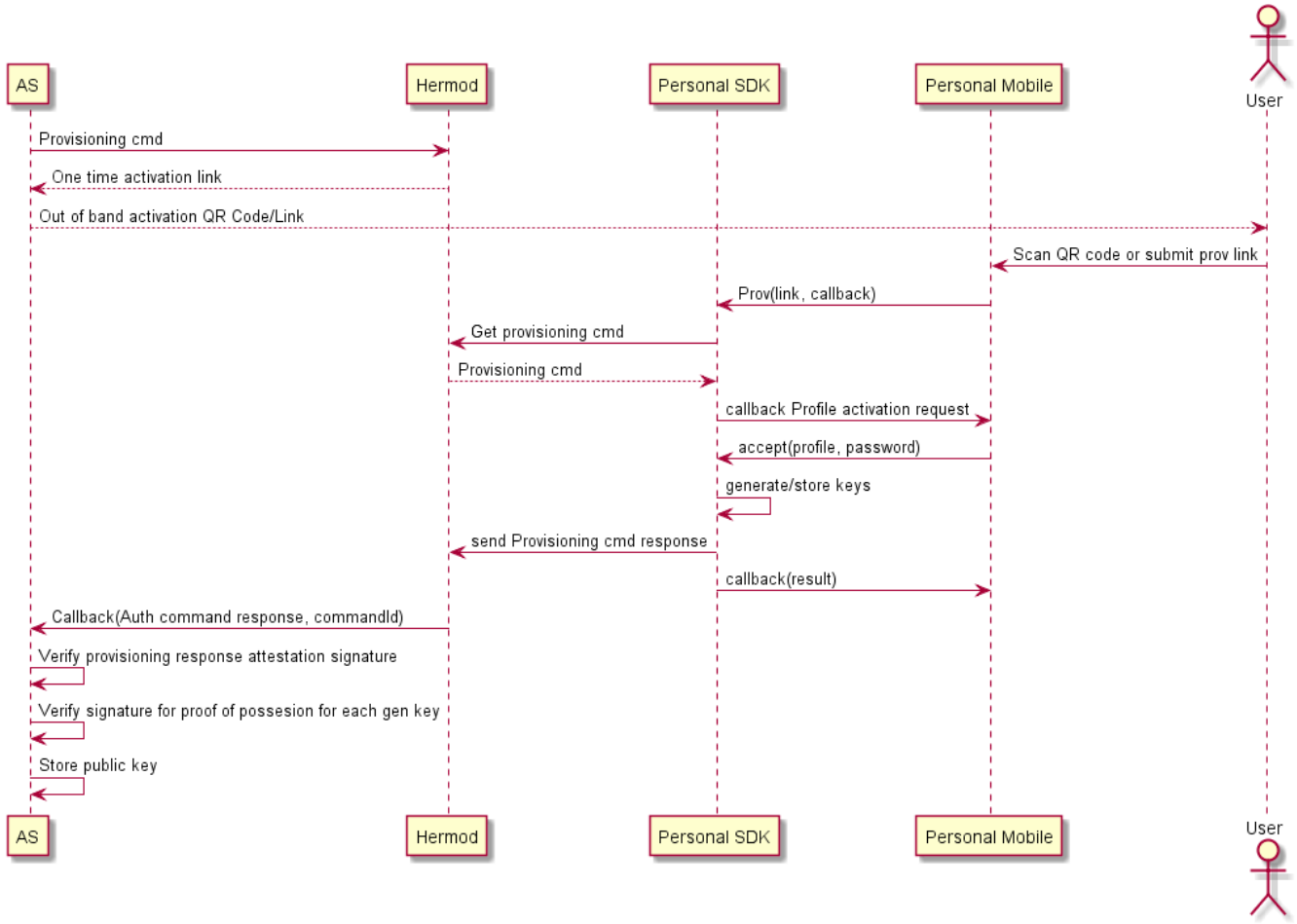
# Example: Personal Mobile provisioning




Expand/Collapse All

## Related information

- Install Hermod

## Prerequisites

Prerequisites

- Installed Hermod, see here.

