REST API

本节用于描述各类节点功能的http接口和使用方式

接口分为本地处理的接口以及需要与父节点通信的接口两种

需要与父节点通信的接口

需要先确认其父节点server的运行，子节点的相关参数由json文件传入，运行时需要在加入json文件名，例如：

```
python3 python/restAPI.py –c client.json
```

服务端

客户端

节点申请加入管理域 /sk/request

如果user.local_sk存在，返回base64编码后的私钥内容sk及json格式的参数验证信息local-cert；否则，向父节点请求私钥，保存到user.local_sk并返回base64编码后的私钥内容sk及json格式的参数验证信息local-cert。

管理域及验证信息生成 /domain/request

返回新生成管理域的主私钥msk，新域管理节点的私钥sk，新管理域的主公钥mpk(均为base64编码)及json格式的新域参数验证信息admin-cert

本地处理的接口

不需要server的运行，由http中POST以json的格式传入相关的参数

加密数据 /encrypt


```
{
 "message": "SGVsbG8=",
 "mpk":
"MIHqBgoqgRzPVQGCLgYBBgkqgRzPVQGCLgMGCiqBHM9VAYIuBAEEQQQ_J5Nihxu3dttODZjkVd
WKYbzfP2_v4XMCG-
EFfFvf9bCNCtWF35qg46M6ewD3bZhCZ0g3Mz9zeCJ7djEM7vrSBIGBBGEcSeqm5v9Mwmk8epi2-
6ONYB3BgvTX-1kvVGSxuswdsvKnAHTijwYEFvQuJRVLrD99qhy-HYnSxvBiVrkcn4Cm-
YJqldVtTKXM66MvB7YthtAnnWVhFbxLaNl_DweNILJS266VGwvf4ycxgKOVdkCmubUO-
zhtsyGn5URX307i",
 "user_id": "Client"
}
```

上图是一个请求body的示例，message和user_id分别为待加密消息（urlsafe_b64encode编码）和通信对手的标识，mpk为urlsafe_b64encode编码的公共参数文件。上述请求(即加密后)得到的结果如下：


```
{
  "cipher": "MIGtBIGBBB0eQ1OhIg8kxGM9RsaDFOur4eepGe9X-
abkXnkzaW97nLiuXyGibouf0pfOSmiuok27WnvyMp6ZitzDqwMzrM2k4ZYJUZxWFjCh-
DT9zgDWkEK0sPvxEmbrYc6-
g7tLg6IqAhdtRbWT2Ud7qiQDwDUiPIzT1u463TTAhQ_7hqSQBAUP64qHDwQg_GW-vYpER7-
gmMdmknjyFoNOxrQSII0SDrh4ils8Gik="
}
```


解密数据 /decrypt


```
{
  "sk":
"MIIBeAYKKoEcz1UBgi4GAQYJKoEcz1UBgi4DBgoqgRzPVQGCLgQBBEEEPyeTYocbt3bbTg2Y5FXVi
mG83z9v7-FzAhvhBXxb3_WwjQrVhd-
aoOOjOnsA922YQmdINzM_c3gie3YxDO760gSBgQRhHEnqpub_TMJpPHqYtvujjWAdwYL01_tZL1Rk
sbrMHbLypwB04o8GBBb0LiUVS6w_faocvh2J0sbwYla5HJ-
ApvmCapXVbUylzOujLwe2LYbQJ51lYRW8S2jZfw8HjSCyUtuulRsL3-MnMYCjlXZAprm1Dvs4bbMhp-
VEV99O4gQGQ2xpZW50BEEELy4AEBX4UdCoG47PF0J0b6t7p-
lP6EzUywxF0aXeLTOxQDQm4H321ALRZdE9GqVKYDBymYVsCk1PatEBncZ73QRBBAQJNViWyWCAq
KBV4SlsuPAVHR6F7eZ_iqrHj3RBuJ6wNpsbMIb31w2AtTCAvoFSGtauDxqYHq14ABimHs-vys8=",
  "cipher":"MIGtBIGBBB0eQ1OhIg8kxGM9RsaDFOur4eepGe9X-
abkXnkzaW97nLiuXyGibouf0pfOSmiuok27WnvyMp6ZitzDqwMzrM2k4ZYJUZxWFjCh-
DT9zgDWkEK0sPvxEmbrYc6-
g7tLg6IqAhdtRbWT2Ud7qiQDwDUiPIzT1u463TTAhQ_7hqSQBAUP64qHDwQg_GW-vYpER7-
gmMdmknjyFoNOxrQSII0SDrh4ils8Gik="
}
```


上图是一个请求body的示例，sk和cipher分别为用户私钥和密文（均为urlsafe_b64encode编码）。上述请求(即解密后)得到的结果如下：


```
{
  "dmessage": "SGVsbG8="
}
```


