جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

# دستورالعمل فنی عملیات تولید، پشتیبان‌گیری و بازیابی کلید

**طبقه‌بندی: عادی**

**شماره بازنگری: ۲,۱**

## فهرست مطالب

**عنوان** **صفحه**

# ۱ مقدمه

با توجه به اهمیت بسیار بالای عملیات تولید، پشتیبان‌گیری و بازیابی کلید مراکز صدور گواهی الکترونیکی از دیدگاه امنیتی، لازم و ضروری است که الزامات امنیتی منطبق با استانداردهای بین‌المللی جهت انجام عملیات مذکور، اعمال گردد. الزامات کلی مربوط به عملیات تولید کلید در سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» آورده شده است و استانداردهای متناظر در سند «معرفی استانداردهای زیرساخت کلید عمومی کشور» معرفی شده‌اند. لازم به ذکر است که اسناد مذکور از طریق وب‌سایت مرکز دولتی صدور گواهی الکترونیکی ریشه قابل دریافت می‌باشند.

سند پیش‌رو با هدف ارائه یک دستورالعمل فنی به منظور انجام عملیات تولید زوج‌کلید RSA و پشتیبان‌گیری و بازیابی کلید خصوصی مراکز صدور گواهی الکترونیکی میانی موجود در زیرساخت کلید عمومی کشور، منطبق با سیاست‌های مرکز دولتی صدور گواهی الکترونیکی ریشه و بر اساس استاندارد PKCS#11، تدوین شده است.

# ۲ روال فنی فرآیند تولید کلید

در مراسم تولید کلید مراکز صدور گواهی الکترونیکی میانی، حداقل می‌بایست ۲ نقش مجاز از مرکز میانی و یک نقش مجاز از مرکز دولتی صدور گواهی الکترونیکی ریشه حضور داشته باشند. فرآیند تولید کلید بسته به سطح اطمینان مرکز میانی می‌بایست همراه با کنترل چند نفره صورت پذیرد. الزامات مربوط به کنترل چند نفره در سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» از طریق وب‌سایت مرکز دولتی صدور گواهی الکترونیکی ریشه منتشر شده است.

روش اجرایی تولید و پشتیبان‌گیری از کلید با توجه به نوع HSM مورد استفاده در مرکز صدور گواهی الکترونیکی، متفاوت خواهد بود؛ در ادامه روش‌های اجرایی قابل استفاده جهت انجام عملیات تولید زوج‌کلید و پشتیبان‌گیری و بازیابی کلید خصوصی، شرح داده شده است.

## ۲-۱ استفاده از قابلیت درهم‌سازی کلید

چنانچه HSM مورد استفاده در مراکز صدور گواهی از قابلیت استخراج کلید به صورت رمز شده[1] پشتیبانی نماید، روال فنی تولید و پشتیبان‌گیری از کلید می‌تواند منطبق با دستورالعمل ذیل صورت پذیرد:

عملیات تولید کلید می‌بایست به صورت on-board در داخل HSM انجام شده و عملیات پشتیبان‌گیری از کلید از طریق توکن پشتیبان و توکن بازیاب صورت گیرد. توکن پشتیبان جهت نگهداری نسخه پشتیبان کلید خصوصی مرکز میانی به صورت رمزگذاری شده و توکن بازیاب جهت نگهداری کلید Wrap/unWrap به منظور رمزگذاری و رمزگشایی کلید خصوصی مرکز میانی به کار می‌رود. توجه داشته باشید که توکن پشتیبان و توکن بازیاب **حتماً می‌بایست در اختیار دو نقش مجاز مختلف از مرکز میانی قرار گیرد**. در الگوریتم‌های ذیل روال فنی تولید، پشتیبان‌گیری و بازیابی کلید منطبق با استاندارد PKCS#11 شرح داده شده است.

[1] Key Wrapping

## الگوریتم تولید کلید و پشتیبان‌گیری

۱. ورود[1] به HSM؛
۲. تولید زوج‌کلید RSA 2048 به طوری که کلید خصوصی دارای مشخصه‌های Private، Extractable و Sensitive و برای مؤلفه توان عمومی[2] از کلید عمومی مقدار 010001 هگزا دسیمال در نظر گرفته شود.
۳. تولید کلید Wrap/unwrap با مکانیزم AES 256 و از نوع Private و Session Object؛
۴. استخراج مقدار کلید Wrap/unwrap؛
۵. استخراج کلید خصوصی RSA به صورت رمزگذاری شده با مکانیزم AES_CBC و تابع C_WrapKey؛
۶. نشاندن مشخصه unExtractable برای کلید خصوصی RSA؛
۷. ورود به توکن پشتیبان؛
۸. انتقال کلید خصوصی رمزگذاری شده به صورت Private Data Object در داخل توکن پشتیبان؛
۹. ورود به توکن بازیاب؛
۱۰. انتقال کلید Wrap/unWrap به صورت AES Key Object و با مشخصه‌های Private، Extractable و nonSensitive به داخل توکن بازیاب.

## الگوریتم بازیابی کلید

۱. ورود به توکن پشتیبان؛
۲. استخراج مقدار کلید خصوصی رمزگذاری شده (Private Data Object)؛
۳. ورود به توکن بازیاب؛
۴. استخراج مقدار کلید Wrap/unwrap؛
۵. ورود به HSM؛
۶. ایجاد کلید unWrap به صورت Private و Session Object؛
۷. ایجاد کلید خصوصی RSA با استفاده از تابع C_UnWrapKey و با مشخصه‌های Private، Sensitive و unExtractable.

[1] Login
[2] Public Exponent

## ۲-۲ استفاده از توکن پشتیبان HSM

در صورت عدم پشتیبانی HSM مورد استفاده در مراکز صدور گواهی از قابلیت استخراج کلید به صورت رمز شده (Key Wrapping)، فرآیند تولید و پشتیبان‌گیری از کلید به شرح ذیل می‌تواند صورت پذیرد.

- در این حالت عملیات تولید زوج‌کلید RSA 2048 به صورت on-board در داخل HSM همراه با مشخصه‌های Private، UnExtractable، Sensitive و UnModifiable برای کلید خصوصی و برای مؤلفه توان عمومی از کلید عمومی مقدار 010001 هگزا دسیمال در نظر گرفته شود.
- پشتیبان‌گیری از کلید خصوصی و بازیابی آن، با استفاده از توکن پشتیبان HSM و همراه با اعمال کنترل دسترسی از طریق احراز هویت چند عامله[1] می‌بایست صورت پذیرد و کلید خصوصی باید به صورت رمزگذاری شده در توکن پشتیبان نگهداری گردد.

[1] Multi-Factor Authentication