**باسمه تعالی**



**رمزنگاری پیشرفته**

**دکتر سلماسی‌زاده - دکتر احمدی**

**تمرین سری اول – بخش دوم**

**مشخصات امضای دیجیتال در سازمان توسعه‌ی تجارت الکترونیکی**

**پوریا دادخواه**

**401201381**

* **توليد و نصب زوج كليد**
  + **توليد زوج كليد**
    - **توليد زوج كليد مراكز صدور گواهي**

مركز دولتي ريشه از زوج كليد الگوريتم RSA جهت صدور گواهي، پشتيباني مينمايد. انجام عمليات توليد

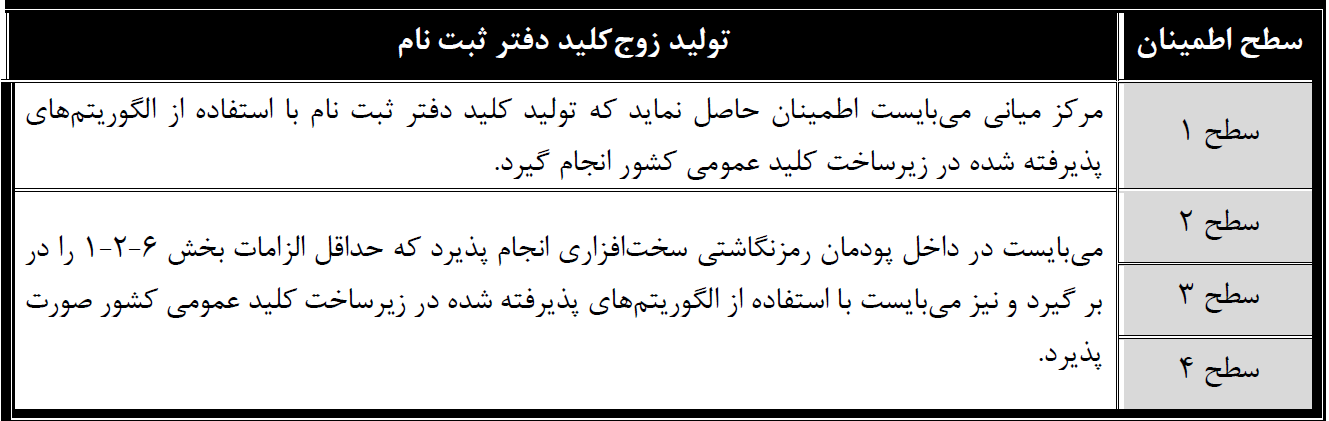
كليد در اين مركز از طريق يك HSM مورد تأييد مركز دولتي ريشه كه در آن ملزومات امنيتي مطابق استاندارد

FIPS 140-2درسطح سوم رعايت شده است و به روش كنترل چند نفره 3 از 5 صورت ميپذيرد. الزامات

مربوط به عمليات توليد كليد براي مراكز مياني در جدول زير قيد شده است.



* + - **توليد زوج كليد دفاتر ثبت نام**



* + - **توليد زوج كليد مالك گواهي**



لازم به ذكر است چنانچه مركز صدور گواهي مياني به نمايندگي از متقاضي اقدام به توليد زوج كليد نمود،

ميبايست اين موضوع در توافق نامه طرفين ذكر شود. مركز مياني ميبايست فرايند اين عمليات را در

دستورالعمل اجرايي خود تشريح نمايد.

* + **تحويل كليد خصوصي به موجوديت نهايي**



* + **تحويل كليد عمومي به مركز صدور گواهي**

چنانچه عمليات توليد كليد توسط مالك گواهي و يا دفتر ثبت نام صورت گيرد، تحويل كليد عمومي به مركز

صدور گواهي ميبايست به گونه اي باشد، كه تناظر بين كليد عمومي ارائه شده و كليد خصوصي مالك گواهي

و همچنين حفظ تماميت آن توسط مركز صدور گواهي قابل بررسي باشد.

كليه مراكز مياني جهت ارائه درخواست صدور گواهي به مركز دولتي ريشه ميبايست كليد عمومي خود را در

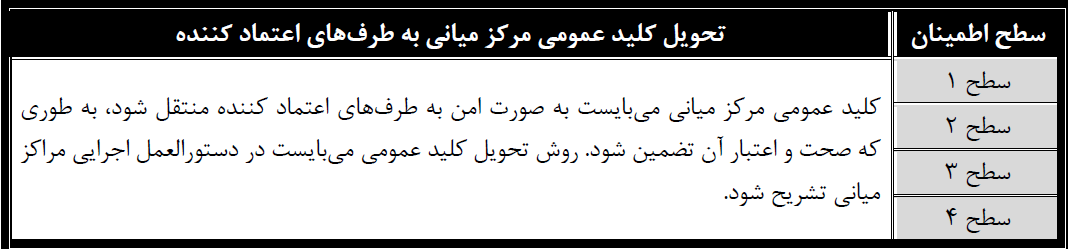
قالب استاندارد PKCS#10 در اختيار مركز دولتي ريشه قرار دهند.

* + **تحويل كليد عمومي مركز صدور گواهي به طرفهاي اعتماد كننده**

مركز دولتي ريشه از طريق مخزن خود كه دسترسي و اعمال تغيير در آن فقط توسط نقشهاي مجاز مركز

دولتي ريشه امكانپذير است، كليد عمومي خود را در اختيار طرف هاي اعتماد كننده قرار ميدهد. الزامات

مربوط به مراكز مياني در جدول زير قيد شده است:



* + **طول كليد**

مركز دولتي ريشه از طول كليد 2048 بيت RSA براي ساختار سلسله مراتبي G2 و از طول كليد 4096 بيت

RSA براي ساختار سلسله مراتبي G3 استفاده مينمايد. لازم به ذكر است ساختارهاي G2 و G3 در بخش

3-1-7 معرفي شده است. از تاريخ 17 / 02 / 1398 تمديد و صدور گواهي الكترونيكي مراكز مياني توسط مركز

دولتي ريشه در ساختار سلسله مرتبي G2 متوقف شده است. الزامات مربوط به طول كليد براي مراكز مياني در

جدول زير قيد شده است:



* + **توليد پارامترهاي كليد عمومي و كنترل كيفيت**

توليد پارامترهاي كليد عمومي براي الگوريتم هاي امضا و همچنين بررسي كيفيت پارامترها مطابق با استاندارد

FIPS 186انجام ميشوند.

* + **موارد كاربرد كليد**