## Step-by-step instruction

Create provisioning request in Hermod

1. Send provisioning request, see code example.

**Example: Provisioning command**

```
POST /rest/command/provision
{
   "commandHeader":{
      "lifespan":1500,
      "timeout":1500
   },
   "provCommand":{
      "nonce":"123456789",
      "userid":"john.doe@nexusgroup.com",
      "responsesignaturekey":"ATTESTATION",
      "responseformat":"jws",
      "profile":{
         "servername":"nexus-hermod1",
         "name":"TestProfile",
         "keygenrequests":[
            {
               "keyid":"signer",
               "usage":"SIG",
               "keytypeprios":[
                  {
                     "keytype":"RSA",
                     "keylength":"2048",
                     "responsemechanism":"RS256"
                  }
               ],
               "storageprios":[
                  "APP"
               ],
               "keystate":"ACTIVE",

"certreq":"MIIDAzCCAesCAQIwgb0xCzAJBgNVBAYTAlNFMRAwDgYD
VQQIDAdVcHBsYW5kMRAwDgYDVQQHDAdVcHBzYWxhMRcwFQYDVQQKDA5
VcHBzYWxhIEtvbW11bjEUMBIGA1UECwwLRnlyaXNza29sYW4xFjAUBg
NVBAMMDUFuZGVycyBSb3PDqW4xLTArBgkqhkiG9w0BCQEWHmNsYWVzL
nJvc2VuYmVyZ0BuZXh1c2dyb3VwLmNvbTEUMBIGCysGAQQBgTwHAQEC
DANBUEEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDV8SX
7mnFExGdNwJe+1VqzQHhN4+2TdtW98uOE7s7jNRAZZGNM7J9hvkyvlj
bHD71/iI6tTvvDAlEU45pe4qYlpgG5WLntYzP1TT+NZR3wvbWZQyoZr
IPqguU/EB77tB38E/quY3BmMZSQeMPidqvAapTotTnSeE/981kj8IyZ
qm2v9WHjJsCj5TexrHnqcswFOVrtI/LhTfWKUn1o3sG890wmQSdjT53
vtiIn4bCgck5WD/4YHozr8TBOKXwXhUwJhOj/uLxLkdDB1+0VX7q8i+
IUzSRKD4WMTG93F0jDzR6jYPWJJfuEPTbDTvTeKfL97CGXSZt772HyR
bqqhUATAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEANmxKbGq+/yzZ
h8doUSnjxaVEygL2gamnCLQ3+hQttxI+zn9Z6smvlD2nJmuGErVgB77
oTKTbLXMDVlKD1QoHmTucoMYpALNd+roVHLAL7/bppO6MWgmQmKyTna
R95466y1lKZRqc0LKgv1xSCP+cJXelOaE2Kxqbj94YkxP5auPcc1GrB
VFjY/CZYjqD2tAozWb8R4l04yKjYo4hGggcAzjxObbVKBLZ5GCV1BV3
84ojHizVdP8SHT0YzULj5ZlWwPVsVxUFGkJGQlF9ze5hl0XMZsKSpwv
ShySDRMZOM+piqAQQh7ktz0daDvEL5HFLpnJQSmY+3YRfoL5hG8Etqw
=="
            }
         ]
      }
   }
}
```

**Example: Provisioning response**

```
Response 200 OK
{
    "commandId": "1011",
    "destinations": [
        {
            "to": "@tmp",
            "bid":
"482ae2ba-3847-4fc8-bb98-73a3f2f809ca",
            "uri":
"com.nexusgroup.plugout:///?url=https%3a%2f%2fnexus-cod
1.test.nexusgroup.com%3A20400%2fhermod%2Frest%2Fms%2F48
2ae2ba-3847-4fc8-bb98-73a3f2f809ca&token=c3c5df6d-59a1-
450f-b2e5-066363959c71",
            "mid":
"66b2fec0-54ba-472b-817a-ef464da5e8fa",
            "location":
"https://nexus-cod1.test.nexusgroup.com:20400/hermod/re
st/ms/482ae2ba-3847-4fc8-bb98-73a3f2f809ca/66b2fec0-54b
a-472b-817a-ef464da5e8fa"
        }
    ],
    "commandType": "PROV",
    "state": "IN_PROGRESS",
    "fqdn": "nexus-cod1.test.nexusgroup.com"
}
```

The user can then enter the URL or scan the QR code (the URL is rendered as a QR code according to standard) in the mobile app. The profile info will be displayed and the user can accept to activate the profile:

### Validate provisioning response

When the user has accepted to activate the profile, then a response will be sent to the Application Server in a callback.

