מדינת ישראל
ממשלת ישראל

משרד הפנים
רשות האוכלוסין וההגירה

משרד האוצר
מטה התקשוב הממשלתי
ממשל זמין

מנפיק ממשלתי לתעודות אימות
(ממיל"א)
מסמך מדיניות תעודה
Certificate Policy - CP
תעודות אלקטרוניות לאימות
לתושבי מדינת ישראל

מהדורה 1.6

תקף החל מ-1 ביולי 2013

מדינת ישראל
ממשלת ישראל

משרד הפנים
רשות האוכלוסין וההגירה

משרד האוצר
מטה התקשוב הממשלתי
ממשל זמין

מעקב אחר מהדורות ושינויים

מהדורה	תאריך	כתב/ערך	פרטי העדכון	סטטוס
1.6	26.6.13	עופר ישי	עדכון אחרון לאחר קבלת הערות רמו"ט ורשות האוכלוסין, לקראת פרסום באתר	מהדורה סופית לפרסום

טבלת אישורים

	שם	תפקיד	חתימה
נערך על ידי	עופר ישי	מרכז הקמת הגמ"מ, ממשל זמין	
נבדק על ידי	יעקב גוטקין	מנהל תחום PKI ומו"פ, ממשל זמין	
אושר על ידי	יוגב שמני	מנהל אגף מערכות מידע, רשות האוכלוסין וההגירה	

מדינת ישראל
ממשלת ישראל

משרד הפנים
רשות האוכלוסין וההגירה

משרד האוצר
מטה התקשוב הממשלתי
ממשל זמין

תוכן עניינים

1. מבוא

1.1. תפישה כוללת

מסמך "מדיניות תעודה" זה בא לתאר את מדיניות ממשלת ישראל באשר להנפקת **תעודות אלקטרוניות לאימות** (להלן גם – "תעודות לאימות" או "תעודות אימות").

מסמך זה נועד הן **לתושבי ישראל** שהם **בעלי התעודות האלקטרוניות לאימות** והן **לגורמים מסתמכים** שיבקשו להסתמך על תעודות אלו לצורך אימות זהות בעליהן.

הבסיס החוקי להנפקת תעודות אלקטרוניות לאימות הוא **חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע – 2009** (להלן – "חוק הכללת אמצעי הזיהוי").

על פי חוק הכללת אמצעי הזיהוי הותקנו **תקנות מרשם אוכלוסין (תעודה אלקטרונית לאימות), התשע"ב-2011** (להלן – "תקנות תעודה לאימות").

מאחר והמדיניות והכללים להנפקת התעודות האלקטרוניות לאימות נקבעו הלכה למעשה בחקיקה הראשית ובתקנות כאמור לעיל, הרי שמסמך "מדיניות תעודה" זה בא להבהיר ולתאר את המדיניות אך לא לקבוע אותה. בנוסף על כך, המסמך מפרט ומסדיר נושאים שונים המתחייבים מהחוק והתקנות. יובהר כי היה ותתגלה סתירה בין האמור במסמך זה לבין האמור בחוק או בתקנות, האמור בחוק או בתקנות גובר.

האחריות החוקית להנפקת תעודות לאימות הינה של רשות האוכלוסין וההגירה במשרד הפנים (להלן – הרשות).

התעודות לאימות ייכתבו על גבי כרטיסי תעודות הזהות, כרטיסי תעודות הזהות יונפקו לתושבים על ידי הרשות ובאחריותה. זיהוי המבקשים (התושבים) לצורך הנפקת התעודה לאימות ייעשה על ידי הרשות ובאחריותה.

הנפקת התעודה לאימות והחזרתה לרשות תיעשה על ידי **מ**נפיק **מ**ממשלתי **ל**תעודות **א**ימות (להלן – **ממיל"א**). הרשות הסמיכה את מערך ממשל זמין במשרד האוצר להקים את התשתית המתאימה לצורך כך ולבצע משימה זאת, במסגרת הסדר בין שני הגופים. העובדה שמדובר בפרויקט לאומי של ממשלת ישראל, מבטיחה פעילות רציפה, מאובטחת ומבוקרת לתועלת תושבי המדינה, החברה והכלכלה.

במהלך הכנת מסמך זה, התייעץ ראש הרשות, הן ישירות והן באמצעות הממיל"א, עם הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (רמו"ט), כנדרש על פי התקנות.

1.2. שם המסמך וזיהויו

מסמך זה מזוהה ע"י מזהה האובייקט (OID) הבא הנמצא בתעודה האלקטרונית לאימות עצמה:

Government-of-Israel—CA -AUTH-CP-v1:== 2.16.376.101.1.2.1.4.1

הממיל"א ינפיק את התעודות לאימות בהתאם למסמך זה. תעודה לאימות הנושאת מזהה אובייקט זה, משמע שהונפקה במסגרת מערך הממיל"א ובהתאם לנהליו. מסמך זה נערך ככלל בהתאם להוראות מסמך RFC 3647 של ארגון IETF ובהתאמות המתחייבות. בנוסף למסמך זה ניתן לעיין ב"מסמך הנהלים" (CPS) אשר יפרט את נהלי העבודה בהקשר להנפקת התעודות לאימות. שניהם מהווים את "מסמך הנהלים" של הממיל"א המוזכר בתקנות תעודה לאימות.

1.3. המשתתפים בתשתית המפתח הציבורי (תמ"ר) עבור התעודה לאימות

1.3.1. רשות האוכלוסין וההגירה (הרשות)

בכל הקשור להנפקת תעודות לאימות, הרשות פועלת הן כאחראית חוקית על המערך כולו והן כ"רשות רושמת" במונחי תשתית מפתח ציבורי (תמ"ר).

הגדרת "קציני הרישום" (RAO) כוללת את מנהלי הלשכות של הרשות, הממונים על תחום המרשם בלשכות ופקידי קבלת הקהל ("נותני השירות") מטעם הרשות. קציני הרישום יוודאו את נכונות ותקינות פרטי המבקש, יחתמו על הבקשה ויעבירו אותה לאישור. הבקשה תאושר ותיחתם בנוסף על ידי מערכת הניהול הממוחשבת של הרשות וזאת כאישור לאימות בדיקת הבקשה, לתקינותה ולכשירות הפקיד (RAO) שחתם על הבקשה, טרם העברת הבקשה לממיל"א.

בעל תעודה יכול ליזום בקשה לביטול תעודתו, במקרה של אובדן שליטה עליה, כמפורט בהמשך מסמך זה. הבקשות לביטול תעודות לאימות ייקלטו על ידי קציני הרישום, או על ידי מוקד הדיווח הטלפוני שיהיה בממיל"א, במערכות המחשוב של הרשות ויועברו לממיל"א בממשק ממוחשב.
יובהר כי בכל מקרה, הבקשה חייבת לעבור באמצעות מערכת המחשוב של הרשות שרק ממנה ניתן להעביר בקשה **לביטול** תעודה לאימות, לממיל"א. הממיל"א אינה רשאית ליזום בקשת ביטול של תעודת תושב.

1.3.2. מנפיק ממשלתי לתעודות אימות (ממיל"א)

הממיל"א הוא הגורם הממשלתי המנפיק את התעודות לאימות עבור הרשות. לצורך כך יוקם ע"י הממיל"א "עוגן אמון" (Anchor of trust) או "שורש הממיל"א" (RCA - ROOT CA) עבור התעודות לאימות. הבהרה: **הממיל"א ימומש בפועל על ידי ארגון הגמ"מ במערך ממשל זמין**.

"עוגן האמון" מהווה נקודת מוצא למערך האמון. כלומר, מי שמקבל לידיו תעודה אלקטרונית כלשהי שנחתמה על ידי "עוגן האמון", יתייחס אליה כאל תעודה מהימנה. על מנת ליצור ולשמר את האמון הזה, נוצרת "שרשרת אמון", שתחילתה "עוגן האמון", וסופה היא התעודה הדיגיטלית הנמסרת לתושב. "עוגן האמון" חותם על השרתים התפעוליים, אשר מצדם חותמים על התעודות לתושבים. ניתן להגיע מהתעודה לתושב, עד ל"עוגן האמון" ולוודא שאכן מדובר באותה "שרשרת אמון".
על מנת להתחיל את "שרשרת האמון", נדרש לוודא שגם התעודה של "עוגן האמון" תיחתם בצורה מאובטחת. בהתאם, גם המפתח הציבורי של "עוגן האמון" נחתם על ידי מנגנון החתימה של "עוגן האמון" עצמו, במה שקרוי "חתימה עצמית", וכך מתקבלת התעודה האלקטרונית של "עוגן האמון".

