الگوی ساختاری سند سیاست‌های امنیتی

فهرست زیر نمونه‌ای از سرفصل‌ها و مطالب حداقلی است که در سند سیاست‌های امنیتی باید قید گردد. البته ممکن است متناسب با نوع پودمان رمزنگاشتی و حوزه کاربردپذیری آن، بخش‌هایی دیگر نیز به آن افزوده شود. جهت دریافت راهنمایی به منظور تدوین سند سیاست‌های امنیتی پودمان رمزنگاشتی به «پیوست‌های الف و ب» از «[استاندارد ملی ملزومات امنیتی پودمان رمزنگاشتی زیرساخت کلید عمومی](http://www.rca.gov.ir/%D8%A7%D9%84%D8%B2%D8%A7%D9%85%D8%A7%D8%AA-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D9%BE%D9%88%D8%AF%D9%85%D8%A7%D9%86-%D9%87%D8%A7%DB%8C-%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B4%D8%AA%DB%8C-%D8%B2%DB%8C%D8%B1%D8%B3%D8%A7%D8%AE%D8%AA-%DA%A9%D9%84%DB%8C%D8%AF-%D8%B9%D9%85%D9%88%D9%85%DB%8C_2242.html)» مراجعه گردد.

**1 مقدمه**

**2 مشخصات پودمان رمزنگاشتی**

2.1 بررسی اجمالی

2.2 توصیف پودمان

2.2.1 سطح امنیتی پودمان

2.2.2 مولفه‌های پودمان

2.2.3 پلتفرم‌ها آزمایش‌شده

2.3 توصیف حیطه رمزنگاری

2.3.1 نموداری بلوکی

2.5 حالات عملیاتی

2.5.1 حالات عملیاتی مصوب

2.5.2 حالات عملیاتی غیر مصوب

**3 درگاه‌ها و واسط‌ها**

**4 نقش‌ها، خدمات و احراز هویت**

4.1 نقش‌ها

4.2 خدمات

4.2.1 خدمات قابل ارائه نیازمند احراز هویت اپراتور

4.2.2 خدمات قابل ارائه بدون نیاز به احراز هویت اپراتور

4.3 احراز هویت اپراتور

4.3.1 احراز هویت در سطح سازنده

4.3.2 احراز هویت در سطح صدور

4.3.3 احراز هویت در سطح کاربرد

4.3.4 گذرواژه‌های اولیه نقش‌های امنیتی

4.4 پیچیدگی و استقامت گذرواه‌ها

4.4.1 آماده‌سازی اولیه کلیدهای پودمان

4.4.2 گذرواژه‌های کاربر و مدیر پودمان

**5 امنیت فیزیکی**

**6 محیط عملیاتی**

6.1 کاربردپذیری

6.2 سیاست بکارگیری

**7 مدیریت کلید**

7.1 تولید اعداد تصادفی

7.2 تولید کلید

7.3 ورود و خروج کلید

7.4 استقرار کلید

7.5 ذخیره‌سازی کلید

7.6 انهدام کلید

**8 تداخل/ سازگاری الکترومغناطیسی**

**9 خودآزمایی**

9.1 آزمون‌های آغازین

9.1.1 آزمون الگوریتم‌های رمزنگاشتی

9.1.2 آزمون تمامیت و یکپارچگی نرم‌افزار و ثابت‌افزار

9.1.3 آزمون‌های الگوریتم (KAT)

9.1.4 آزمون عملیات حیاتی

9.2 آزمون‌های شرطی

9.2.1 آزمون تولید مداوم اعداد تصادفی

9.2.2 آزمون متقابل در عملیات‌های دوطرفه (مانند رمزگذاری و رمزگشایی)

9.2.3 آزمون پیوسته DRBG (بر مبنای SP 800-90A)

9.2.4 آزمون عملیات حیاتی

**10 ضمانت طراحی**

10.1 مدیریت پیکربندی

10.2 راهنمای عملیات امنیتی

10.2.1 راهنمای مدیر

10.2.2 راهنمای کاربر

10.3 توسعه محصول

**11 اقدامات کاهش‌دهنده آسیب در برابر سایر حملات**