

## مستند فنی اتصال به درگاه تلفنی بانک پاسارگاد

شهریور ۱۳۹۳



شناسنامه سند		
طبقه بندی سند	محرمانه (تجاری)	
کد سند	93-F41-SFT297-1-C	
عنوان سند	مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد	
گیرنده (نام شخص، سمت، سازمان)	شرکت مبین وان	
سفارش دهنده	بخش راهکارهای نوین پرداخت و خدمات ارزش افزوده فناپ	
تایید کننده سند	نام سازمان	شرکت فناوری اطلاعات و ارتباطات پاسارگاد آریان
	نام واحد سازمانی یا پروژه	سامانه های مبتنی بر تلفن
	نام، نام خانوادگی و سمت سازمانی تهیه کنندگان	کارشناسان بخش سامانه های مبتنی بر تلفن
	نام، نام خانوادگی سمت سازمانی تایید کنندگان	سولماز اوجاقی - مدیر بخش سامانه های مبتنی بر تلفن
شماره نسخه (فعلی)	۱	
تاریخ تهیه و تنظیم (نسخه یک)	۱۳۹۳/۰۶/۱۱	
تعداد صفحات	۱۷	
تذکرات حقوقی	تمامی حقوق مالکیت فکری و معنوی این سند متعلق به شرکت فناوری اطلاعات و ارتباطات پاسارگاد آریان (فناپ) است و هرگونه بهره برداری جزئی یا کلی از سند و انتشار کاغذی یا الکترونیکی تمام یا بخش هایی از آن منوط به اخذ موافقت قبلی و کتبی شرکت پاسارگاد آریان (فناپ) است و در غیر این صورت مجاز نیست.	
اطلاعات تماس تهیه کننده سند		
آدرس	خیابان مطهری، تقاطع سهروردی، شماره ۹۴ - شرکت فناپ	
کد پستی	۱۵۷۸۷۷۵۵۱۱	
صندوق پستی		
تلفن	۰۲۱- ۸۸۳۲۷۶۰۷-۹	
دورنگار	۰۲۱- ۸۸۳۲۷۶۱۴	
سایت اینترنتی	www.fanap.ir	
پست الکترونیکی	info@fanap.ir	

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد	سازمان تولیدکننده: شرکت فناپ
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان	کد سند: 93-F41-SFT297-1-C
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱
شماره نسخه: ۱	صفحه ۲ از ۱۹ صفحه



## فهرت

- ۱- مقدمه ..... ۴
- ۲- تعاریف اولیه ..... ۵
  - ۱-۲ تعاریف مرتبط با کاربر ..... ۵
  - ۲-۲ تعاریف مرتبط با سرویس دهنده ..... ۵
  - ۳-۲ تعاریف مرتبط با بانک و عملیات مالی ..... ۶
- ۳- مراحل انجام تراکنش ..... ۷
  - ۱-۳ مرحله اول: ..... ۷
  - ۲-۳ مرحله دوم: ..... ۷
  - ۳-۳ مرحله سوم: ..... ۹
  - ۳-۴ مرحله چهارم: ..... ۹
- ۴- دریافت نتیجه تراکنش ..... ۱۰
- ۵- تشریح ErrorCode های ارتباطی ..... ۱۲

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۳ از ۱۹ صفحه



## ۱- مقدمه

امروزه با پیشرفت تکنولوژی و رقابت در عرصه ارائه کالا و خدمات، نحوه پرداخت بسیار حائز اهمیت است. پرداخت ها می تواند به صورت حضوری و غیر حضوری انجام شود. پرداخت به صورت غیر حضوری می تواند از طریق اینترنت، موبایل و تلفن انجام شود. هر کدام از طرق ذکر شده ویژگی های منحصر بفرد خود را دارند. البته پرداخت غیرحضوری از طریق بانکداری مجازی و الکترونیک به دلیل سهولت مورد اقبال همگانی قرار گرفته است. پرداخت از طریق تلفن نیز ویژگی های خاص خود را دارد. سادگی مراحل انجام، در دسترس بودن تلفن حتی در محروم ترین مناطق، عدم نیاز به دانش خاص و کم هزینه بودن آن می تواند مشتریان زیادی را به خود جلب کند.

امروزه سیستم های تلفن گویا و پرداخت و خرید تلفنی به علت در دسترس بودن تلفن و راحتی کار، بسیار مورد توجه قرار گرفته است و به طبع سازمانها و شرکت ها نیز توجه خاصی به این نوع سرویس دهی دارند.

در روش پرداخت از طریق تلفن، کاربر می تواند با استفاده از تلفن و کارت عضو شتاب پرداخت خود را انجام دهد.

پرداخت از طریق تلفن، به دو روش قابل ارائه است:

در روش اول، سرویس دهنده یا مرجعت، کالا یا خدمات خود را به کاربر ارائه می کند و کاربر با انتخاب کالا یا سرویس مورد نظر خود از مرجعت، قبض دریافت می کند<sup>۱</sup>. این قبض حاوی شماره قبض و شماره تلفنی است که شخص می تواند با تماس گرفتن با آن، مراحل پرداخت را تکمیل نماید.

در روش دوم، کاربر با تلفن گویای سرویس دهنده مورد نظر خود تماس گرفته و مراحل انتخاب کالا یا سرویس مورد نظر خود را طی می کند. پس از انتخاب کالا و انتخاب روش پرداخت از طریق تلفن، سرویس دهنده اطلاعات فاکتور را به همراه کاربر به سمت درگاه پرداخت تلفنی بانک ارسال کرده و ارتباط سرویس دهنده با کاربر قطع می شود. پس از آن، کاربر به خط تلفن درگاه پرداخت بانک متصل می شود.

