EzToken Server REST Technical Integration

Document Number
EZM_EZTKSVREST_00

Issue Status
1.0

Issue Date
15 Mar 2016

Version 1.3.2

Prepared for

EZMCOM Software Product administrator

Prepared by

EZMCOM Inc.
4701 PATRICK HENRY DR, SANTA CLARA, CA, 950541863, US.

Tel: +1   510 396 3894
              +60 (0)12 570 1114
Email: info@ezmcom.com

1.1 Sign-up and Activate flow

This secion illustrate the flow of sign-up and activate the EzToken account.

1.1.1 Create QR-code image for activate

To create a QR-code image for the EzToken to scan and activate.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/regeztoken

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.
contactType	No	The contact type. Use 2 for indicating to use contactDetails param as Email type.
contactDetail	No	Contact details. Eg: email address if provided contactType value is 2.

CURL Request Example:

curl
https://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/regeztoken --
data
'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24A
BDD993&userId=testuser01'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

{
  "returnCode":0,
  "returnMessage":"Success",
  "credential":"JQ7DqBKymXvQljFJcDlXlpUrw",
"encodedQRCodeImg":
"iVBORw0KGgoAAAANSUhEUgAAAMgAAADIAQAAAACFI5MzAAADO0
lEQVR42u2YMa6rMBBFB1G4IxuwxDbo2BJsAIcNhC25YxtIbIB0FFbm
37ENeSl+weRLv3nIsvJyotxgz1xfHvHfLvol/5wEovo5L0Shn21H1LXlR
uS0xHH9aDiOdfK239envKkknbFurjcDtTTKp7dfkJq9iEBq2jHWL8nIt
mvTAlA/f0VkDYgftI5MFS0VFvjH6lwlRBY783N0585dJrhCJzsDnTKuxP
quqsskFJ6K/PVZp+BaS3D3/Ipff48zdullVi0JvS8njzkUeQ1q3tP+KIhU
9NaUr6bkHVLlhgri/As0xJCLOmRsgaqZ0XPBKUko9uD2NS3Dq5Ux+Z
K1pDPlBoW4ABB0Hv13dPBlwptBLSedcpqhsFRNWgMNmXb0mZXqhr
V4IiPr4ZQkDE2oGn7u/MDdS0VL+bCS4KoZRS1OgBkVDUM9eu4yCT
BOUfBy63AFeNXxCxSEp9lWxsJN8fWdwcBe1WqySb0EEWmiFCqoWZ
ySBNgAoVFEp95aFA5Km7QE2yLnWJXNQMbZP9eJ7AZFeI7KpC5REH
H3Ld969ire1UR89LaHWypt0SG8cEoC1wzUlPcWx7XMW0NuTj2nIKLg
4pz8oJ8XeaElbsZfUtrQiV61OJ90NGQgqWUooIjwKectZRfTkM4wDkbo
xLxDPSNJrawlZEpknBH22YpXDVQflaggcKmowJxmnmEJi5pM6DCPP
SmfjC3ieyuuoCXhti9Vi6QTYtjBDNmgJbhw61IvmJNXvR32Mgk9r3fx0
ehVlAJjUJOhlROsFzVsVGq71MEKwuOcPP7tVY98NipItD3zkRNd7jkFk
Zu+04eIZB8lwSltB6no00rrcc5rrSBVu46SdxDHYFSIsZQzhYogrY9SO
LAZe/P2llKPksAMFooi95zF8HbOO9cJUoDU8qEgm1Pk5xINISOFk8L1t
CfbO7zqMpG8g3KmRrI/xkB4Ujk6WEMki/HO8lxilgE6Xk3kmekGgzcxi
5mFJJSRmji21OL0XgrGIwXWAzrMWtLFICaDREHObVN/QeqnT1lM1M
RHz5NJQ6AgEUw+wnIKyVGpJViDIebE064QY1lLSHJi+HwUPnfuKvn9
D9P/J38A4Psy0XDYCfMAAAAASUVORK5CYII\u003d"
}

Response JSON object parameters:

Parameter	Description

returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -13 = License exhausted • -20 = Invalid group or it is not found • -28 = Token quota reach – This indicated user has an active token. To allow user to reactivate from this flow, kindly call the REST API: Delete active token. • -47 = Invalid group state is not enabled • -106 = Invalid SAML Identifier
returnMessage	A summary message of the return code.
credential	A unique credential token. It may be used to check if the generated QR-code image has been scanned and activated by EzToken mobile app. Refer to REST API: Check QR-code image activate status.
encodeQRCodeImg	QR-code image content in Base64 encoded format.

