZHHMMSS
institution id	AO	variable-length required field
patron identifier	AA	variable-length required field
terminal password	AC	variable-length required field
patron password	AD	variable-length required field

Critical field description:

Field name	Description of Usage
patron identifier	The AuthSP Server fills this field with the user id.
patron password	The AuthSP Server did prompt the user for its password. The password is sent to the SIP2 Server in this field.

2.1.2. Patron Status Response, Message 24

The SIP2 Server must send this message in response to a Patron Status Request, Message 23.

24<patron status><language><transaction date><institution id><patron identifier><personal name><valid patron><valid patron password><currency type><fee amount><screen message><print line>

Field	ID	Format
patron status		14-char, fixed length required field
Language		3-char, fixed length required field
transaction date		18-char, fixed length required field: YYYYMMDDZZZZZHHMMSS
institution id	AO	variable-length required field
patron identifier	AA	variable-length required field
personal name	AE	variable-length required field
valid patron	BL	1-char, **optional** field: Y or N
valid patron password	CQ	1-char, **required** field: Y or N
currency type	BH	3-char, fixed length optional field
fee amount	BV	variable-length optional field
screen message	AF	variable-length optional field

print line	AG	variable-length optional field

Critical field description:

Field name	Description of Usage
patron identifier	Must contain the identical information contained in the initiating Patron Status Request.
valid patron	A-Select (AuthSP) strongly encourages the use of this field. This information allows the AuthSP Server to determine if the user is known/allowed to authenticate against the SIP2 Server. If this field is not present, the AuthSp Server will take a look at the 'patron status' field.
valid patron password	This field must contain 'Y' or 'N' to indicate if the patron password was correct.
patron status	Only if the field 'valid patron' is not present, the AuthSP Server will look at the first of 14 characters in this field. If the first character is 'Y', the user is blocked for any reason. So if the SIP2 Server does not support the 'valid patron' field, the first character in 'patron status' should be 'Y' to indicate that it is an unknown/blocked user.

3. UDB with SIP2

A-Select is built up of modules to be able to serve all different types of infrastructures. To be able to integrate with user databases already in use within organizations, A-Select has modules for widely used user databases (UDB's).
For every supported database, A-Select has defined a layout that is needed by A-Select to use this database.

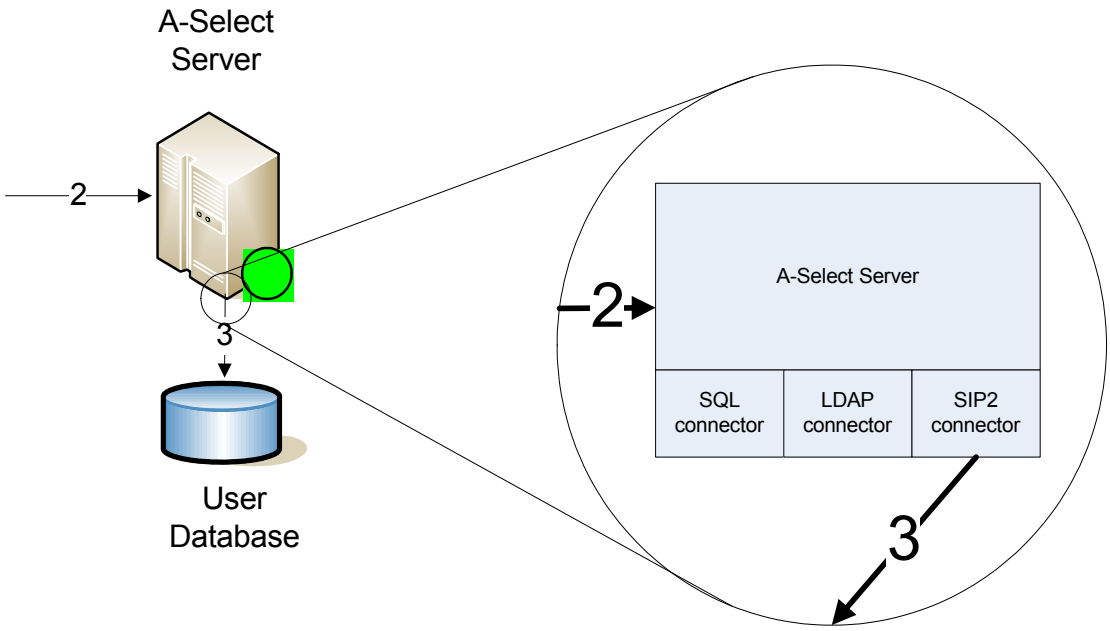

Figure 3: SIP2 user database

3.1. Global user database layout

The user database used within A-Select must be independent of the supported authentication back-ends used within an organization. This means that a SIP2 user database has in fact no relation with a SIP2 authentication back-end.
For every user there must be a record in the database with the following information:

