شاپرک

شرکت شبکه الکترونیکی پرداخت کارت (سهامی خاص)

ضوابط و مقررات شاپرک

پروتکل رمزنگاری داده‌های اطلاعات هویتی دارنده کارت

جهت پیاده‌سازی توسط ذینفعان مجاز

محرمانه

کد مستند: SHP_INS_NIOPDC_CRDINQ

ویرایش: 01.00

۱۴۰۱/۰۵/۰۳

بسم الله الرحمن الرحیم

شناسنامه‌ی مستند	
نگارنده	شبکه الکترونیکی پرداخت کارت-شاپرک
عنوان مستند	پروتکل رمزنگاری داده‌های اطلاعات هویتی دارنده کارت
کد مستند	SHP_INS_NIOPDC_CRDINQ
شماره ویرایش	01.00
تاریخ تدوین/بازنگری	۱۴۰۱/۰۵/۰۳
طبقه‌بندی محرمانگی	محرمانه
تاریخ اجرا	بلافاصله پس از ابلاغ
تاریخ مؤثر سند	بلافاصله پس از ابلاغ
جامعه هدف	جهت پیاده‌سازی توسط ذینفعان مجاز
مراجع	ندارد.
مدارک ذیربط	ندارد.

محرمانه

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

کنترل نسخ مستندات

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

جدول ثبت تغییرات مدرک (مربوط به آخرین نسخه)

شماره تغییر	صفحه	محل تغییر	تغییرات اعمال شده	تاریخ بازنگری	نگارنده
-	-	-	-	-	-

محرمانه

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

فهرست مطالب

۱- مقدمه ۶
۲- اهداف ۶
۳- کاربران ۶
۴- تعاریف ۶
۴-۱- شرکت شاپرک ۶
۴-۲- شرکت ارائه دهنده خدمات پرداخت ۶
۵- شرح ۷
۵-۱- نکات فنی ۷
۵-۱-۱- کوته واژه‌های مورد استفاده در مستند ۷
۵-۱-۲- ساختار کلی اطلاعات هویتی پس از رمزگشایی ۸
۵-۲- جداول پایه ۹
۵-۲-۱- جدول شناسه هویتی ۹

محرمانه

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

فهرست جداول

جدول ۱: انواع اقلام داده‌ای ۸
جدول ۲: ساختار کلی رشته اطلاعات هویتی رمزگشایی شده..... ۹
جدول ۳: جدول شناسه هویتی..... ۹

محرمانه

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۱- مقدمه

مستند حاضر به ساختار اطلاعات هویتی دارنده کارت ارسالی به شرکت‌های پرداخت جهت استفاده توسط ذینفعان مجاز می‌پردازد. شرکت شاپرک جهت احراز هویت این اطلاعات، براساس مقررات، اطلاعات هویتی ارسالی را با شماره کارت دریافتی از شرکت‌های پرداخت با مراجعه به داده‌های دارندگان کارت موجود در مجموعه بانک مرکزی تطبیق می‌دهد. شرکت‌های پرداخت نیز اطلاعات دریافت شده از ذینفع را به صورت رمزنگاری شده و بدون دخل و تصرف به شرکت شاپرک ارائه می‌نمایند.

۲- اهداف

هدف از تدوین این مستند، ارائه روشی یکپارچه و امن به منظور رمزنگاری اطلاعات هویتی دارنده کارت و ارسال 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

۴-۱- 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.

۴-۲- 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.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

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 می‌کند. شرکت‌های پرداخت می‌توانند 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 صورت‌گیری از طریق کارت بانکی توسط شرکت‌های پرداخت در اختیار ذینفع سرویس قرار می‌گیرد.

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 می‌گردد. این عدد برای تاریخ‌های پیش از مبدا یاد شده به صورت منفی ارائه می‌گردد.
- در این مستند مرجع اصلی پیاده‌سازی، جداول بوده و نمونه‌های 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[۱]، اقلام اطلاعاتی عددی به اختصار N[۲]، اقلام اطلاعاتی دو انتخابی (بولین) به اختصار B[۳]، اقلام اطلاعاتی Timestamp (شامل تاریخ و زمان) که دقت آن تا ثانیه می‌باشد به اختصار T، اشیاء که خود شامل تعدادی فیلدهای اطلاعاتی می‌باشند به اختصار O[۴] و فیلدهای آرایه‌ای که شامل مجموعه‌ای از سایر اقلام اطلاعاتی می‌باشند، به اختصار A[۵] در جداول نمایش داده شده است.

[۱] Sting
[۲] Number
[۳] Boolean
[۴] Object
[۵] Array

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

ردیف	اختصار	عنوان
۱	S	رشته
۲	N	عدد
۳	B	دو انتخابی (بولی)
۴	T	تاریخ و زمان
۵	O	شیء
۶	A	آرایه

جدول ۱: انواع اقلام داده‌ای

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

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 می‌شود.

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 شده‌اند.

```
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.
- برای رمزنگاری اطلاعات از الگوریتم AES/CBC/PKCS5Padding با طول کلید ۱۲۸ استفاده می شود.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

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

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

جدول ۲: ساختار کلی رشته اطلاعات هویتی رمزگشایی شده

۵-۲- جداول پایه

۵-۲-۱- جدول شناسه هویتی

ردیف	مقدار	عنوان
۱	۰	حقیقی ایرانی
۲	۱	حقوقی ایرانی
۳	۲	اتباع خارجی

جدول ۳: جدول شناسه هویتی

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.