شماره : ۴/۴۶۷۰

تاریخ : ۱۳۹۰/۰۷/۲۰

پیوست :

جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

مرکز توسعه تجارت الکترونیکی

« سال جهاد اقتصادی»

سیستم اتوماسیون

مدیرعامل محترم شرکت

با سلام،

نظر به کاربرد روزافزون توکن‌های امنیتی در زیرساخت کلید عمومی کشور و با توجه به راه‌اندازی آزمایشگاه توکن در مرکز دولتی صدور گواهی الکترونیکی ریشه، لازم و ضروری است تمامی توکن‌های امنیتی اعم از داخلی و خارجی که از زیرساخت کلید عمومی کشور، استفاده می‌نمایند گواهی تاییدیه این مرکز را دریافت نمایند. لذا بدین‌وسیله به اطلاع می‌رساند، جهت تست و ارزیابی توکن/های آن شرکت محترم، لازم است موارد ذیل در پاکت دربسته به آدرس تهران - بلوار کشاورز- خیابان شهید نادری – نبش کوچه شهید حجت دوست - ساختمان شماره یک وزارت بازرگانی، طبقه پنجم- مرکز توسعه تجارت الکترونیکی ارسال گردد.

الف - توکن‌های داخلی:

۱- سند سیاست‌ها و دستورالعمل اجرایی توکن امنیتی، مطابق با ساختار ارائه شده در پیوست؛

۲- چهار عدد توکن مورد آزمون؛

۳- یک نمونه برد کامل مدار الکترونیکی توکن بطوریکه سالم و قابل استفاده باشد (یک عدد توکن مورد آزمون بدون بدنه یا پوشش)؛

۴- کلیه واسط‌ها و نرم‌افزارهای جانبی مورد نیاز؛

۵- کلیه مستندات راهنما جهت استفاده از توکن؛

۶- معرفی‌نامه نماینده فنی شرکت جهت تعامل با مرکز ریشه.

ب - توکن‌های خارجی:

۱- سند سیاست‌ها و دستورالعمل اجرایی توکن امنیتی با ساختار ارائه شده در پیوست و یا یک سند معادل بطوریکه حتی‌الامکان الزامات قید شده در پیوست را پوشش دهد.

۲- چهار عدد توکن مورد آزمون؛

۳- در صورت امکان برد کامل مدار الکترونیکی توکن و یا مدل تراشه توکن؛

۴- یک نسخه از مدرک گواهی/های امنیتی صادره برای توکن (چنانچه گواهی امنیتی صادره متعلق به استاندارد بومی یک کشوری است، یک نسخه از این استاندارد نیز مورد نیاز می‌باشد)؛

۵- کلیه واسط‌ها و نرم‌افزارهای جانبی مورد نیاز؛

۶- کلیه مستندات راهنما جهت استفاده از توکن؛

۷- معرفی‌نامه نماینده فنی شرکت جهت تعامل با مرکز ریشه.

فرانک رازقی اسکویی
قائم مقام مرکز و
رئیس مرکز دولتی صدور گواهی الکترونیکی ریشه

رونوشت:

- شرکت فناوری اطلاعات ایران بازگشت به نامه شماره ۴۶۲/۲۰۹۲۶
- سازمان صنعت، معدن و تجارت خراسان رضوی بازگشت به نامه شماره ۱۱۹/۱/۲۰۵۵۶۵ درخصوص درخواست اتحادیه صنف املاک
- سازمان آمار و فناوری اطلاعات شهرداری تبریز بازگشت به نامه شماره ۳۸۸۴/۱۵/۱
- سازمان توسعه تجارت ایران بازگشت به نامه شماره ۹۰/۵۱۰/۵۶۵

« نامه‌های صادره بدون مهر برجسته اتوماسیون اداری فاقد اعتبار می‌باشد »

آدرس: تهران - بلوار کشاورز - خیابان شهید نادری - جنب کوچه حجت دوست - پلاک ۱۵ – کد پستی ۱۴۱۶۶۴۳۸۵۱-صندوق پستی ۶۳۸۵-۱۴۱۵۵

WebSite :www.Ecommerce.gov.ir Email: Info@Ecommerce.gov.ir

جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

الزامات سند سیاست‌ها و دستورالعمل اجرایی

توکن امنیتی

طبقه‌بندی: عادی

شماره بازنگری :۲.۰

تاریخ بازنگری : ۱۳۹۰/۷/۱۰

حق طبع و نشر

این ویرایش از گزارش، در تاریخ ۹۰/۷/۱۰ توسط مرکز دولتی صدور گواهی الکترونیکی ریشه جهت فراهم آوردن مقدمات تست و ارزیابی توکن‌های امنیتی مورد استفاده در زیرساخت کلید عمومی کشور، تحت عنوان "الزامات سند سیاست‌ها و دستورالعمل اجرایی توکن‌های امنیتی" ارائه گردیده است. تمامی حقوق این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران بوده و هرگونه استفاده از آن منوط به کسب مجوز از صاحب اثر می‌باشد.

