UNION COMMUNITY
Server SDK For Windows

Programmer's Guide
Version 4.0 (revision 2)

October, 2009

Software Development Department

UNION COMMUNITY Co., Ltd.

Copyright © 2008, UNION COMMUNITY Co., Ltd.
All rights reserved.

Union Community Co., LTD.
Hyundai Topics Bldg., 44-3, Bangi-dong, Songpa-gu, Seoul 138-050 Korea
Tel : +82-6488-3000, Fax : +82-6488-3099 http://www.unioncomm.co.kr

USER License Agreement for Software Developer's Kit

Designed by Union Community Co., Ltd

This agreement is a legal usage license agreement between Union Community Co., Ltd. and the user.
If you do not agree with the terms and condition of the agreement, please return the product promptly. If you return the product, you will receive a refund.

1. Usage License

UNION COMMUNITY Co., Ltd. Grants licensee to use this SDK a personal, Limited, non-transferable, non-exclusive right to install and use one copy of the SDK on a single computer exclusively.
The software is considered 'being used' if it is stored in a computer's main or other storage device. The number of software copies will be determined by taking the greater number of the number of computers 'used' by the software and the number of computers where the software is stored.
Licensee may use the SDK solely for developing, designing, and testing UNION software applications for use with UNION products ("Applications").

2. Right to Upgrade

If you have purchased the software by upgrading an older version, the usage license of the old version is transferred to the new version. However, you may only use the old version under the condition that the old and new versions are not running simultaneously. Therefore, you are prohibited from transferring, renting or selling the old version. You maintain the usage license for the program and ancillary files that are in the old version but not in the new version.

3. Assignment of License

If you wish to transfer the usage license of this software to a third party, you must first obtain a written statement indicating that the recipient agrees with this agreement. You must then transfer the original disk and all other program components, and all copies of the program must be destroyed. After the transfer is completed, you must notify UNION COMMUNITY Co., Ltd. to update the customer registration.
Licensee shall not rent, lease, sell or lend the software application developed using the SDK to a third party without UNION's prior written consent.
Licensee shall not copy and redistribute the SDK without UNION's prior written consent.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

No other uses and/or distribution of the SDK or Sample Code are permitted without UNION's prior written consent. UNION reserves all rights not expressly granted to Licensee.

4. Copyright

All copyrights and intellectual properties of the software and its components belong to UNION COMMUNITY Co., Ltd., and these rights are protected under Korean and international copyright laws. Therefore, you may not make copies of the software other than for your personal backup purposes. In addition, you may not modify the software other than for reverse-engineering purposes to secure compatibility. Finally, you may not modify, transform or copy any part of the documentation without written permission from UNION COMMUNITY. (If you're using a network product, you may copy the documentation in the amount of the number of users)

5. Installation

An individual user can install this software in his/her PCs at home and office, as well as in a mobile PC. However, the software must not be running from two computers simultaneously. A single product can be installed in two or more computers in one location, but one of those computers must have a usage rate of at least 70%. If another computer has a usage rate of 31% or higher, another copy of the software must be purchased.

6. Limitation of Warranty

UNION COMMUNITY Co., Ltd. guarantees that the CD-ROM and all components are free of physical damage for a year after purchase.

UNION DISCLAIMS ALL WARRANTIES NOT EXPRESSLY PROVIDED IN THIS AGREEMENT INCLUDING, WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE. If you find any manufacture defect within the warranty period, we will replace the product. You must be able to prove that the product has been purchased within a year to receive a replacement. However, we will not replace a product damaged due to your mishandling or negligence. UNION COMMUNITY Co., Ltd. does not guarantee that the software and its features will satisfy your specific needs, and is not liable for any consequential damages arising out of the use of this product.

7. Liabilities

UNION COMMUNITY Co., Ltd. is not liable for any verbal, written or other agreements made by third parties, including product suppliers and dealers.

8. Termination

This agreement is valid until the date of termination. However, the agreement shall terminate automatically if you damaged the program or its components, or failed to comply with the terms described in this agreement.

9. Customer Service

UNION COMMUNITY Co., Ltd. makes every effort to provide registered customers with technical assistance and solutions to problems regarding software applications under certain system environments. When a customer submits a suggestion about any inconvenience or anomaly experienced during product usage, UNION COMMUNITY Co., Ltd. will take corrective action and notify the customer of the result.

10. General Terms

You acknowledge that you have read, understood and agree with the terms of this agreement. You also recognize the fact that this agreement has precedence over user agreements of older versions, past order agreements, advertisement notifications and/or other written agreements.

11. Contact

If you have any questions about this agreement, please contact UNION COMMUNITY Co., Ltd. via telephone, fax or e-mail.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Table of Contents

1. Overview 18
    1.1 Application 18
    1.2 Special Features 18
    1.3 Development Environment 19
    1.4 Module Organization 19
    1.5 Development Model 21
    1.6 Terminology Description 22
2. Installation 30
    2.1 System Requirements 30
    2.2 Installation 31
    2.3 Files to be installed 35
        2.3.1 Windows System Directory 35
        2.3.2 GAC (Global Assembly Cache) Folder 35
        2.3.3 (Installation Folder) \ Bin 35
        2.3.4 (Installation Folder) \ dotNET 35
        2.3.5 (Installation Folder) \ dotNET \ Setup 36
        2.3.6 (Installation Folder) \ Inc 36
        2.3.7 (Installation Folder) \ Lib 36
        2.3.8 (Installation Folder) \ Samples 36
        2.3.9 (Installation Folder) \ Skins 37
3. API Reference for DLL 38
    3.1 Type definitions 38
        3.1.1 Basic types 38
            UCSAPI_SINT8 / UCSAPI_SINT16 / UCBioAPI_SINT32 38
            UCSAPI_UINT8 / UCSAPI_UINT16 / UCBioAPI_UINT32 38
            UCSAPI_SINT / UCSAPI_UINT 38
            UCSAPI_VOID_PTR 38
            UCSAPI_BOOL 38
            UCSAPI_CHAR / UCSAPI_CHAR_PTR 38

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_NULL 38
UCSAPI_HWND 39
3.1.2 General types 39
UCSAPI_RETURN 39
UCSAPI_DATE_TIME_INFO 39
UCSAPI_MESSAGE 39
3.1.3 User information related types 40
UCSAPI_ACCESS_DATE_TYPE 40
UCSAPI_ACCESS_AUTHORITY 40
UCSAPI_CARD_DATA 41
UCSAPI_FINGER_DATA 41
UCSAPI_FACE_INFO 42
UCSAPI_FACE_DATA 43
UCSAPI_AUTH_DATA 43
UCSAPI_PICTURE_HEADER 44
UCSAPI_PICTURE_DATA 44
UCSAPI_USER_COUNT 45
UCSAPI_USER_INFO 46
UCSAPI_USER_DATA 46
UCSAPI_ERROR_TYPE 47
3.1.4 Log related types 47
UCSAPI_GET_LOG_TYPE 48
UCSAPI_ACCESS_LOG_DATA 48
3.1.5 Callback related types 49
UCSAPI_CALLBACK_EVENT_HANDLER 49
UCSAPI_CALLBACK_PARAM_0 50
UCSAPI_PROGRESS_INFO 51
UCSAPI_CALLBACK_PARAM_1 51
UCSAPI_CALLBACK_DATA_TYPE 52
3.1.6 Access control setting related types 52
UCSAPI_TIMEZONE 52
UCSAPI_ACCESS_TIMEZONE 53
UCSAPI_ACCESS_TIMEZONE_DATA 53
UCSAPI_ACCESS_HOLIDAY 54
UCSAPI_ACCESS_HOLIDAY_DATA 54

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_ACCESS_TIMEZONE_CODE....55
UCSAPI_ACCESS_TIME....56
UCSAPI_ACCESS_TIME_DATA....56
UCSAPI_ACCESS_GROUP....57
UCSAPI_ACCESS_GROUP_DATA....58
UCSAPI_ACCESS_CONTROL_DATA_TYPE....58
UCSAPI_ACCESS_CONTROL_DATA....59
3.1.7 Authentication related types....59
UCSAPI_AUTH_TYPE....59
UCSAPI_AUTH_MODE....60
UCSAPI_INPUT_DATA_CARD....60
UCSAPI_INPUT_DATA_PASSWORD....61
UCSAPI_INPUT_DATA_FINGER_1_TO_1....61
UCSAPI_INPUT_DATA_FINGER_1_TO_N....62
UCSAPI_INPUT_DATA_TYPE....63
UCSAPI_INPUT_DATA....63
UCSAPI_INPUT_ID_TYPE....64
UCSAPI_INPUT_ID_DATA....65
UCSAPI_AUTH_INFO....65
UCSAPI_AUTH_NOTIFY....66
3.1.8 Terminal option setting related types....67
UCSAPI_TERMINAL_TIMEZONE....67
UCSAPI_TERMINAL_DAY_SCHEDULE....68
UCSAPI_HOLIDAY_TYPE....69
UCSAPI_TERMINAL_HOLIDAY_INFO....69
UCSAPI_TERMINAL_SCHEDULE....70
UCSAPI_SECURITY_LEVEL....71
UCSAPI_ANTIPASSBACK_LEVEL....71
UCSAPI_SERVER_INFO....72
UCSAPI_TERMINAL_OPTION_FLAG....73
UCSAPI_TERMINAL_OPTION....73
3.1.9.1 ACU (Access Control Unit) option setting related types (MCP040)....76
UCSAPI_ACU_OPTION....76
UCSAPI_ACU_NET_SETTING....77
UCSAPI_ACU_READER_OPTION....79

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_ACU_PARTITION_OPTION 82
UCSAPI_ACU_ZONE_OPTION 84
UCSAPI_ACU_PGM_OPTION 85
UCSAPI_ACU_DOOR_OPTION 87
UCSAPI_ACU_INPUT_OPTION 88
UCSAPI_ACU_LOCKSCHEDULE 91
3.1.9 Monitoring related types 91
UCSAPI_TERMINAL_STATUS 91
UCSAPI_ACU_STATUS_INFO 93
UCSAPI_TERMINAL_CONTROL 94
3.2 API References 96
3.2.1 General API 96
UCSAPI_ServerStart 96
UCSAPI_ServerStop 98
UCSAPI_SetTerminalTimezone 99
UCSAPI_SetError 101
UCSAPI_SetWiegandFormatToTerminal 102
3.2.2 Terminal User Management API 104
UCSAPI_AddUserToTerminal 104
UCSAPI_DeleteUserFromTerminal 106
UCSAPI_DeleteAllUserFromTerminal 108
UCSAPI_GetUserCountFromTerminal 109
UCSAPI_GetUserInfoListFromTerminal 110
UCSAPI_GetUserDataFromTerminal 111
UCSAPI_RegistFaceFromTerminal 112
3.2.3 Log related API 113
UCSAPI_GetAccessLogCountFromTerminal 113
UCSAPI_GetAccessLogCountFromTerminalEx 114
UCSAPI_GetAccessLogFromTerminal 116
UCSAPI_GetAccessLogFromTerminalEx 118
3.2.4 Authentication related API 120
UCSAPI_SendAuthInfoToTerminal 120
UCSAPI_SendAntipassbackResultToTerminal 122
UCSAPI_SendAuthResultToTerminal 124
3.2.5 Terminal Management API 126

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_GetTerminalCount 126
UCSAPI_GetFirmwareVersionFromTerminal 127
UCSAPI_UpgradeFirmwareToTerminal 128
UCSAPI_SendUserFileToTerminal 129
UCSAPI_GetOptionFromTerminal 130
UCSAPI_SetOptionToTerminal 132
UCSAPI_OpenDoorToTerminal 132
UCSAPI_SetDoorStatusToTerminal 133
UCSAPI_SendTerminalControl 134
UCSAPI_SetAccessControlDataToTerminal 136
UCSAPI_GetTerminalInfo 137
UCSAPI_SendPrivateMessageToTerminal 138
UCSAPI_SendPublicMessageToTerminal 139
UCSAPI_SendSirenToTerminal 140
UCSAPI_SetSmartCardLayoutToTerminal 142
3.2.6 ACU Management API 144
UCSAPI_GetOptionFromACU 144
UCSAPI_SetOptionToACU 144
UCSAPI_GetLockScheduleFromACU 145
UCSAPI_SetLockScheduleToACU 146
UCSAPI_SetDoorStatusToACU 147
3.3 Callback Event References 149
3.3.1 Events for request from terminal 149
UCSAPI_CALLBACK_EVENT_CONNECTED 149
UCSAPI_CALLBACK_EVENT_DISCONNECTED 149
UCSAPI_CALLBACK_EVENT_TERMINAL_STATUS 149
UCSAPI_CALLBACK_EVENT_ACU_STATUS 149
3.3.2 Events of Response for server command 150
UCSAPI_CALLBACK_EVENT_REALTIME_ACCESS_LOG 150
UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG 150
UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG_COUNT 150
UCSAPI_CALLBACK_EVENT_ADD_USER 150
UCSAPI_CALLBACK_EVENT_DELETE_USER 150
UCSAPI_CALLBACK_EVENT_DELETE_ALL_USER 151
UCSAPI_CALLBACK_EVENT_GET_USER_COUNT 151

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_CALLBACK_EVENT_GET_USER_INFO_LIST 151
UCSAPI_CALLBACK_EVENT_GET_USER_DATA 151
UCSAPI_CALLBACK_EVENT_VERIFY_USER_AUTH_INFO 151
UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1 151
UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_N 152
UCSAPI_CALLBACK_EVENT_VERIFY_CARD 152
UCSAPI_CALLBACK_EVENT_VERIFY_PASSWORD 152
UCSAPI_CALLBACK_EVENT_GET_TERMINAL_OPTION 152
UCSAPI_CALLBACK_EVENT_SET_TERMINAL_OPTION 152
UCSAPI_CALLBACK_EVENT_FW_UPGRADING 152
UCSAPI_CALLBACK_EVENT_FW_UPGRADED 153
UCSAPI_CALLBACK_EVENT_FW_VERSION 153
UCSAPI_CALLBACK_EVENT_USERFILE_UPGRADING 153
UCSAPI_CALLBACK_EVENT_USERFILE_UPGRADED 153
UCSAPI_CALLBACK_EVENT_OPEN_DOOR 153
UCSAPI_CALLBACK_EVENT_TERMINAL_CONTROL 153
UCSAPI_CALLBACK_EVENT_PICTURE_LOG 153
UCSAPI_CALLBACK_EVENT_ANTIPASSBACK 154
UCSAPI_CALLBACK_EVENT_SET_ACCESS_CONTROL_DATA 154
UCSAPI_CALLBACK_EVENT_REGIST_FACE 154
UCSAPI_CALLBACK_EVENT_GET_TERMINAL_OPTION 155
UCSAPI_CALLBACK_EVENT_SET_TERMINAL_OPTION 155
UCSAPI_CALLBACK_EVENT_GET_ACU_OPTION 155
UCSAPI_CALLBACK_EVENT_SET_ACU_OPTION 155
UCSAPI_CALLBACK_EVENT_GET_ACU_LOCKSCHEDULE 155
UCSAPI_CALLBACK_EVENT_SET_ACU_LOCKSCHEDULE 156
UCSAPI_CALLBACK_EVENT_GET_SIREN 156
UCSAPI_CALLBACK_EVENT_SET_SIREN 156
UCSAPI_CALLBACK_EVENT_SET_SMARTCARD_LAYOUT 156
3.4 Error definitions 157
3.4.1 Success 157
UCSAPIERR_NONE 157
3.4.2 General error definitions 157
UCSAPIERR_INVALID_POINTER 157
UCSAPIERR_INVALID_TYPE 157

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPIERR_INVALID_PARAMETER 158
UCSAPIERR_INVALID_DATA 158
UCSAPIERR_FUNCTION_FAIL 158
UCSAPIERR_NOT_SERVER_ACTIVE 158
UCSAPIERR_INVALID_TERMINAL 158
UCSAPIERR_PROCESS_FAIL 159
UCSAPIERR_USER_CANCEL 159
UCSAPIERR_UNKNOWN_REASON 159
3.4.3 Data size related error definitions 159
UCSAPIERR_CODE_SIZE 159
UCSAPIERR_USER_ID_SIZE 160
UCSAPIERR_USER_NAME_SIZE 160
UCSAPIERR_UNIQUE_ID_SIZE 160
UCSAPIERR_INVALID_SECURITY_LEVEL 160
UCSAPIERR_PASSWORD_SIZE 160
UCSAPIERR_PICTURE_SIZE 161
UCSAPIERR_INVALID_PICTURE_TYPE 161
UCSAPIERR_RFID_SIZE 161
UCSAPIERR_MAX_CARD_NUMBER 161
UCSAPIERR_MAX_FINGER_NUMBER 161
3.4.4 Authentication related error definitions 162
UCSAPIERR_INVALID_USER 162
UCSAPIERR_UNAUTHORIZED 162
UCSAPIERR_PERMISSION 162
UCSAPIERR_FINGER_CAPTURE_FAIL 162
UCSAPIERR_DUP_AUTHENTICATION 163
UCSAPIERR_ANTIPASSBACK 163
UCSAPIERR_NETWORK 163
UCSAPIERR_SERVER_BUSY 163
UCSAPIERR_FACE_DETECTION 163
4. API Reference for COM 164
4.1 UCSAPI Object 164
4.1.1 Properties 164
ErrorCode 164
ConnectionsOfTerminal 164

TerminalUserData....165
ServerUserData....165
AccessLogData....165
AccessControlData....166
TerminalMacAddr....166
4.1.2 Methods....166
ServerStart....166
ServerStop....168
SetTerminalTimezone....169
SetError....171
GetTerminalCount....172
GetFirmwareVersionFromTerminal....173
UpgradeFirmwareToTerminal....174
SendUserFileToTerminal....175
OpenDoorToTerminal....176
SetDoorStatusToTerminal....177
SendTerminalControl....178
SendPrivateMessageToTerminal....179
SendPublicMessageToTerminal....179
SetWiegandFormatToTerminal....180
SetDoorStatusToACU....181
4.2 IServerUserData Interface....182
4.2.1 Properties....182
UserID....182
UniqueID....182
UserName....182
AccessGroup....183
SecurityLevel....183
IsCheckSimilarFinger....183
IsAdmin....184
IsIdentify....184
Password....184
FaceNumber....184
FaceData....185
IsFace1toN....185

Copyright 2009 UNIONCOMMUNITY Co., LTD.

IsBlacklist 185
4.2.2 Methods 186
InitUserData 186
SetAuthType 186
SetFPSampleData 188
AddFingerData 188
SetDuressFinger 189
SetCardData 190
SetPictureData 191
SetAccessDate 192
AddUserToTerminal 193
4.3 ITerminalUserData Interface 194
4.3.1 Properties 194
CurrentIndex / TotalNumber 194
UserID 194
UniqueID 195
UserName 195
AccessGroup 195
IsAdmin 196
IsIdentify 196
AccessDateType 196
StartAccessDate/EndAccessDate 197
SecurityLevel 197
IsAndOperation 198
IsFinger 199
IsFPCard 199
IsCard 200
IsCardID 200
IsPassword 201
Password 201
CardNumber 201
RFID 202
PictureDataLength 202
PictureData 203
TotalFingerCount 203

Copyright 2009 UNIONCOMMUNITY Co., LTD.

FingerID 204
SampleNumber 204
FPSampleData 205
FaceNumber 205
FaceData 205
IsBlacklist 206
4.3.2 Methods 207
GetUserCountFromTerminal 207
GetUserDataFromTerminal 209
DeleteUserFromTerminal 210
DeleteAllUserFromTerminal 211
RegistFaceFromTerminal 211
4.4 IAccessLogData Interface 213
4.4.1 Properties 213
CurrentIndex / TotalNumber 213
UserID 213
AuthType 214
AuthMode 214
DateTime 215
IsAuthorized 215
RFID 215
PictureDataLength 216
PictureData 216
4.4.2 Methods 217
SetPeriod 217
GetAccessLogCountFromTerminal 218
GetAccessLogFromTerminal 220
4.5 IAccessControlData Interface 222
4.5.1 Properties 222
4.5.2 Methods 223
InitData 223
SetTimeZone 224
SetAccessTime 226
SetHoliday 228
SetAccessGroup 229

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetAccessControlDataToTerminal 230
4.6 IServerAuthentication Interface 232
4.6.1 Properties 232
DeviceID 232
4.6.2 Methods 233
SetAuthType 233
SendAuthInfoToTerminal 235
SendAuthResultToTerminal 236
SendAntipassbackResultToTerminal 238
4.7 ITerminalOption Interface 239
4.7.1 Properties 239
flagSecuLevel / flagInputIDLength / flagAutoEnterKey / flagSound / flagAuthenticatoin / flagApplication / flagAntipassback / flagNetwork / flagInputIDType / flagAccessLevel / flagPrintText / flagSchedule 239
SecurityLevel_1To1 / SecurityLevel_1ToN 239
InputIDLength 240
AutoEnterKey 240
Sound 241
Authentication 241
Application 242
Antipassback 242
NetworkType / TerminalIP / Subnet / Gateway / ServerIP / Port 243
InputIDType 244
AccessLevel 244
PrintText 245
IsUse / StartHour / StartMinute / EndHour / EndMinute 245
Month / Day 246
4.7.2 Methods 248
SetOptionToTerminal 248
GetOptionFromTerminal 249
SetDaySchedule 251
GetDaySchedule 253
SetHoliday 254
GetHoliday 255
Clear 256

Copyright 2009 UNIONCOMMUNITY Co., LTD.

get_ACUStatusValue....257
ACUGetReaderVersion....257
GetOptionFromACU....258
SetOptionToACU....259
GetLockScheduleFromACU....259
SetLockScheduleToACU....260
ClearSirenConfig....261
SetSirenConfig....261
SetSirenToTerminal....261
GetSirenFromTerminal....262
GetSirenConfig....262
4.8 ISmartCardLayout Interface....263
4.8.1 Properties....263
SectorNumber....263
4.8.2 Methods....263
ClearSectorLayout....263
SetSectorLayout....264
SetSmartCardLayoutToTerminal....265
4.9 Events of COM....266
EventUserFileUpgrading....266
EventUserFileUpgraded....267
EventRegistFace....267
EventACUStatus....268
EventGetLockScheduleFromACU....269
EventSetLockScheduleToACU....269
EventSetSirenToTerminal....270
EventGetSirenFromTerminal....270
EventSetSmartCardLayout....270
5. Error definitions....271
5.1 Success....271
UCSAPIERR_NONE....271
5.2 General error definitions....271
UCSAPIERR_INVALID_POINTER....271
UCSAPIERR_INVALID_TYPE....272
UCSAPIERR_INVALID_PARAMETER....272

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPIERR_INVALID_DATA 272
UCSAPIERR_FUNCTION_FAIL 272
UCSAPIERR_NOT_SERVER_ACTIVE 272
UCSAPIERR_INVALID_TERMINAL 273
UCSAPIERR_PROCESS_FAIL 273
UCSAPIERR_USER_CANCEL 273
UCSAPIERR_UNKNOWN_REASON 273
5.3 Data szie related error definitions 273
UCSAPIERR_CODE_SIZE 273
UCSAPIERR_USER_ID_SIZE 274
UCSAPIERR_USER_NAME_SIZE 274
UCSAPIERR_UNIQUE_ID_SIZE 274
UCSAPIERR_INVALID_SECURITY_LEVEL 274
UCSAPIERR_PASSWORD_SIZE 274
UCSAPIERR_PICTURE_SIZE 275
UCSAPIERR_INVALID_PICTURE_TYPE 275
UCSAPIERR_RFID_SIZE 275
UCSAPIERR_MAX_CARD_NUMBER 275
UCSAPIERR_MAX_FINGER_NUMBER 275
5.4 Authentication related error definitions 276
UCSAPIERR_INVALID_USER 276
UCSAPIERR_UNAUTHORIZED 276
UCSAPIERR_PERMISSION 276
UCSAPIERR_FINGER_CAPTURE_FAIL 276
UCSAPIERR_DUP_AUTHENTICATION 276
UCSAPIERR_ANTIPASSBACK 277
UCSAPIERR_NETWORK 277
UCSAPIERR_SERVER_BUSY 277
UCSAPIERR_FACE_DETECTION 277

Copyright 2009 UNIONCOMMUNITY Co., LTD.

1. Overview

UCS (UNION COMMUNITY Server) SDK was created in the form of a high-level SDK to facilitate the development of application programs that can work with the network-type fingerprint recognition device of UNION COMMUNITY.

UCS SDK provides the interface (application Programming Interface, API) required in the development of fingerprint recognition server application programs. It can be used with UCBioBSP SDK for fingerprint registration and authentication.

1.1 Application

UCS SDK defines the server application program interface that can work with network-type terminal products provided by UNION COMMUNITY. It is therefore applied in application areas such as access control, time/attendance, drinking water, and school record management to facilitate easy and stable program development.

1.2 Special Features

■ Centralized Management Type

As a method that connects the terminal to UCS SDK, all terminals can be managed centrally. This type of connection is very useful in configuring a network using public networks.

If public networks using the measured rate system (system that charges according to the duration of line usage) are used, the method that connects directly to the terminal without implementing SDK's server function can be used.

■ Provides various APIs for terminal management

Various APIs are provided for user management, log management and access control management.

■ Provides various development modules and sample sources

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCS SDK provides COM-based modules to facilitate development with tools such as Visual Basic, Delphi and DotNET as well as C/C++. Sample sources required in SDK use are also provided.

■ Provides various authentication methods

Authentication methods using tools such as fingerprint, password and card and various combinations of these tools are provided for user identification.

1.3 Development Environment

Modules provided by UCS SDK were compiled at VC2008, and programming using this SDK can be done using most of 32bit compilers such as Visual C++.

For developers using Visual Basic, Delphi and DotNET as well as C/C++, COM-based modules and .NET class libraries are provided to facilitate development using these tools. Refer to each of sample sources on how to use the modules.

1.4 Module Organization

■ **Basic Module : UCSAPI40.dll**

As a core module of UCS SDK, it is the main module that implements all functions related to communication with the terminal. This module must be included for development using UCS SDK.

APIs that can be used in C/C++ are provided.

Relevant sample codes can be found at the DLL folder of the Samples folder.

■ **COM Module : UCSAPICOM.dll**

It is a COM (Component Object Module) module developed to support users of RAD (Rapid Application Development) tools such as Visual Basic and Delphi, DotNet.

As UCSAPICOM.dll exists at a higher level compared to UCSAPI40.dll, UCSAPI40.dll is required for operation. Also, this module does not provide all functions provided by UCSAPI40.dll but it has some functions that are not provided by UCSAPI40.dll.

Relevant sample codes can be found at the COM folder of the Samples folder.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Because COM can be used after registration at the system registry, a process of registering the COM module at the system is required by entering the following line at the command line appeared after pressing [Windows key + R] button.

Regsvr32 UCSAPICOM.dll

After this process, the COM module can be used.

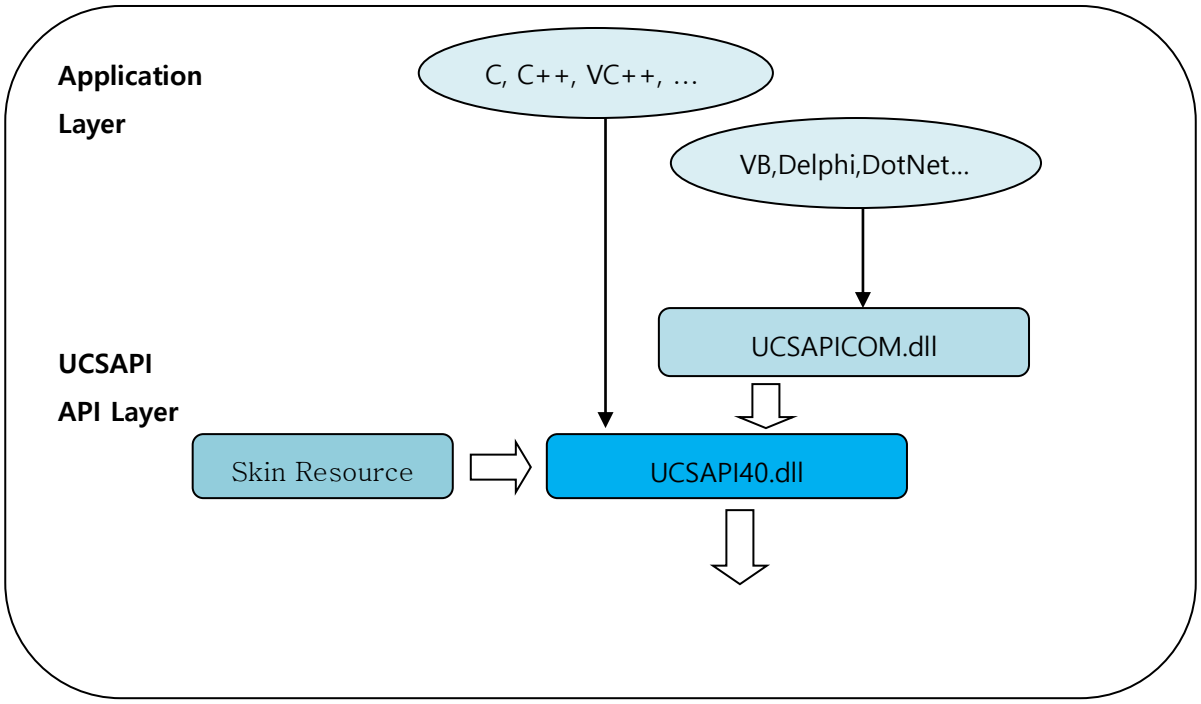
■ **Winsock Engine Module : WSEngine.dll**

It is the module that handles socket I/O (Input/Output). WSEngine.dll exists at a lower level compared to UCSAPI40.dll

Copyright 2009 UNIONCOMMUNITY Co., LTD.

