فرم خوداظهاری آزمایشگاه پودمان رمزنگاشتی

این فرم به منظور ارائه اطلاعات الزامی جهت انجام آزمون­های امنیتی و کارکردی روی پودمان­های رمزنگاشتی تهیه شده است. لذا می‌بایست محتویات این فرم در قالب یک سند تهیه و به آزمایشگاه تحویل داده شود. توجه داشته باشید که پاسخ به پرسش­های ذکرشده در این پرسش­نامه، به‌عنوان اطلاعات خوداظهاري تحويل داده شده از سوي ارائه­کنندگان پودمان رمزنگاشتی تلقي شده و چنانچه در حين انجام فرآيند ارزیابی يا پس از آن هر گونه مغايرت آشکار با اطلاعات قيد شده مشاهده شود، نسبت به لغو گواهي، اقدامات لازم صورت خواهد گرفت.

**اطلاعات متقاضی:**

|  |  |
| --- | --- |
| عنوان: |  |
| شناسه حقوقی: |  |
| آدرس: |  |
| کشور: |  |
| وب سایت: |  |
| **تماس اصلی** |  |
| پست الکترونیک: |  |
| تلفن: |  |
| دورنگار: |  |

**اطلاعات محصول**

|  |
| --- |
| نام محصول: |
| کشور سازنده: |
| نسخه و تاریخ انتشار سخت‌افزار: |
| نسخه و تاریخ انتشار میان‌افزار: |
| نسخه و تاریخ انتشار نرم‌افزار: |
| نسخه و تاریخ انتشار نرم‌افزار کاربردی همراه محصول: |
| نسخه و تاریخ انتشار واسط‌های نرم‌افزاری: |

1. **دلیل ارائه این محصول برای ارزیابی امنیتی چیست؟**

 الزام دولت  نیاز مشتری  بهبود امنیت  بهبود کیفیت

1. نوع تراشه پودمان رمزنگاشتی چیست؟

 تک-تراشه  چند-تراشه­ای تعبیه شده  چند تراشه­ای مستقل

1. این محصول بر روی کدام پلتفرم‌ها قابل اجرا است؟

  32 بیتی   64 بیتی   سایر: ............................................

1. این محصول بر روی کدام سیستم عامل(ها) قابل اجرا است؟

 Linux  Mac  Windows  Andoid  iOS  سایر **: .......................................**

1. پودمان رمزنگاشتی از چه نوع واسط‌های استانداردی پشتیبانی می‌کند؟(مشخصات کامل کلیه واسط‌ها می‌بایست در مستندات ذکر گردد)

 PKCS#11  MS CAPI  APDU Command  سایر

1. پودمان رمزنگاشتی از کدام قابلیت‌های اصلی زیر پشتیبانی می‌کند. در مورد پشتیبانی سخت‌افزاری یا نرم‌افزاری هر یک توضیح دهید.

 درهم‌سازی  تولید کلید  مشتق‌گیری کلید  امضای دیجیتال  رمزنگاری نامتقارن  رمزنگاری متقارن  کنترل چندنفره احراز هویت  عملیات دوگانه سایر

1. تعداد و نوع نشست‌های قابل پشتیبانی توسط پودمان رمزنگاشتی را به تفکیک نوع دسترسی و همزمانی و نوع کاربر ذکر نماید.
2. میزان حافظه پودمان رمزنگاشتی را به تفکیک نوع دسترسی ذکر نماید.
3. توضیح دهید آیا پودمان رمزنگاشتی قابلیت کار در حالت Fips Enabled و Non Fips Enabled را دارد؟
4. این محصول مطابق با کدام سطح امنیتی استاندارد ملی پودمان‌های رمزنگاشتی طراحی شده است؟

|  | **حوزه ارزیابی** | **سطح 1** | **سطح 2** | **سطح 3** | **سطح 4** |
| --- | --- | --- | --- | --- | --- |
| 1 | مشخصات پودمان رمزنگاشتي |  |  |  |  |
| 2 | درگاه‌ها و واسط‌هاي پودمان رمزنگاشتي |  |  |  |  |
| 3 | نقش­ها، خدمات و احرازهويت |  |  |  |  |
| 4 | مدل حالت متناهی |  |  |  |  |
| 5 | امنيت فيزيكي |  |  |  |  |
| 6 | محيط عملياتي |  |  |  |  |
| 7 | مديريت کليدهاي رمزنگاري |  |  |  |  |
| 8 | تداخل/ سازگاري الكترومغناطيسي |  |  |  |  |
| 9 | خودآزمايي |  |  |  |  |
| 10 | ضمانت طراحي |  |  |  |  |
| 11 | اقدامات کاهش‌دهنده آسیب در برابر سایر حملات |  |  |  |  |
|  | **سطح امنیت عمومی** |  |  |  |  |

توضیحات مرتبط : ...............................................................................................................................................................................................