پرداخت نوین آرین

نام مستند:	کلیدگذاری دستگاه (PAXD 180) MPOS
شماره مستند:	01.00
سطح محرمانگی:	عمومی
محل نگهداری:	
تعداد صفحات:	8
تاریخ آخرین اصلاح:	96/09/18
شماره بازنگری:	1

تهیه کننده: زیبا زینلی	تأیید کننده: امیر افشانی	تصویب کننده: علیرضا آقاخانی
امضاء:	امضاء:	امضاء:
تاریخ:	تاریخ:	تاریخ:

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.

تاریخچه‌ی اصلاحات

بازنگری	تاریخ	اقدام کننده	شرح تغییرات
1	96/09/18	پریسا راستا	ایجاد مستند

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.

فهرست

- هدف 4
- مدیریت کلیدها با استفاده از مکانیزم **DUKPT** 4
- تولید کلید **DUKPT** در مرکز مدیریت ترمینال 4
- کلید گذاری ترمینال با کلید اصلی (مستر) 6
- تراکنش **LOG ON** و دریافت کلید اولیه **INITIALIZE ENCRYPTION KEY** 6
- رمز نگاری تراکنش ها با استفاده از **DUKPT** در ترمینال 6
- بررسی و رمز گشایی تراکنش ها در سوئیچ 7
- استراتژی تغییر کلید **DUKPT** ترمینال ها 7

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.

هدف

این مستند نحوه ی بارگذاری کلید روی دستگاه MPOS متعلق به شرکت پرداخت نوین آرین را نشان می دهد.

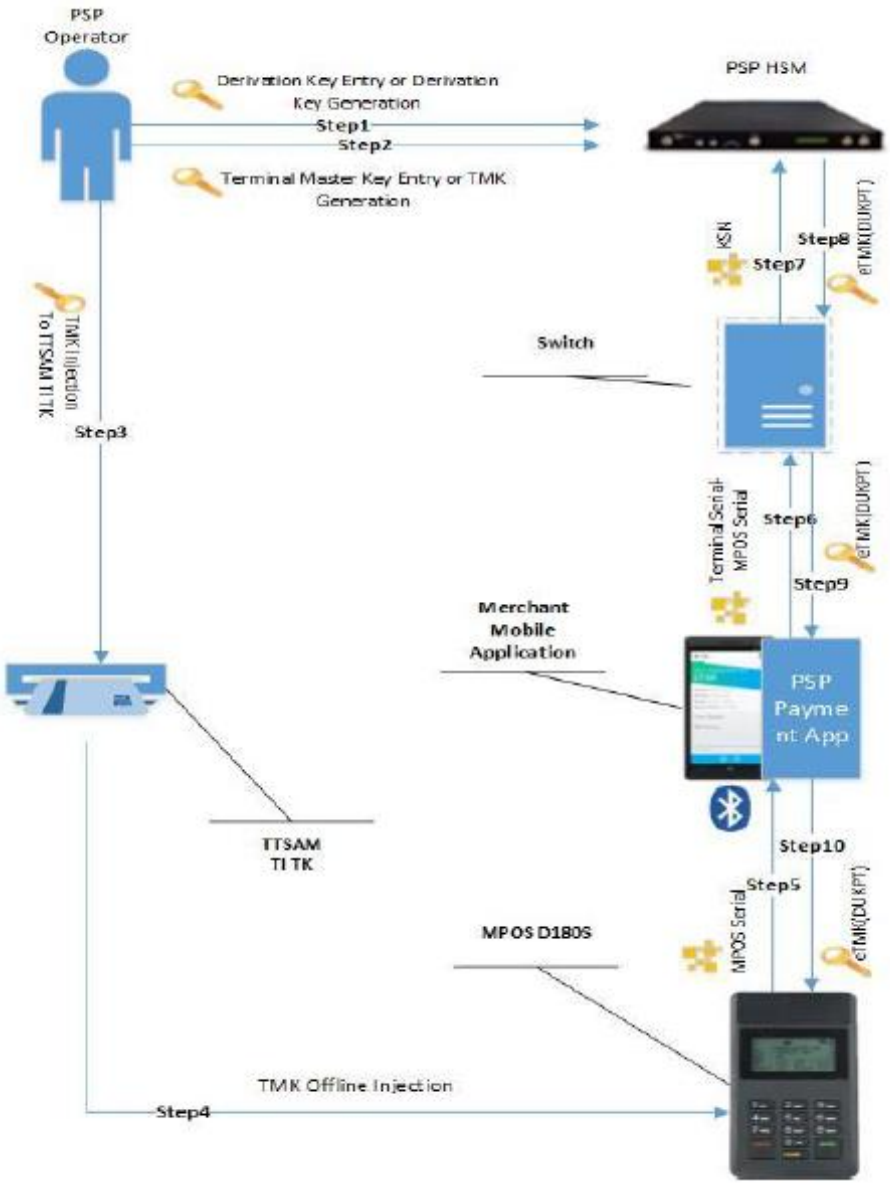
مدیریت کلیدها با استفاده از مکانیزم DUKPT