מתחת ל"עוגן האמון" נמצאים ופועלים שרתים תפעוליים (OCA- Operational CA), שהמפתחות הציבוריים שלהם נחתמים על ידי "עוגן האמון", במסגרת התעודות האלקטרוניות של השרתים התפעוליים. השרתים התפעוליים מצדם חותמים על התעודות לאימות של תושבי מדינת ישראל.
הבקשות להנפקת התעודות והתעודות החתומות של התושבים מועברות בממשק יישומי מקוון (API) דו-כיווני בין מערכת המידע של הרשות לבין מערכת המידע של הממיל"א. יצירת התעודה לאימות וכתיבתה על כרטיס תעודת הזהות מתבצעת כאשר התושב נוכח פיזית בלשכות הרשות מול נותן השירות.

הממיל״א יטפל, עבור הרשות, בכל תהליכי מחזור החיים של התעודות לאימות, לרבות – יצירתן, ביטולן במקרה הצורך ופרסום מידע על הסטטוס שלהן לצדדים מסתמכים.
תפקידיו המרכזיים של הממיל״א בהקשר לתעודות לאימות הם:

א. הנפקת תעודות לאימות לתושבים, על סמך הזיהוי המבוצע על ידי הרשות.
ב. ניהול מאגר תעודות לאימות שהונפקו על ידו.
ג. ביטול תעודה לאימות לפי בקשת בעל התעודה, או לפי בקשה של הרשות, מיד לאחר קבלת הבקשה ואימות זהות המבקש או בהתקיים נסיבות אחרות המנויות בחוק ובתקנות.
ד. ניהול מאגר תעודות לאימות בטלות באופן שיהיה זמין ברמה גבוהה לצדדים מסתמכים. מאגר זה יהיה זמין באינטרנט לעיון הציבור.

״עוגן האמון״ (RCA) והשרתים התפעוליים (OCA) שישמשו את הממיל״א לצורך הנפקת התעודות לאימות, יופרדו פיזית ולוגית מתשתית ממשל זמין בכלל ומתשתית הגמ״מ להנפקת תעודות אלקטרוניות לחתימה בפרט. יחד עם זאת, חלק מהתשתית ההיקפית, כגון מערך התקשורת ואבטחת המידע, תהיה משותפת עם התשתית להנפקת תעודות אלקטרוניות לחתימה.

הממיל״א עושה שימוש במערכות חומרה ותוכנה מהימנות, המעניקות הגנה סבירה מפני חדירה, שיבוש, הפרעה או גרימת נזק לחומר מחשב ומקנות רמה סבירה של זמינות ואמינות. הממיל״א יעמוד בכל זמן פעילותו בדרישות אבטחת מידע פיזית ולוגית, נהלי עבודה מסודרים ודרישות תיעוד.
מערכות ההגנה כוללות ״ליבה״ מאובטחת של תוכנת חתימה אלקטרונית ומערך של אמצעי תקשורת ואבטחה שנועדו להגן על הליבה, כך שיגיעו אליה רק בקשות ממקור מוסמך, מאובטח ובדוק. אמצעי האבטחה כוללים חומת אש, הצפנה, שרת קדמי – ״פרוקסי״ (proxy) - הבודק את המידע לפני הגעתו לשרת הפנימי הרגיש, וכן מנגנוני בקרה וביקורת הרושמים כל פעולה שבוצעה במערכת.
הממיל״א יפעיל מערכות אלה, וכל מערכת נוספת הנדרשת לפי שיקול דעתו.
<u>הבהרה</u>: בארכיטקטורה של הממיל״א לא נכלל גורם מאשר ביניים – (Intermediate CA). השרתים התפעוליים נחתמים ישירות על ידי ״עוגן האמון״.

1.3.3. בעלי התעודות

בעלי התעודות הינם תושבי מדינת ישראל שלהם יונפקו תעודות לאימות בהתאם למסמך זה.

1.3.4. צדדים מסתמכים

הסתמכות גורמים צד ג׳ (גורמים מסתמכים) על התעודות לאימות תיעשה בהתאם לחוק, לתקנות ולמסמך זה, באמצעות כלים לבדיקת תוקפן ותקפותן.
על סמך זיהוי האמצעי לאימות החתימה של הממיל״א, צד מסתמך יכול להיות בטוח כי מדובר בתעודה שנחתמה על ידי אמצעי החתימה של הממיל״א. צד מסתמך יוכל לבדוק כי במועד בדיקתו את רישומו של הממיל״א, הממיל״א היה פעיל ותקף.
צד מסתמך יכול להיות בטוח, בכפוף לאמור במסמך זה, כי בעל התעודה לאימות זוהה כנדרש בטרם הונפקה לו התעודה לאימות.

1.3.5. משתתפים אחרים

בשלב זה אין משתתפים אחרים בתהליך.

1.4. שימושים בתעודה לאימות

1.4.1. שימושים מורשים

ניתן להשתמש בתעודה לאימות לצורך הזדהות ואימות הזיהוי בגישה למערכות מידע ורשתות מחשבים אשר הותאמו לעבודה עם תעודות לאימות. ככלל, יובהר כי כל שימוש בתעודה לאימות על תעודת הזהות הינו מותר, אלא אם כן נאמר מפורשות אחרת.
האחריות בגין שימוש בתעודה הינו באחריות בעליה. בהתאם, האחריות בגין הסתמכות על השימוש בתעודה הינו באחריות המסתמך.

1.4.2. שימושים אסורים

תעודה לאימות לא תשמש לחתימה אלקטרונית בכלל ולא להצפנת מידע.

1.5. ניהול המדיניות

1.5.1. הארגון האחראי על ניהול המסמך

ראש רשות האוכלוסין הוא האחראי על ניהול המסמך, עדכונו ובקרתו, באמצעות מנהל הממיל"א ואיש הקשר מטעמו.

1.5.2. איש קשר

תפקיד: מנהל הממיל"א, או מי מטעמו

דוא"ל: info-igca@tehila.gov.il

טלפון: 02-6664666

איש הקשר זמין למענה על שאלות בעניין מסמך זה.

1.5.3. אחראי על קביעת התאמת המסמך למדיניות

האחראי לכך הינו ראש רשות האוכלוסין באמצעות איש הקשר שצוין בסעיף 1.5.2 לעיל.

1.5.4. תהליכי אישור המסמך

תהליך אישור המסמך כולל אישור פנימי על ידי הנהלת רשות האוכלוסין ועל ידי הנהלת הממיל"א.

1.6. הגדרות וקיצורים

ראה נספח 1.6 למסמך זה.

2. אחריות לפרסום ומאגרי מידע

2.1. מאגרי מידע

הממיל"א אחראי לפרסום מידע לגבי פעילותו וכן לתפעול שוטף של מאגרי המידע שלו שכוללים:

- מאגר תעודות שהונפקו: כולל את כל התעודות שהונפקו. זהו מאגר פנימי של הממיל"א שאינו חשוף לגורמי חוץ.
- מאגר תעודות בטלות: כולל את רשימת התעודות הבטלות בלבד (CRL). מאגר זה זמין לציבור הרחב ללא הגבלה.
- מאגר תקפות תעודות: מאגר שיאפשר לגורמים מורשים בלבד לקבל מידע מקוון על תקפות תעודה מסוימת, על ידי הפניית שאילתה בפרוטוקול OCSP (הערה: הפעלת ה-OCSP לא בהכרח תתבצע מתחילת ההפעלה המבצעית).

2.2. פרסום מידע

כל תעודה לאימות שתונפק על פי מסמך זה, תפרט את המיקומים והפרוטוקולים השונים בהם ניתן לקבל מידע על מצבה (התקפות שלה). במיקומים אלו תתפרסם רשימת התעודות הבטלות העדכנית וכן ניתן יהיה לקבל מידע על רשימות תעודות בטלות היסטוריות לתקופה מוגבלת. באתר הממיל"א שכתובתו http://e.gov.il/Services/Approve/Pages/DigitalId.aspx, תתפרסם תעודת המפתח הציבורי של הממיל"א לצורך אימות תעודות לאימות של תושבים, שנחתמו על ידי הממיל"א.

2.3. זמן ותדירות הפרסום

מנהל הממיל"א אחראי לפרסם כל שינוי המותר לפרסום במסמך זה תוך לא יאוחר מ-30 ימי עבודה ממועד אישור השינוי. השינוי יאושר על ידי ראש הרשות. לא יהיה ניתן להחיל שינויים רטרואקטיבית.
מנהל הממיל"א אחראי לעדכן באופן מידי אם בוצע שינוי בסטטוס תעודת "עוגן האמון", תוך שעתיים לכל היותר מרגע שינוי הסטטוס, באישור ראש הרשות.
מנהל הממיל"א יעדכן את רשימת התעודות לאימות הבטלות של התושבים אחת ל- 12 שעות.
תוקף רשימת תעודות בטלות שתונפק יהיה למשך 72 שעות. הכוונה בכך היא להבטיח כי גם אם משום מה יש עיכוב בפרסום רשימה חדשה, עד כדי 72 שעות, הרשימה הקודמת עדיין בתוקפה. רשימת התעודות הבטלות העדכנית תימצא ב"נקודת פרסום הרשימה" באתר הממיל"א – CDP – CRL Distribution Point, שההפניה אליו תהיה מהתעודה עצמה.
על גורמים מסתמכים לערוך בדיקה מקוונת במאגר התעודות הבטלות הנ"ל, טרם הסתמכותם על תעודה לאימות מסוימת, על מנת לוודא בדיקת תקפות לפי הרשימה העדכנית ביותר. אם לא בוצעה בדיקה, הרי שככל שייגרם נזק למסתמך, יהיה נזק זה באחריות המסתמך בלבד. אם בוצעה בדיקה בצורה תקינה של רשימת התעודות הבטלות העדכניות, האחריות במקרה של תקלה תהיה של הרשות.
הממיל"א יאפשר גם גישה לרשימות קודמות, למשך כשנה אחת לאחור.