فهرست مطالب

۱ مقدمه ۴

۲ الزامات تدوین سند ۵

۲-۱ مشخصات توکن امنیتی ۵

۲-۲ پورت‌ها و واسط‌های توکن امنیتی ۶

۲-۳ نقشها، سرویس‌ها و احرازهویت ۶

۲-۴ مدل حالت متناهی ۷

۲-۵ امنیت فیزیکی ۷

۲-۶ محیط عملیاتی ۸

۲-۷ مدیریت کلیدهای رمزنگاری ۸

۲-۸ تداخل/سازگاری الکترومغناطیسی ۹

۲-۹ آزمون‌های خودکار ۹

۲-۱۰ ضمانت طراحی ۱۰

۲-۱۱ اقدامات متقابل در برابر سایر حملات ۱۱

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۱ مقدمه

سند سیاست‌ها و دستورالعمل اجرایی توکن امنیتی می‌بایست دربردارنده سیاست‌ها و رویه‌های به کار گرفته شده توسط تولیدکنندگان توکن‌های امنیتی جهت اعمال ملزومات امنیتی منطبق با الزامات استاندارد FIPS ۱۴۰-۲ باشد. این سند می‌بایست حداقل از ۱۱ بخش مختلف جهت تشریح سیاست‌ها و رویه‌های اعمال شده در توکن امنیتی بر اساس حوزه‌های یازده‌گانه توصیف شده در استاندارد FIPS ۱۴۰-۲، تشکیل شده باشد. در سند پیش‌رو ساختار و اطلاعات مورد نیاز جهت ارائه در هر بخش از مستند "سیاست‌ها و دستورالعمل اجرایی توکن‌های امنیتی" آورده شده است.

توجه : سند "سیاست‌ها و دستورالعمل اجرایی توکن امنیتی" بعنوان اطلاعات خوداظهاری تحویل داده شده از سوی ارائه‌کنندگان توکن تلقی شده و می‌بایست با دقت کامل و بر اساس الزامات قید شده در سند پیش‌رو تدوین و به مرکز دولتی صدور گواهی الکترونیکی ریشه، جهت تست و ارزیابی توکن ارائه گردد. بر اساس سیاست‌های مرکز ریشه چنانچه در حین انجام فرآیند تست و یا پس از آن هر گونه مغایرت آشکار با اطلاعات قید شده در سند مذکور مشاهده شود، نسبت به صدور یا لغو گواهی امنیتی توکن، اقدامات لازم صورت خواهد گرفت.

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۲ الزامات تدوین سند

در این بخش ساختار و الزامات تدوین سند سیاست‌ها و دستورالعمل اجرایی توکن امنیتی برای هر یک از یازده حوزه ارائه شده در استاندارد FIPS ۱۴۰-۲، شرح داده شده است. از الزامات قید شده در این بخش، اطلاعاتی که **(ضروری)** تعیین شده، از اهمیت بالاتری جهت ارائه به آزمایشگاه و ارزیابی محصول برخوردار می‌باشد.

۲-۱ مشخصات توکن امنیتی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تعیین اجزای سخت‌افزاری توکن شامل نام کامل تراشه‌ها، پردازنده‌های کمکی رمزنگاری[۲] (در صورت وجود)، نوع واسطهای I/O، نوع و حجم حافظه (RAM/ROM/EEPROM)و ... ؛ **(ضروری)**
- ارائه مشخصات امنیتی سخت‌افزار (در صورت وجود) شامل سنسورهای تغییر دما، تغییر ولتاژ و تغییر فرکانس، آشکارساز حملات Fault Injection، سنسورهای نوری و ... ؛ (ضروری)
- تعیین جنس ماده سازنده بدنه توکن؛ **(ضروری)**
- ارائه معماری فیزیکی ماژول شامل نقشه مدار الکترونیکی ماژول و بلوک دیاگرام نمایش‌دهنده تمامی اجزای سخت‌افزاری توکن امنیتی شامل تمامی پردازنده‌ها، بافرهای ورودی و خروجی، بافرهای کنترلی، مخزن کلید و حافظه؛ **(ضروری)**
- تعیین مشخصات نرم‌افزار و Firmware توکن؛
- لیست توابع امنیتی پذیرفته شده و پذیرفته نشده در زیرساخت کلید عمومی کشور و مدهای عملیاتی آن‌ها که در توکن امنیتی پیاده‌سازی شده است[۳] و همچنین تعیین اینکه عملیات