私钥生成 /sk

<未实现>

如果user.local_sk存在，返回base64编码后的私钥内容，否则，返回空。


```
{
 "msk":
```

```
"MIIBDQYKKoEcz1UBgi4GAQYJKoEcz1UBgi4DBgoqgRzPVQGCLgQBBEEEArxw6TXGybvmD_KG6Ba
s8UDgslLWp0U-LjZ5N-NO51VqdN-
5vU_2DeyZuO8uCfDvR49KMjfM01l1lIO2007YeQSBgQQ7KqYGzK49qn9nM_lA_mt1OQICkpjJ2FP26
5H6MeQoi1OGE2nh2EFyirVPmx0qz1jt-WAVReSQIW6dHcU5_n-FrA3ZB_KmiDMMHift1-
3YDukyVy9qePg-jiPW3qgRlSMEWFNI7wAEu_-OkbmcQc-
g1o3E74WOCRota1bhjFE3cwIhAIbcnYyhVJWWp3U23o0SSXLJs-aAQJ8aVBGeY3FYWAMp",
 "user_id": "Server1"
}
```


上图是一个请求body的示例，msk和user_id分别为主私钥（urlsafe_b64encode编码）和用户id。上述请求(即私钥生成后)得到的结果如下：


```
{
 "sk":
"MIIBeQYKKoEcz1UBgi4GAQYJKoEcz1UBgi4DBgoqgRzPVQGCLgQBBEEEArxw6TXGybvmD_KG6Ba
s8UDgslLWp0U-LjZ5N-NO51VqdN-
5vU_2DeyZuO8uCfDvR49KMjfM01l1lIO2007YeQSBgQQ7KqYGzK49qn9nM_lA_mt1OQICkpjJ2FP26
5H6MeQoi1OGE2nh2EFyirVPmx0qz1jt-WAVReSQIW6dHcU5_n-FrA3ZB_KmiDMMHift1-
3YDukyVy9qePg-jiPW3qgRlSMEWFNI7wAEu_-OkbmcQc-
g1o3E74WOCRota1bhjFE3cwQHU2VydmVyMQRBBGugoLGN5zHz3E3ji-at-
qMJEd0QsSurh_jKZd96Q0PxYfkFC6ocQ7_m_7Or3YEptq11O6LM-
kg4efLzxpRLSzsEQQRGbGz7Wh7QZ0CrFYEYp-bmUk3c60NDry-UXsswVbxC1pryQSYPBQu-
YuyK845Zp5tOAAqt1HtxXXv3-LnJWvXn"
}
```


域生成 /gen-domain/request


```
{
 "user_id": "Server1"
}
```


上图是一个请求body的示例，user_id为用户id。上述请求(即域生成后)得到的结果如下：


```
{
 "msk":
"MIIBDAYKKoEcz1UBgi4GAQYJKoEcz1UBgi4DBgoqgRzPVQGCLgQBBEEEAcg7B5MINNgaSzex883n
Nq4DIEHEGTWsaAyACE7iIEafQuiygzGpNcN_pWRnVPBiPHuYbeS8S-
3YVJcm_6QDngSBgQRSbSXNosAM1-OqWdDyb05ngCZ7Mz65aC5MOl4w_sEWtzgWDm-
WJrQI6IfKScHYkHu4GTv7c68DRPRB9poe5tpIV1qGfv2zoqG1QztPEswodGZv74kRD3Gx0gcP79zWx
NJXN6PiPdxs3HFALwr0bVFkIpVIxIrhSWQWh4cidUz5YQIgVMJ1-
EQ0fKrR46p2I_VUBuJuzHSj_t1L2T6qZU76xt0=",
 "mpk":
"MIHqBgoqgRzPVQGCLgYBBgkqgRzPVQGCLgMGCiqBHM9VAYIuBAEEQQQByDsHkwg02BpLN7Hzz
ec2rgMgQcQZNaxoDIAITuIgRp9C6LKDMak1w3-
lZGdU8GI8e5ht5LxL7dhUlyb_pAOeBIGBBFJtJc2iwAzX46pZ0PJvTmeAJnszPrloLkw6XjD-
wRa3OBYOb5YmtAjoh8pJwdiQe7gZO_tzrwNE9EH2mh7m2khXWoZ-
_bOiobVDO08SzCh0Zm_viREPcbHSBw_v3NbE0lc3o-
```

I93GzccUAvCvRtUWQilUjEiuFJZBaHhyJ1TPlh",
"sk":
"MIIBeQYKKoEcz1UBgi4GAQYJKoEcz1UBgi4DBgoqgRzPVQGCLgQBBEEEAcg7B5MINNgaSzex883n
Nq4DIEHEGTWsaAyACE7iIEafQuiygzGpNcN_pWRnVPBiPHuYbeS8S-
3YVJcm_6QDngSBgQRSbSXNosAM1-OqWdDyb05ngCZ7Mz65aC5MOl4w_sEWtzgWDm-
WJrQI6IfKScHYkHu4GTv7c68DRPRB9poe5tpIV1qGfv2zoqG1QztPEswodGZv74kRD3Gx0gcP79zWx
NJXN6PiPdxs3HFALwr0bVFkIpVIxIrhSWQWh4cidUz5YQQHU2VydmVyMQRBBGJ4jQh-R4-
KLmTwFxOz4fC1S3zShdHk8EtbzTBbNkK6UOcBNFCSfRPHPypgn2v-
4_L5VPNxmuJdmk7TDAs2Gg8EQQRZgYnlIDxU1lnKwZodcy1x6Db8OGpOMFPRxkPp_HKXjjGaaA9
WXgxVCKmaqRKKztuBA2lkgoWlVcFIiBBr9rqd"
}