Network Working Group
Request for Comments: XXXX
Category: Draft

Daniel Dworski
AAU
October 2024

Application Layer Protocol For ATMs

Status of This Memo

This document specifies a protocol used for the communication between ATMs and their central server. It is not any kind of standard.

Abstract

In this document the protocol is defined, which is meant for a save communication between the ATM and its central server. It will not include which encryption algorithms or standards are best for the communication, but define what information shall be transferred in order to minimize risk.

Table of Contents

Introduction

The ATM should minimize using valuable data when communication with the central server. In order to do so the protocol is session based. This means the server should be able to save a session key for every ATM which is registered to it.

Protocol Definition

There are three types of messages the ATM can send to the central server:

1. CREATE_SESSION_REQUEST
2. WITHDRAW_REQUEST
3. CLOSE_SESSION_REQUEST

Each one of them has the basic structure:
|Messagetype|Timestamp|ATM_ID|Session_ID|
Additionally, when requesting to create a session the number and pin of the entered card is being transferred. On the other hand, the WITHDRAW_REQUEST contains the amount of money the customer wishes to withdraw.

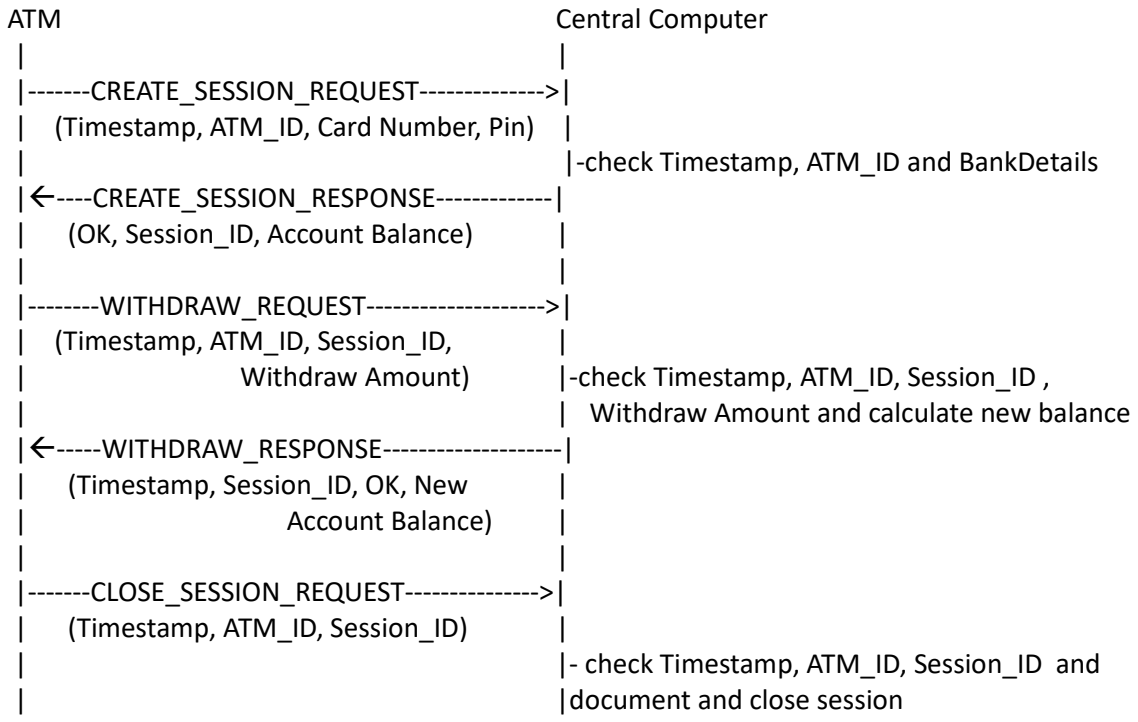
The server can only answer with two kinds of responses:

1. CREATE_SESSION_RESPONSE
2. WITHDRAW_RESPONSE

The basic structure of these responses is:
|Messagetype|Timestamp|Session_ID|Status|
Dependent on the status of the response an additional field containing the error message may be added. When successfully identifying the ATM and creating a session, its ID and the balance of the involved account will be added to the response. The WITHDRAW_RESPONSE only contains additionally the new balance of the account.

Not included is the encryption of the defined data, because this protocol only aims to minimize the critical communication between the ATM and the central server. The save encryption and decryption is the responsibility of the transport layer. Please make sure you apply an up-to-date encryption algorithm on the transport layer.

Visual Procedure Of The Protocol



Security Considerations

Considering there is no encryption algorithm or standard defined, make sure that the connection is End-to-end save. This document assumes the correct measures have already been made in the transport layer.

IANA Considerations

This protocol is not meant to be applied in the real world so no action is required by IANA.

References

RFC 3: Documentation Conventions

RFC Editor, "How to Write an RFC – A Tutorial", IETF-62, Minneapolis, MN, USA, March 2005. Available at: https://www.ietf.org/proceedings/62/slides/editor-0.pdf.