---

[۱] Cryptographic Module Specification

[۲] چنانچه توکن امنیتی دارای پردازنده‌های کمکی باشد، می‌بایست نوع پردازنده‌های کمکی تعیین گردد. بعنوان مثال Triple DES Coprocessor ، AES Coprocessor، Public Key or PKI Coprocessor و ...

[۳] لیست توابع امنیتی یا الگوریتم‌های رمزنگاری پذیرفته شده در زیرساخت کلید عمومی کشور در سند "معرفی استانداردهای زیرساخت کلید عمومی کشور" معرفی شده است. این سند از وب‌سایت مرکز دولتی صدور گواهی الکترونیکی ریشه قابل دریافت می‌باشد.

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

رمزنگاری متناظر با هر تابع امنیتی بصورت On-board و توسط تراشه انجام می‌گیرد و یا خیر؛ **(ضروری)**

- تعیین کلیه اطلاعات امنیتی شامل کلیدهای رمزنگاری سری و خصوصی، اطلاعات هویت شناسی (مثل کلمات عبو یا PIN) و اطلاعات محافظت شده دیگر مانند رویدادهای بازرسی که آشکار شدن و یا ایجاد تغییر در آن‌ها امنیت توکن امنیتی را بخطر می‌اندازد.

۲-۲ پورت‌ها و واسط‌های توکن امنیتی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تعیین مشخصات پورت‌های فیزیکی (بعنوان مثال مشخصات و اتصالات مربوط به پورت USB)؛
- تعیین مشخصات واسط‌های منطقی (بعنوان مثال نحوه کنترل ورود و خروج اطلاعات از طریق سیستم عامل با تعریف قاعده کنترل دسترسی[۲]).

۲-۳ نقش‌ها، سرویس‌ها و احرازهویت[۳]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تعیین کلیه نقش‌های مجاز پشتیبانی شده توسط توکن امنیتی؛
- تعیین کلیه سرویس‌ها، عملیات و یا توابع امنیتی قابل اجرا توسط هر نقش؛
- برای هر سرویس یا تابع امنیتی قابل اجرا برای هر نقش، می‌بایست نوع دسترسی به کلیدهای رمزنگاری و اطلاعات محرمانه ذخیره شده در توکن تعیین گردد؛
- تعیین کلیه سرویس‌ها و عملیات فراهم شده توسط توکن امنیتی که کاربر برای انجام آن‌ها نیاز ندارد که یک نقش مجاز باشد و می‌بایست مشخص گردد که اجرا و انجام این نوع عملیات و توابع هیچ نوع دسترسی به اطلاعات محرمانه ذخیره شده در توکن ایجاد نمی‌نماید؛
- تشریح مکانیزم احراز هویت شخصیت محور[۴] پشتیبانی شده توسط توکن (در صورت وجود) و نوع اطلاعات مورد نیاز جهت اعمال مکانیزم احرازهویت شخصیت محور (بعنوان مثال پین‌کد و اطلاعات بایومتریک).

---

[۱] Cryptographic Module Ports and Interfaces

[۲] Access Control rule : Access Type & Security Condition

[۳] Roles, Services, And Authentication

[٤] Identity-based Authentication

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۲-۴ مدل حالت متناهی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- توصیف کامل مدل‌های حالت تعریف شده برای توکن امنیتی از طریق دیاگرام‌ها و جداولی که سطوح دسترسی برای هر حالت و چگونگی گذار از یک حالت به حالت دیگر را تعیین می‌کند؛ همچنین تشریح رخدادهای ورودی (شامل داده‌های ورودی و کنترل‌های خروجی) که باعث گذار از یک حالت به حالت دیگر می‌شوند و رویدادهای خروجی (شامل شرایط ماژول‌های داخلی، داده‌های خروجی و وضعیت خروجی) که در اثر گذار از یک حالت به حالت دیگر واقع می‌شوند.