2.4. בקרת גישה למאגרים

מידע שהוא נחלת הציבור יהיה זמין באמצעות אתר האינטרנט של הממיל"א ללא צורך בתהליכי זיהוי ובקרת גישה מיוחדים. מידע זה כולל את רשימת התעודות הבטלות העדכנית ורשימות קודמות של עד שנה לאחור במקוון (רשימות קודמות יישמרו במאגרי הממיל"א למקרה שיידרשו בעתיד).

באתר האינטרנט של הממיל"א לא יפורסם מידע חסוי, כגון - נהלי עבודה פנימיים. מנהל הממיל"א ידאג לשמירה על חסיון מידע זה באמצעות הימנעות מפרסומו ואבטחת אתר האינטרנט באמצעים המקובלים, ויאפשר גישה רק למורשים לכך.
כמו כן, באחריות מנהל הממיל"א לוודא שבאתר האינטרנט לא יפורסם מידע אישי שאסור לפרסום על פי חוק הגנת הפרטיות.
מידע הנמסר מהרשות כחלק ממערכת "אביב" לצרכי ביטול תעודות לאימות, יימסר לאחר קבלת אישור מתאים בהתאם לחוק הגנת הפרטיות.

3. זיהוי ואימות

תהליכי הזיהוי והאימות מתבססים על התשתית החוקית של חוק מרשם האוכלוסין, חוק הכללת אמצעי זיהוי וחוק חתימה אלקטרונית, והתקנות לפיהם.
סעיף זה מתאר את התהליכים שבאמצעותם מזהים ומאמתים את מבקש התעודה לאימות טרם הנפקתה, הנפקת תעודה חדשה או בקשה לביטול תעודה קיימת.
סעיף זה דן בנוסף בקביעת השמות לבעלי התעודות במסגרת מבנה התעודה ובאופן הבטחת חד-ערכיות במרחב השמות.
התהליך כולל באופן סכמתי את תהליכי המשנה הבאים שיפורטו בהמשך:

- זיהוי ואימות המבקש בלשכה, כולל תהליכי הרכשת הביומטריה על ידי הרשות, כהגדרתם בסעיף 3 לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע – 2009.
- הגשת הבקשה לכרטיס תעודת זהות חדש.
- הנפקת כרטיס תעודת הזהות במפעל מילוי הפרטים והעברתו ללשכות כולל חילול צמד המפתחות לאימות וסיסמאות ראשוניות.
- הנפקת תעודה לאימות על בסיס המפתח הציבורי של הכרטיס מול הממיל"א (מתבצע בלשכות הרשות).
- כתיבת התעודה על גבי כרטיס תעודת הזהות ומסירתו לתושב (מתבצע בלשכות הרשות).

3.1. מוסכמות הגדרת שמות

3.1.1. סוגי שמות

תעודה לאימות תכלול בפרט את השמות הבאים:

- שדה ה"נושא" (Subject) יכיל שם בשפה האנגלית. בנוסף לרישום בשדה "השם המקובל" (CN) יירשם השם פרטי (Given name) ושם המשפחה (Surname).
- שדה "שם נושא חלופי" (Subject Alternate Name) יכלול את השם בשפה העברית (במבנה Directory string), הן ב-CN והן בשם הפרטי ובשם המשפחה.

3.1.2. הצורך בשם משמעותי

- שדה ה"נושא" (Subject) יכיל את "השם הייחודי" באנגלית (Distinguished name –DN) כחלק משדה ה"השם המקובל" (CN) כולל מספר הזהות, משום ששם בלבד אינו מהווה זיהוי חד-ערכי ומשמעותי.
- ערך שדה ה"מדינה" (Country -C) בתוך שדה ה"נושא" (Subject) יהיה IL.

3.1.3. סוגי שמות שונים

שמות לא יתורגמו. שמות באנגלית ושמות בעברית יופיעו בשדות נפרדים.

3.1.4. חד-ערכיות השם

שם התושב (שם פרטי ושם משפחה) במרשם האוכלוסין בפני עצמו אינו חד-ערכי. לכן, לשם התושב יתווסף מספר הזהות ההופך את פרטי התושב לחד-ערכיים.

3.2. זיהוי ואימות ראשוני

3.2.1. הוכחת החזקה במפתח פרטי של כרטיס תעודת הזהות

תהליך הנפקת כרטיס תעודת הזהות על כל רכיביו מבוקר ומנוהל על ידי מדינת ישראל, באמצעות הרשות, על מנת להבטיח את מהימנותו.
בשלב ראשון מתבצע תהליך זיהוי ואימות מקיף כמפרט בסעיף 3.2.3.
בשלב הבא נשלחת בקשה להנפקת כרטיס תעודות זהות חדש, כולל כל הפרטים הנדרשים להנפקה זאת, לרבות נתונים ביומטריים.
צמד המפתחות לאימות הכולל את "המפתח הפרטי" ו"המפתח הציבורי", נוצר בתהליך הייצור האוטומטי הראשוני במפעל מילוי הפרטים, על גבי כרטיס תעודת הזהות, וזאת ללא נוכחות בעל כרטיס תעודת הזהות.
המפתח הפרטי אינו יכול להיות מיוצא החוצה מכרטיס תעודת הזהות, בשום מצב במחזור חיי כרטיס תעודת הזהות.
החל מסיום תהליך מילוי הפרטים במפעל ועד לקבלת כרטיס תעודת הזהות על ידי בעל התעודה בתהליך המסירה, **הכרטיס סגור ונעול באמצעות סיסמאות ולא ניתן לבצע בו שום פעולה**.
בתהליך מסירת כרטיס תעודת הזהות מקבל בעל התעודה מעטפה ובה סיסמאות שונות, שחלקן נועדו לפתיחת כרטיס תעודת הזהות, לאתחולו ולשחרורו מהנעילה וחלקן לשימוש שוטף לאחר מכן. את הסיסמאות ניתן לראות רק לאחר פתיחת המעטפה הפיזית והורדת הכיסוי שמודבק מעליהן, בצורה שמאפשרת לפסול מעטפה שנפתחה קודם לכן.
כרטיס תעודת הזהות בנוי טכנולוגית כך שלא ניתן לייצא את המפתח הפרטי ממנו וכן לא ניתן לייבא אליו מפתח פרטי ממקור חיצוני. כתוצאה מכך, כשהתושב מקבל כרטיס תעודת זהות בתהליך המסירה מנותן השירות, מובטח שאכן מדובר בכרטיס תעודת הזהות השייך לו ולו בלבד וכי לא ניתן היה לגשת למפתח הפרטי ולעשות בו כל שימוש עד לשלב זה.
בשלב מסירת התעודות על ידי נותן השירות בלשכות הרשות, כרטיס תעודת הזהות מוכנס לקורא כרטיסים מאובטח והתושב מקיש את הסיסמה הידועה רק לו, מבלי שעמדת המחשב תיחשף לסיסמה. באופן זה מבטיחים כי הבקשה לתעודה אלקטרונית המגיעה לממיל"א, בוצעה כאשר כרטיס תעודת הזהות נמצא פיזית בידי התושב וכי התושב אפשר את ביצוע הפעולה על ידי הקשת הסיסמה הידועה רק לו.

3.2.2. אימות זהות ארגונית

לא רלבנטי.

3.2.3. אימות זהות אישית

תהליך זה מבוצע על ידי נותני השירות ברשות. תהליך האימות כולל, בין היתר, בדיקת תיעוד מזהה קודם ותחקור המבקש.
המבקש יעבור תהליך בדיקה קפדני עד שזהותו תאומת ובקשתו תאושר.
התושב יתבקש למסור עד שתי שאלות מזהות ייחודיות שאינן רשומות במרשם, אשר יאפשרו לזהותו במקרה שיתקשר לדווח על אובדן כרטיס תעודת הזהות או על פגיעה כלשהי בשליטתו בה ויבקש לבטלה.
תעודה לאימות תונפק לכל בגיר שזכאי לקבל תעודת זהות.
תעודה לאימות תונפק לקטינים שזכאים לקבל תעודת זהות.
תעודה לאימות תונפק גם לחסויים עפ"י חוק הכשירות המשפטית והאפוטרופסות, התשכ"ב-1962, בהתאם להנחיות הזיהוי המופיעות בתקנות.

