مستندات فنی و پروتکل ارتباط با نت بی پوز

نسخه سند 1.5 سازگار با نت پوز 1.5.0

آخرین ویرایش: 1403/04/13 توسط محمد استکی

فهرست

نصب و تنظیم

ابتدا از طریق پشتیبانی از نصب بودن برنامه نت بی پوز بر روی دستگاه خود اطمینان حاصل کنید. پروتکل خرید تحت شبکه در پوز را فعال کنید. البته این موضوع در ارائه دهنده های مختلف اسم های متفاوتی دارد (انجام این امر نیازمند ارتباط با پشتیبانی ارائه دهنده پوز است). از اتصال پوز و دستگاه به یک شبکه دارای اینترنت پایدار اطمینان حاصل کنید. سپس تنظیمات پوز در برنامه (مانند IP) را با توجه به پوز نصب شده روی دستگاه خود، اعمال کنید.

اگر فقط نیاز به تست اتصال پوز دارید باید در بخش امنیت کلید عمومی نت را در جای کلید عمومی شما کپی کرده و ذخیره کنید.

برای ذخیره سازی اطلاعات و آزمایش اتصال میتوانید یک عدد دلخواه را وارد کرده و روی پرداخت کلیک کنید. دیالوگ تایید اطلاعات پرداخت باز خواهد شد که با کلیک روی پرداخت، اطلاعات خرید روی پوز نمایش داده میشود. اگر اطلاعات را روی پوز مشاهده نکردید بار دیگر مراحل بالا را بررسی کنید.

کیف پول

اگر از کیف پول کاینو استفاده میکنید فیلدهای آن را با استفاده از مشخصات دریافتی از کاینو تکمیل کنید.

نحوه ارتباط

پلتفرم ارتباط با نت بی پوز بر پایه سوکت تحت شبکه است. اطلاعات اتصال شامل موارد زیر است.

آدرس: 0.0.0.0 یا 127.0.0.1 یا همان localhost

پورت: 2448

درخواست ها

تمامی درخواست های قابل اجرا در ادامه توضیح داده میشود. درخواست ها در قالب JSON به صورت رشته و تک خطی میباشد. توجه داشته باشید باید در انتهای رشته JSON کاراکتر \n را اضافه کنید. قالب کلی درخواست ها به شکل زیر است.

نام	توضیحات	نوع	اجباری
type	نوع درخواست که یکی از مقادیر زیر است: payment_request	رشته	☑
data	داده ها که بر اساس درخواست متفاوت است	متغیر	☑

درخواست خرید

برای ارسال درخواست خرید، موارد زیر در آبجکت data و در قالب json ارسال میشود.

نام	توضیحات	نوع	اجباری
amount	مبلغ تراکنش	عدد (به ریال)	☑
stan_id	شناسه یکتا برای شناسایی تراکنش	رشته	☑
payload	فیلدی اختیاریست که از آن برای تفکیک درخواست ها استفاده میشود. هرچیزی که در آن قرار گیرد همان مقدار در پاسخ ارسال میشود.	رشته	☒

sign	امضای قالب #amount, stan_id ,payload# به وسیله کلید خصوصی برای اطلاعات بیشتر به بخش امنیت مراجعه کنید	رشته	☑
entity_type	نوع شی که برای خرید، مقدار payment_request است.	رشته	☑

رویداد ها

در زمان یک رویداد، اطلاعاتی برای شما ارسال میشود که قالب آن در جدول زیر آمده است. توجه داشته باشید که بعد از دریافت هر رویداد سوکت بسته شده و برای درخواست جدید مجددا باید به سوکت متصل شوید.

نام	توضیحات	نوع	اجباری
type	نوع رویداد که یکی از مقادیر زیر است: payment_success, payment_failed	عدد (به ریال)	☑
data	داده های رویداد (با توجه به هر رویداد داده آن متفاوت است)	متغیر	☑

رویداد payment_success

در صورت پرداخت موفق آمیز، رویداد payment_success فراخوانی میشود که فیلد data به صورت زیر خواهد بود.

