



אפי
האגף לפיקוח על היצוא הבטחוני



משרד הביטחון
MINISTRY OF DEFENCE

עקרונות פרק 5 חלק 2 של ואסנאר

היערכות מומלצת - כבר בשלב זה למוצרים אשר סביר להניח כי יוותרו תחת פיקוח

בחינת המוצר לפי פרק 5.2*

רישום היצואן במרשם היצוא
הביטחוני באפ"י

רישום מוצר באפ"י

כללי - תכולת פרק 5 חלק 2 בלמ"ס

החרגות כלליות (מוצרים שלא יידרשו בפקוח)

רכיבי חומרה / תוכנות הרצה

"מוצרי מדף"

ציוד לשימוש אישי

5.B - 5.E

ציוד בדיקה
וייצור, תוכנה
וידע

5.A.4 - התגברות על אבטחת מידע

מוצרים
שעוקפים
מנגנוני הצפנה

5.A.3 - אבטחת מידע לא קריפטוגרפית

מוצרים
שעוסקים
בכבילת
תקשורת

5.A.2 - אבטחת מידע קריפטוגרפית

מוצרים
שאבטחת מידע
היא הפונקציה
הראשית שלהם

טכניקות הצפנה
לתיעול, ערבול,
אפנון ופיזור

הניסוחים במצגת
הינם כלליים ונועדו
להמחשה כללית
ואינם מחליפים
בחינה מעמיקה
של סעיפי הפרק -
באחריות היצואן



אפ"י
האגף לפיקוח על היצוא הביטחוני

בלמ"ס

החרגה כללית

(לגבי סעיפים: 5.A2, 5.D.2.a.1, 5.D.2.b, 5.D.2.c.1)

הערה 3 (Cryptography Note) - בתחילת הפרק - לא נדרשים בפיקוח:

רכיבי חומרה או 'תוכנת הרצה' (exe.):

- "אבטחת מידע" אינה הפונקציה הראשית שלהם
- לא משנים את יכולות ההצפנה של המוצר או מוסיפים יכולת הצפנה חדשה
- התכונות לא ניתנות לשינוי לפי מפרט הלקוח
- המפרט זמין להצגה לפי דרישת הרשויות

***** נדרשת עמידה בכל הסעיפים *****

OR

"מוצרי מדף":

- קהל יעד רחב
- זמין לרכישה ברשתות קמעונאיות / באופן מקוון / בדואר / בטלפון
- המחיר והמידע על הפונקציונליות העיקרית של הפריט זמינים לפני הרכישה ללא צורך להתייעץ עם הספק או המוכר
- **לא ניתן לשנות את תכונות ההצפנה**
- לא נדרשת תמיכה בהתקנה
- המפרט זמין להצגה לפי דרישת הרשויות

***** נדרשת עמידה בכל הסעיפים *****





האגף לפיקוח על היצוא הביטחוני

בלמ"ס

5.A.2 - אבטחת מידע קריפטוגרפית

הצפנה לחיסיון נתונים, שכוללת 'אלגוריתם האבטחה המתואר' ועונה על הבאים:

1. מוצרים עם "אבטחת מידע" כפונקציה ראשית
2. מערכות, ציוד או רכיבים של תקשורת דיגיטלית או עבודה ברשת (NetWorking) (שאבטחת מידע אינה פונקציה ראשית בהם)
3. מחשבים, פריטי אחסון או עיבוד מידע (שאבטחת מידע אינה פונקציה ראשית בהם)
4. תומכת בפונקציה לא ראשית של המוצר; **וגם** - מיושמת ע"י ציוד או תוכנה אשר יהפכו כמוצר בפני עצמו המפוקח לפי חלק זה.

***** "אלגוריתם האבטחה המתואר" - מבוסס על אחד מהבאים:**

1. אלגוריתם סימטרי עם מפתח מעבר ל-56 ביט
2. אלגוריתם א-סימטרי עם מפתח מעבר ל-512 ביט
3. אלגוריתם קוואנטי (post-quantum, quantum-safe or quantum-resistant)



האגף לפיקוח על היצוא הביטחוני

החרגות לסעיף 5.A.2 (דגשים מרכזיים)

(note 2) המוצרים והרכיבים הבאים לא נדרשים בפיקוח:

(בהתאם להגדרות המדויקות המפורטות בפרק)

- כרטיסים חכמים או מסמך אישי אלקטרוני (כמו Token או e-passport - 'cryptographic activation token' - **נדרש בפיקוח**)
- קוראים / מקודדים של כרטיס חכם
- מכשירי רדיו - טלפון ניידים לשימוש אזרחי בלבד שהותאמו ליישום ספיציפי של תעשייה אזרחית ספיציפית
- נתבים, מתגים, שערים או ממסרים שבהם פונקציונאליות אבטחת מידע מוגבלת לתפעול / ניהול / תחזוקה ושמטמיעים רק שיטות אבטחת מידע ואלגוריתמים ציבוריים או מסחריים

'ההצפנה לחיסיון נתונים' לא כוללת:

(בהתאם להגדרות המדויקות המפורטות בפרק)