1. Validate the response and check the following:
    1. That the signature of the complete payload and that a trusted attestation key is used.
    2. Proof of possession, by checking the signature of each generated key.
2. Store the public key to be able to verify future authentications.

**Example: Provision response callback**

```
POST
https://my-registered-callbackserver/rest/callback/provision
{
  "responseHeader" : {
    "inReplyTo" :
"https://nexus-cod1.test.nexusgroup.com:20400/hermod/rest/ms/2
1b279cc-3f82-48e2-b200-fd9bbc5dfb4a/08aeef86-b789-4bf3-88fa-ab
0c96824a6c",
    "status" : 200
```

```
  },
  "provResponse" : {
    "code" : 0,
    "result" : {
      "contenttype" : "jws",
      "data" :
"eyJraWQiOiJBVFRFU1RBVElPTiIsIm5vbmNlIjoiMTIzNDU2Nzg5IiwiYWxnI
joiUlMyNTYiLCJqd2siOnsidXNlIjoic2lnIiwia2lkIjoiYXR0ZXN0YXRpb24
iLCJuIjoiQU9JN1UtcHJrSThIUktvYUpLRDNRdFRTTm1zbTFfcF91aVhiMVFMe
TlnTVN1R2paOEhOcnBWVDRrY1IxVXVkdzNwT0tuZG43TkJlYzViOTJBZ001V3Z
TUHhHRE9ZZmdLM3hLUlVheXl3RkQzSjZSVjF2VVh0alc0d0xtdnpHYnRZd0hIU
HlycWhUNzNLckhobkxoMmRwSjNNTzVTQ0FXdU5iaVE2RVZsbkxkU3hZcGhGeEd
2bmdxY0pHNl9ESmhrb2xyOWJfTExUdDE0OXRHa3lZcUw3YWlPNk9qVnRKUlFkV
WxIYUpFVmV3Z29tR0JuWURXRFV2WGxJM3FDakliWkFrc283NzAxMnFXbnRpX3R
qTlNIYmZFUXItZF9KRzR3bnFKalVvaHdFM1ZyN3VJR0JmS1FaMTZROUFlb0dzY
khscDRIZkk5cS1pMmladG5OSFFuU2ZOVSIsImUiOiJBUUFCIiwia3R5IjoiUlN
BIiwiYWxnIjoiUlMyNTYifX0=.

eyJwcm9maWxlIjp7ImlkIjoiNGI0NzBlYzgtMDAzMy00ZmFlLWIzZDgtNWUyND
hkOWU3YmMzIiwidXNlcmlkIjoiam9obi5kb2VAbmV4dXNncm91cC5jb20iLCJz
aWduZWRrZXlzIjpbImV5SmhiR2NpT2lKU1V6STFOaUlzSW10cFpDSTZJbk5wWj
I1bGNpSXNJbTV2Ym1ObElqb2lNVEl6TkRVMk56ZzVJbjA9LmV5SjFjMlVpT2lK
VFNVY2lMQ0poYkdjaU9pSlNVekkxTmlJc0ltdDBlU0k2SWxKVFFTSXNJbVVpT2
lKQlVVRkNJaXdpYmlJNkluaHhXWE5pWTNWSFNURTVUbFZzVjJveFVIRXpXRGN6
UWxOWmJrbzRla1JtVUY4M09YWlZjRkJ4U25WdGFrVXpOV3BxZWtNNVIycG1ZWF
JGYTFCR056UlZWVk0wVldGcVpuSmhOSEp0VGtscmJYVnRkM2QyTFdKdVRIVjJk
MDlYZGxaRGJuUm9aVlUwV2xoU2NrVnhNUzEzY1hkSVZtNUVaM2R1UWtaVlMwaD
FPVTlIYVU1bk5UVkVlVkpqWlZsaFJqbDFUME16UlVKSGRrNW1iMnBtZFVVNVRu
UkVRalJRTURaWGNVbGhSMGRVWTNGWFVqTlROVkEwVFRCalQzVm5ZVmxSWVZobW
JXeFJUWFEyU0dSblZXSm5UVE5NYmtOT1YzTkdhVkZRUkMxaFRrVXpXSEJJYmtk
MlkxOUJXbmRaT1ROelMzcE9TVXBKVGxwdVQzQklTbTFDVFZSSlpIbHpSM05EZE