از آنجایی که در راهکار مرتبط با MPos در مسیر انجام تراکنش از نقطه ی تولید تراکنش (ترمینال) تا سوئیچ پذیرنده، ممکن است نقاط و دستگاه های واسط همانند تجهیز هوشمند (تلفن همراه هوشمند) فروشنده و یا سرور های مدیریت کسب و کار فروشنده نیز قرار گرفته باشند، امکان لاگ گیری از اطلاعات تراکنش و یا اطلاعات حساس دارنده ی کارت ، در جهت تکرار آن در زمان های آتی، وجود دارد.از طرف دیگر به دلیل استاتیک بودن اطلاعات رمز اول کارت و اطلاعات کارت مشتری ، این امکان برای دستگاه های واسط ایجاد می شود که از اطلاعات دارنده ی کارت سوء استفاده شده و با استفاده از آن اطلاعات ، تراکنش ها را تکرار نمایند.جهت برطرف شدن این دغدغه و از بین بردن حفره ی امنیتی ، راهکار استفاده از" کلید مشتق شده (موقت) به ازای هر تراکنش" ارائه شده است.در این روش که DUKPT نام دارد، ترمینال قادر خواهد بود تا بر اساس اطلاعات متغیری همچون یک شمارنده ی مشترک با سوئیچ ، به ازای هر تراکنش، یک کلید موقت و یکبار مصرف تولید نماید و اطلاعات حساس دارنده ی کارت با این کلید موقت و یکبار مصرف ، رمز نگاری کند. کلید مشتق شده فقط برای تراکنش جاری معتبر است و اطلاعات حساس کاربر در تراکنش های قبلی و بعدی نیز، به خطر نمی افتد.اصول مدیریت کلید DUKPT در سمت مرکز و ترمینال به شرح ذیل می باشد:

تولید کلید DUKPT در مرکز مدیریت ترمینال

در مرکز مدیریت ترمینال و با استفاده از HSM ،ابتدا Derivation Key در HSM ذخیره می گردد.این کلید در نقش پدر کلیدهای اولیه ی ترمینال ها خواهد بود.به ازای هر ترمینال نیز یک داده ی 10 بایتی Key Serial Number تعریف می گردد.متغیرKSN از دو قسمت "اطلاعات ترمینال " و "شمارنده ی رمزنگاری" تشکیل شده است.برای هر ترمینال و با استفاده از کلید پدر DK و داده ی منحصر به فرد همان ترمینال ، KSN ، یک DUKPT Key تولید می گردد. این کلید که با استفاده از اطلاعات منحصر به فرد ترمینال و از کلید اصلی DK ، مشتق شده است، برای هر ترمینال منحصر به فرد است.

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.



شمای کلیدگذاری DUKPT

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.

کلید گذاری ترمینال با کلید اصلی (مستر)

با استفاده از کارت های هوشمند TK(Terminal Key) و TI(Terminal Initializer) ، کلید مستر ترمینال در ترمینال ها، کلیدگذاری می گردد.به همین منظور از راهکار پرداخت نوین برای بارگذاری آفلاین کلید مستر ترمینال ها استفاده شده است.

تراکنش Log On و دریافت کلید اولیه Initialize Encryption Key

در زمان پیکربندی ترمینال و با استفاده از تراکنش Log On، DUKPT Key برای ترمینال ارسال می گردد. این کلید توسط کلید مستر ترمینال، رمز نگاری شده است.ترمینال پس از دریافت کلید رمز نگاری شده ی DUKPT ، آنرا داخل حافظه ی SE خود تزریق می نماید و در داخل حافظه ی SE ترمینال ، مقدار کلید رمز شده ی DUKPT توسط کلید مسترترمینال، رمزگشایی و در داخل SE ترمینال ، ذخیره می گردد.