پس از اتصال کاربر به خط درگاه پرداخت تلفنی بانک، کاربر با تایید اطلاعات پرداخت، با وارد کردن شماره کارت عضو شتاب و رمز اینترنتی، تراکنش پرداخت را انجام می دهد. سپس درگاه پرداخت کاربر را به خط سرویس دهنده فرستاده و کاربر می تواند به ادامه سیر منوهای سرویس دهنده بپردازد. در این مستند، مراحل پرداخت از طریق تلفن، به روش دوم، به اختصار ارائه خواهد شد.

<sup>۱</sup> دریافت قبض می تواند از طریق تلفن گویای سرویس دهنده باشد.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۴ از ۱۹ صفحه



## ۲- تعاریف اولیه

### ۱-۲ تعاریف مرتبط با کاربر

- کاربر: هویتی است که توسط یکی از انواع کارت های بانکی عضو شبکه شتاب و با مراجعه به سیستم تلفنی سرویس دهنده تقاضای پرداخت قبوض خود را دارد.

### ۲-۲ تعاریف مرتبط با سرویس دهنده

- سرویس دهنده: هویتی است که با آماده سازی بستر پرداخت تلفنی قبوض، اقدام به انجام این کار از طریق سیستم تلفنی خود می نماید.
- شماره شناسائی سرویس دهنده (MerchCode<sup>۲</sup>): کدی است که توسط بانک به سرویس دهنده اختصاص می یابد و در حین انجام تراکنش برای شناسایی سرویس دهنده از آن استفاده می گردد.
- شماره شناسائی ترمینال (TermCode<sup>۳</sup>): کدی است که توسط بانک به سرویس دهنده اختصاص می یابد و در حین انجام تراکنش از آن استفاده می گردد.
- کلید خصوصی سرویس دهنده (Private Key): کلیدی است که سرویس دهنده برای احراز هویت از آن استفاده می کند و تمامی داده های ارسالی خود به بانک را با آن کلید، امضای دیجیتال می کند.
- کلید عمومی سرویس دهنده (Public Key): کلیدی است که بانک جهت تایید امضای دیجیتال سرویس دهنده از آن استفاده می کند.
- مبلغ فاکتور (Amount): برابر با مجموع مبالغ قبوضی است که جهت پرداخت به درگاه بانک ارسال شده اند.
- شماره درخواست (InvNumber<sup>۴</sup>): هر درخواستی که از سمت سرویس دهنده ارسال می شود باید دارای شماره ی خاص خود باشد.
- تاریخ درخواست (InvDate<sup>۵</sup>): تاریخ ارسال درخواست است و فرمت آن به انتخاب سرویس دهنده است.

<sup>۲</sup> Merchant Code

<sup>۳</sup> Terminal Code

<sup>۴</sup> Invoice Number

<sup>۵</sup> Invoice Date

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۵ از ۱۹ صفحه



- **\*توجه\***: لازم به ذکر است که تاریخ و شماره درخواست، باید به گونه ای تخصیص داده شوند که از ترکیب آن ها شناسه یکتایی بدست آید تا همیشه بتوان برای شناسایی یک تراکنش از آن استفاده کرد.
- **امضای دیجیتال (Digital Signature)**: امضای دیجیتال روشی مبتنی بر الگوریتم های رمزنگاری نامتقارن است که به کمک آن می توان اطمینان حاصل کرد که داده های ارسالی از جانب سرویس دهنده ی مشخصی ارسال شده است.
- **CustNum<sup>۶</sup>**: شماره تلفن کاربر است.
- **Timestamp**: زمان ارسال داده به درگاه پرداخت تلفنی بانک را Timestamp می گویند که فرمت آن به شکل "YYYY/MM/DD HH:MM:SS" بوده و به تاریخ میلادی ارسال می گردد. اگر هرکدام از عده های ماه، روز، ساعت، دقیقه یا ثانیه یک رقاست با قرارداد یک صفر در سمت چپ آن باید عدد دو رقمی تولید شده و برای بانک ارسال شود. نکته ی مهم در اینجا این است که مقداری که در فیلد Timestamp قرار می گیرد باید دقیقا با مقداری که تحت همین عنوان در امضای دیجیتال قرار می گیرد یکی باشد، همچنین هیچ دو درخواستی، نمی توانند دارای Timestamp یکسان باشند. Timestamp هر تراکنش باید از Timestamp تراکنش قبلی بزرگتر باشد.

## ۲-۳ تعاریف مرتبط با بانک و عملیات مالی

- **بانک**: منظور از بانک در این مستند بانک پاسارگاد است.
- **درگاه پرداخت تلفنی بانک**: درگاه پرداخت تلفنی متعلق به بانک است. سرویس دهنده بر بستر VOIP و پروتکل SIP v2.0<sup>۷</sup> با آن ارتباط برقرار کرده و کاربر را پس از انتخاب کالا یا سرویس مورد نظر، به سمت آن انتقال می دهد. کاربر پس از انتقال به سمت درگاه تلفنی بانک، اطلاعات کارت جهت پرداخت را در این درگاه وارد می کند.<sup>۸</sup>
- **نوع تراکنش (Action)**: نشان دهنده نوع عملیات مالی مورد نظر است که در این مستند ۱۰۰۱ در نظر گرفته شده است.
- **نوع درخواست (RequestType)**: نشان دهنده نوع درخواست مورد نظر سرویس دهنده است که در این مستند ۱۰۰۱ جهت پرداخت قبض و ۹۱۰۰۱ جهت دریافت نتیجه تراکنش است.

