راهنمای سرویس های پیکو

نسخه ۱,۲

تاریخچه تغییرات

تاریخ	نسخه	توضیحات
۱۳۹۶/۰۹/۰۵	۱,۰	سرویس Push و سرویس Charge
۱۳۹۶/۰۹/۰۷	۱,۱	اضافه کردن تاریخچه تغییرات
۱۳۹۶/۰۹/۰۹	۱,۲	امضای دیجیتال

فهرست مطالب

عضویت در سرویس همراه اول

در سرویس همراه اول کاربر با استفاده از رمز یک بار مصرف (OTP) تایید می کند که مایل است از سرویس توسعه دهنده استفاده نماید. در نتیجه برای عضویت یک کاربر، ابتدا یک کد فعال سازی به کاربر ارسال می شود و سپس توسعه دهنده آن کد را از کاربر دریافت و به سیستم پیکو ارسال می کند. برای ارسال کد فعالسازی توسعه دهنده سرویس Push را فراخوانی می کند. در مرحله بعد پس از اینکه کاربر در برنامه توسعه دهنده، کد فعالسازی خود را وارد نمود، باید سرویس Charge فراخوانی گردد.

سرویس Push

با فراخوانی این سرویس یک کد فعالسازی ۴ رقمی به کاربر ارسال می شود.

درخواست سرویس PUSH

آدرس سرویس برابر است با:

https://pg.appson.ir/api/otp/push

اطلاعات مربوط به Header های درخواست در جدول ۱ و Body درخواست در جدول ۲ آمده است.

نام	توضیح	مثال
Content-Type	نوع داده ای که به سرور ارسال می شود. این مقدار باید برابر با: application/json; charset=utf-8 باشد.	application/json; charset=utf-8
PRODUCT	کد محصول	PRD-Book
SIGNATURE	امضای Body درخواست HTTP	MaDpoN4ktzD9wGFBpQxn03tuqDw0j3K2jqfci3presH0iFLvLVjpn+V2GBhzVcTf2LK4nC27MRiavrFTo3LL3oeZh81blzipXY4eztTNLtmVzfKk9+YjwjcAgNGr4F7WhuSeFEI0Z3hRq9kyZbhhYQwBdhpacMrLonVTsGxadQtDwgWPdDuSK57tQ6JW4HkoRXqjVYXgdrR1Gg/ZCIXCxdbFWbcIoy1fpKn3d5FMZ6Z/ht8ooAc5dWK3lnNV5JX3erx5zUn+yoQKfzZeLsYgx3FA69yPfsow1cbpFa7WEkr9n5ESSqYLQfqEvLOBFx4erak==fCZIjOdtqst6d8Zmy1Q
RUID	کد یکتای درخواست HTTP. کلاینت باید این کد رو در هر درخواست HTTP تولید کند.	d46ca97e58ff4b09898eecefee15dd53

REQUESTDATE	تاریخ و زمان حال UTC به فرمت: yyyyMMddhhmmss	20171126120001

جدول ۱ – Header های درخواست سرویس Push

نام فیلد	توضیح	مثال
PhoneNumber	شماره همراه کاربر	09124800000
ProductItemCode	کد کالا	PRD-Book-2aad43ee-1bb1-4075-a972-acd56777d2d6
ReferenceCode	کد پیگیری از سمت توسعه دهنده	19e1e8dbd8cb4ffd8648bf42f07ac254
Date	برابر است با REQUESTDATE در Header	20171126120001
ProductCode	کد محصول	PRD-Book
RUID	برابر است با RUID در Header	d46ca97e58ff4b09898eecefee15dd53

