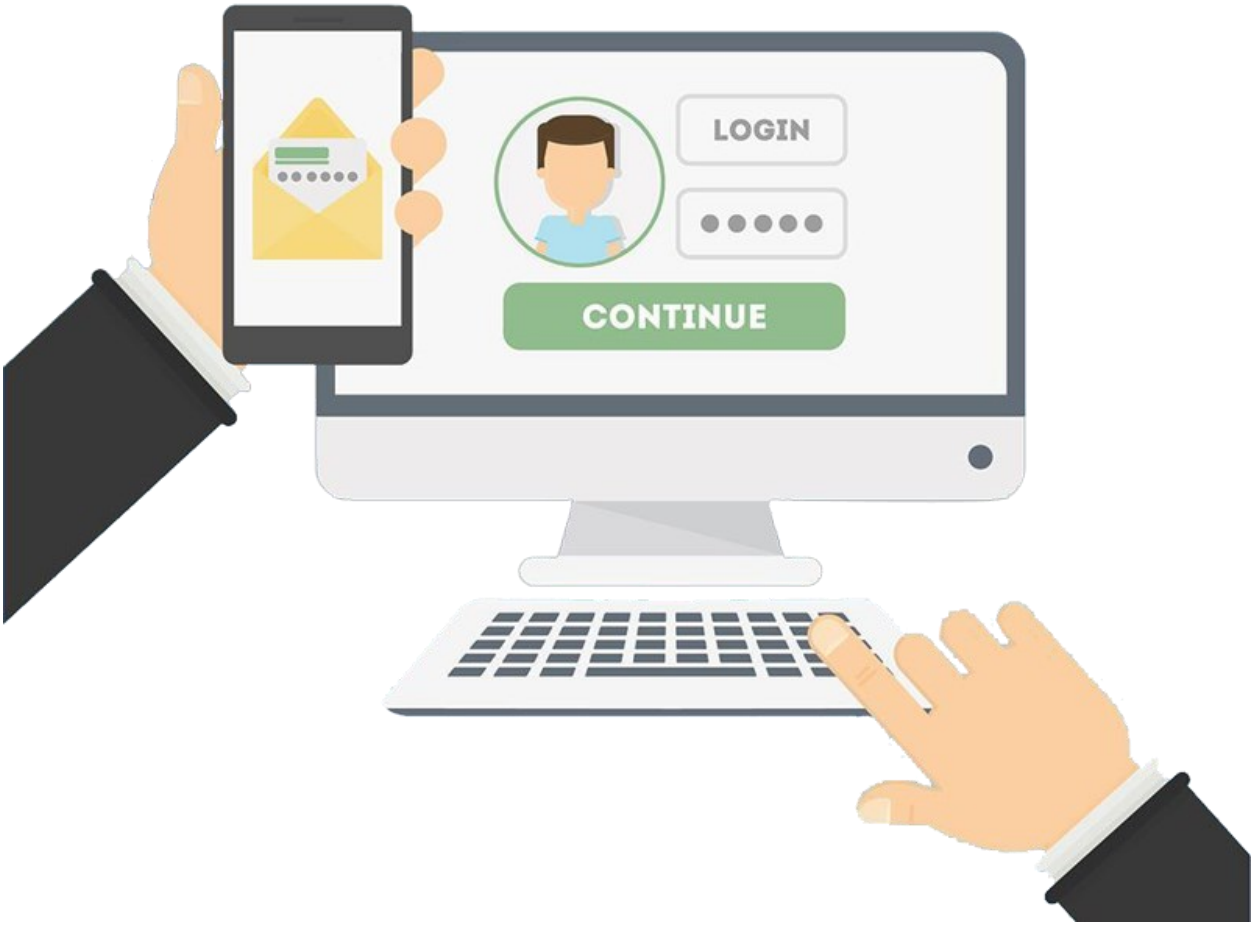
مستند اتصال به وب سرویس رمز یکبار مصرف فام



نسخه ۴.۳

تاریخ تهیه: ۱۳۹۷/۱۲/۱۵

تاریخ ویرایش: ۱۴۰۴/۰۲/۱۴

تهیه کننده: مهدی طالب

لیست تغییرات

تاریخ	نسخه	تغییرات
۱۳۹۹/۰۶/۱۵	۴.۳	اضافه شدن فیلد aquire به اعتبار سنجی رمز پویا بر اساس مستند پرسش و پاسخ شرکت کاشف، اضافه شدن فیلد description در پاسخ اعتبار سنجی/صفحه ۵

لاگین به وب سرویس

آدرس سرویس:

Http://ip:٦٩٦٦/api/v١,٠/login

داده های ورودی:

- فیلدهای اطلاعات کاربری (username , password) را در بدنه (Body) درخواست ارسال نمایید .
- توجه داشته باشید متد درخواست می‌بایست POST باشد .

```
{
    “username”: username,
    “password”: password
}
```

داده های خروجی:

- پس از فراخوانی صحیح و اجرای مراحل فوق، پاسخ سرویس(Response) ، شامل موارد زیر خواهد بود :

```
{
    "login": True,
    "token":  "token"
}
```

زمان انقضای توکن دریافتی ۱ ساعت بوده و پس از گذشت آن باید مجددا لاگین انجام گیرد.