hacGFWcGhaRW8xYldZNGVYSkdVa3hpZG1wZlR6UmxWVzlwWWsxQlRtbGFUVEJM
Y0RKcVMyUjRSRk5HUmtKYVIxOVlUVzFLVEZJMFEwRklVR3hsWmxJNFUyZE9hel
pKV1hkSWR5SXNJbXRwWkNJNkluTnBaMjVsY2lJc0ltNGpiR1Z1SWpvaU1qQTBP
Q0lzSW10bGVWOXpkR0YwWlNJNklrRkRWRWxXUlNKOS5vU25HcE0xWkN3VjRMN3
VtMUc1TFVwc3h5cXVRcG9TMDhINEstTUJNZVBuVk10VzhoRHpzSVVLRTc2WW1Y
eldGVkFoNy05RC1EaE91V0JicHRXV3ZMa2lMcURWRk1IXzlUVXA3WGh2MFZNaW
pNQUpfcTN2M0UyamJJMXh0MUZsQUZjejBULS1LS081SS03SXNrMGUxejI1X0Q4
R0FaajJqNFhZeTFxZjZ1UmFwSFNweG1wdlh1TE9fbXg1ZUdiR1p1cEVkamlaeU
NyWDd1dUJ2TGNnTVJVYnpMNXBHaEIwd2RrSGJHNXlraEJlekVGLXFBNmlvSElC
NGRSYmhxcWsxZl9TcjFzZE1SRHUtM2tnWnZXMlljUExBNmljTEE5VzZHVXBxQm
UydUs5NlZFemt6TUh5N0Y5aUU0ZUVEd3RRb0FsaWxId3NESFFnbHZub2VQemtn
UnciXSwibmFtZSI6IlRlc3RQcm9maWxlIiwic2VydmVybmFtZSI6Im5leHVzLW
hlcm1vZDEiLCJib3h1cmwiOiJodHRwczpcL1wvbmV4dXMtY29kMS50ZXN0Lm5l
eHVzZ3JvdXAuY29tOjIwNDAwXC9oZXJtb2RcL3Jlc3RcL21zXC8zOGIwMGFmOC
03YjYwLTQ0YzEtOGFmMS05ZDM3NDFjZjBhMzEifSwiZGV2aWNlaW5mbyI6eyJv
cGVyYXRpbmdzeXN0ZW0iOiJpT1MgKDEwLjMuMikiLCJtb2RlbCI6ImlQaG9uZS
IsImFwbmRldmljZXRva2VuIjoiNjU1MmNkZmEzN2M4NTgyODYwNjRmOTk1ZjFh
YThiYWY3OTc4MjhlMzIzOGZkN2Y4NDFmYmZhMzRiYWViNjlkNCIsIm5hbWUiOi
JBbmRlcnPigJlzIGlQaG9uZSJ9fQ==

.Sx54ArHOVWRPVcvozInXbRobI5WbVqCuH9gp7OnE0UPq1IcMHLr47Cf5mVhAO
w7VS_93cCoZwRWVo3y6z1iFv40RyGuu7bqiOKtgZ4tWy601ITSS91Ur8GGux-w
Ug6eYM8DmhL_yPoVQqZvlSadrAZEOKP1pIYBu9snONK2Qmg4d30qWDPl4LImbJ
stFv3kIfuD1_ul2i1QLOH51A5-8HPcnFVNwglYFKtPQoTjUBS6_ioP3KdnqeI6
eGDVcqsRxkdV9Uum5JXkF2Amnq72fbxqtYeic-_DCIn9m6h8g31ovoEPzftv8M
pkvKSvxly4QSxVlkztRN7jK65Cu7KW2PA"
    }
  },
  "commandId" : "1101",
  "destinations" : [ {
```

```
    "to" : "@tmp",
    "bid" : "21b279cc-3f82-48e2-b200-fd9bbc5dfb4a",
    "uri" :
"com.nexusgroup.plugout:///?url=https%3a%2f%2fnexus-cod1.test.
nexusgroup.com%3A20400%2fhermod%2Frest%2Fms%2F21b279cc-3f82-48
e2-b200-fd9bbc5dfb4a&token=a8b6eeb1-8218-497a-b8f8-14c81435060
e",
    "mid" : "08aeef86-b789-4bf3-88fa-ab0c96824a6c",
    "location" :
"https://nexus-cod1.test.nexusgroup.com:20400/hermod/rest/ms/2
1b279cc-3f82-48e2-b200-fd9bbc5dfb4a/08aeef86-b789-4bf3-88fa-ab
0c96824a6c"
  } ],
  "commandType" : "PROV",
```

```
  "state" : "COMPLETED",
  "fqdn" : "nexus-cod1.test.nexusgroup.com"
}
```