<sup>۶</sup> Customer Number

<sup>۷</sup> توضیحات تکمیلی در پیوست ۱ توضیح داده شده است.

<sup>۸</sup> جهت ارتباط VIOP المانهای IP و Port پس از عقد قرارداد اعلام خواهد شد.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۶ از ۱۹ صفحه



- کد رهگیری (TransactionReferenceID): شماره ای است که درگاه بانک پس از انجام تراکنش به همراه کاربر به سمت سرویس دهنده انتقال می دهد، این کد جهت استعلام نتیجه مورد استفاده قرار می گیرد.

### ۳- مراحل انجام تراکنش

#### ۱-۳ مرحله اول:

کاربر با سیستم تلفن گویای سرویس دهنده تماس گرفته و بعد از طی مراحل آن سیستم و انتخاب پرداخت قبض مورد نظر، آماده اتصال به درگاه پرداخت تلفنی بانک، برای پرداخت مبلغ قبض می گردد.

#### ۲-۳ مرحله دوم:

سرویس دهنده اطلاعات مربوط به تراکنش را درون SIP Header قرار داده و به همراه کاربر به سمت TelPayGateway بر روی پروتکل SIP v2.0 مبتنی بر RFC 3261 ارسال می کند. سرویس دهنده برای این مقصود، قدم های زیر را دنبال می کند:

قدم اول: تولید x-Info جهت درج در SIP Header ارسالی به سمت درگاه پرداخت

در این قدم اطلاعات فاکتور را به شرح زیر به فرمت JSON تبدیل می شود.

#### x-Info:

```
{"MerchCode":"123456789","TermCode":"123456789","InvNum":"1234567890123456789",
"InvDate":"1392/06/31 08:10:56","Amount":"15000000000","TimeStamp":"2013/06/25
08:10:58","Action":"1001","CustNum":"989201234567"}
```

\*توجه\*: در صورتی که این header با فرمت درخواستی پر نشده باشد، تماس پاسخ داده می شود و هشدار مناسب برای کاربر خوانده می شود. سپس یک header با نام ErrorCode و با مقدار عددی خطای رخ داده به سمت سرویس دهنده باز گردانده (Transfer) می شود.

#### قدم دوم:

تولید x-Sign جهت درج در SIP Header ارسالی به سمت درگاه پرداخت

سرویس دهنده اطلاعات تولید شده x-Info را، با PrivateKey خود امضا می کند. مراحل تولید امضای دیجیتال عبارت است از:

- اجرای الگوریتم درهم سازی SHA1 بر روی رشته x-Info.
- امضای رشته ای حاصل از بند دوم به وسیله PrivateKey، که نتیجه آن یک رشته ی باینری است.
- تبدیل رشته ی باینری به رشته ای با فرمت base64String، که این رشته امضای دیجیتال سرویس دهنده برای تراکنش محسوب می شود.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۷ از ۱۹ صفحه



## قدم سوم: انتقال کاربر به درگاه پرداخت تلفنی

در مرحله آخر سرویس دهنده، موارد تولید شده در مراحل قبل را درون پیام Invite قرار داده و به همراه کاربر به سمت درگاه پرداخت ارسال می کند.

مورد تولید شده در قدم اول، Key با نام x-Info، مورد تولید شده در قدم دوم با نام x-Sign درون SIP Message از نوع Invite قرار داده می شود. سپس کاربر را به آدرس زیر انتقال می دهد.<sup>۹</sup>  
کاربر به آدرس زیر، توسط سرویس دهنده، انتقال داده می شود:

To : RequestType \* CustomerSessionID@ TelPayGatewayIP

CustomerSessionID : مقدار موجود در این فیلد توسط سیستم سرویس دهنده وارد می شود، که می تواند شامل، مکانی در منو که کاربر قبل از انتقال به درگاه پرداخت در آن بوده است، و یا یک شماره Session مربوط به آن کاربر خاص، باشد. این داده جهت از سر گرفتن ادامه ی عملیات کاربر سمت سرویس دهنده استفاده می شود که عیناً هنگام بازگرداندن کاربر به سرویس دهنده به آن تحویل داده می شود. البته ارسال این داده اختیاری است.

RequestType: عددی است که نشان دهنده نوع عملیات در خواستی سرویس دهنده است، مانند پرداخت قبض ۱۰۰۱، گرفتن نتیجه تراکنش پرداخت قبض ۹۱۰۰۱ و ...

TelPayGatewayIP: IP درگاه پرداخت تلفنی بانک است که پس از عقد قرارداد به اطلاع رساننده می شود.