جدول ۲– HTTP Body درخواست در سرویس Push

نمونه ای از HTTP Request کامل در زیر آمده است:

```
POST https://pg.appson.ir/api/otp/push HTTP/1.1
RUID: d46ca97e58ff4b09898eecefee15dd53
PRODUCT: PRD-Book
REQUESTDATE: 20171126120001
SIGNATURE:
MaDpoN4ktzD9wGFBpQxn03tuqDw0j3K2jqfci3presH0iFLvLVjpn+V2GBhzVcTf2LK4nC27MRiav
rFTo3LL3oeZh81blzipXY4eztTNLtmVzfKk9+YjwjcAgNGr4F7WhuSeFEI0Z3hRq9kyZbhhYQwBdh
pacMrLonVTsGxadQtDwgWPdDuSK57tQ6JW4HkoRXqjVYXgdrR1Gg/ZCIXCxdbFWbcIoy1fpKn3d5F
MZ6Z/ht8ooAc5dWK3lnNV5JX3erx5zUn+yoQKfzZeLsYgx3FA69yPfsow1cbpFa7WEkr9n5ESSqYL
QfqEvLOBFx4erakfCZljOdtqst6d8Zmy1Q==
Content-Type: application/json; charset=utf-8
Host: pg-test.appson.ir
Content-Length: 237
Expect: 100-continue
Connection: Keep-Alive

{"PhoneNumber":"09124800000","ProductItemCode":"PRD-Book-2aad43ee-1bb1-4075-
a972-
acd56777d2d6","ReferenceCode":"19e1e8dbd8cb4ffd8648bf42f07ac254","Date":"2017
1126120001","ProductCode":"PRD-
Book","RUID":"d46ca97e58ff4b09898eecefee15dd53"}
```

دامپ ۱ – درخواست سرویس Push

پاسخ سرویس Push

مقدار HTTP Body پاسخ در جدول ۳ آمده است.

نام	توضیح	مثال
IsSuccess	موفق یا نا موفق بودن یک درخواست را نشان می دهد.	true
Response	در صورتی که سرویس موفق باشد، این فیلد پر می شود. (مقدار شی Response در ادامه توضیح داده می شود.)	{"ReferenceCode":"19e1e8dbd8cb4ffd8648bf42f07ac254","TransactionId":"d7f98049c4a34ab3be0b233786817c96"}
Error	در صورتی که سرویس با خطا مواجه گردد این فیلد پر می شود.	{"Code":"PG-000955","Message":"در فروخوانی پیروکسی خطا رخ داده است","Description":"در فروخوانی پیروکسی خطا رخ داده است","Params":[]}

جدول ۳ – HTTP Body پاسخ سرویس Push

نمونه ای از HTTP Response کامل در دامپ ۲ آمده است.

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: application/json; charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
PAYMENT-VERSION: 1.0.0
X-Powered-By: ASP.NET
Date: Sun, 26 Nov 2017 12:00:10 GMT
Content-Length: 146

{"IsSuccess":true,"Response":{"ReferenceCode":"19e1e8dbd8cb4ffd8648bf42f07ac254","TransactionId":"d7f98049c4a34ab3be0b233786817c96"},"Error":null}
```

دامپ ۲- پاسخ سرویس Push

مقدار شی Response نیز در جدول4 آمده است.

نام	توضیح	مثال
ReferenceCode	کد پیگیری از سمت توسعه دهنده	19e1e8dbd8cb4ffd8648bf42f07ac254
TransactionId	کدی است که در فراخوانی سرویس بعدی (یعنی سرویس Charge) به همراه کد فعالسازی کاربر ارسال می شود.	d7f98049c4a34ab3be0b233786817c96

جدول4 – فیلد های شی Response در پاسخ سرویس Push

پیاده سازی

نمونه پیاده سازی سرویس Push با زبان C# در قطعه کد ۱ آمده است.

```
var phone = "09124800000";
var productItemCode = "PRD-Book-2aad43ee-1bb1-4075-a972-acd56777d2d6";
var url = "https://pg.appson.ir/api/otp/push";
var dto = new PiqoDto.PushRequestDto
{
    ReferenceCode = Guid.NewGuid().ToString("N"),
    Date = DateTime.UtcNow.ToString("yyyyMMddHHmmss"),
    PhoneNumber = phone,
    ProductCode = "PRD-Book",
    ProductItemCode = productItemCode,
    RUID = Guid.NewGuid().ToString("N")
};

