باسمه تعالی

رمزنگاری پیشرفته

دکتر سلماسی‌زاده - دکتر احمدی

تمرین سری اول – بخش دوم

مشخصات امضای دیجیتال در سازمان توسعه‌ی تجارت الکترونیکی

پوریا دادخواه

401201381

- **تولید و نصب زوج کلید**
  - **تولید زوج کلید**
    - **تولید زوج کلید مراکز صدور گواهی**

مرکز دولتی ریشه از زوج کلید الگوریتم RSA جهت صدور گواهی، پشتیبانی مینماید .انجام عملیات تولید کلید در این مرکز از طریق یک HSM مورد تأیید مرکز دولتی ریشـــه که در آن ملزومات امنیتی مطابق استاندارد
FIPS 140-2 درسطح سوم رعایت شده است و به روش کنترل چند نفره 3 از 5 صورت میپذیرد .الزامات مربوط به عملیات تولید کلید برای مراکز میانی در جدول زیر قید شده است.

سطح اطمینان	تولید زوج‌کلید مرکز میانی
سطح ۱	مرکز میانی می‌بایست اطمینان حاصل نماید که تولید کلید مرکز با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور و توسط نقش مورد اعتماد و مجاز صورت می‌پذیرد.
سطح ۲ سطح ۳ سطح ۴	تولید زوج کلید مرکز میانی: • می‌بایست توسط متصدیانی با نقش مورد اعتماد و مجاز برای تولید کلید صورت پذیرد. • می‌بایست در داخل پودمان رمزنگاشتی سخت‌افزاری انجام پذیرد که حداقل الزامات بخش ۱-۶-۲ را در بر گیرد • می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد. • در سطح سوم و چهارم می‌بایست انجام عملیات تولید کلید از طریق کنترل چند نفره مطابق با بخش ۶-۲-۲ صورت گیرد. • مرکز میانی می‌بایست فرایند تولید کلید را مستند نماید و دلایل و شواهد لازم را برای اثبات اینکه مراحل مستند شده انجام گرفته‌اند، ارائه نماید.

- **تولید زوج کلید دفاتر ثبت نام**

سطح اطمینان	تولید زوج‌کلید دفتر ثبت نام
سطح ۱	مرکز میانی می‌بایست اطمینان حاصل نماید که تولید کلید دفتر ثبت نام با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور انجام گیرد.
سطح ۲ سطح ۳ سطح ۴	می‌بایست در داخل پودمان رمزنگاشتی سخت‌افزاری انجام پذیرد که حداقل الزامات بخش ۶-۲-۱ را در بر گیرد و نیز می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.

- **تولید زوج کلید مالک گواهی**

سطح اطمینان	تولید زوج‌کلید مالک گواهی
سطح ۱	• تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.
سطح ۲	• تولید زوج کلید برای مالک گواهی می‌بایست در یک پودمان رمزنگاشتی نرم‌افزاری و ترجیحاً سخت‌افزاری که در آن حداقل الزامات بخش ۶-۲-۱ رعایت شده است، صورت پذیرد (تولید کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر، به دفتر ثبت نام یا مرکز میانی باید همراه با اثبات مالکیت کلید خصوصی باشد). • تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.
سطح ۳	• تولید زوج کلید برای مالک گواهی می‌بایست در داخل یک پودمان رمزنگاشتی سخت‌افزاری که در آن حداقل الزامات بخش ۶-۲-۱ رعایت شده است، صورت پذیرد.
سطح ۴	• تولید زوج کلید برای مالکان گواهی می‌بایست با استفاده از الگوریتم‌های پذیرفته شده در زیرساخت کلید عمومی کشور صورت پذیرد.

لازم به ذکر است چنانچه مرکز صدور گواهی میانی به نمایندگی از متقاضی اقدام به تولید زوج کلید نمود، میبایست این موضوع در توافق نامه طرفین ذکر شود .مرکز میانی میبایست فرایند این عملیات را در دستورالعمل اجرایی خود تشریح نماید.

- **تحویل کلید خصوصی به موجودیت نهایی**

سطح اطمینان	تحویل کلید خصوصی به موجودیت نهایی
سطح ۱	تولید زوج کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر به مرکز میانی یا دفتر ثبت نام باید همراه با اثبات مالکیت کلید خصوصی باشد.
سطح ۲	چنانچه عملیات تولید کلید توسط دفتر ثبت نام و یا مرکز میانی به نمایندگی از مالک گواهی صورت گیرد، می‌بایست این عملیات به صورت داخلی توسط یک سخت‌افزار رمزنگاشتی مورد تأیید (منطبق با بخش ۶-۱-۱) انجام گیرد و کلید خصوصی از طریق این سخت‌افزار در اختیار مالک گواهی قرار داده شود. تولید زوج کلید به صورت نرم‌افزاری صرفاً می‌بایست توسط مالک گواهی صورت گیرد و تحویل کلید عمومی متناظر به مرکز میانی یا دفتر ثبت نام باید همراه با اثبات مالکیت کلید خصوصی باشد.
سطح ۳	چنانچه عملیات تولید کلید توسط دفتر ثبت نام و یا مرکز میانی به نمایندگی از مالک گواهی صورت گیرد، می‌بایست این عملیات به صورت داخلی توسط یک سخت‌افزار رمزنگاشتی مورد تأیید (منطبق با بخش ۶-۱-۱) انجام گیرد و کلید خصوصی از طریق این سخت‌افزار در اختیار مالک گواهی قرار داده شود.
سطح ۴	