نمونه پیام ارسالی از پذیرنده به سمت درگاه پرداخت تلفنی :

```
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:1001*1230 SIP/2.0
Message Header
From: <sip:1001*1230>
To: <sip:1001*1230>
Call-ID: 5
CSeq: 1 INVITE
Via: SIP/2.0/UDP
Max-Forwards: 70
Supported: replaces
x-Info: {"MerchCode": "12345678912", "TermCode": "1234567891", "InvNum": "124536789123456789", "Invdate": "1392/06/05 12:
Contact: <sip:
Allow: INVITE, CANCEL, ACK, BYE, OPTIONS, INFO, REFER, NOTIFY
Allow-Events: refer
x-Sign: BJWU+6GIqaQyr9xqnMun3VZkmxH2gmM100q3y0vpDCIaHKNa3rwa0ZrEC/U1RNdB3M2C/hs0b+B3TnoI0qr4gn9IpoUv/h36qmvhRwXBJ3m
```

**\*توجه\*:** در صورتی که فیلد RequestType خالی ارسال شده باشد و یا مقداری غیر از مقادیر مورد انتظار بوده باشد، به دلیل مشخص نبودن عملیات درخواستی، تماس reject خواهد شد. جهت مشخص نمودن خطای رخ داده برای سرویس دهنده، یک header با نام ErrorCode با مقدار کد خطای رخ داده در هنگام رد تماس، تنظیم شده و باز گردانده می شود.

<sup>۹</sup> این انتقال باید به صورتی باشد که اتصال کاربر با سرویس دهنده کامل قطع شود.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۸ از ۱۹ صفحه





نمونه پیام دریافتی پذیرنده در حالت Error به شکل زیر است:

```

Frame 8: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface 0
Ethernet II, Src: [redacted], Dst: [redacted]
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
User Datagram Protocol, Src Port: [redacted], Dst Port: [redacted]
Session Initiation Protocol (480)
  Status-Line: SIP/2.0 480 Temporarily Unavailable
  Message Header
    From: [redacted]; tag=7ecad103b0
    To: <[redacted]>; tag=59f0b18-33001dac-1f9a-50022-1e6fd4-210cd1df-1e6fd4
    Call-ID: 99389E8510FE4CFE993BD554880F5F7B0x0a140a0f
    CSeq: 1 INVITE
    Via: SIP/2.0/UDP 10.20.10.15;rport=5060;branch=z9hG4bK0a140a0f000000d952d14de90000343000000060
    Supported: replaces
  ErrorCode: 401
  Content-Length: 0
  
```

### ۳-۳ مرحله سوم:

پس از انتقال کاربر به سمت درگاه پرداخت تلفنی بانک، اطلاعات پرداخت برای کاربر خوانده می شود و کاربر در صورت عدم تایید صحت آن با وارد کردن کلید مربع، از پرداخت آن انصراف داده و به سمت سرویس دهنده ارجاع داده می شود و در غیر این صورت، با وارد کردن اطلاعات کارت (شماره کارت و رمز اینترنتی) درخواست پرداخت را تکمیل می نماید.

### ۳-۴ مرحله چهارم:

در این مرحله تراکنش توسط بانک پردازش گردیده و عملیات لازم در مرکز بانک پاسارگاد، شتاب و بانک صادرکننده کارت انجام می پذیرد. در صورت صحت ورود داده ها و وجود وجه کافی در حساب کاربر، عملیات مالی در این مرحله توسط بانک صورت می گیرد، در غیر این صورت با خواندن پیام مناسب عدم موفقیت تراکنش به کاربر اطلاع داده خواهد شد. در انتها، شماره پیگیری و شماره ارجاع برای کاربر خوانده می شود. کاربر می تواند توسط آن ها تراکنش خود را پیگیری نماید.

سپس کاربر به همراه اطلاعات زیر در فیلد CallerId، به سمت سرویس دهنده انتقال داده می شود.

RequestType \* CustomerSessionID \* ReturnValue \* Result @ MerchantIP

CustomerSessionID: مقدار موجود در این فیلد توسط سیستم سرویس دهنده وارد می شود، که می تواند شامل مکانی در منو که کاربر قبل از انتقال به درگاه پرداخت در آن بوده است، و یا یک شماره Session مربوط به آن کاربر خاص، باشد. این داده جهت از سر گرفتن ادامه ی عملیات کاربر سمت سرویس دهنده استفاده می شود که عیناً هنگام بازگرداندن کاربر به سرویس دهنده به آن تحویل داده می شود. البته ارسال این داده اختیاری است.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۹ از ۱۹ صفحه



**RequestType**: عددی است که نشان دهنده نوع عملیات درخواستی سرویس دهنده است مانند پرداخت قبض، گرفتن نتیجه تراکنش و ... در مرحله شماره درخواست ارسالی توسط سرویس دهنده، است.

**ReturnValue**: در صورتی که عملیات پرداخت سمت بانک انجام شده باشد، این فیلد حاوی کد رهگیری تراکنش (**TransactionReferenceID**) است، که جهت استعلام نتیجه تراکنش توسط سرویس دهنده مورد استفاده قرار می گیرد. در غیر این صورت، این فیلد حاوی کد خطای مربوطه است که در بخش "تشریح **ErrorCode** های ارتباطی" به تفصیل توضیح داده شده است.

**Result**: نتیجه تراکنش است. در صورت تراکنش موفق مقدار 1 و در غیر این صورت مقدار 0 ارسال می شود.

**MerchantIP**: IP سرویس دهنده است که کاربر در ابتدا از آن IP به سمت درگاه پرداخت آمده است.

### توجه مهم:

به دلیل مسائل امنیتی، سرویس دهنده به هیچ وجه به نتیجه دریافتی، **Result**، در مرحله قبل نباید اکتفا کند و سرویس دهنده ملزم به استعلام نتیجه تراکنش از درگاه پرداخت تلفنی یا درگاه پرداخت اینترنتی است. در غیر این صورت، عواقب آن با سرویس دهنده بوده و بانک هیچ گونه مسئولیتی در قبال آن به عهده ندارد.