var jsonSerializer = new JsonSerializer<PiqoDto.PushRequestDto>();
var key =

"<RSAKeyValue><Modulus>jY9y20Sz1hiPG9B0Xqo4vDDsgUOjLhYeNlEpKRt25goNDxb/Imjv92
2W2OiZiqd0kRNFJB8g6RiUn2SYs+AtT2U0m7RG262dlJlXkcLlhzO2upZDMpgREQYnzapQdNSxFHN
IE1rDa1flC2LtgRI3SaKVGSsxM7rssHcusN7rye8bkr8CnXFU81PIc8Ahh+dfsNg5TiiKSjTfmdnv
qMnHXLnVXnFCPFp7PafevPextp8cTtBHv7quimpzOUUopW3EWfqJt2R1WeD0keXXQqbZdFb6GXEXd
qw2bRnydVqojCVJsYu+S1qfH971ZAxG5ihizt8pNroBAyAkHKvS+IHd1Q==</Modulus><Exponen
t>AQAB</Exponent><P>9G/1S/1YGRQLF+qv9NSZPhBLUxfZf2vlph9HrNwUikv2DKe0g8+OsskEC
eqqMLMIumBUOcaHtTldEgHZ09NhsHUx/pjkaKuDfS1hkkz39uULIitjxYPVINKWt2YVlM5MaBPe1d
UK8F4gZbyVFSy1A3mH8c/XDVWNvJsaelsL5e0=</P><Q>lEGwl/I0K5PQZeAckHSOlCg+rPMSRx6Z
m+NWipy8Chmgc2YESkRLDNXjTNyX2FBWZUJ6WZ3SiriDYkLKkGmoHX2uQ+WMvwBdabqUy82WFhzEN
pZ27uoLd+Jpb6Lt2izRCMW5OMeEVbo6zuDPDqrhhuNOLoM9WOK9j6jvsue42ok=</Q><DP>3BXyRv
lU2T+yvVYSF99UGw2QxMA0lQYRQAHqBzohRGQgpkRZxFSdp1xWxpcDpdWNhkI1k8+tYP7FTfFcr90
jmD3tRc9j2NqVCaBSueeTXDneTGXE75JD08nI6liAFfup0AwUF3Q65THa+b9SfD5EvVwviwoYF2lw
tODydjiD/gE=</DP><DQ>duAZPiyp4ks6bYV+weGDtY5zeu/INxh1KMbnzGsSZ7LWsdEaHYaW+urB
wA6c/oikTbs5KYRfnnWGe5J8o8DkWQk+Yxi7eydKv40o5CWrc32LYw3QvY8StQTpb+cferI2xibsd
necR7T0lI8z11nzTdoTBT6cQRpFztwxnq0ozqk=</DQ><InverseQ>IE/cYdvjAdHxvTwyFFyEj9e
r61AC3K0kpAEAbckHG0JZ5ZY16ptYAcr1auEv2F461360r3R+Cfgld1NSGtWTQc6KomEDXIiHHwwL
ntL7Zmyk2Bzp67Ax/WvIkatCp4c9POBeX2QhbNCO9Fs2tkxVmkfwCYn9sfcIKcDyA/XQZEs=</Inv
erseQ><D>DXK9RJtoQkSfA9Nv2rZtIWO8dCNK00wCnsJjGKalSwFVcEONBWXWtjjRBdZDD+sMpeOg
w+e5JqvRIrtZzmzToSFKOCiOOrxppf5TVWOgjpGZIGy6AYp0xJtDGMS/U/oIwJqbFEuhGQeGmOhTC
9oBKpupcnSp/fIaHkGUS/VBjTNmqr/KLFcAj0rkPNy30TY9aFp2Ei8poYLNb9qaiuQvtU7EAiEj19
0y9cfwoqUZW74OcQDQc4Xbu94QPIkxX4FvnSff8Ecc8BTNN4GqjuacNZ0w9LMywVkmqKC6tJYsv9x
w+0MJQ5/J227lUloSyoWMfHjjQU0wQWirAMeKiJNowQ==</D></RSAKeyValue>";

var text = jsonSerializer.SerializeToString(dto);

var sign = Signature.Sign(key, text);