Item	Description
`aselectAccountEnabled`	Tells A-Select if this user is allowed to authenticate with A-Select.
For every supported authentication back-end:	An organization using A-Select may choose to support more than one authentication method[1]. Depending on the organization which authentication methods are supported, there may be more than one authentication method.
`aselect`<authentication name>`Registered`	Tells A-Select if the user is allowed to use this specific authentication method.
`aselect`<authentication name>`UserAttributes`	Tells A-Select which attributes should be used for this user to authenticate.

[1] Since A-Select supports different levels of authentication, organizations may choose to support 'weak' authentication methods and 'strong' authentication methods for different applications.

If an organization is using the following authentication back-ends for example:

- Radius password
- PKI Certificate
- Mobile Phone

The database should contain the following information for every user:

aselectAccountEnabled	"TRUE" or "FALSE"
aselectRadiusRegistered	"TRUE" or "FALSE"
aselectRadiusUserAttributes	user id as present in radius back-end (may differ from initial user id within A-Select).
aselectPkiRegistered	"TRUE" or "FALSE"
aselectPkiUserAttributes	<certificate blob>
aselectPhoneRegistered	"TRUE" or "FALSE"
aselectPhoneUserAttributes	<mobile phone number of this user>

Note: Currently the Libraries involved within the "Landelijk Lenen" pilot only use the SIP2 authentication back-end as described in chapter 2.

3.2. SIP2 UDB lay-out

Since the Netherlands Public Library Association uses its library back-end as user database, which is the same as the authentication back-end, there is chosen to use SIP2 also as protocol for connecting to the database.

To use the SIP2 back-end as A-Select user database, it must be able to provide A-Select with the information as described in the previous chapter.
During the pilot of "Landelijk Lenen" we assume that libraries do only offer a SIP2 authentication back-end to their users. This means that the user database must be able to provide the following information:

Attribute name	Type	Value
aselectAccountEnabled	Character	"TRUE" or "FALSE"
aselectSip2Registered	Character	"TRUE" or "FALSE"
aselectSip2UserAttributes	Character	<patron identifier[2]>

Note: Keep in mind that an organization may choose to offer more/different authentication methods in the future. In that case the user database should contain information for these authentication methods also.

[2] The 'patron identifier' which should be used in the SIP2 authentication process as described in chapter 2.

3.3. Message definition

This section describes the SIP2 messages that are sent from the A-Select Server to the SIP2 Server (user database). Additional information pertaining to error detection, checksums and sequence numbers are described in chapter 5.
This chapter describes only how the extension should be used and interpreted. The initial connection setup between A-Select and SIP2 Server is described in chapter 4.

Since SIP2 does not support messages to retrieve data from the back-end database other than data as described within SIP2, there is chosen to extend the SIP2 protocol with a message that is aware of the data A-Select want to retrieve from the SIP2 Server.
There is chosen to extend an existing SIP2 message instead of defining a complete new message.
The standard 'Patron Status request, Message 23' combined with the 'Patron Status Response, Message 24' seemed to be the best message to use for this extension.

3.3.1. Patron Status Request, Message 23 extension

This command message is initiated by the A-Select Server every time it requires information about a patron regarding A-Select.
The SIP2 Server (database) must respond to this command with the Patron Status Response, Message 24 extension as described in chapter 3.3.2.

The extension relies only to the values of the standard fields used in the standard Patron Status Request. There are no fields added to this message.
It is not possible to retrieve all A-Select information at once from the SIP2 Server, therefore a separate message is initiated for every needed attribute.

