**Communication Protocol Version1.0**

Contents

Introduction 1

 Packet structure 2

Protocol 2

 Heartbeat 2

 Cipher 3

 Upgrade 4

 Restart 5

## Introduction

As the smart self-service equipment need to be deployed in different positions distributed around a city, this requires us to give a kind of communication way which can send request from smart equipment to the front-end aggregation server, as well as receive transaction result.

The architecture picture shows the comprehensive construction of application based on xml-UI framework.



### Packet structure

We define a common TCP/IP packet structure that comprises of three parts, the first is command code, the second is packet length, and the third is XML payload.

## Protocol

For convenience of communication, we utilize text message as content, and text message takes standard XML and JSON format to represent different type of stuff, such as array structure, string structure and so on.

### Heartbeat

Heartbeat is very important and plain-vanilla message which keeps client know if the front aggregation server is alive. If there is no valid heartbeat response coming from server, the client will prompt erroneous message to user.

Sample heartbeat message sent from client:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<TLS>**

**<counter>3</counter> <!-- global counter number to represent message from this client -->**

**<prscode>sanlogin</prscode> <!-- action of message -->**

**<terminalid>00000001</terminalid> <!-- the ID of equipment -->**

**<token>usjdfjksa75ks832okudsjd94877akjdua</token> <!-- the token of equipment -->**

**<branchno>test\_bank\_division</branchno> <!-- the alias of organization -->**

**<terminalstate>0</terminalstate> <!-- the state of equipment -->**

**<startid>1440743273124</startid> <!-- the startup time of equipment -->**

**<keyboardstate>1</keyboardstate> <!-- the state of embedded keyboard -->**

**<prtstate>1</prtstate> <!-- the state of embedded printer -->**

**<version>Unknown</version> <!-- the software version of equipment -->**

**</TLS>**

Sample heartbeat message come from aggregation server:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<TLS>**

**<retcode>0</retcode> <!-- response code, 0 is successful -->**

**<terminalid>00000001</terminalid> <!-- the ID of equipment -->**

**<okmsg>终端注册成功</okmsg> <!-- the content of successful response message -->**

**<errmsg/> <!-- the conent of erroneous response message -->**

**<restart>0</restart> <!-- the signal of restart equipment, 0 is none of restart -->**

**<changekey>0</changekey> <!-- the signal of update cipher key of keyboard, 0 is none of change -->**

**</TLS>**

### Cipher

There is a keyboard in client equipment, and this keyboard has encryption functionality. But the equipment need to download the latest and mutative encryption key from aggregation server when it’s brought up. We use another xml message to describe this type message.

Sample encryption key message sent from client:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<TLS>**

**<counter>3</counter> <!-- global counter number to represent message from this client -->**

**<prscode>downloadkey</prscode> <!-- action of message -->**

**<terminalid>00000001</terminalid> <!-- the ID of equipment -->**

**<token>usjdfjksa75ks832okudsjd94877akjdua</token> <!-- the token of equipment -->**

**<branchno>test\_bank\_division</branchno> <!-- the alias of organization -->**

**<terminalstate>0</terminalstate> <!-- the state of equipment -->**

**<startid>1440743273124</startid> <!-- the startup time of equipment -->**

**<keyboardstate>1</keyboardstate> <!-- the state of embedded keyboard -->**

**<prtstate>1</prtstate> <!-- the state of embedded printer -->**

**<version>Unknown</version> <!-- the software version of equipment -->**

**</TLS>**

Downloading message is like heartbeat message except prscode is ‘downloadkey’.

Sample downloading message come from aggregation server:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<TLS>**

**<retcode>0</retcode>**

**<terminalid>00000001</terminalid>**

**<okmsg>**

**{**

**"maKey": "01234789ABCDEF",**

**"masterKey": "01234789ABCDEF",**

**"workSecretKey": "01234789ABCDEF"**

**}**

**</okmsg> <!-- the content of successful response message -->**

**</TLS>**

Response message is a complex construction including XML and JSON. Aggregation server puts encryption keys into okmsg field, and encryption keys are constructed by JSON format based on {key:value}.

### Upgrade

This is about equipment software upgrade/downgrade requirement. As these equipment are distributed in different bank outlets, we cannot upgrade or downgrade software manually. So we will send software update message from aggregation server to all equipment, and those equipment will fetch designated software package to update after receiving upgrade/downgrade message.

Sample upgrade/downgrade message come from aggregation server:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<TLS>**

**<retcode>0</retcode>**

**<terminalid>0X12347890ABCDEF</terminalid>**

**<update>1</update> <!—signal of change, 0 is none of update, 1 is update-->**

**<updatefile> <!—path is software package url and md5 is result of package md5 caculating, version is software’s internal id-->**

**{**

**"path": "http://10.117.5.10/bankApp-upgrade.zip",**

**"version": "2.1",**

**"md5": "7f90530983ff438ff57dcf11ab342ba4"**

**}**

**</updatefile>**

**</TLS>**

### Restart

This is about software application and equipment restart operation