## ۴- دریافت نتیجه تراکنش

پس از انجام تراکنش، سرویس دهنده ملزم به استعلام نتیجه تراکنش از سمت درگاه پرداخت تلفنی است.

جهت دریافت نتیجه تراکنش از درگاه پرداخت، سرویس دهنده باید اطلاعات فاکتور یا کد رهگیری دریافت شده از درگاه را در **SIP Header** قرار داده و به سمت درگاه با **CallerID** زیر ارسال کند:

To : RequestType @ TelPayGatewayIP

**RequestType**: جهت درخواست "دریافت نتیجه تراکنش" عدد ۹۱۰۰۱ ارسال شود.

سپس با ارسال اطلاعات فاکتور در **Header** با **key** با نام **x-Info** به دو روش زیر می توان از نتیجه تراکنش باخبر شد.

\*توجه\*: در صورتی که فیلد **RequestType** خالی باشد و یا مقداری غیر از مقادیر مورد انتظار

ارسال شده باشد، به دلیل مشخص نبودن عملیات درخواستی، تماس **reject** خواهد شد. جهت

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۰ از ۱۹ صفحه



مشخص نمودن خطای رخ داده برای سرویس دهنده، یک header با نام ErrorCode با مقدار کد خطای رخ داده در هنگام رد تماس تنظیم شده و باز گردانده می شود.

با ارسال کد رهگیری، TransactionReferenceID دریافت شده از جانب بانک با فرمت JSON.

**x-Info :** {"TransRefID": "635154612243027344"}

و نیز در صورتی که سرویس دهنده به هر دلیلی موفق به دریافت TransactionReferenceID از سمت درگاه پرداخت، نشود می تواند با ارسال InvDate، InvNum، MerchCode و TermCode تراکنش مورد نظر، به فرمت JSON، از نتیجه تراکنش باخبر شود.

**x-Info :**

{"MerchCode": "123456789", "TermCode": "123456789", "InvNum": "1234567890123456789", "InvDate": "1392/06/31 08:10:56"}

\*توجه\*: در صورتی که این header با فرمت درخواستی پر نشده باشد ارتباط برقرار نشده و یک header با نام ErrorCode و با مقدار عددی خطای رخ داده در جواب پذیرنده ارسال می شود.

درگاه پرداخت تلفنی، پس از دریافت اطلاعات ارسالی، نتیجه تراکنش را با فیلدهای زیر در Header جایگزین کرده و به سمت سرویس دهنده ارسال کرده و ارتباط قطع می شود.

**x-Info :**

{"MerchCode": "123456789", "TermCode": "123456789", "InvNum": "1234567890123456789", "InvDate": "1392/06/31 08:10:56", "Amount": "1500000000", "Action": "1001", "TransRefID": "635154612243027344", "Result": "0|1", "traceNumber": "5446464646", "referenceNumber": "65464646544", "transactionDate": "2013/09/22 15:41:40"}

**x-Sign :**

این فیلد با امضای فیلد x-Info پر شده است.

سرویس دهنده باید رشته x-Info دریافت شده فوق الذکر را با مقدار فیلد x-sign و کلید عمومی دریافتی از بانک، چک کرده (VerifySign) و در صورت اطمینان از صحت داده ها، نتایج را استخراج کرده و سپس با Action، InvoiceNumber، InvoiceDate، MerchantCode و TerminalCode موجود در فیلدهای ارسالی تطبیق دهد و در صورت اطمینان از آن، نتیجه تراکنش را خوانده و اقدام مقتضی را انجام می دهد.

\*توجه\*: شایان ذکر است که کلید عمومی امضای دیجیتال نتیجه تراکنش با کلید خصوصی

دریافتی از بانک جهت امضای داده های پرداخت قبض متفاوت است. این کلید عمومی پس از عقد قرارداد در اختیار سرویس دهنده قرار خواهد گرفت.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۱ از ۱۹ صفحه



نمونه پیام دریافتی پذیرنده در حالت دریافت نتیجه تراکنش به شکل زیر است:

```
Frame 416: 972 bytes on wire (7776 bits), 972 bytes captured (7776 bits) on interface 0
Ethernet II, Src: C..., Dst: ...
Internet Protocol Version 4, Src: ..., Dst: ...
User Datagram Protocol, Src Port: ..., Dst Port: sip (5060)
Session Initiation Protocol (480)
  Status-Line: SIP/2.0 480 Temporarily unavailable
  Message Header
    From: "":tag=32a72a408442
    To: <:tag=82c4938-100a140a-1f9a-50022-ab2-7bbeb66c-ab2>
    Call-ID: AE87FF6AC5E84C049B29B8C375E7B8600xac1d0033
    Cseq: 1 INVITE
    Via: SIP/2.0/UDP 172.29.0.51;rport=5060;branch=z9hG4bKac1d00330000003946f51c8a000051c00000007
    Supported: replaces
    X-Info: {"MerchCode":"1024","TermCode":"1","InvNum":"111111","InvDate":"2013/08/04 14:32:41","Amount":"165965000.00","Action":"1001","TransactionR
    X-Sign: Qxht5jqbvax90yqvnd8E9chry2c9fZ5sD0uc6147R8/rxp+LogxRD3bv20xrXNRk6nUwgo20cGIZTt9HLcFLZ5fGGFIum6250a83FImz7QgJQLTSLqTz9vax56JP81/G000AVF493
```

## ۵- تشریح ErrorCode های ارتباطی

در این مرحله به تشریح حالاتی که ممکن است در طی ارتباط رخ دهد تا پرداخت انجام نگیرد، می پردازیم:

ردیف	نام	کد خطا
۱	ErrorOnCallerID	۴۰۱
دلیل بروز: در صورت دریافت مقادیر خارج از استاندارد های مستند در CallerID ارسالی		
راه حل: در این صورت سرویس دهنده باید به لاگ های خود رجوع کرده و نسبت به عملیات درخواستی خود، مقدار CallerID ارسالی به بانک را چک کرده و طبق مستند عمل کرده و دوباره تلاش کند.		
۲	ErrorOnHeader	۴۰۲
دلیل بروز: در صورت دریافت مقادیر خارج از استاندارد های مستند در SIP Header ها		
راه حل: در این صورت سرویس دهنده باید به لاگ های خود رجوع کرده و نسبت به عملیات درخواستی خود، مقادیر Header پیام ارسالی به بانک را چک کرده و طبق مستند عمل کرده و دوباره تلاش کند. اشتباهات می تواند شامل فرمت نادرست JSON، خالی بودن Header مورد نظر آن عملیات و مواردی از این دست باشد.		
۳	CanceledByUser	۴۰۳
دلیل بروز: در صورت انصراف کاربر از پرداخت		
راه حل: در این صورت کاربر با وارد نکردن ورودی های مورد نظر و یا عدم تایید پرداخت، از انجام تراکنش انصراف داده است.		

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱
		صفحه ۱۲ از ۱۹ صفحه



۴۰۴	ErrorServiceUnreachable	۴
دلیل بروز: در صورت در دسترس نبودن سرویس های پرداخت بانک		
راه حل: در این صورت سرویس دهنده باید بعد از چند ثانیه دوباره تلاش کند.		

در صورت بروز هر یک از شرایط ذکر شده، کاربر به سمت سرویس دهنده برگردانده شده و  
 CallerID ارسالی به سمت سرویس دهنده به فرمت زیر خواهد بود:

RequestType \* CustomerSessionID \* ReturnValue \* Result @ MerchantIP

CustomerSessionID: مکانی در منو که کاربر قبل از انتقال به درگاه پرداخت در آن بوده است، و  
 یا یک شماره Session مربوط به آن کاربر.

RequestType: نوع عملیات درخواستی سرویس دهنده.

ReturnValue: کد خطای رخ داده، که مقادیر آن در جدول بالا ذکر شده است.

Result: نتیجه تراکنش است. در صورت ارسال ReturnValue حاوی کد خطا مقدار آن 0 خواهد بود.

MerchantIP: IP سرویس دهنده است که کاربر در ابتدا از آن IP به سمت درگاه پرداخت آمده است.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱
		صفحه ۱۳ از ۱۹ صفحه



## پیوست ۱: SIP V2.0 RFC 3261

SIP یکی از پروتکل های انتقال صدا<sup>۱۰</sup> بر روی شبکه و اینترنت است. SIP مخفف Session Initiation Protocol به معنای پروتکل آغازگر جلسه است. این پروتکل قویترین پروتکل انتقال صدا بر روی شبکه و اینترنت است که می توان آن را جایگزینی برای TCP/IP در دنیای شبکه برشمرد. این پروتکل در لایه سوم شبکه کار می کند. این پروتکل جهت ارتباط سگنالینگ بین سرور و کلاینت، از پیام هایی استفاده می کند. این پیام ها به دو دسته تقسیم می شود: Request و Response. چند پیام مهم این پروتکل به شرح زیر است: پیام: INVITE یک نوع Request است که جهت ایجاد ارتباط ارسال می شود و در صورت قبول آن از سمت مقابل، ارتباط تشکیل می شود. پیام: ACK یک نوع Response است که در صورت صحت دریافت بسته های SIP ارسال می شود. پیام: BYE یک نوع Request است که جهت خاتمه دادن به تماس ارسال می شود.

البته این پیام ها گوشه ای از پیام های SIP است و به عنوان مثال بیان شده است. جهت اطلاع بیشتر به سایت زیر مراجعه فرمایید:

<http://tools.ietf.org/html/rfc3261>

<sup>10</sup> VOIP یا Voice over IP

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۴ از ۱۹ صفحه

پیوست ۲: نمونه کد به زبان C#

نمونه کد ارسال داده‌ها

```
private void setSendingInfo() {
    int merchantCode = 115; // کد پذیرنده
    int terminalCode = 12; // کد ترمینال
    int amount = 2000000; // جمع مبلغ قبوض
    string customerNumber = "989201234567"; // شماره کاربر تماس گیرنده
    string timeStamp = DateTime.Now.ToString("yyyy/MM/dd HH:mm:ss");
    string invoiceNumber = "1234567890123456789"; // شماره فاکتور
    string invoiceDate = "1392/06/31 08:10:56"; // تاریخ فاکتور
    string action = "1001";

    // مراحل تولید x-Info
    string x-info =
        string.Format("{\"MerchCode\":\"{0}\",\"TermCode\":\"{1}\",\"InvNum\":\"{2}\",\"InvDate\":\"{3}\",\"Amount\":\"{4}\",\"TimeStamp\":\"{5}\",\"Action\":\"{6}\",\"CustNum\":\"{7}\"}", merchantCode, terminalCode, invoiceNumber, invoiceDate, amount, timeStamp, action, customerNumber);

    // مراحل تولید x-Sign
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString("<RSAKeyValue><Modulus>oQRshGhLf2Fh... ");
    // کلید خصوصی سرویس دهنده

    string infoForSign = x-info;

    byte[] signMain =
        rsa.SignInfo(Encoding.UTF8.GetBytes(infoForSign),
            new SHA1CryptoServiceProvider());
    string x-sign = Convert.ToBase64String(signMain);

    // Set SIP Header
    SetSipHeader("x-Info", x-info);
    SetSipHeader("x-Sign", x-sign);

    // Transfer Customer to TelPayGateway
    TransferCallTo("1001*" + CustomerSessionID + "@"
+TelPayGatewayIP);
}
```

\*توجه\*:

شایان ذکر است که توابعی که وظیفه ارتباط بر بستر پروتکل SIP همچون **SetSipHeader** و **TransferCallTo** را دارند، باید توسط سرویس دهنده پیاده‌سازی شوند.



