Retrieving endorsement keys

You can retrieve the public portion of the endorsement key (EKPub) from a Shielded VM
(https://cloud.google.com/security/shielded-cloud/shielded-vm) instance, for both the encryption key
and the signing key. You can use the encryption key to encrypt data so that only the vTPM can
read it, or the signing key to verify signatures that the vTPM makes. You can also use the key
to ascertain the identity of a VM instance before sending sensitive information to it.

You must have the `getShieldedInstanceIdentity` permission to retrieve endorsement keys.

Retrieving endorsement keys using the `gcloud` command-line tool

Use the `gcloud compute instances get-shielded-identity` command to retrieve the public
portion of the endorsement key from a Shielded VM instance.

```
gcloud compute instances get-shielded-identity [INSTANCE_NAME]
```

The results returned look similar to the following:

```
encryptionKey:
    -----BEGIN PUBLIC KEY-----
    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4ucWqhLjIkcEJyqc8KJM
    12345678abcdefghijklmnopqrstuvwxyz12345678abcdefghijklmnopqrstu
    oBSrm0swIu3x4LWR/Ebl5KA0EKe9YFGaS9Pguun1m6X8Ld2zAqmoIwnxDiOqxQEU
    mx2wxkjf0bbjxG5ZI1i3t/c/QzeaE2WWTlKdgnUDyxSloDBq63yywtoIrp1nbDLj
    X8qdBymixu8jXXp1iGwmEUltnEnx779JKTpKgKTEednri+NcfRmXHrnPCxfiPudQ
    4wIDAQAB
    -----END PUBLIC KEY-----
kind: compute#shieldedVmIdentity
signingKey:
    -----BEGIN PUBLIC KEY-----
    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzQvcD+2LAnsXAgdsVYAc
    12345678abcdefghijklmnopqrstuvwxyz12345678abcdefghijklmnopqrstu
    V/7WHasUuGlkbqiDOuDWgb15FAn35PU64HGey67McZTUT9EvrkT/ryXi4kZgBtoM
    lQIDAQAB
    -----END PUBLIC KEY-----
```

Retrieving endorsement keys using the Compute Engine API

You can use the Compute Engine API to view endorsement key information. For more information on how to use the API, see the How-to guides (https://cloud.google.com/compute/docs/api/how-tos/how-tos).

```
GET /compute/v1/projects/[PROJECT_ID]/zones/[ZONE]/instances/[INSTANCE_NAME]/getShie

{
  "signing": {
    "ekCert": [PEM-formatted certificate data]
    "ekPub": [PEM-formatted key]
  }
  "encryption": {
    "ekCert": [PEM-formatted certificate data]
    "ekPub": [PEM-formatted key]
  }
}
```