1.5 Development Model

The structure of the development model is shown in the following figure.



Copyright 2009 UNIONCOMMUNITY Co., LTD.

1.6 Terminology Description

■ **Terminal**

It is the network-type fingerprint recognition terminal provided by UNION COMMUNITY.

■ **Terminal ID(TerminalID)**

Terminal connected to the system to distinguish between them is the value for the Key.

How to set, refer to the manual of the terminal

■ **Client**

It is the application program that communicates with the provided network-type fingerprint recognition terminal.

■ **Client ID (ClientID)**

The client ID is used to develop an application program with the client/server model.

The server module requires the key that identifies each client to support the multi-client environment, and this key is called ClientID.

■ **1:1 인증Authentication (1 to 1, Verification)**

It is the 1:1 process that compares the submitted sample with the fingerprint template (or card, password) corresponding to the user ID for user identification.

■ **1:N Authentication (1 to N, Identification)**

It is the 1:N process that compares the submitted sample with a part of or all fingerprint templates for user identification.

■ **Authentication Type**

The authentication types used during user authentication are defined.

In case the fingerprint recognition terminal uses the server authentication method after the terminal enters UserID or UniqueID for user identification, the terminal requests the authentication type to the server to obtain the authentication type of the user registered in the server.

Type	Value	Contents

Copyright 2009 UNIONCOMMUNITY Co., LTD.

1:N Fingerprint	0	1:N fingerprint authentication
1:1 Fingerprint	1	1:1 fingerprint authentication
Card & Fingerprint	2	By storing fingerprints at the smart card, this type implements 1:1 authentication between the input fingerprint and stored fingerprint.
Card	3	Card authentication
Password	4	Password authentication

■ **Registration Authentication Type**

The authentication types that are available during user registration are defined.

Authentication methods using tools for user identification such as fingerprint, password and card and various combinations of these tools are provided.

Type	Contents
Fingerprint	The fingerprint is used as authentication tool.
Fingerprint Card	The Fingerprint card is used as authentication tool. By storing user's fingerprint templates at the smart card, the fingerprint card implements 1:1 authentication between the sample entered during authentication and stored template.
Password	The password is used as authentication tool. The password is a character string value with a maximum of 8 digits.
Card	The card is used as authentication tool.
Card or Fingerprint	The card or fingerprint is used as authentication tool.
Card and Fingerprint	The combination of card and fingerprint is used as authentication tool.
Card or Password	The card or password is used as authentication tool.
Card and Password	The combination of card and fingerprint is used as authentication tool.
(ID and Fingerprint) or (Card and Fingerprint)	The combination of ID and fingerprint or the combination of card and fingerprint is used as authentication tool.
(ID and Password) or (Card and Password)	The combination of ID and password or the combination of card and password is used as authentication tool.
Fingerprint and Password	The combination of fingerprint and password is used as authentication tool.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Fingerprint or Password	After fingerprint authentication fails, the password is used as authentication tool.
Card and Password and Fingerprint	The combination of card, password and fingerprint is used as authentication tool.

■ **Fingerprint Security Level**

The security level to be used during fingerprint authentication is defined. The value ranges from 1~9. UCS SDK recommends developers to use the following level values. If the level value is high, the false reject rate (FRR) is increased and the false acceptance rate (FAR) is decreased. UCS SDK recommends level 4 for 1:1 authentication (verification) and level 5 for 1:N authentication (identification). If FAR is high compared to the recommended default level, an application program can increase the authentication level. On the other hand, if FRR is high, the authentication level can be decreased.

■ **Terminal Authentication Mode**

The operation modes for user's authentication and log record are defined.

Mode	Value	Contents
N / S	0	User authentication is implemented at the server when the network is online and at the terminal when the network is offline. The authentication record is stored at the server during server authentication. If the network is disconnected, the terminal stores the authentication record and sends the stored authentication record to the server when the server is connected.
S / N	1	When the network is online, user authentication is implemented at the terminal. For the user authentication request that is not stored at the terminal, the terminal requests authentication to the server. The authentication record is always stored at the terminal. When the network is online, only the authentication result is sent to the server to be stored.
N / O	2	User authentication is implemented only at the server. If the network is offline, user authentication cannot be implemented.
S / O	3	User authentication is implemented only at the terminal. When the network is online, only the authentication log is sent to the server.
S / S	4	The terminal does not attempt connection to the server but it only waits for the connection of an application program. Authentication is

Copyright 2009 UNIONCOMMUNITY Co., LTD.

		implemented at the terminal.

■ **Terminal Application Mode**

Program operation modes provided by the terminal are defined.

Mode	Value	Contents
Access Control	0	The terminal is operated for access control.
Time/Attendance	1	The terminal is operated for time/attendance management.
Drinking Water	2	The terminal is operated for drinking water management.

■ **User Authentication Mode**

The authentication purposes during user authentication are defined. The expanded authentication mode can be used by setting up the expanded mode option of the terminal. The authentication mode can be used when the program is operated for time/attendance and drinking water management purpose.

Mode	Value	Contents
Office Start	0	Authenticates with office start mode
Office Leave	1	Authenticates with office leave mode
General	2	Authenticates with general mode
Work Outside	3	Authenticates with work outside mode
Return to Office	4	Authenticates with return to office mode

■ **Log Get Type**

UCS SDK defines three types of log to obtain log data from the terminal.

The number of logs that can be stored internally varies according to the terminal model. If the maximum capacity is exceeded, new logs are stored by deleting some of the existing records.

Type	Value	Contents
New Log	0	New log that was not sent to the server
Old Log	1	Log that was already sent to the server
All Logs	2	All logs stored at the terminal

■ **User Property**

It is the 1byte-sized data field that defines authentication type and indicates whether the user is an administrator or not.

The value of 1 or 0 can be designated to each field. To use the property value of the corresponding field, the value of 1 is designated.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	Operation (AND) or (OR)	Card ID	Card	Password	Reserved	Fingerprint

-Admin:

The user can be designated as terminal administrator.

-Identify:

The user can be designated to use 1:N fingerprint authentication.

-Operation:

Each of authentication types can be designated to be used with AND or OR combination.
1 is set for AND combination while 0 is set for OR combination.

-CardID:

RFID can be designated to be used like UserID or UniqueID. CardID does not use card's RFID as authentication tool but instead, the card's RFID is simply used as an identifier like UserID.
It must be designated using AND combination with other authentication type.

-Card:

The user can be designated to use card authentication.

-Password:

The user can be designated to use password authentication.

-Fingerprint:

The user can be designated to use fingerprint authentication.

The user property can be represented by the following 12 values.

① Fingerprint

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	0	0	0	1

Copyright 2009 UNIONCOMMUNITY Co., LTD.

② Fingerprint-Card

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	0	0	1	0

③ Password

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	0	1	0	0

④ Card

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	1	0	0	0

⑤ Card or Fingerprint

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	1	0	0	1

⑥ Card and Fingerprint

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	1	0	1	0	0	1

⑦ Card or Password

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	1	1	0	0

⑧ Card and Password

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	1	0	1	1	0	0

⑨ (ID and Fingerprint) or (Card and Fingerprint)

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	1	0	0	0	1

⑩ (ID and Password) or (Card and Password)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	1	0	1	0	0

⑪ Fingerprint and Password

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	1	0	0	1	0	1

⑫ Fingerprint or Password : Password authentication in case of fingerprint authentication failure

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	Identify	0	0	0	1	0	1

⑬ Card and Password and Fingerprint

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Admin	0	1	0	1	1	0	1

■ Terminal Admin

The terminal administrator is a user who has rights to change terminal's setting information and register/delete users. If more than 1 terminal administrator is designated at the terminal, the administrator login process is required when entering the setup screen of the terminal. For the safe use of the terminal, the registration of the terminal administrator is recommended.

■ Terminal Status

The terminal periodically or immediately sends to the server the status of the terminal and devices connected to the terminal when the status is changed.

Terminal Lock Status:

This value represents the operability status value of the terminal.

SDK can set up terminal's operation status as lock/unlock. In lock state, the logon and network connection of the terminal are maintained, but the operation and access of the terminal are not allowed. The terminal in lock state does not even allow keypad operation.

Locking Device Control Status:

This value represents the status value of the locking device connected to the terminal.

SDK can set/unset the status of the locking device connected to the terminal as open state. In open state,

Copyright 2009 UNIONCOMMUNITY Co., LTD.

access is allowed without user authentication.

Locking Device Monitoring Status:

This value represents open/closed status value of the locking device received from the locking device with monitoring support.

Terminal Cover Status:

This value represents the open/closed status value of the terminal cover.

Status	Value	Content
Terminal Status	0	Normal
	1	Lock state
Locking Device Control Status	0	Closed state
	1	Open state
Locking Device Monitoring Status	0	Closed state
	1	Open state
	2	State that is not monitoring
Terminal Cover Open Status	0	Closed state
	1	Open state

< Terminal Status Information Summary >

Copyright 2009 UNIONCOMMUNITY Co., LTD.

2. Installation

2.1 System Requirements

■ **CPU**

Intel Pentium 133MHz or higher

■ **Memory**

16MB or higher

■ **USB Port**

USB 1.1

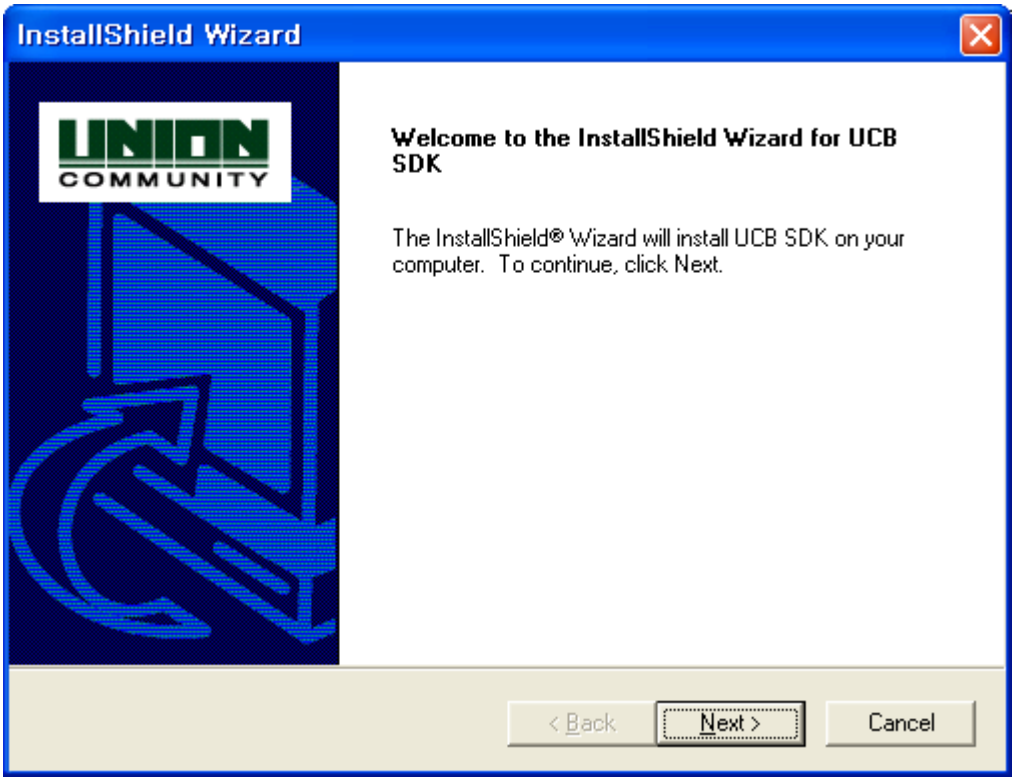
■ **OS**

Windows 98/ME or 2000/XP/2003/Vista/Windows 7

Copyright 2009 UNIONCOMMUNITY Co., LTD.

2.2 Installation

If the installation CD is inserted, Setup.exe is executed automatically.

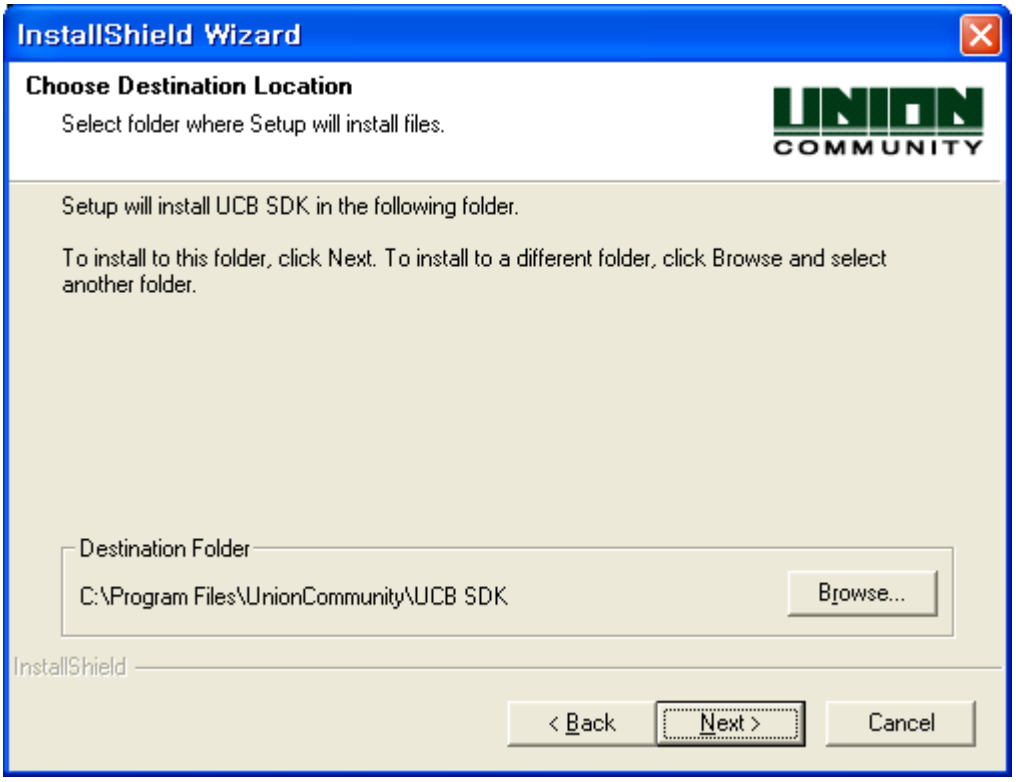


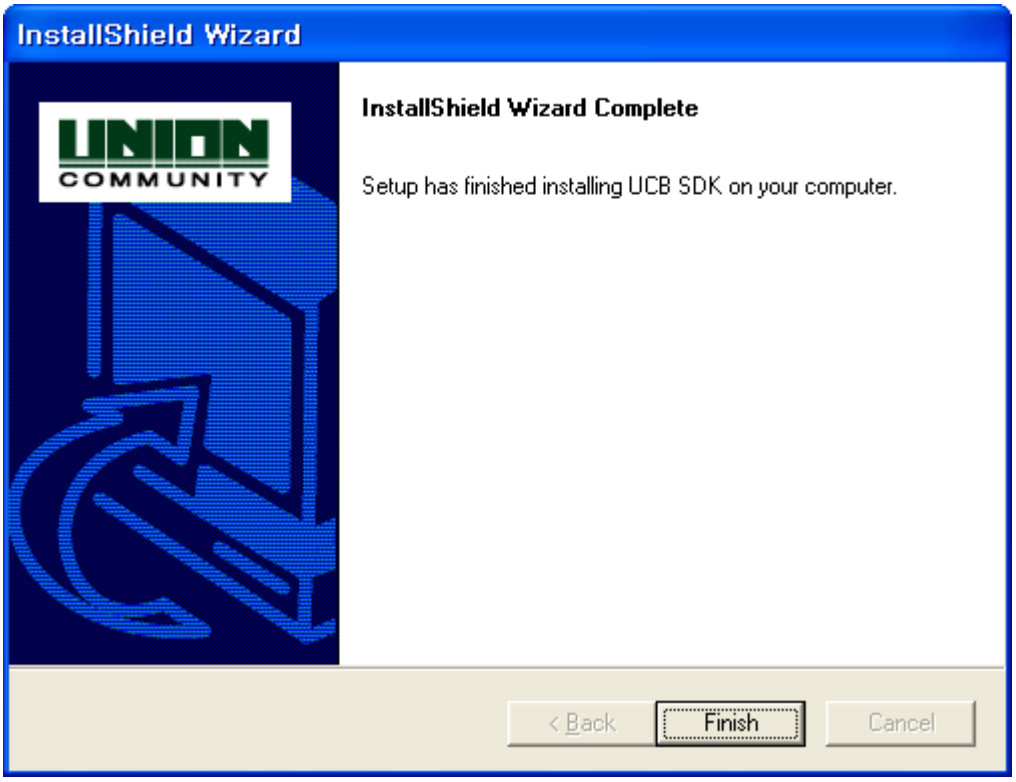
Copyright 2009 UNIONCOMMUNITY Co., LTD.

Follow the step-by-step procedures for installation.



Enter the user information and product serial number.





Copyright 2009 UNIONCOMMUNITY Co., LTD.

2.3 Files to be installed

When SDK installation is completed normally, the following files are installed at the designated installation folders.

2.3.1 Windows System Directory

Core modules for the use of SDK are installed. The following files are installed.

UCSAPI40.dll

Core module of UCS SDK. It is in charge of performing all functions of SDK.

UCSAPICOM.dll

COM module for RAD tool developer.

WSEngine.dll

Communication module for Windows socket I/O handling.

2.3.2 GAC (Global Assembly Cache) Folder

The following file is installed at the GAC folder where class library for .NET framework environment is installed. It is installed when installing the library for .NET during SDK installation.

2.3.3 (Installation Folder) \ Bin

Core files and sample execution files required in SDK execution are included.

UCSAPI40.dll / UCSAPICOM.dll / WSEngine.dll

Files identical to the ones installed at the Windows system32 folder.

Demo application

Several numbers of demo programs that can be used to test the functions of UCS SDK are included. All demo program sources are provided at the Samples folder.

2.3.4 (Installation Folder) \ dotNET

Class library files for .NET required in SDK execution are included.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UNIONCOMM.SDK.UCSAPI40.dll

The class library module for .NET. File identical to the one installed at GAC.

2.3.5 (Installation Folder) \ dotNET \ Setup

Files to install class library for .NET at GAC are included.

Setup.exe (UCSAPI40.NET_Setup.msi)

Class library installation file for .NET

2.3.6 (Installation Folder) \ Inc

UCSAPI.h

In case this file is included as the main header file of UCS SDK, UCSAPI_Basic.h, UCSAPI_Error.h and UCSAPI_Type.h files are included internally and automatically.

UCSAPI_Basic.h

The default data types used in UCS SDK are defined.

UCSAPI_Error.h

Error values used in UCSAPI40 module are defined.

UCSAPI_Type.h

Data type and structure information used in UCS SDK are defined.

2.3.7 (Installation Folder) \ Lib

The link library file for development at VC++ using SDK is included.

UCSAPI40.lib

The link library file created for VC++. It is used to link UCBioBSP.dll statically at VC++.

2.3.8 (Installation Folder) \ Samples

Sample source codes for each of the language are included in separate folders.

DLL

The sample code that can be developed using UCSAPI40.dll is included.

1) VC6: The sample created for Visual C++ 6.0 is included.

COM

The sample code that can be developed using UCSAPICOM.dll is included.

1) VB6: The sample created for Visual Basic 6.0 is included.

dotNET

The sample code that can be developed under Microsoft .NET environment using UNIONCOMM.SDK.UCSAPI40dll is included.

1) C#: The sample created for VisualStudio.NET 2005 and C# is included.

2.3.9 (Installation Folder) \ Skins

The skin resource file for each of the languages is included. Currently, only the English and Korean versions are included.

3. API Reference for DLL

Types and APIs to use a DLL module, UCSAPI40.dll, are described in the chapter.

3.1 Type definitions

3.1.1 Basic types

Basic types declared at UCSAPI_Basic are defined. Basic types are redefined for OS or CPU independent development. The following descriptions are based on the development with C++ under Windows.

UCSAPI_SINT8 / UCSAPI_SINT16 / UCBioAPI_SINT32

Signed 1byte / 2bytes / 4bytes value

UCSAPI_UINT8 / UCSAPI_UINT16 / UCBioAPI_UINT32

Unsigned 1byte / 2bytes / 4bytes value

UCSAPI_SINT / UCSAPI_UINT

Int/Unsigned int value that varies according to OS. It operates with 4bytes for 32bit OS and with 8bytes for 64bit OS.

UCSAPI_VOID_PTR

This type represents void*.

UCSAPI_BOOL

This type can have UCSAPI_FALSE(0) / UCBioAPI_TRUE(1) value. It is handled in the same way as int.

UCSAPI_CHAR / UCSAPI_CHAR_PTR

This type represents char and char*. 1byte character and character string value.

UCSAPI_NULL

This type represents NULL. It is defined with the value of ((void*)0).

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_HWND

This type is the HWND value that represents Windows handle.

3.1.2 General types

Declaration is made at UCAPI_Type.h, and general types are defined.

UCSAPI_RETURN

Prototype:

typedef UCSAPI_UINT32 UCSAPI_RETURN;

Description:

Values returned by functions of UCSAPI SDK are defined. In general, error values of UCS SDK are included. Refer to the error definition for more information on error values.

UCSAPI_DATE_TIME_INFO

Prototype:

```
typedef struct ucsapi_datetime_info
{
    UCSAPI_UINT16    Year;
    UCSAPI_UINT8     Month;
    UCSAPI_UINT8     Day;
    UCSAPI_UINT8     Hour;
    UCSAPI_UINT8     Min;
    UCSAPI_UINT8     Sec;
    UCSAPI_UINT8     Reserved;
} UCSAPI_DATE_TIME_INFO, *UCSAPI_DATE_TIME_INFO_PTR;
```

Description:

The structure that contains the date and time information

UCSAPI_MESSAGE

```
#define UCSAPI_MESSAGE    128
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

3.1.3 User information related types

Declaration is made at UCAPI_Type.h, and user information related types are defined.

UCSAPI_ACCESS_DATE_TYPE

Prototype:

```
typedef UCSAPI_UINT32        UCSAPI_ACCESS_DATE_TYPE;
```

Description:

Data types of the UCSAPI_ACCESS_DATE structure are defined. 3 data types can be defined for access period data; not used, allowed access period, and access restriction period. The following values are available.

```
#define UCSAPI_DATE_TYPE_NOT_USE          0
#define UCSAPI_DATE_TYPE_ALLOW            1
#define UCSAPI_DATE_TYPE_RESTRICTION      2
```

UCSAPI_ACCESS_AUTHORITY

Prototype:

```
typedef struct ucsapi_access_authority
{
    UCSAPI_DATA_PTR          AccessGroup;
    UCSAPI_ACCESS_DATE_TYPE  AccessDateType;
    UCSAPI_ACCESS_DATE_PTR   AccessDate
} UCSAPI_ACCESS_AUTHORITY, UCSAPI_ACCESS_AUTHORITY_PTR;
```

Description:

The structure that contains the access rights information of the user. Each of values is described below.

AccessGroup:

The pointer on the structure that contains access rights group code information

AccessDateType:

The type of data that the UCSAPI_ACCESS_DATE structure has is designated.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

AccessDate:

The pointer on the structure that contains access period information

UCSAPI_CARD_DATA

Prototype:

```
typedef struct ucsapi_card_data
{
    UCSAPI_UINT32           CardNum;
    UCSAPI_DATA_PTR         RFID[UCSAPI_CARD_NUMBER_MAX];
} UCSAPI_CARD_DATA, UCSAPI_CARD_DATA_PTR;
```

Description:

The structure that contains code information. Each of values is described below.

CardNum:

It designates the total number of RFID. RFID information corresponding to the number designated here are included as array.

RFID:

The pointer array of the structure that contains RFID information

UCSAPI_FINGER_DATA

Prototype:

```
typedef struct ucsapi_finger_data
{
    UCSAPI_UINT32           SecurityLevel;
    UCSAPI_UINT8            TemplateFormat;
    UCSAPI_UINT8            DuressFinger[10];
    UCSAPI_BOOL             IsCheckSimilarFinger;
    UCSAPI_EXPORT_DATA_PTR  ExportData;
} UCSAPI_FINGER_DATA, UCSAPI_FINGER_DATA_PTR;
```

Description:

The structure that contains fingerprint information. Each of values is described below.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SecurityLevel :

It designates the security level used during authentication.

Refer to the UCBioAPI_FIR_SECURITY_LEVEL definition of UCBioBSP SDK for available values.

TemplateFoarmat:

It is type of Template. One of below value.

#define UCBioAPI_TEMPLATE_FORMAT_UNION400 (0)

#define UCBioAPI_TEMPLATE_FORMAT_ISO500 (1)

#define UCBioAPI_TEMPLATE_FORMAT_ISO600 (2)

Default value is 0.(ref. UCBioAPI_Type.h)

DuressFinger:

This is contains duress finger information, and consis of 10 bytes.

Byte position is mean finger position. (0:Right Thumb, ... 5:Left Thumb, ... 9: Left little)

Each value mean normal finger or duress finger.

If duress finger input terminal, terminal work normal status.

But terminal trans result to server with error code 0x21(33)

IsCheckSimilarFinger :

When adding user fingerprint data to the terminal, It designates whether to check a similar fingerprint or not.

If this value is designated as true, the terminal checks if a similar fingerprint exists by comparing with the fingerprints of all registered users. If a similar fingerprint is detected, registration fails. As this flag can slow down user addition job by the terminal, performance may be degraded if there are a large number of registered users. It is used during UCSAPI_AddUserToTerminal call.

ExportData:

The pointer of the structure that contains converted template data

Refer to UCBioAPI_EXPORT_DATA structure of UCBioBSP SDK.

UCSAPI_FACE_INFO

Prototype:

```
typedef struct ucsapi_face_info
{
        long Length;
        BYTE* Data;
} UCSAPI_FACE_INFO, *UCSAPI_FACE_INFO_PTR;
```

Description:

The structure that contains face data information

length :

the size value of data

Data :

Face data

UCSAPI_FACE_DATA

Prototype:

```
typedef struct ucsapi_face_data
{
        long FaceNumber;
        UCSAPI_FACE_INFO_PTR    FaceInfo[UCSAPI_MAX_FACE_NUMBER];
} UCSAPI_FACE_DATA, *UCSAPI_FACE_DATA_PTR;
```

Description:

Whole face data for 1 user. 1 user can have 10 face info.

FaceNumber :

Registed face number. Max is 10.

FaceInfo :

Real face data. 1 time, you can regist 3 or 5 face info.(Normal : 5, Quick : 3) And you can regist face 2 times. So Face number is from 3 to 10

UCSAPI_AUTH_DATA

Prototype:

```
typedef struct ucsapi_auth_data
{
        UCSAPI_DATA_PTR             Password;
        UCSAPI_CARD_DATA_PTR        Card;
        UCSAPI_FINGER_DATA_PTR      Finger;
        UCSAPI_FACE_DATA_PTR        Face;
} UCSAPI_AUTH_DATA, UCSAPI_AUTH_DATA_PTR;
```

Description:

The structure that contains authentication information. Each of values is described below.

Password:

The pointer of the structure that contains password information

Card :

The pointer of the structure that contains card information

Finger:

The pointer of the structure that contains fingerprint information

UCSAPI_PICTURE_HEADER

Prototype:

```
typedef struct ucsapi_picture_header
{
        UCSAPI_UINT8        Format[4];      /* must be "jpg" */
        UCSAPI_UINT32       Length;         /* max length is 7 kbytes */
} UCSAPI_PICTURE_HEADER, UCSAPI_ PICTURE_HEADER_PTR;
```

Description:

The structure that contains the header information of picture data. Each of the values is described below.

Format :

It contains the format information of picture data. (Currently, only "JPG" format is supported.)
It designates the file extension value with the character string.

Length:

It has the size value of picture data. The maximum data that can be designated is 7KB.

UCSAPI_PICTURE_DATA

Prototype:

```
typedef struct ucsapi_picture_data
{
```

```
    UCSAPI_PICTURE_HEADER       Header;
    UCSAPI_UINT8*               Data;
} UCSAPI_PICTURE_DATA, UCSAPI_ PICTURE_DATA_PTR;
```

Description:

The structure that contains picture data information

Header :

It contains the header information of picture data.

Data :

The pointer of the buffer that contains image data in UCSAPI_PICTURE_HEADER format (Binary stream). The resolution of "JPG" data is 320*240.

UCSAPI_USER_COUNT

Prototype:

```
typedef struct ucsapi_user_count
{
    UCSAPI_UINT32       AdminNumber;
    UCSAPI_UINT32       UserNumber;
} UCSAPI_USER_COUNT, *UCSAPI_USER_COUNT_PTR;
```

Description:

The structure that contains the number of users registered in the terminal.

There are two types of users; administrator and general user.

After the UCSAPI_GetUserCountFromTerminal function called, it can be obtained from UCSAPI_CALLBACK_EVENT_GET_USER_COUNT event. Each of the values is described below.

AdminNumber:

It has the value of the number of registered administrators.

UserNumber :

It has the value of the number of registered general users.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_USER_INFO

Prototype:

```
typedef struct ucsapi_user_info
{
        UCSAPI_UINT32               UserID;
        UCSAPI_DATA_PTR             UserName;
        UCSAPI_DATA_PTR             UniqueID;
        UCSAPI_USER_PROPERTY        Property;
        UCSAPI_UINT8                AuthType;
        UCSAPI_UINT8                Reserved[2];
UCSAPI_ACCESS_AUTHORITY_PTR   AccessAuthority;
} UCSAPI_USER_INFO, UCSAPI_ USER_INFO_PTR;
```

Description:

The structure that contains user information. Each of the values is described below.

UserID **:**

It contains user ID information. This value can use only numeric data up to 8 digits.

UserName **:**

The pointer of the structure that contains user name information. This value can be designated up to the size of UCSAPI_DATA_SIZE_USER_NAME.

UniqueID**:**

The pointer of the structure that contains unique ID (employee ID) information. This value can be used in place of UserID for user identification. It can be designated up to the size of UCSAPI_DATA_SIZE_UNIQUE_ID.

Property**:**

The structure that contains user property (authentication type and whether a user is an administrator or not) information

AuthType:

This is value of cerification method.(1:FP,..., 26: Card & FP & FA & PW)

* refer UCSAPI_Type.h file for each value

AccessAuthority:

The pointer of the structure that contains access rights information

UCSAPI_USER_DATA

Prototype:

```
typedef struct ucsapi_user_data
{
        UCSAPI_USER_INFO            UserInfo;
        UCSAPI_AUTH_DATA_PTR        AuthData;
        UCSAPI_PICTURE_DATA_PTR     PictureData;
} UCSAPI_USER_DATA, UCSAPI_ USER_DATA_PTR;
```

Description:

The structure that contains user data. It is used during UCSAPI_AddUserToTerminal call. Each of the values is described below.

UserInfo :

The structure that contains user information

AuthData :

The pointer of the structure that contains access rights data

PictureData :

The pointer of the structure that contains picture data

UCSAPI_ERROR_TYPE

Prototype:

```
typedef UCSAPI_UINT32    UCSAPI_ERROR_TYPE
        #define UCSAPI_ERROR_TYPE_NONE          0
        #define UCSAPI_ERROR_TYPE_ACCESS_LOG    1
```

Description:

Define Error Type for returning back to terminal with received Callback Event.

3.1.4 Log related types

Declaration is made at UCAPI_Type.h, and authentication log related types are defined.

UCSAPI_GET_LOG_TYPE

Prototype:

typedef UCSAPI_UINT32 UCSAPI_GET_LOG_TYPE;

Description:

To obtain log data from the terminal, three log types are to be defined.

The number of logs that can be stored internally varies according to terminal model. If the maximum storage capacity is exceeded, new logs are stored by deleting some of the existing records.

It is used during UCSAPI_GetAccessLogCountFromTerminal / UCSAPI_GetAccessLogFromTerminal call.

