# Obtaining a token for an external system

Short description

The system authorization token (key) is obtained by means of an H2H connection. The request to receive the token is initiated by the mobile application server. To successfully complete the request, an administrator for the external system must be created on the mPOS server, and this administrator must have a callback address in the system, at which a SetToken request from the mPOS server to set the token value will occur.

In general, the scheme for requesting / setting a token is as follows:

1. The external application server sends a GetToken request to the mPOS server
2. The mPOS server calls the SetToken method of the external application server API and passes the token
3. The external application server sets the token and responds to the mPOS server
4. The mPOS server responds to the external application server for a GetToken request

Scheme for obtaining a token for an external system:
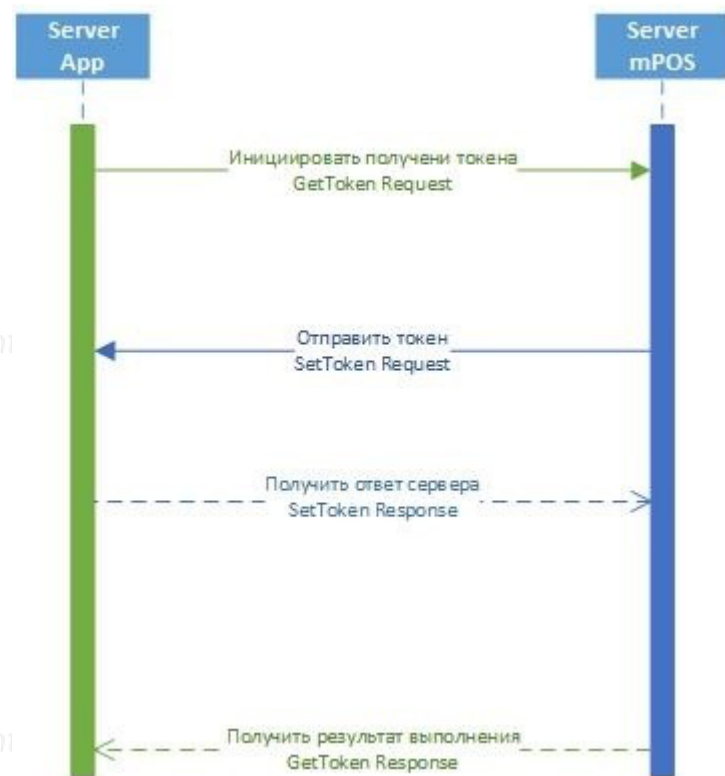
Detailed description

Get token request

The external application server sends a GetToken request to the mPOS server. Url for request: http(s)://[IP]:[PORT]/json/GetToken

GetToken

{
  "@MsgNum": "[Unique MSG number. This field has any format. UUID is recommended]",
  "OpLogin": "[Phone or email of the operator for which you need to get an authorization token]",
  "SysLogin": "[External system administrator login. Set in the AWP in the section of external administrators]",
  "SysPwd": "[Hash of the external system administrator password. Instruction: Generating a hash of the external system administrator password (SysPwd)]",
  "Lang": "[Language designation, for example, rus. The list of all available languages can be viewed and configured at your discretion in AWP: \"Settings\" -> \"Dictionaries\" -> \"Identifier\".]",
  "Info": "[Information about the external system. This field is intended for logging and can have any type and structure at the discretion of the client. For example, you can send information about the name of the system and its version.]"
}

Example:

```
{
 "@MsgNum": "2a487dbd-ebbe-4304-b1eb-8b9c6466f0ba",
 "OpLogin": "OperatorLogin@example.com",
 "SysLogin": "ExtOperatorLogin",
 "SysPwd": "2ff92e6f2fd7be4536361674653e2695f652f0953c04386fb080261e5e5bf19a",
 "Lang": "eng",
 "Info": "Windows 10 Pro"
}
```

✅ SysPwd instruction "Generating a hash of the external system administrator password (SysPwd)"

Set token request

After receiving the request GetToken the mPOS server calls the SetToken method of the external application server API and passes the token. The request URL is set in an external administrator in AWP.

