

ضوابط و مقررات شا پرک

پروتکل رمزنگاری دادههای اطلاعات هویتی دارنده کارت

جهت پیادهسازی توسط ذینفعان مجاز

کد مستند: SHP_INS_NIOPDC_CRDINQ

ويرايش: 01.00

14-1/-0/-4



ضوابط و مقررات شاپرک_پروتکل رمزنگاری دادههای اطلاعات هویتی دارنده کارت-جهت پیادهسازی توسط ذینفعان مجاز



شناسنامهی مستند	
شبکه الکترونیکی پرداخت کارت-شاپرک	نگارنده
پروتکل رمزنگاری دادههای اطلاعات هویتی دارنده کارت	عنوان مستند
SHP_INS_NIOPDC_CRDINQ	کد مستند
01.00	شماره ویرایش
14.1/.۵/.٣	تاریخ تدوین/بازنگری
محرمانه	طبقهبندی محرمانگی
بلافاصله پس از ابلاغ	تاريخ اجرا
بلافاصله پس از ابلاغ	تاريخ مؤثر سند
جهت پیادهسازی توسط ذینفعان مجاز	جامعه هدف
ندارد.	مراجع
ندارد.	مدارک ذیربط

صفحهی ۲ از ۹	SHP_INS_NIOPDC_CRDINQ	14.1/.0/.4	ويرايش 01.00

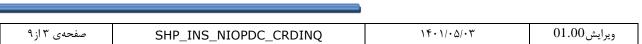


كنترل نسخ مستندات

نگارنده	تاریخ بازنگری	موضوع بازنگری	شماره ویرایش
_	-	تاکنون بازنگری نشده است.	-

جدول ثبت تغییرات مدرک (مربوط به آخرین نسخه)

نگارنده	تاریخ بازنگری	تغييرات اعمال شده	محل تغيير	صفحه	شماره ت غ ییر
_	-	-	-	-	-

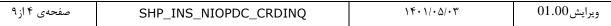




پیادهسازی توسط ذینفعان مجاز

فهرست مطالب

۶	۱– مقدمه
9	٢- اهداف
۶	٣– كاربران
9	۴– تعاریف
۶	1-۴ شرکت شاپرک
۶	۲-۴ شرکت ارائه دهنده خدمات پرداخت
Υ	۵- شرح
	۵–۱– نکات فنی
Υ	۱-۵-۱ کوته واژههای مورد استفاده در مستند
۸	۵-۱-۲ ساختار کلی اطلاعات هویتی پس از رمزگشایی
	2-4 جداول پایه
٩	1–۲–۵ جدول شناسه هو <i>بتی</i>

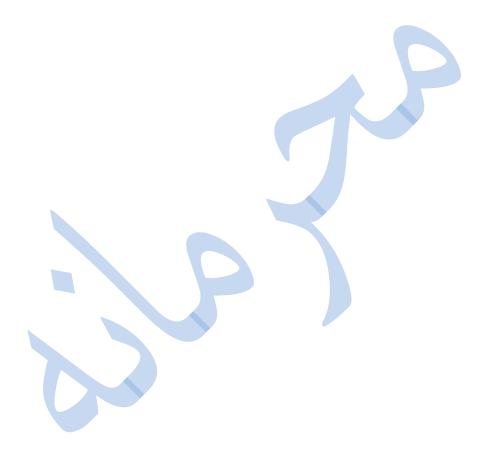




ضوابط و مقررات شاپرک_پروتکل رمزنگاری دادههای اطلاعات هویتی دارنده کارت-جهت پیادهسازی توسط ذینفعان مجاز

فهرست جداول

1	ندول ۱: انواع اقلام دادهای
٩	ـدول ۲: ساختار کلی رشته اطلاعات هویتی رمزگشایی شده
٩	ىدول ٣: جدول شناسه هو ىتى



SHP_INS_NIOPDC_CRDINQ ۱۴۰۱/۰۵ صفحه ی ۵ از ۹	ويرايش 01.00
---	--------------



پیادهسازی توسط ذینفعان مجاز

۱- مقدمه

مستند حاضر به ساختار اطلاعات هویتی دارنده کارت ارسالی به شرکتهای پرداخت جهت استفاده توسط ذینفعان مجاز می پردازد. شرکت شاپرک جهت احراز هویت این اطلاعات، براساس مقررات، اطلاعات هویتی ارسالی را با شماره کارت دریافتی از شرکتهای پرداخت بیز شرکتهای پرداخت بیز مرکزی تطبیق می دهد. شرکتهای پرداخت نیز اطلاعات دریافت شده از ذینفع را به صورت رمزنگاری شده و بدون دخل و تصرف به شرکت شاپرک ارائه می نمایند.