```
#define UCSAPI_GET_LOG_TYPE_NEW          0
#define UCSAPI_GET_LOG_TYPE_OLD          1
#define UCSAPI_GET_LOG_TYPE_ALL          2
#define UCSAPI_GET_LOG_TYPE_PEROID       3
```

UCSAPI_ACCESS_LOG_DATA

Prototype:

```
typedef struct ucsapi_access_log_data
{
    UCSAPI_UINT32           UserID;
    UCSAPI_DATE_TIME_INFO   DataTime;
    UCSAPI_UINT8            AuthMode;
    UCSAPI_UINT8            AuthType;
    UCSAPI_UINT8            Reserved[2];
    UCSAPI_BOOL             IsAuthorized;
    UCSAPI_DATA_PTR         RFID;
    UCSAPI_PICTURE_DATA_PTR PictureData;
} UCSAPI_ACCESS_LOG_DATA, UCSAPI_ACCESS_LOG_DATA_PTR;
```

Description:

The structure that contains authentication log data

It can be obtained from the UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG event after UCSAPI_GetAccessLogFromTerminal is called. Each of the values is described below.

UserID :

It has the user ID value.

***DateTime* :**

The structure that contains authentication time information

***AuthMode*:**

It has the authentication mode value. Refer to UCSAPI_AUTH_MODE definition.

***AuthType*:**

It has the authentication type value. Refer to UCSAPI_AUTH_TYPE definition.

IsAuthorized:

It has the authentication result value. It has the value of 1 for success and the value of 0 for failure.

RFID:

The pointer of the structure that contains RFID data used during card authentication

PictureData:

The pointer of the structure that contains picture data taken during authentication. This value is available only for terminals that can take picture.

3.1.5 Callback related types

Declaration is made at UCAPI_Type.h, and callback event types are defined.

To notify data received from the terminal to the application program, SDK uses the callback function. The callback event consists of two parts; response to application program's request and request from the terminal.

UCSAPI_CALLBACK_EVENT_HANDLER

Prototype:

```
typedef UCSAPI_RETURN   (UCSAPI * UCSAPI_CALLBACK_EVENT_HANDLER) (
UCSAPI_UINT32 TerminalID, UCSAPI_UINT32 EventType,
UCSAPI_UINT32 wParam,   UCSAPI_UINT32 lParam);
```

Description:

This type defines the callback function to receive the event generated from the terminal.

EventType :

This type defines Event.

wParam :

Point of UCSAPI_CALLBACK_PARAM_0

lParam :

Point of UCSAPI_CALLBACK_PARAM_1

UCSAPI_CALLBACK_PARAM_0

Prototype:

```
typedef struct ucsapi_callback_param_0
{
        UCSAPI_UINT32           ClientID;
        UCSAPI_UINT32           ErrorCode;
        UCSAPI_PROGRESS_INFO    Progress;
} UCSAPI_CALLBACK_PARAM_0, *UCSAPI_CALLBACK_PARAM_0_PTR;
```

Description:

The structure passed as the third element of UCSAPI_CALLBACK_EVENT_HANDLER.

Each of the values is described below.

ClientID :

ID of the client that requested the job. (It is used in client/server model development.)

ErrorCode :

It contains the value on errors generated from the executed job.

The value of 0 represents success, while all other values represent failure.

Progress :

The structure that contains the progress information of the executed job.

It can be obtained after below functions are called.

- UCSAPI_GetUserInfoListFromTerminal
- UCSAPI_GetAccessLogFromTerminal

Copyright 2009 UNIONCOMMUNITY Co., LTD.

- USCAPI_UpgradeFirmwareToTerminal

UCSAPI_PROGRESS_INFO

Prototype:

```
typedef struct ucsapi_progress_info
{
        UCSAPI_UINT32           CurrentIndex;
        UCSAPI_UINT32           TotalNumber;
} UCSAPI_PROGRESS_INFO, *UCSAPI_PROGRESS_INFO_PTR;
```

Description:

The structure that contains the progress information of the executed job. When notifying several records to the application program, UCS SDK includes progress information in this structure and notifies it to the application program along with the UCSAPI_CALLBACK_PARAM_0 structure.
It can be obtained after UCSAPI_GetUserInfoListFromTerminal / UCSAPI_GetAccessLogFromTerminal / USCAPI_UpgradeFirmwareToTerminal functions are called. Each of the values is described below.

CurrentIndex:
The index of the record currently in transmission

TotalNumber :
The total number of records to be sent

UCSAPI_CALLBACK_PARAM_1

Prototype:

```
typedef struct ucsapi_callback_param_1
{
        UCSAPI_CALLBACK_DATA_TYPE       DataType;
        Union {
                UCSAPI_USER_INFO_PTR            UserInfo;
                UCSAPI_USER_DATA_PTR            UserData;
                UCSAPI_ACCESS_LOG_DATA_PTR      AccessLog;
                UCSAPI_FACE_INFO_PTR            FaceInfo;
              } Data;
} UCSAPI_CALLBACK_PARAM_1, *UCSAPI_CALLBACK_PARAM_1_PTR;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The structure passed as the fourth element of UCSAPI_CALLBACK_EVENT_HANDLER. Each of the values is described below.

DataType:

The type of data that this structure has is designated.

Refer to UCSAPI_CALLBACK_DATA_TYPE.

Data:

The union structure that designates real data. Values of UserInfo, UserData and AccessLog can be used by storing them with a single identical address pointer.

UCSAPI_CALLBACK_DATA_TYPE

Prototype:

typedef UCSAPI_UINT32 UCSAPI_CALLBACK_DATA_TYPE;

Description:

Data types of the UCSAPI_CALLBACK_PARAM_1 structure are defined.

```
#define UCSAPI_CALLBACK_DATA_TYPE_USER_INFO        0
#define UCSAPI_CALLBACK_DATA_TYPE_USER_DATA        1
#define UCSAPI_CALLBACK_DATA_TYPE_ACCESS_LOG       2
#define UCSAPI_CALLBACK_DATA_TYPE_FACE_INFO        3
```

3.1.6 Access control setting related types

Declaration is made at UCAPI_Type.h, and terminal access control related types are defined.

UCSAPI_TIMEZONE

Prototype:

```
typedef struct ucsapi_timezone
{
        UCSAPI_TIME_HH_MM       StartTime;
        UCSAPI_TIME_HH_MM       EndTime;
} UCSAPI_TIMEZONE, * UCSAPI_TIMEZONE_PTR;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The structure that contains time zone information

StartTime/ EndTime:

The structure that contains time information from start to end

UCSAPI_ACCESS_TIMEZONE

Prototype:

```
typedef struct ucsapi_access_timezone
{
    UCSAPI_CHAR             Code[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_TIMEZONE         Zone[12];
    UCSAPI_UINT8            Reserved[4]
} UCSAPI_ACCESS_TIMEZONE, * UCSAPI_ACCESS_TIMEZONE_PTR;
```

Description:

The structure that contains information on the time zone allowed for access during a day

Up to 12 time zones can be designated into a single time code. Each of the values is described below.

Code:

As the identifier code value of the time zone, it is a character string of fixed UCSAPI_DATA_SIZE_CODE size.

Zone:

The structure array that contains time zone information

UCSAPI_ACCESS_TIMEZONE_DATA

Prototype:

```
typedef struct ucsapi_access_timezone_data
{
    UCSAPI_UINT32           TimezoneNum;
    UCSAPI_ACCESS_TIMEZONE  Timezone[UCSAPI_ACCESS_TIMEZONE_MAX];
} UCSAPI_ACCESS_TIMEZONE_DATA, * UCSAPI_ACCESS_TIMEZONE_DATA_PTR;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The structure that contains the allowed access time zone data. Up to 128 time zone code information can be designated.

TimezoneNum:

It designates the total number of allowed access time zone codes. Time zone information corresponding to the number designated here are included in the form of an array.

Timezone:

The structure array that contains the allowed access time zone code information

UCSAPI_ACCESS_HOLIDAY

Prototype:

```
typedef struct ucsapi_access_holiday
{
        UCSAPI_CHAR             Code[UCSAPI_DATA_SIZE_CODE4];
        UCSAPI_DATE_MM_DD       Date[32];
} UCSAPI_ACCESS_HOLIDAY, * UCSAPI_ACCESS_HOLIDAY_PTR;
```

Description:

The structure that contains holiday information

Up to 32 holidays can be designated into the holiday code. Each of the values is described below.

Code:

As the identifier code value of a holiday, it is a character string of fixed UCSAPI_DATA_SIZE_CODE size.

Date:

The structure array that contains holiday information

UCSAPI_ACCESS_HOLIDAY_DATA

Prototype:

```
typedef struct ucsapi_access_holiday_data
{
```

```
    UCSAPI_UINT32                HolidayNum;
    UCSAPI_ACCESS_TIMEZONE       Holiday[UCSAPI_ACCESS_HOLIDAY_MAX];
} UCSAPI_ACCESS_HOLIDAY_DATA, * UCSAPI_ACCESS_HOLIDAY_DATA_PTR;
```

Description:

The structure that contains holiday data.

Up to 64 holiday code data can be designated. Each of the values is described below.

HolidayNum:

It designates the total number of holiday codes. Holiday information corresponding to the number designated here are included in the form of an array.

Holiday:

The structure array that contains holiday code information

UCSAPI_ACCESS_TIMEZONE_CODE

Prototype:

```
typedef struct ucsapi_access_timezone_code
{
    UCSAPI_CHAR                  Sun[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Mon[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Tue[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Wed[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Thu[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Fri[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Sat[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR                  Hol[UCSAPI_DATA_SIZE_CODE4];
} UCSAPI_ACCESS_TIMEZONE_CODE, * UCSAPI_ACCESS_TIMEZONE_CODE_PTR;
```

Description:

The structure that contains the allowed the access time zone code for each day of the week. Each of the values is described below.

Sun / Mon / Tue / Wed / Thu / Fri / Sat:

They have the allowed access time zone code value for each day of the week to be used during

authentication.

Hol:

It has the allowed access time zone code value to be applied to the holiday during authentication.

UCSAPI_ACCESS_TIME

Prototype:

```
typedef struct ucsapi_access_time
{
    UCSAPI_CHAR                     Code[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_ACCESS_TIMEZONE_CODE     Timezone;
    UCSAPI_CHAR                     Holiday[UCSAPI_DATA_SIZE_CODE4];
} UCSAPI_ACCESS_TIME, * UCSAPI_ACCESS_TIME_PTR;
```

Description:

The structure that contains the allowed access time information. Each of the values is described below.

Code:

As the identifier code value of allowed access time, it is a character string of fixed UCSAPI_DATA_SIZE_CODE size.

Timezone:

It has the allowed access time zone code for each day of the week.

Holiday:

It has the holiday code value to be used in the allowed access time code.

The time zone designated at Hol of the UCSAPI_ACCESS_TIMEZONE_CODE structure is applied to the holiday code designated here.

UCSAPI_ACCESS_TIME_DATA

Prototype:

```
typedef struct ucsapi_access_time_data
{
    UCSAPI_UINT32               AccessTimeNum;
```

```
    UCSAPI_ACCESS_TIME          AccessTime[UCSAPI_ACCESS_TIME_MAX];
} UCSAPI_ACCESS_TIME_DATA, * UCSAPI_ACCESS_TIME_DATA_PTR;
```

Description:

The structure that contains the allowed access time data.

Up to 128 allowed access time code information can be designated. Each of the values is described below.

AccessTimeNum:

It designates the total number of allowed access time codes. AccessTime information corresponding to the number designated here are included in the form of an array.

AccessTime:

The structure array that contains the allowed authentication time code information

UCSAPI_ACCESS_GROUP

Prototype:

```
typedef struct ucsapi_access_group
{
    UCSAPI_CHAR             Code[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR             AccessTime1[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR             AccessTime2[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR             AccessTime3[UCSAPI_DATA_SIZE_CODE4];
    UCSAPI_CHAR             AccessTime4[UCSAPI_DATA_SIZE_CODE4];
} UCSAPI_ACCESS_GROUP, * UCSAPI_ACCESS_GROUP_PTR;
```

Description:

The structure that contains the access group code information. Each of the values is described below.

Up to 4 allowed access time codes can be designated to the access group code.

Code:

As the identifier code value of the access group, it is a character string of fixed UCSAPI_DATA_SIZE_CODE size.

AccessTime1 / AccessTime2 / AccessTime3 / AccessTime4:

They contain the allowed access time code information to be used in the access group.

UCSAPI_ACCESS_GROUP_DATA

Prototype:

```
typedef struct ucsapi_access_group_data
{
        UCSAPI_UINT32           AccessGroupNum;
        UCSAPI_ACCESS_GROUP     AccessGroup[UCSAPI_ACCESS_GROUP_MAX];
} UCSAPI_ACCESS_GROUP_DATA, * UCSAPI_ACCESS_GROUP_DATA_PTR;
```

Description:

The structure that contains access group data. Up to 128 access group code information can be designated.

Each of the values is described below.

AccessGroupNum:

It designates the total number of access group codes. Access group information corresponding to the number designated here are included in the form of an array.

AccessGroup:

The structure array that contains the access group code information

UCSAPI_ACCESS_CONTROL_DATA_TYPE

Prototype:

```
typedef UCSAPI_UINT32           UCSAPI_ACCESS_CONTROL_DATA_TYPE

#define UCSAPI_ACCESS_CONTROL_DATA_TYPE_TIMEZONE        0
#define UCSAPI_ACCESS_CONTROL_DATA_TYPE_HOLIDAY         1
#define UCSAPI_ACCESS_CONTROL_DATA_TYPE_TIME            2
#define UCSAPI_ACCESS_CONTROL_DATA_TYPE_GROUP           3
```

Description:

It designates the data type that the UCSAPI_ACCESS_CONTROL_DATA structure has.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_ACCESS_CONTROL_DATA

Prototype:

```
typedef struct ucsapi_access_control_data
{
        UCSAPI_ACCESS_CONTROL_DATA_TYPE         DataType;
        union {
                UCSAPI_ACCESS_TIMEZONE_DATA_PTR         Timezone;
                UCSAPI_ACCESS_HOLIDAY_DATA_PTR          Holiday;
                UCSAPI_ACCESS_TIME_DATA_PTR             AccessTime;
                UCSAPI_ACCESS_GROUP_DATA_PTR            AccessGroup;
        } Data;
} UCSAPI_ACCESS_CONTROL_DATA, * UCSAPI_ACCESS_CONTROL_DATA_PTR;
```

Description:

The structure that contains the access control information. Values of Timezone, Holiday, AccessTime and AccesGroup can be used by storing them with a single identical address pointer.
It is used in the UCSAPI_SetAccessControlDataToTerminal function.
Each of the values is described below.

DataType:

The type of data that this structure has is designated. Refer to UCSAPI_ACCESS_CONTROL_DATA_TYPE.

3.1.7 Authentication related types

Declaration is made at UCAPI_Type.h, and user authentication related types are defined.

UCSAPI_AUTH_TYPE

Prototype:

```
typedef UCSAPI_UINT32 UCSAPI_AUTH_TYPE;
```

Description:

The authentication type is defined during authentication.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

```
#define UCSAPI_AUTH_TYPE_FINGER_1_TO_N      0
#define UCSAPI_AUTH_TYPE_FINGER_1_TO_1      1
#define UCSAPI_AUTH_TYPE_FINGER_CARD        2
#define UCSAPI_AUTH_TYPE_CARD               3
#define UCSAPI_AUTH_TYPE_PASSWORD           4
#define UCSAPI_AUTH_TYPE_FACE_1_TO_N        5
#define UCSAPI_AUTH_TYPE_FACE_1_TO_1        6
```

UCSAPI_AUTH_MODE

Prototype:

```
typedef UCSAPI_UINT32 UCSAPI_AUTH_MODE;
```

Description:

The authentication mode is defined during user authentication. The authentication mode defines its purpose during authentication. In general, it can be applied when the terminal is used for time/attendance management.

```
#define UCSAPI_AUTH_MODE_ATTENDANCE     0
#define UCSAPI_AUTH_MODE_LEAVE          1
#define UCSAPI_AUTH_MODE_NORMAL         2
#define UCSAPI_AUTH_MODE_OUT            3
#define UCSAPI_AUTH_MODE_RETURN         4
```

UCSAPI_INPUT_DATA_CARD

Prototype:

```
typedef struct ucsapi_input_data_card
{
    UCSAPI_UINT32           AuthMode;
    UCSAPI_DATA             RFID;
} UCSAPI_INPUT_DATA_CARD, *UCSAPI_INPUT_DATA_CARD_PTR;
```

Description:

The structure that contains the information entered during card authentication at the terminal. Each

of the values is described below.

AuthMode:

It has the authentication mode value entered at the terminal. Refer to UCSAPI_AUTH_MODE.

RFID:

The structure that contains the RFID information entered at the terminal.

UCSAPI_INPUT_DATA_PASSWORD

Prototype:

```
typedef struct ucsapi_input_data_password
{
        UCSAPI_UINT32           UserID;
        UCSAPI_UINT32           AuthMode;
        UCSAPI_DATA             Password;
} UCSAPI_INPUT_DATA_PASSWORD, *UCSAPI_INPUT_DATA_PASSWORD_PTR;
```

Description:

The structure that contains the information entered during password authentication at the terminal. Each of the values is described below.

UserID:

It has user ID information.

AuthMode:

It has the authentication mode value. Refer to UCSAPI_AUTH_MODE.

Password:

The structure that contains password information

UCSAPI_INPUT_DATA_FINGER_1_TO_1

Prototype:

```
typedef struct ucsapi_input_data_finger_1_to_n
{
        UCSAPI_UINT32           UserID;
```

```
    UCSAPI_UINT32           AuthMode;
    UCSAPI_UINT32           SecurityLevel;
    UCSAPI_DATA             Finger;
} UCSAPI_INPUT_DATA_FINGER_1_TO_1, *UCSAPI_INPUT_DATA_FINGER_1_TO_1_PTR;
```

Description:

The structure that contains the information entered during 1:1 fingerprint authentication at the terminal. Each of the values is described below.

UserID:

It has user ID information.

AuthMode:

It has the authentication mode value. Refer to UCSAPI_AUTH_MODE.

SecurityLevel:

It has the security level value to be used during authentication.
Refer to the UCBioAPI_FIR_SECURITY_LEVEL definition of UCBioBSP SDK for available values.

Finger:

The structure that contains fingerprint information

UCSAPI_INPUT_DATA_FINGER_1_TO_N

Prototype:

```
typedef struct ucsapi_input_data_finger_1_to_n
{
    UCSAPI_UINT32           AuthMode;
    UCSAPI_UINT32           SecurityLevel;
    UCSAPI_UINT32           InputIDLength;
    UCSAPI_DATA             Finger;
} UCSAPI_INPUT_DATA_FINGER_1_TO_N, *UCSAPI_INPUT_DATA_FINGER_1_TO_N_PTR;
```

Description:

The structure that contains the information entered during 1:N fingerprint authentication at the

terminal. Each of the values is described below.

UserID:

It has user ID information.

AuthMode:

It has the authentication mode value. Refer to UCSAPI_AUTH_MODE.

SecurityLevel:

It has the security level value to be used during authentication.

InputIDLength:

It has the length value of ID entered at the terminal. This value can be used to improve the speed of 1:N fingerprint authentication by reducing the authentication range. If the UserID value is 5 and the InputIDLength value is 3 in case the ID range of the registered user is 0001~1000, then the authentication ID range becomes 0500~1000.

Finger:

The structure that contains the fingerprint information entered at the terminal.

UCSAPI_INPUT_DATA_TYPE

Prototype:

```
typedef UCSAPI_UINT32          UCSAPI_INPUT_DATA_TYPE;

#define UCSAPI_INPUT_DATA_TYPE_FINGER_1_TO_N      0
#define UCSAPI_INPUT_DATA_TYPE_FINGER_1_TO_1      1
#define UCSAPI_INPUT_DATA_TYPE_PASSWORD           2
#define UCSAPI_INPUT_DATA_TYPE_CARD               3
#define UCSAPI_INPUT_DATA_TYPE_FINGER_CARD        4
```

Description:

The type of data that the UCSAPI_INPUT_DATA_TYPE structure has is designated.

UCSAPI_INPUT_DATA

Prototype:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

```
typedef struct ucsapi_input_data
{
        UCSAPI_ANTIPASSBACK_LEVEL       AntipassbackLevel;
        UCSAPI_INPUT_DATA_TYPE          DataType;
        Union {
                UCSAPI_INPUT_DATA_FINGER_1_TO_1_PTR         Finger1To1;
                UCSAPI_INPUT_DATA_FINGER_1_TO_N_PTR         Finger1ToN;
                UCSAPI_INPUT_DATA_CARD_PTR                  Card;
                UCSAPI_INPUT_DATA_PASSWORD_PTR              Password;
        } Data;
} UCSAPI_INPUT_DATA, *UCSAPI_INPUT_DATA_PTR;
```

Description:

The structure that contains the information entered at the terminal during user authentication. Authentication request can be made to the application program by storing the input information at this structure. Each of the values is described below.

AntipassbackLevel:

It has the anti-passback level set up at the terminal. The application program can refer to this value when implementing the anti-passback function.

DataType:

The type of data that this structure has is designated. Refer to UCSAPI_INPUT_DATA_TYPE.

Data:

The union structure that designates real data. Values of Finger1To1, Finger1ToN, Card and Password are used by storing them with a single identical address pointer.

UCSAPI_INPUT_ID_TYPE

Prototype:

```
typedef UCSAPI_UINT32           UCSAPI_INPUT_ID_TYPE;

#define UCSAPI_INPUT_ID_TYPE_USER_ID            0
#define UCSAPI_INPUT_ID_TYPE_UNIQUE_ID          1
#define UCSAPI_INPUT_ID_TYPE_RFID               2
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The type of ID entered at the terminal is designated. The ID type entered during 1:1 authentication can be changed at the terminal option settings. The default value is the UCSAPI_INPUT_ID_TYPE_USER_ID type. The maximum size of the user ID value is 8 digits. If the maximum number of digits is exceeded, the use of the UCSAPI_INPUT_ID_TYPE_UNIQUE_ID type increases the maximum size to 20 digits.

UCSAPI_INPUT_ID_DATA

Prototype:

```
typedef struct ucsapi_input_id_data
{
        UCSAPI_INPUT_ID_TYPE        DataType;
        Union {
                UCSAPI_UINT32*      UserID;
                UCSAPI_DATA_PTR     UniqueID
                UCSAPI_DATA_PTR     RFID;
        } Data;
} UCSAPI_INPUT_ID_DATA, *UCSAPI_INPUT_ID_DATA_PTR;
```

Description:

The structure that contains the ID information entered at the terminal during user authentication at the server. Each of the values is described below.

DataType:

The type of data that this structure has is designated. Refer to UCSAPI_INPUT_ID_TYPE.

Data:

The union structure that designates real data. Values of UserID, UniqueID and RFID can be used by storing them with a single identical address pointer.

UCSAPI_AUTH_INFO

Prototype:

```
typedef struct ucsapi_auth_info
```

```
{
        UCSAPI_UINT32               UserID;
        UCSAPI_BOOL                 IsAccessibility;
        UCSAPI_USER_PROPERTY        Property;
        UCSAPI_UINT32               ErrorCode;
} UCSAPI_AUTH_INFO, *UCSAPI_AUTH_INFO_PTR;
```

Description:

The structure that contains the user's authentication information. It is used in the UCSAPI_SendAuthInfoToTerminal function.

Each of the values is described below.

UserID:

It has the user's ID value.

IsAccessibility:

It has the value on whether the user has authentication rights or not.

Property:

The structure that contains user property (authentication type and administrator) information

ErrorCode:

In case the user does not have authentication rights, it has the corresponding error code value. Refer to error code table.

UCSAPI_AUTH_NOTIFY

Prototype:

```
typedef struct ucsapi_auth_notify
{
        UCSAPI_UINT32               UserID;
        UCSAPI_BOOL                 IsAuthorized;
        UCSAPI_BOOL                 IsVistor;
        UCSAPI_DATE_TIME_INFO       AuthorizedTime;
        UCSAPI_UINT32               ErrorCode;
} UCSAPI_AUTH_NOTIFY, *UCSAPI_AUTH_NOTIFY_PTR;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The structure that contains the user's authentication result information.

It is used in the UCSAPI_SendAuthResultToTerminal function.

UserID:

It has the ID value of the authenticated user or the user who attempted authentication.

IsAuthorized:

It has the authentication result value.

IsVisitor:

It has the value on whether the authenticated user is a visitor or not.

AuthorizedTime:

The structure that contains authentication time information

ErrorCode:

It has the error code value in case of authentication failure. Refer to the error code table.

3.1.8 Terminal option setting related types

Declaration is made at UCAPI_Type.h, and terminal option setting related types are defined.