23<language><transaction date><institution id><patron identifier><terminal password><patron password>

Field	ID	Format
Language		3-char, fixed length required field
transaction date		18-char, fixed length required field: YYYYMMDDZZZZZHHMMSS
institution id	AO	variable-length required field
patron identifier	AA	variable-length required field
terminal password	AC	variable-length required field
patron password	AD	variable-length required field

Critical field description:

Field name	Description of Usage
Institution id	The A-Select Server wants to let you know, it wants to read or write in the database. The field contains one of the following values: "<aselect>aselectread</aselect>" or "<aselect>aselectwrite</aselect>"[3]
patron identifier	The A-Select Server fills this field with the user id. This is the user, which A-Select needs some additional information for.
terminal password	This field tells which A-Select Specific attribute it wants to read/write. The field contains one of the following values[4]: "<aselect>aselectAccountEnabled</aselect>" or "<aselect>aselectSip2Registered</aselect>" or "<aselect>aselectSip2UserAttributes</aselect>"
patron password	Since A-Select does not want to authenticate a person here, no password is known yet. This field is sent but the password will be zero length.

[3] Currently A-Select only wants to retrieve data from the SIP2 Server database. In the future A-Select may want to set a value of an A-Select specific attribute.

[4] As stated in chapter 3.2, there might come more attributes in the future.

3.3.2. Patron Status Response, Message 24 extension

The SIP2 Server must send this message in response to a Patron Status Request, Message 23 extension.
The extension relies only to the values of the standard fields used in the standard Patron Status Request. There are no fields added to this message.

24<patron status><language><transaction date><institution id><patron identifier><personal name><valid patron><valid patron password><currency type><fee amount><screen message><print line>

Field	ID	Format
patron status		14-char, fixed length required field
Language		3-char, fixed length required field
transaction date		18-char, fixed length required field: YYYYMMDDZZZZZHHMMSS
Institution id	AO	variable-length required field
patron identifier	AA	variable-length required field
personal name	AE	variable-length required field
valid patron	BL	1-char, **required** field: Y or N
valid patron password	CQ	1-char, optional field: Y or N
currency type	BH	3-char, fixed length optional field
fee amount	BV	variable-length optional field
screen message	AF	variable-length **required** field
print line	AG	variable-length optional field

Critical field description:

Field name	Description of Usage
Institution id	Must contain the identical information contained in the initiating Patron Status Request extension: “<aselect>aselectread</aselect>” or “<aselect>aselectwrite</aselect>”
patron identifier	Must contain the identical information contained in the initiating Patron Status Request.
valid patron	This field should contain the value “Y” to indicate that the user is known in the SIP2 server database.
screen message	This field should contain the value of the attribute asked for in the Patron Status Request extension (terminal password) described in detail further on: “<aselect>[value]</aselect>

Additional information for the screen message field:

The following table describes more in detail how the 'screen message' field should be filled. Since support for writing to the SIP2 Server database is not yet required this table only applies to <aselect>aselectread</aselect> requests.

Patron Status Request 'terminal password' value	Patron Status Response 'screen message' value
<aselect>aselectAccountEnabled</aselect>	"<aselect>TRUE</aselect>" or "<aselect>FALSE</aselect>"
<aselect>aselectSip2Registered</aselect>	"<aselect>TRUE</aselect>" or "<aselect>FALSE</aselect>"
<aselect>aselectSip2UserAttributes</aselect>	Must contain the user attribute needed for SIP2 authentication as described in chapter 2. (mostly identical to the 'patron identifier') "<aselect>[user_id]</aselect>"
<aselect>[unknown]</aselect>	If the request contains an unknown value, the SIP2 Server should return an empty string but with 'tags': <aselect></aselect>

4. Communication mechanisms

The A-Select and AuthSP Server can be connected to the SIP2 server in two ways. The connection is implemented by using sockets or TELNET with TCP/IP.
Since database and authentication functionality are strictly separated within A-Select, there are in fact two connections when using the SIP2 Server for both user database and authentication back-end.

At startup of the A-Select system, all needed connections are set up and kept alive till the A-Select system is shut down. All messages needed for A-Select to work are sent over these existing connections.