3.2.4. אימות הסמכות

אימות הסמכות לבקשת תעודה לאימות על ידי תושב, תיבדק במסגרת נוהל העבודה של הרשות. האימות יחול גם במקרה של מייצג, כגון – אפוטרופוס או מי שהוסמך משפטית לפעול בשם תושב אחר בכל צורה שהיא. יובהר כי מסמך זה אינו עוסק באימות של סמכות אדם לפעול בשם ארגון כזה או אחר, אלא רק בישויות שהן אנשים (תושבים) ולא בישויות משפטיות (כגון, תאגיד או אנשי מקצוע בעלי מעמד סטטוטורי כגון רואי חשבון ועורכי דין).

3.3. בקשות למפתח חדש

3.3.1. בקשות למפתח חדש ("אמצעי אימות" על פי תקנות תעודה לאימות)

אם יידרש לחולל צמד מפתחות חדש לאימות, יבוצע תהליך **הנפקת כרטיס תעודת זהות חדש**. לא יבוצע תהליך של חילול צמד מפתחות חדש לאימות, או הנפקת תעודה חדשה לאימות לאחר ביטול התעודה הקודמת, **על גבי כרטיס תעודת זהות קיים**. גם אם זמן קצר לאחר הביטול (כגון עקב דיווח על אובדן), נמצאה האבדה של כרטיס תעודת הזהות הקודם, לא ניתן לחדש כרטיס זה ויש להנפיק כרטיס תעודת זהות חדש.

4. דרישות תפעוליות של מחזור חיי התעודה לאימות

4.1. בקשה לתעודה לאימות

4.1.1. מי יכול להגיש בקשה

כל תושב שזכאי לקבל כרטיס תעודת זהות מהרשות, על פי חוק, תגיש הרשות בקשה לממיל״א להנפקת תעודה לאימות עבורו. הנפקה זאת מחויבת על פי החוק ומהווה חלק בלתי נפרד מהנפקת כרטיס תעודת הזהות, וזאת להבדיל מתעודה לחתימה שתונפק רק לאחר בקשה מפורשת של התושב. במלים אחרות, התושב מגיש בקשה לרשות להנפקת כרטיס תעודת הזהות; הרשות פונה לממיל״א בבקשה להנפיק תעודה אלקטרונית לאימות עבור התושב; הממיל״א מנפיק את התעודה, מחזיר אותה לרשות, אשר משלימה את התהליך על ידי כתיבת התעודה על כרטיס תעודת הזהות. כרטיס תעודת הזהות נמסר במצב זה לתושב.
הבהרה: קטין או חסוי, החייב לשאת תעודת זהות, תונפק לו תעודה לאימות.

4.1.2. תהליך הרישום והאחריות

לאחר אימות וזיהוי המבקש, נותן השירות ייצור את הבקשה, יחתום עליה (חתימת RAO) וישגר אותה למערכת המחשב המרכזית של הרשות. אם הבקשה תימצא תקינה, אזי היא תיחתם אלקטרונית על ידי מערכת המחשוב המרכזית של הרשות, תועבר לממיל״א אשר לאחר בדיקתה ינפיק תעודה לאימות ויחזירה לרשות. הרשות אחראית לכתיבת התעודה האלקטרונית לאימות על גבי השבב שנמצא בכרטיס תעודת הזהות.

4.2. תהליך עיבוד הבקשה

4.2.1. ביצוע זיהוי ואימות

תעודה לאימות תונפק לאחר שהתושב יזדהה כנדרש בלשכת הרשות בפני נותן השירות וזהותו תאומת, על פי נהלי העבודה.

4.2.2. אישור או דחיה של בקשות לתעודות לאימות

הרשות תעביר לממיל״א בקשה לתעודה לאימות רק אם תהליך הזיהוי והאימות הסתיים בהצלחה.
הרשות תדחה העברת בקשות לממיל״א אם תהליך הזיהוי והאימות לא הסתיים בהצלחה, או אם המבקש נדרש להיות מיוצג על פי חוק הכשרות המשפטית והמייצג אינו עומד בהוראות חוק זה.
ככל שיידרש לשלם אגרה עבור הבקשה, תשלום האגרה מהווה תנאי לאישור הבקשה.

4.2.3. משך הזמן הנדרש לעיבוד בקשה לתעודה לאימות

עיבוד בקשה לתעודה לאימות יהיה מידי ויתבצע בעת ההנפקה כאשר התושב נמצא באתרי הרשות.

4.3. הנפקת התעודה לאימות

4.3.1. פעולות הממיל"א במהלך הנפקת התעודה לאימות

הבקשה החתומה תיבדק על ידי הממיל"א. אם ימצא שהבקשה אינה תקינה על פי רשימת בדיקות לוגיות שנקבעה, שעיקרן בדיקת החתימות, בדיקת התחביר ובדיקות טכניות של תאימות לפרוטוקולים ואבטחת מידע, תוחזר הודעה לרשות עם פירוט סיבת הדחייה. אם הבקשה תקינה, תונפק התעודה לאימות ותוחזר לרשות לצורך כתיבתה על גבי כרטיס תעודת הזהות.

4.3.2. הודעה לבעל התעודה לאימות

כחלק מתהליך הנפקת כרטיס תעודת הזהות, תועבר על ידי הרשות הודעה לתושב על מנת שיגיע למקום המסירה שסוכם עימו מראש בעת הגשת הבקשה, לקבלתה. כרטיס תעודת הזהות יועבר למקום המסירה. המעטפה עם הסיסמאות השונות לפתיחה ולשימוש בכרטיס, תועבר ממפעל מילוי הפרטים בהעברה נפרדת ואף פעם לא באותה הובלה עם כרטיסי תעודות הזהות המקבילים. המעטפה תימסר לתושב על ידי נותן השירות ברשות. בעת מסירת התעודה, על התושב יהיה לבדוק כי המעטפה סגורה וכי לא ניתן לראות מבחוץ את פרטי הסיסמאות המופיעות בה. אם התושב יגלה או יחשוד שהמעטפה נפתחה קודם לכן, יופעל נוהל העבודה המתאים של הרשות.
הסיסמאות המתאימות שקיבל, ישמשו את התושב לצורך שחרור כרטיס תעודת הזהות מנעילה, אתחולו ושימוש שוטף בו לצורך אימות.
כמו כן, יומלץ לתושב על ידי נותן השירות ברשות, להחליף בהקדם האפשרי את הסיסמה שקיבל במעטפה בסיסמה חדשה שתיבחר על ידי התושב באופן עצמאי. החלפת הסיסמה תוכל להיעשות בלשכת הרשות בעת קבלת כרטיס תעודת הזהות או מאוחר יותר באמצעות תוכנת תל"ם-אישי.

4.4. קבלת התעודה לאימות

4.4.1. התנהלות בתהליך קבלת התעודה לאימות

התעודה לאימות תונפק באופן מאובטח ע"י הממיל"א במסגרת תהליך מסירת כרטיס תעודת הזהות לתושב. המסירה תתבצע ככלל בלשכות הרשות. הערה: אם תתקיים מסירה גם באתרים אחרים שיאושרו על ידי הרשות, יותאמו הנהלים לתהליכי מסירה אלו.
התושב יידרש טרם המסירה להזדהות ביומטרית על מנת לוודא שכרטיס תעודת הזהות נמסר לאדם הנכון שנתוניו הביומטריים נמצאים על גבי כרטיס תעודת הזהות. במקרה ולא נלקחו טביעות אצבע של התושב בעת ההרכשה, או במקרים אחרים בהתאם לנהלי הרשות, ההזדהות תהיה על סמך זיהוי של מקבל הכרטיס מול התצלום מהכרטיס שלא באמצעות תוכנה.

4.4.2. פרסום התעודה לאימות

משיקולי הגנה על הפרטיות, כל התעודות לאימות שינופקו יישמרו במאגר מידע פנימי של הממיל"א. הגישה למאגר זה תוגבל לעובדים מורשים בלבד של הממיל"א. גישה על ידי גורמים חיצוניים תתאפשר רק לפי דרישה על פי חוק או הליך משפטי.
בנוסף על כך, יהיה מאגר חיצוני של סטטוס התעודות לאימות שיהיה מאגר אנונימי, כלומר - ללא ציון מספרי זהות ושמות בעל התעודה אלא רק מספרי התעודות לאימות וסטטוס התעודה לאימות.

4.4.3. הודעה על הנפקת התעודה לאימות לישויות אחרות

לא תימסר הודעה לישויות אחרות במהלך השוטף, אלא לפי דרישה על פי חוק או בגין הליך משפטי ולפי החלטה מפורשת.

4.5. צמד המפתחות והשימוש בתעודה לאימות

4.5.1. המפתח הפרטי של המנוי והשימוש בתעודה לאימות

באחריות התושב להשתמש בתעודה לאימות אך ורק למטרות שהוגדרו במפורש במסמך זה (ר' בפרט סעיף 1.4 לעיל). השימוש יהיה בהתאמה לרשום בשדה "שימוש במפתח" (key-usage) וכן בשדה "שימוש מתקדם במפתח" (enhanced key-usage). ככלל, כל שימוש בתעודה לאימות שעל תעודת הזהות מותרת, אלא אם נאמר מפורשות אחרת.