- אימות או הרשאות מסוג חתימה דיגיטלית
- תקינות נתונים
- ניהול זכויות יוצר דיגיטליות
- הצפנה או פענוח לתמיכה בבידור / שידורים מסחריים / ניהול תיקים רפואיים
- "רשת מקומית אישית" אלחוטית עם תקני הצפנה מסחריים
- ציוד מאובטח לשימוש בנקאי או עסקאות כסף
- הצפנה שלא הופעלה ויכולה להיות מופעלת רק באמצעות "הפעלת הצפנה" מאובטחת



5.A.2 - אבטחת מידע קריפטוגרפית (2)

▶ "אסימון הפעלה קריפטוגרפי" ('cryptographic activation token') = פריט שתוכנן או עבר שינוי עבור:

➤ הצפנה שהופכת את המוצר למפוקח

➤ **או -** הצפנה שמוסיפה יכולת למוצר

▶ קריפטוגרפיה קוואנטית / Quantum Key Distribution (QKD)

▶ הצפנה ליצירת קודי הפרדת ערוצים; (תיעול – channelizing codes) **או** ערבול

(scrambling) **או** קודי זיהוי רשת

▶ הצפנה ליצירת קוד הפיזור למערכות "ספקטרום מורחב" ("spread spectrum") **כולל** קוד הדילוג למערכות "תדר מדלג"

5.A.3- "אבטחת מידע" לא קריפטוגרפית

מערכות, ציוד ורכיבים עבור "אבטחת מידע" שאינה קריפטוגרפית, כדלקמן:

a. מערכות כבילת תקשורת שתוכננו או הותאמו תוך שימוש באמצעים

מכניים, חשמליים או אלקטרוניים לגילוי חדירה חשאית

הערה 5.A.3.a. חל רק על אבטחת שכבות פיזיות = שכבה 1 של מודל ההתייחסות של חיבור

מערכות פתוחות (ISO / IEC 7498-1) (OSI).

b. תוכננו לצמצם זליגת נתונים מאותות נושאי מידע מעבר למה שנחוץ

לתקינות, בטיחות או לתקני התערבות / הפרעה אלקטרומגנטית.

5.A.4- הכשלה, החלשה או עקיפה של אבטחת מידע

סעיף 5.A.4.a:

- עקיפת מנגנוני הצפנה באמצעות 'פונקציות קריפטאנליטיות' על מנת לשאוב נתונים חסויים / רגישים, כולל טקסט, סיסמאות או מפתחות הצפנה; כולל שימוש ב-Reverse Engineering.

סעיף 5.A.4.b:

- מוצרים שלא צוינו בסעיפים 4.A.5 או 5.A.4.a שנועדו לעקוף בקרות "אימות" או הרשאה של המכשיר על מנת לחלץ מידע גולמי ממכשיר מחשוב או תקשורת

5.A.4.b. - **אינו חל על:**

- מערכות או ציוד המיועד במיוחד לפיתוח או ייצור של מכשיר מחשוב או תקשורת.
- Debugger (גילוי באגים), hypervisor (תוכנה להרצת מכונות וירטואליות);
- פריטים המוגבלים לחילוץ נתונים לוגיים;
- שאיבת נתונים באמצעות חילוץ שבבים (chip-off) או JTAG (=חדירה פיזית אלקטרונית ישירות לזכרון הפיזי של המכשיר).
- פריטים שתוכננו במיוחד ומוגבלים ל-jail-breaking או rooting (תהליכים למתן הרשאות על מכשיר).

סעיפים 5.B - 5.E

5.B - בדיקות, ציוד בדיקה וציוד ייצור:

- ציוד ומוצרים לבדיקה, לפיתוח ולמדידה של מוצרים שהוזכרו בסעיף 5.A

5.D – תוכנה:

- תוכנה שנועדה לתמוך בפונקציה קריפטוגרפית של פריט מפוקח כלשהו

5.E – טכנולוגיה:

- ידע לפיתוח, ייצור ושימוש של הציוד המפורט בסעיפים 5.A.2 , 5.A.3, 5.A.4

או 5.B.2

סיכום



- עם ביטול צו הצופן - אמצעי הצפנה יפוקחו בהתאם לפרק 5.2 בהסדר ואסנאר.
- הפרק מתחיל בהחרגות מפיקוח של מוצרי מדף / רכיבי חומרה עבורם / ציוד לשימוש אישי.
- עיקרי תכולת הפרק:
 - מוצרים שעוסקים באבטחת מידע קריפטוגרפית
 - טכניקות הצפנה לתיעול, ערבול, אפנון ופיזור
 - מוצרים שעוסקים בכבילת תקשורת
 - מוצרים שעוקפים מנגנוני הצפנה
 - ציוד בדיקה וייצור, תוכנה וידע

באחריות היצואן לבחון האם מוצריו נכנסים תחת פיקוח במסגרת צווי הפיקוח ובכלל זה במסגרת פרק 5 (חלק 2) ברשימת הטובין וטכנולוגיות דו-שימושיים שנקבעה בידי הסדר ואסנאר