
SGIWEBSRV WEB API Programmers Manual

SDK version 0.9
(DRAFT)



SecuGen India Pvt. Ltd.
C-605, Solaris, Saki Vihar Road,
Andheri, Mumbai 400057
(INDIA)
www.secugenindia.com

Copyright 2015 SecuGen India Pvt. Ltd.

Disclaimer

Contents of this document are subject to change without notice, SecuGen India does not warranty correctness of the material herein or fitness for any purpose. This document is supplied without any expressed or implied warranties.

SecuGen India Pvt. Ltd.

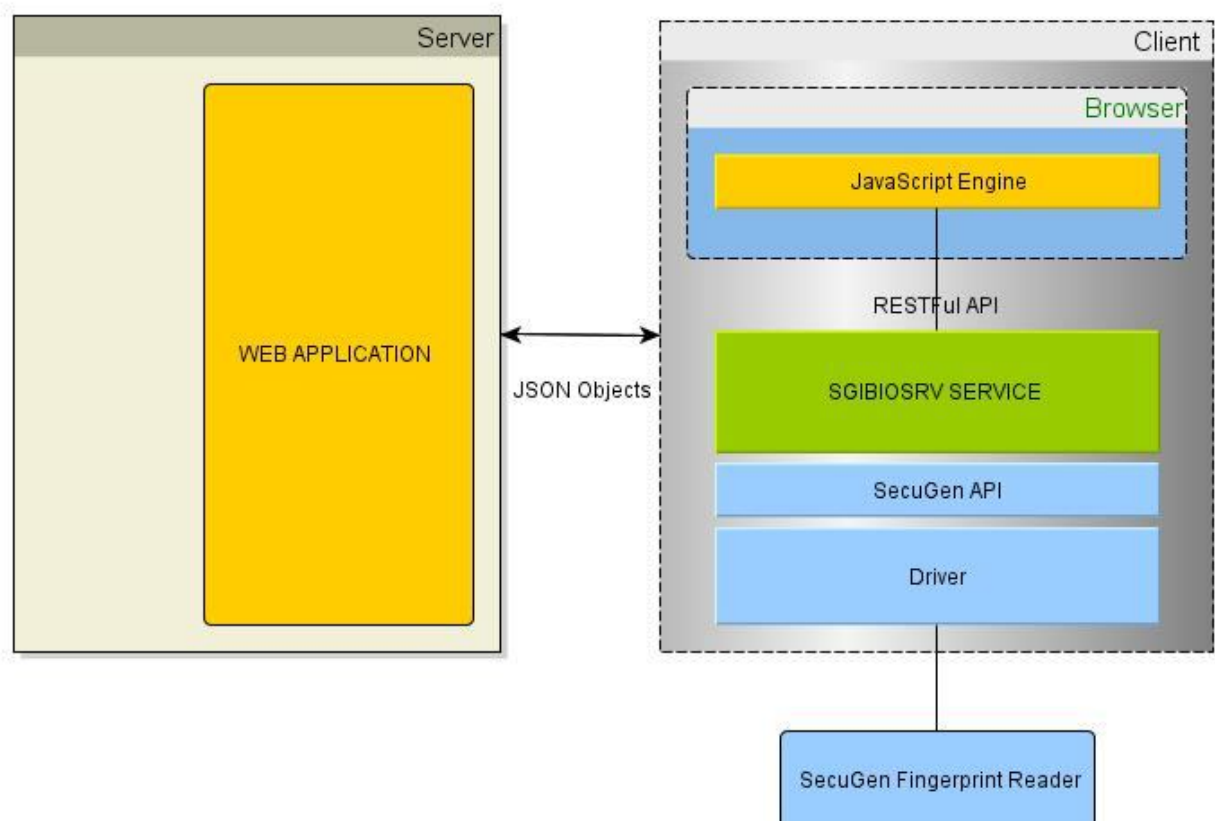
1. License Agreement

2. Introduction

SecuGen WEB API supports JavaScript access to SecuGen fingerprint readers, enabling browser based applications to access SecuGen fingerprint sensors. JavaScript access permits cross browser functioning and extremely fast capturing of fingerprint data in a browser based application.

SecuGen WEB API makes it very simple to incorporate fingerprint capturing functionality in your browser based application through JavaScript. Applications written using WEB API work on almost all modern browsers. Using WEB API eliminates need for JAVA runtime or browser plug-in on the client machine as well as applet signing and deployment issues related to different JRE versions and browser versions. This document describes the RESTFUL web service calls supported by WEB API SDK.

