Digital Signature Api Documentation

Toci

August 18, 2015

Contents

1 Indtroduction

API Resources

- Resource: /api/passwordsign

  Resource destination: This resource allows to sign in data using sent *.pfx file with private key.

- Resource: /api/verify

  Resource destination: This resource allows to verify signed data using signature and certificate with public key (*.cer).

2 Signing data

Example usage:

POST /api/passwordsign

Accepted request formats:

- application/x-www-form-urlencoded
- application/json

Request body:

- data - contains base64 string with data to sign
- cert - certificate file in base64 string
- password - password to open the certificate

Response formats: JSON Example JSON Response structure:

"B2cA[...]IwRg2"

Error handling:

Error message format:

- String "Error message" response.

3 Verifying data

Example usage:

POST /api/verify

Accepted request formats:

- application/x-www-form-urlencoded
- application/json

Request body:

- data - contains base64 string with data to verify
- signature - signature of data (produced by /api/passwordsign)
- password - password to open the certificate

Response:string specifying if verification succeeded.

Response formats: JSON Example JSON Response structure:

true

Examples of full requests and responses are placed in Appendix.

4 Appendix

Example sign request :
Request format:

- application/x-www-form-urlencoded

  You can find the example in the attached sign-x-www-form-urlencoded.txt file.

- application/json

  You can find the example in the attached sign-json.txt file.

Example verify request :
Request format:

- application/x-www-form-urlencoded

  You can find the example in the attached verify-x-www-form-urlencoded.txt file.

- application/json

  You can find the example in the attached verify-json.txt file.

Example request response:

true