۲-۵ امنیت فیزیکی[۲]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تشریح مکانیزم‌های بکار گرفته شده برای امنیت فیزیکی توکن در صورت وجود (بعنوان مثال مکانیزم‌های بکارگرفته شده در توکن جهت اعمال قابلیت تشخیص نفوذ[۳])؛ **(ضروری)**
- تشریح مکانیزم‌های پاسخگویی به نفوذ[۴] و بازنویسی حافظه[۵] در اثر نفوذ، در صورتی‌که توکن دارای بدنه جداشدنی باشد و یا دسترسی به مدار الکترونیکی توکن امکان‌پذیر باشد؛ **(ضروری)**
- تعیین رنج عملیاتی توکن (برای ولتاژ و دما)؛ همچنین تشریح مولفه‌های به کار بسته شده در توکن برای اعمال قابلیت EFP [۶] (در صورت وجود).

[۱] Finite State Model

[۲] Phisical Security

[۳] Tamper Evidence

[۴] Tamper Response

[۵] Zeroization

[۶] Environmental Failure Protection

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۲-۶ محیط عملیاتی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تشریح محیط عملیاتی توکن (سیستم عامل و یا Firmware)؛ **(ضروری)**
- تشریح کامل نحوه اعمال کنترل دسترسی به واحدهای اطلاعاتی ذخیره شده در توکن (نظیر کلیدهای رمزنگاری) و امنیت آن (بعنوان مثال چنانچه برای یک واحد اطلاعاتی ذخیره شده در توکن سطح دسترسی غیر قابل استخراج[۲] تعریف شده باشد، می‌بایست عنوان گردد که امکان تغییر این سطح دسترسی به حالت استخراج‌شدنی[۳] وجود دارد یا خیر)؛
- تشریح کامل مشخصات سیستم عامل توکن (درصورت وجود) و تعیین سطح اطمینان C.C و Protection Profile مربوطه. **(ضروری)**

۲-۷ مدیریت کلیدهای رمزنگاری[۴]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تعیین انواع و طول کلیدهای رمزنگاری پشتیبانی شده توسط توکن؛
- تعیین نوع مولدهای اعداد تصادفی مورد استفاده در توکن امنیتی (چه پذیرفته شده و چه پذیرفته نشده در زیرساخت کلید عمومی کشور)؛ **(ضروری)**
- تعیین متدهای تولید کلید بکاربسته شده توسط توکن (چه پذیرفته شده و چه پذیرفته نشده در زیرساخت کلید عمومی کشور) و همچنین تعیین اینکه عملیات تولید کلید متناظر با هر یک از انواع کلید پشتیبانی شده توسط توکن، بصورت On-board و توسط تراشه صورت می‌گیرد یا خیر؛ **(ضروری)**
- تعیین متدهای ورود و خروج کلید بکاربسته شده در توکن؛
- چنانچه توکن از مکانیزم‌های دانش انشعابی[۵] و یا تسهیم راز[۶] پشتیبانی نماید، می‌بایست اثبات امنیت آن آورده شود بعبارت دیگر می‌بایست اثبات گردد که استخراج کلید اصلی

---

[۱] Operational Environment

[۲] Unextractable

[۳] Extractable

[۴] Cryptographic Key Management

[۵] Split Knowledge

[۶] Secret Sharing

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

نیاز به دانستن n جز از کلید دارد و داشتن هر n-۱ جز از کلید هیچ اطلاعاتی از کلید اصلی بجز طول آن، در اختیار قرار نمی‌دهد. علاوه بر این می‌بایست نوع و رویه تکنیک دانش انشعابی بکاربسته شده در توکن، تشریح گردد؛

- تشریح متدهای ذخیره‌سازی کلید در توکن (بعنوان مثال تشریح محل ذخیره‌سازی کلید، فرمت ذخیره‌سازی کلید و ملاحظات امنیتی اعمال شده)؛ **(ضروری)**

۲-۸ تداخل/سازگاری الکترومغناطیسی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- در صورت وجود، ارائه شواهدی مبنی بر رعایت الزامات تداخل و سازگاری الکترومغناطیسی (EMI/EMC) منطبق با استانداردهای معتبر نظیر FCC Part ۱۵، EN ۵۵۰۲۲، CISPR ۱۱ و EN ۶۱۳۲۶-۱ . **(ضروری)**

