תקן כלל-ממשלתי למימוש תיעוד ממלכתי מבוסס כרטיס חכם משולב תמ"ר

פרק 2 – גוף התקן לתמ"ר

משרד האוצר - אגף החשב הכללי
רח' קפלן 1 ירושלים 91131 ת"ד 13185 טל': 5317531-02 פקס: 5631285-02

תקן ממשלתי למימוש תיעוד ממלכתי מבוסס כרטיס חכם משולב תמ"ר

פרק 2 - גוף התקן לתמ"ר

1. מבוא

פרק זה מגדיר את התקן הממשלתי למימוש תמ"ר על בסיס תיעוד ממלכתי מבוסס כרטיס חכם, בהתייחס לדרישות מרכיבים שונים של תשתית מפתח ציבורי (תמ"ר).

2. רכיבי מערכת תמ"ר

2.1 המערכת תתבסס על הרכיבים המרכזיים הבאים:

2.1.1 תעודות דיגיטליות, על פי תקן X.509 (ISO/IEC 9594-8).

2.1.2 ניהול ספריות (directories) על פי תקן X.500 (ISO/IEC 9594).

2.1.3 מבנה כרטיס חכם תואם תמ"ר (טיוטת תקן ISO/IEC 7816-15).

2.1.4 ניהול ספריות לתעודות מבוטלות (CRL) (ISO/IEC 9594-8).

2.1.5 פרוטוקול גישה לספריה: DAP ו – LDAP (ISO/IEC 9594-5).

2.2 התקן המרכזי לפיו ימומש תמ"ר, הינו תקן ISO/IEC 9594-8. תקן זה יובהר להלן, תוך התייחסות לסעיפיו השונים ואימוצם בתקן הממשלתי.

2.3 תקן מרכזי נוסף הינו תקן ISO/IEC 7816-15. התקן נמצא אמנם בשלבי **טיוטת תקינה** בלבד, אך עקב חשיבותו, הוא מאומץ כבר כעת בתקן הממשלתי, בגרסתו הנוכחית, תוך עדכונו בעתיד בהתאם לצורך.

3. תמיכה בתקן ISO/IEC 9594-8

3.1 מבוא ותכולה

משרד האוצר - אגף החשב הכללי
רח' קפלן 1 ירושלים 91131 ת"ד 13185 טל': 02-5317531 פקס: 02-5631285

3.1.1 קיימת סדרת תקנים בסיסיים המטפלת בכל הקשור בישות הנקראת "ספריה" (DIRECTORY), ושימוש בספריה לצורך אימות (Authentication).

3.1.2 התקן הבסיסי מגדיר את צורת שמירת המידע לאימות בספריה, כיצד לקבל מידע זה, כיצד המידע נוצר מלכתחילה ומועבר לספריה ומהם הדרכים להשתמש במידע לצורך שירותי אבטחת מידע לאימות.

3.1.3 הפרוטוקול שבו נעשה שימוש לשליפת נתונים מהספרייה הוא DAP (Directory Access Protocol), המוגדר בתקן ISO/IEC 9594-5 (X519). התקן הממשלתי מאמץ תקן זה וכן את הפרוטוקול הידוע בשם "LDAP" (Light DAP).

3.2 <u>אימות חזק (סעיף 7 בתקן הבסיסי)</u>

3.2.1 התקן הממשלתי יתבסס על שיטת "אימות חזק" (Strong Authentication) המוגדרת בסעיף 7 בתקן הבסיסי.

3.2.2 ייצור תעודות דיגיטליות ייעשה על ידי "גורם מאשר".

3.2.3 ככלל, מסגרת האימות (אותנטיקציה) אינה תלויה בשימוש באלגוריתם הצפנה מסויים דווקא, ובלבד שיש לאותו אלגוריתם את התכונות המתוארות בסעיף 7 בתקן הבסיסי. לכאורה, ניתן להשתמש באלגוריתמים שונים. ואולם, משתמשים אשר מעונינים לבצע אימות, צריכים לתמוך באותו אלגוריתם הצפנה, על מנת שהאימות יתבצע בצורה נכונה. כך, במסגרת ההקשר של קבוצת יישומים מסויימת, הבחירה באלגוריתם אחד תשרת את המטרה של הרחבה מרבית של קהילת המשתמשים אשר מסוגלים לבצע אימות ותקשורת בצורה בטוחה.

3.2.4 בהתאם לכלל זה, התקן הממשלתי תומך באלגוריתם הצפנה יחיד לתשתית מפתח פומבי, קרי - RSA, המתואר בין היתר בנספח D של התקן הבסיסי.

3.2.5 לצורך ייצור החתימה הדיגיטלית של הגורם המאשר, ייעשה שימוש באלגוריתם RSA (Rivest- Shamir-Adelman algorithm) באורך מפתח של 2,048 ביט.

משרד האוצר - אגף החשב הכללי
רח' קפלן 1 ירושלים 91131 ת"ד 13185 טל': 02-5317531 פקס: 02-5631285

3.2.6 לצורך ייצור החתימה הדיגיטלית של משתמש הקצה, ייעשה שימוש באלגוריתם RSA (Rivest- Shamir-Adelman algorithm) באורך מפתח של 1,024 ביט.

3.2.7 פונקציות ערבול (HASHING) : ייעשה שימוש בפונקצית הערבול המפורטת להלן, כמוגדר בתקן הבסיסי ISO/IEC 10118-3: 1998 : Dedicated Hash Function 3 (SHA-1).

3.3 תעודות דיגיטליות, המפתח הציבורי של המשתמש ואמצעי שונים לניהול התעודות

3.3.1 התקן הממשלתי מאמץ את סעיפים 8 – 13 בתקן הבסיסי.

3.3.2 בפרט, מאומץ מבנה התעודה הדיגיטלית, תואם ל- X.509, המוגדר בתקן הבסיסי.

3.3.3 להלן טבלה המציגה את הערכים הבסיסיים שיהיו בתעודה הדיגיטלית הממשלתית :

משמעות	ערך	שדה
תעודת X.509 גירסא 3	2	VERSION
מספר חד-ערכי של התעודה, אצל כל גורם מנפיק	מספר התעודה	SerialNumber
מזהה האלגוריתם, עבור אלגוריתם החתימה שבשימוש הגורם המאשר	sha1With RSA 2048Encryption	Signature
פרטי מנפיק התעודה	Country = IL קוד מנפיק שם מנפיק	Issuer
תאריכי תוקף התעודה	תאריך תחילה תאריך פג תוקף	Validity
פרטי בעל התעודה	Country = IL ; שם משפחה ; שם פרטי ; מספר הזהות ;	Subject

משרד האוצר - אגף החשב הכללי
רח' קפלן 1 ירושלים 91131 ת"ד 13185 טל' : 02-5317531 פקס : 02-5631285

	שם הארגון ; יחידת משנה בארגון ; תואר.	
מזהה אלגוריתם חתימה של בעל התעודה	RSA Encryption	SubjectPublicKey
עבור תעודה מס' 1 לזיהוי ואימות	Identification & authentication	KeyUsage#1
עבור תעודה מס' 2 לחתימה דיגיטלית	Digital Signature & Non Repudiation	KeyUsage#2

משרד האוצר - אגף החשב הכללי
רח' קפלן 1 ירושלים 91131 ת"ד 13185 טל' : 02-5317531 פקס : 02-5631285