Where the generated profile and its keys are included in the data field and where data is a compact *JSON Web Signature (JWS)* base64url(header).base64url(payload).base64url(signature).

**Example: header, payload, and signature**

```
header
{
    "kid":"ATTESTATION",
    "nonce":"123456789",
    "alg":"RS256","
    jwk":{
        "use":"sig",
        "kid":"attestation",

"n":"AOI7U-prkI8HRKoaJKD3QtTSNmsm1_p_uiXb1QLy9gMSuGjZ8HNrpVT4k
cR1Uudw3pOKndn7NBec5b92AgM5WvSPxGDOYfgK3xKRUayywFD3J6RV1vUXtjW
4wLmvzGbtYwHHPyrqhT73KrHhnLh2dpJ3MO5SCAWuNbiQ6EVlnLdSxYphFxGvn
gqcJG6_DJhkolr9b_LLTt149tGkyYqL7aiO6OjVtJRQdUlHaJEVewgomGBnYDW
DUvXlI3qCjIbZAkso77012qWnti_tjNSHbfEQr-d_JG4wnqJjUohwE3Vr7uIGB
fKQZ16Q9AeoGsbHlp4HfI9q-i2iZtnNHQnSfNU",
        "e":"AQAB",
        "kty":"RSA",
        "alg":"RS256"
    }
}
payload
{
    "profile":{
        "id":"4b470ec8-0033-4fae-b3d8-5e248d9e7bc3",
        "userid":"john.doe@nexusgroup.com",

"signedkeys":["eyJhbGciOiJSUzI1NiIsImtpZCI6InNpZ25lciIsIm5vbmN
lIjoiMTIzNDU2Nzg5In0=.eyJ1c2UiOiJTSUciLCJhbGciOiJSUzI1NiIsImt0
eSI6IlJTQSIsImUiOiJBUUFCIiwibiI6InhxWXNiY3VHSTE5TlVsV2oxUHEzWD
czQlNZbko4ekRmUF83OXZVcFBxSnVtakUzNWpqekM5R2pmYXRFa1BGNzRVVVM0
VWFqZnJhNHJtTklrbXVtd3d2LWJuTHV2d09XdlZDbnRoZVU0WlhSckVxMS13cX
dIVm5EZ3duQkZVS0h1OU9HaU5nNTVEeVJjZVlhRjl1T0MzRUJHdk5mb2pmdUU5
TnREQjRQMDZXcUlhR0dUY3FXUjNTNnA0TTBjT3VnYVlRYVhmbWxRTXQ2SGRnVW
JnTTNMbkNOV3NGaVFQRC1hTkUzWHBIbkd2Y19BWndZOTNzS3pOSUpJTlpuT3BI
Sm1CTVRJZHlzR3NDdHZpaVphZEo1bWY4eXJGUkxidmpfTzRlVW9pYk1BTmlaTT
BLcDJqS2R4RFNGRkJaR19YTW1KTFI0Q0FIUGxlZlI4U2dOazZJWXdIdyIsImtp
ZCI6InNpZ25lciIsIm4jbGVuIjoiMjA0OCIsImtleV9zdGF0ZSI6IkFDVElWRS
J9.oSnGpM1ZCwV4L7um1G5LUpsxyquQpoS08H4K-MBMePnVMtW8hDzsIUKE76Y
mXzWFVAh7-9D-DhOuWBbptWWvLkiLqDVFMH_9TUp7Xhv0VMijMAJ_q3v3E2jbI
1xt1FlAFIz0T--KKO5I-7Isk0e1z25_D8GAZj2j4XYy1qf6uRapHSpxmpvXuLO
_mx5eGbGZupEdjiZyCrX7uuBvLcgMRUbzL5pGhB0wdkHbG5ykhBezEF-qA6ioH
IB4dRbhqqk1f_Sr1sdMRDu-3kgZvW2YcPLA6icLA9W6GUpqBe2uK96VEzkzMHy
7F9iE4eEDwtQoAlilHwsDHQglvnoePzkgRw"],
        "name":"TestProfile",
        "servername":"nexus-hermod1",

"boxurl":"https:\/\/nexus-cod1.test.nexusgroup.com:20400\/herm
od\/rest\/ms\/38b00af8-7b60-44c1-8af1-9d3741cf0a31"
```

```
        },
        "deviceinfo":{
            "operatingsystem":"iOS (10.3.2)",
            "model":"iPhone",

"apndevicetoken":"6552cdfa37c858286064f995f1aa8baf797828e3238f
d7f841fbfa34baeb69d4",
            "name":"Anders’s iPhone"
        }
}
signature

Sx54ArHOVWRPVcvozInXbRobI5WbVqCuH9gp7OnE0UPq1IcMHLr47Cf5mVhAOw
7VS_93cCoZwRWVo3y6z1iFv40RyGuu7bqiOKtgZ4tWy601ITSS91Ur8GGux-wU
g6eYM8DmhL_yPoVQqZvlSadrAZEOKP1pIYBu9snONK2Qmg4d30qWDPl4LImbJs
```

```
tFv3kIfuD1_ul2i1QLOH51A5-8HPcnFVNwglYFKtPQoTjUBS6_ioP3KdnqeI6e
GDVcqsRxkdV9Uum5JXkF2Amnq72fbxqtYeic-_DCIn9m6h8g31ovoEPzftv8Mp
kvKSvxly4QSxVlkztRN7jK65Cu7KW2PA==
```