## نمونه کد دریافت نتیجه پرداخت

```
private getTransResult() {
    int merchantCode = 115; // کد پذیرنده
    int terminalCode = 12; // کد ترمینال
    int amount = 2000000; // جمع مبلغ قبوض
    string invoiceNumber = "1234567890123456789"; // شماره فاکتور
    string invoiceDate = "1392/06/31 08:10:56"; // تاریخ فاکتور
    string transRefID = "635154612243027344"; // کد رهگیری دریافتی از درگاه

    // روش اول: x-Info مراحل تولید
    string x-info = string.Format("{\"MerchCode\":\"{0}\",\"TermCode\":\"{1}\",\"InvNum\":\"{2}\",\"InvDate\":\"{3}\"}", merchantCode, terminalCode, invoiceNumber, invoiceDate);

    // روش دوم: x-Info مراحل تولید
    string x-info = string.Format("{\"TransRefID\":\"{0}\"}", transRefID);

    // Set SIP Header
    SetSipHeader("x-Info", x-info);

    // Connect to TelPayGateway
    ConnectTo("91001@" + TelPayGatewayIP);

    // Get SIP Header
    string bankInfo = GetSipHeader("x-Info");
    string bankSign = GetSipHeader("x-Sign");

    string strForCheckSign = bankInfo;

    byte[] data = Encoding.UTF8.GetBytes(strForCheckSign);
    SHA1 encoder = new SHA1Managed();
    byte[] hashData = encoder.ComputeHash(data);

    string xmlKey = "<RSAKeyValue><Modulus>..."; // Bank Public Key
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString(xmlKey);

    // Try to Check Sign And Export the result
    if(rsa.VerifyHash(hash, "SHA1", Convert.FromBase64String(bankSign)))
        // continue correctly
        invoiceObject = DeserializeJSON(bankInfo);
}

*توجه*:
```

شایان ذکر است که توابعی که وظیفه ارتباط بر بستر پروتکل SIP همچون **SetSipHeader**، **GetSipHeader** و **ConnectTo** را دارند، باید توسط سرویس دهنده پیاده سازی شوند.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۶ از ۱۹ صفحه





### پیوست ۳: الگوریتم رمز نگاری نامتقارن

الگوریتم های رمز گذاری نامتقارن نوعی از الگوریتم های رمز نگاری هستند که دارای دو کلید مختلف است که از یکی جهت رمز نگاری و از دیگری جهت رمز گشایی استفاده می شود. این الگوریتم ها در گستره وسیعی از کاربردها به کار می رود. در این الگوریتم ها کلید اول را کلید عمومی (**Public Key**) و کلید دوم را کلید خصوصی (**Private Key**) می نامند. یکی از کاربردهای مهم الگوریتم های رمز نگاری نامتقارن استفاده از آن ها در تولید امضای دیجیتال است.

#### مفهوم امضای دیجیتال :

امضای دیجیتال روشی مبتنی بر الگوریتم های رمز نگاری نامتقارن است که به کمک آن می توان اطمینان حاصل کرد که داده های ارسالی از جانب شخص مشخصی ارسال شده است. نمونه ای از این الگوریتم ها می توان به RSA و DSA اشاره کرد.

روال کار در امضای دیجیتال به این شکل است که پیش از ارسال داده ها، اطلاعات را با استفاده از الگوریتم های درهم سازی یک طرفه (Hash Algorithms) به یک کد درهم (Hash) تبدیل می شود. از نمونه این الگوریتم ها می توان به MD5, SHA1 و ... اشاره کرد. یک طرفه بودن در این الگوریتم ها به این معنی است که پس از کد شدن اطلاعات به هیچ عنوان نمی توان از روی این کدها، اطلاعات اصلی را به دست آورد. پس از در هم سازی اطلاعات، به منظور تولید امضای دیجیتال، باید از یکی از الگوریتم های رمز نگاری نامتقارن استفاده شود، و با استفاده از کلید خصوصی (**Private Key**) آن الگوریتم، رشته ی تولید شده توسط الگوریتم درهم سازی را امضا نمود.

#### مفهوم کلید عمومی و کلید خصوصی :

کلید عمومی بخشی از کلید است که بین همه توزیع می شود و هیچ نگرانی از لو رفتن و دزدیده شدن آن وجود ندارد به واقع لفظ "عمومی" نیز بیان گر همین مطلب است. اگر داده ای برای صاحب کلید عمومی (پخش کننده کلید عمومی) باید رمز شود با استفاده از این کلید رمز نگاری شده و ارسال می شود. نکته مهم الگوریتم های نامتقارن در این مطلب است که داده های رمز شده با کلید عمومی فقط و فقط با کلید خصوصی قابل رمز گشایی هستند و دوباره با همان کلید عمومی نمی توان آن ها را رمز گشایی کرد به همین دلیل داشتن کلید عمومی کمکی به رمز گشایی داده ها نخواهد کرد.