var result =
    ServiceUtility.Post<object>(
        url,
        dto,
        new List<KeyValuePair<string, string>>
        {
new KeyValuePair<string, string>("RUID", dto.RUID),
new KeyValuePair<string, string>("PRODUCT", dto.ProductCode),
new KeyValuePair<string, string>("REQUESTDATE", dto.Date),
new KeyValuePair<string, string>("SIGNATURE", sign),
        });
```

سرویس Charge

با فراخوانی این سرویس اگر کالا اشتراکی باشد، کاربر عضو سرویس می شود و برای کالاهای مصرفی، کاربر شارژ می گردد.

درخواست سرویس Charge

آدرس سرویس برابر است با:

https://pg.appson.ir/api/otp/charge

Header های درخواست در جدول ۵ آمده است.

نام	توضیح	مثال
Content-Type	نوع داده ای که به سرور ارسال می شود. این مقدار باید برابر با: application/json; charset=utf-8 باشد.	application/json; charset=utf-8
PRODUCT	کد محصول	PRD-Book
SIGNATURE	امضای Body درخواست HTTP	iy2CdtzHcjJ2NxinAxIx4NqwfcGVBiOu4pYAfu5Pwl8wCVUbO2KcbDmxaGRR6CyCcMqLCzSl7Hw0T9OE/nvpbnSBL11C0BCXajTNKyZLuxu4ujHJ1Q/iOrvdux8G+VYZtgKQ3bxPSziM3fM3zzxlAuhyzEmq5eSIyiJTqb2Q03p4+gB2UcVIN0xKUSh40NZLYSpmFPJMhAnrwZU0oIObNIECgPM6tyz+HYUKJQfQB9qJM4msXo4AJjpdO61P64ElMwm922ar1ckaFmEh4Iueyfd4AGS98EtKrASjynCTs/m+pPBzOVmx1vjIhVlkIDoLzx==4vdnSlj8qd8P4HpPol8w
RUID	کد یکتای درخواست HTTP	4d8cbddf9dac4196aa277f365b38a879
REQUESTDATE	تاریخ و زمان حال UTC به فرمت: yyyyMMddhhmmss	20171126134319

جدول ۵ – Header های درخواست سرویس Charge

و Body درخواست نیز در جدول ۶ آمده است.

نام فیلد	توضیح	مثال
Pin	کد فعالسازی که توسط کاربر وارد می شود.	9931
TransactionId	همان مقداری است که در سرویس Push برگردانده شد.	d7f98049c4a34ab3be0b233786817c96
ReferenceCode	کد پیگیری از سمت توسعه دهنده	284bec959ca74c70bf956bb6cae909f4
Date	برابر است با REQUESTDATE در Header	20171126134319
ProductCode	کد محصول	PRD-Book
RUID	برابر است با RUID در Header	4d8cbddf9dac4196aa277f365b38a879

جدول ۶- Body درخواست در سرویس Charge

نمونه ای از HTTP Request کامل در دامپ ۳ آمده است.

```
POST https://pg.appson.ir/api/otp/charge HTTP/1.1
RUID: 4d8cbddf9dac4196aa277f365b38a879
PRODUCT: PRD-Book
REQUESTDATE: 20171126134319
SIGNATURE:
iy2CdtzHcjJ2NxinAxIx4NqwfcGVBiOu4pYAfu5Pwl8wCVUbO2KcbDmxaGRR6CyCcMqLCzSl7Hw0T
9OE/nvpbnSBL11C0BCXajTNKyZLuxu4ujHJ1Q/iOrvdux8G+VYZtgKQ3bxPSziM3fM3zzxlAuhyzE
mq5eSIyiJTqb2Q03p4+gB2UcVIN0xKUSh40NZLYSpmFPJMhAnrwZU0oIObNIECgPM6tyz+HYUKJQf
QB9qJM4msXo4AJjpdO61P64ElMwm922ar1ckaFmEh4Iueyfd4AGS98EtKrASjynCTs/m+pPBzOVmx
1vjIhVlkIDoLzx4vdnSlj8qd8P4HpPol8w==
Content-Type: application/json; charset=utf-8
Host: pg-test.appson.ir
Content-Length: 207
Expect: 100-continue
Connection: Keep-Alive