1.1.2 Check QR-code image activate status

To check if the QR-code image generated from the REST API: Create QR-code image, has been scanned and activated by the EzToken mobile app.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/getEzAuthCredentialSoftTkActivateStatus

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description

credential	Yes	A unique credential token generated from REST API: Create QR-code image for activate.

CURL Request Example:

```
curl
https://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/getEzAuthCre
dentialSoftTkActivateStatus --data
'credential=JQ7DqBKymXvQljFJcDlXlpUrw'
```

Http Response Example:

Response Header:

```
HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8
```

Response Body:

```
{
   "returnCode": 0
}
```

Response JSON object parameters:

Parameter	Description
returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success. This indicates the created QR-code has been scanned and activated by the EzToken mobile app. • -1 = System error • -2 = Bad parameter • -5 = Invalid token state. • -25 = Provided credential not found or expired. • -101 = Success Pending. This indicates the created QR-code is pending for activating.

1.2 Push Notification Login flow

This secion illustrate the flow of login via a push notification.

1.2.1 Request push notification for login

To request a push notification being sent to the activated EzToken mobile app account for login.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/auth/authtx/reqpush

Http Request Method:

POST

Http Request Content-Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.
txDetails	Yes	The transaction details in JSON formatted string (flat structure of key-value mapping), i.e. {"IP": "211.25.18.246", "Location": "Kuala Lumpur, Malaysia"}.
txExpiryMins	Yes	The transaction expiry in minutes.
txType	Yes	The transaction type. Use value "1" (Authenticate Direct)
mobilePush	No	The mobile push identifier. If not provided or empty value, the push notification will be attempted to deliver to the default registered push device.

txFlags	No	The transaction flags containing the flag of transaction details. It's a JSON formatted string. Eg: {"txUBio": 0}.
		
		• txUBio = Keys to indicate the authenticate options upon signing on mobile app:
		    o 0 = Default depending on user configuration.
		    o 1 = Voice or Facial recognition.
		    o 2 = Voice and Facial recognition.

CURL Request Example:

```
curl
https://<HOSTNAME>/ezwsrest/rest/engine/auth/authtx/reqpush -
-data
'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24A
BDD993&userId=testuser01&txDetails={"IP": "211.25.18.246",
"Location": "Kuala Lumpur, Malaysia"}&txExpiryMins=3&txType=1'
```

Http Response Example:

Response Header:

```
HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8
```

Response Body:

```
{
  "returnCode":0,
  "refcode":"9d6c1f9489b13b43",
  "pushmsg":
"eyJyYyI6MCwiZ2lkIjo2MiwidWlkIjoiVEVTVFVFVTRVIwMSIsInJlZiI6Ijlk
NmMxZjk0ODliMTNiNDMifQ\u003d\u003d"
}
```

Response JSON object parameters:

Parameter	Description

returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -3 = Invalid user • -5 = Invalid token state. • -20 = Invalid group or it is not found • -65 = No active token found • -47 = Invalid group state is not enabled • -98 = Error in sending push message • -101 = Invalid user OOB contact • -104 = Transaction not found. • -106 = Invalid SAML Identifier
refcode	A unique reference code. It may be used to check if the push notification has been approved/rejected at EzToken mobile app. Refer to REST API: Check push notification approval status for login.
pushmsg	Push message sent.

1.2.2   Check push notification approval status

To check if a particular push notification requested from the REST AP: Request push notificaiton, has been approved/rejected at EzToken mobile app. Note: This apply for both Login and Transaction type push notification request.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/auth/tx/pullstatus

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.

txRef	Yes	The transaction reference.