4.5.2. השימוש בתעודה לאימות ובמפתח הציבורי על ידי גורמים מסתמכים

גורמים מסתמכים יוכלו להתבסס על התעודה לאימות לצורך השימושים כאמור בסעיף 4.5.1 לעיל ובהתאמה לרשום בשדה "שימוש במפתח" (key-usage) ושימושים מתקדמים במפתח (enhanced key-usage).
שימוש ביישומים נוספים, שאינם בגדר "אימות" ואינם מוגדרים בסעיף 4.5.1 לעיל, מעבר לכך יהיה על אחריותו של התושב והצדדים המסתמכים במקרים אלו.
על גורם מסתמך לבדוק לפני ההסתמכות את סטטוס התעודה לאימות באמצעות הכלים שיעמיד לרשותו הממיל"א, שהם – רשימת התעודות הבטלות (CRL) באתר האינטרנט או שאילתה מקוונת לתקפות תעודה (OCSP) לגורמים שסוכם שיעבדו בדרך זאת. במידה ותתבצע הסתמכות ללא בדיקה כאמור, תחול האחריות לתוצאת ההסתמכות על הגורם המסתמך בלבד. לצורך הבהרה, ככלל בדיקה האם תעודה דיגיטלית תקפה נעשית בצורה אוטומטית ביישום המתאים. במידה ויש ספק, יש לבדוק זאת עם הגורם האחראי על היישום. במידה ומשתמש מבקש לבדוק זאת בצורה עצמאית, ניתן לעשות זאת באמצעות גישה ישירה לאתר הממיל"א, ובדיקה מול קובץ התעודות הבטלות המצוי באתר.

4.6. חידוש תעודה לאימות

תוקף התעודה לאימות הינו עד 10 שנים והוא זהה לתוקף כרטיס תעודת הזהות, ותוקפן יפקע בהכרח באותו מועד.

לא יתקיים תהליך של חידוש תעודה לאימות. בסוף התקופה התושב יידרש לעבור תהליך בקשה חדשה, הנפקת כרטיס תעודת זהות חדש ותעודה לאימות חדשה.

4.7. חידוש מפתח לתעודה לאימות

תוקף התעודה לאימות הינו עד 10 שנים והוא זהה לתוקף כרטיס תעודת הזהות. לא יתקיים תהליך של חידוש מפתח תעודה לאימות. בסוף התקופה או לאחר אובדן התושב יידרש לעבור תהליך חדש של בקשה והנפקת כרטיס תעודת זהות חדש ותעודה לאימות חדשה. בהתאם, יונפק גם כרטיס תעודת זהות חדש.

4.8. עדכונים לתעודה לאימות

במקרה של צורך בעדכונים לתעודה לאימות, תונפק תעודה לאימות חדשה. לא יבוצעו עדכונים על גבי תעודה קיימת.

4.9. ביטול תעודה לאימות

4.9.1. תנאים לביטול תעודה לאימות

בדומה לקבוע בסעיף 20 לחוק חתימה אלקטרונית, ישנם כמה מצבים בהם יש לבטל תעודה לאימות. העיקרון שמאחורי הביטול הוא למנוע שימוש לרעה בתעודה על ידי מי שאינו מורשה לכך, תוך מניעת ביטול על ידי מי שאיננו מורשה. כמו כן יש צורך בביטול במצבים הנוגעים לסטטוס של בעל התעודה, כמו מוות או ביטול רישיון ישיבה בישראל.
מצבים אלה יכולים להיות בשל אחד משבעה סוגי מצבים, אשר נקבעו בתקנות מרשם האוכלוסין (תקופת תוקפן ופקיעת תוקפן של תעודות זהות), התשע"ב - 2011, שהינן התקנות המהותיות המסדירות את פקיעת תוקפן של תעודות זהות, ומשכך מביאות לביטול התעודה האלקטרונית לאימות:

"(א) עקב בקשת בעל התעודה משנודע לו על קיום בעיה הקשורה בתקפות התעודה;
(ב) על פי החלטת עובד מוסמך על סמך מידע הקשור לתעודה המסוימת, אך אין מקורו בבעל התעודה;
(ג) עם קבלת כרטיס תעודת זהות שנמצאה שלא ברשות בעליה באחת מלשכות רשות האוכלוסין;
(ד) בשל פגם הקשור בחתימתו האלקטרונית של ראש רשות האוכלוסין או במערכות המשמשות להנפקת אמצעי החתימה;
(ה) עקב ביטול רישיון ישיבה בישראל או אזרחות ישראלית;
(ו) עקב החלפת תעודת הזהות בתעודת זהות חדשה (למעט הספח);
(ז) עקב מות בעל התעודה.
עם ביטול התעודה, בהתאם לעילות המפורטות לעיל, יירשם דבר הביטול במאגר התעודות הבטלות."

4.9.2. מי יכול להגיש בקשה לביטול תעודה לאימות

בקשה לביטול תעודה לאימות תהיה בהתאם למצבים המתוארים בסעיף הקודם, כדלקמן:

(א) בעל התעודה.
(ב) – (ז): עובד מוסמך.

4.9.3. בקשה לביטול תעודה לאימות

התושב יוכל לפנות ישירות לרשות או למוקד ביטול התעודות שיופעל ע"י הממיל"א.
התושב יידרש למסור את פרטי הזיהוי שלו ובפרט את התשובות לשאלות האישיות הייחודיות שאותן מסר כפרטי זיהוי במקרה של צורך בביטול כרטיס תעודת הזהות והתעודה לאימות (ראה סעיף 3.2.3). "העובד המוסמך" כהגדרתו בחוק (נותן שירות ברשות או עובד המוקד בממיל"א), יבחן את הבקשה לביטול ויפעל על פיה.
אם החליט העובד המוסמך לבטל את התעודה לאימות, הוא ידווח על כך במסך הדיווח שיהיה במערכת הממוחשבת של הרשות. לאחר מכן תועבר הבקשה לביטול למערכת הממוחשבת של הממיל"א, ובה יתבצע תהליך ביטול התעודה, רישום הביטול והכללת התעודה ברשימת התעודות הבטלות.

4.9.4. ארכה לביטול תעודה לאימות

במידה והעובד המוסמך לא השתכנע כי הפונה הוא אכן בעל כרטיס תעודת הזהות וכי ייתכן ומדובר בניסיון זיוף או התחזות או מניעת שירות, עליו להעביר את המידע לעובד מוסמך בכיר יותר ("קו שני") על מנת שיקבל החלטה בעניין.
על מנת למנוע מצבי ביניים לא מוגדרים, לא יוגדר מצב של "תעודה מושעית" (suspended) ובכל פנייה כאמור לעיל תתקבל החלטה לכאן או לכאן.

4.9.5. משך הזמן שבו מחויב הממיל״א לעבד את בקשת הביטול

הממיל״א יעבד את בקשת הביטול בתוך עד 12 שעות ממועד קבלתה במוקד ביטול התעודות.

4.9.6. דרישת בדיקת תקפות תעודות לאימות על ידי גורמים מסתמכים

הממיל״א מעמיד לרשות בעלי התעודות וגורמים המסתמכים מאגר תעודות בטלות הכולל את אמצעי אימות החתימה של הממיל״א ורשימת התעודות הבטלות (CRL) שניתן להגיע אליה מכתובת אתר האינטרנט http://e.gov.il/http://e.gov.il/GovCertification/GovCertification/Pages/GCCRL.aspx
גורמים מסתמכים נדרשים לבדוק את רשימת התעודות הבטלות טרם הסתמכות על פעולת אימות על פי כרטיס תעודת הזהות והתעודה לאימות. ללא בדיקה כזו, אין להסתמך על התעודה.

4.9.7. תדירות יצירת רשימת תעודות לאימות בטלות

הממיל״א ייצור ויפרסם ככלל רשימת תעודות בטלות מלאה, אחת ל- 12 שעות לכל הפחות.

4.9.8. תקופת חוסר-עדכון מרבית לרשימת תעודות לאימות בטלות

הממיל״א יעדכן את הרשימה ככלל בתוך עד 12 שעות. תוקף הרשימה יהיה ל- 72 שעות כמפורט לצד הרשימה, באופן שיכסה מקרים של תקלות או ימים מיוחדים בהם המידע לא יתעדכן.

4.9.9. זמינות בדיקת סטטוס ביטול תעודות לאימות במקוון

הממיל״א יפעיל שירות מקוון (OCSP) לבדיקת תקפות התעודות לאימות שהונפקו על ידו ובוטלו.