The keys are included in the signed keys field. The *JSON Web Key (JWK)* is signed by itself for proof of possession.

**Example: Decoded signed_keys element**

```
Header
{
    "alg":"RS256",
    "kid":"signer",
    "nonce":"123456789"
}
Payload (JWK)
{
    "use":"SIG",
    "alg":"RS256",
    "kty":"RSA",
    "e":"AQAB",

"n":"xqYsbcuGI19NUlWj1Pq3X73BSYnJ8zDfP_79vUpPqJumjE35jjzC9Gjfa
tEkPF74UUS4Uajfra4rmNIkmumwwv-bnLuvwOWvVCntheU4ZXRrEq1-wqwHVnD
gwnBFUKHu9OGiNg55DyRceYaF9uOC3EBGvNfojfuE9NtDB4P06WqIaGGTcqWR3
S6p4M0cOugaYQaXfmlQMt6HdgUbgM3LnCNWsFiQPD-aNE3XpHnGvc_AZwY93sK
zNIJINZnOpHJmBMTIdysGsCtviiZadJ5mf8yrFRLbvj_O4eUoibMANiZM0Kp2j
KdxDSFFBZG_XMmJLR4CAHPlefR8SgNk6IYwHw",
    "kid":"signer",
    "n#len":"2048",
    "key_state":"ACTIVE"
}
.
oSnGpM1ZCwV4L7um1G5LUpsxyquQpoS08H4K-MBMePnVMtW8hDzsIUKE76YmXz
WFVAh7-9D-DhOuWBbptWWvLkiLqDVFMH_9TUp7Xhv0VMijMAJ_q3v3E2jbI1xt
1FlAFIz0T--KKO5I-7Isk0e1z25_D8GAZj2j4XYy1qf6uRapHSpxmpvXuLO_mx
5eGbGZupEdjiZyCrX7uuBvLcgMRUbzL5pGhB0wdkHbG5ykhBezEF-qA6ioHIB4
dRbhqqk1f_Sr1sdMRDu-3kgZvW2YcPLA6icLA9W6GUpqBe2uK96VEzkzMHy7F9
iE4eEDwtQoAlilHwsDHQglvnoePzkgRw
```