۲-۹ آزمون‌های خودکار[۲]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تشریح کامل آزمون‌های خودکار انجام شده توسط توکن شامل آزمون‌های Power-up و آزمون‌های شرایطی[۳] (در صورت وجود) و تعیین کلیه توابع امنیتی اجرا شده در طی فرآیند آزمون خودکار بر اساس آزمون‌های تعریف شده در استاندارد FIPS ۱۴۰-۲؛ **(ضروری)**
- در صورت وجود، تعیین حالت‌های خطایی که توکن در اثر شکست یک آزمون خودکار وارد آن حالت‌ها می‌شود و همچنین تعیین شرایط و عملیاتی که لازم است تا توکن از حالت خطا خارج شده و به حالت عملیات عادی خود بازگردد.

[۱] Electromagnetic Interference/ Electromagnetic Compatibility

[۲] Self Tests

[۳] Conditional test

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۲-۱۰ ضمانت طراحی[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- تشریح رویه‌های نصب، تولید و راه‌اندازی امن توکن؛
- تعیین رویه‌های مورد استفاده توسط سازنده توکن جهت حفظ و نگهداری امنیت توکن از زمان تست و ارزیابی توکن در آزمایشگاه تا زمانی‌که توکن به کاربران عرضه می‌گردد؛
- ارائه توضیحات فنی تکمیلی در ارتباط با تناظر و ارتباط بین طراحی اجزای سخت-افزاری، نرم‌افزار و Firmware توکن با ملزومات بیان شده در استاندارد FIPS ۱۴۰-۲ و سیاست امنیتی اعمال شده در توکن؛
- ارائه کد منبع نرم‌افزار و Firmware توکن به همراه توضیحات مرتبط با هر بخش از کد بطوریکه بوضوح تناظر و تطابق بین اجزای مختلف طراحی ماژول را توصیف نماید (در صورت عدم ارائه کد منبع توسط تولید کننده توکن، کد منبع از قلمروی تست و ارزیابی توکن و تاییدیه محصول خارج می‌گردد)؛
- طرح شماتیک اجزای سخت‌افزاری توکن و ارتباط آن‌ها؛
- بخش مربوط به **راهنمای استفاده از توکن برای نقش راهبر** حداقل می‌بایست شامل موارد ذیل باشد (این بخش می‌تواند در قالب یک مستند مجزا ارائه گردد):
  - توابع و عملیات اجرایی قابل انجام توسط نقش راهبر و وقایع امنیتی، پارامترهای امنیتی، درگاه‌های فیزیکی و واسط‌های منطقی قابل دسترس توسط نقش راهبر؛
  - روال اعمال مدیریت توکن امنیتی به روش امن (بعنوان مثال چگونگی راه‌اندازی اولیه توکن و روال Unblock نمودن پین‌کد کاربر)؛
  - مفروضات و ملاحظات امنیتی لازم برای نقش راهبر جهت عملکرد مطمئن و امن توکن. **(ضروری)**
- بخش مربوط به **راهنمای استفاده از توکن برای نقش کاربر** حداقل می‌بایست شامل موارد ذیل باشد (این بخش می‌تواند در قالب یک مستند مجزا ارائه گردد):
  - توابع و عملیات اجرایی قابل انجام توسط نقش کاربر و وقایع امنیتی، پارامترهای امنیتی، درگاه‌های فیزیکی و واسط‌های منطقی قابل دسترس توسط نقش کاربر؛
  - کلیه ملزومات، ملاحظات و مسئولیت‌های امنیتی ضروری برای نقش کاربر جهت عملکرد مطمئن و امن توکن. **(ضروری)**

[۱] Design Assurance

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰

۲-۱۱ اقدامات متقابل در برابر سایر حملات[۱]

الزامات تدوین این بخش به شرح ذیل می‌باشد:

- چنانچه در توکن امنیتی اقدامات متقابل در برابر حملات خاصی نظیر حملات کانال جانبی[۲] اعمال شده باشد، می‌بایست در این بخش این اقدامات بطور کامل تشریح گردد.

[۱] Mitigation of Other Attacks

[۲] Side Channel Attacks

کلیه حقوق مادی و معنوی این اثر متعلق به مرکز توسعه تجارت الکترونیکی ایران می‌باشد ، ۱۳۹۰