نام	توضیحات	نوع	اجباری
amount	مبلغ تراکنش	عدد (به ریال)	☑
rrn	کد مرجع	رشته	☑
serial	سریال تراکنش	رشته	☑
trace	کد رهگیری (ممکن است در بعضی پوز ها همان کد پیگیری باشد)	رشته	☑
card_number	شماره کارت خریدار	رشته	☑
datetime	تاریخ و ساعت (در پوز های مختلف فرمت آن متغیر است)	رشته	☑
stan_id	شناسه یکتا برای شناسایی تراکنش	رشته	☑
payload	فیلدی اختیاریست که از آن برای تفکیک درخواست ها استفاده میشود. هرچیزی که در آن قرار گیرد همان مقدار در پاسخ ارسال میشود.	رشته	☒
sign	امضای قالب #amount,rrn,serial,trace,card_number,datetime,stan_id, payload# برای اطلاعات بیشتر به بخش امنیت مراجعه کنید	رشته	☑

رویداد payment_failed

در صورت هرگونه خطا و لغو پرداخت، رویداد payment_failed فراخوانی میشود که فیلد data به صورت زیر خواهد بود.

نام	توضیحات	نوع	اجباری
error	متن خطا	رشته	✓
stan_id	شناسه یکتا برای شناسایی تراکنش	رشته	✓
payload	فیلدی اختیاریست که از آن برای تفکیک درخواست ها استفاده میشود. هرچیزی که در آن قرار گیرد همان مقدار در پاسخ ارسال میشود.	رشته	✗
sign	امضای قالب #error,stan_id ,payload# برای اطلاعات بیشتر به بخش امنیت مراجعه کنید	رشته	✓

امنیت

برای امنیت بیشتر و اعتبارسنجی درخواست ها و رویداد ها بین سرور و کلاینت سوکت، هر کدام از آن ها توسط ارسال کننده امضا میشوند. این امضا با استفاده از کلید خصوصی با **الگوریتم SHA256ECDSA** انجام میشود. در نتیجه شما باید یک جفت کلید خصوصی/عمومی با **الگوریتم EC-prime256v1** ایجاد کنید.

کلید عمومی نت بی

شما باید از کلید عمومی نت بی، **الگوریتم SHA256ECDSA** و امضا، برای اعتبارسنجی اطلاعات دریافتی از سوکت، استفاده کنید. کلید عمومی نت بی را میتوانید از بخش امنیت برنامه کپی کرده و در جای امن سمت خودتان ذخیره کنید.

کلید عمومی شما

کلید عمومی خود را در نت بی پوز، بخش **امنیت -> کلید عمومی شما**، وارد کرده و ذخیره کنید. ما از کلید عمومی شما برای اعتبارسنجی درخواست هایی که از سمت شما ارسال میشود، استفاده میکنیم.

توجه داشته باشید که در صورت وارد کردن کلید عمومی خودتان، امکان پرداخت در برنامه نت بی پوز وجود نخواهد داشت. البته این امکان صرفا جهت تست اتصال پوز است و استفاده دیگری ندارد.

روش های مختلفی برای ساخت جفت کلید خصوصی/عمومی وجود دارد. ساده ترین آن مراجعه به سایت fyicenter است. پیشنهاد میشود که خودتان به صورت programmatically کلید را ایجاد کنید.

امضای درخواست

شما باید از کلید خصوصی خودتان برای امضای درخواست ها استفاده کنید. تمامی پارامتر های داخل درخواست در قالب زیر قرار گرفته سپس با کلید خصوصی و **الگوریتم SHA256WithECDSA** امضا میشود.

#parameter1,parameter2,parameterN#

به عنوان مثال درخواست خرید 10000 ریال را به پوز سداد در نظر بگیرید.

```
{
        “type”: “payment_request”,
        “data” :  {
                “amount” : 10000,
                “stan_id” : “29935e1e-634a-417c-95f9-437ae1c0f972”
                “payload” : ”factor_id=A1”
        }
}
```

قالب امضا با توجه به اطلاعات بالا به شکل زیر است. توجه داشته باشید که ترتیب قرار دادن پارامتر مهم است و باید به همین ترتیب باشد.

```
#10000 , 29935e1e-634a-417c-95f9-437ae1c0f972,factor_id=A1#
```

بعد از امضا به عنوان مثال نتیجه MY_SIGN شده است. درخواست نهایی شما باید به شکل زیر باشد.

```
{
        “type”: “payment_request”,
        “data” : {
                “amount” : 10000,
                “stan_id” : “29935e1e-634a-417c-95f9-437ae1c0f972”
                “payload” : ”factor_id=A1”,
                “sign” : “MY_SIGN”
        }
}
```