4.9.10. דרישות בדיקת תעודות לאימות במקוון

השירות שיינתן ע״י הממיל״א לצורך כך יעמוד בדרישות הבאות:

- תמיכה בפרוטוקול OCSP.
- מיקום השירות וההפניה אליו יפורסם בתעודה לאימות.
- עדכון המידע יתבצע בתוך עד 12 שעות מרגע שהתעודה לאימות בוטלה.
- תישמר זמינות גבוהה לגורמים מסתמכים שיהיו מנויים על שירות זה.
- הממיל״א יהיה רשאי לגבות תשלום עבור השימוש בשירות זה, בכפוף לאישורים המתאימים.

4.9.11. צורות אחרות זמינות של פרסום ביטול תעודות לאימות

לא תהיינה צורות אחרות זמינות.

4.9.12. דרישות מיוחדות במקרה של פגיעה במפתח

בכל מקרה של פגיעה במפתח הפרטי של תעודה לאימות, על התושב לפעול באופן מידי על מנת לבטל את התעודה, למעט אם יש חשש למניעת זכות חוקית אחרת (כגון – הצבעה בבחירות). הכוונה במונח ״פגיעה״ הוא למצב בו כרטיס תעודת הזהות נגנב, אבד, או שיש חשש כלשהו של התושב שהמפתח הפרטי שלו נחשף או יצא משליטתו.

4.9.13. תנאים להשעיית תעודה לאימות

לא יתקיים מצב של השעיית תעודה (Suspension) במהלך תוקפה של התעודה לאימות.

4.10. מתן שירותי מידע על סטטוס תעודות לאימות

שירותי המידע יינתנו באמצעות פרסום רשימת התעודות האלקטרוניות הבטלות (CRL) באינטרנט בכתובת http://e.gov.il/http://e.gov.il/GovCertification/GovCertification/Pages/GCCRL.aspx לקהל הרחב. בנוסף יינתן שירות מידע מקוון ללקוחות מוסדיים ומורשים (OCSP).

4.11. סיום תוקף

סיום תוקף התעודה לאימות יהיה בהתאם לתוקף שנרשם בתעודה לאימות בעת יצירתה, ויהיה זהה לתוקף כרטיס תעודת הזהות. תאריך תוקף זה מתקבל תמיד בעת העברת הבקשה מהרשות לממיל"א ואינו נקבע באופן אוטומטי.
סיום התוקף יכול להגיע באופן טבעי עם סיום התקופה האמורה, או סיום מוקדם לפני מועד סיום תוקפה עקב פגיעה בתעודה לאימות שאז היא תהפוך לתעודה בטלה.

4.12. שמירת מפתח אצל צד שלישי ושחזור מפתח

בשום מקרה לא ישמר המפתח הפרטי הקשור למפתח הציבורי של תעודה לאימות מחוץ לכרטיס תעודת הזהות, לא במשמורת אצל צד שלישי כלשהו ובפרט לא ברשות או בממיל"א. בהתאם, לא יתאפשר לשחזר מפתח פרטי של תושב.

5. תשתיות, ניהול ובקרה תפעולית

5.1. ראה במסמך הנהלים של הממיל"א (CPS).

6. בקרות אבטחת מידע טכניות

6.1. חילול והתקנת צמד מפתחות

6.1.1. חילול צמד המפתחות

חילול צמד המפתחות יתבצע על גבי כרטיס תעודת הזהות. חילול המפתחות ייעשה במפעל מילוי הפרטים ושחרור הכרטיס החכם וצמד המפתחות לאימות ייעשה באמצעות סיסמאות אישיות שיונפקו ויימסרו בצורה מאובטחת לתושב, כחלק מתהליך המסירה, כאשר התושב יימצא פיזית מול נותן השירות (עובד הרשות).
כרטיס תעודת הזהות מבוסס על טכנולוגיה של כרטיס חכם ועומד בדרישות התקנות המתאימות. הכרטיס החכם לרבות מערכת ההפעלה הוא בעל הסמכה לפי תקן אבטחה Common Criteria (ISO/IEC 15408) לרמת סמך EAL4+ לפחות.
הממיל״א יחתום על התעודות לאימות שהוא ינפיק, באמצעות רכיב אבטחת מידע בחומרה (HSM) שעומד בדרישות FIPS-140-2 level 3.

6.1.2. העברת המפתח פרטי לתושב

המפתח הפרטי יחולל על כרטיס תעודת הזהות ולא ייצא ממנה לעולם. בפרט, לא יתבצע תהליך של חילול מפתחות חיצוני וייבוא מפתחות. שני התנאים הנ״ל מבוססים על טכנולוגיית כרטיס תעודת הזהות ולא על נהלי עבודה.

6.1.3. העברת המפתח ציבורי למנפיק התעודה

המפתח הציבורי יישלח בפרוטוקול בפורמט תקני מהרשות לממיל״א לצורך יצירת התעודה לאימות וחתימה עליה ע״י הממיל״א.
הפרוטוקול נקרא CMP והוא מבוסס על פרסומי ה- IETF RFC 4210 ו-RFC 4211.

6.1.4. העברת המפתח הציבורי של הממיל״א לצדדים מסתמכים

המפתחות הציבוריים של עוגן האמון של הממיל״א ושל השרתים התפעוליים של הממיל״א יופצו כחלק מתעודות אלקטרוניות בחבילת התוכנה תל״ם-אישי. העברתם מהממיל״א תתבצע בצורה מאובטחת.
המפתח הציבורי של הממיל״א יהיה זמין באתר הממיל״א וניתן יהיה להעתיקו משם. ההעברה מהממיל״א לאתר תתבצע בצורה מאובטחת.
בעתיד, הכוונה שהמפתחות הציבוריים של הממיל״א יופצו כחלק מרשימות גורמים מאשרים מוסמכים המתפרסמות על ידי יצרני דפדפנים.

6.1.5. אורכי מפתחות

המפתחות שיחוללו על תעודת הזהות יהיו מפתחות RSA באורך 2048 סיביות.
חתימת הממיל״א על התעודות האלקטרונית תתבצע באמצעות מפתח RSA באורך 4096 סיביות.
פונקציות המיצוי (HASH) שיבוצע בהן שימוש תהיה:

- SHA-256

6.1.6. פרמטרים ליצירת מפתח ציבורי ובקרת איכות

הפרמטרים והבקרות לחילול המפתח הציבורי יהיו על פי תקן FIPS 186.

6.1.7. מטרות שימוש במפתח (שדה "שימוש במפתח" כמוגדר ב-X.509 גרסה 3)

שימוש המפתח (keyUsage) שיימצא בתעודה לאימות יהיה digital signature בלבד. באשר ל- enhanced key-usage, הערכים יהיו של client authentication ושל smartcard logon. ראה גם סעיף 4.5.1 לעיל. יובהר כי השימוש בכל מקרה הינו לאימות בלבד.

6.2. הגנה על המפתח הפרטי ובקרות הנדסיות על המודול הקריפטוגרפי

6.2.1. תקנים ובקרות על המודול הקריפטוגרפי

המודול הקריפטוגרפי שבכרטיס תעודת הזהות השומר בין היתר על המפתח הפרטי עומד בתקן אבטחה Common Criteria (ISO/IEC15408) בפרופיל הגנה SSCD (Secure Signature Creation Device) ברמה של EAL 4+. הערה: סעיף זה מתייחס לכרטיס תעודת הזהות עצמו ולא למערך ההצפנה בממילי"א.

6.2.2. שליטה של מספר אנשים על המפתח הפרטי (n מתוך m)

לצורך שחזור המפתח הפרטי של הממילי"א במקרים חריגים, ימומש מנגנון n מתוך m, או מנגנון שווה ערך, שיפורט בנהלי העבודה של הממילי"א. אין שימוש במנגנון זה באופן שוטף ובמקום זאת נעשה שימוש במנגנוני אבטחה אחרים. הבהרה: אין מדובר במפתח הפרטי של התעודה לאימות של משתמש הקצה, אלא של הממילי"א.

6.2.3. הפקדת המפתח הפרטי (key escrow)

בשום מקרה לא תופקד שליטה על המפתח הפרטי של הממילי"א בידי גורם צד שלישי.

6.2.4. גיבוי של המפתח הפרטי

למפתח הפרטי של הממילי"א יהיו שני עותקי גיבויים לכל היותר, שיאפשרו המשכיות עסקית.

6.2.5. ארכוב מפתח פרטי

המפתח הפרטי של הממילי"א ישמר בכספת בהתאם לנהלי העבודה של הממילי"א.

6.2.6. העברת המפתח הפרטי לתוך ומתוך המודול הקריפטוגרפי

המפתח הפרטי של הממילי"א יחולל באופן עצמאי על ידי המודול הקריפטוגרפי ב- HSM של ה- RCA ושל ה- OCA.

6.2.7. אחסון המפתח הפרטי על המודול הקריפטוגרפי

המפתח הפרטי של עוגן האמון של הממילי"א יאוחסן על ה- HSM הרלבנטי, בצורה מאובטחת.

6.3. היבטים נוספים של ניהול צמד המפתחות

6.3.1. ארכוב המפתח הציבורי

המפתח הציבורי של הממיל״א יישמר בארכיב הממיל״א.