۲- اهداف

هدف از تدوین این مستند، ارائه رو شی یکپارچه و امن به منظور رمزنگاری اطلاعات هویتی دارنده کارت و ار سال این اطلاعات به شرکتهای پرداخت، در راستای اعتبارسنجی اطلاعات هویتی دارنده کارت توسط شرکت شاپرک میباشد.

۳- کاربران

کاربران این سند، ذینفعان سرویس احراز هویت اطلاعات دارنده کارت میباشند. جهت استفاده از سرویس مذکور، نیاز است ذینفع از شرکت شاپرک مجوز دریافت کند.

۴- تعاریف

4-1- شرکت شاپرک

شبکه الکترونیکی پرداخت کارت «شاپرک»، شبکهای است که به منظور ساماندهی نظام پرداخت در کشور ایجاد شده و کلیه تراکنشهای حاصل از «ابزارهای پذیرش» توسط این شبکه نظارت و کنترل میشود و به طور کلی نظارت بر عملکرد فنی و اجرایی را برعهده دارد.

۲-۴ شرکت ارائه دهنده خدمات پرداخت

شخصیت حقوقی است که در جمهوری اسلامی ایران در قالب شرکت سهامی به ثبت رسیده و براساس موافقتنامه منعقده با شرکت شاپرک و بر طبق مقررات ناظر بر ارائهدهندگان خدمات پرداخت و دستورالعملها و الزامات ابلاغی بانک مرکزی و شرکت شاپرک فعالیت مینماید.





۵- شرح

سرویس احراز هویت مالک کارت به منظور بررسی تطبیق اطلاعات هویتی رمزنگاری شده دارندگان کارت طراحی و پیادهسازی گردیده است. علاوه بر پاسخ وضعیت احراز هویت، تاریخی به شرکتهای ارائه دهنده خدمات پرداخت ارائه میشود که زمان اعتبار استعلام انجام شده را مشخص می کند. شرکتهای پرداخت می توانند نتیجه استعلام را موقتا و صرفا در بازه اعتبار نتیجه استعلام ذخیره نموده و از استعلام مجدد در این بازه در صورت در دسترس نبودن سرویس اجتناب نمایند. این اطلاعات در نهایت بدون دخل و تصرف در لحظه صورت گیری از طریق کارت بانکی توسط شرکتهای پرداخت در اختیار ذینفع سرویس قرار می گیرد.

۵–**۱-** نکات فنی

نکات ذیل پیرو پیادهسازی کلی فنی قابل ذکر است:

- در تمامی موارد قالب String های ارسالی UTF-8 می باشد.
- منظور از Timestamp تعداد ثانیههای سپری شده از تاریخ مبدا ۱۹۷۰/۰۱/۰۱ میلادی به مرجع UTC میباشد که همواره به صورت عددی ارائه می گردد.
 - در این مستند مرجع اصلی پیاده سازی، جداول بوده و نمونه های ارائه شده صرفا جنبه اطلاعات تکمیلی دارند.

۵-۱-۱- کوته واژههای مورد استفاده در مستند

با توجه به اینکه در ساختار پیشبینی شده، صرفا شش نوع کلی داده وجود خواهد داشت، در جداول زیر اقلام اطلاعاتی رشتهای به اختصار 'S، اقلام اطلاعاتی عددی به اختصار 'N، اقلام اطلاعاتی دو انتخابی (بولین) به اختصار 'S، اقلام اطلاعاتی عددی به اختصار (شامل تاریخ و زمان) که دقت آن تا ثانیه میباشد به اختصار T، اشیاء که خود شامل تعدادی فیلدهای اطلاعاتی میباشند به اختصار 'O، و فیلدهای آرایهای که شامل مجموعهای از سایر اقلام اطلاعاتی میباشند، به اختصار 'A در جداول نمایش داده شده است.