CURL Request Example:

curl https://<HOSTNAME>/ezwsrest/rest/engine/auth/tx/pullstatus
--data 'actionBy=uaeexchange&txRef=9d6c1f9489b13b43'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "rc":0,
  "s":1
}
```

Response JSON object parameters:

Parameter	Description
rc	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -104 = Transaction not found. • -105 = Transaction data corrupted. • -180 = Token will be locked next failure attempt
s	Transaction status. • 0 = Pending • 1 = Approved • 2 = Rejected • 3 = Expired • 4 = Failed

1.3   Offline One-Time-Password Login flow

This secion illustrate the flow of login with offline One-Time-Password.

1.3.1   Verify One-Time-Password

To verify the offline One-Time-Password generated from EzToken mobile app.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/eziden/s/verifyAllOtp

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.
otp	Yes	The One-Time-Password.

CURL Request Example:

curl https://<HOSTNAME>/ezwsrest/rest/engine/eziden/s/verifyAllOtp --data 'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24ABDD993&userId=testuser01&otp=758410'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "returnCode":0
}
```

Response JSON object parameters:

Parameter	Description
returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -3 = Invalid user • -5 = Invalid token state. • -7 = Invalid OTP. • -20 = Invalid group or it is not found

1.4 Push Notification Transaction Signing flow

This secion illustrate the flow of create and sign a transaction, then approve it via a push notification.

1.4.1 Request push notification for transaction

To request a push notification being sent to the activated EzToken mobile app account for transaction signing and approve.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/auth/sigtx/reqpush

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.
txDetails	Yes	The transaction details in JSON formatted string (flat structure of key-value mapping), i.e. {"From": "1122334455", "To": "9988776655", "Amount": "100.22"}.
txExpiryMins	Yes	The transaction expiry in minutes.
txType	Yes	The transaction type. Use value "2" (Transaction)
mobilePush	No	The mobile push identifier. If not provided or empty value, the push notification will be attempted to deliver to the default registered push device.

txFlags	No	The transaction flags containing the flag of transaction details. It's a JSON formatted string. Eg: {"txUBio": 0}.
		
		 • txUBio = Keys to indicate the authenticate options upon signing on mobile app:
		     o 0 = Default depending on user configuration.
		     o 1 = Voice or Facial recognition.
		     o 2 = Voice and Facial recognition.

CURL Request Example:

curl https://<HOSTNAME>/ezwsrest/rest/engine/auth/sigtx/reqpush --data 'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24ABDD993&userId=testuser01&txDetails={"From": "1122334455", "To": "9988776655", "Amount": "100.22"}&txExpiryMins=3&txType=2'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "returnCode":0,
  "refcode":"6e85d6a904f6b594",
  "pushmsg":
"eyJyYyI6MCwiZ2lkIjo2MiwidWlkIjoiVEVVVCVFVTRVIwMSIsInJlZiI6IjZlODVkNmE5MDRmNmI1OTQifQ\u003d\u003d"
}
```

Response JSON object parameters:

Parameter	Description

returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -3 = Invalid user • -5 = Invalid token state. • -20 = Invalid group or it is not found • -65 = No active token found • -47 = Invalid group state is not enabled • -98 = Error in sending push message • -101 = Invalid user OOB contact • -104 = Transaction not found. • -106 = Invalid SAML Identifier
refcode	A unique reference code. It may be used to check if the push notification has been approved/rejected at EzToken mobile app. Refer to REST API: Check push notification approval status.
pushmsg	Push message sent.

![EZMCOM CONVENIENTLY SECURE]

1.5   Offline Transaction Signing flow

This secion illustrate the flow of create a QR-code image for transaction signing/approval purpose.

1.5.1   Create QR-code image for transaction

To request a QR-code image for offline transactioning signing.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/auth/sigtx/reqqr

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.
txDetails	Yes	The transaction details in JSON formatted string (flat structure of key-value mapping), i.e. {"From": "1122334455", "To": "9988776655", "Amount": "100.22"}.
txExpiryMins	Yes	The transaction expiry in minutes.
txType	Yes	The transaction type. Use value "2" (Transaction)
ota	Yes	Over-the-air flag. Use value "false".

txFlags	No	The transaction flags containing the flag of transaction details. It's a JSON formatted string. Eg: {"txUBio": 0}.
		• txUBio = Keys to indicate the authenticate options upon signing on mobile app:
		o 0 = Default depending on user configuration.
		o 1 = Voice or Facial recognition.
		o 2 = Voice and Facial recognition.

CURL Request Example:

```
curl https://<HOSTNAME>/ezwsrest/rest/engine/auth/sigtx/reqqr --data
'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24A
BDD993&userId=testuser01&txDetails={"From": "1122334455",
"To": "9988776655", "Amount":
"100.22"}&txExpiryMins=3&txType=2&ota=false'
```

Http Response Example:

Response Header:

```
HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8
```

Response Body:

```
{
  "returnCode":0,
  "refcode":"d6ff80cea8d0cfe9",
  "qrcode":
"iVBORw0KGgoAAAANSUhEUgAAAMgAAADIAQAAAACFI5MzAAADm
klEQVR42u2YTc6rOBBFK2LALGwAydvwjC2FDfCzAbIlz9gGGkjcAMw9Q
qo+B9Hs96AH1tdSTF6EI+URgl6tuXUf03z7yh/znZBepO+/eSZ6ldKJj
KlaR3kp6dRriJLo2dVfuncQtDxrJq6z7eXnMSxX040XKYgv1T0ieLM9Oc
Sjd0MQfkmfpJs/SiYTT9CNCDCa/dKUb1Y3zwq9+i85twv608z+u16+d
u0vyZ2jcxNK17hr3npf+V1bdJbs0dRV2xgYptsSNVFcMLIRN1jky9ki8h
JvlKU6NRLe5GIO+QzGmc9b88IioiYzcpvrZ5AHyUcr4DlGt5D0Tg4JwV
loMQmgpO7WS/eV3xj6lTsLq6yrp4K+aM5BKRXz8NMx3aZMbg1Tpir
WBdAIkfXTydZvYcOl8YSZZopCEFMe0PJg+6nK9x0B0KFGCPLYF9CB
+qONwVomFfMqa1Xd51sXHI4H7NWsTGUrVwC2lvLyk5oWq0UqO4k
hMnJ1xn0YI6qd0VnLGYK8SQaV1sFGsoO6tZG14MFKKfC4I1YMdk8V
MNJDRZCL1capLcemohey54aSsLrlDnjKjYiZViNtMHce12U91GXxtJcxa
ng1q6tZLR2uRMw8MBH3a2yN3Hlr3gd3m21kJykfDWVplcyTLVVm34
aujt8nezwR16VECeuMhhP23094nOQa0WTKaEunYq1lECrWSt5KD6L
G0gXw8Wtm1HgPZefbE5Wk+unpEtBZ/6eh9olOZ02fw0pKAiQATXTU
T/FcbqBJu4poVuqCIeyNhf3ATjqTuNR5JrbRuMxGMmLgxkdoIPOpSX
+piIl1DXmdnR6OY6B6eIj6rxECOB0t2dsjMOJNHe3V5CgvZAuvGctLA
T3VRdEuNZH96IWvy2OXsaJJnJhqIjmF5Hio1lZeODuVZJQaCv0Y1eYk
gKses4/tynRbC8MDr6BWHI9uyzHyd921Cu8Ax7X3uG8QSudof4VyPg
ZDXCIwbPKVWcIzANr71m/H3Cf5rS7TEusrHiCKfJ65uZiGY1qlk6Vzxs
LF0WjPhw+GGHd5fUqwIqqf/fM8YFsJYXPOrsBUcXve/Nf4+wTSRMln2
2hlPR8FxbHJqJZznSG0ieuwPmir9XJjJKzcfh3WlaSCilLJcLs1GyMS4.erd
lW7E8vcPJ/oQ8wvLKpwcqGOOJzDsz6TWf+CtqN5x+J37PJRbCObjKK
```

iXZKmZ1cb/9U3KX/PmH6f8nfwFvRICbsTJWNAAAAABJRU5ErkJggg\
u003d\u003d"
}

Response JSON object parameters:

Parameter	Description
returnCode	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -3 = Invalid user (a more precise indication user has no enrollment record, generally indicating this user has no 2FA tokens). NOTE: similar to -65. • -4 = Invalid token serial no. • -5 = Invalid token state, token is not active. • -20 = Invalid group is not found • -47 = Invalid group state is not enabled • -65 = No token bound records found (a more precise indication that token bind record don't even exist, generally indicating this user has no 2FA tokens). NOTE: similar to -3. • -86 = Invalid configuration. • -98 = Unable to send message (OOB engine delivery failure) • -101 = Invalid user contact (missing mobile push) • -102 = Invalid OOB channel. • -103 = QRCode data reached limit constraint. • -104 = Transaction didn't manage to create, it was not found during the logic to send OOB message.
refcode	A unique reference code. It may be used to check if the created transaction approval status.
qrcode	A Base64 encoded image, decoding this will give you the PNG bytes.

1.5.2 Verify signature One-Time-Password

To verify signature One-Time-Password generated from EzToken mobile app.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/auth/tx/approval

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
txRef	Yes	The transaction reference.
txStatus	Yes	· The transaction status code to indicate either: • 1 = Approved • 2 = Rejected
otp	Yes	The signature One-Time-Password.
txComment	No	Transaction comment. Can take empty value.

CURL Request Example:

curl https://<HOSTNAME>/ezwsrest/rest/engine/auth/tx/approval
--data
'actionBy=uaeexchange&txRef=d7a779cbb434caf6&txStatus=1&otp=978891'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "rc":0,
  "ref":"d7a779cbb434caf6"
}
```

