CENTAGATE

CENTAGATE API Documentation

WWW.SECUREMETRIC.COM

Table of Contents

ABOUT 3
1. About This Document 4
1.1. Audience 4
1.2. Definition 4
1.3. Technical Support 4
CENTAGATE API 5
2. Introduction 6
3. API 7
3.1. Authentication API 7
3.1.1. Operations 8
3.1.1.1. Username/Password Authentication 8
3.1.1.2. Adaptive Authentication 11
3.1.1.3. OTP Authentication 14
3.1.1.4. SMS OTP Authentication 17
3.1.1.5. CR OTP Authentication 19
3.1.1.6. PKI Authentication 22
3.1.1.7. Simple PKI Authentication 25
3.1.1.8. PKCS#7 PKI Authentication 27
3.1.1.9. QR Code Authentication 30
3.1.1.10. Security Question Authentication 33
3.1.1.11. FIDO Authentication 36
3.1.1.12. Secugen Authentication 36
3.1.1.13. Request Challenge Question 39
3.1.1.14. Request Random String 41
3.1.1.15. Request SMS OTP 42
3.1.1.16. Request OTP Challenge 44
3.1.1.17. Request QR Code 46

3.1.1.18. Request Mobile Soft Certificate Authentication 48
3.1.1.19. Request Mobile Audio Pass Authentication 49
3.1.1.20. Request Mobile Push CR OTP Authentication 52
3.1.1.21. Check Authentication State 53
3.1.1.22. Logout 56
3.1.2. Constants 57
3.1.2.1. Authentication Methods 57
3.2. Server API 57
3.2.1. Operations 58
3.2.1.1. User registration 58
3.2.1.2. Token registration 59
3.2.1.3. Token registration (One Time PIN) 60
3.2.1.4. Token registration (PKI) 62
3.2.1.5. OTP token registration (Offline) 63
3.2.1.6. Unregister Token 64
3.2.1.7. Unlock OTP Token 65
3.2.1.8. Sync Token 66
3.2.1.9. Save Question & Answer 67
3.2.1.10. Reset Question & Answer 68
3.2.1.11. Request Number of Question to Reset 69
3.2.1.12. Request Question List 70
3.2.1.13. Request User Question List 71
3.2.1.14. Request List of user bound authentication methods 72
3.2.1.15. Check Token Status 74
3.2.1.16. Update user status 75
3.2.1.17. Update token status 75
3.2.1.18. Unbind and delete user 77
3.2.1.19. Verify Signature 78

3.2.1.20. Unlock User 79

3.2.1.21. Update user profile..... 79

3.2.1.22. Update user password..... 81

3.2.1.23. Check user session..... 83

3.2.1.24. Secugen fingerprint registration..... 83

3.3. Question List 85

ABOUT

This section explains about this Documentation, the intended audience, related term's definition and technical support information.

Topics in this chapter include:

- "About this Document"

1. ABOUT THIS DOCUMENT

This guide explains how to use CENTAGATE API.

1.1. Audience

This document is intended for the system integrator that includes 3rd party programmers who want to integrate with CENTAGATE and others involved.

1.2. Definition

Here are the explanations on terms used with this document:

TERM	DEFINITION
CENTAGATE	Centralized Authentication Gateway
SAML	Security Assertion Markup Language
API	Application Programming Interface
2FA	Two Factor Authentication
SSO	Single Sign On

1.3. Technical Support

Contact information for support is available to customers at SecureMetric website:

http://www.securemetric.com/contact-details.php

Mailing Address:

SecureMetric Technology Sdn. Bhd. (Reg. no. 759614-V)

Level 5-E-6, Enterprise 4, Technology Park Malaysia

Lebuhraya Sg. Besi - Puchong, Bukit Jalil, 57000 Kuala Lumpur, Malaysia.

CENTAGATE API

This section provides general information about the features of the CENTAGATE API and how to begin using it.

Topics in this chapter include:

- "Introduction"
- "API"

2. INTRODUCTION

CENTAGATE API is an API that allows 3rd party system integrators to integration their existing system and outsource the authentication to the CENTAGATE. CENTAGATE API is a RESTful based API, which means virtually any system that supports calling to the RESTful API will be able to integrate seamlessly with CENTAGATE.

This document provides the operations provided by the CENTAGATE API complete with the parameters and the return values.