SetToken

{
  "@MsgNum": "[Unique MSG number (as in request)]",
  "OpLogin": "[Operator login for which you need to get an authorization token]",
  "Token": "[Token]",
  "TokenTimeout": "[Token lifetime]",
  "ServerTime": "[Server time dd.mm.yyyy hh24: mi: ss TZH: TZM]"
}

Exaplme:

```
{
 "@MsgNum": "9c99d681-e128-4047-9ae8-f4e55c04548a",
 "OpLogin": "OperatorLogin@example.com",
 "Token": "3967047c-4e07-4554-b0c1-7f13b5d707c9",
 "TokenTimeout": 3000,
 "ServerTime": "30.07.2020 09:33:57 GMT+03:00"
}
```

Set token response

The external application server sets the token and responds to the mPOS server

SetToken

```
{
 "@MsgNum": "[Unique MSG number (as in request)]",
 "ServerTime": "[Server time dd.mm.yyyy hh24: mi: ss TZH: TZM]",
 "Response": {
  "Code": "[Server response code. Will be used in response to GetToken. If successful, code 00 is recommended.]",
  "Description": "[Server response text. Will be used in response to GetToken.]",
  "Info": "[Additional information on the answer. It has an arbitrary format and can have any kind and structure.]"
 }
}
```

Example:

```
{
 "@MsgNum": "9c99d681-e128-4047-9ae8-f4e55c04548a",
 "ServerTime": "30.07.2020 09:33:57 GMT+03:00",
 "Response": {
  "Code": "00",
  "Description": "OK"
 }
}
```

Get token response

After receiving an answer to the request SetToken the mPOS server responds to the external application server for a GetToken request

GetToken

```
{
 "@MsgNum": "[Unique MSG number (as in request)]",
 "ServerTime": "[Server time dd.mm.yyyy hh24: mi: ss TZH: TZM]",
 "Response": {
  "Code": "[Server response code. Possible response codes for errors in token generation on the mPOS side are shown in the table below. If the
generation of the token on the mPOS side is successful and a response to the SetToken is received, the Code from the SetToken response will be used.] ",
  "Description": "[Server response text. If the generation of the token on the mPOS side is successful and a response to the SetToken is received, the
Description from the SetToken response will be used.] ",
  "Info": "[Additional information on the answer. It has any format and can have any kind and structure.] "
 },
 "TokenTimeout": "[Token lifetime. It is obtained in numeric format and contains the time in seconds. The default is 3000, which is equivalent to 50
minutes. You can configure it in AWP in the \"System settings\" tab -> \"Sessions\" -> \"Token lifetime for the external system (seconds)\"] "
}
```

Example:

- In case of success

```
{
 "@MsgNum": "2a487dbd-ebbe-4304-b1eb-8b9c6466f0ba",
 "ServerTime": "29.07.2020 19:53:35 GMT+03:00",
 "Response": {
  "Code": "00",
  "Description": "OK"
 },
 "TokenTimeout": 3000
}
```

- In case of failure

```
{
  "@MsgNum": "2a487dbd-ebbe-4304-b1eb-8b9c6466f0ba",
  "ServerTime": "29.07.2020 19:56:14 GMT+03:00",
  "Response": {
    "Code": "041",
    "Description": "Incorrect password.",
    "Info": "\r\ncore.model.exception.WrongPasswordException: \r\n\tat core.logic.AuthLogic.generateExtToken(AuthLogic.java:72)\r\n\t at core.
api.json.request.impl.GetTokenRequest.handleJsonRequest(GetTokenRequest.java:38)\r\n\t at core.api.json.request.base.BaseJsonRequest.
handleRequest(BaseJsonRequest.java:147)\r\n\t at core.api.json.request.base.BaseJsonRequest.handle(BaseJsonRequest.java:142)\r\n\tat..."
  }
}
```

⚠️ Stack trace in the Info block is sent only if debug mode is enabled on the mPOS server.

Possible response codes in case of errors on the mPOS server side

Code	Description
030	Invalid message format. Contact Support.
040	Unknown operator login. Check the correctness of the data or contact the support service.
041	Incorrect password.
099	A technical error. Try the operation again or contact support.
150	Unknown external system administrator login. Check the correctness of the data or contact the support service.
160	Connection error with external system. Try the operation again or contact support.
403	Access is denied. Contact Support.