UCSAPI_TERMINAL_TIMEZONE

Prototype:

```
typedef struct ucsapi_terminal_timezone
{
        UCSAPI_UINT8        IsUsed;
        UCSAPI_UINT8        StartHour;
        UCSAPI_UINT8        StartMin;
        UCSAPI_UINT8        EndHour;
        UCSAPI_UINT8        EndMin;
} UCSAPI_TERMINAL_TIMEZONE, * UCSAPI_TERMINAL_TIMEZONE_PTR;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

The structure that contains the time information used at the lock/open schedule of the terminal. Each of the values is described below.

IsUsed :

It has information on whether the value that the UCSAPI_TERMINAL_TIMEZONE structure has is valid or not.

StartHour / StartMin:

It contains the start time information.

EndHour / EndMin :

It contains the end time information.

UCSAPI_TERMINAL_DAY_SCHEDULE

Prototype:

```
typedef struct ucsapi_terminal_day_schedule
{
        UCSAPI_TERMINAL_TIMEZONE        Lock1;
        UCSAPI_TERMINAL_TIMEZONE        Lock2;
        UCSAPI_TERMINAL_TIMEZONE        Lock3;
        UCSAPI_TERMINAL_TIMEZONE        Open1;
        UCSAPI_TERMINAL_TIMEZONE        Open2;
        UCSAPI_ TERMINAL_TIMEZONE       Open3;
} UCSAPI_TERMINAL_DAY_SCHEDULE, * UCSAPI_TERMINAL_DAY_SCHEDULE_PTR;
```

Description:

The structure that contains terminal's lock/open schedule information for each day of the week. Regarding the schedule for each day of the week, up to three lock/open time zones per day can be designated. Each of the values is described below.

Lock1 / Lock2 / Lock3:

They have the time zone value to lock the terminal during a day.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Open1 / Open2 / Open3:

They have the time zone value to open the terminal during a day.

UCSAPI_HOLIDAY_TYPE

Prototype:

```
typedef UCSAPI_UINT8            UCSAPI_HOLIDAY_TYPE;

#define UCSAPI_HOLIDAY_TYPE_1       1
#define UCSAPI_HOLIDAY_TYPE_2       2
#define UCSAPI_HOLIDAY_TYPE_3       3
```

Description:

The holiday type to be used in the lock/open schedule of the terminal is designated. Up to 3 holiday types can be designated. Each of the values is described below.

UCSAPI_TERMINAL_HOLIDAY_INFO

Prototype:

```
typedef struct ucsapi_holiday_info
{
    UCSAPI_UINT8        Month;
    UCSAPI_UINT8        Day;
    UCSAPI_UINT8        HolidayType;
} UCSAPI_TERMINAL_HOLIDAY_INFO, * UCSAPI_TERMINAL_HOLIDAY_INFO_PTR
```

Description:

The structure that contains holiday information

Month/Day:

These structures contain the holiday's date information.

Holidaytype:

It has the holiday type value. Refer to UCSAPI_HOLIDAY_TYPE.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_TERMINAL_SCHEDULE

Prototype:

```
typedef struct ucsapi_terminal_schedule
{
        UCSAPI_TERMINAL_DAY_SCHEDULE        Sun;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Mon;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Tue;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Wed;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Thu;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Fri;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Sat;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Holiday1;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Holiday2;
        UCSAPI_TERMINAL_DAY_SCHEDULE        Holiday3;
        UCSAPI_TERMINAL_HOLIDAY_INFO        Holidays[100];
} UCSAPI_TERMINAL_SCHEDULE, * UCSAPI_TERMINAL_SCHEDULE_PTR;
```

Description:

The structure that contains the terminal's lock/open schedule information for each day of the week. Up to 100 holidays can be set up. The holiday type can be designated at Holiday1, Holiday2 and Holiday3. Each of the values is described below.

Sun / Mon / Tue / Wed / Thu / Fri / Sat:

The structure that contains the lock/open schedule information for each day of the week

Holiday1 / Holiday2 / Holiday3:

The structure that contains the lock/open schedule information for each holiday type

Holidays:

The structure that contains holiday information. One schedule from Holiday1, Holiday2 and Holiday3 is applied to each holiday.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_SECURITY_LEVEL

Prototype:

```
typedef struct ucsapi_security_level
{
        UCSAPI_UINT8    Verify          :4;   /* 1:1 default level = 4*/
        UCSAPI_UINT8    Identify        :4;   /* 1:N default level = 5*/
} UCSAPI_SECURITY_LEVEL, * UCSAPI_SECURITY_LEVEL_PTR;
```

Description:

The structure that contains the security level information to be used during fingerprint authentication. It can have any of the following values.

1 - LOWEST
2 - LOWER
3 - LOW
4 - BELOW_NORMAL
5 - NORMAL
6 - ABOVE_NORMAL
7 - HIGH
8 - HIGHER
9 - HIGHEST

Verify:

1:1 authentication level value. The default value is 4.

Identify

1:N authentication level value. The default value is 5.

UCSAPI_ANTIPASSBACK_LEVEL

Prototype:

```
typedef UCSAPI_UINT32           UCSAPI_ANTIPASSBACK_LEVEL;

#define UCSAPI_ANTIPASSBACK_LEVEL_NOT_USE                       0
#define UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_ALLOW      1
#define UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_PROHIBIT   2
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

It has the anti-passback level value set up at the terminal. To use the anti-passback function, the terminal needs to be set as UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_ALLOW or UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_PROHIBIT.

UCSAPI_ANTIPASSBACK_LEVEL_NOT_USE:

Anti-passback not used

UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_ALLOW:

Access allowed when connection to the server is disabled

UCSAPI_ANTIPASSBACK_LEVEL_WHEN_DISCONNECTION_PROHIBIT:

Access not allowed when connection to the server is disabled

UCSAPI_SERVER_INFO

Prototype:

```
typedef struct ucsapi_server_info
{
        UCSAPI_UINT8            IP[4];
        UCSAPI_UINT16           Port;
        UCSAPI_UINT8            Reserved[2];
} UCSAPI_SERVER_INFO;
```

Description:

The structure that contains the network information for the terminal to connect to the server. Each of the values is described below.

IP :

The buffer array that contains the address value of server IP

Port :

It has the socket port value for connection to the server.

UCSAPI_TERMINAL_OPTION_FLAG

Prototype:

```
typedef struct ucsapi_terminal_option_flag
{
    UCSAPI_UINT32    SecurityLevel    :1;
    UCSAPI_UINT32    InputIDLength    :1;
    UCSAPI_UINT32    AutoEnterKey     :1;
    UCSAPI_UINT32    Sound            :1;
    UCSAPI_UINT32    Authentication   :1;
    UCSAPI_UINT32    Application      :1;
    UCSAPI_UINT32    Antipassback     :1;
    UCSAPI_UINT32    Network          :1;
    UCSAPI_UINT32    Server           :1;
    UCSAPI_UINT32    InputIDType      :1;
    UCSAPI_UINT32    AccessLevel      :1;
    UCSAPI_UINT32    PrintText        :1;
    UCSAPI_UINT32    Schedule         :1;
} UCSAPI_TERMINAL_OPTION_FLAG, *UCSAPI_TERMINAL_OPTION_FLAG_PTR;
```

Description:

It has the reference flag on each item of the UCSAPI_TERMINAL_OPTION structure. Only when the flag value of an item is true, the value of that item can be referenced.

Refer to the UCSAPI_TERMINAL_OPTION structure for description on each item.

UCSAPI_TERMINAL_OPTION

Prototype:

```
typedef struct ucsapi_terminal_option
{
    UCSAPI_TERMINAL_OPTION_FLAG  Flags;
    UCSAPI_SECURITY_LEVEL        SecurityLevel;
    UCSAPI_UINT8                 InputIDLength;
    UCSAPI_UINT8                 AutoEnterKey;
    UCSAPI_UINT8                 Sound;
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

```
    UCSAPI_UINT8                    Authentication;
    UCSAPI_UINT8                    Application;
    UCSAPI_UINT8                    Antipassback;
    UCSAPI_NETWOARK_INFO            Network;
    UCSAPI_SERVER_INFO              Server;
    UCSAPI_UINT8                    InputIDType;
    UCSAPI_UINT8                    AccessLevel;
    UCSAPI_UINT8                    PrintText[32];
    UCSAPI_TERMINAL_SCHEDULE        Schedule;
} UCSAPI_TERMINAL_OPTION, *UCSAPI_TERMINAL_OPTION_PTR;
```

Description:

The structure that contains the option setting value of the terminal.

It is used in the UCSAPI_SetOptionToTerminal/UCSAPI_GetOptionFromTerminal function. Each of the values is described below.

Flags :

It has the reference flag value on each item of the structure.

To set up the terminal's option items using the UCSAPI_SetOptionToTerminal function, designate the flag value of an item as true and designate the value of that item.

SecurityLevel :

It designates the security level to be used during authentication.

Refer to the UCBioAPI_FIR_SECURITY_LEVEL definition of UCBioBSP SDK for available values.

InputIDLength :

It has the length value of ID entered at the terminal. The maximum length of 8 digits can be designated in case of using UserID while the maximum of length of 20 digits in case of using UniqueID.

AutoEnterKey :

It has the value on whether the terminal can use the automatic Enter key function or not. When key input corresponds to InputIDLength, this function enters the "Enter" key automatically.

Sound :

It has the sound volume value of the terminal. The range of the volume value that can be designated is 0~20. To set the terminal's sound to mute, 0 is designated.

Authentication :

It has the authentication type value of the terminal.

Refer to "Terminal Authentication Type" in Section 1.6 Terminology Description for available values.

Application:

It has the mode value of the terminal program. The terminal can be used as access control, time/attendance and drinking water management function. Refer to "Terminal Program Mode" in Section 1.6 Terminology Description for available values.

Antipassback:

It has the anti-passback level value of the terminal.

Refer to the UCSAPI_ANTIPASSBACK_LEVEL definition for available values.

Network:

The structure that contains terminal's network information

Server:

The structure that contains network information for the terminal to connect to the server

InputIDType:

It has the type value of ID entered at the terminal during authentication. The following values are available.

0 – UserID

1 – UniqueID

AccessLevel:

It has the access level value. This is the function that restricts the authentication type, allowing only the designated types for authentication. The following values are available. The default value is 0.

0 – No restriction

1 – Only fingerprint and password authentication allowed

Copyright 2009 UNIONCOMMUNITY Co., LTD.

PrintText:

It is the buffer array that contains character strings to be printed at the drinking water printer connected to the terminal.

This value can be used when the drinking water printer is connected to the terminal.

Schedule : The structure that contains lock/open schedule information

3.1.9.1 ACU (Access Control Unit) option setting related types (MCP040)

Declaration is made at UCAPI_Type.h.

UCSAPI_ACU_OPTION

First use **UCSAPI_GetOptionsFromACU (Get)** , then after modifing the appropriate structure (reader, partition, zone, pg., netSettings, etc), finally use the set UCSAPI_SetOptionsToACU (Set).

UCSAPI_GetOptionFromACU - this function will READ all options from the MCP (ACU). It will be stored in structure USCAPI_ACU_OPTION.

UCSAPI_SetOptionToACU - this function will WRITE all options in MCP (ACU), from the instance pointed to USCAPI_ACU_OPTION structure. It is important to use GetOptionFromACU First to get the current options.

For more details of each setting refer to the MCP040 Confirguration manual.

Prototype:

```
#define MAX_CP040_READER        12
#define MAX_CP040_PARTITION     4
#define MAX_CP040_ZONE          8
#define MAX_CP040_PGM           8
#define MAX_CP040_DOOR          4
#define MAX_CP040_INPUT         4
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

```
typedef struct ucsapi_acu_option
{
    ACU_NET_SETTING             ACU_NET_SETTINGS
    ACU_READER_OPTION           ACU_READER_OPTIONS [MAX_CP040_READER]
    ACU_PARTITION_SETTING       ACU_PARTITION_SETTINGS [MAX_CP040_PARTITION]
    ACU_ZONE_OPTION             ACU_ZONE_OPTIONS [MAX_CP040_ZONE]
    ACU_PGM_OPTION              ACU_PGM_OPTIONS [MAX_CP040_PGM]
    ACU_DOOR_OPTION             ACU_DOOR_OPTIONS [MAX_CP040_DOOR]
    ACU_INPUT_OPTION            ACU_INPUT_OPTION [MAX_CP040_INPUT]
    ACU_SYSTEM_OPTION           ACU_SYSTEM_OPTIONS;
    UCSAPI_UINT8                unused[55];
} UCSAPI_ACU_OPTION, *UCSAPI_ACU_OPTION_PTR;
```

Description:

The structure that contains the option setting value of the ACU.

It is used in the UCSAPI_SetOptionToACU / UCSAPI_GetOptionFromACU function.

Refer to sample source for detail struct description.

Note: It is important to keep the offset for any reader, partition, PGM , zone and 'unused' values.

UCSAPI_ACU_NET_SETTING

Prototype:

```
typedef struct ACU_NET_SETTINGS
{
    UCSAPI_UINT8        NetworkType;
    UCSAPI_UINT8        IP[4];
    UCSAPI_UINT8        Subnet[4];
    UCSAPI_UINT8        Gateway[4];
    UCSAPI_UINT8        dhcpIP[4];
    UCSAPI_UINT8        dhcpGW[4];
```

```
    UCSAPI_UINT8        dhcpSUB[4];
    UCSAPI_UINT32       port;
} UCSAPI_ ACU_NET_SETTING;
```

Description:

The structure that contains the terminal's network setting information

NetworkType :

It has the type value of IP address. The static IP is supported for the value of 0, while the dynamic IP is supported for the value of 1.

IP :

The array of the buffer that contains the IP address value of the terminal

Subnet :

The array of the buffer that contains the subnet mask value

Gateway :

The array of the buffer that contains the gateway address value.

dhcpIP,dhcpGW,dhcpSUB

Automatically set when DHCP is enabled. Use for READ-ONLY.

port

This is the server port value. 0-65535.

UCSAPI_ACU_READER_OPTION

#define MAX_CP040_READER 12

There is (1) ACU_READER_OPTION per reader, for a maximum of 12 readers connected to the MCP.

Offset value 0-11. Reader 0-7 are readers connected to RS485, readers 8-11 are Wiegand 1-4 readers.

Prototype:

```
typedef struct ACU_READER_OPTION
{
    UCSAPI_UINT8        type
    UCSAPI_UINT8        partlock
    UCSAPI_UINT8        openTime
    UCSAPI_UINT8        mode
    UCSAPI_UINT32       apentry
    UCSAPI_UINT32       apexit
    UCSAPI_UINT8        aptype
    UCSAPI_UINT8        aphour
    UCSAPI_UINT8        apmin
    UCSAPI_UINT8        apsec
    UCSAPI_UINT8        logmode;
    UCSAPI_UINT8        notused[15]
}
```

type :

Numeric value representing the reader type connected. This value is read only.

partlock :

Partition and lock assignments. This value is an 8 bit representation of the Partition Assigments and lock assignments. .

Partition: A Reader can be assigned to multiple partitions when using the security function. At least one partition should be assigned.

Lock: A Reader can be assigned to multiple locks. When a registered card is used, the assigned lock at the reader will open.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Partition 4	Partition 3	Partition 2	Partition 1	Lock 4	Lock 3	Lock 2	Lock 1

openTime :

When an authorized user is authorized at this reader the lock will unlock for the programmed open time.

The relay can be triggered to remain open from 100ms up to 250 seconds. Values 0 – 255.

.

mode:

0 = **ACCESS**: When a valid user is authorized the lock assigned to the reader will open for the duration of the Open Time. (Normal Access Mode)

1 = ACCESS+SECURITY: When a valid user is authorized the lock assigned to the reader will open for the duration of the Open Time. (Security Mode for Arm/Disarm)

If the F1 key is pressed (AC2100/5000) and a valid card/user is authorized, the partition assigned to the reader and user will ARM. If the partition is already armed the partition assigned to the reader and user will automatically disarm and unlock the door

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Reader Anti-passback

apentry/apexit :

Used for Anti-passback. This value is the four byte ascii value for the entry reader or exit reader.
As the identifier code value of antipassback, it is a character string of fixed UCSAPI_DATA_SIZE_CODE(4) size. If value is not used it is '****' = 2A2A2A2A. example: Code '0001' would be 30303031, Code '0002' is 30303032.

aptype :

Type of anti-passback.

0, Disabled

1, Hard Passback (If a user is in passback violation, reader will not allow access)

2, Soft Passback (If a user is in passback violation, reader will allow access but log a warning)

3, Timed Passback (if a user is in passback violation, the reader will not allow access until the lockout duration expires.

aphour : (0-23)

Anti-passback hour period from 00~23.

apmin: (0-59)

Anti-passback minute period from 00~59.

apsec: (0-59)

Anti-passback seconds period from 00~59.

When **Timed Passback** is used, this is the period in which the user will be locked out if in passback violation and timed passback option is set.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

logmode:

This mode will always be used when user is authenticating at the reader. This is used instead of using function keys. This is useful for readers that do not have function keys. (VSR20D or Wiegand)

0 = Disabled

1 = ENTER

2 = EXIT

3 = OUT

4 = IN.

UCSAPI_ACU_PARTITION_OPTION

#define MAX_CP040_PARTITION 4

There is (1) ACU_PARTITION_OPTION for each partition for a maximum of 4 partitions per MCP.

Partition 1 – 4 , offset into array 0-3

Prototype:

typedef struct ACU_PARTITION_SETTING

{

UCSAPI_UINT8	enable
UCSAPI_UINT8	unused[3]
UCSAPI_UINT8	name[16]
UCSAPI_UINT8	account[4]
UCSAPI_UINT8	entrydelay
UCSAPI_UINT8	exitdelay1
UCSAPI_UINT8	exitdelay2
UCSAPI_UINT16	sirentime
UCSAPI_UINT8	alarmcount
UCSAPI_UINT8	partoptions

} UCSAPI_ ACU_PARTITION_SETTING

Copyright 2009 UNIONCOMMUNITY Co., LTD.

enable (1:0) :

1 = Partition enabled, 0 = Partition disabled.

name :

Partition name – 16 ASCII Characters Maximum

account :

Hexadecimal 4 digits maximum. Reporting account number per partition.

entrydelay : 0-255 seconds

Zones defined as EXIT1/EXIT2 type will have this entry delay.

exitdelay1 : 0-255 seconds

Zones defined as EXIT1 type will have this exit delay.

exitdelay2 : 0-255 seconds

Zones defined as EXIT2 type will have this exit delay.

sirentime : 0-255 seconds

When any zone alarm occurs the bell output will activate for this period.

alarmcount : 0-255

This is maximum times a partition will go into alarm during an armed period.

partoptions

Each Bit represents an option for the partition settings.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
						Unlock on disarm	Chime ON

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_ACU_ZONE_OPTION

#define MAX_CP040_ZONE 8

There is (1) ACU_ZONE_OPTION per zone for a maximum of 8 zones connected to the MCP.

Zone 1 – 8 , offset into array 0-7.

Prototype:

```
typedef struct ACU_ZONE_OPTION
{
        UCSAPI_UINT8        notused
        UCSAPI_UINT8        name[10]
        UCSAPI_UINT8        response
        UCSAPI_UINT8        double
        UCSAPI_UINT8        partition
        UCSAPI_UINT8        type
        UCSAPI_UINT8        notused[17[
}
```

name :

Ascii 10 digits representing the name of the zone.

response :

0 – Set for standard 500ms debounce period.

1 – Set for quick 100ms debounce period.

double :

0 – default – single zone operation

1 – double zone operation, if connecting two zones to the zone input

partition

Each Bit represents the assignment of the zone on a partition 1-4.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Not used	Not used	Not used	Not used	Partition	Partition	Partition	Partition

Copyright 2009 UNIONCOMMUNITY Co., LTD.

				4	3	2	1

Type :

Zone type (see MCP Configuration manual for zone types)

Value 0-255 (hexadecimal)

Zone types

```
typedef enum
{
    UNUSED_type = 0,
    EXIT1_type,
    EXIT2_type,
    INSTANT_type,
    INTERIOR_type,
    EMERGENCY24_type,
    SILENTPANIC_type,
    WATER_type,
    GASZ_type,
    FIREZ_type,
    ARMDIS_type,
    EndNoType,
    UNASSIGNEDzone = 0xff,
} Zone_TypeDef;
```

UCSAPI_ACU_PGM_OPTION

#define MAX_CP040_PGM 8

There is (1) ACU_ACU_PGM_OPTION per output, for a maximum of 8 outputs connected to the MCP.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Offset value 0-7.

Prototype:

```
typedef struct ACU_PGM_OPTION
{
    UCSAPI_UINT8        time
    UCSAPI_UINT8        param1
    UCSAPI_UINT8        param2
    PGM_TypeDef         type
    UCSAPI_UINT8        notused[4]
}
```

time : 0-255 (hexadecimal value)

Activation period for PGM Output.

param1 : 0-255 (hexadecimal value)

This value has a different meaning depending on the output 'type'. Please see MCP configuration manual. (Lock 1-4 or Partition 1-4)

param2 :

This value is a bit value for options of the output.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Not used	Not used	Not used	Not used	Not used	Not used	Not used	Inverted

type :

PGM Output Types. When the below events occur the PGM output will activate.

typedef enum

```
{
    pgm_unused,
    pgm_auth,              // matching success
    pgm_noauth,            // matching failed
    pgm_sched,             // scheduled output
    pgm_alarm,             // alarm output
    pgm_tbl,               // tbl (ac loss, battery, bell, comm)
    pgm_armStat,           // arm/disarm status
    pgm_fire,              // fire alarm
    pgm_silent,            // silent alarm
    pgm_otl,               // open too long ( door#1-4)
    pgm_forced,            // door forced (door#1-4)
    pgm_typeEnd
} PGM_TypeDef;
```

UCSAPI_ACU_DOOR_OPTION

#define MAX_CP040_DOOR 4

There is (1) ACU_DOOR_OPTION per door/lock for a maximum of 4 locks connected to the MCP.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Lock 1-4 , offset into array 0-3.

Prototype:

typedef struct ACU_DOOR_OPTION

{

UCSAPI_UINT8	zone
UCSAPI_UINT8	option
UCSAPI_UINT8	warn
UCSAPI_UINT8	notused[5]

}

zone (0-7):

This is the monitoring zone assigned to the lock/door. This value is the zone number 0-7.

option:

This value is a bit value for door options.

7 Bit	6 Bit	5 Bit	4 Bit	3 Bit	2 Bit	1 Bit	0 Bit
Not used	Not used	Not used	Not used	Not used	Not used	Door Forced Audible	Door Forced Enabled

warn (0-255):

This is the delay in seconds before a door open too long event is generated.

UCSAPI_ACU_INPUT_OPTION

#define MAX_CP040_INPUT 4

There is (1) ACU_INPUT_OPTION per input for a maximum of 4 inputs connected to MCP.

Input 1-4 , offset into array 0-3.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Prototype:

```
typedef struct ACU_INPUT_OPTION
{
        UCSAPI_UINT8                    type
        UCSAPI_UINT8                    time
        UCSAPI_UINT8                    param
        UCSAPI_UINT8                    notused[5]
}
```

type:

This is the input type. 0-6

```
typedef enum
{
   pgmin_unused ,0
   pgmin_egressNC,
   pgmin_egressNO,
   pgmin_fireNC,
   pgmin_fireNO,
   pgmin_securityNC,
   pgmin_securityNO,
   pgmin_end,
} PGM_TypeInDef;
```

time (0-255):

Activation period. This only applies when input is set for EGRESS. It will activate the lock for the period set.

param (0-3):

This value usually refers to lock 1-4 or Partition 1-4, See MCP Configuration manual.

ACU_SYSTEM_OPTIONS:

There is (1) ACU_SYSTEM_OPTION per MCP.

Prototype:

```
typedef struct ACU_SYSTEM_OPTION
```

{

UCSAPI_UINT8	forcearm
UCSAPI_UINT8	notused[2]
UCSAPI_UINT8	notused_one
UCSAPI_UINT32	terminalID
UCSAPI_UINT8	timesync
UCSAPI_UINT8	eolzone
UCSAPI_UINT8	egresslog
UCSAPI_UINT8	Authentication
UCSAPI_UINT8	passbackmode
UCSAPI_UINT8	interlocking
UCSAPI_UINT8	notused_two[18]

} (total 32 bytes)

forcearm: (0 or 1)

Enable or disable force arming.

terminalID:

Terminal ID

timesync: (0 or 1)

Enable or disable time synchronization from UNIS.

eolzone: (0 or 1)

Enable or disable end of line resistors.

egresslog: (0 or 1)

Enable or disable logging when egress button is activated.

Authentication :

It has the authentication type value of the terminal.

Refer to "Terminal Authentication Type" in Section 1.6 Terminology Description for available values

passbackmode: (0 or 1)

Enable or disable server pass back mode.

0=local MCP passback

1=Server Global passback

interlocking: (0 or 1)

Enable or disable interlocking on locks that are monitored. If set to 1 , other doors cannot open until previous door is closed.

UCSAPI_ACU_LOCKSCHEDULE

Prototype:

```
#define MAX_ACU_LOCK        4

typedef struct ucsapi_acu_lockschedule
{
        UCSAPI_UINT8                LockIndex; // 0 - 3
        UCSAPI_TERMINAL_SCHEDULE    Schedule;
} UCSAPI_ACU_LOCKSCHEDULE, *UCSAPI_ACU_LOCKSCHEDULE_PTR;
```

Description:

The structure that contains schedule for setted lock of ACU.

It is used in the UCSAPI_SetLockScheduleToACU / UCSAPI_GetLockScheduleFromACU

Refet to TerminalOption for UCSAPI_TERMINAL_SCHEDULE

3.1.9 Monitoring related types

Declaration is made at UCAPI_Type.h, and monitoring related types are defined.

UCSAPI_TERMINAL_STATUS

Prototype:

```
typedef struct ucsapi_terminal_status
```

```
{
        UCSAPI_UINT32       Terminal;
        UCSAPI_UINT32       Door;
        UCSAPI_UINT32       Cover;
        UCSAPI_UINT32       Lock;
        UCSAPI_UINT32       Open;
        UCSAPI_UINT32       Reserved1;
        UCSAPI_UINT32       Reserved2;
        UCSAPI_UINT32       Reserved3;
} UCSAPI_TERMINAL_STATUS, *UCSAPI_TERMINAL_STATUS_PTR;
```

Description:

The structure that contains terminal's status value. Each of the values is described below.

Terminal:

It has the lock status value of the terminal. The following values are available.

0 – UnLock

1 – Lock

2 – Shutdown(Global Locking)

Door:

It has the locking device status value of the terminal. This value is supported only for locking devices with the monitoring function. The following values are available.

0 – Close

1 – Open

2 – Not used

3 – Forced Open

4 – Not Closed

. ***Cover***:

It has the cover status value of the terminal. The following values are available.

0 – Close

1 – Open

Lock:

It has the lock status value of gate. The following values are available.

0 – Normal

1 – Error

Open:

It has the open type value of gate open. The following values are available.

0 – Normal Open

1 – Continuous Open

acuStatus:

If terminal is ACU(MCP-040), then this area set with acu status.

(Refer ACU_STATUS struct from UCSAPI_Type.h file and ACU manual)

UCSAPI_ACU_STATUS_INFO

Prototype:

```
#define MAX_ACU_PARTITION      4
#define MAX_ACU_ZONE           8
#define MAX_ACU_LOCK           4
#define MAX_ACU_READER         8

typedef struct acu_reader_ver
{
        BYTE hw;
        BYTE major;
        BYTE minor;
        BYTE custom1;
        BYTE custom2;
        BYTE order;
        BYTE reserved[2];
} ACU_READER_VER;

typedef struct acu_reader
{
        BYTE id;
        BYTE reader_type;
        ACU_READER_VER ver; // 8
} ACU_READER;

typedef struct acu_status
{
```

```
        BYTE    partition[MAX_ACU_PARTITION];
        BYTE    zone[MAX_ACU_ZONE];
        BYTE    lock[MAX_ACU_LOCK];
        BYTE    reader[MAX_ACU_READER];
        ACU_READER reader_ver[MAX_ACU_READER];
        BYTE    Reserved[8];
} ACU_STATUS;

typedef struct ucsapi_acu_status_info
{
        UCSAPI_UINT8    Notice;
        ACU_STATUS      Status;
} UCSAPI_ACU_STATUS_INFO, *UCSAPI_ACU_STATUS_INFO_PTR;
```

Description:

The structure that contains ACU terminal's status value.

For each of the values, refer to the ACU manual.

UCSAPI_TERMINAL_CONTROL

Prototype:

```
typedef struct ucsapi_terminal_control
{
        UCSAPI_UINT8            lockStatus;
        UCSAPI_UINT8            lockType;
} UCSAPI_TERMINAL_CONTROL, *UCSAPI_TERMINAL_CONTROL_PTR;
```

Description:

The structure that contains for terminal control value. Each of the values is described below.

lockStatus:

It has the lock status value of the terminal. The following values are available.

0 – UnLock

1 – Lock

lockType:

It has the lock type value of the terminal locking. The following values are available.

0 – Normal

1 – Global(Shutdonw)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

3.2 API References

Definitions on various APIs used in UCS SDK, instructions on function use and elements are 7described.

3.2.1 General API

APIs to start/stop UCS SDK are described.