3. API

3.1. Authentication API

The return codes for Authentication API are as below:

No.	Return Code	Detail
1.	0	Success
2.	10001	Permission not allowed
3.	10002	Invalid input
4.	10003	Database protection error
5.	10004	Database error
6.	20007	Company is not active
7.	22002	User not found
8.	22004	User is not active
9.	22005	User mobile not found
10.	23001	Invalid credentials
11.	23002	Please wait before requesting for another SMS OTP
12.	23003	Generate random string failed
13.	23004	Generate SMS OTP failed
14.	23005	Generate OTP challenge failed
15.	23006	Push mobile soft certificate failed
16.	23007	Authentication is pending
17.	23008	Invalid SMS OTP
18.	23009	SMS OTP is expired
19.	23010	SMS OTP has not been generated
20.	23012	Certificate is revoked
21.	23013	User does not bind with any device
22.	23014	Unknown device OS
23.	23015	Push mobile audio pass failed
24.	23016	Authentication data does not exist
25.	23017	Authentication method is not enabled
26.	23018	Invalid authentication request status

27.	23019	Authentication request owner not match
28.	23020	Authentication request rejected. API is not come from trusted IP address list
29.	23021	Authentication request rejected. User's group is not allowed to access this API
30.	23022	Authentication request rejected. Invalid API signature
31.	23023	Authentication request rejected. Request expired
32.	23024	API not found
33.	23025	Authentication API error
34.	23026	Authentication request rejected
35.	23035	OTP token out of sync
36.	23036	OTP token locked
37.	25009	Insufficient SMS credit
38.	29002	Token not active
39.	36004	User device not active

3.1.1. Operations

3.1.1.1. Username/Password Authentication

Description: Authentication function that verify username and password combination.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authBasic

RESTful parameters:

Key	Description
username	The user's username
password	The user's password. Can be a plain password or encrypted password. If the password needs to be encrypted, use AES 256 with encryption key = secret key + @ |0N5 4 C3NTAG4T3v1 Example: If secret key = 5yfpQcsYGo9a, then encryption key = 5yfpQcsYGo9a@ |0N5 4 C3NTAG4T3v1

integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
supportFido	Put in the value “true” or “false”. Or leave it empty
ipAddress	The caller’s IP address. This is optional. You can leave it empty
userAgent	The caller’s user agent. This is optional. You can leave it empty
browserFp	The caller’s browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + password + integrationKey + unixTimestamp + supportFido + ipAddress + userAgent + browserFp Password is from “password” parameter: Either plain password or encrypted password depends on “isPasswordEncrypted” below.
isPasswordEncrypted	Stated whether the password is encrypted or not. Only set isPasswordEncrypted = 1 if the password is encrypted. Otherwise, you can leave it empty / null / any value, or no need to pass this parameter.

RESTful output:

Key	**Description**
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	**Description**
appId	The application ID the authentication is

	performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma. Only applicable for user with MFA = Always Apply. Otherwise, it will not be shown.
sessionTimeout	The session timeout of the user in milliseconds.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier
userAppId	The user's application ID
userClientId	The user's client ID
userUniqueId	The user's unique ID

Return Code	**Detail**
0	Success
10002	Invalid input

10011	Cryptographic error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.2. Adaptive Authentication

Description: This function did not do authentication. It does risk calculation return you the return object that is similar to normal authentication function. From there you will know whether you need to perform step-up authentication or not.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/adaptive

RESTful parameters:

Key	Description
username	The user's username
authResult	Either "true" or "false". **True** = Authentication success. This function will return and tell you whether need step up authentication or not **False** = Authentication failed. This value send back to CENTAGATE for indexing statistic purpose.
integrationKey	The integration key

unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value “true” or “false”. Or leave it empty
ipAddress	The caller’s IP address. This is optional. You can leave it empty
userAgent	The caller’s user agent. This is optional. You can leave it empty
browserFp	The caller’s browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + authResult + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.

authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	**Detail**
0	Success
10002	Invalid input
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired

23024	API not found
23025	Authentication API error

3.1.1.3. OTP Authentication

Description: Authentication function that verify username and OTP combination.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authOtp

RESTful parameters:

Key	Description
username	The user's username
otp	The user's OTP
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + otp + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information.

	Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail

0	Success
10002	Invalid input
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
23035	OTP token out of sync
23036	OTP token locked

3.1.1.4. SMS OTP Authentication

Description: Authentication function that verify username and SMS OTP combination. User has to request a SMS OTP before call this function (Refer to 3.1.1.14). SMS will be send to the relative user out of band.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authSmsOtp

RESTful parameters:

Key	Description
username	The user's username
smsOtp	The user's SMS OTP
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + smsOtp + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is

	successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success

10001	Permission not allowed
10002	Invalid input
10003	Database protection error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.5. CR OTP Authentication

Description: Authentication function that verify username and Challenge Response OTP combination. User has to request an OTP challenge code before call this function (Refer to 3.1.1.15). User will generate a correspond OTP based on the challenge code.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authCrOtp

RESTful parameters:

Key	Description
username	The user's username
challenge	Challenge code that is sent from server to user
crOtp	CR token OTP
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is

	optional. You can leave it empty
supportFido	Put in the value “true” or “false”. Or leave it empty
ipAddress	The caller’s IP address. This is optional. You can leave it empty
userAgent	The caller’s user agent. This is optional. You can leave it empty
browserFp	The caller’s browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text username + crOtp + challenge + integrationKey + unixTimestamp + authToken + suppotFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is

	using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
10004	Database error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request

	expired
23024	API not found
23025	Authentication API error
23035	OTP token out of sync
23036	OTP token locked

3.1.1.6. PKI Authentication

Description: Authentication function that verify username and PKI signature. User has to request a random before call this function (Refer to 3.1.1.13). The random value is then being signed and sends to CENTAGATE for verification.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/authPkiWithSignature

RESTful parameters:

Key	Description
username	The user's username
certFingerprintSha1	The user' certificate fingerprint is encoded using SHA1 and the result is encoded into hexadecimal value. This is the certificate that is used to sign the random string
signature	Perform signature (SHA1WithRSA) on the random string. The result is encoded in Base64
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is

	optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + certFingerprintSha1 + signature + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.

authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
23001	Invalid credentials
23012	Certificate is revoked
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.7. Simple PKI Authentication

Description: Authentication function that verify username and PKI. Call this function when you implements Client SSL authentication. Once your user passed the Client SSL authentication, submit the certificate fingerprint to CENTAGATE to verify the remaining

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authPki

RESTful parameters:

Key	Description
username	The user's username
certFingerprintSha1	The user' certificate fingerprint is encoded using SHA1 and the result is encoded into hexadecimal value
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + certFingerprintSha1 + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication

message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.8. PKCS#7 PKI Authentication

Description: Authentication function that verify username and PKI using PKCS#7 signature.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authPkiPkcs7

RESTful parameters:

Key	Description
username	The user's username
signature	The PKCS#7 attached signature encoded in Base64
algorithm	The algorithm used during the signing. Valid values are: - 0: SHA-1 - 1: SHA-256

	- 2: SHA-384 - 3: SHA-512
plainText	The plain text of the signed string encoded in Base64
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + signature + algorithm + plainText + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.

userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
23001	Invalid credentials
23016	Authentication data does not exist

23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.9. QR Code Authentication

Description: Authentication function that verify username and QR. User has to request a QR code before call this function (Refer to 3.1.1.16). You have to convert the QR code value to a QR and display on the screen to let user scans it.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/authQRCode

RESTful parameters:

Key	Description
username	The user's username
otp	The OTP generated based on the QR code
challenge	The OTP challenge
details	The transaction information based on requested QR code encoded using Base64. Format: <account ID>|<request ID>|<details> Alternatively, the information is returned as plainText during QR code request.
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty

supportFido	Put in the value “true” or “false”. Or leave it empty
ipAddress	The caller’s IP address. This is optional. You can leave it empty
userAgent	The caller’s user agent. This is optional. You can leave it empty
browserFp	The caller’s browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text username + otp + challenge + details + integrationKey + unixTimestamp + authToken + suppotFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.

useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
10004	Database error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature

23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
23035	OTP token out of sync
23036	OTP token locked

3.1.1.10. Security Question Authentication

Description: Authentication function that verify username and security question. User has to request a list of question that needs to be answered before call this function (Refer to 3.1.1.12).

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authQna

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
data	Base64 encoded of the list of questions and answer. The format for each question and answer is: **QuestionID:Answer** separated by comma. Example: 1:Hello World,2:Foo123 will be sent as MTpIZWxsbyB3b3JsZA==,MjpGb28xMjM=
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty

browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + data + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.

authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
10004	Database error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.11. FIDO Authentication

Description: Authentication function that verify username and FIDO token.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authFido

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
fidoJson	Result generated from the FIDO API (Chrome Browser). * This API will only work with Chrome Browser.
challenge	Any random string. Must not empty.
authToken	The previous generated authToken. This is optional. You can leave it empty
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + fidoJson + challenge + authToken + supportFido + ipAddress + userAgent + browserFp

3.1.1.12. Secugen Authentication

Description: Authentication function that verify username by using secugen token.