WEB API provides simple call to capture fingerprint data and template in one method. It also provides UIDAI specific calls to capture PID block for single or multiple fingers, UIDAI BFD (Best Finger Detection) support provides RBD block with local duplicate check. Applications such as AADHAAR authentication, E-KYC based on AADHAAR and BFD are extremely easy to develop and deploy as web based applications using SecuGen WEB API.



3. Installation and pre-requisites

<< TO COMPLETE >>

4. SGIFPCapture

This service returns fingerprint data, details of sensor and extracted template to the caller as JSON object. In case of HTTP request this service can be called as URI <http://localhost:8000/SGIFPCature>. The port number may change depending on the way the service is configured, 8000 is default port for the service.

Parameters

Following table describes the parameters and their permissible values that can be passed to the service. All the parameters are optional and their defaults are described below.

Name	Type	Description
Licstr	STRING	This is the license key provided for the domain, when not used the WEB server will work only for limited period (usually 90 days)
Timeout	INTEGER	Specifies the timeout in milliseconds to wait for the sensing operation to complete. If fingerprint image is not captured within this time (user does not place the finger on the sensor) then an error is generated. Defaults to 10000.
Quality	INTEGER	Specifies the quality of the image desired value is from 1 to 100. Higher value implies better image. Default value is 50.
TemplateFormat	STRING	Extractor template format is specified in this parameter, currently supported values are "ISO" and "ANSI". Defaults to "ISO".

JSON Object Returned

Web service returns JSON formatted object, that contains following fields.

Name	Type	Description
ErrorCode	INTEGER	Integer value, describes error if any, value of 0 indicates no error other wise the error code or non-zero indicates various errors described in this document elsewhere. <i>You must check of this value before accessing other fields of JSON object, if this is not 0 then other fields are NULL or undefined.</i>
Manufacturer	STRING	Currently "SecuGen" .
Model	STRING	Currently "HU20" indicating SecuGen Hamster Pro-20
SerialNumber	STRING	String containing the unique serial number of the connected device.
ImageWidth	INTEGER	Integer value indicating the width of the fingerprint image in pixels.
ImageHeight	INTEGER	Integer value indicating the height of the fingerprint image in pixels.

ImageDPI	INTEGER	Integer value indicating resolution of the fingerprint image in dots per inch.
ImageQuality	INTEGER	Integer value indicating the quality of the image actually captured it will always be equal to or higher than the quality parameter passed as argument.
NFIQ	INTEGER	Integer value, NIST Finger Image Quality number from 1 – 5 . 1 is best and 5 is worst.
ImageDataBase64	STRING	String containing actual Image data (raw) encoded as base64 string.
BMPBase64	STRING	String value fingerprint image in .BMP format encoded as base 64 string, useful for display in browser using data element in image tag.
TemplateBase64	STRING	String value containing Template encoded as base 64 format. This value is encrypted if called with session key parameter.

Notes

5. SGIEncrollCapture

This web service is useful for capturing multiple fingerprints from the fingerprint reader. Parameters required are same as SGIFPCapture and can be used to capture one fingerprint as well. Call this service once for each capture along with the same server handle to accumulate fingerprints. The service also ensures that one fingerprint is present only once in the array i.e. local duplicate check is performed on the client end. JSON object returned contains array of templates

6. SGIUIDAI_AUTHCapture

This web service provides UIDAI authentication related service. As per the specification of UIDAI Authentication API version 1.6. The service returns encrypted PID block along with encrypted SHA256 hash value and session key (optionally encrypted with public key).

Browser based applications can call this service via JavaScript to get the data that can be directly used on the AUA or ASA backend for further processing (such as adding wrapper XML and signing). Develop of UIDAI AADHAAR authentication applications can write single portable application using JavaScript. The service supports single or multi finger authentication as required by the specifications.

Parameters

Following table describes the parameters and their permissible values that can be passed to the service. All the parameters are optional and their defaults are described below.