UCSAPI_ServerStart

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_ServerStart(
        IN UCSAPI_UINT32 MaxTerminal,
        IN UCSAPI_UINT32 Port,
        IN UCSAPI_INT32   Reserved,
        IN UCSAPI_CALLBACK_EVENT_HANDLER CallBackEventFunction);
```

Description:

This API initializes UCSAPI modules and implements server functions.

Parameters:

MaxTerminal::

This parameter defines the maximum number of terminals that can be connected. SDK can improve speed by assigning internal memory capacity in advance according to the maximum number of terminals. If the number of connected terminals exceeds the maximum number, memory is increased automatically to increase the number of connections.

Port:

The communication port for terminal connection. The server is in standby mode for terminal's connection to the designated port. The default value is 9870. If this value is changed, the terminal's port value also needs to be changed.

CallBackEventFunction:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

The pointer on the callback function to notify an event to an application program

Returns:

UCSAPIERR_NONE

UCSAPIERR_FUNCTION_FAILED

Callback:

UCSAPI_CALLBACK_EVENT_CONNECTED

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 CallBack0

lParam:

UCSAPI_UINT8 TerminalIP[4]:

The array of the buffer that has the terminal's IP address

UCSAPI_ServerStop

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_ServerStop();

Description:

This API disconnects all connected terminals and stops server functions.

Parameters:

N/A

Returns:

UCSAPIERR_NONE

Callback:

N/A

Callback Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_SetTerminalTimezone

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetTerminalTimezone(

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_CHAR_PTR pTimezoneName);

Description:

Set Terminal time from connected terminal

Terminal is using linked server's time but if terminal and server time is different, terminal need to be set as local time.

Parameters:

TerminalID:

Terminal ID

pTimezoneName:

Set Terminal zone name

Time zone name can be checked from following list.

HKEY_LOCAL_MACHINE\SOFRWARE\Microsoft\Windows NT\CurrentVersion\TimeZones

Returns:

UCSAPIERR_NONE

Callback:

N/A

Callback Parameters:

N/A.

※ GMT

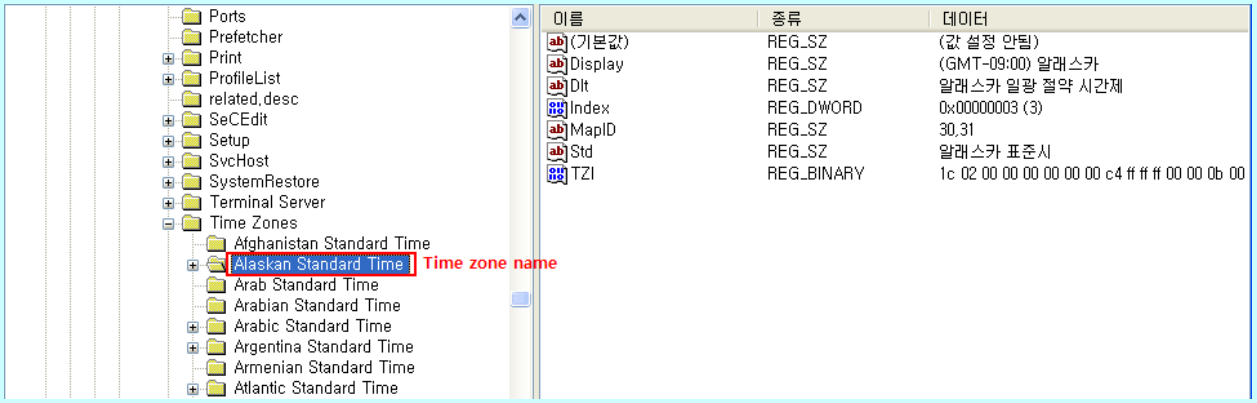
To check standard time, GMT can be a reference

. GMT stand for Greenwich Mean time, that if GMT +9 Korea means it is 9 hour earlier then Greewich time.

※ Time zone Name

Time zone Name can be checked from below Registry.

HKEY_LOCAL_MACHINE\SOFRWARE\Microsoft\Windows NT\CurrentVersion\TimeZones



UCSAPI_SetError

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetError(

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_ERROR_TYPE ErrorType);

Description:

Receive Callback Event from terminal and return back error code with setting.

Parameters:

TerminalID:

Terminal ID

ErrorType:

Have Error Type value for returning to the eart

.

For example, After call out UCSAPI_GetAccessLogFromTerminal, and fail to save received Log Data. Set ErrorType as UCSAPI_ERROR_TYPE_ACCESS_LOG in Callback Event function. After that call USCAPI_SetError then the terminal will refresh log with most recent log status and sending new log.

.

Returns:

UCSAPIERR_NONE

Callback:

N/A

Callback Parameters:

N/A.

UCSAPI_SetWiegandFormatToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetWiegandFormatToTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_WIEGAND_DATA wgdType,

IN UCSAPI_CHAR_PTR FilePath);

Description:

To set terminal's Wiegand In/Out Format.

Wiegand Format File cand be created by using Wiegand Tool fom SDK.

Parameters:

ClientID:

Use for Client/Server model development

TerminalID:

Terminal ID

wgdType:

Type value for defining Wiegand In or Out.

#define UCSAPI_WIEGAND_DATA_TYPE_OUT

#define UCSAPI_WIEGAND_DATA_TYPE_IN

FilePath:

Entire path for the file of Wiegand Format data

Returns:

UCSAPIERR_NONE

Callback:

UCSAPI_CALLBACK_EVENT_SET_WIEGAND_FORMAT

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

3.2.2 Terminal User Management API

APIs that can manage terminal users are described.

For command parameter of APIs,

- ClientID : ID of the client that requested a job. (It is used in client/server model development.)
- TerminalID : ID of the target terminal

UCSAPI_AddUserToTerminal

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_AddUserToTerminal(
        IN UCSAPI_INT32    ClientID,
        IN UCSAPI_INT32    TerminalID,
        IN UCSAPI_BOOL     IsOverwrite,
        IN UCBioAPI_USER_DATA_PTR* pUserData);
```

Description:

This API sends the user information to a designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

IsOverwrite:

This parameter designates whether to overwrite an already registered user or not. The default value is 1.

pUserData:

The pointer of the structure that contains user data

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE
UCSAPIERR_INVALID_POINTER
UCSAPIERR_INVALID_TERMINAL
UCSAPIERR_USER_NAME_SIZE
UCSAPIERR_UNIQUE_ID_SIZE
UCSAPIERR_INVALID_SECURITY_LEVEL
UCSAPIERR_INVALID_PARAMETER
UCSAPIERR_CODE_SIZE
UCSAPIERR_PASSWORD_SIZE
UCSAPIERR_MAX_CARD_NUMBER
UCSAPIERR_MAX_FINGER_NUMBER
UCSAPIERR_PICTURE_SIZE

Callback:

UCSAPI_CALLBACK_EVENT_ADD_USER

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_UINT32 UserID;

※ Note

In case of sending a multiple numbers of user data to the terminal using UCSAPI_AddUserToTerminal function, the UCSAPI_CALLBACK_EVENT_ADD_USER event must be checked after UCSAPI_AddUserToTerminal is called. The next user data is sent only after transmission is processed normally.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_DeleteUserFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_DeleteUserFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_INT32 UserID);

Description:

This API deletes the user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

UserID:

ID of a user to delete

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_DELETE_USER

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_UINT32 UserID;

※ Note

In case of deleting several users of the terminal using UCSAPI_DeleteUserFromTerminal function, the UCSAPI_CALLBACK_EVENT_DELETE_USER event must be checked after UCSAPI_DeleteUserFromTerminal is called. The next user is deleted only after deletion is processed normally.

UCSAPI_DeleteAllUserFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_DeleteAllUserFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID);

Description:

This API deletes all user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_DELETE_ALL_USER

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_GetUserCountFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetUserCountFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID);

Description:

This API obtains the number of registered users from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_USER_COUNT

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_UINT32 nUserCount

This parameter contains the number of users.

UCSAPI_GetUserInfoListFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetUserInfoListFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID);

Description:

This API obtains the list of all registered user information from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_USER_INFO_LIST

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_CALLBACK_PARAM_1_PTR pCallback1

pCallback1.DataType = UCSAPI_CALLBACK_DATA_TYPE_USER_INFO

UCSAPI_GetUserDataFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetUserDataFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_UINT32 TerminalID

IN UCSAPI_UINT32 UserID);

Description:

This API obtains the user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

UserID:

User ID

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_USER_DATA

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_CALLBACK_PARAM_1_PTR pCallback1;

pCallback1.DataType = UCSAPI_CALLBACK_DATA_TYPE_USER_DATA

UCSAPI_RegistFaceFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_RegistFaceFromTerminal (

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_UINT8 opt);

Description:

When receive this command, terminal start the face registration.

Terminal make a number of events until the ergistation is finished or canceled.

(Regular Registration : 5 events, Quick Registration : 3 events)

Parameters:

opt :

0 : Start registration , 1 : Cancel registration

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

Callback:

UCSAPI_CALLBACK_EVENT_REGIST_FACE

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

- TotalNumber & CurrentIndex in Progress are zero when Cancel event

lParam:

Face Data at normal situation(UCSAPI_FACE_INFO_PTR)

3.2.3 Log related API

APIs to obtain log data stored at the terminal are described.

UCSAPI_GetAccessLogCountFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetAccessLogCountFromTerminal(
IN UCSAPI_INT32 ClientID,
IN UCSAPI_INT32 TerminalID,
IN UCSAPI_GET_LOG_TYPE LogType);

Description:

This API obtains the number of authentication logs from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the log type to obtain. Refer to UCSAPI_GET_LOG_TYPE for available values.

Returns:

UCSAPIERR_NONE
UCSAPIERR_NOT_SERVER_ACTIVE
UCSAPIERR_INVALID_PARAMETER
UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG_COUNT

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_UINT32 nLogCount;

This parameter contains the number of logs.

UCSAPI_GetAccessLogCountFromTerminalEx

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetAccessLogCountFromTerminalEx(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_GET_LOG_TYPE LogType,

IN UCSAPI_DATE_PERIOD_PTR Period);

Description:

GetAccessLogCountFromTerminal is an extended API of function. To get periodic log information, parameter for setting period is added.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the log type to obtain. Refer to UCSAPI_GET_LOG_TYPE for available values.

Period:

It is a pointer of structure containing date information of log data. It is for getting the periodic log information.

This value is used as LogType is set LOG_TYPE_PERIOD.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_PARAMETER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG_COUNT

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_UINT32 nLogCount;

This parameter contains the number of logs.

UCSAPI_GetAccessLogFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetAccessLogFromTerminal(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_GET_LOG_TYPE LogType);

Description:

This API obtains the authentication log data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the log type to obtain. Refer to UCSAPI_GET_LOG_TYPE for available values.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_PARAMETER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

In case several numbers of log records exist,

the UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG event corresponding to the number of records are generated. Refer to the pCallback0->Progress value for the total number of logs and the index information of the current log.

lParam:

UCSAPI_CALLBACK_PARAM_1_PTR pCallback1;

pCallback1->DataType = UCSAPI_CALLBACK_DATA_TYPE_ACCESS_LOG;

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_GetAccessLogFromTerminalEx

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetAccessLogFromTerminalEx(

IN UCSAPI_INT32 ClientID,

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_GET_LOG_TYPE LogType,

IN UCSAPI_DATE_PERIOD_PTR Period);

Description:

GetAccessLogFromTerminal is an extended API of function. To get periodic log information, parameter for setting period is added.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the log type to obtain. Refer to UCSAPI_GET_LOG_TYPE for available values.

Period:

It is a pointer of structure containing date information of log data. It is for getting the periodic log information.

This value is used as LogType is set LOG_TYPE_PERIOD.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_PARAMETER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

In case several numbers of log records exist, the UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG event corresponding to the number of records are generated. Refer to the pCallback0->Progress value for the total number of logs and the index information of the current log.

lParam:

UCSAPI_CALLBACK_PARAM_1_PTR pCallback1;

pCallback1->DataType = UCSAPI_CALLBACK_DATA_TYPE_ACCESS_LOG;

Copyright 2009 UNIONCOMMUNITY Co., LTD.

3.2.4 Authentication related API

APIs to implement authentication at the server are described.
In case terminal's authentication type is N/S, NO mode, the terminal requests authentication to the server.

UCSAPI_SendAuthInfoToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SendAuthInfoToTerminal(
IN UCSAPI_INT32 TerminalID,
IN UCSAPI_AUTH_INFO_PTR pUserAuthInfo);

Description:

During 1:1 authentication, the terminal notifies the UCSAPI_CALLBACK_EVENT_VERIFY_USER_AUTH_INFO event to the application program to obtain user's authentication information.
Then, the application program needs to include the user's authentication information in the UCSAPI_AUTH_INFO structure and send it to the terminal immediately.
The UCSAPI_CALLBACK_EVENT_VERIFY_USER_AUTH_INFO event is always generated before the following events.
UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1,
UCSAPI_CALLBACK_EVENT_VERIFY_CARD,
CSAPI_CALLBACK_EVENT_VERIFY_PASSWORD

Parameters:

TerminalID:
Terminal ID

pUserAuthInfo:
The pointer of the structure that contains user's authentication information

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_VERIFY_USER_AUTH_INFO

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_INPUT_ID_DATA_PTR pInputID;

The structure that contains the ID information entered from the terminal

UCSAPI_SendAntipassbackResultToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SendAntipassbackResultToTerminal(

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_INT32 UserID,

IN UCSAPI_BOOL bResult);

Description:

If Terminal is setted with Antipassback option with stand alone. This application is used for checking out status of current Antipassback. This application will contain the status of Antipassback into bResult then send straight forward to the terminal. This even will activate only at the terminal to terminal verification.

Parameters:

TerminalID:

Terminal ID

UserID:

User ID

bResult:

Status of weather enter by Antipassback. Value 1 if for access granted

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_ANTIPASSBACK

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_UINT32 UserID;

UCSAPI_SendAuthResultToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SendAuthResultToTerminal(

IN UCSAPI_INT32 TerminalID,

IN UCSAPI_AUTH_NOTIFY_PTR pResult);

Description:

The terminal notifies the following events to an application program for user authentication.

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_N (1:N fingerprint authentication request)

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1 (1:1 fingerprint authentication request)

UCSAPI_CALLBACK_EVENT_VERIFY_CARD (Card authentication request)

UCSAPI_CALLBACK_EVENT_VERIFY_PASSWORD (Password authentication request)

Then, the application program needs to include the user's authentication result in the UCSAPI_AUTH_NOTIFY structure and send it to the terminal immediately.

Parameters:

TerminalID:

Terminal ID

pResult:

The pointer of the structure that contains authentication results

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_N

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1

UCSAPI_CALLBACK_EVENT_VERIFY_CARD

UCSAPI_CALLBACK_EVENT_VERIFY_PASSWORD

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam :

UCSAPI_INPUT_DATA_PTR pInputData;

The pointer of the structure that contains the sample data entered from the terminal

3.2.5 Terminal Management API

APIs to manage the terminal are described.

UCSAPI_GetTerminalCount

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_GetTerminalCount(
        IN UCSAPI_UINT32* pTerminalCount);
```

Description:

This API obtains the number of terminals connected to the server.

Parameters:

pTerminalCount:

The pointer of the value to contain the number of terminals

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

Callback:

N/A

Callback Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_GetFirmwareVersionFromTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetFirmwareVersionFromTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID);

Description:

This API obtains the firmware version of the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_FW_VERSION

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_DATA_PTR pVersion;

The pointer of the structure that contains version information

UCSAPI_UpgradeFirmwareToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_UpgradeFirmwareToTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_CHAR_PTR pFilePath);

Parameters:

This API upgrades the firmware of the designated terminal. Upgrade progress information is notified with the following event.

UCSAPI_CALLBACK_EVENT_FW_UPGRADING / UCSAPI_CALLBACK_EVENT_FW_UPGRADED

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

pFilePath:

The pointer of the value that contains the path of the firmware file

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_FW_UPGRADING

UCSAPI_CALLBACK_EVENT_FW_UPGRADED

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 pCallback0;

For upgrade progress information, refer to the pCallback0->Progress structure.

lParam:

N/A

UCSAPI_SendUserFileToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SendUserFileToTerminal (

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_UINT32 FileType,

IN UCSAPI_CHAR_PTR FilePath);

Parameters:

This API downloads the user file to terminal.

Parameters:

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

FileType

1:String file(.csv),

2:Background image file(.jpg),

3:Voice file to success(.wav),

4:Voice file to fail(.wav),

5:Video file(.mp4)

FilePath:

Full path of the file(Absolute Path)

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback:

UCSAPI_CALLBACK_EVENT_USERFILE_UPGRADING : 다운로드 진행 중

UCSAPI_CALLBACK_EVENT_ USERFILE_UPGRADED : 다운로드 완료 후

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 pCallback0;

다운로드 진행 정보는 pCallback0->Progress 구조체 참조.

lParam:

N/A

UCSAPI_GetOptionFromTerminal

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_GetOptionFromTerminal(
        IN UCSAPI_UINT16 ClientID,
        IN UCSAPI_UINT32 TerminalID);
```

Description:

This API obtains the option setting value from the designated terminal.

Parameters:

ClientID , TerminalID: See above

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback Parameters:

UCSAPI_CALLBACK_EVENT_GET_TERMINAL_OPTION

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam:

UCSAPI_TERMINAL_OPTION_PTR pOption;

UCSAPI_SetOptionToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetOptionToTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_TERMINAL_OPTION_PTR pOption);

Description:

This API sets up the option value of the designated terminal.

Parameters:

ClientID , TerminalID: See above

pOption:

The pointer of the UCSAPI_TERMINAL_OPTION structure

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_SET_TERMINAL_OPTION

wParam

UCSAPI_CALLBACK_PARAM_0_PTR pCallBack0;

lParam:

N/A

UCSAPI_OpenDoorToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_OpenDoorToTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID);

Description:

This API temporarily opens the locking device of the designated terminal.

Parameters:

ClientID , TerminalID: See above

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_OPEN_DOOR

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_SetDoorStatusToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetDoorStatusToTerminal(

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_UINT32 Status);

Description:

This API control lock to fit the status value

Parameters:

ClientID , TerminalID: See above

Status:

Lock Status (0: temporarily open, 1:start unlock, 2:end unlock)

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_OPEN_DOOR

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_SendTerminalControl

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_SendTerminalControl (
        IN UCSAPI_UINT16 ClientID,
        IN UCSAPI_UINT32 TerminalID,
        IN UCSAPI_UINT32 lockStatus,
        IN UCSAPI_UINT32 lockType);
```

Description:

This API control terminal to fit the parameter value.

Global locking means terminal shutdown.

Parameters:

ClientID , TerminalID: See above

lockStatus:

Lock Status (0:Unlock, 1:Lock)

lockType:

Lock Type (0:Normal, 1:Global)

Returns:

UCSAPIERR_NONE

Callback:

UCSAPI_CALLBACK_EVENT_TERMINAL_CONTROL

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

UCSAPI_TERMINAL_CONTROL pCtrl;

UCSAPI_SetAccessControlDataToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetAccessControlDataToTerminal(

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_ACCESS_CONTROL_DATA_PTR pAccessControlData);

Description:

This API sends the access control information to the designated terminal. Time zone, access time, holiday and access group information need to be sent separately. Access control information is used during authentication at the terminal. If no stored access control information is available, the terminal does not perform access control separately.

Parameters:

ClientID , TerminalID: See above

pAccessControlData:

The pointer of the structure that contains access control information

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_SET_ACCESS_CONTROL_DATA

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_GetTerminalInfo

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_GetTerminalInfo(
        IN UCSAPI_UINT32 TerminalID,
        OUT UCSAPI_TERMINAL_INFO_PTR pInfo);
```

Description:

This API can get detail terminal infomations. (EX : IP Address, Mac Address, other info…)

Parameters:

ClientID , TerminalID: See above

UCSAPI_TERMINAL_INFO_PTR: Point for Terminal information struct.

```
typedef struct ucsapi_terminal_info
{
        UCSAPI_UINT32   TerminalID;
        UCSAPI_UINT8    TerminalIP[4];
        UCSAPI_UINT8    TerminalStatus;
        UCSAPI_UINT8    DoorStatus;
        UCSAPI_UINT8    CoverStatus;
        UCSAPI_UINT8    LockStatus;
        UCSAPI_UINT8    ExtSignal[4];
        UCSAPI_VERSION  Firmware;
        UCSAPI_VERSION  Protocol;
        UCSAPI_VERSION  CardReader;
        UCSAPI_UINT16   ModelNo;
        UCSAPI_UINT8    TerminalType;
        UCSAPI_UINT8    MacAddr[6];
} UCSAPI_TERMINAL_INFO, *UCSAPI_TERMINAL_INFO_PTR;
```

Returns:

UCSAPIERR_NONE

UCSAPIERR_INVALID_TERMINAL

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback: None

UCSAPI_SendPrivateMessageToTerminal

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_SendPrivateMessageToTerminal(
        IN UCSAPI_UINT16 ClientID,
        IN UCSAPI_UINT32 TerminalID,
        IN UCSAPI_UINT32 Reserved,
        IN UCSAPI_PRIVATE_MESSAGE_PTR Message)
```

Description:

This API can send message for display on terminal LCD.

In struct of Message, there are display time(second) and text for display.

Parameters:

ClientID , TerminalID: See above

Message : The pointer on the structure that contains private message information

```
typedef struct ucsapi_private_message
{
   UCSAPI_UINT16          messageSize;
   UCSAPI_UINT16          displayTime;
   UCSAPI_CHAR            messageData[UCSAPI_MESSAGE];
} UCSAPI_PRIVATE_MESSAGE, *UCSAPI_PRIVATE_MESSAGE_PTR;
```

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_PRIVATE_MESSAGE

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_SendPublicMessageToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SendPublicMessageToTerminal(

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_BOOL Show,

IN UCSAPI_PUBLIC_MESSAGE_PTR Message)

Description:

This API can send public message for display on terminal LCD.

Public message display for setted period and setted time

Parameters:

ClientID , TerminalID: See above

Message : The pointer on the structure that contains public message information

```
typedef struct ucsapi_public_message
{
  UCSAPI_UINT16                 Reserved1;
  UCSAPI_UINT8                  Reserved2[2];
  UCSAPI_DATE_YYYY_MM_DD        StartDate;
  UCSAPI_DATE_YYYY_MM_DD        EndDate;
  UCSAPI_TIME_HH_MM             StartTime;
  UCSAPI_TIME_HH_MM             EndTime;
  UCSAPI_CHAR                   Message[UCSAPI_MESSAGE];
} UCSAPI_PUBLIC_MESSAGE, *UCSAPI_PUBLIC_MESSAGE_PTR;
```

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_PUBLIC_MESSAGE

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

UCSAPI_SendSirenToTerminal

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_SendSirenToTerminal(
        IN UCSAPI_UINT16 ClientID,
        IN UCSAPI_UINT32 TerminalID,
        IN UCSAPI_UINT8 opt,
        IN UCSAPI_UINT8 cntSiren,
        IN UCSAPI_SIREN_CONFIG_PTR pSiren)
```

Description:

Bring the siren data that has been set from the terminal or transmit the siren date to the terminal. If it is obtaining the siren data (opt=0), parameter value of next will be ignored.

Parameters:

ClientID , TerminalID: Refer to the above documents

opt:

Command issuing option (0: Obtaining siren data, 1: Writing siren data)

cntSiren:

It is the number of UCSAPI_SIREN_CONFIG value included in pSiren (Max. 100)

pSiren : Siren data structure

```
#define MAX_SIREN_CONFIG        100
struct WeekDay_Flag
```

```
{
        BYTE    Sunday          :1;
        BYTE    Monday          :1;
        BYTE    Tuesday         :1;
        BYTE    Wednesday       :1;
        BYTE    Thursday        :1;
        BYTE    Friday          :1;
        BYTE    Saturday        :1;
        BYTE    OffHoliday      :1;
};
typedef struct siren_config
{
        BYTE                    Hour;
        BYTE                    Minute;
        WeekDay_Flag            wf;
        BYTE                    Duration;       // Seconds
        BYTE                    Reserved[4];
} UCSAPI_SIREN_CONFIG, *UCSAPI_SIREN_CONFIG_PTR;
```

Hour: Siren rings at Minute time during Duration (sec).
Repeat is available for each day and holidays can be excluded.

Callback:

UCSAPI_CALLBACK_EVENT_GET_SIREN : In case when opt value is 0.
UCSAPI_CALLBACK_EVENT_SET_SIREN : In case when opt value is 1.

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;
In case when opt value is 0. pCallback0->Progress.TotalNumber is the number of siren data.

lParam:

In case when opt value is 0, it will be UCSAPI_SIREN_CONFIG_PTR

UCSAPI_SetSmartCardLayoutToTerminal

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetSmartCardLayoutToTerminal (

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_SMARTCARD_LAYOUT_PTR pCardLayout)

Description:

It transmits the card layout data to the terminal to set up the card layout that is going to be read on the terminal.

Parameters:

ClientID , TerminalID: Refer to the above document

pCardLayout : Card layout data structure

```
#define UCSAPI_SMARTCARD_SECTOR_MAX                 128
typedef UCSAPI_UINT32 UCSAPI_SMARTCARD_KEYTYPE;
        #define UCSAPI_SMARTCARD_KEYTYPE_A          0x60
        #define UCSAPI_SMARTCARD_KEYTYPE_B          0x61

typedef struct ucsapi_smartcard_sector_layout
{
        UCSAPI_UINT8                SectorNumber;       // Sector Number(0..127)
        UCSAPI_SMARTCARD_KEYTYPE    KeyType;            // Key A = 0x60, Key B = 0x61)
        UCSAPI_UINT8                KeyData[6];                 // Key Value
        UCSAPI_UINT8                BlockNumber;        // Block Number(0..3)
        UCSAPI_UINT8                Start;          // Start Location in Block
        UCSAPI_UINT8                Length;  // Data Length
        UCSAPI_UINT8                AID[2];   // AID of MAD Card. If AID not use then set 0xff
        // (This field is using for MAD Card and If byte value is   0xff then this byte is not use)
        UCSAPI_UINT8                Reserved[3];

} UCSAPI_SMARTCARD_SECTOR_LAYOUT, *UCSAPI_SMARTCARD_SECTOR_LAYOUT_PTR;

typedef UCSAPI_UINT32 UCSAPI_SMARTCARD_TYPE;
        #define UCSAPI_SMARTCARD_TYPE_DATA          0
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

```
        #define UCSAPI_SMARTCARD_TYPE_FINGER            1

typedef UCSAPI_UINT32 UCSAPI_SMARTCARD_READTYPE;
        #define UCSAPI_SMARTCARD_READTYPE_SERIAL    0
        #define UCSAPI_SMARTCARD_READTYPE_DATA      1
        #define UCSAPI_SMARTCARD_READTYPE_MAD       2

typedef UCSAPI_UINT8 UCSAPI_SMARTCARD_SERIALFORMAT;
        #define UCSAPI_SMARTCARD_SERIALFORMAT_DEFAULT       0
        #define UCSAPI_SMARTCARD_SERIALFORMAT_HEXA          1
        #define UCSAPI_SMARTCARD_SERIALFORMAT_DECIMAL       2
        #define UCSAPI_SMARTCARD_SERIALFORMAT_35DECIMAL     3

typedef struct ucsapi_smartcard_layout
{
        UCSAPI_SMARTCARD_TYPE               CardType;
        UCSAPI_SMARTCARD_READTYPE           ReadType;
        UCSAPI_SMARTCARD_SERIALFORMAT       SerialFormat;
// if ReadType is UCSAPI_SMARTCARD_READTYPE_SERIAL then this value is valid data.
        UCSAPI_UINT8                        SectorNumber; // 0..127
        UCSAPI_UINT8                        Reserved[6];
        UCSAPI_SMARTCARD_SECTOR_LAYOUT Layouts[UCSAPI_SMARTCARD_SECTOR_MAX];
// max card size is 8k
} UCSAPI_SMARTCARD_LAYOUT, *UCSAPI_SMARTCARD_LAYOUT_PTR;
```

Callback:

UCSAPI_CALLBACK_EVENT_SET_SMARTCARD_LAYOUT

Callback Parameters:

wParam:

```
UCSAPI_CALLBACK_PARAM_0_PTR         pCallback0;
```

lParam:

N/A

3.2.6 ACU Management API

APIs to manage the ACU are described.

UCSAPI_GetOptionFromACU

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetOptionFromACU (

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID);

Description:

This API obtains the option setting value from the designated ACU.

Parameters:

ClientID , TerminalID: See above

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback Parameters:

UCSAPI_CALLBACK_EVENT_GET_ACU_OPTION

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam:

UCSAPI_ACU_OPTION_PTR pOption;

UCSAPI_SetOptionToACU

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetOptionToACU (

IN UCSAPI_UINT32 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_ACU_OPTION_FLAG fOption,

IN UCSAPI_ACU_OPTION_PTR pOption);

Description:

This API sets up the option value of the designated ACU.

Parameters:

ClientID , TerminalID: See above

fOption:

The struct of the UCSAPI_ACU_OPTION_FLAG

pOption:

The pointer of the UCSAPI_ACU_OPTION structure

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_POINTER

UCSAPIERR_INVALID_TERMINAL

Callback:

UCSAPI_CALLBACK_EVENT_SET_ACU_OPTION

wParam

UCSAPI_CALLBACK_PARAM_0_PTR pCallBack0;

lParam:

N/A

UCSAPI_GetLockScheduleFromACU

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_GetLockScheduleFromACU (

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_UINT8 LockIndex);

Description:

This API obtains the schedule setting value of lock from the designated ACU.

(refer to TerminalOption for schedule.)

Parameters:

ClientID , TerminalID: See above

LockIndex:

The lock Index for get Schedule.(Index base is zero)

Be careful not to exceed the maximum value.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback Parameters:

UCSAPI_CALLBACK_EVENT_GET_ACU_LOCKSCHEDULE

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam:

UCSAPI_ACU_LOCKSCHEDULE_PTR pLockSchedule;

UCSAPI_SetLockScheduleToACU

Prototype:

```
UCSAPI_RETURN UCSAPI UCSAPI_SetLockScheduleToACU (
        IN UCSAPI_UINT32 ClientID,
        IN UCSAPI_UINT32 TerminalID,
        IN UCSAPI_UINT8 LockIndex,
        IN UCSAPI_TERMINAL_SCHEDULE_PTR pSchedule);
```

Description:

This API sets up the lock schedule value of the designated ACU.

(refer to TerminalOption for schedule.)

Parameters:

ClientID , TerminalID: See above

LockIndex:

The lock Index for set Schedule.(Index base is zero)

Be careful not to exceed the maximum value.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback Parameters:

UCSAPI_CALLBACK_EVENT_SET_ACU_LOCKSCHEDULE

wParam

UCSAPI_CALLBACK_PARAM_0_PTR pCallBack0;

lParam:

N/A

UCSAPI_SetDoorStatusToACU

Prototype:

UCSAPI_RETURN UCSAPI UCSAPI_SetDoorStatusToACU(

IN UCSAPI_UINT16 ClientID,

IN UCSAPI_UINT32 TerminalID,

IN UCSAPI_UINT8 Status,

IN UCSAPI_UINT8 DoorID);

Description:

This API control ACU door lock to fit the status value

Parameters:

ClientID , TerminalID: See above

Status:

Lock Status (0: temporarily open, 1:start unlock, 2:end unlock, 3:arm, 4:disarm)

DoorID:

Door ID of ACU.

Returns:

UCSAPIERR_NONE

UCSAPIERR_NOT_SERVER_ACTIVE

UCSAPIERR_INVALID_TERMINAL

Callback: 2 event occur continuously.

UCSAPI_CALLBACK_EVENT_OPEN_DOOR

UCSAPI_CALLBACK_EVENT_ACU_STATUS

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR pCallback0;

lParam:

N/A

3.3 Callback Event References

Declaration is made at UCAPI_Type.h, and callback event types are defined.
To notify data received from the terminal to the application program, SDK uses the callback function. The callback event consists of two parts; response to application program's request and request from the terminal.

3.3.1 Events for request from terminal

This is event for changing for terminal status.

UCSAPI_CALLBACK_EVENT_CONNECTED

Prototype:

#define UCSAPI_CALLBACK_EVENT_CONNECTED UCSAPI_CALLBACK_EVENT+1

Description:

When the terminal is connected to the server, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_DISCONNECTED

Prototype:

#define UCSAPI_CALLBACK_EVENT_DISCONNECTED UCSAPI_CALLBACK_EVENT+2

Description:

When the terminal is disconnected from the server, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_TERMINAL_STATUS

Description:

The SDK module periodically or immediately notifies the server about the status information of the terminal and devices connected to the terminal when the status is changed.

UCSAPI_CALLBACK_EVENT_ACU_STATUS

Description:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

The SDK module periodically or immediately notifies the server about the status information of the ACU terminal and devices connected to the ACU terminal when the status is changed.

Callback Parameters:

lParam:

UCSAPI_ACU_STATUS_INFO_PTR

3.3.2 Events of Response for server command

The events of the response according to the command sent to the terminal.

UCSAPI_CALLBACK_EVENT_REALTIME_ACCESS_LOG

Description:

When the terminal operates in S/N mode and the terminal implemented user authentication, SDK notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG

Description:

In response to the application program's request for authentication logs stored at the terminal, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_ACCESS_LOG_COUNT

Description:

In response to the application program's request for the number of authentication logs stored at the terminal, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_ADD_USER

Description:

In response to the user addition request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_DELETE_USER

Description:

In response to the user deletion request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_DELETE_ALL_USER

Description:

In response to the all user deletion request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_USER_COUNT

Description:

In response to the application program's request for the number of users stored at the terminal, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_USER_INFO_LIST

Description:

In response to the application program's request for user lists stored at the terminal, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_USER_DATA

Description:

In response to the application program's request for user data stored at the terminal, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_VERIFY_USER_AUTH_INFO

Description:

To obtain information (authentication type) required in 1:1 server authentication, the terminal notifies this event to the application program. Then, the application program needs to send the authentication type information to the terminal. This event is generated only when authentication is implemented at the server, and it is always issued before the next event.

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1,

UCSAPI_CALLBACK_EVENT_VERIFY_CARD,

UCSAPI_CALLBACK_EVENT_VERIFY_PASSWORD

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_1

Description:

During 1:1 fingerprint authentication, the terminal notifies this event to the application program. Then, the application program needs to send the authentication results to the terminal. This event is generated only when authentication is implemented at the server.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPI_CALLBACK_EVENT_VERIFY_FINGER_1_TO_N

Description:

During 1:N fingerprint authentication, the terminal notifies this event to the application program. Then, the application program needs to send the authentication results to the terminal. This event is generated only when authentication is implemented at the server.

UCSAPI_CALLBACK_EVENT_VERIFY_CARD

Description:

During card authentication, the terminal notifies this event to the application program. Then, the application program needs to send the authentication results to the terminal. This event is generated only when authentication is implemented at the server.

UCSAPI_CALLBACK_EVENT_VERIFY_PASSWORD

Description:

During password authentication, the terminal notifies this event to the application program. Then, the application program needs to send the authentication results to the terminal. This event is generated only when authentication is implemented at the server.

UCSAPI_CALLBACK_EVENT_GET_TERMINAL_OPTION

Description:

In response to the terminal option setting information request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_SET_TERMINAL_OPTION

Description:

In response to the terminal option setting request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_FW_UPGRADING

Description:

In response to the firmware upgrade request by the application program, the SDK module notifies this event to the application program. It is the event to notify the upgrade progress information to the application program.

UCSAPI_CALLBACK_EVENT_FW_UPGRADED

Description:

In response to the firmware upgrade request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_FW_VERSION

Description:

In response to the firmware version request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_USERFILE_UPGRADING

Description:

In response to the userfile download request by the application program, the SDK module notifies this event to the application program. It is the event to notify the download progress information to the application program.

UCSAPI_CALLBACK_EVENT_USERFILE_UPGRADED

Description:

In response to the ussefile download request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_OPEN_DOOR

Description:

In response to the temporary door open request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_TERMINAL_CONTROL

Description:

In response to the request for terminal control by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_PICTURE_LOG

Description:

When the picture log is received from the terminal, the SDK module notifies the picture log data to the application program. If authentication is implemented with the terminal authentication type, the

picture log is sent to the application program along with the UCSAPI_CALLBACK_EVENT_REALTIME_ACCESS_LOG event. But, if authentication is implemented with the server authentication type, the terminal notifies the picture log to the application program separately after receiving the authentication results from the application program.

UCSAPI_CALLBACK_EVENT_ANTIPASSBACK

Description:

In case that the anti-passback option is not set, the terminal notifies this event to the application program to obtain the user's current anti-passback status during user authentication. Then, the application program needs to immediately send user's anti-passback status to the terminal. This event is generated only when authentication is implemented at the terminal.

UCSAPI_CALLBACK_EVENT_SET_ACCESS_CONTROL_DATA

Description:

In response to the access rights setting request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_REGIST_FACE

Description:

In response to regist face from terminal request by the application program, the SDK module notifies this event to the application program.

Terminal start registration with display registration on LCD display, and capture face 3 or 5 times. (Regular registration : 5 capture, Quick registration : 3 capture)

Each capture time make event for that with progress. value,

Callback Parameters:

wParam:

UCSAPI_CALLBACK_PARAM_0_PTR

CurrentIndex in progress is increase from 1.

If TotalNumber and CurrentIndex in progress are zero, then registration is canceled.

lParam:

UCSAPI_CALLBACK_PARAM_1_PTR

- DataType : UCSAPI_CALLBACK_DATA_TYPE_FACE_INFO
- Data : UCSAPI_FACE_INFO_PTR

In normal time, lParam is Face data

UCSAPI_CALLBACK_EVENT_GET_TERMINAL_OPTION

Description:

In response to the terminal option setting information request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_SET_TERMINAL_OPTION

Description:

In response to the terminal option setting request by the application program, the SDK module notifies this event to the application program.

UCSAPI_CALLBACK_EVENT_GET_ACU_OPTION

Description:

In response to the ACU option information request by the application program,
the SDK module notifies this event to the application program.

Callback Parameters:

wParam: Result for command

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: The address of the Option struct

UCSAPI_ACU_OPTION_PTR pOption;

UCSAPI_CALLBACK_EVENT_SET_ACU_OPTION

Description:

In response to the ACU option setting request by the application program, the SDK module notifies this event to the application program.

Callback Parameters:

wParam: Result for command

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: N/A

UCSAPI_CALLBACK_EVENT_GET_ACU_LOCKSCHEDULE

Description:

In response to the ACU lock schedule request by the application program,

Callback Parameters:

wParam: Result for command

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: The address of the LockSchedule struct

UCSAPI_ACU_LOCKSCHEDULE_PTR pSchedule;

UCSAPI_CALLBACK_EVENT_SET_ACU_LOCKSCHEDULE

Description:

In response to the ACU lock schedule setting request by the application program.

Callback Parameters:

wParam: Result for command

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: N/A

UCSAPI_CALLBACK_EVENT_GET_SIREN

Description:

It is response of result for UCSAPI_SendSirenToTerminal (In case when opt value is o.)

Callback Parameters:

wParam: Result Value

UCSAPI_CALLBACK_PARAM_0 pCallback0;

In case when opt value is 0, pCallback0->Progress.TotalNumber is the number of siren data.

lParam:

In case when opt value is 0, it will be UCSAPI_SIREN_CONFIG_PTR

UCSAPI_CALLBACK_EVENT_SET_SIREN

Description:

It is response of the result for UCSAPI_SendSirenToTerminal (In case when opt value is 1.)

Callback Parameters:

wParam: Result value

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: Not use

UCSAPI_CALLBACK_EVENT_SET_SMARTCARD_LAYOUT

Description:

It is response of the result for UCSAPI_SetSmartCardLayoutToTerminal

Callback Parameters:

wParam: Result Value

UCSAPI_CALLBACK_PARAM_0 pCallback0;

lParam: Not use

3.4 Error definitions

Gives definition of error and its value from the error value from SDK

Entire Error value is defined in UCSAPI_Error.h file

3.4.1 Success

Definition used for success in error code.

UCSAPIERR_NONE

Prototype:

#define UCSAPIERR_NONE (0)

Description:

Error value when its succed. By mean that not Error is succeed, but the function.

3.4.2 General error definitions

Definition of general error value

This error value starts with UCSAPIERR_BASE_GENERAL(0)

UCSAPIERR_INVALID_POINTER

Prototype:

#define UCSAPIERR_INVALID_POINTER (0x0001)

Description:

Applied with wrong pointer value..

UCSAPIERR_INVALID_TYPE

Prototype:

#define UCSAPIERR_INVALID_TYPE (0x0002)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

Applied with wrong type value

.

UCSAPIERR_INVALID_PARAMETER

Prototype:

#define UCSAPIERR_INVALID_PARAMETER (0x0003)

Description:

Applied with wrong parameter value.

UCSAPIERR_INVALID_DATA

Prototype:

#define UCSAPIERR_INVALID_DATA (0x0004)

Description:

Applied with wrong data value.

UCSAPIERR_FUNCTION_FAIL

Prototype:

#define UCSAPIERR_FUNCTION_FAIL (0x0005)

Description:

.Occur when internal function error by causing process fail.

UCSAPIERR_NOT_SERVER_ACTIVE

Prototype:

#define UCSAPIERR_NOT_SERVER_ACTIVE (0x0006)

Description:

Server has not started.

UCSAPIERR_INVALID_TERMINAL

Prototype:

#define UCSAPIERR_INVALID_TERMINAL (0x0007)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

Terminal is not connected.

UCSAPIERR_PROCESS_FAIL

Prototype:

#define UCSAPIERR_PROCESS_FAIL (0x0008)

Description:

Failed during processing

.

UCSAPIERR_USER_CANCEL

Prototype:

#define UCSAPIERR_USER_CANCEL (0x0009)

Description:

.Cancel process by a user

UCSAPIERR_UNKNOWN_REASON

Prototype:

#define UCSAPIERR_UNKNOWN_REASON (0x0010)

Description:

Unkown Error

3.4.3 Data size related error definitions

Definition of error value for a data.

This error value starts from UCSAPIERR_BASE_MEMORY (0X0200).

UCSAPIERR_CODE_SIZE

Prototype:

#define UCSAPIERR_CODE_SIZE (0x0201)

Description:

.Eceed value for Access Group Code.

UCSAPIERR_USER_ID_SIZE

Prototype:

#define UCSAPIERR_USER_ID_SIZE (0x0202)

Description:

Eceed value of User ID size

UCSAPIERR_USER_NAME_SIZE

Prototype:

#define UCSAPIERR_USER_NAME_SIZE (0x0203)

Description:

Eceed value of User's name size.

UCSAPIERR_UNIQUE_ID_SIZE

Prototype:

#define UCSAPIERR_UNIQUE_ID_SIZE (0x0204)

Description:

Eceed value of UNIQUE ID size.

UCSAPIERR_INVALID_SECURITY_LEVEL

Prototype:

#define UCSAPIERR_INVALID_SECURITY_LEVEN (0x0205)

Description:

Eceed value of authentication level range.

UCSAPIERR_PASSWORD_SIZE

Prototype:

#define UCSAPIERR_PASSWORD_SIZE (0x0206)

Description:

Eceed size of password value.

UCSAPIERR_PICTURE_SIZE

Prototype:

#define UCSAPIERR_PICTURE _SIZE (0x0207)

Description:

Eceed value of User's picture image

UCSAPIERR_INVALID_PICTURE_TYPE

Prototype:

#define UCSAPIERR_INVALID_PICTURE_TYPE (0x0208)

Description:

Does not support user's picture image.

UCSAPIERR_RFID_SIZE

Prototype:

#define UCSAPIERR_RFID_SIZE (0x0209)

Description:

Eceed value of maximum user card size

UCSAPIERR_MAX_CARD_NUMBER

Prototype:

#define UCSAPIERR_MAX_CARD_NUMBER (0x0211)

Description:

Eceed maximum card number. Five cards are limited per user

UCSAPIERR_MAX_FINGER_NUMBER

Prototype:

#define UCSAPIERR_MAX_FINGER_NUMBER (0x0212)

Description:

Eceed number of fingerprint. Five fingerprint per user.

3.4.4 Authentication related error definitions

Definition of error value realated to verification.

.This error value starts with UCSAPIERR_BASE_AUTHENTICATION (0X0300)

.

UCSAPIERR_INVALID_USER

Prototype:

#define UCSAPIERR_INVALID_USER (0x0301)

Description:

Unregistered User.

UCSAPIERR_UNAUTHORIZED

Prototype:

#define UCSAPIERR_UNAUTHORIZED (0x0302)

Description:

FP, Card, PIN matching fail.

UCSAPIERR_PERMISSION

Prototype:

#define UCSAPIERR_PERMISSION (0x0303)

Description:

No authorization.

UCSAPIERR_FINGER_CAPTURE_FAIL

Prototype:

#define UCSAPIERR_FINGER_CAPTURE_FAIL (0x0304)

Description:

FP capture fail

UCSAPIERR_DUP_AUTHENTICATION

Prototype:

#define UCSAPIERR_DUP_AUTHENTICATION (0x0305)

Description:

Continous vification trial. Design to prevent duplicate meal.

UCSAPIERR_ANTIPASSBACK

Prototype:

#define UCSAPIERR_ANTIPASSBACK (0x0306)

Description:

Failed authentication for anti-passback.

UCSAPIERR_NETWORK

Prototype:

#define UCSAPIERR_NETWORK (0x0307)

Description:

No response from a network server.

UCSAPIERR_SERVER_BUSY

Prototype:

#define UCSAPIERR_SERVER_BUSY (0x0308)

Description:

Authentication can not be done, cause of busy server.

UCSAPIERR_FACE_DETECTION

Prototype:

#define UCSAPIERR_FACE_DETECTION (0x0309)

Description:

Face detection fail.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4. API Reference for COM

Properties and methods to use a COM module, UCSAPICOM.dll, are described in this chapter.

4.1 UCSAPI Object

As the main object to use UCSAPICOM.dll, it provides the basic functions of UCS SDK and operates as the basic object that obtains various child objects. To use SDK, this object must therefore be declared.

4.1.1 Properties

Various properties of UCSAPI objects are described.

ErrorCode

Prototype:

[ReadOnly] long ErrorCode;

Description:

This property contains the value on errors that occurred during executed method and property setup.

The value of 0 represents success, while all other values represent failure.

Errors that occurred during child object's method and property setup can also be obtained with this value.

ConnectionsOfTerminal

Prototype:

[ReadOnly] long ConnectionsOfTerminal;

Description:

This property contains the value of the number of terminals connected to the server.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

This value can be obtained after the GetTerminalCount() method is called.

TerminalUserData

Prototype:

[ReadOnly] VARIANT TerminalUserData;

Description:

This property obtains the interface to obtain the user information from the terminal.

This interface needs to be obtained and used to obtain user information from EventGetUserInfoList / EvetGetUserData callback events after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called. Refer to IterminalUserData description for more details.

ServerUserData

Prototype:

[ReadOnly] VARIANT ServerUserData;

Description:

This property obtains the interface to send user information to the terminal.

This interface needs to be obtained and used to set up user information to be sent to the terminal before the AddUserToTerminal method is called. Refer to IServerUserData description for more details.

AccessLogData

Prototype:

[ReadOnly] VARIANT AccessLogData;

Description:

This property obtains the interface to obtain authentication log from the terminal.

This interface needs to be obtained and used to obtain authentication log from the EventGetAccessLog callback event occurred after the GetAccessLog method is called. Refer to IAccessLogData description for more details.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

AccessControlData

Prototype:

[ReadOnly] VARIANT AccessControlData;

Description:

This property obtains the interface to set up access control data with the terminal.

This interface needs to be obtained and used in order to set up the access rights data before the SetAccessControlDataToTerminal method is called. Refer to IAccessControlData description for more details.

TerminalMacAddr

Prototype:

[ReadOnly] LONG TerminalID

Description:

Get the MAC address for the specified terminal(Mac Address return by Hex String)

4.1.2 Methods

Various methods of UCSAPI objects are described.

ServerStart

Prototype:

HRESULT ServerStart(long MaxTerminal, long Port);

Description:

This method initializes UCSAPI SDK and implements server functions.

Parameters:

MaxTerminal:

This parameter defines the maximum number of terminals that can be connected. SDK can improve speed by assigning internal memory capacity in advance according to the maximum number of terminals. If the

number of connected terminals exceeds the maximum number, memory is increased automatically to increase the number of connections.

Port :

The communication port for terminal connection. The default value is 9870. If this value is changed, the terminal's port value also needs to be changed.

Related Properties

ErrorCode

Callback Event:

EventTerminalConnected(long TerminalID, BSTR TerminalIP);

Event Parameters:

TerminalID:

Terminal ID

TerminalIP:

The character string that contains the terminal's IP address value

ServerStop

Prototype:

HRESULT ServerStop();

Description:

This method disconnects all connected terminals and stops server functions.

Parameters:

N/A

Related Properties

ErrorCode

Callback Event:

N/A

Event Parameters

N/A

SetTerminalTimezone

Prototype:

HRESULT SetTerminalTimezone(long TerminalID, BSTR TimezoneName);

Description:

Set up standard time from connected terminal.

Terminal will be using connected terminal's time when it is default, but if Terminal's time and server's time is different, Terminal need to be set as local time

Parameters:

TerminalID:

Terminal ID

TimezoneName:

Select modifying Time zone.

Time zone name can be found from under registry.

HKEY_LOCAL_MACHINE\SOFRWARE\Microsoft\Windows NT\CurrentVersion\TimeZones

Related Properties

ErrorCode

Callback Event:

N/A

Event Prameters

N/A

※ GMT

To check standard time, GMT can be a reference

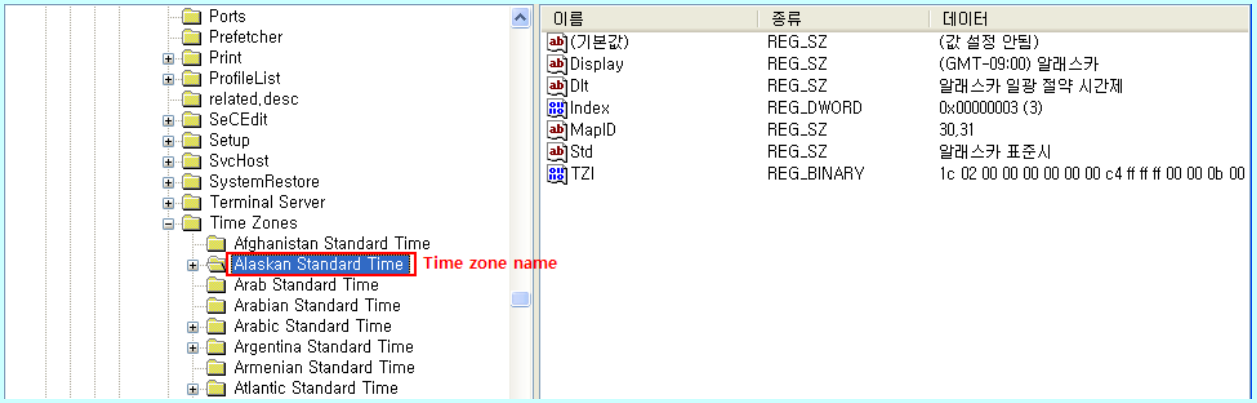
. GMT stand for Greenwich Mean time, that if GMT +9 Korea means it is 9 hour earlier then Greenwich time.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

※ Time zone Name

Time zone Name can be checked from below Registry.

HKEY_LOCAL_MACHINE\SOFRWARE\Microsoft\Windows NT\CurrentVersion\TimeZones



SetError

Prototype:

HRESULT SetError(long TerminalID, long EventType);

Description:

Using callback event from the terminal and send back error code when its return.

Parameters:

TerminalD:

Terminal ID

EventType:

Getting Type Error value for returing to terminal

. 0 – None

1 – Access Log

For example call GetAccessLogFromTerminal then save Log Data to received database.

If fail, setting ErrorType to 1 in the Callback Event function. Calling SetError will make terminal remains updated log and send call again when asking next New Log.

Related Properties

ErrorCode

Related Callback Event:

EventGetAccessLogFromTerminal

Event Prameters

GetTerminalCount

Prototype:

HRESULT GetTerminalCount(void);

Description:

This method obtains the number of terminals connected to the server. This number can be obtained using the ConnectionsOfTerminal property.

Parameters:

N/A

Related Properties

ErrorCode, ConnectionsOfTerminal

Callback Event:

N/A

Event Parameters

N/A

GetFirmwareVersionFromTerminal

Prototype:

HRESULT GetFirmwareVersionFromTerminal(long ClientID, long TerminalID);

Description:

This method obtains the firmware version of the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Related Properties

ErrorCode

Callback Event:

EventFirmwareVersion(long ClientID, long TerminalID, BSTR Version);

Event Parameters

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Version:

This parameter contains the firmware version value in the form of a character string.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UpgradeFirmwareToTerminal

Prototype:

HRESULT UpgradeFirmwareToTerminal (long ClientID, long TerminalID, BSTR FilePath);

Description:

This method upgrades the firmware of the designated terminal. Upgrade progress information is notified with the following event.

EventFirmwareUpgrading / EventFirmwareUpgraded

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

FilePath:

This parameter designates the full path of the firmware file with a character string.

Related Properties

ErrorCode

Callback Event:

EventFirmwareUpgrading(long ClientID, long TerminalID, long CurrentIndex, long TotalNumber);

EventFirmwareUpgraded(long ClientID, long TerminalID);

Event Parameters

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

CurrentIndex:

This parameter contains the index value of the data block under transmission.

TotalNumber:

This parameter contains the total number of data blocks to be sent.

SendUserFileToTerminal

Prototype:

HRESULT SendUserFileToTerminal (long ClientID, long TerminalID, LONG FileType, BSTR FilePath);

Description:

This method send user file to terminal

Parameters:

ClientID: see 1.6 Terminology Description

TerminalID: 1.6 Terminology Description

FileType :

Type of file to download.(see UCSAPI_SendUserFileToTerminal)

FilePath:

Full path of the file

Related Properties

ErrorCode

Callback Event:

EventUserFileUpgrading(long ClientID, long TerminalID, long CurrentIndex, long TotalNumber);

EventUserFileUpgraded(long ClientID, long TerminalID);

Event Prameters

ClientID: see 1.6 Terminology Description

TerminalID: 1.6 Terminology Description

CurrentIndex:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

This parameter contains the index value of the data block under transmission.

TotalNumber:

This parameter contains the total number of data blocks to be sent.

OpenDoorToTerminal

Prototype:

HRESULE OpenDoorToTerminal(long ClientID, long TerminalID);

Description:

This method temporarily opens the locking device of the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Related Properties

ErrorCode

Callback Event:

EventOpenDoor (long ClientID, long TerminalID);

Event Parameters

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetDoorStatusToTerminal

Prototype:

HRESULE SetDoorStatusToTerminal(long ClientID, long TerminalID, long Status);

Description:

This method control lock to fit status value

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Status:

Lock Status (0: temporarily open, 1:start unlock, 2:end unlock)

Related Properties

ErrorCode

Callback Event:

EventOpenDoor (long ClientID, long TerminalID);

Event Parameters

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SendTerminalControl

Prototype:

HRESULE SendTerminalControl(long ClientID, long TerminalID, long lockStatus, long lockType

Description:

This method control terminal to fit parameter values

Parameters:

ClientID: See above

TerminalID: See above

lockStatus:

Lock Status (0:Unlock, 1:Lock)

lockType:

Lock Type (0:Normal, 1:Global) * Global locking ➔ Shutdown

Related Properties

ErrorCode

Callback Event:

EventTerminalControl (long ClientID, long TerminalID, long lockStatus, long lockType);

Event Prameters

ClientID: See above

TerminalID: See above

lockStatus:

Lock Status (0:Unlock, 1:Lock)

lockType:

Lock Type (0:Normal, 1:Global) * Global locking ➔ Shutdown

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SendPrivateMessageToTerminal

Prototype:

HRESULT SendPrivateMessageToTerminal(

LONG ClientID, LONG TerminalID,

LONG Reserved, BSTR TextMessage, short displayTime)

Description:

This method send message for display on terminal LCD.

Parameters:

ClientID: See above

TerminalID: See above

TextMessage :

Text for display.(ref. UCSAPI_SendPrivateMessageToTerminal)

displayTime :

Time(Second value) for display

Related Properties

Callback Event:

EventPrivateMessage(long ClientID, long TerminalID);

Event Prameters

SendPublicMessageToTerminal

Prototype:

HRESULT SendPublicMessageToTerminal(

LONG ClientID, LONG TerminalID, BOOL Show,

BSTR StartDate, BSTR EndDate, BSTR StartTime, BSTR EndTime, BSTR TextMessage)

Description:

This method send public message for display on terminal LCD.

Public message display for setted period and setted time

Parameters:

ClientID: See above

TerminalID: See above

TextMessage :

Public message for display(ref. UCSAPI_SendPublicMessageToTerminal)

StartDate, EndDate :

Period for display(ex : "2012-03-25" or "20120325")

StartTime, EndTime :

Time for display.(ex : "08:30" or "0830")

Related Properties

Callback Event:

EventPublicMessage(long ClientID, long TerminalID);

Event Prameters

SetWiegandFormatToTerminal

Prototype:

HRESULT SetWiegandFormatToTerminal(LONG ClientID, LONG TerminalID, LONG wgdType,
BSTR FilePath);

Description:

To set Wiegand In/Out Format from the terminal. Wiegand Format File comes with SDK and can be created by Wiegand Tool.

Parameters:

ClientID: See above

TerminalID: See above

wgdType:

Getting Type value for define whether Wiegand In or Out.

FilePath:

Entire directory for Wiegand Format Data File

Related Properties

ErrorCode

Related Callback Event:

EventSetWiegandFormat

Event Prameters

SetDoorStatusToACU

Prototype:

HRESULE SetDoorStatusToTerminal(long ClientID, long TerminalID, long Status, long DoorID);

Description:

This method control ACU door lock to fit status value

Parameters:

ClientID: See above

TerminalID: See above

Status:

Lock Status (0: temporarily open, 1:start unlock, 2:end unlock, 3:arm, 4:disarm)

DoorID:

ACU Door ID to control.

Related Properties

ErrorCode

Callback Event:

EventOpenDoor

EventACUStatus

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.2 IServerUserData Interface

The interface to send the user information to the terminal. To send user information to the terminal, the AddUserToTerminal method is called after setting up the user information related properties. After sending the user information, check whether transmission was completed normally by checking the error code of the EventAdduserToTerminal event.

4.2.1 Properties

Various properties of the IServerUserData interface are described.

UserID

Prototype:

[WriteOnly] long UserID;

Description:

This property designates the user ID value. This value can be designated only with numeric data of up to 8 digits.

UniqueID

Prototype:

[WriteOnly] BSTR UniqueID;

Description:

This property designates the unique ID (employee ID) with character string. This value can be used in place of UserID for user identification. The maximum data size that can be designated is 20bytes.

UserName

Prototype:

[WriteOnly] BSTR UserName;

Description:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

This property designates the user name value with character string. The maximum data size that can be designated is 16bytes.

AccessGroup

Prototype:

[WriteOnly] BSTR AccessGroup;

Description:

This property designates the access group code value with character string. The code value consists of a 4byte character string.

SecurityLevel

Prototype:

[WriteOnly] long SecurityLevel;

Description:

This property can set up the authentication security level to be used in fingerprint authentication. It can have any of the following values.

1 - LOWEST
2 - LOWER
3 - LOW
4 - BELOW_NORMAL
5 - NORMAL
6 - ABOVE_NORMAL
7 - HIGH
8 - HIGHER
9 - HIGHEST

The default level is 4 for 1:1 authentication and 5 for 1:N authentication.

IsCheckSimilarFinger

Prototype:

[WriteOnly] BOOL IsCheckSimilarFinger;

Description:

When adding user's fingerprint data to the terminal, the process of whether to check for a similar

Copyright 2009 UNIONCOMMUNITY Co., LTD.

fingerprint or not is designated.

If this value is designated as true, the terminal checks if a similar fingerprint exists by comparing with the fingerprints of all registered users. If a similar fingerprint is detected, registration fails. Since this flag can slow down user addition job by the terminal, the performance may be degraded if there are a large number of registered users.

IsAdmin

Prototype:

[WriteOnly] BOOL IsAdmin;

Description:

This property can designate a user as an administrator. For the terminal with more than 1 registered administrator, the use of the terminal menu can be restricted through the administrator logon process during entry to the setup menu.

IsIdentify

Prototype:

[WriteOnly] BOOL IsIdentify;

Description:

This property can designate to allow the user to use 1:N fingerprint authentication.

Password

Prototype:

[WriteOnly] BSTR Password;

Description:

In case that the user uses the password authentication method, this property designates a password character string. The maximum size of data that can be designated is 8bytes.

FaceNumber

Prototype:

HRESULT FaceNumber([in] long newVal);

Description:

This is the face count that is included in face data.

This is download to terminal for face authentificaion.

This value is in the range of 3 to 10

Related methods:

AddUserToTerminal

Related properties:

FaceData

FaceData

Prototype:

HRESULT FaceData([in] VARIANT newVal);

Description:

This is the face data that is used when face authentication.

This data consists of multiple face information. And FaceNumber notify how many faces in this data.

Related methods:

AddUserToTerminal

Related properties:

FaceNumber

IsFace1toN

Prototype:

HRESULT IsFace1toN([in] BOOL newVal);

Description:

This property can designate to allow the user to use 1:N face authentication.

IsBlacklist

Prototype:

HRESULT IsBlacklist([in] BOOL newVal);

Description:

This property can designate of value for blacklist user

4.2.2 Methods

Various methods of the IServerUserData interface are described.

InitUserData

Prototype:

HRESULT InitUserData()

Description:

Initialize all properties.

Parameters:

None

SetAuthType

Prototype:

HRESULT SetAuthType(BOOL AndOperation, BOOL Finger, BOOL FPCard, BOOL Password, BOOL Card, BOOL CardID);

Description:

This method designates user's authentication type. Each authentication type can be used through AND or OR combination according to the AndOperation flag.

Parameters:

AndOperation:

This parameter designates to allow the use of each authentication type through AND or OR combination.

1 is set for AND combination and 0 for OR combination. For more details, refer to User Property in Section 1.6 Terminology Description.

Finger:

This parameter designates to allow the use of fingerprint authentication.

FPCard:

This parameter designates to allow the use of fingerprint card authentication. The fingerprint card uses a method that authenticates by storing the fingerprint information at the smart card.

Password:

This parameter designates to allow the use of password authentication.

Card:

This parameter designates to allow the use of card authentication.

CardID:

This parameter designates to allow the use of RFID as UserID or UniqueID. CardID does not use the card's RFID as authentication tool, but instead, the card's RFID is simply used as an identifier like UserID.

It must be designated using AND combination with other authentication type.

Related methods

AddUserToTerminal, SendAuthInfoToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SetFPSampleData

- Change to AddFingerData

Prototype:

HRESULT SetFPSampleData(BOOL bInitialize, long nSrcFPDataType, long nFPDataSize,
VARIANT FPData1, VARIANT FPData2);

Description:

This method designates the binary stream data of the template for each finger of FIR converted for fingerprint authentication. For more detailed description on the template, refer to UCBioBSP SDK.

Parameters:

bInitialize:

This parameter designates whether to initialize FIR data and produce new data or not.
If this value is false, the added template data are appended to the FIR data produced internally to produce one FIR data with several template data. If this value is true, all existing FIR data are deleted and new data are produced.

nSrcFPDataType :

The type information of the template to be added. Refer to UCBioAPI_TEMPLATE_TYPE for relevant values.

nFPDataSize :

The size data of the template to be added

FPData1:

Template data to be added. (Binary stream data)

FPData2:

The second template data of a finger to be added. (Binary stream data)

Related properties:

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

AddFingerData

Prototype:

HRESULT AddFingerData(long FingerID, long FPDataType,
VARIANT FPData1, VARIANT FPData2);

Description:

This method designates the finger information and the binary stream data of the template for each finger of FIR converted for fingerprint authentication.

For more detailed description on the template, refer to UCBioBSP SDK.

Parameters:

FingerID :

Finger Infomation(1:Right_Thumb, 10:Left_Little)

FPType :

The type of the template to be added

FPData1:

Template data to be added. (Binary stream data)

FPData2:

The second template data of a finger to be added. (Binary stream data)

Related properties:

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SetDuressFinger

Prototype:

HRESULT SetDuressFinger(long FingerID, long Value)

Description:

Set duress finger.

If duress finger input terminal, terminal work normal status.

But terminal trans result 0x21(33) - not zero - to server

Parameters:

FingerID :

Duress finger ID(1:Right_Thumb, 10:Left_Little)

Value :

Is duress finger or not(0:normal finger, 1:duress finger)

Related properties:

ErrorCode

SetCardData

Prototype:

HRESULT SetCardData(BOOL bInitialize, BSTR RFID);

Description:

This method designates RFID data for card authentication.

Parameters:

bInitialize:

This parameter designates whether to initialize RFID data and produce new data or not.

If this value is false, the added RFID data are appended to the RFID data produced internally to produce several RFID data.

If this value is true, all existing RFID data are deleted and new data are produced.

RFID :

This parameter designates the RFID value to be added with the character string. The maximum size of data that can be designated is 16bytes.

Related properties:

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SetPictureData

Prototype:

HRESULT SetPictureData(long PictureDataLength, BSTR PictureDataType, VARIANT PictureData);

Description:

This method designates the picture data with binary stream.

Parameters:

PictureDataLength:

This parameter designates the length of picture data.

PictureDataType:

This parameter designates the type value of picture data with the character string. (Currently, only "JPG" is supported.)

It designates the file extension value with the character string.

PictureData:

Picture data to be added. (Binary stream data)

Related properties:

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetAccessDate

Prototype:

HRESULT SetAccessDate(long AccessDateType, long StartYear, long StartMonth, long StartDay, long EndYear, long EndMonth, long EndDay);

Description:

This method designates the period allowed for access or the period not allowed for access. Three access period data can be designated; not used, allowed access period, and access restriction period. The following values are available.

Parameters:

AccessDateType:

This parameter designates the type of access period data. The following values are available.

0 - Not used
1 - Period allowed for authentication designated
2 - Period not allowed for authentication designated

StartYear / StartMonth / StartDay:

This parameter designates the start date of the access period.

EndYear / EndMonth / EndDay:

This parameter designates the end date of the access period.

Related properties:

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

AddUserToTerminal

Prototype:

HRESULT AddUserToTerminal(long ClientID, long TerminalID, BOOL IsOverwrite);

Description:

This method sends the user information to the designated terminal. User information needs to be produced using the user information related properties and methods before the AddUserTerminal method is called.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

IsOverwrite:

This parameter designates whether to overwrite an already registered user or not. The default value is 1.

Related properties:

ErrorCode

Callback Event:

EventAddUser

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

※ Note

In case of sending multiple numbers of user data to the terminal using the AddUserToTerminal method, the EventAddUser callback event must be checked after the AddUserToTerminal method is called. The next user data is sent only after the transmission is processed normally.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.3 ITerminalUserData Interface

The interface related to terminal's user information management and get function. This interface needs to be obtained and used in order to obtain or delete the number of users, user information list, and user data.

4.3.1 Properties

Various properties of the ITerminalUserData interface are described.

CurrentIndex / TotalNumber

Prototype:

[ReadOnly]	long	CurrentIndex;
[ReadOnly]	long	TotalNumber;

Description:

In case of obtaining multiple numbers of user information lists, this property contains the total number of lists and the index of the current record. It can be obtained after the GetUserInfoListFromTerminal method is called.

Related methods:

GetUserInfoListFromTerminal,

UserID

Prototype:

[ReadOnly]	long	UserID;

Description:

This property contains the user ID value.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UniqueID

Prototype:

[ReadOnly] BSTR UniqueID;

Description:

This property contains the unique ID value (employee ID).

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

UserName

Prototype:

[ReadOnly] BSTR UserName;

Description:

This property contains the user name value.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

AccessGroup

Prototype:

[ReadOnly] BSTR AccessGroup;

Description:

This property contains the access group code value.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

IsAdmin

Prototype:

[ReadOnly] BOOL IsAdmin;

Description:

This property contains the flag value on whether the user is an administrator or not.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

IsIdentify

Prototype:

[ReadOnly] BOOL IsIdentify;

Description:

This property contains the flag value on whether 1:N fingerprint authentication is allowed or not.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsFinger, TotalFingerCount, FingerID, FPSampleDataLength, SampleNumber, FPSampleData, SecurityLevel

AccessDateType

Prototype:

[ReadOnly] long AccessDateType;

Description:

This property contains the type value of access period data. The following values are available.
It can be obtained after the GetUserDataFromTerminal method is called.

0 - Not used
1 - Period allowed for authentication designated
2 - Period not allowed for authentication designated

Related methods:

GetUserDataFromTerminal

Related properties:

StartAccessDate, EndAccessDate

StartAccessDate/EndAccessDate

Prototype:

[ReadOnly]	BSTR	StartAccessDate;
[ReadOnly]	BSTR	EndAccessDate;

Description:

This property contains the start/end date of access period.
The data format is yyyy-MM-dd.
It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserDataFromTerminal

Related Properties:

AccessDateType

SecurityLevel

Prototype:

[ReadOnly]	long	SecurityLevel;

Description:

This property contains the authentication security level to be used in fingerprint authentication.
It can be obtained after the GetUserDataFromTerminal method is called.
The following values are available.

1 - LOWEST
2 - LOWER
3 - LOW
4 - BELOW_NORMAL
5 - NORMAL
6 - ABOVE_NORMAL
7 - HIGH
8 - HIGHER
9 - HIGHEST

The default value is 4 for 1:1 authentication and 5 for 1:N authentication.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger, TotalFingerCount, FingerID, FPSampleDataLength, SampleNumber, FPSampleData

IsAndOperation

Prototype:

[ReadOnly] BOOL IsAndOperation;

Description:

This property contains the flag value on the AND/OR combination of the authentication type. This value allows the use of fingerprint, card, and password authentication types through AND or OR combination. For more details, refer to User Property in Section 1.6 Terminology Description.
It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger, IsFPCard, IsCard, IsPassword

IsFinger

Prototype:

[ReadOnly] BOOL IsFinger;

Description:

This property contains the flag value that allows user's fingerprint authentication.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsAndOperation, TotalFingerCount, FingerID, FPSampleDataLength, SampleNumber, FPSampleData, SecurityLevel

IsFPCard

Prototype:

[ReadOnly] BOOL IsFPCard;

Description:

This property contains the flag value that allows user's fingerprint card authentication.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsAndOperation

IsCard

Prototype:

[ReadOnly] BOOL IsCard;

Description:

This property contains the flag value that allows user's card authentication.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsAndOperation, CardNumber, RFID

IsCardID

Prototype:

[ReadOnly] BOOL IsCardID;

Description:

This property contains the flag value on whether Card user's RFID is used as ID for user identification or not.

CardID does not use the card's RFID as authentication tool, but instead, the card's RFID is simply used as an identifier like UserID. It must be designated using AND combination with other authentication type.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsAndOperation

Copyright 2009 UNIONCOMMUNITY Co., LTD.

IsPassword

Prototype:

[ReadOnly] BOOL IsPassword;

Description:

This property contains the flag value that allows password authentication.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

IsAndOperation, Password

Password

Prototype:

[ReadOnly] BSTR Password;

Description:

This property contains the password value in the form of a character string. The maximum size of data that can be designated is 8bytes.

It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:

GetUserDataFromTerminal

Related properties:

IsPassword

CardNumber

Prototype:

[ReadOnly] long CardNumber;

Description:

In case that the user uses the card authentication method, this property contains the value of the number of registered RFIDs.
It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:
GetUserDataFromTerminal

Related properties:
IsCard, RFID

RFID

Prototype:
[ReadOnly] BSTR RFID(long nIndex);

Description:
In case that the user uses the card authentication method, this property contains the data value of registered RFID.
It can be obtained after the GetUserDataFromTerminal method is called.

Parameters:
nIndex
The index number of RFID to be obtained

Related methods:
GetUserDataFromTerminal

Related properties:
IsCard, CardNumber

PictureDataLength

Prototype:
[ReadOnly] long PictureDataLength;

Description:
This property contains the size value of picture data.

It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:

GetUserDataFromTerminal

Related properties:

PictureData

PictureData

Prototype:

[ReadOnly] VARIANT PictureData;

Description:

This property contains the picture data value in the form of a binary stream. The length value of data is contained in the PictureDataLength property.

It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserDataFromTerminal

Related properties:

PictureDataLength

TotalFingerCount

Prototype:

[ReadOnly] long TotalFingerCount;

Description:

This property contains the total number of fingers of converted FIR.

It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger, FingerID, FPSampleDataLength, SampleNumber, FPSampleData

FingerID

Prototype:

[ReadOnly] long FingerID(long nIndex);

Description:

This property contains the finger ID information of converted FIR in the form of an array.
nIndex can have a value between 0 and (TotalFingerCount-1).
It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger,TotalFingerCount, FPSampleDataLength, SampleNumber, FPSampleData

SampleNumber

Prototype:

[ReadOnly] long SampleNumber;

Description:

This property contains the number of templates for each finger of converted FIR. It contains the value of 1 or 2.
It can be obtained after the GetUserDataFromTerminal method is called.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger, TotalFingerCount, FingerID, FPSampleDataLength, FPSampleData

Copyright 2009 UNIONCOMMUNITY Co., LTD.

FPSampleData

Prototype:

[ReadOnly] VARIANT FPSampleData(long nFigerID, long nSampleNum);

Description:

This property contains template's binary stream data for each finger of converted FIR.
nFingerID and SampleNum can be obtained using the FingerID and SampleNumber property.
The length value of binary stream data can be obtained using the FPSampleDataLength property.
It can be obtained after the GetUserDataFromTerminal method is called.

Parameters:

nFingerID:

Finger ID number to be obtained

nSampleNum:

Sample number to be obtained. The value of 0 or 1 is used.

Related methods:

GetUserDataFromTerminal

Related properties:

IsFinger, TotalFingerCount, FingerID, FPSampleDataLength, SampleNumber

FaceNumber

Prototype:

HRESULT FaceNumber([out, retval] long *pVal);

Description:

This property contains count of face in FaceData(min 3, max 10)

Related methods:

GetUserDataFromTerminal

Related properties:

FaceData

FaceData

Prototype:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

HRESULT FaceData([out, retval] VARIANT *pVal);

Description:

This property contains template's binary stream data for each face data
Each face data is composed 4bytes length and nbytes binary data.

Related methods:

GetUserDataFromTerminal

Related properties:

FaceNumber

IsBlacklist

Prototype:

[ReadOnly] BOOL IsBlacklist;

Description:

This property contains the flag of blacklist user.
It can be obtained after GetUserInfoListFromTerminal / GetUserDataFromTerminal methods are called.

Related methods:

GetUserInfoListFromTerminal, GetUserDataFromTerminal

Related properties:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.3.2 Methods

Various methods of the ITerminalUserData interface are described.

GetUserCountFromTerminal

Prototype:

HRESULT GetUserCountFromTerminal(long ClientID, long TerminalID);

Description:

This method obtains the total number of registered users from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Related Properties

ErrorCode

Callback Event:

EventGetUserCount

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

AdminNumber:

The number of registered administrators

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UserNumber:

The number of registered users

GetUserDataFromTerminal

Prototype:

HRESULT GetUserDataFromTerminal(long ClientID, long TerminalID, long UserID);

Description:

This method obtains the user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

UserID:

User ID

Related Properties

ErrorCode, UserID, UserName, UniqueID, AccessGroup, AccessDateType, StartAccessDate, EndAccessDate, IsAdmin, IsIdentify, IsAndOperation, IsFinger, IsFPCard, IsCard, IsPassword, IsCardID, Password, CardNumber, RFID, SecurityLevel, TotalFingerCount, FingerID, FPSampleDataLength, SampleNumber, FPSampleData, PictureDataLength, PictureData

Callback Event:

EventGetUserData

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Copyright 2009 UNIONCOMMUNITY Co., LTD.

DeleteUserFromTerminal

Prototype:

HRESULT DeleteUserFromTerminal(long ClientID, long TerminalID, long UserID);

Description:

This method deletes the user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

UserID:

User ID

Related Properties

ErrorCode

Callback Event:

EventDeleteUser

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

UserID:

User ID

Copyright 2009 UNIONCOMMUNITY Co., LTD.

DeleteAllUserFromTerminal

Prototype:

HRESULT DeleteAllUserFromTerminal(long ClientID, long TerminalID);

Description:

This method deletes all user data from the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Related Properties

ErrorCode

Callback Event:

EventDeleteAllUser

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

RegistFaceFromTerminal

Prototype:

HRESULT RegistFaceFromTerminal (long ClinetID, long TerminalID, long Opt);

Description:

This method get regist face data from terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

Opt :

This is command opotion(0:Start, 1:cancel)

Related Properties

ErrorCode

Callback Event:

EventRegistFace

4.4 IAccessLogData Interface

The interface related to the authentication log get function of the terminal. This interface is required to obtain the authentication log of the terminal.

4.4.1 Properties

Various properties of the IAccessLogData interface are described.

CurrentIndex / TotalNumber

Prototype:

[ReadOnly]	long	CurrentIndex;
[ReadOnly]	long	TotalNumber;

Description:

In case of obtaining several numbers of log records, this property contains the total number of records and the index of the current record.

It can be obtained after GetAccessLogFromTerminal methods are called.

Related methods:

GetAccessLogFromTerminal

UserID

Prototype:

[ReadOnly]	long	UserID;

Description:

This property contains the user ID value.

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

Copyright 2009 UNIONCOMMUNITY Co., LTD.

AuthType

Prototype:

[ReadOnly] long AuthType;

Description:

This property contains the authentication type value. The following values are available.

0 - 1:N fingerprint authenticaiton
1 - 1:1 fingerprint authenticaiton
2 - Fingerprint and card authentication
3 - Card authentication
4 - Password authentication

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

AuthMode

Prototype:

[ReadOnly] long AuthMode;

Description:

This property contains the authentication mode value. The following values are available.

0 - Office start
1 - Office leave
2 - General (General access)
3 - Work outside
4 - Return to office

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

Copyright 2009 UNIONCOMMUNITY Co., LTD.

DateTime

Prototype:

[ReadOnly] BSTR DateTime;

Description:

This property contains the authentication time data in the form of a character string.

The data format is "yyyy-MM-dd hh:mm:ss".

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

IsAuthorized

Prototype:

[ReadOnly] BOOL IsAuthorized;

Description:

This property contains the authentication result value. This value is 0 for authentication success and 1 for failure.

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

RFID

Prototype:

[ReadOnly] BSTR RFID;

Description:

In case the authentication type is card, this property contains the RFID value in the form of a character string.

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

PictureDataLength

Prototype:

[ReadOnly] long PictureDataLength;

Description:

This property contains the size value of picture data.

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

Related properties:

PictureData

PictureData

Prototype:

[ReadOnly] VARIANT PictureData;

Description:

This property contains picture data in the form of a binary stream. The PictureDataLength property contains the length value of data.

It can be obtained after the GetAccessLogFromTerminal method is called.

Related methods:

GetAccessLogFromTerminal

Related properties:

PictureDataLength

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.4.2 Methods

Various methods of the IAccessLogData interface are described.

SetPeriod

Prototype:

HRESULT SetPeriod(long StartYear, long StartMonth, long StartDay,
long EndYear, long EndMonth, long EndDay);

Description:

Period information is set in case user wants to get authentication record information for a limited period.

This Method is GetAccessLogCountFromTerminal, GetAccessLogFromTerminal Method. When calling, it is used in case of LogType = 3.

Parameters:

StartYear/StartMonth/StartDay:

Specify the start date.

EndYear/EndMonth/EndDay:

Specify the end date.

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

GetAccessLogCountFromTerminal

Prototype:

HRESULT GetAccessLogCountFromTerminal(long ClientID, long TerminalID, long LogType);

Description:

This method obtains the number of authentication logs stored at the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the type of the log to obtain. The following values are available.

0 - New log
1 - Log already sent to the server
2 - All stored logs
3 - Period logs

If LogType = 3, firstly set period information using SetPeriod method.

Related properties

ErrorCode

Callback Event:

EventGetAccessLogCount

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogCount:

The number of authentication logs

GetAccessLogFromTerminal

Prototype:

HRESULT GetAccessLogFromTerminal(long ClientID, long TerminalID, long LogType);

Description:

This method obtains the authentication log stored at the designated terminal.

Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

LogType:

This parameter designates the type the log to obtain. The following values are available.

0 - New log
1 - Log already sent to the server
2 - All stored logs
3 - Period Log

If LogType = 3, firstly set period information using SetPeriod method.

Related Properties

ErrorCode, TotalNumber, CurrentIndex, UserID, DateTime, AuthType, AuthMode, IsAuthorized, RFID, PictureDataLength, PictureData

Callback Event:

EventGetAccessLog

Event Parameters:

ClientID:

ID of the client that requested a job. (It is used in client/server model development.)

TerminalID:

Terminal ID

4.5 IAccessControlData Interface

The interface to transmit access control data to the terminal. This interface needs to be loaded and used to set up access control information with the terminal.

4.5.1 Properties

Various properties of IAccessControlData interface are described.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.5.2 Methods

Various methods of IAccessControlData interface are described.

InitData

Prototype:

HRESULT InitData(void);

Description:

This method designates whether to initialize access control data and create new data or not.

Parameters:

N/A

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetTimeZone

Prototype:

HRESULT SetTimeZone(BSTR Code, long nIndex, long StartHour, long StartMinute,
long EndHour, long EndMinute);

Description:

This method adds a time zone during a day allowed for authentication.
Up to 128 time zone codes can be added, and up to 12 time zones can be added to a single time zone code. SDK contains the added information in the form of an array.

Parameters:

Code:

As the identification code value of the time zone to be set up, this parameter is a fixed 4byte character string.

nIndex:

Index on time zone information. This value can have a value between 0 and 11.

StartHour / StartMinute:

This parameter designates the start time of the time zone.

EndHour / EndMinute:

This parameter designates the end time of the time zone.

Related methods

SetAccessControlDataToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Event Parameters:

N/A

SetAccessTime

Prototype:

HRESULT SetAccessTime(BSTR Code, BSTR Sun, BSTR Mon, BSTR Tue, BSTR Wed, BSTR Thu, BSTR, Fri, BSTR Sat, BSTR Hol, BSTR Holiday);

Description:

This method adds an allowed access time for each day of the week.
Up to 128 allowed access time codes can be added, and SDK contains the added information in the form of an array.

Parameters:

Code:

As the identification code value of the allowed access time to be set up, this parameter is a fixed 4byte character string.

Sun/Mon/Tue/Wed/Thu/Fri/Sat/Hol:

These parameters designate the allowed access time zone code for each day of the week to be used during authentication and the allowed access time zone code to be applied to holidays.

Holiday:

This parameter designates the holiday code that was set up at the SetHoliday method. The time zone of the Hol code is applied to the designated holiday code.

Related methods

SetAccessControlDataToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SetHoliday

Prototype:

HRESULT SetHoliday(BSTR Code, long nIndex, long Month, long Day);

Description:

This method adds holiday information.

Up to 64 holiday codes can be added, and up to 32 holidays can be added to a single holiday code. SDK contains added information in the form of an array.

Parameters:

Code:

As the identification code value of the holiday to be set up, this parameter is a fixed 4byte character string.

nIndex:

Index value of the holiday to be added. This value can have a number between 0 and 63.

Month / Day:

This parameter designates the date for the holiday.

Related methods

SetAccessControlDataToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SetAccessGroup

Prototype:

HRESULT SetAccessGroup(BSTR Code, long nIndex, BSTR AccessTime);

Description:

This method adds access group information.

Up to 128 access group codes can be added, and up to 4 allowed access time codes can be added to a single access group code. SDK contains added information in the form of an array.

Parameters:

Code:

As the identification code value of the access group to be set up, this parameter is a fixed 4byte character string.

nIndex:

The index value of the allowed access time code to be added. This value can have a number between 0 and 3.

AccessTime:

This parameter designates the allowed access time code to be used at the access group.

Related methods

SetAccessControlDataToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetAccessControlDataToTerminal

Prototype:

HRESULT SetAccessControlDataToTerminal(long ClientID, long TerminalID, long DataType);

Description:

This method sends to the designated terminal the access control data added by SetTimeZone, SetAccessTime, SetHoliday, SetAccessTime and SetAccessGroup methods. Time zone, access time, holiday and access group information need to be sent separately. Access control information is used at the terminal during authentication. In case stored access control information is not available, the terminal does not implement access control.

Parameters:

ClientID:

ID of the client that requested a job (It is used in client/server model development.)

TerminalID:

Terminal ID

DataType:

This parameter designates access control data to be sent to the terminal. The following values are available.

0 - Time zone information
1 - Holiday information
2 - Allowed access time information
3 - Access group information

Related methods

SetTimeZone, SetHoliday, SetAccessTime, SetAccessGroup

Related properties

ErrorCode

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Callback Event:

HRESULT EventSetAccessControlData(long ClientID, long TerminalID, long DataType);

Event Parameters:

ClientID:

ID of the client that requested a job (It is used in client/server model development.)

TerminalID:

Terminal ID

DataType:

The type value of access control data

4.6 IServerAuthentication Interface

The interface to implement server authentication. The application program requires this interface to reply to the user authentication request from the terminal.

4.6.1 Properties

Various properties of the IServerAuthentication interface are described.

DeviceID

Prototype:

[ReadOnly] long DeviceID;

Description:

This is Input Device ID.

You can use this propety after events about server authentication.

Related Events:

EventAuthTypeWithUserID

EventAuthTypeWithUniqueID

EventVerifyCard

EventVerifyFinger1to1

EventVerifyFinger1toN

EventVerifyPassword

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.6.2 Methods

Various methods of the IServerAuthentication interface are described.

SetAuthType

Prototype:

HRESULT SetAuthType(BOOL AndOperation, BOOL Finger, BOOL FPCard, BOOL Password, BOOL Card, BOOL CardID);

Description:

This method designates the user's authentication type. Each authentication type can be used through AND or OR combination according to the AndOperation flag. It must be used before the SendAuthInfoToTerminal method is called.

Parameters:

AndOperation:

If this value is true, authentication with AND combination is allowed. If this value is false, authentication with OR combination is allowed.

Finger:

This parameter designates to allow the use of fingerprint authentication.

FPCard:

This parameter designates to allow the use of fingerprint card authentication. The fingerprint card uses the method that authenticates by storing the fingerprint information at the smart card.

Password:

This parameter designates to allow the use of password authentication.

Card:

This parameter designates to allow the use of card authentication.

CardID:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

This parameter designates to allow the use of RFID as UserID or UniqueID. CardID does not use card's RFID as authentication tool, but instead, the card's RFID is simply used as an identifier like UserID.
It must be designated using AND combination with other authentication type.

Related methods

SendAuthInfoToTerminal

Related properties

ErrorCode

Callback Event:

N/A

Event Parameters:

N/A

SendAuthInfoToTerminal

Prototype:

HRESULT SendAuthInfoToTerminal(long TerminalID, long UserID, BOOL IsAccessibility, long ErrorCode);

Description:

When the terminal operates in server authentication mode, the application program needs to immediately send user's authentication information to the terminal in response to the EventAuthTypeWithUserID/EventAuthTypeWithUniqueID event. It must be used after the SetAuthType method is called.

Parameters:

TerminalID:

Terminal ID

UserID:

ID of the user who attempted authentication

IsAccessibility:

This parameter designates the flag value on whether the user has access rights or not. If this value is false, authentication fails at the terminal.

Related Properties

ErrorCode

Callback Event:

N/A

Event Parameters

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SendAuthResultToTerminal

Prototype:

HRESULT SendAuthResultToTerminal(long TerminalID, long UserID, BOOL IsAccessibility, BOOL IsVisitor, BOOL IsAuthorized, BSTR AuthorizedTime, long ErrorCode);

Description:

For user authentication, the terminal notifies the following events to the application program. EventVerifyCard, EventVerifyPassword, EventVerifyFinger_1_TO_1, EventVerifyFinger_1_TO_N Then, the application program must send the user's authentication result to the terminal immediately.

Parameters:

TerminalID:

Terminal ID

UserID:

ID of the authenticated user or the user who attempted authentication

IsAccessibility:

This parameter designates the flag on whether the user has access rights or not. If this value is false, authentication fails at the terminal.

IsVistor:

This parameter designates whether the user is a visitor or not.

IsAuthorized:

This parameter designates whether authentication is success or not.

AuthorizedTime:

This parameter designates the authentication time. The character string in the form of "yyyy-MM-dd hh:mm:ss" is designated for this value.

ErrorCode:

This parameter designates the code of the error that occurs during authentication. The value of 0

Copyright 2009 UNIONCOMMUNITY Co., LTD.

represents no error. Refer to the ErrorCode table for more information.

Related Properties

ErrorCode

Callback Event:

N/A

Event Parameters

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SendAntipassbackResultToTerminal

Prototype:

HRESULT SendAntipassbackResultToTerminal(long TerminalID, long UserID, BOOL bResult);

Description:

. Terminal has its Antipassback option. Event when verification has made, terminal will get status of Antipassback. In orderto get this, Terminal will send EventAntipassback to application program. At the time, program will contain Antipassback status to bResult and send to terminal in real time. This event will only occur when authentication done from the terminal.

Parameters:

TerminalID:

Terminal ID

UserID:

Already verified or attempt user ID

.

bResult:

. Authorization status by Antipassback. Value 1 means enter available

Related Properties

ErrorCode

Callback Event:

EventAntipassback

Event Prameters

N/A

4.7 ITerminalOption Interface

Terminal option setting interface.

Application program is for set and retrieve option from a terminal. Terminal's options are Default, Network setting, lock, Holiday.

4.7.1 Properties

IterminalOption defines each interfaces' Property

.

flagSecuLevel / flagInputIDLength / flagAutoEnterKey / flagSound / flagAuthenticatoin / flagApplication / flagAntipassback / flagNetwork / flagInputIDType / flagAccessLevel / flagPrintText / flagSchedule

Prototype:

[WriteOnly]	long	flagSecuLevel~flagSchedule;

Description:

Getting a flag value from option reference. Only if Flag value is 1, value can be referenced. Terminal can only get reference if flag value is set as 1.

Set related falg and value before call SetOptionToTerminal Method.

Related methods:

SetOptionToTerminal

SecurityLevel_1To1 / SecurityLevel_1ToN

Prototype:

[Read/Write]	long	SecurityLevel_1To1;
[Read/Write]	long	SecurityLevel_1ToN;

Description:

Terminal gets authentication level for 1:1, 1:N. To set this value flagSecuLevel 1. Value can have

Copyright 2009 UNIONCOMMUNITY Co., LTD.

below

1 - LOWEST
2 - LOWER
3 - LOW
4 - BELOW_NORMAL
5 - NORMAL
6 - ABOVE_NORMAL
7 - HIGH
8 - HIGHER
9 - HIGHEST

This value can set flag and related value to SetOptionToTerminal or able to get reference from GetOptionFromTerminal Method.

Related methods:
SetOptionToTerminal
GetOptionFromTerminal

InputIDLength

Prototype:
[Read/Write] long InputIDLength;

Description:
Getting a ID lenghth for the terminal input. Maximum 8 digit number can be set when using UserID. Maximum 20 digit for UniqueID. To set this value need to set 1 in flagInputIDLenght.

This value is to set flag and related value before call SetOptionToTerminal or can get reference after call GetOptionFromTerminal Method

Related methods:
SetOptionToTerminal
GetOptionFromTerminal

AutoEnterKey

Prototype:
[Read/Write] long AutoEnterKey;

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

Ables you to get value for using Terminal Auto Enter. This feature is for inputting Enter Key automatically when it has input key for InputIDLenghth. To set this feature Set value to 1 in flagAutoEnterKey

This value is to set flag and related value before SetOptionToTerminal or reference after call GetOptionFromTerminal Method

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

Sound

Prototype:

[Read/Write] long Sound;

Description:

Can have sound valume from the terminal. Volume can be set from 0 to 20. To Mute terminal set 0. Set value 1 to set flagSound.

This value is to set flag and related value before SetOptionToTerminal or reference after call GetOptionFromTerminal Method

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

Authentication

Prototype:

[Read/Write] long Authentication;

Description:

Getting a value for terminal's authentication method. Check Chepter 1.5 for "Terminal Authentication method" Set value 1 fom flagAuthentication.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method.

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

Application

Prototype:

[Read/Write] long Application;

Description:

Getting mode value in terminal program. Terminal can be used for Access, TNA, Meal. For the reference check Chepter 1.5 "Terminal program mode" To set this vaule 1 in flagApplication.

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method..

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

Antipassback

Prototype:

[Read/Write] long Antipassback;

Description:

Terminal gets antipassback level.

To set, value 1 in flagAntipassback.

This can have following value.

0- Not in Use

1- Authentication during network disconnection.

2- No Authentication during network disconnection.

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

NetworkType / TerminalIP / Subnet / Gateway / ServerIP / Port

Prototype:

[ReadOnly]	long	NetworkType;
[ReadOnly]	BSTR	TerminalIP;
[ReadOnly]	BSTR	Subnet;
[ReadOnly]	BSTR	Gateway;
[ReadOnly]	BSTR	ServerIP;
[ReadOnly]	long	Port;

Description:

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method.

NetworkType

Getting type value for IP address. If 0, static, or 1 for DHCP.

TerminalIP

Getting Terminal a IP.

Subnet

. Getting Terminal Subnet Mask value.

Gateway

Getting Terminal Getway value

ServerIP

Getting IP value terminal connection.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Port

Getting terminal's Port value. Default will be 9870

Related methods:

SetOptionToTerminal

InputIDType

Prototype:

[Read/Write] long InputIDType;

Description:

Getting ID Type value.

value 1 in flagInputIDType for setting

. This value lead to below

0- UserID

1- UniqueID

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method.

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

AccessLevel

Prototype:

[Read/Write] long AccessLevel;

Description:

Getting approach level value. Appointed type for limit authentication type from using input authentication method. 0 will be default value.

set value 1 in flagAccessLevel to use it.

0- Limitless

1- Only to Fingerprint and Password authentication.

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

PrintText

Prototype:

[Read/Write] long PrintText;

Description:

Buffer sequence for the text which will be printed out that the meal printer which is integrated to the terminal.

This value can only be used when printer is connected to the terminal.

Input value 1 in flagPrintText to set.

This value is to set flag and related value before call SetOptionToTerminal Method or can get reference after call GetOptionFromTerminal Method

Related methods:

SetOptionToTerminal

GetOptionFromTerminal

IsUse / StartHour / StartMinute / EndHour / EndMinute

Prototype:

[ReadOnly] long IsUse;

[ReadOnly] long StartHour;

Copyright 2009 UNIONCOMMUNITY Co., LTD.

[ReadOnly]	long	StartMinute;
[ReadOnly]	long	EndHour;
[ReadOnly]	long	EndMinute;

Description:

Getting Lock or Open schedule in the Time zone.

Reference can be done after calling GetDaySchedule Method.

IsUse

Set validation for the Time zone, if 1, time zone validate.

StartHour

Getting Time zone starting time. Start from 0 to 23

StartMinute

Getting minute value from the Time zone. Start from 0 to 59.

EndHourGetting end time from Time zone. Start from 0 to 23.

EndMinute

Getting end minute from Time zone. Start from 0 to 59.

Related methods:

GetOptionFromTerminal

GetDaySchedule

Month / Day

Prototype:

[ReadOnly]	long	Month;
[ReadOnly]	long	Day;

Description:

Able to get Holiday information.

Refence can be found after calling GetHoliday Method.

Month

Getting Month value from Date. From 1 to 12.

Day

. Getting Day value. From 1 to 31.

Related methods:

GetOptionFromTerminal

GetHoliday

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.7.2 Methods

.Explain Method of All ITerminalOption interface

SetOptionToTerminal

Prototype:

HRESULT SetOptionToTerminal(LONG ClinetID, LONG TerminalID);

Description:

Set terminal option. Need to fill related value on regarding Properties and Method.
Please refer to chepter 4.7.1 for regarding Properties and Method.

Parameters:

ClientID:

ID of requested client (For Client/Server model development.)

Terminal ID:

Terminal ID

Related methods

SetHoliday
SetDaySchedule

Related properties

flagSecuLevel ~ flagSchedule
SecurityLevel
InputIDLength
AutoEnterKey
Sound
Authentication
Application
Antipassback

Copyright 2009 UNIONCOMMUNITY Co., LTD.

InputIDType

AccessLevel

PrintText

NetworkType

TerminalIP

Subnet

Gateway

ServerIP

Port

Callback Event:

EventSetTerminalOption

Event Parameters:

ClientID:

ID of requested client ID (For Client/Server model development.)

TerminalID:

Terminal ID

GetOptionFromTerminal

Prototype:

HRESULT GetOptionFromTerminal(LONG ClinetID, LONG TerminalID);

Description:

Import option from the Terminal. After Method call from EventGetTerminalOption, value can be found from Properties and Method.

Please refer to chepter 4.7.1 for Properties and Method.

Parameters:

ClientID:

ID of requested client. (For Client/Server model development.)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Terminal ID:

Terminal ID

Related methods

GetHoliday

GetDaySchedule

Related properties

SecurityLevel_1To1

SecurityLevel_1ToN

InputIDLength

AutoEnterKey

Sound

Authentication

Application

Antipassback

InputIDType

AccessLevel

PrintText

NetworkType

TerminalIP

Subnet

Gateway

ServerIP

Port

Callback Event:

EventGetTerminalOption

Event Parameters:

ClientID:

ID of requested client. (For Client/Server model development.)

TerminalID:

Terminal ID

SetDaySchedule

Prototype:

HRESULT SetDaySchedule(BOOL Initialize, LONG DayOfWeek, LONG ScheduleType, LONG Index, LONG StartHour, LONG StartMinute, LONG EndHour, LONG EndMinute);

Description:

This Method is in use of adding Lock or Open Time zone before calling SetOptionToTerminal.

Parameters:

Initialize:

Appoint to initialize and create new Lock & Open Schedule.

If False(=0) Time zone data will be added continuously and make number of time zone. If True(=1), erase all time zone and create new.

For Schedule, 3 Lock Time zone and 3 Open Time zone each per a day.

DayOfWeek:

Set day and Holiday type.

0 – Sun

1 – Mon

2 – Tue

3 – Wed

4 – Thu

5 – Fri

6 – Sat

7 – Holiday 1

8 – Holiday 2

9 – Holiday 3

ScheduleType:

Appoint whether lock and open

Copyright 2009 UNIONCOMMUNITY Co., LTD.

.

0 – Lock

1 – Open

Index:

Getting Lock and Open Time zone Index vaule.

1 – Lock 1 or Open 1

2 – Lock 2 or Open 2

3 – Lock 3 or Open 3

StartHour

Getting Time zone start value. Value from 0~23.

StartMinute

Getting Mininute value, From 0~59.

EndHour

Getting Hour value, From 0~23.

EndMinute

Getting minute value from Time zone end. From 0~59.

Related methods

SetOptionToTerminal

Related properties

N/A

Callback Event:

N/A

Event Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

GetDaySchedule

Prototype:

HRESULT GetDaySchedule(LONG DayOfWeek, LONG ScheduleType, LONG Index);

Description:

This Method is calling GetOptionFromTerminal Method then getting schedule information from EventGetTerminalOption.

Parameters:

DayOfWeek:

Set date and Holiday Type.

0 – Sun

1 – Mon

2 – Tue

3 – Wed

4 – Thu

5 – Fri

6 – Sat

7 – Holiday 1

8 – Holiday 2

9 – Holiday 3

ScheduleType:

. Set type Lock or Open.

0 – Lock

1 – Open

Index:

Getting Index vaule for Lock and Open Time zone.

1 – Lock 1 or Open 1

2 – Lock 2 or Open 2

3 – Lock 3 or Open 3

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Related methods

GetOptionFromTerminal

Related properties

IsUse, StartHour, StartMinute, EndHour, EndMinute

Callback Event:

N/A

Event Parameters:

N/A

SetHoliday

Prototype:

HRESULT SetHoliday(BOOL Initialize, LONG HolidayType, LONG Month, LONG Day);

This Method is used for for adding Holiday before call SetOptiontoTerminal Method.
Holiday can be set as 3 type. Each Type can be set with each Time zone.
Holiday can be added up to 100.

Parameters:

Initialize:

Appoint whether initialize Holiday and start from new.
If this value is False(=0) then Holiday data will be added continuously with data that has been made internally and make various holiday data. This value is True(=0) then, erase all holiday and create new.

HolidayType:

Appoint Holiday type 1, 2, 3
1 – Holiday 1
2 – Holiday 2
3 – Holiday 3

Month

Getting Month value. Start from 1 to 12.

Day

Getting Day value. Start from 1 to 31.

Related methods

SetOptionToTerminal

Related properties

N/A

Callback Event:

N/A

Event Parameters:

N/A

GetHoliday

Prototype:

HRESULT GetHoliday(LONG Index);

This Method is to check Holiday information through EventGetTerminalOption from terminal by call GetOptionFromTerminal Method. After call Method then refer HolidayType, Month, Day Properties. Holiday can be set maximum 100, so that Index need to be made from 0~99 and call repeatedly.

Parameters:

Index:

Set Index value for importing. This value start from 0 to 99.

Related methods

GetOptionFromTerminal

Related properties

HolidayType, Month, Day

Callback Event:

N/A

Event Parameters:

N/A

Clear

Prototype:

HRESULT Clear();

Description:

This Method erase all internal option setting data.
This is used for when initialize before call GetOptionFromTerminal or after SetOptionToTerminal.

Parameters:

Related methods

GetOptionFromTerminal
SetOptionToTerminal

Related properties

Callback Event:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Event Parameters:

N/A

get_ACUStatusValue

Prototype:

long get_ACUStatusValue(long StatusIndex, long ValueIndex)

Description:

This is property for get ACU Status after receive EventACUStatus.

(Refer to UCSAPI_ACU_STATUS_INFO)

StatusIndex

Set status type for get.

#define UCSAPI_ACU_STATUS_PARTITION 0

#define UCSAPI_ACU_STATUS_ZONE 1

#define UCSAPI_ACU_STATUS_LOCK 2

#define UCSAPI_ACU_STATUS_READER 3

ValueIndex

Set index for get.(base is zero)

Be careful not to exceed the maximum value.

#define MAX_ACU_PARTITION 4

#define MAX_ACU_ZONE 8

#define MAX_ACU_LOCK 4

#define MAX_ACU_READER 8

ACUGetReaderVersion

Prototype:

HRESULT ACUGetReaderVersion(long Index, long *pID, long *pType, long *pHW, long *pMajor, long *pMinor, long *pCustom1, long *pCustom2, long *pOrder);

Description:

This is method for get ACU Reader version after receive EventACUStatus.

(Refer to UCSAPI_ACU_STATUS_INFO)

Index:

Set index for get.

Be careful not to exceed the maximum value.

Ref Parameters:

These are refer values for Reader Version items.

GetOptionFromACU

Prototype:

HRESULT GetOptionFromACU (LONG ClinetID, LONG TerminalID);

Description:

Import option from the ACU. After Method call from EventGetOptionFromACU, value can be found from Properties and Method.

(Refer to UCSAPI_ACU_OPTION)

Parameters:

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Related properties

ACUNetType, ACUNetSPort

get_ACUReaderType

get_ACUReaderOpenTime

get_ACUReaderMode

Related methods

ACUGetNetAddress

ACUGetPartLock

ACUGetReaderPassback

ACUGetPartition

ACUGetZone

ACUGetProgramOption

ACUGetDoorOption

ACUGetInputOption

ACUGetSystemOption

Callback Event:

EventGetOptionFromACU

Copyright 2009 UNIONCOMMUNITY Co., LTD.

SetOptionToACU

Prototype:

HRESULT SetOptionToACU (LONG ClinetID, LONG TerminalID);

Description:

Set ACU option. Need to fill related value on regarding Properties and Method before call. (Refer to UCSAPI_ACU_OPTION)

Parameters:

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Related properties

set_ACUReaderType

set_ACUReaderOpenTime

set_ACUReaderMode

Related methods

ClearACUOptionFlag

ClearACUOptionData

SetACUOptionFlag

ACUSetNetAddress

ACUSetPartLock

ACUSetReaderPassback

ACUSetPartition

ACUSetZone

ACUSetProgramOption

ACUSetDoorOption

ACUSetInputOption

ACUSetSystemOption

Callback Event:

EventSetOptionToACU

GetLockScheduleFromACU

Prototype:

HRESULT GetLockScheduleFromACU (LONG ClinetID, LONG TerminalID, long LockIndex);

Description:

Import lock schedule from the ACU. After Method call from EventGetLockScheduleFromACU, value can be found from Properties and Method.

(Refer to GetDaySchedule for get schedule value)

Parameters:

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Related properties

Refer to GetDaySchedule in TerminalOption

Related methods

Refer to GetDaySchedule in TerminalOption

Callback Event:

EventGetLockScheduleFromACU

SetLockScheduleToACU

Prototype:

HRESULT SetLockScheduleToACU (LONG ClinetID, LONG TerminalID, long LockIndex);

Description:

Set lock schedule of ACU. Need to fill related value on regarding Properties and Method before call this method.

(Refer to SetDaySchedule for get schedule value)

Parameters:

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Related properties

Refer to SetDaySchedule in TerminalOption

Related methods

Refer to SetDaySchedule in TerminalOption

Callback Event:

EventSetLockScheduleFromACU

ClearSirenConfig

Prototype:

HRESULT ClearSirenConfig();

Description:

It initializes the Siren config value and Siren Count value.

Callback Event:

N/A

SetSirenConfig

Prototype:

HRESULT SetSirenConfig(BYTE Hour, BYTE Minute, BYTE Duration,
BYTE Sun, BYTE Mon, BYTE Tue, BYTE Wed, BYTE Thu, BYTE Fri, BYTE Sat, BYTE OffHoliday);

Description:

Set Sirent Config value. Siren Count value will be increased internally.

Callback Event:

N/A

SetSirenToTerminal

Prototype:

HRESULT SetSirenToTerminal(LONG ClientID, LONG TerminalID);

Description:

It transmits to the terminal which designates the Sirent Config value set by SetSirenConfig.

Parameters:

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

Related methods

ClearSirenConfig, SetSirenConfig

Callback Event:

EventSetSirenToTerminal

GetSirenFromTerminal

Prototype:

HRESULT GetSirenFromTerminal(LONG ClientID, LONG TerminalID);

Description:

Obtaining Siren Config which has set in the terminal.

Parameters:

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

Related methods

GetSirenConfig

Callback Event:

EventGetSirenFromTerminal

GetSirenConfig

Prototype:

HRESULT GetSirenConfig(BYTE index, BYTE* Hour, BYTE* Minute, BYTE* Duration,
BYTE* Sun, BYTE* Mon, BYTE* Tue, BYTE* Wed,
BYTE* Thu, BYTE* Fri, BYTE* Sat, BYTE* OffHoliday);

Description:

When obtaining setting value of the terminal, EventGetSirenFromTerminal will be appeared
and it gets Siren Config value of the terminal through this Method.
Index value increases from 0 and gets Siren Config as much as Siren Count which has issued from EventGetSirenFromTerminal

Callback Event:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

4.8 ISmartCardLayout Interface

It is the interface for setting the card layout applying when reading smart card on the terminal.

4.8.1 Properties

It explains about various Property of the interface of ISmartCardLayout

SectorNumber

Prototype:

[ReadOnly] long SectorNumber

Description:

It obtains the number of SectorLayout set on COM.

Everytime when conducting SetSectorLayout, it increases 1 by 1 and when conducing ClearSectorLayout, it will be initialized as 0.

Related methods:

ClearSectorLayout

SetSectorLayout

4.8.2 Methods

It explains about various Property of the interface of ISmartCardLayout

ClearSectorLayout

Prototype:

HRESULT ClearSectorLayout();

Description:

It initializes SectorLayout Data which has saved on COM.

Parameters:

N/A

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Related methods

SetSectorLayout

SetSmartCardLayoutToTerminal

Related properties

SectorNumber

Callback Event:

N/A

SetSectorLayout

Prototype:

HRESULT SetSectorLayout(LONG Sector, LONG KeyType, BSTR KeyData,
LONG Block, LONG StartPoint, LONG DataLength, BYTE Aid0, BYTE Aid1)

Description:

Set the Sector Layout to COM applying to smartcard Layout.

SectorNumber of internal COM will be increased 1 by 1 when setting.

Parameters:

Sector:

It is Sector Number to be applied. Max. 127 (In case of 8K smartcard)

KeyType:

It designates the type of Key Data to get access to the related Sector.

#define UCSAPI_SMARTCARD_KEYTYPE_A 0x60

#define UCSAPI_SMARTCARD_KEYTYPE_B 0x61

KeyData:

It designates the type of Key Data to get access to the related Sector.

Designation value is Hex String (Ex: "000000FFFFFF")

Block:

It is Block Number containing real data. (Range: 0 ~ 3)

StartPoint:

It designates the start point where the real data included in the related Block.

DataLength:

It designates the real length of data to be applied.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Aid0, Aid1:

It is AID value in case when Read type is UCSAPI_SMARTCARD_READTYPE_MAD

Related methods

ClearSectorLayout

SetSmartCardLayoutToTerminal

Related properties

SectorNumber

Callback Event:

N/A

SetSmartCardLayoutToTerminal

Prototype:

HRESULT SetSmartCardLayoutToTerminal(LONG ClientID, LONG TerminalID,
LONG CardType, LONG ReadType, LONG SerialFormat);

Description:

Set the Card Layout applying when reading card on the terminal transmitting the Sector information of COM which has saved as Given Parameter and SetSectorLayout.

Parameters:

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

CardType:

Designates the card type. Refer to the define below.