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/authFprint

RESTful parameters:

Key	Description
username	The user's username
fprint	Result generated from the secugen API (IE Browser). * This API currently will only work with Internet Explorer Browser.
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
browserFp	The caller's browser fingerprint. This is optional. You can leave it empty.
supportFido	Put in the value "true" or "false". Or leave it empty
authToken	The previous generated authToken. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + fprint + authToken + supportFido + ipAddress + userAgent + browserFp

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.
companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required.
email	The user email who performs the authentication.
groupId	The group ID of the user who authenticates.
lastSuccessLogin	The last success login of the user in milliseconds
uuid	The universally unique identifier

Return Code	Detail
0	Success
10001	Permission not allowed

10002	Invalid input
10003	Database protection error
10004	Database error
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
23037	Fingerprint is not match
56000	Fingerprint is not registered

3.1.1.13. Request Challenge Question

Description: Return list of question that need to be answer during security question authentication. The question will be return randomly if the question list is more than one.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/kba/getQuestions

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty

ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information that includes n number of questions need to be answered. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
id	id: The ID of the question
question	The full text of the question

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come

	from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.14. Request Random String

Description: Return a random value for PKI authentication.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestRandomString

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication

object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
randomString	The generated random string

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.1.15. Request SMS OTP

Description: Request to send a SMS OTP to the corresponding user.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestSmsOtp

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
phone	The mobile phone to which the SMS code is sent.
smsOtp	The request SMS code.
timeout	The timeout of the SMS code in seconds.

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input

22002	User not found
22004	User is not active
22005	User mobile not found
23001	Invalid credentials
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
25009	Insufficient SMS credit
29002	Token not active

3.1.1.16. Request OTP Challenge

Description: Request an OTP challenge code for CR OTP authentication.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestOtpChallenge

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty

userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
otpChallenge	The OTP challenge string

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
10004	Database error
22002	User not found
22004	User is not active
23001	Invalid credentials
23005	Generate OTP challenge failed
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come

	from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
29002	Token not active

3.1.1.17. Request QR Code

Description: Request a QR code for QR code authentication.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestQrCode

RESTful parameters:

Key	Description
username	The user's username
details	The transaction details encoded using Base64
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + details + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description

code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication is successful. See below for the details.

RESTful object content:

Key	Description
qrCode	The generate QR Code string
otpChallenge	The OTP challenge string
plainText	The information of the transaction with requestor's ID.

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
10003	Database protection error
10004	Database error
22002	User not found
22004	User is not active
23001	Invalid credentials
23005	Generate OTP challenge failed
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired

23024	API not found
23025	Authentication API error
29002	Token not active

3.1.1.18. Request Mobile Soft Certificate Authentication

Description: Call this function to push a mobile soft certificate authentication request to the mobile application via iOS/Android Push.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestMobileSoftCert

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. For this function it will always return empty

RESTful object content:

Key	Description
authToken	The authentication token for the current authentication phase.

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
22004	User is not active
23001	Invalid credentials
23006	Push mobile soft certificate failed
23013	User does not bind with any device
23014	Unknown device OS
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
36004	User device not active

3.1.1.19. Request Mobile Audio Pass Authentication

Description: Call this function to push a mobile audio pass authentication request to the mobile application via iOS/Android Push.

RESTful method: **POST**

RESTful link:

https://cloud.centagate.com/CentagateWS/webresources/auth/requestMobileAudioPass

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. For this function it will always return empty

RESTful object content:

Key	Description
authToken	The authentication token for the current authentication phase.

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found

22004	User is not active
23001	Invalid credentials
23013	User does not bind with any device
23014	Unknown device OS
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
36004	User device not active

3.1.1.20. Request Mobile Push CR OTP Authentication

Description: Call this function to push a mobile CR OTP authentication request to the mobile application via iOS/Android Push.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/requestMobilePushCR

RESTful parameters:

Key	Description
username	The user's username
details	The transaction details encoded using Base64
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is optional. You can leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. For this function it will always return empty

RESTful object content:

Key	Description
authToken	The authentication token for the current authentication phase.

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
22004	User is not active
23001	Invalid credentials
23013	User does not bind with any device
23014	Unknown device OS
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
23036	OTP token locked
36004	User device not active

3.1.1.21. Check Authentication State

Description: Call this function to check the out-of-band authentication status (QR, mobile soft cert, audio pass, push CR OTP).

RESTful method: **POST**

RESTful link: https://cloud.centagate.com/CentagateWS/webresources/auth/statecheck

RESTful parameters:

Key	Description

username	The user's username
authMethod	The authentication methods that you wish to check. Currently, only support "MSOFTCERT", "MAUDIOPASS","QRCODE" and "CROTP"
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is mandatory.
supportFido	Put in the value "true" or "false". Or leave it empty
ipAddress	The caller's IP address. This is optional. You can leave it empty
userAgent	The caller's user agent. This is optional. You can leave it empty
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + authMethod + integrationKey + unixTimestamp + authToken + supportFido + ipAddress + userAgent

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. Will be only filled-in if the authentication status is COMPLETED (2) or MULTISTEP (3). See below for the details.

