



## ارسال پیام دریافتی از کاربر به اکسترنال CP

نسخه ۳.1.۰,۰

تاریخ ۱۳۹۷/03/30

برای دریافت پیام کاربر باید یک post Api بر روی پروتکل http وجود داشته باشد. این آدرس Api باید در اختیار شرکت فناپ قرار بگیرد.

پس از دریافت پیام کاربر، سامانه پیام رسان فناپ، اطلاعات زیر را در اختیار شرکت مشتری قرار می دهد.

## Http request body:

بدنه پیام دارای object ی به فرمت آرایه ای تک عضوی از پارامترهای زیر است:

Muid	شناسه منحصر به فردی که توسط پیام رسان فناپ به پیام اختصاص داده شده است.
ReceiveTime	زمان دریافت پیام توسط سامانه ( <a href="#">Iso 8601</a> ) universal time به فرمت : "yyyy-MM-ddTHH:mm:ss.fffZ"
AccountId	شناسه کاربر
ChannelType	درگاهی که پیام کاربر از آن دریافت شده است، شامل مقادیر:  Pardis, Imi, Mtn, Rightel, Magfa  است.
Channel	سرشماره ای که پیام کاربر از آن دریافت شده است
Actor	عامل پیام دریافتی که دارای مقادیر:  Sms Cp, Tajmi, Ussd, Operator  است.
MessageType	نوع پیام دریافتی که دارای مقادیر:  Content, Subscription, Unsubscription, PremiumContent

	است.
Content	متن پیام ارسال شده توسط کاربر
Sid	شناسه منحصر به فرد مشتری که توسط شرکت فناپ در اختیار مشتری قرار گرفته و به منظور شناسایی مشتری از آن استفاده میکند.
Signature	پیام امضا شده توسط شرکت فناپ

در صورتی که متقاضی دریافت شماره کاربر هستند input، مقادیر زیر نیز ارسال می گردد:

UserPhoneNumber	شماره تلفن کاربر
-----------------	------------------

مثال:

```
[
  {
    "Muid": "74c925a6211f483fafb29650feb821c7",
    "Sid": " d45987d89490432990f4af64ee2c3cd6",
    "ReceiveTime": "2018-04-23T10:22:21.028Z",
    "ChannelType": "Imi",
    "Channel": "983048",
    "Actor": "Sms",
    "AccountId": "VL6DUI5T5TKUBJKGOSOB47P7XOUQ",
    "UserPhoneNumber": "98990***4656",
    "MessageType": "Content",
    "Content": "test",
    Signature:
    LSrRIM9Jh8HA9C6WtOZHxiRd4jt24vpALjr4FFvhda4TA2A4MO+xYtm93bxUcl3LANHDd5fMs2ruRUqAadB
    xpDWRG+AVOLDR8uQHOyRNsZvUYKdoDnnahRx6f3GI0abx6Lw1xUxzSUTr1Dk6PywllkVL2pmbaM6mL5PR
    +tBO2Ps=
  }
]
```

توضیحات فیلد ها:

: MessageType

نوع پیام دریافتی دارای یکی از مقادیر زیر است :

- Content عادی
- Subscription عضویت
- unSubscription لغو عضویت
- PremiumContent پیام پولی

: Actor

عامل پیام دریافتی دارای یکی از مقادیر زیر است :

کلیه عملیات کاربر غیر از کانال اس ام اس نیز برای مشتری ارسال میشود .

- Sms ارسال پیامک
- Cp درخواست مشتری
- Tajmi پنل تجمیعی
- Ussd سامانه USSD
- Operator اپراتور

مثال :

- عضویت بر روی سرویس از طریق اپ مشتری و ارسال OTP توسط کاربر:

Actor : Cp  
MessageType : Subscription

- لغو عضویت بر روی سرویس از طریق درخواست مشتری:

Actor : Cp  
MessageType : Unsubscription

- لغو عضویت کاربر از طریق پنل تجمیعی :

Actor : Tajmi  
MessageType : Unsubscription

- لغو عضویت از طریق کال ستر اپراتور :

Actor : Operator  
MessageType : Unsubscription

## Signature

برای احراز هویت و اثبات صحت پیام می‌باشد. فناپ با توجه به پارامترهای بدنه‌ی پیام، پیام فرمت شده‌ای را می‌سازد که همان پیام را توسط کلید خصوصی خود امضا می‌کند و در پارامتر Signature قرار می‌دهد. شرکت خصوصی محتوای این پیام را با کلید عمومی فناپ واقع در آدرس زیر

<https://github.com/appson/messaging-public/blob/master/SignaturePublicKey/publicKey.txt>

رمزگشایی می‌کند.

پیام فرمت شده بدین ترتیب ایجاد شده است :

( توضیح آنکه، مقادیر داخل براکت با توجه به مقادیر پارامترهای نظیر در بدنه‌ی پیام به صورت جدا شده با ویرگول، پر می‌شوند و ترتیب از چپ به راست حتما رعایت شود):

[ReceiveTime],[Sid],[ChannelType],[Channel],[Muid],[Content],[MessageType],[AccountId]



شرکت فناپ منتظر پاسخ فراخوانی مشتری نمی ماند و در صورتی که مشتری قصد ارسال پیام به کاربر را دارد باید وب سرویس ارسال پیام به مشتری پیاده سازی شود و از طریق آن پیام ها ارسال شود. سرویس ارسال پیام به مشتری نیازمند یک کلید نامتقارن است که برای امضا و احراز هویت مشتری مورد استفاده قرار میگیرد، بنابراین کلید عمومی آن در فرمت XML باید در اختیار شرکت فناپ قرار بگیرد.

**\*\*** برای اینکه آن شرکت بتواند پیام دریافتی از سامانه‌ی پیام‌رسان فناپ را در اختیار سامانه‌ی پیکو (سامانه‌ی پرداخت فناپ) قرار دهد مقدار پارامتر signature و پیام فرمت شده ای را که از بدنه پیام به منظور احراز هویت ساخته اید به پیکو ارسال کنید.

پیوست 1:

نحوه sign کردن فناپ :

الگوریتم مورد استفاده برای asymmetric cryptography ، الگوریتم RSA است که الگوریتم hash آن نیز SHA1 است نمونه کد در زیر آمده است.

```
public static string Sign(string key, string text)
{
    using (var rsaProvider = new RSACryptoServiceProvider(CspParams))
    {
        rsaProvider.FromXmlString(key);

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

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

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

پیوست 2:

نمونه کد احراز هویت :

```
public static bool Check(string key, string signedText, string text)
{
    if (string.IsNullOrEmpty(text)) return false;
    try
    {
        // Select target CSP
        var cspParams = new CspParameters { ProviderType = 1 };
        // PROV_RSA_FULL
        //cspParams.ProviderName; // CSP name
        var rsaProvider = new RSACryptoServiceProvider(cspParams);

        // Import private/public key pair
        rsaProvider.FromXmlString(key);

        var encryptedBytes = Convert.FromBase64String(signedText);
        var plainInput = Encoding.UTF8.GetBytes(text);

        // Decrypt text
        var check =
            rsaProvider.VerifyData(plainInput, new SHA1CryptoServiceProvider(), encryptedB
            ytes);
        return check;
    }
    catch (Exception exception)
    {
        Log.Error(exception.Message, exception);
        return false;
    }
}
```