Name	Type	Description
Licstr	STRING	This is the license key provided for the domain, when not used the WEB server will work only for limited period (usually 90 days)
Timeout	INTEGER	Specifies the timeout in milliseconds to wait for the sensing operation to complete. If fingerprint image is not captured within this time (user does not place the finger on the sensor) then an error is generated. Defaults to 10000.
Quality	INTEGER	Specifies the quality of the image desired value is from 1 to 100. Higher value implies better image. Default value is 50.
Timestamp	STRING	Current time should be provided based on the server time rather than depending on the client machine time which may be incorrect. Also for E-KYC application the time stamp need to be provided even at the outer XML, must match the one in the PID block. <i>We highly recommend passing this parameter based on server time in format YYYY-MM-DDTHH:MM:SS</i>
SessionKey	STRING	This is the session key that will be used for encrypting the PID block as well as SHA256 hash value. This must be in BASE64 encoded format with URI encoding. If not specified random session key will be generated. If AuthCert is specified then this key is encrypted using UIDAI public key.
Fingerpos	STRING	Finger Position as specified in UIDAI specifications, if not provided "UNKNOWN" is the default.
SrvHandle	INTEGER	Used for context maintenance when multi finger PID is desired.
AuthCert	STRING	Base64 string containing the data in .CER format, UIDAI public

key certificates can be read as string and used as the value for this parameter. Validity of the certificate is NOT checked by this call.

JSON Object Returned

Web service returns JSON formatted object, that contains following fields.

Name	Type	Description
ErrorCode	INTEGER	Integer value, describes error if any, value of 0 indicates no error other wise the error code or non-zero indicates various errors described in this document elsewhere. You must check of this value before accessing other fields of JSON object, if this is not 0 then other fields are NULL or undefined.
Manufacturer	STRING	Currently " SecuGen ".
Model	STRING	Currently " HU20 " indicating SecuGen Hamster Pro-20
SerialNumber	STRING	String containing the unique serial number of the connected device.
ImageWidth	INTEGER	Integer value indicating the width of the fingerprint image in pixels.
ImageHeight	INTEGER	Integer value indicating the height of the fingerprint image in pixels.
ImageDPI	INTEGER	Integer value indicating resolution of the fingerprint image in dots per inch.
ImageQuality	INTEGER	Integer value indicating the quality of the image actually captured it will always be equal to or higher than the quality parameter passed as argument.
NFIQ	INTEGER	Integer value, NIST Finger Image Quality number from 1 – 5 . 1 is best and 5 is worst.
PIDBase64	STRING	Encrypted PID encoded as base 64 string. Session key is used to encrypt the PID block (AES256 PKCS7 padding)
BMPBase64	STRING	String value fingerprint image in .BMP format encoded as base 64 string, useful for display in browser using data element in image tag.
SerHandle	INTEGER	Context handle of the service, for multiple finger PID store this handle and pass as argument in next call, the new scanned finger FMR is added to existing PID, If this is NULL or omitted then a new session starts every time.
SHA256Base64	STRING	String value of encrypted SHA256 hash of the PID block encoded as base 64 string.
SessionKeyBase64	STRING	Session key 256 bit encoded as base 64 string, this is returned when session is generated on the client machine. If public key was provided in AuthCert parameter, then this is an RSA encrypted based64 encoded string.
Timestamp	STRING	Current date time as string in YYYY-MM-DDTHH:MM:SS format if generated on the local machine.

LocalIP	STRING	IP address of the machine on which SGIBIOSRV is running. This may be behind NAT in which case you will need to get the router address.
---------	--------	--

Although the parameters are optional we highly recommend that the developer pass Timestamp and AuthCert as parameters, for proper authentication and EKYC.

Notes

Out of the fields returned, for UIDAI authentication and EKYC purpose, you will only need the PIDBase64, SHA256Base64, Timestamp, SerialNumber and SessionKeyBase64 along with the AADHAAR number. Additionally 'fdc' value for SecuGen Pro-20 is **SGIH20SGN**. These values can be used to construct portions of UIDAI auth XML directly.

Note that the API only supports XML and not Proto Buffs.

7. SGIUIDAI_BFDCapture

UIDAI best finger detection API 1.6 required the RBD encrypted block and this web service provides the Encrypted RBD block. As per the specification of UIDAI BFD API version 1.6. The service returns encrypted RBD block along with encrypted SHA256 hash value and session key (optionally encrypted with given public key).

Browser based applications can call this service via JavaScript to get the data that can be directly used on the AUA or ASA backend for further processing (such as adding wrapper XML and signing). Developer of BFD applications can write single portable application using JavaScript. The service support multi finger capture as required by the specifications.

Parameters

Following table describes the parameters and their permissible values that can be passed to the service. All the parameters are optional and their defaults are described below.

