RSA Key Pair Generation and Storage

For each agent created, the API generates an RSA key pair consisting of a public key and a private key. The key pair is generated using a modulus length of 4096 bits. The generated keys are stored in the MySQL database along with other agent information.

Key Generation Process

When a new agent is created, the API performs the following steps to generate the RSA key pair:

1. Generates an RSA key pair using the `crypto.generateKeyPairSync` method with the following options:
   - Algorithm: RSA
   - Modulus Length: 4096 bits
   - Public Key Encoding: PKCS#1 format in PEM encoding
   - Private Key Encoding: PKCS#1 format in PEM encoding
2. The generated public key and private key are converted to string representations.
3. The public key string is stored in the `pubKey` field of the agent's record in the MySQL database.
4. The private key string is stored in the `privKey` field of the agent's record in the MySQL database.

Example

When a new agent is created, the API generates an RSA key pair. Let's assume the key generation process produces the following keys:

- Public Key:

  ```
  -----BEGIN RSA PUBLIC KEY-----

  MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAyDRa5PEVYl2T3EzvG1on

  ...

  d8Ou9azXQIDAQAB

  -----END RSA PUBLIC KEY-----
  ```

- Private Key:

```
-----BEGIN RSA PRIVATE KEY-----

MIIJKQIBAAKCAgEAyDRa5PEVYl2T3EzvG1onC4vPwL...

...

8RTgJ8SPaHv/SmB2DhYO98C6HpU=

-----END RSA PRIVATE KEY-----
```

The generated keys are then stored in the agent's record in the MySQL database.

Revision #1
Created 28 June 2023 09:55:00 by Makito
Updated 3 July 2023 09:39:09 by Makito