Technical documentation

Server-server connection

JWE configuration

For some endpoints we need from you enc and alg from JWE parameters. Acceptable values are:

- Algorithm used by Verestro to encipher content of message (enc) - A256GCM,
- Algorithm used by Verestro to encipher encryption key (alg) - RSA-OAEP-256,
- Algorithm needed from you to encipher content of message (enc) - A256GCM,
- Allowed algorithms for key encryption (alg) - RSA-OAEP-256 or RSA-OAEP.

Recommended JWE libraries for various programming languages:

- PHP,
- JAVA.

Request:

To process encrypted message you need to perform a few additional steps on top of standard message processing:

- Verestro add headlines:
  - Public-Key through which you can encrypt response to us (if needed),
  - Encrypted-Request headline confirming message encryption; value true or false,
- Expose endpoint with your Public Key - you will find a similar endpoint in our technical documentation, GET /secure/public_key
- Use Verestro Public Key to create JWE and transfer data in payload,

Response:

When the response contains sensitive data that requires encryption, use Verestro public key encryption available here GET /secure/public_key

Additional information:

- In case of errors (i.e. validation errors) you will receive unencrypted response,
  - ENCRYPTION_REQUIRED,
  - INVALID_PUBLIC_KEY,
  - INVALID_PAYLOAD,
  - CANT_DECRYPT_PAYLOAD.

Example request:

Correct request	Sent request (incorrect)	Received by CMS Antaca (after decipher action with private key)
`{"card_no" : 1337}`	{"payload" : "eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIn0.rdUrW12XCZQgLFDJ-2zAHWYYnaAanctceE1-Y6yJUpIX0B2dLu-bvYOEJ83KxxUs-ZjA41R4PmAVilx1cTF4pv-7CZR0_ki85XRATBYF2-MvZdcC81fHy2QPU_ZsAEWAW00a1wKJmuEsgPB2m1aLZ7oK4fC1hciep4PyAtuWQRYHjhNb-UDT41_gDKTbnSGTwheL7S0mAJ_HsKfnZFHYUrM77UcxQGZKnH7Mzqvndf9THiMo0-3MWliYFDAm1bqN2_KTIoBNCprYjFnyIXPCjib73bjWX_P2ip5Ul84cngbQmFVzc7o91JrpJvYou1INS7zL4XKLFcADN4nZ_9ePWsm5_kX5SOMyUyEhOC9gusrLNAJ0MHaIFHni8WqnMAWM3_MC4OQDYetKax5bnHK6x42_5eFaf6ZmzmioKny5aGm-4Vo8TEu691FmPxglhyenWlMhvBvf6ZeVsy58Ofr0mi3TXjwYbAyas7m6sncxZu1FhEJ4da6gtNjmjuKdikOOntu8V71QQ07nczNqfGlUv0RcUc9uKJq5je4b9BEbK9WuQcroxmALqC4HTt1xhICHrVUA0d_t3fglhS2n7wNaKKCFq70ZWIrpdTaBd35kdVQOEjZgCavSjbZOzgOzcEqS6P2Blm7bZ7ZZBmnfk8y8M4m0xWoQNTmLC6nqz9bSbME.UEryKNClDxQZpyWu.6Lw_5CcZ9HiVxHfi_XTAFw.pYbQ6tdmQYe1kiPonm1GhA"}	`{"card_no" : 1337}`

Example response:

Correct response	Sent response by CMS Antaca	Received by you

`{"card_no" : 1338}`	{"payload" : "eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIn0.iPmvEKtMAMrrEiR89vlwsL77ZfqxXrcMiy-bx3z6_7HAo__aQzBpMVDtLyj3kTHYWxen8bhPuVyebXyaIHL20sekFzcIFFzvaGoyQYU6zOK8tPv81tgixQe8SDnEr5v9VWBfiHxtPvqlpQlig2is5ynBkyqjdpQWEagR3MpqpATGl7f-omG82Jq0OwZByWI8I6P89hczwgK37F-MUnQDxcRUM3RagbHKNeIcfmPdJpNeqFZHe45y4wUkTWN0uzW72qydkN_4uM9fy0nrUpgsJNbtJGAVIUVmDz4pIZkiI1zyGbfZX-PT7Wh9UNM06gEUf4i2goZY-m4wPB0n2zXvxzcEdfTH27iPp-aKiJjfJpYb_ZnHyklk__gZlAy9r7W0594dY-eBJ_iUa5aeDsFS2TIfsfjMJsL8NRWY2noiTw5lsneD8dwvr6N_rYcWoFXDyWXHoRitSSd2iYrB80gbeSOBW0wfKtPxNIZrR0uDhkE8FouS5Pk7QBw412kd43GtrEpAijqn3ne7MNUpCtuNfJ8e_NdGDLTR7CSHhC0jfFlchpIvklF42o216NO-OnyJsjdv1w4_w1ugs61fTHDl8lgBalOjOxauKwIvJJOyFdWmpjlXuzJhrray7ov25uh2ibvFv3Gfd2iuGUnLIZzYBOTT8ftGWTCGXTDvVOvzGbs.c3qMNb2Bne-7g0Wz.PInghFM6Q8Gn0p4Tlebig32s-ZrpLqTMqQDlpXLLYx0iq-StrKco_HrjdN4MxondP4CicCgseIjcV8JR29jKYX-nqKdchEYq_vVIzFHcNI_Mx7y1el192QbMyx6b0Gbj5L79wpuB7qCUqTBNhJZ2c07PuyPsewcNwglvnc-OrA-2vL6lJnBi5ZGH8gBH1cZCgmbrMpZGNFPG3oFpOn9JPzmnvQxe9tvSFFj5989A8d_XMHP-ZQ.dJZxnBRxJeMKswDsCA3cXA"}	Check yourself by using Private Key included in the response.

Public Key

This method is used to share your public key for encryption.

```
GET https://server-domain.com/public-key
```

Headers:

```
Content-Type: application/json
```

response:

```
200 OK
{
  "publicKey": "QSBwdWJsaWMga2V5IHNob3VsZCBiZSBoZXJlIGhvd2V2ZXIgaXQgd2FzIHRvbyBsb25nIDoo"
}
```

@swagger="https://s3.verestro.dev/quicko-prepaid/devzone/api-docs-secure.json?AWSAccessKeyId=quicko-prepaid&Signature=0hLv91hrIjIu%2Fdg8N%2BPEVvfpcm4%3D&Expires=2020026755"

Revision #9
Created 24 June 2022 09:00:19 by Tadeusz Krysa
Updated 2 January 2025 12:17:59 by Barbara Tudruj