Name	Type	Description
Licstr	STRING	This is the license key provided for the domain, when not used the WEB server will work only for limited period (usually 90 days)
Timeout	INTEGER	Specifies the timeout in milliseconds to wait for the sensing operation to complete. If fingerprint image is not captured within this time (user does not place the finger on the sensor) then an error is generated. Defaults to 10000.
Quality	INTEGER	Specifies the quality of the image desired value is from 1 to 100. Higher value implies better image. Default value is 50.
Timestamp	STRING	Current time should be provided based on the server time rather than depending on the client machine time which may be incorrect. We highly recommend passing this parameter based on server time in format YYYY-MM-DDTHH:MM:SS
SessionKey	STRING	This is the session key that will be used for encrypting the PID block as well as SHA256 hash value. This must be in BASE64 encoded format with URI encoding. If not specified random session will be generated.
Fingerpos	STRING	Finger Position as specified in UIDAI specifications, This value must be provided and "UNKNOWN" is not allowed in BFD application.
SrvHandle	INTEGER	Used for context maintenance when multi finger RBD is desired.
AuthCert	STRING	Base64 string containing the data in .CER format, UIDAI public key certificates can be read as string and used as the value for this parameter. Validity of the certificate is NOT checked by this

call.

JSON Object Returned

Web service returns JSON formatted object, that contains following fields.

Name	Type	Description
ErrorCode	INTEGER	Integer value, describes error if any, value of 0 indicates no error other wise the error code or non-zero indicates various errors described in this document elsewhere. You must check of this value before accessing other fields of JSON object, if this is not 0 then other fields are NULL or undefined.
Manufacturer	STRING	Currently " SecuGen ".
Model	STRING	Currently " HU20 " indicating SecuGen Hamster Pro-20
SerialNumber	STRING	String containing the unique serial number of the connected device.
ImageWidth	INTEGER	Integer value indicating the width of the fingerprint image in pixels.
ImageHeight	INTEGER	Integer value indicating the height of the fingerprint image in pixels.
ImageDPI	INTEGER	Integer value indicating resolution of the fingerprint image in dots per inch.
ImageQuality	INTEGER	Integer value indicating the quality of the image actually captured it will always be equal to or higher than the quality parameter passed as argument.
NFIQ	INTEGER	Integer value, NIST Finger Image Quality number from 1 – 5 . 1 is best and 5 is worst.
Attempts	INTEGER	Number of attempts for capture of the specific fingerprint. Useful for implementing capture of best quality finger within specified attempts.
RBDBase64	STRING	Encrypted RBD encoded as base 64 string. Session key is used to encrypt the RBD block (AES256 PKCS7 padding)
BMPBase64	STRING	String value fingerprint image in .BMP format encoded as base 64 string, useful for display in browser using data element in image tag.
SerHandle	INTEGER	Context handle of the service, for multiple finger PID store this handle and pass as argument in next call, the new scanned finger FMR is added to existing RBD, If this is NULL or omitted then a new session starts every time. For BFD application you need to capture 10 fingerprints. The service automatically checks for duplicates.
SHA256Base64	STRING	String value of encrypted SHA256 hash of the RBD block encoded as base 64 string.

SessionKeyBase64	STRING	Session key 256 bit encoded as base 64 string, this is returned when session is generated on the client machine. If public key was provided in AuthCert parameter, then this is an RSA encrypted based64 encoded string.
LocalIP	STRING	IP address of the machine on which SGIBIOSRV is running. This may be behind NAT in which case you will need to get the router address.
Timestamp	STRING	Current date time as string in YYYY-MM-DDTHH:MM:SS format if generated on the local machine.

Although the parameters are optional we highly recommend that the developer pass Timestamp and AuthCert as parameters.

Notes

Error Codes

ERROR CODE	DESCRIPTION
0	No Error
1	Creation failed (fingerprint device not installed correctly driver files error)
2	Function failed (wrong type of sensor or not correctly installed)
3	Internal (invalid parameters to sensor API)
5	DLL load failed
6	DLL load failed for driver
7	DLL load failed for Algorithm
51	System file load failure
52	Sensor chip initialization failed
53	Sensor line dropped
54	Timeout
55	Device not found
56	Driver load failed
57	Wrong image
58	Lack of bandwidth
59	Device busy
60	Can not get serial number of the device
61	Unsupported device
101	Very low minutiae count
102	Wrong template type
103	Invalid template
104	Invalid template
105	Could not extract features
106	Match failed
1000	No memory
4000	Invalid parameter passed to service
2000	Internal Error
3000	Internal error extended
6000	Certificate error can not decode
10001	License error
10002	Invalid domain
10003	License expired