پارامترهای ورودی

نام داده	شرح
username *	نام کاربری
password *	رمز عبور

پارامترهای خروجی

نام داده	شرح
token	توکن

درخواست فعالسازی رمزیکبارمصرف اول و دوم

آدرس سرویس:

Http://ip:٦٩٦٦/api/v١,٠ /createOTP/<pinType>

منظور از <pinType> رمز اول یا دوم می باشد:

مقدار آن باید pin١ یا pin٢ باشد.

پارامترهای ورودی (body)

نام داده	شرح
time *	زمان ارسال درخواست
cardNumber *	شماره کارت درخواست کننده
phoneNumber *	شماره موبایل درخواست کننده

پارامترهای خروجی

نام داده	شرح
key	کد اتصال به فام که باید بر روی رسید چاپ گردد.

درخواست اعتبارسنجی رمز

آدرس سرویس:

Http://ip:٦٩٦٦/api/v١,٠ /verify/<pinType>

منظور از <pinType> رمز اول یا دوم می باشد:

مقدار آن باید pin١ یا pin٢ باشد.

پارامترهای ورودی(body)

نام داده	شرح
time*	زمان ارسال درخواست
cardNumber*	شماره کارت درخواست کننده
pin*	رمز وارد شده
amount*	مبلغ تراکنش
acceptorTerminalId*	شماره پایانه
acceptorId*	شناسه پذیرنده
prCode*	کد پردازش تراکنش
terminalTypeCode*	کد نوع پایانه
nationalCode*	کد ملی صاحب کارت
cardAcceptorName*	نام پذیرنده کارت
cardAcceptorId*	شماره شناسایی پذیرنده کارت
requesterId*	**شناسه موسسه درخواست کننده**
acquire*	شناسه پذیرنده کارت

پارامترهای خروجی

نام داده	شرح
verify	مقداری این متغییر Boolean است که اعتبار یا عدم اعتبار رمز را مشخص می کند.
description	در صورتی که تراکنش با درخواست رمز پویا انطباق نداشته باشد.

درخواست ارسال پیامک تولید رمز به مشتری

آدرس سرویس:

Http://ip:٦٩٦٦/api/v١,٠ / requestOtpInternal/<pinType>

منظور از <pinType> رمز اول یا دوم می باشد:

مقدار آن باید pin١ یا pin٢ باشد.

پارامترهای ورودی(body)

نام داده	شرح
time*	زمان ارسال درخواست
trace*	کد پیگیری
amount*	مبلغ
terminalTypeCode*	**کد نوع پایانه**
prCode*	کد پردازش تراکنش
cardAcceptorId*	شماره شناسایی پذیرنده کارت
pan*	شماره کارت درخواست کننده
expireDate	تاریخ انقضا
cardAcceptorName*	نام پذیرنده کارت
cardAcceptorUrl	آدرس اینترنتی پذیرنده
acceptorTerminalId*	**شماره شناسایی پذیرنده**
otpRequesterId*	**شناسه موسسه درخواست کننده رمز پویا**
acquire*	**شناسه پذیرنده کارت**

پارامترهای خروجی

نام داده	شرح
status	مقدار صفر موفق خواهد بود. مقدار غیر صفر با کد های خطا مشابه است.

با توجه به نامه بانک مرکزی مبنی بر استاندارد سازی پیامک های رمز دوم پویا مقادیر ورودی های زیر از سوی پذیرندگان (اینترنت بانک، همراه بانک، تلفن بانک و...) باید به شکل استاندارد ارسال شوند:

۱- نوع تراکنش:

نوع تراکنش	prCode
خرید	۰۰
انتقال	۴۶
پرداخت	۵۰
شارژ	۵۰
مانده گیری	۳۱
گردش حساب	۳۴
فراموشی رمز اینترنت بانک	۹۹

۲- دریافت کننده وجه:

نوع تراکنش	مقدار cardAcceptorName
خرید	نام پذیرنده
انتقال	شماره کارت مقصد
پرداخت قبض	نام سازمان دریافت کننده وجه قبض
پرداخت قسط	نام سازمان دریافت کننده قسط یا عنوان تسهیلات ارئه شده
شارژ	شماره تلفن همراه اظهار شده

نکته: در فراموشی رمز اینترنت بانک مبلغ تراکنش مقدار صفر ارسال شود.

۳- **مبلغ:** فیلد مبلغ تراکنش باید بدرستی پر شده باشد.

لیست خطاها

Response ٤٠٠:

errorCode	errorMessage
۵	messageStructureError
۷	timeException
۸	sessionExpired/tokenExpire
۱۰	beforeActived
۱۱	bankNotExist
۱۳	noResult
۱۵	bankNotValid

خطای ۴۰۴ یافت نشد

خطای ۵۰۰ خطای ناشناخته

نحوه رمزنگاری

بجز سرویس لاگین در مابقی سرویس ها کلیه پیام ها به صورت رمزنگاری شده تبادل می گردد. در این رمزنگاری از الگوریتم AES و mode CBC استفاده می شود و کلید رمزنگاری به شکل زیر ساخته می شود:

Key=(Token xor md۵(username+md۵(password))) xor p۱

P۱ کدی است که برای هر آی پی در زمان ایجاد نام کاربری ساخته می شود.