RESTful object content:

Key	Description
appId	The application ID the authentication is performed to.
userId	The user ID who performs the authentication.
companyId	The company ID of the user who authenticates.

companyName	The company name of the user who authenticates.
role	The role of the user who authenticates.
timezone	The time-zone of the user who authenticates.
authToken	The authentication token for the current authentication phase.
useSystemPassword	The flag indicating whether or not the user is using system generated password.
passwordExpired	The flag indicating whether or not the password has expired.
secretCode	The secret code that will be used to secure the communication with server. Empty value means user will need to re-authenticate themselves.
authMethods	The list of available authentication methods separated with comma.
sessionTimeout	The session timeout of the user in milliseconds.
multiStepAuth	The flag indicating whether or not multi-step is required. Will be empty if the status is COMPLETED (2).

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid input
23001	Invalid credentials
23007	Authentication is pending
23016	Authentication data does not exist
23017	Authentication method is not enabled
23018	Invalid authentication request status
23019	Authentication request owner not match
23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API

	signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error
23026	Authentication request rejected

3.1.1.22. Logout

Description: Call this function to properly logout the user.

RESTful method: **POST**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/logout

RESTful parameters:

Key	Description
username	The user's username
integrationKey	The integration key
unixTimestamp	The current time in unix timestamp
authToken	The previous generated authToken. This is mandatory
hmac	The hmac value calculated using SHA256 with secret key as key and plain text from username + integrationKey + unixTimestamp + authToken

RESTful output:

Key	Description
code	The return code of the authentication
message	The return message of the authentication
object	The object containing additional information. For this function it will always return empty

Return Code	Detail
0	Success

23020	Authentication request rejected. API is not come from trusted IP address list
23022	Authentication request rejected. Invalid API signature
23023	Authentication request rejected. Request expired
23024	API not found
23025	Authentication API error

3.1.2. Constants

3.1.2.1. Authentication Methods

Key	Description
PASS	Username/Password authentication
PKI	PKI Authentication
OTP	OTP Authentication
SMS	SMS OTP Authentication
CROTP	CR OTP Authentication
MSOFTCERT	Mobile Soft Certificate Authentication
MAUDIOPASS	Mobile AudioPass Authentication
FIDO	FIDO Authentication
QR	QR Code Authentication
QNA	Security Question Authentication
FPRINT	Secugent Authentication

3.2.Server API

To execute server API, integration system have to complete the authentication API and retrieve the ***authToken*** and ***secretCode***.

From there, you have to generate ***cenToken***,

cenToken = HMAC-SHA256 (key=***secretCode*** , plaintext= ***admin username + authToken***);

3.2.1. Operations

3.2.1.1. User registration

Description: Call this function to add an active user.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/user/registerUserActivate/{admin username}

RESTful parameters:

Key	Description
firstName	The user's first name
lastName	The user's last name
username	The user's username
userApp	The user's application ID
userUniqueId	The user's unique ID
userClientId	The user's client ID
userAdditionalData1	Optional, The user's additional data 1
userAdditionalData2	Optional, The user's additional data 2
userAdditionalData3	Optional, The user's additional data 3
userAdditionalData4	Optional, The user's additional data 4
userAdditionalData5	Optional, The user's additional data 5
userEmail	Optional, The user's email
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
Object	If success, it will return user id. Otherwise, it will return empty string.

Return Code	Detail
0	Success

10002	Invalid Input
10003	DB protection error
10004	DB error
20002	Company not found
21001	Group not found
22001	Duplicate user email
22011	User self register failed
22013	Users limit reached
22025	Duplicate username
27001	Invalid license file

3.2.1.2. Token registration

Description: Call this function to register an active SMS or OTP token

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/registerActiveToken/{admin username}

RESTful parameters:

Key	Description
username	The user's username
tokenSn	The mobile number. This mandatory for token type SMS
tokenType	The token type 1 = SMS 2 = OTP
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information.

	Key	Description	
	boundUser	Bound username	
	boundUser FirtName	Bound user first name	
	boundUserLastName	Bound user last name	
	boundMobileDefault	Mobile default flag 0=No 1=Yes	
	boundTokenStatus	Bound token status. 0=Inactive 1=active 2=active and locked 3=pending 4=pending and locked	

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input
10003	DB protection error
10004	DB error
22002	User not found
29001	Token not found
29002	Token not active
29004	Phone number had been used
29008	An OTP token already registered to this user
29011	Invalid token activation code
29017	Invalid token status
6002	Token register to user failed
6007	User is not allowed to bind with CR OTP token

3.2.1.3. Token registration (One Time PIN)

Description: Call this function to register an One Time PIN token. You can specify the token status during the registration.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/device/register/onetimepin/{admin username}

RESTful parameters:

Key	Description
username	The user's username
status	Token status: - 1 = pending - 2 = valid - 3 = temp deactivated - 4 = deactivated
validity	Optional. Specify the validity of the SMS code. In seconds. If this value is not set, default 5 minutes will be used.
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information that includes a list of questions to reset. See below for the details.