{"ReferenceCode":"284bec959ca74c70bf956bb6cae909f4","TransactionId":"d7f98049
c4a34ab3be0b233786817c96","Pin":"9931","Date":"20171126134319","ProductCode":
"PRD-Book","RUID":"4d8cbddf9dac4196aa277f365b38a879"}
```

دامپ ۳- درخواست در سرویس Charge

پاسخ سرویس Charge

فیلد های Body پاسخ در جدول ۷ آمده است.

نام	توضیح	مثال
IsSuccess	موفق یا نا موفق بودن یک درخواست را نشان می دهد.	true
Response	در صورتی که سرویس موفق باشد، این فیلد پر می شود. (مقدار شی	{"SubscriptionExpireDate":"2017-11-27T13:43:24.4459727Z","TransactionCode":"3da559e099384b8189a8aaf6ac2dc558","A

ccountId":"C55GPTK5QBAUFOSHYFE76CNRX6KA"}	Response در ادامه توضیح داده می شود.)	
{"Code":"PG-000955","Message":" در فروخوانی "Description":"پیروکسی خطا رخ داده است در فروخوانی "Params":[]}"پیروکسی خطا رخ داده است	در صورتی که سرویس با خطا مواجه گردد این فیلد پر می شود.	Error

جدول ۷- Body پاسخ در سرویس Charge

نمونه ای از HTTP Response کامل در دامپ ۴ آمده است.

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: application/json; charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
PAYMENT-VERSION: 1.0.0
X-Powered-By: ASP.NET
Date: Sun, 26 Nov 2017 13:43:24 GMT
Content-Length: 196

{"IsSuccess":true,"Response":{"SubscriptionExpireDate":"2017-11-
27T13:43:24.4459727Z","TransactionCode":"3da559e099384b8189a8aaf6ac2dc558","A
ccountId":"C55GPTK5QBAUFOSHYFE76CNRX6KA"},"Error":null}
```

دامپ ۴- پاسخ سرویس Charge

مقدار شی Response در جدول ۸ آمده است.

نام	توضیح	مثال
SubscriptionExpireDate	تاریخ انقضای کالایی که کاربر عضو آن شده است (برای محصولات اشتراکی)	2017-11-27T13:43:24.4459727Z
TransactionCode	کد پیگیری برای پیگیری های آینده	3da559e099384b8189a8aaf6ac2dc558
AccountId	شناسه کاربر	C55GPTK5QBAUFOSHYFE76CNRX6KA