- **تحویل کلید عمومی به مرکز صدور گواهی**

چنانچه عملیات تولید کلید توسط مالک گواهی و یا دفتر ثبت نام صورت گیرد، تحویل کلید عمومی به مرکز صدور گواهی میبایست به گونه ای باشد، که تناظر بین کلید عمومی ارائه شده و کلید خصوصی مالک گواهی و همچنین حفظ تمامیت آن توسط مرکز صدور گواهی قابل بررسی باشد.
کلیه مراکز میانی جهت ارائه درخواست صدور گواهی به مرکز دولتی ریشه میبایست کلید عمومی خود را در قالب استاندارد PKCS#10 در اختیار مرکز دولتی ریشه قرار دهند.

- **تحویل کلید عمومی مرکز صدور گواهی به طرفهای اعتماد کننده**

مرکز دولتی ریشه از طریق مخزن خود که دسترسی و اعمال تغییر در آن فقط توسط نقشهای مجاز مرکز دولتی ریشه امکانپذیر است، کلید عمومی خود را در اختیار طرف های اعتماد کننده قرار میدهد .الزامات مربوط به مراکز میانی در جدول زیر قید شده است:

سطح اطمینان	تحویل کلید عمومی مرکز میانی به طرف‌های اعتماد کننده
سطح ۱	کلید عمومی مرکز میانی می‌بایست به صورت امن به طرف‌های اعتماد کننده منتقل شود، به طوری که صحت و اعتبار آن تضمین شود. روش تحویل کلید عمومی می‌بایست در دستورالعمل اجرایی مراکز میانی تشریح شود.
سطح ۲	
سطح ۳	
سطح ۴	

- **طول کلید**

مرکز دولتی ریشه از طول کلید 2048 بیت RSA برای ساختار سلسله مراتبی G2 و از طول کلید 4096 بیت RSAبرای ساختار سلسله مراتبی G3 استفاده مینماید .لازم به ذکر است ساختارهای G2 و G3 در بخش 7-1-3معرفی شده است .از تاریخ 1398 / 02 / 17 تمدید و صدور گواهی الکترونیکی مراکز میانی توسط مرکز
دولتی ریشه در ساختار سلسله مرتبی G2 متوقف شده است .الزامات مربوط به طول کلید برای مراکز میانی در جدول زیر قید شده است:

سطح اطمینان	الزامات طول کلید
سطح ۱	حداقل طول کلید برای مراکز میانی، ۲۰۴۸ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۱۰۲۴ بیت RSA ،یا ۲۲۴ بیت برای الگوریتم ECC یا ۲۵۶ بیت (معادل ۳۲ بایت) برای الگوریتم Ed25519 می‌باشد.
سطح ۲	
سطح ۳	حداقل طول کلید برای مراکز میانی ۲۰۴۸ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۲۰۴۸ بیت RSA ،یا ۳۸۴ بیت برای الگوریتم ECC یا ۴۵۶ بیت (معادل ۵۷ بایت) برای الگوریتم Ed25519 می‌باشد.
سطح ۴	حداقل طول کلید برای مراکز میانی ۴۰۹۶ بیت RSA می‌باشد. حداقل طول کلید برای موجودیت‌های نهایی، ۲۰۴۸ بیت RSA، یا ۵۱۲ بیت برای الگوریتم ECC یا ۴۵۶ بیت (معادل ۵۷ بایت) برای الگوریتم Ed25519 می‌باشد.

- **تولید پارامترهای کلید عمومی و کنترل کیفیت**

تولید پارامترهای کلید عمومی برای الگوریتم های امضا و همچنین بررسی کیفیت پارامترها مطابق با استاندارد FIPS 186 انجام میشوند.

- **موارد کاربرد کلید**

سطح اطمینان	موارد کاربرد کلید
سطح ۱	کلید خصوصی متناظر با گواهی الکترونیکی می‌بایست صرفاً منطبق با کاربردهای در نظر گرفته شده در فیلد KeyUsage و ExtendedKeyUsage گواهی مورد استفاده قرار گیرد. کاربردهای در نظر گرفته شده برای گواهی الکترونیکی در بخش ۱-۴-۱ توصیف شده است. ضمن اینکه فیلد کاربرد کلید گواهی می‌بایست مطابق با سند جامع پروفایل‌های زیرساخت کلید عمومی کشور به‌کار رود.
سطح ۲	
سطح ۳	
سطح ۴	