RESTful object content:

Key	Description
qr	QR code value.
passcode	The SMS code

Return Code	Detail

0	Success
10001	Permission not allowed
10002	Invalid Input
10003	DB protection error
10004	DB error
10011	Crypto error
22002	User not found
22004	User is not active
22027	User already bound with a token

3.2.1.4. Token registration (PKI)

Description: Call this function to register a PKI token. You can specify the token status during the registration

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/cert/register/pkcs7/{admin username}

RESTful parameters:

Key	Description
username	The user's username
signature	The PKCS#7 attached signature encoded in Base64
algorithm	The algorithm used during the signing. Valid values are: - 0: SHA-1 - 1: SHA-256 - 2: SHA-384 - 3: SHA-512
timestamp	Unix timestamp in millisecond when user register the certificate. Server will reject the request if the request is 5 minutes more or less than the server current time.
status	Token status: - 1 = pending

	- 2 = valid - 3 = temp deactivated - 4 = deactivated
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input
10003	DB protection error
10004	DB error
10011	Crypto error
22002	User not found
22004	User is not active
22027	User already bound with a token

3.2.1.5. OTP token registration (Offline)

Description: Call this function to register offline OTP token.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/register/otp/offline/{admin_username}

RESTful parameters:

Key	Description
username	The user's username that want to bind the

	token
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

RESTful object content:

Key	Description
key	Key that use for offline provisioning

Return Code	Description
0	Success
10001	Permission not allowed
22002	User not found
29001	Token not found
29008	An OTP token already registered to this user

3.2.1.6. Unregister Token

Description: Call this function to unregister a token.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/unregisterActiveToken/{admin username}

RESTful parameters:

Key	Description
username	The user's username
type	The token type - 1 = Mobile Token

	- 2 = SMS - 3 = CH Token - 4 = PKI
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input
10003	DB protection error
10004	DB error
22002	User not found
29001	Token not found
29013	Token doesn't belong to a user
26011	Certificate not found
36000	Device not found

3.2.1.7. Unlock OTP Token

Description: Call this function to unlock/unsuspend OTP token.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/unlockToken/{admin username}

RESTful parameters:

Key	Description
username	The OTP owner username
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
29001	Token not found
29017	Invalid token status

3.2.1.8. Sync Token

Description: Call this function to synchronize OTP token.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/syncToken/{admin username}

RESTful parameters:

Key	Description
username	The OTP owner username
otpStr1	The first OTP
otpStr2	The second OTP
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin

	username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid input
22002	User not found
29001	Token not found
29002	Token is not active
29003	Token is not bound to the user
29013	Token is not bound to anyone
54002	Sync OTP failed

3.2.1.9. Save Question & Answer

Description: Save question and answer for the owner of cenToken.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/security/saveUserQuestions/{admin username}

RESTful parameters:

Key	Description
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken
data	Base64 encoded of the list of questions and answer.

	Format: Base64 (<ID_1>:<Custom question_1 if ID_1=0. Otherwise, empty string>:<Answer_2> ,<ID_2>:<Custom question_2 if ID_2=0. Otherwise, empty string >:<Answer_2>) Example: 0:Quest1:Hello World,2::Foo123 will be sent as MDpRdWVzdDE6SGVsbG8gV29ybGQsMjo6Rm9vMTIz * refer 3.3 for full list of question and id

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
22002	User not found
38000	Invalid security question

3.2.1.10. Reset Question & Answer

Description: Reset question and answer for the given username.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/security/resetQaBPI/{admin_username}

RESTful parameters:

Key	Description
username	The username
data	Base64 encoded of the list of questions and

	answer. Format: Base64 (<ID_1>:<Custom question_1 if ID_1=0. Otherwise, empty string>:<Answer_2> ,<ID_2>:<Custom question_2 if ID_2=0. Otherwise, empty string >:<Answer_2>) Example: 0:Quest1:Hello World,2::Foo123 will be sent as MDpRdWVzdDE6SGVsbG8gV29ybGQsMjo6Rm9vMTIz * refer 3.3 for full list of question and id
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
22002	User not found

3.2.1.11. Request Number of Question to Reset

Description: Call this function to know how many question need to be reset.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/security/getNumOfQuestionsToSetBPI

RESTful parameters:

Key	Description
username	The user's username

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information.

RESTful object content:

Key	Description
numOfQuestion	The number of questions to reset

Return Code	Description
0	Success
10001	Permission not allowed
22002	User not found

3.2.1.12. Request Question List

Description: Call this function to retrieve list of available security question.

RESTful method: **GET**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/security/getQuestion

RESTful parameters: **None**

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information that includes a list of questions to reset. See below for the details.