جدول ۸- فیلدهای Response در پاسخ سرویس Charge

پیاده سازی

نمونه پیاده سازی سرویس Charge با زبان C# در قطعه کد ۲ آمده است.

```
var pCode = "PRD-Book";
var pin = "9931";
var transactionId = "d10b91c20a4c4f109f75b6bad8c21947";
var url = "https://pg.appson.ir/api/otp/charge"

var dto = new PiqoDto.ChargeRequestDto
{
    ReferenceCode = Guid.NewGuid().ToString("N"),
    Date = DateTime.UtcNow.ToString("yyyyMMddHHmmss"),
    TransactionId = transactionId,
    ProductCode = pCode,
    Pin = pin,
    RUID = Guid.NewGuid().ToString("N")
};

var jsonSerializer = new JsonSerializer<PiqoDto.ChargeRequestDto>();
var key =

"<RSAKeyValue><Modulus>dUzy20Sz1hiPG9B0Xqo4vDDsgUOjLhYeNlEpKRt25goNDxb/Imjv92
2W2OiZiqd0kRNFJB8g6RiUn2SYs+AtT2U0m7RG262dlJlXkcLlhzO2upZDMpgREQYnzapQdNSxFHN
IE1rDa1flC2LtgRI3SaKVGSsxM7rssHcusN7rye8bkr8CnXFU81PIc8Ahh+dfsNg5TiiKSjTfmdnv
qMnHXLnVXnFCPFp7PafevPextp8cTtBHv7quimpzOUUopW3EWfqJt2R1WeD0keXXQqbZdFb6GXEXd
qw2bRnydVqojCVJsYu+S1qfH97lZAxG5ihizt8pNroBAyAkHKvS+IHd1Q==</Modulus><Exponen
t>AQAB</Exponent><P>9G/1S/1YGRQLF+qv9NSZPhBLUxfZf2vlph9HrNwUikv2DKe0g8+OsskEC
eqqMLMIumBUOcaHtTldEgHZ09NhsHUx/pjkaKuDfS1hkkz39uULIitjxYPVINKWt2YVlM5MaBPe1d
UK8F4gZbyVFSy1A3mH8c/XDVWNvJsaelsL5e0=</P><Q>lEGwl/I0K5PQZeAckHSOlCg+rPMSRx6Z
m+NWipy8Chmgc2YESkRLDNXjTNyX2FBWZUJ6WZ3SiriDYkLKkGmoHX2uQ+WMvwBdabqUy82WFhzEN
pZ27uoLd+Jpb6Lt2izRCMW5OMeEVbo6zuDPDqrhhuNOLoM9WOK9j6jvsue42ok=</Q><DP>3BXyRv
lU2T+yvVYSF99UGw2QxMA0lQYRQAHqBzohRGQgpkRZxFSdp1xWxpcDpdWNhkI1k8+tYP7FTfFcr90
jmD3tRc9j2NqVCaBSueeTXDneTGXE75JD08nI6liAFfup0AwUF3Q65THa+b9SfD5EvVwviwoYF2lw
tODydjiD/gE=</DP><DQ>duAZPiyp4ks6bYV+weGDtY5zeu/INxh1KMbnzGsSZ7LWsdEaHYaW+urB
wA6c/oikTbs5KYRfnnWGe5J8o8DkWQk+Yxi7eydKv40o5CWrc32LYw3QvY8StQTpb+cferI2xibsd
necR7T0lI8z11nzTdoTBT6cQRpFztwxnq0ozqk=</DQ><InverseQ>IE/cYdvjAdHxvTwyFFyEj9e
r61AC3K0kpAEAbckHG0JZ4ZY16ptYAcr1auEv2F461360r3R+Cfgld1NSGtWTQc6KomEDXIiHHwwL
ntL7Zmyk2Bzp67Ax/WvIkatCp4c9POBeX2QhbNCO9Fs2tkxVmkfwCYn9sfcIKcDyA/XQZEs=</Inv
erseQ><D>DXK9RJtoQkSfA9Nv2rZtIWO8dCNK00wCnsJjGKalSwFVcEONBWXWtjjRBdZDD+sMpeOg
w+e5JqvRIrtZzmzToSFKOCiOOrxppf5TVWOgjpGZIGy6AYp0xJtDGMS/U/oIwJqbFEuhGQeGmOhTC
9oBKpupcnSp/fIaHkGUS/VBjTNmqr/KLFcAj0rkPNy30TY9aFp2Ei8poYLNb9qaiuQvtU7EAiEj19
0y9cfwoqUZW74OcQDQc4Xbu94QPIkxX4FvnSff8Ecc8BTNN4GqjuacNZ0w9LMywVkmqKC6tJYsv9x
w+0MJQ5/J227lUloSyoWMfHjjQU0wQWirAMeKiJNowQ==</D></RSAKeyValue>";

var text = jsonSerializer.SerializeToString(dto);

var sign = Signature.Sign(key, text);

var result =
    ServiceUtility.Post<object>(
        url,
        dto,
        new List<KeyValuePair<string, string>>
        {
            new KeyValuePair<string, string>("RUID", dto.RUID),
            new KeyValuePair<string, string>("PRODUCT", dto.ProductCode),
            new KeyValuePair<string, string>("REQUESTDATE", dto.Date),
            new KeyValuePair<string, string>("SIGNATURE", sign),
        });
```

امضای دیجیتال

تمامی سرویس های سیستم پیکو می بایست توسط برنامه توسعه‌دهنده امضا گردد. امضای یک فراخوانی سرویس تایید می کند که فراخوانی حتما توسط توسعه دهنده صورت گرفته است. برای اطلاعات بیشتر در مورد امضای دیجیتال می توانید به آدرس های زیر مراجعه نمایید:

- http://searchsecurity.techtarget.com/definition/digital-signature
- https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

برای اینکه بتوانید یک درخواست سرویس را امضا کنید، نیاز به کلید خصوصی دارید. پیکو برای راحت تر شدن تولید جفت کلید های خصوصی و عمومی یک ابزار را در اختیار توسعه دهندگان قرار می‌دهد که با استفاه از آن می توانید جفت کلید های عمومی و خصوصی را تولید نمایید.