4.1. TELNET Connection

The A-Select system supports establishing a connection between the A-Select system and the SIP2 Server by means of setting up a TELNET session.
The A-Select system can be configured to set the necessary parameters needed to establish the socket connection (IP address and port) as well as to login to the SIP2 Server's computer.

The A-Select system implements the TELNET protocol set up a connection with the SIP2 Server. Within this protocol the A-Select system is able to pass and receive parameters to the server computer to login.
After a successful TELNET session has been set up, the A-Select system will send a 'SC Status, Message 99'. The SIP2 Server should respond with a 'ACS Status, Message 98'.

4.1.1. Message passing scenario

This schema shows the message-passing scenario at startup of the A-Select system with TELNET connection to the SIP2 Server.

A-Select System	SIP2 Server
1. Establish TELNET connection	
	2. Establish TELNET connection
	3. Login script (expects)
4. Login script (sends):	. login
. [username]	. password
. [password]	. granted access
. receive login ok	
5. SC Status (99)	
	6. ACS Status (98)

The point 3 and 4 login script steps take place to log in to the SIP2 Server computer and can be configured to handle any character strings needed for this login.

4.2. Socket Connection

The A-Select system supports establishing a socket connection to the SIP2 Server, allowing the connection to the SIP2 Server to be over the network but eliminating the need for a TELNET session and its remote login.
The A-Select system can be configured to set the necessary parameters needed to establish the socket connection (IP address and port).
Currently A-Select always sends the 'Login, Message 93' as the first message sent over the connection; it contains a user name and password (configurable within the A-Select system) which establishes the A-Select system as a valid user of the service provided by the SIP2 Server.
After a successful response 'Login Response, Message 94' the A-Select system will send a 'SC Status, Message 99'. The SIP2 Server should respond with a 'ACS Status, Message 98'.

4.2.1. Message passing scenario

This schema shows the message-passing scenario at startup of the A-Select system with Sockets connection to the SIP2 Server.

A-Select System	SIP2 Server
1. Establish Socket connection	
	2. Establish Socket connection
3. Login (93) with: user id and password	

	4. Login Response (94) with:
	if (user id and password OK)
	ok = 1
	else
	ok = 0

5. SC Status (99)	
	6. ACS Status (98)

5. Additional information about the SIP2 connection

This chapter describes all additional features of SIP2 that are implemented in the A-Select system.
These features apply to both the user database and the authentication backend connection.

date_time_sync
The date time synchronization between the A-Select system and the SIP2 Server is not implemented by A-Select.

error_detection
The A-Select system can be configured to perform error detection. When error detection is enabled, sequence numbers and checksums are added as fields in SIP2 messages.
When error detection is enabled, the A-Select system also expects that sequence numbers and checksum fields are present in the response from the SIP2 Server. Sequence numbers and checksums are verified within the A-Select system. If the A-Select system receives a message with a sequence number not expected, the A-Select system will discard the response and wait for another. Invalid checksum fields will cause A-Select too send a ‘Request ACS Resend, Message 97’.

circ_tickle_interval
The A-Select system can be configured to use a circular tickle interval. With this option enabled the A-Select system will periodically send ‘SC Status, Message 99’ to make sure the SIP2 Server is still alive.

retries_allowed
The A-Select system can be configured to work with retries.

timeout_period
When a message is sent from the A-Select system to the SIP2 Server, the A-Select system waits for a response until a timer expires. If the timer expires without a response, the message is re-transmitted, until the maximum number of tries is reached.

terminal_password
The A-Select system never makes use of the terminal password field in SIP2 messages.

request SC Resend, Message 96

The A-Select system has implemented the functionality if the SIP2 Server did ask for a resend. When receiving this message, the A-Select system will re-transmit its last message.

protocol version

The A-Select system will not check any protocol numbering version.

field_delimiter

The A-Select can be configured to use any character to delimit field.

6. Bibliography

[Ref A-Select] A-Select information,
http://aselect.surfnet.nl/

[Ref SIP2 descr] Standard Interchange Protocol description,
3M™ Standard Interchange Protocol
Document Revision 2.10, Updated September 17, 1998
75-0500-2589-1

[Ref SIP2 dev] Standard Interchange Protocol developer's guide,
3M Standard Interchange Protocol V2.00
Document Version 2.21, Updated June 7, 1999
78-6970-7216-9