Response JSON object parameters:

Parameter	Description
rc	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -5 = Transaction status is in an invalid state for this API call (expecting to be in pending state). • -7 = Invalid OTP. • -18 = Token is locked • -75 = Transaction expired. • -104 = Transaction not found. • -105 = Transaction data corrupted.
ref	Transaction reference.

1.6   User Token Helpdesk Utilities

This secion explains how to perform token helpdesk task, eg: Check if user has an active token, delete an active token, etc.

1.6.1   Check if user has an active token

To check if user is having an active token.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/checkUserHasActiveSoftTk

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.
userId	Yes	The user identifier. Preferable use email address as userId.

CURL Request Example:

curl https://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/checkUserHasActiveSoftTk --data 'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24ABDD993&userId=testuser01'

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "rc":0,
  "hasActive":1
}
```

Response JSON object parameters:

Parameter	Description
rc	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -20 = Invalid group or it is not found • -47 = Invalid group state is not enabled • -106 = Invalid SAML Identifier
hasActive	An integer value to indicate if the user has active token or not. 0 = NO ACTIVE TOKEN, 1 = HAS ACTIVE TOKEN.

1.6.2 Delete active token from user

To delete and unassign token from a particular user.

URL:

http(s)://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/dregeztoken

Http Request Method:

POST

Http Request Content–Type:

Application/x-www-form-urlencoded

Http Request Form Parameters:

Parameter	Mandatory	Description
actionBy	Yes	The action by. A non-empty value. For audit trail purpose.
samlId	Yes	The EzIdentity Group SAML Identifier.

userId	Yes	The user identifier. Preferable use email address as userId.
pushId	No	The mobile push identifier. If not provided or empty value, the system will try to delete and unassign all active soft token associated to the user.

CURL Request Example:

```
curl
https://<HOSTNAME>/ezwsrest/rest/engine/softtk/s/dregeztoken -
-data
'actionBy=uaeexchange&samlId=385FBF38420D7C3832E03DC24A
BDD993&userId=testuser01'
```

Http Response Example:

Response Header:

HTTP/1.1 200 OK
Content-Type:application/json;charset=UTF-8

Response Body:

```
{
  "returnCode":0,
  "returnMessage":"Success",
  "unassignedSno":["A001021640264427"]
}
```

Response JSON object parameters:

Parameter	Description
rc	An integer value to report in the status of the execution. Below are the common return codes. Note that the codes include but not limited to these: • 0 = Success • -1 = System error • -2 = Bad parameter • -65 = No active token found • -47 = Invalid group state is not enabled • -106 = Invalid SAML Identifier
unassignedSno	The token serial number(s) deleted from this REST call.