[†] Number

[\] Sting

^τ Boolean

[†] Object

^a Array





عنوان	اختصار	ردیف
رشته	S	١
عدد	N	۲
دو انتخابی (بولی)	В	٣
تاریخ و زمان	Т	۴
شىء	0	۵
آرایه	А	۶

جدول ۱: انواع اقلام دادهای

لازم به ذکر است، برای اقلام اطلاعاتی رشته ای یا عددی، در داخل پرانتز، حداقل و حداکثر طول قابل قبول فیلدهای اطلاعاتی نیز ذکر گردیده است. به عنوان مثال اگر فیلدی از جنس رشته ای با حداقل طول ۸ کاراکتر و حداکثر طول ۶۴ کاراکتر باشد، به اختصار (8,64) در جدول نمایش داده می شود.

۵-۱-۲- ساختار کلی اطلاعات هویتی پیش از رمزنگاری

در این بخش به طور کلی ساختار اطلاعات هویتی ارسالی به شرکتهای پرداخت پیش از رمزنگاری توضیح داده می شود. پیش از رمزنگاری اطلاعات هویتی ارسالی به شرکت پرداخت، به ترتیب از چپ به راست، نوع شخصیت، شناسه هویتی و رشتهی گسترش تصادفی وجود دارد. در رشتهی ارسالی این اقلام توسط کاراکتر pipe یا نمایه "|" از هم تفکیک شده اند.

PersonalityType|NationalId|RandomSalt

- کاراکتر جداکننده (Separator) در تولید رشته پایه، "|" (PIPE) میباشد.
 - پیغام تولید شده پس از رمزنگاری با قالب Base-64 کد شده است.
- نمونه پیغام رمزگشایی شده به همراه کلید رمزنگاری عملیاتی، بردار اولیه (iv) عملیاتی و نمونه دیتای صحیح جهت
 آزمون عملکرد، در قالب محرمانه مورد توافق، تقدیم حضور خواهد گردید.
 - براى رمزنگارى اطلاعات از الگوريتم AES/CBC/PKCS5Padding با طول كليد ۱۲۸ استفاده مى شود.

صفحهی ۸ از ۹	SHP_INS_NIOPDC_CRDINQ	14.1/.0/.4	ويرايش 01.00



ساختار کلی فیلدهای موجود در محتوای رمزگشایی شده به شرح ذیل می باشد:

توضيحات	نوع فيلد	نام فارسی	نام فیلد	ردیف
نوع شخصیت دارنده کارت در این فیلد ذخیره می شود و مطابق جدول شناسه هویتی تکمیل می گردد.	N(1,1)	نوع شخصیت	PersonalityType	١
شناسه هویتی دارنده کارت در این فیلد ذخیره می شود. در این فیلد برای اشخاص حقیقی ایرانی کد ملی ۱۰ رقمی، برای اشخاص حقوقی ۱۱ رقمی و اشخاص حقوقی ایرانی، شناسه ملی اشخاص حقوقی ۱۱ رقمی برای اتباع خارجی، شناسه فراگیر اتباع خارجی ۱۰ تا ۱۶ رقمی درج می گردد.	S(10,16)	شناسه هویتی	NationalId	۲
رشتهی گسترش تصادفی در این فیلد ذخیره می شود و تنها کاربرد آن جلوگیری از امکان dictionary attack و امنسازی بیشتر دادهها می باشد.	N(1,7)	رشتهی گسترش تصادفی	RandomSalt	٣

جدول ۲: ساختار کلی رشته اطلاعات هویتی رمزگشایی شده

۵-۲**-** جداول پایه

۵-۲-۱- جدول شناسه هویتی

عنوان	مقدار	ردیف
حقیقی ایرانی	•	١
حقوقی ایرانی	١	۲
اتباع خارجى	٢	٣

جدول ۳: جدول شناسه هویتی