کلید خصوصی در واقع بخشی از کلید است که به وسیله آن داده های رمز شده به وسیله کلید عمومی را می توان رمز گشایی کرد. صاحب کلید خصوصی باید حداکثر محافظت از این کلید را انجام دهد و به هیچ عنوان اجازه ندهد که این کلید در دست کسی غیر از خودش قرار گیرد. علاوه بر این با استفاده از کلید خصوصی می توان اسناد و مدارک مانند Document ها، Email ها و پیغام ها را امضا کرد و امضای صورت گرفته را در انتهای Email، Document و یا پیغام قرار داد. در این حالت گیرنده پیغام با داشتن

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولید کننده: شرکت فناپ	
واحد تولید کننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۷ از ۱۹ صفحه

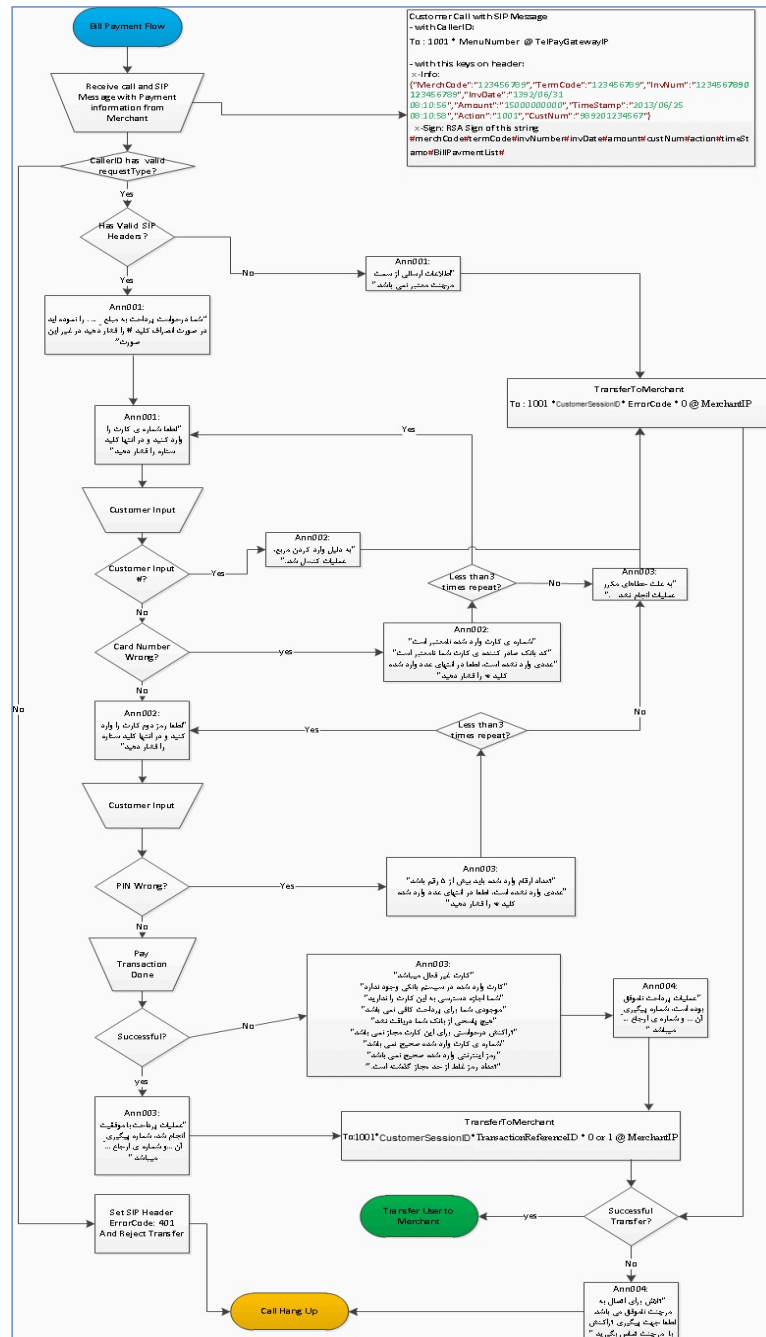


اصل پیغام، امضای دیجیتال زیر آن و کلید عمومی شما می تواند از صحت امضا اطمینان حاصل کند و مطمئن شود که داده ها از جانب شما ارسال شده است. اما با کلید عمومی به هیچ عنوان نمی تواند امضای شما را جعل کند.

عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد		سازمان تولیدکننده: شرکت فناپ	
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان		کد سند: 93-F41-SFT297-1-C	طبقه بندی: محرمانه (تجاری)
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱	شماره نسخه: ۱	صفحه ۱۸ از ۱۹ صفحه



## پیوست ۴: روال درگاه پرداخت تلفنی سمت بانک



عنوان سند: مستند فنی اتصال به درگاه پرداخت تلفنی بانک پاسارگاد	سازمان تولیدکننده: شرکت فناپ
واحد تولیدکننده: پرداخت الکترونیک - امور مشتریان	کد سند: 93-F41-SFT297-1-C
تاریخ تنظیم: ۱۳۸۸/۰۶/۱۱	آخرین به روز رسانی: ۱۳۹۳/۰۶/۱۱
شماره نسخه: ۱	صفحه ۱۹ از ۱۹ صفحه