RESTful object content:

Key	Description
id	id: The ID of the question
question	The full text of the question

Return Code	Description
0	Success
10001	Permission not allowed

3.2.1.13. Request User Question List

Description: Call this function to retrieve user security question list.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/security/getUserQuestions/{admin username}

RESTful parameters:

Key	Description
username	The user's username that want to get the security question list
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information that includes a list of questions to save. See below for the details.

RESTful object content:

Key	Description
id	id: The ID of the question
question	The full text of the question

Return Code	Description
0	Success
10001	Permission not allowed

3.2.1.14. Request List of user bound authentication methods

Description: Call this function to retrieve list of token information that is bound with user.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/user/auth/list/{admin username}

RESTful parameters:

Key	Description
username	The user's username that want to get the list
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information that includes a list of token. See below for the details.

RESTful object content:

Key	Description
tokenList	List of following objects. Empty mean no token bound **Key** / **Description** sn / Token serial number type / Token type. 1= SMS 2=OTP 3=FIDO status / Token status.

	0=Inactive 1=active 2=active and locked 3=pending 4=pending and locked
certList	List of following objects. Empty mean no certificate bound

Key	Description
sn	Certificate serial number
fingerprint	Certificate fingerprint, in SHA1, encoded to HEX value.
subjectDn	Certificate subject DN value
issuerDn	Certificate issuer DN value
revoked	True= certificate revoked False= certificate is active
validFrom	Certificate effective start date, in unix timestamp in miliseconds. Eg: 1456831134000
validTo	Certificate effective end date, in unix timestamp in miliseconds. Eg: 1456831134000

device	Device. Empty mean no device bound

Key	Description
name	Device name
model	Device model
os	Device OS
status	Device status 0=inactive 1=active 2=pending

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input

22002	User not found

3.2.1.15. Check Token Status

Description: Call this function to get user token status.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/getStatus{admin username}

RESTful parameters:

Key	Description
username	The user's username that want to get the list
type	Type of the token - 1 = Mobile Token - 2 = SMS Token - 3 = CH Token - 4 = PKI Token
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	Object contain token status, value as below: - Empty string = no token - 1 = Pending - 2 = Valid - 3 = Temp Deactivated - 4 = Deactivated - 5 = Suspended

Return Code	Description
0	Success
10001	Permission not allowed

10002	Invalid Input
22002	User not found

3.2.1.16. Update user status

Description: This function allows admin change the user status. This function will not change MFA status.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/user/status/update/{admin username}

RESTful parameters:

Key	Description
username	The user's username that need to update the status
status	1=active 0=inactive
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input
22002	User not found

3.2.1.17. Update token status

Description: This function allows admin change the token status.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/update/token/status/{admin username}

RESTful parameters:

Key	Description
username	The user's username that own the token
type	Token that needs to update. - 1 = Mobile Token - 2 = SMS Token - 3= Challenge Question Token - 4 = PKI Token
status	Token status. - 1=Pending - 2=Valid - 3= Temp Deactivate - 4= Deactivate
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input
22002	User not found
29001	Token not found

3.2.1.18. Unbind and delete user

Description: Call this function to unbind all token belong to the user and delete the user after that.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/user/unbindAndDelete/{admin username}

RESTful parameters:

Key	Description
username	The user's username that need to unbind and delete
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input
22002	User not found

3.2.1.19. Verify Signature

Description: Call this function to verify the PKCS#7 signature.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/validator/verifySignature

RESTful parameters:

Key	Description
username	The user's username
signature	The PKCS#7 attached signature encoded in Base64
algorithm	The algorithm used during the signing. Valid values are: - 0: SHA-1 - 1: SHA-256 - 2: SHA-384 - 3: SHA-512
plainText	The plain text of the signed string encoded in Base64

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input
22002	User not found
26010	Certificate is not owned by the user
26011	Certificate revoked
55000	Invalid signature

3.2.1.20. Unlock User

Description: Call this function to unlock user

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/user/unlockUser/{admin username}

RESTful parameters:

Key	Description
lockedUsername	The locked user's username
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
object	The object containing additional information. For this function it will always return empty

Return Code	Description
0	Success
10001	Permission not allowed
10002	Invalid Input
20002	Company not found
22002	User not found
22006	Requestor and user is the same user
22016	User not in locked status

3.2.1.21. Update user profile

Description: Call this function to update user's profile.

RESTful method: **PUT**

RESTful link:

https://cloud.centagate.com/CentagateWS/webresources/user/updatebyusername/{admin username}

RESTful parameters:

Key	Description
username	The user's username
firstName	The user's first name (optional*)
lastName	The user's last name (optional*)
address	The user's address (optional*)
zip	The user's zip (optional*)
city	The user's city (optional*)
state	The user's state (optional*)
statusUser	The user's status (optional*)
email	The user's email (optional*)
userCountryId	The user's country ID (optional*)
userTimeZoneId	The user's time zone ID (optional*)
availApps	The user's application ID (optional*)
clientId	The user's client ID (optional*)
userType	The user's type (optional*)
userGroupName	The user's group name (optional*)
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from admin username + authToken

*NULL value will be treated as optional.