```
typedef UCSAPI_UINT32 UCSAPI_SMARTCARD_TYPE;
    #define UCSAPI_SMARTCARD_TYPE_DATA      0
    #define UCSAPI_SMARTCARD_TYPE_FINGER    1
```

ReadType:

Designates the data type reading card. Refer to the define below.

```
typedef UCSAPI_UINT32 UCSAPI_SMARTCARD_READTYPE;
    #define UCSAPI_SMARTCARD_READTYPE_SERIAL    0
    #define UCSAPI_SMARTCARD_READTYPE_DATA      1
```

Copyright 2009 UNIONCOMMUNITY Co., LTD.

#define UCSAPI_SMARTCARD_READTYPE_MAD 2

SerialFormat:

Designates the type of indicating serial number when reading the serial number.

Refer to the define below.

typedef UCSAPI_UINT8 UCSAPI_SMARTCARD_SERIALFORMAT;

#define UCSAPI_SMARTCARD_SERIALFORMAT_DEFAULT 0

#define UCSAPI_SMARTCARD_SERIALFORMAT_HEXA 1

#define UCSAPI_SMARTCARD_SERIALFORMAT_DECIMAL 2

#define UCSAPI_SMARTCARD_SERIALFORMAT_35DECIMAL 3

Related properties

SetSectorLayout

Related methods

Callback Event:

EventSetSmartCardLayout

4.9 Events of COM

Events of a COM module, UCSAPICOM.dll, are described in this chapter.

EventUserFileUpgrading

Prototype:

HRESULT EventUserFileUpgrading(

long ClientID,

long TerminalID,

long CurrentIndex,

long TotalNumber);

Description:

This is event to notify the download progress information to the application program.

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

CurrentIndex:

This parameter contains the index value of the data block under transmission.

TotalNumber:

This parameter contains the total number of data blocks to be sent.

Reference

SendUserFileToTerminal

EventUserFileUpgraded

Prototype:

```
HRESULT EventUserFileUpgraded(
        long ClientID,
        long TerminalID);
```

Description:

This is event to notify the download complete information to the application program.

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Reference

SendUserFileToTerminal

EventRegistFace

Prototype:

```
HRESULT EventRegistFace (
        long ClientID,
        long TerminalID,
        long CurrentIndex,
        long TotalNumber,
        VARIANT RegFaceData);
```

Description:

This is event to notify the process of registing face from terminal

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

CurrentIndex:

This parameter contains the current index value of processing for regist face. Base value is 1.

If this value is 0 then this event mean process cancel.

TotalNumber:

This parameter contains the whole input face value. In normal regist, this value is 5, in quick regist, this value is 3. If this value is 0 then this event mean process cancel.

RegFaceData:

Real input face data.(data type is byte array)

Reference

RegistFaceFromTerminal

EventACUStatus

Prototype:

```
HRESULT EventACUStatus (
        long ClientID,
        long TerminalID,
        long Notice,
        VARIANT binStatus,
        BSTR strStatus);
```

Description:

This is periodically event to notify the status of ACU.

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Notice:

This parameter mean that ACU has any problem.

binStatus:

The binary array for struct of ACU_STATUS.

strStatus:

The hex string for struct of ACU_STATUS.

Reference

SetDoorStatusToACU

EventGetLockScheduleFromACU

Prototype:

HRESULT EventGetLockScheduleFromACU (

long ClientID,

long TerminalID,

long LockIndex);

Description:

This is response event for call GetLockScheduleFromACU().

When receive this event, you can get schedule valus using property and method about schedule.

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

LockIndex:

Lock index of ACU for get schedule.

Reference

GetLockScheduleFromACU

EventSetLockScheduleToACU

Prototype:

HRESULT EventSetLockScheduleToACU (

long ClientID,

long TerminalID);

Description:

This is response event for call SetLockScheduleToACU().

Event Prameters

ClientID: See 1.6 Terminology Description

TerminalID: See 1.6 Terminology Description

Reference

SetLockScheduleToACU

EventSetSirenToTerminal

Prototype:

HRESULT EventSetSirenToTerminal(long ClientID, long TerminalID);

Description:

SDK module notifies this event as the result of Sirent Config set on the terminal.

Event Prameters

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

Reference

ClearSirenConfig

SetSirenConfig

SetSirenToTerminal

EventGetSirenFromTerminal

Prototype:

HRESULT EventGetSirenFromTerminal(long ClientID, long TerminalID);

Description:

SDK module notifies this event as the result of Sirent Config set on the terminal.

Event Prameters

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

Reference

GetSirenFromTerminal

GetSirenConfig

EventSetSmartCardLayout

Prototype:

HRESULT EventSetSmartCardLayout(long ClientID, long TerminalID);

Description:

SDK module notifies this event as the result of Sirent Config set on the terminal.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Event Prameters

ClientID: 1.6 Refer to the term explanation

TerminalID: 1.6 Refer to the term explanation

Reference

SetSmartCardLayoutToTerminal

5. Error definitions

Define all Error value and about Error value from UCS SDK.

5.1 Success

Definition for Error value in Success..

UCSAPIERR_NONE

Prototype:

LONG UCSAPIERR_NONE (0)

Description:

Error value when sccuess. Means that not Error but success in function.

5.2 General error definitions

UCSAPIERR_INVALID_POINTER

Prototype:

UCSAPIERR_INVALID_POINTER (1)

Description:

Wrong Pointer value in use.

.

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPIERR_INVALID_TYPE

Prototype:

LONG UCSAPIERR_INVALID_TYPE (2)

Description:

Wrong type value is in use

.

UCSAPIERR_INVALID_PARAMETER

Prototype:

LONG UCSAPIERR_INVALID_PARAMETER (3)

Description:

Used for wrong parameter.

.

UCSAPIERR_INVALID_DATA

Prototype:

LONG UCSAPIERR_INVALID_DATA (4)

Description:

Use in wrong data

UCSAPIERR_FUNCTION_FAIL

Prototype:

LONG UCSAPIERR_FUNCTION_FAIL (5)

Description:

. Error from internal function and fail processing

UCSAPIERR_NOT_SERVER_ACTIVE

Prototype:

LONG UCSAPIERR_NOT_SERVER_ACTIVE (6)

Description:

Server is not on start

Copyright 2009 UNIONCOMMUNITY Co., LTD.

UCSAPIERR_INVALID_TERMINAL

Prototype:

LONG UCSAPIERR_INVALID_TERMINAL (7)

Description:

Terminal is not connected

UCSAPIERR_PROCESS_FAIL

Prototype:

LONG UCSAPIERR_PROCESS_FAIL (8)

Description:

Fail during process

UCSAPIERR_USER_CANCEL

Prototype:

LONG UCSAPIERR_USER_CANCEL (9)

Description:

Process cancel from a user.

UCSAPIERR_UNKNOWN_REASON

Prototype:

LONG UCSAPIERR_UNKNOWN_REASON (16)

Description:

Unknown error.

5.3 Data szie related error definitions

Definition for data size error

UCSAPIERR_CODE_SIZE

Prototype:

LONG UCSAPIERR_CODE_SIZE (513)

Description:

Copyright 2009 UNIONCOMMUNITY Co., LTD.

. Exceed of Access Group Code size.

UCSAPIERR_USER_ID_SIZE

Prototype:

LONG UCSAPIERR_USER_ID_SIZE (514)

Description:

Maximum size of user ID exceed.

UCSAPIERR_USER_NAME_SIZE

Prototype:

LONG UCSAPIERR_USER_NAME_SIZE (515)

Description:

Exceed of user name length.

UCSAPIERR_UNIQUE_ID_SIZE

Prototype:

LONG UCSAPIERR_UNIQUE_ID_SIZE (516)

Description:

Exceed of UNIQUE ID length.

UCSAPIERR_INVALID_SECURITY_LEVEL

Prototype:

LONG UCSAPIERR_INVALID_SECURITY_LEVEN (517)

Description:

Exceed of authentication level.

UCSAPIERR_PASSWORD_SIZE

Prototype:

LONG UCSAPIERR_PASSWORD_SIZE (518)

Description:

Exceed of maximum User PIN size

UCSAPIERR_PICTURE_SIZE

Prototype:

LONG UCSAPIERR_PICTURE _SIZE (519)

Description:

User's Picture image type is not in support

UCSAPIERR_INVALID_PICTURE_TYPE

Prototype:

LONG UCSAPIERR_INVALID_PICTURE_TYPE (520)

Description:

User's Picture image type is not in support

UCSAPIERR_RFID_SIZE

Prototype:

LONG UCSAPIERR_RFID_SIZE (521)

Description:

Exceed of maximum card number length

UCSAPIERR_MAX_CARD_NUMBER

Prototype:

LONG UCSAPIERR_MAX_CARD_NUMBER (529)

Description:

Exceed maximum card capacity. Maximum 5 card can be stored per user.

.

UCSAPIERR_MAX_FINGER_NUMBER

Prototype:

LONG UCSAPIERR_MAX_FINGER_NUMBER (530)

Description:

Exceed maximum fingerprint capacity. Maximum 5 fingerprint can be stored per user

5.4 Authentication related error definitions

Definition for error related to authentication

UCSAPIERR_INVALID_USER

Prototype:

LONG UCSAPIERR_INVALID_USER (769)

Description:

Unregistered user..

UCSAPIERR_UNAUTHORIZED

Prototype:

LONG UCSAPIERR_UNAUTHORIZED (770)

Description:

Fingerprint, card, PIN matching fail.

UCSAPIERR_PERMISSION

Prototype:

LONG UCSAPIERR_PERMISSION (771)

Description:

No autoriztion.

UCSAPIERR_FINGER_CAPTURE_FAIL

Prototype:

LONG UCSAPIERR_FINGER_CAPTURE_FAIL (772)

Description:

FP capture fail

UCSAPIERR_DUP_AUTHENTICATION

Prototype:

LONG UCSAPIERR_DUP_AUTHENTICATION (773)

Copyright 2009 UNIONCOMMUNITY Co., LTD.

Description:

Multiple authentication. Prevent to have duplicate by using card from meal management

UCSAPIERR_ANTIPASSBACK

Prototype:

LONG UCSAPIERR_ANTIPASSBACK (774)

Description:

Authentication fail for antipassback.

UCSAPIERR_NETWORK

Prototype:

LONG UCSAPIERR_NETWORK (775)

Description:

No response from a server due to network problem.

UCSAPIERR_SERVER_BUSY

Prototype:

LONG UCSAPIERR_SERVER_BUSY (776)

Description:

Authentication has not been made due to busy server.

UCSAPIERR_FACE_DETECTION

Prototype:

LONG UCSAPIERR_FACE_DETECTION (777)

Description:

Face detection failed when it set.

Copyright 2009 UNIONCOMMUNITY Co., LTD.