6.3.2. תקופות תפעוליות של התעודה לאימות ותקופת שימוש בצמד המפתחות

התעודה האלקטרונית של שורש האמון של הממיל״א תהיה תקפה למשך 25 שנים (או 25 שנים ו- 6 חודשים לצורך מהלך חפיפה).
התעודה האלקטרונית של השרת התפעולי תהיה תקפה למשך 15 שנה (או למשך 15 שנים ו- 13 חודשים לצורך מהלך חפיפה).
אחת לכל 4 שנים, יוחלט באשר לתהליך של חידוש תעודה כאמור לעיל – להמשיך עם התעודה הקיימת לשנה אחת נוספת ; לנפק תעודה חדשה עם אותו מפתח אך לפרק זמן מוארך או לחולל צמד מפתחות חדשים ולהנפיק תעודה חדשה ל- RCA או ל- OCA.
התעודה לאימות של התושב תהיה תקפה למשך תקופת תוקפו של כרטיס תעודת הזהות.

6.4. מידע לאתחול

כל הסיסמאות הנדרשות להפעלת כרטיס תעודת הזהות, לרבות אתחול ופתיחת כרטיס תעודת הזהות והפעלתו לצורך יצירת התעודה לאימות והתפעול השוטף, מחוללות באמצעות מחולל רחש אמיתי (TRNG) ונשמרות על כרטיס תעודת הזהות עצמו ולא באופן חיצוני. כל המידע הנוסף שנדרש לתפעול מערכות המידע של הממיל״א, כגון - מפתחות הצפנה וסיסמאות, יעמדו בדרישות תקן ISO 27001.

6.5. בקרות אבטחת מערכת המחשב: ראה במסמך הנהלים של הממיל״א (CPS).

6.6. בקרות אבטחת מחזור החיים: ראה במסמך הנהלים של הממיל״א (CPS).

6.7. בקרות אבטחת רשת התקשורת: ראה במסמך הנהלים של הממיל״א (CPS).

7. פרופיל תעודות אלקטרוניות ורשימת תעודות בטלות (CRL)

7.1. פרופיל תעודה לאימות

הפרופיל עבור תעודה לאימות לתושב מצ"ב למסמך זה בקובץ נפרד, שיוגדר לצורך כך **כנספח 7.1**. הערה: מסמך מבנה התעודה הופרד לקובץ נפרד משיקולי עריכה טכניים, מהותית הוא חלק ממסמך ה- CP ועם אותו OID.

7.1.1. מספר גרסה

התעודה תונפק על פי גרסה 3 של תקן X.509 (ערך "2" בשדה version בתעודה).

7.1.2. הרחבות תעודה אלקטרונית

ראה **בנספח 7.1**.

7.1.3. מזהה עצם של אלגוריתמים קריפטוגרפים (OID)

המזהים של העצמים הייחודיים של הממיל"א נקבעו בהתאם לענף שהוקצה לממשלת ישראל ובתוכו לממיל"א. ניהול המזהים נעשה על ידי מערך ממשל זמין עבור כלל הממשלה.

7.1.4. תבנית השם

ראה **בנספח 7.1**.

7.1.5. אילוצים על שמות

ראה **בנספח 7.1**.

7.1.6. מזהה עצם מדיניות תעודה (Certificate Policy)

תעודה שעומדת בדרישות מסמך זה תכיל את מספר מזהה העצם של ה- CPS. ראה פירוט **בנספח 7.1**.

7.1.7. שימוש בהרחבת אילוצי מדיניות (Policy constraints)

ראה **בנספח 7.1**.

7.2. פרופיל רשימת תעודות בטלות

פרופיל רשימת תעודות בטלות הינו בהתאם לתקן ישראלי ת"י 9548-8.

8. ביקורת, תאימות והערכות אחרות: ר' מסמך הנהלים של הממיל"א (CPS).

9. עניינים עסקיים ומשפטיים אחרים: ר' מסמך הנהלים של הממיל"א (CPS).

נספח 1.6 - הגדרות וקיצורים

טבלה מס' 1 – קיצורים (למידע בלבד)

הבהרה: מדובר ככלל בקיצורים טכניים שאינם נגזרים מחוק חתימה אלקטרונית, גם אם יש בהם שימוש במונחים מהחוק.

קיצור באנגלית	קיצור בעברית	משמעות באנגלית	משמעות בעברית
CA	ג"מ	Certification Authority	גורם מאשר
CARL		Certificate Authority Revocation List	רשימת תעודות בטלות של גורם מאשר
CP		Certificate Policy	מדיניות תעודה
CPS		Certification Practice Statement	הצהרה על נהלי עבודה להנפקת תעודות ("מסמך נהלים"
CRL		Certificate Revocation List	רשימת תעודות בטלות
DN		Distinguished Name	שם ייחודי
FIPS PUB		Federal Information Processing Standard Publication	פרסום תקן של ארגון העו"א הפדרלי של ארה"ב
GCA	גמ"מ	Government Certification Authority	גורם מאשר ממשלתי
IETF		Internet Engineering Task Force	כוח משימה הנדסי בנושא אינטרנט
ISO		International Organization for Standardization	ארגון התקינה הבינלאומי
ITU		International Telecommunications Union	איגוד התקשורת הבינלאומי
NIST		National Institute of Standards and Technology	המכון הלאומי לתקנים וטכנולוגיה, ארה"ב
OID		Object Identifier	מזהה עצם
PIN		Personal Identification Number	מספר זיהוי אישי, סיסמה
PKCS		Public Key Certificate Standard	תקן תעודת מפתח ציבורי
PKI	תמ"ר	Public Key Infrastructure	תשתית מפתח ציבורי
PKIX		Public Key Infrastructure X.509	תשתית מפתח ציבורי ע"פ תקן X.509
RA		Registration Authority	רשות רישום

טבלה מס׳ 2 (למידע בלבד) – הרחבת הגדרות טכניות

הבהרה: מדובר ככלל במונחים טכניים שאינם נגזרים מחוק חתימה אלקטרונית, גם אם יש בהם שימוש במונחים מהחוק.

תיאור המונח	אנגלית	עברית
היכולת להשתמש במשאב כלשהו של מערכת מידע	Access	גישה
תהליך של הענקת גישה למשאבי מערכת מידע רק למשתמשים מורשים, תכניות, תהליכים או מערכות אחרות.	Access Control	בקרת גישה
גורם שהגיש בקשה לתעודה, בסטטוס שלפני השלמת תהליך הנפקת התעודה.	Applicant	מבקש
אחסון פיזי נפרד, לטווח ארוך.	Archive	ארכיון
בדיקה עצמאית ובחינה של רשומות ופעילויות, לצורך הערכת התאמת הבקרות במערכת, על מנת להבטיח תאימות עם מדיניות מוגדרת ופרוצדורות תפעוליות, ועל מנת להמליץ על שינויים נדרשים בבקרות, במדיניות או בתהליכים.	Audit	ביקורת
רישום כרונולוגי של פעילויות מערכת על מנת לאפשר שיחזור ובחינה של רצף אירועים ושינויים באירוע.	Audit Data	מידע לביקורת
לאשר ולוודא זהות של ישות, כאשר זהות זו מוצגת לבדיקה.	Authenticate	לוודא/ לאמת
אמצעי בטחון המתוכנן לבסס את התקפות של שידור, מסר, או מקור מידע, או אמצעים לאמת את ההרשאה והסמכות של אדם לקבל קטגוריות ספציפיות של מידע.	Authentication	וידוא/ אימות
ייצוג דיגיטלי של מידע העונה על כל התנאים המצטברים הבאים לפחות: (1) מזהה את הגורם שהנפיק אותו; (2) קורא בשם או מזהה את המנוי; (3) כולל את המפתח הפומבי של המנוי; (4) מזהה את תקופת התפעול התקיפה; (5) נחתם אלקטרונית על ידי הג״מ שהנפיק אותו.	Certificate	תעודה
רשות אשר משתמש אחד או יותר בוטחים בה, לצורך הנפקה וניהול של תעודות מפתח פומבי ורשימת תעודות בטלות.	Certification Authority (CA)	גורם מאשר
רשימה חתומה, כולל חתימת זמן, של מספרים סדרתיים של מפתחות ציבוריים של תעודות ג״מ, כולל תעודות-צולבות, אשר בוטלו.	Certification Authority Revocation List (CARL)	רשימת תעודות בטלות של ג״מ
אוסף של ציוד, כוח אדם, תהליכים ומבנים, בהם עושה ג״מ שימוש, על מנת לבצע הנפקה של תעודות וביטולן בעת הצורך.	CA Facility	מתקן ג״מ
תוכנות לניהול מפתחות ושימוש באמצעי הצפנה, שבהן נעשה שימוש להנפקת תעודות למנויים.	Certification Authority Software	תוכנת גורם מאשר
הצהרה על הנהלים אשר גורם מאשר מיישם בהנפקה, השעיה, ביטול וחידוש של תעודות ומתן הגישה אליהן, בהתאמה לדרישות מסוימות. מסמך פומבי מחייב, הנקבע על פי מדיניות גמ״מ ואופן פעולתו.	Certification Practice Statement (CPS)	הצהרת נוהל עבודה להנפקת תעודות
מידע, כגון כתובת הדואר של המנוי, שאינה כלולה בתעודה עצמה. עשוי לשמש לצורכי ניהול על ידי הגורם המאשר.	Certificate - Related Information	מידע קשור לתעודה
רשימה המנוהלת על ידי גורם מאשר, של כל התעודות שהוא הנפיק	Certificate	רשימת תעודות