همچنین همراه با پاسخ تراکنش Log On ، داده ی KSN نیز به ترمینال ارسال می گردد که مقدار KSN نیز در داخل SE ترمینال ، ذخیره می گردد.

رمز نگاری تراکنش ها با استفاده از DUKPT در ترمینال

ترمینال با استفاده از DUKPT Key و مقدار فیلد KSN ، به ازای هر تراکنش با استفاده از الگوریتم های مشتق سازی کلید DUKPT، یک کلید جدید موقت و منحصر به فرد برای تراکنش جاری، مشتق می نماید.شایان ذکر است که عملیات مشتق سازی کلید موقت تراکنش ، در داخل حافظه ی HSM ترمینال انجام می شود.بدین ترتیب و با فراخوانی سرویس های دریافت PIN کاربر در داخل ترمینال به ازای هر تراکنش و با استفاده از کلید منحصر به فرد همان تراکنش، پین بلاک مشتری رمز نگاری می شود.همچنین داده های حساس مشتری همچون اطلاعات Track 2 نیز با کلید منحصر به فرد همان تراکنش، رمز نگاری می شود.

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.

بررسی و رمز گشایی تراکنش ها در سوئیچ

با استفاده از کلید DK که در HSM ذخیره شده است و فیلد دریافتی KSN (یکی از فیلدهای ارسالی تراکنش از سوی ترمینال)، سوئیچ می تواند اطلاعات PIN Block رمز شده با کلید DUKPT ترمینال ، به کلید کانال شاپرک که در همان HSM است، translate نماید.همچنین داده های حساس مشتری نیز با استفاده از HSM و DUKPT Key نیز قابل رمزگشایی و استفاده در سوئیچ پذیرنده است.همچنین در سوئیچ، ابتدا قسمت شمارنده ی رمزنگاری داده ی KSN قبلی ترمینال که در مرکز ذخیره شده است، مقایسه می گردد . همواره مقدار شمارنده ی رمزنگاری داده ی KSN ترمینال، می بایست از مقدار شمارنده ی رمز نگاری داده ی KSN سوئیچ، بزرگتر باشد تا تراکنش مورد قبول واقع شود .در صورت بر پا بودن شرط فوق، مقدار KSN سوئیچ با مقدار KSN ترمینال جایگزین می گردد.

استراتژی تغییر کلید DUKPT ترمینال ها

همانگونه که ذکر شد در پاسخ به تراکنش Log On ترمینال، کلید اصلی DUKPT به ترمینال ارسال می گردد.بر اساس پارامترها و شرایط تصمیم گیری که مرتبط با سیاست های شرکت پرداخت نوین است، ممکن است نیاز به تغییر کلید اصلی DUKPT در مقاطع زمانی مختلف باشد.این پارامترهای تصمیم گیری می توانند بازه ی خاص، تعداد تراکنش های ترمینال یا پارامتر های دیگری باشد.همچنین در مشتق سازی کلید اصلی DUKPT ترمینال، می بایست داده ی KSN که انحصاری به هر ترمینال اختصاص یافته است، نیز مجددا بروزرسانی گردد تا کلید اصلی DUKPT ترمینال، در دوره ی جدید یک کلید جدید و منحصر به فرد باشد.به همین منظور، فیلد شمارنده ی sequence در قسمت "اطلاعات ترمینال" داده ی KSN ، به ازای هر بار تراکنش Log On و تغییر کلید اصلی DUKPT ترمینال، یک واحد افزایش می یابد.در سوئیچ نیز به ازای هر ترمینال، حالت ترمینال، (Terminal State) نگهداری می شود که در حالت نرمال به مفهوم قبول تراکنش است و در حالت Force Log On به مفهوم اینکه ترمینال می بایست تراکنش Force Log On ارسال نماید.

این مستند متعلق به شرکت پرداخت نوین آرین است و هیچ کس بدون اجازه کتبی حق انتشار، کپی‌برداری و افشای آن را ندارد.