تولید کلیدهای عمومی و خصوصی

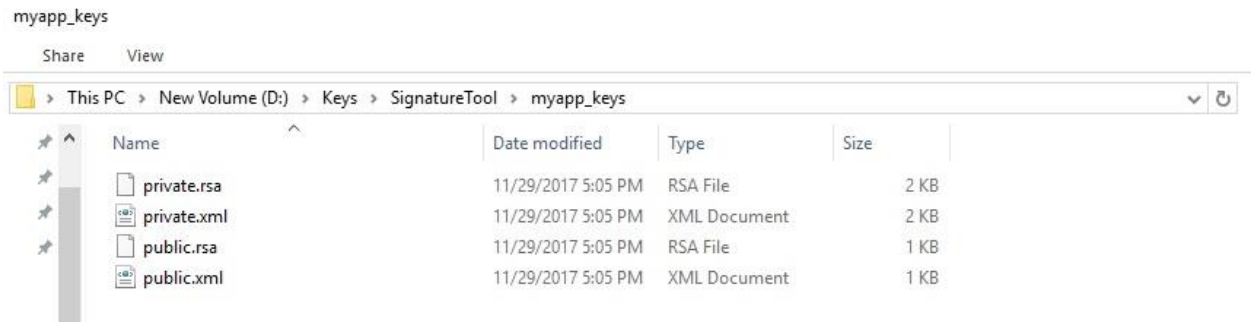
ابتدا فایل SignatureTool.zip را از آدرس http://piqo.ir/resources/RSAKeyTools/SignatureTool.zip دانلود نموده و سپس محتویات فایل را در مسیر مناسبی از حالت فشرده سازی خارج نمایید. برنامه Command Prompt را باز نموده و به این مسیر بروید. سپس عبارت Appson.Security.KeyGenerator.Console.exe در وارد کنید و کلید Enter را فشار دهید. از شما نام دایرکتوری کلید ها پرسیده می شود. تصویر ۱ این فرایند را نشان می دهد.

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>d:

D:\>cd D:\Keys\SignatureTool

D:\Keys\SignatureTool>Appson.Security.KeyGenerator.Console.exe
Enter destination directory: myapp_keys
Keys generated successfully at the following address
D:\Keys\SignatureTool\myapp_keys
Continue (y/N)?
```

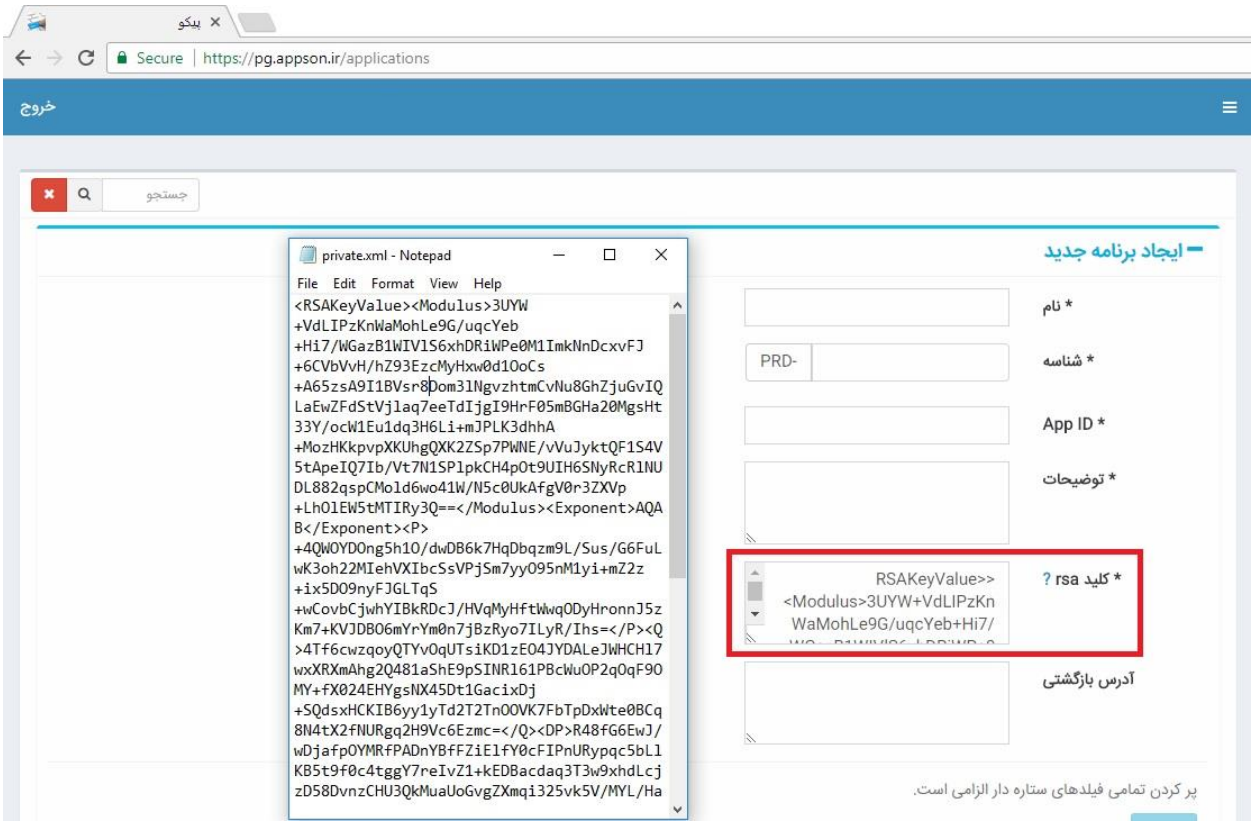
تصویر ۱- تولید کلیدهای عمومی و خصوصی

پس از وارد کردن نام دایرکتوری همانند تصویر ۲، کلید خصوصی و عمومی ایجاد می شود.

برخی از کتابخانه ها از فرمت xml پشتیبانی می کنند و بعضی کتابخانه های دیگر از فرمت rsa پشتیبانی می کنند. در برنامه خود میتوانید از private.xml یا private.rsa استفاده کنید. اما در پنل پیکو در هنگام تعریف برنامه می بایست محتویات public.xml را مانند تصویر 3 وارد نماید.



تصویر ۲- ایجاد کلید های عمومی و خصوصی در ۲ فرمت متفاوت



تصویر 3 – وارد کردن کلید عمومی در پنل پیکو

امضای Body درخواست

برای اضافه کردن امضا به درخواست باید مقدار Body را بدست آورده و سپس آن را امضا کنید. برای نمونه مقدار رشته Body در درخواست دامپ ۳، در دامپ ۵ قابل مشاهده است. برای تولید امضا، Body درخواست HTTP را با الگوریتم SHA1 درهم سازی نموده و سپس با الگوریتم RSA و با کلید خصوصی خود آن را رمز کنید. در نهایت داده رمزشده را به فرمت Base64 تبدیل کنید.

```
{"ReferenceCode":"284bec959ca74c70bf956bb6cae909f4","TransactionId":"d7f98049
c4a34ab3be0b233786817c96","Pin":"9931","Date":"20171126134319","ProductCode":
"PRD-Book","RUID":"4d8cbddf9dac4196aa277f365b38a879"}
```

دامپ ۵- مقدار Body در یک درخواست HTTP

نکته: برخی از فریم‌ورک‌ها ممکن است، شی ای که به عنوان Body به آن فریم‌ورک تحویل می دهید را تغییر داده و سپس Serialize و ارسال کنند. لذا توصیه می کنیم در صورتی که با خطای امضا مواجه شدید، مقدار رشته Body را قبل از ارسال از همان فریم‌ورکی که از آن استفاده می کنید بدست آورده و امضا نمایید.

پیاده سازی

پیاده سازی امضای درخواست با استفاده از زبان C# در قطعه کد ۳ آمده است.

```
public static string Sign(string privateKey, string httpBody)
{
    var cspParams = new CspParameters {ProviderType = 1};
    var rsaProvider = new RSACryptoServiceProvider(cspParams);
    rsaProvider.FromXmlString(privateKey);

    var plainBytes = Encoding.UTF8.GetBytes(httpBody);

    var encryptedBytes = rsaProvider.SignData(plainBytes, new
SHA1CryptoServiceProvider());

    return Convert.ToBase64String(encryptedBytes);
}
```

قطعه کد ۳- امضای متن با کلید خصوصی در C#