בטלות	Revocation List (CRL)	ואשר בוטלו לפני מועד פג התוקף המקורי שהוגדר עבורן.
לקוח (יישום)	Client (application)	ישות מערכתית, בדר"כ תהליך ממוחשב הפועל מטעם משתמש אנושי, שעושה שימוש בשירות המסופק על ידי השרת.
סיכון ופגיעה	Compromise	גילוי של מידע לאנשים בלתי מוסמכים, או פגיעה במדיניות אבטחת המידע של מערכת, שכתוצאה מכך נגרמה פגיעה מכוונת או בלתי מכוונת, שינוי, מחיקה או אובדן במידע.
סודיות	Confidentiality	בטחון שמידע לא נמסר לישויות או לתהליכים בלתי מאושרים.
תעודה צולבת	Cross-Certificate	תעודה שנעשה בה שימוש ליצירת קשרי אימון בין שני גורמים מאשרים.
שלמות מידע	Data Integrity	בטחון שמידע לא השתנה מאז יצירתו ועד לקבלתו.
חתימה דיגיטלית	Digital Signature	התוצאה של טרנספורמציה של מסר על ידי שימוש במערכת קריפטוגרפית המשתמשת במפתחות כך שגורם המסתמך על החתימה יכול לקבוע: (1) האם הטרנספורמציה נוצרה תוך שימוש במפתח הפרטי שמתאים למפתח הפומבי שנמצא בתעודה הדיגיטלית של החותם; ו- (2) האם המסר שונה על ידי מישהו, מאז שבוצעה הטרנספורמציה. להלן מספר הגדרות מקבילות הלקוחות מחוק חתימה אלקטרונית, התשס"א – 2001: "חתימה אלקטרונית" – חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או נקשר למסר אלקטרוני. "חתימה אלקטרונית מאובטחת" – חתימה אלקטרונית שמתקיימים בה כל אלה: (1) היא ייחודית לבעל אמצעי חתימה; (2) היא מאפשרת זיהוי לכאורה של בעל אמצעי החתימה; (3) היא הופקה באמצעי חתימה הניתן לשליטתו הבלעדית של בעל אמצעי החתימה; (4) היא מאפשרת לזהות שינוי שבוצע במסר האלקטרוני לאחר מועד החתימה; "חתימה אלקטרונית מאושרת" – חתימה אלקטרונית מאובטחת אשר גורם מאשר הנפיק תעודה אלקטרונית בדבר אמצעי אימות החתימה המזהה אותה;"
משך	Duration	שדה בתוך תעודה שמורכב משני שדות משנה: "תאריך הנפקה" ו"תאריך פג תוקף".
שלמות	Integrity	הגנה כנגד שינוי או השמדה לא מורשית של מידע. מצב שבו מידע נשאר ללא שינוי מהנקודה שבה נוצר על ידי המקור, במשך השידור, האחסון והקבלה על ידי היעד.
גורם מאשר ביניים	Intermediate CA	גורם מאשר שהינו כפוף לג"מ אחר, ושיש לו ג"מ שכפוף אליו.
הפקדת מפתחות	Key Escrow	הפקדה של מפתח פרטי של מנוי ומידע רלבנטי אחר, בהתבסס על הסכם הפקדה או חוזה אחר, הקובע עבור המנוי, את התנאים שבהם נדרש סוכן אחד או יותר, להחזיק את המפתח הפרטי של המנוי לתועלת המנוי, עובד/ מועסק או צד אחר, בהתאם לתנאים המוגדרים בהסכם.
החלפת מפתחות	Key Exchange	תהליך של החלפת מפתחות ציבוריים במטרה לבסס תקשורת בטוחה.
חומרי חילול מפתחות	Key Generation Material	מספרים אקראיים, כעין-מספרים אקראיים ופרמטרים קריפטוגרפים שבשימוש בתהליך יצירת מפתחות קריפטוגרפים.

צמד מפתחות	Key Pair	שני מפתחות מתמטיים הקשורים זה לזה, בעלי התכונות - (1) ניתן להשתמש במפתח אחד להצפין מסר כך שניתן לפענחו רק באמצעות המפתח השני, ו- (2) גם אם מפתח אחד ידוע, לא ניתן ואין זה מעשי לגלות בצורה חישובית את המפתח השני.
אימות הדדי	Mutual Authentication	תהליך המתרחש כאשר שני הצדדים בשני קצות התקשורת, מבצעים וידוא פעיל האחד לשני.
אי-הכחשה	Non-Repudiation	בטחון שלשולח מספקים הוכחה לאישור המשלוח ולמקבל מסופקת הוכחה על זהות השולח כך שאף אחד מהם לא יכול להכחיש שהוא עיבד את המידע.
מפתח פרטי	Private Key	המפתח בצמד המפתחות שבו משתמשים ליצירת החתימה הדיגיטלית. מפתח זה חייב להישמר סודי.
מפתח ציבורי	Public Key	המפתח מתוך צמד מפתחות לחתימה דיגיטלית, שנועד לאמת חתימה דיגיטלית. המפתח זמין לציבור בצורה של תעודה דיגיטלית.
תשתית מפתח ציבורי	Public Key Infrastructure (PKI)	אוסף של מדיניות, תהליכים, פלטפורמות שרתים, תוכנה ועמדות עבודה, שבהם נעשה שימוש לניהול תעודות וצמדי מפתחות פרטי-ציבורי, כולל היכולת להנפיק, לתחזק, לנהל ולבטל תעודות מפתח ציבורי.
רשות רישום/ גורם רושם	Registration Authority (RA)	גורם שאחראי על זיהוי ווידוא של נושאי תעודות, אולם אינו חותם ומנפיק תעודות בעצמו.
מפתוח מחדש של תעודה דיגיטלית	Re-Key (a certificate)	שינוי של ערך מפתח הצפנה שנעשה בו שימוש במערכת קריפטוגרפית. בדרך כלל, משמעות הדבר היא הנפקת תעודה חדשה על המפתח הציבורי החדש.
צד מסתמך	Relying Party	אדם או גוף שמקבלים מידע שכולל תעודה וחתימה דיגיטלית שניתנת לאימות בהתייחס למפתח פומבי המפורט בתעודה, ונמצא במצב שהוא מסתמך עליהם. לעניין תוצאות הסתמכות כאמור, ראה פירוט במסמך זה.
חידוש תעודה	Renew (a certificate)	הפעולה או התהליך של הארכת תוקף המידע הקשור לתעודת מפתח ציבורי, על ידי הנפקת תעודה חדשה.
מאגר	Repository (directory)	בסיס נתונים הכולל מידע המתייחס לתעודות. ניתן להגדרה גם כ"ספריה".
ביטול תעודה	Revoke a Certificate	לסיים באופן קבוע את תקופת ההפעלה של תעודה, בזמן ספציפי.
גורם מאשר "שורש"/ עוגן אמון	Root CA	בארכיטקטורה היררכית של תמ"ר, זהו הגורם המאשר שהמפתח הפומבי שלו משמש כמידע הנאמן ביותר שניתן לסמוך עליו (כלומר – תחילת מסלול האמון), עבור תחום אבטחת מידע.
תעודת חתימה	Signature Certificate	תעודת מפתח ציבורי שכוללת מפתח ציבורי שמיועד לאימות חתימות דיגיטליות, ולא להצפנת מידע או לביצוע פונקציות הצפנה אחרות.
גורם מאשר כפוף	Subordinate CA	במסגרת תמ"ר היררכי, זהו גורם מאשר אשר מפתח החתימה של תעודותיו, מאושר על ידי גורם מאשר אחר, ואשר פעולותיו מוגבלות על ידי גורם מאשר אחר זה.
מנוי	Subscriber	ישות אשר (1) היא שם נושא התעודה או שמזוהה בתעודה המונפקת לאותה ישות, (2) מחזיק במפתח פרטי שמקביל למפתח הציבורי הרשום בתעודה, ו- (3) לא מנפיק בעצמו תעודות לכל גורם אחר.
גורם מאשר בכיר	Superior CA	ב- תמ"ר היררכי, זהו גורם מאשר שאישר את תעודת החתימה של גורם מאשר אחר, ואשר מגביל את פעילות הגורם המאשר האחר.
עדכון תעודה	Update (a certificate)	פעולה או תהליך לפיהם פריטי מידע הקשורים לתעודת מפתח פומבי קיימת ובפרט הרשאות הניתנות לנושא התעודה, משתנים על ידי הנפקת תעודה חדשה.