RESTful output:

Key	Description
code	The return code
message	The return message
Object	Return empty string

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input

10003	DB protection error
10004	DB error
20002	Company not found
21001	Group not found
22002	User not found
22029	User edit pending approval
22031	User edit fail

3.2.1.22. Update user password

Description: Call this function to update user's password.

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/password/updatesimple/{username}

RESTful parameters:

Key	Description
password	The user's current password. Can be a plain password or encrypted password. If the password needs to be encrypted, use AES 256 with encryption key = secret key + @ |0N5 4 C3NTAG4T3v1 Example: If secret key = 5yfpQcsYGo9a, then encryption key = 5yfpQcsYGo9a@ |0N5 4 C3NTAG4T3v1
newPassword	The user's new password. If the "password" param is encrypted, this param also needs to be encrypted. Use AES 256 with encryption key = secret key + @ |0N5 4 C3NTAG4T3v1 Example: If secret key = 5yfpQcsYGo9a, then encryption key = 5yfpQcsYGo9a@ |0N5 4 C3NTAG4T3v1
integrationKey	The application's integration key. This is only required if the password needs to be encrypted. Otherwise, you can leave it empty / null, or no

	need to pass this parameter.

RESTful output:

Key	Description
code	The return code
message	The return message
Object	Return empty string

Return Code	Detail
0	Success
10002	Invalid Input
10003	DB protection error
10004	DB error
10011	Cryptographic error
20002	Company not found
23001	Invalid credentials (User not found / User is not active/Invalid current password)
23025	Web API error
28001	Password policy content is not up-to-date. Please update your Group Setting.
28003	You are not allowed to use the last X passwords
28004	Password must at least contain X characters
28005	Password must mix letters and digits Password must mix lower and upper letters and digits Password must mix lower and upper letters, digits and special characters
28006	Password is blacklisted. Please choose another password
28007	New password must be different from the current password
28008	You are changing your password too frequent. Password cannot be changed within X (day)
28010	Password must not have more than 2

	consecutive repeated characters
28011	Password must not be equal to username

3.2.1.23. Check user session

Description: Call this function to check user session is active or inactive

RESTful method: **GET**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/auth/sessioncheck/{username}/{cenToken}

RESTful parameters:

Key	Description
username	The user's username
cenToken	The hmac value calculated using SHA256 with secretCode as key and plain text from username + authToken

RESTful output:

Key	Description
code	The return code
message	The return message
Object	Return empty string

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input

3.2.1.24. Secugen fingerprint registration

Description: Call this function to register fingerprint by using secugen

RESTful method: **PUT**

RESTful link:
https://cloud.centagate.com/CentagateWS/webresources/token/registerFprint/{username}/{authToken}

RESTful parameters:

Key	Description
username	The user's username
authToken	The generated authToken
userId	The user's id
tokenType	6 = Secugen fingerpint
byteEncode1	Result generated from the secugen API (First fingerprint scan). * This API currently will only work with Internet Explorer Browser.
byteEncode2	Result generated from the secugen API (Second fingerprint scan). * This API currently will only work with Internet Explorer Browser.

RESTful output:

Key	Description
code	The return code
message	The return message
Object	Return empty string

Return Code	Detail
0	Success
10001	Permission not allowed
10002	Invalid Input
10003	DB protection error
10004	DB error
22002	User not found
29001	Token not found
29002	Token not active
23037	Fingerprint is not match
23038	Fingerprint exceed two record

3.3.Question List

ID	Question
0	Create your own security question
1	What is the food you least liked as a child?
2	What is the name of your first stuffed animal?
3	What did you earn your first medal or award for?
4	What is your favorite security question?
5	What is the toy/stuffed animal you liked the most as a kid?
6	What was the first computer game you played?
7	What is your favorite movie quote?
8	What was the mascot of the first sports team you played on?
9	What music album or song did you first purchase?
10	What is your favorite piece of art?
11	What was your grandmothers favorite dessert?
12	What was the first thing you learned to cook?
13	What was your dream job as a child?
14	Where did you have your first kiss?
15	Where did you meet your spouse/significant other?
16	Where did you go for your favorite vacation?
17	Where were you on New Years Eve in the year 2000?
18	Who is your favorite speaker/orator?
19	Who is your favorite book/movie character?
20	Who is your favorite sports player?
21	What is your favourite childrens book?
22	What was your childhood nickname?
23	What was the model of your first motorised vehicle?
24	What was your favourite singer or band in school?
25	What was your favourite film star or character in school?