

**امضای دیجیتال (ارسال پیام)**

**نخسه 0.1**

فهرست

[**امضای دیجیتال** 2](#_Toc515190530)

[**تولید کلیدهای عمومی و خصوصی** 2](#_Toc515190531)

[**امضای درخواست** 4](#_Toc515190532)

# **امضای دیجیتال**

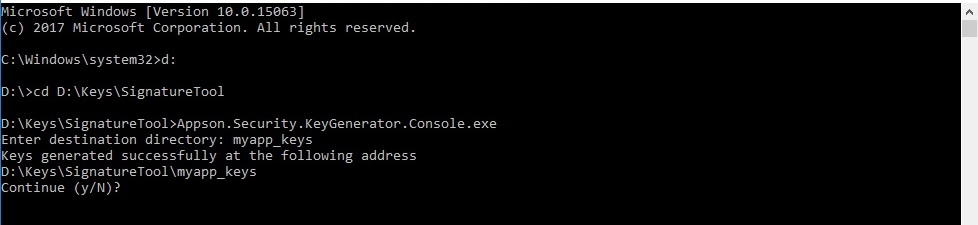
تمامی سرویس های سیستم ارسال و دریافت پیام، می بایست توسط برنامه توسعه‌دهنده امضا گردد. امضای یک فراخوانی سرویس تایید می کند که فراخوانی حتما توسط توسعه دهنده صورت گرفته است. برای اطلاعات بیشتر در مورد امضای دیجیتال می توانید به آدرس های زیر مراجعه نمایید:

* <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. برای راحت تر شدن تولید جفت کلید های خصوصی و عمومی یک ابزار توسط این شرکت ارائه شده که با استفاه از آن می توانید جفت کلید های عمومی و خصوصی را تولید نمایید.

**تولید کلیدهای عمومی و خصوصی**

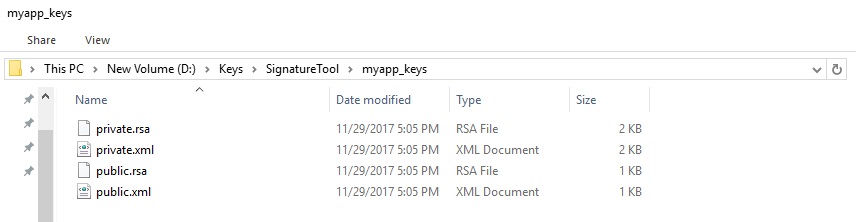
ابتدا فایل SignatureTool.zip را از آدرس <http://piqo.ir/resources/RSAKeyTools/SignatureTool.zip> دانلود نموده و سپس محتویات فایل را در مسیر مناسبی از حالت فشرده سازی خارج نمایید. برنامه Command Prompt را باز نموده و به این مسیر بروید. سپس عبارت Appson.Security.KeyGenerator.Console.exe را وارد کنید و کلید Enter را فشار دهید. از شما نام دایرکتوری کلید ها پرسیده می شود. تصویر 1 این فرایند را نشان می دهد.



*تصویر 1- تولید کیلیدهای عمومی و خصوصی*

پس از وارد کردن نام دایرکتوری همانند تصویر 2، 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 هنگام استفاده از توابع ارسال و دریافت پیام این شرکت می بایست محتویات public.xml را ارائه کنید.



*تصویر 2- ایجاد کلید های عمومی و خصوصی در 2 فرمت متفاوت*

**امضای درخواست**

هر پیام باید بر اساس ترکیب پارامترهای زیر، پیام فرمت شده‌ای را بسازد و آن را با کلید خصوصی خود امضا کند و در پارامتر قرار دهد.

ترکیب پارامترها از چپ به راست:

[Date],[Uid],[Sid],[ChannelType],[MessageType],[AccountId],[Content]

تاریخ درخواست باید UTC و با فرمت [Iso 8601](https://en.wikipedia.org/wiki/ISO_8601) باشد. (“yyyy-MM-ddTHH:mm:ss.fffZ”)

نمونه SignaturePattern :

var plaintext = $"{requestDateTime.ToStringIso8601Z()},

{requestUid},

{message.Sid},

{message.ChannelType},

{message.MessageType},

{message.AccountId ?? message.UserPhoneNumber},

{message.Content}";

var signatureParameter = "2018-04-09T07:11:48.011Z,

9d6efd381534443e9e852abaf889d217,

914a0a94-a5b5-47c9-9a19-a8926643b1e9,

Imi,

Content,

53EF14CD98B64D2F814FA5E5428A,

This is a test message"

روش امضا کردن : الگوریتم مورد استفاده برای asymmetric cryptography، الگوریتم RSA است که الگوریتم hash آن نیز SHA1 است.

Signature = Sign(privateKey, signatureParameter);

پیاده سازی امضای درخواست با استفاده از زبان C# در قطعه کد 3 آمده است.

