

פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית לחתימה אלקטרונית מאושרת

תקפה כ"חתימה אלקטרונית מאושרת" לצורך סעיף 2
לחוק החתימה האלקטרונית, התשס"א-2001

גרסה 1.0

בתוקף: מ – 15.8.2011

פרסונל איי.די. בע"מ
רח' בן-גוריון 34
רמת-גן
ישראל 52573

073-2900047	טלפון:
073-2900379	פקס:
office@personalid.co.il	דוא"ל:
www.personalid.co.il	אתר:

הודעת זכויות יוצרים

כל הזכויות במסמך נהלים זה שייכות לפרסונל איי.די. בע"מ ("פרסונל איי.די."). אין להעתיק, להפיץ, לשכפל, לצלם, להקליט, לתרגם, להציג, לאחסן במאגר מידע, לשדר או לשנות מסמך זה, בכל אמצעי שהוא – לרבות בכל אמצעי אלקטרוני, אופטי, מכאני או אחר – ללא אישור מפורש בכתב ומראש מפרסונל איי.די..

הענקת מסמך הנהלים בפורמט PDF או HTML למחשב והדפסתו למטרת עיון בו מותרת בזאת מראש למעיין.

הערות והצעות

אנו מקבלים בברכה הערות והצעות לשינויים שיושמו בגרסה חדשה של מסמך נהלים זה, אם תופץ. אנא שלחו אותן ל: office@personalid.co.il, או בדואר רגיל ל:

מנהל הגורם המאשר
פרסונל איי.די. בע"מ
בן-גוריון 34
רמת-גן
ישראל 52573

תודות

פרסונל איי.די. מודה לקבוצת האינטרנט, ה-IT וזכויות היוצרים במשרד פרל כהן צדק לצר על עזרתם הרבה בגיבוש מסמך נהלים זה.

8	מבוא	1
8	סקירה והגדרות	1.1
8	סקירת מסמך הנהלים	1.1.1
9	הגדרות	1.1.2
10	זיהוי	1.2
11	מסמך נהלי הנפקת התעודה	1.2.1
11	מזהה עצם (OID)	1.2.2
11	ישויות משתתפות	1.3
11	מערך הנפקה	1.3.1
11	מערך רישום	1.3.2
11	בעלי תעודות	1.3.3
11	ישויות נוספות	1.3.4
11	שימושי תעודה מאושרת	1.4
12	שימושים הולמים בתעודה	1.4.1
12	שימושים אסורים בתעודה	1.4.2
12	ניהול מסמך המדיניות	1.5
12	אחראי על מסמך המדיניות	1.5.1
13	פרטי התקשרות	1.5.2
13	אישור מסמך המדיניות	1.5.3
14	חובות פרסום ואחסון	2
14	ארכיון	2.1
14	פרסום מסמכי פרסונל איי.די.	2.2
14	זמן ותדירות פרסום	2.3
15	בקרת גישה	2.4
16	זיהוי והזדהות	3
16	מתן שמות	3.1
16	סוגי שמות ייחודיים	3.1.1
16	דרישת היות שם בעל התעודה אמיתי	3.1.2
16	מנויים אנונימיים	3.1.3
16	כללי פירוש של צורות שם שונות	3.1.4
16	ייחודיות השם	3.1.5
16	הכרה ואימות החזקה בשם מסחר	3.1.6
17	אימות זיהוי ראשוני	3.2
17	שיטה להוכחת החזקה במפתח פרטי	3.2.1
17	אימות זהות של ארגון	3.2.2
17	אימות זהות של אדם	3.2.3
18	מבקש תעודה שפרטיו לא אומתו	3.2.4
18	הסתמכות על זיהוי שביצעו גורמים מאשרים אחרים	3.2.5
18	אימות זהות בחידוש תעודה	3.3
18	אימות זהות בחידוש תעודה	3.3.1
18	אימות זהות בחידוש תעודה שבוטלה	3.3.2
18	אימות זהות בעת בקשה לביטול תעודה	3.4
20	היבטים תפעוליים במחזור חיים של תעודה אלקטרונית	4
20	בקשה להנפקת תעודה חדשה	4.1
20	מי יכול להגיש בקשה לתעודה	4.1.1
20	תהליך רישום	4.1.2
20	חובותיו של מבקש התעודה בתהליך הרישום	4.1.3
21	טיפול בבקשה להנפקת תעודה ועיבוד	4.2
21	אופן תהליך אימות הזהות	4.2.1
21	אישור או דחייה של בקשה לתעודה	4.2.2
21	משך זמן להנפקת התעודה	4.2.3
21	הנפקת התעודה	4.3
21	פעולות הגורם המאשר בזמן הנפקת התעודה	4.3.1
21	יידוע בעל התעודה על הנפקתה	4.3.2
21	מסירת תעודה וקבלתה על-ידי בעל התעודה	4.4
21	מסירת התעודה לבעליה	4.4.1

21.....	פרסום התעודה ע"י הגורם המאשר.....	4.4.2
21.....	יידוע גורמים חיצוניים על הנפקת התעודה.....	4.4.3
22.....	שימוש בתעודה אלקטרונית ובצמד מפתחות.....	4.5
22.....	חובותיו של בעל התעודה בעת שימוש במפתח הפרטי.....	4.5.1
22.....	השימוש של הצד המסתמך במפתח הציבורי והתעודה.....	4.5.2
22.....	חידוש תעודה אלקטרונית.....	4.6
22.....	נסיבות חידוש תעודה אלקטרונית.....	4.6.1
22.....	מי רשאי לבקש חידוש תעודה.....	4.6.2
22.....	תהליך העיבוד של בקשות לחידוש תעודה אלקטרונית.....	4.6.3
23.....	יידוע בעל התעודה על הנפקה.....	4.6.4
23.....	מסירת התעודה לבעליה.....	4.6.5
23.....	פרסום תעודה שחודשה.....	4.6.6
23.....	הודעה לישויות חיצוניות.....	4.6.7
23.....	הנפקה של תעודה קיימת, עם צמד מפתחות חדש (RE-KEY).....	4.7
23.....	שינויים בתעודה.....	4.8
23.....	ביטול תעודה או התלייתה.....	4.9
23.....	עילות לביטול תעודה.....	4.9.1
24.....	זהות הרשאים לבקש ביטול תעודה.....	4.9.2
24.....	תהליך לביטול תעודה.....	4.9.3
25.....	תקופת חסד עד לביטול תעודה.....	4.9.4
25.....	פרק הזמן שבו הגורם המאשר מחויב לבצע את הביטול.....	4.9.5
25.....	בדיקת רשימת התעודה הבטלות ע"י צד מסתמך.....	4.9.6
25.....	תדירות הנפקת רשימת תעודות מבוטלות (CRL).....	4.9.7
25.....	זמינות בדיקה מקוונת של תוקף תעודה.....	4.9.8
26.....	דרישות מקדימות לבדיקה מקוונת של תוקף תעודה.....	4.9.9
26.....	צורות אחרות של פרסום תוקף תעודה.....	4.9.10
26.....	דרישות מיוחדות בעת חשיפת מפתח פרטי של תעודה.....	4.9.11
26.....	נסיבות להתליית תעודה.....	4.9.12
26.....	זהות הרשאי לבקש התליית תוקף תעודה.....	4.9.13
26.....	תהליך התליית תוקף תעודה.....	4.9.14
26.....	מגבלות על התליית תוקף תעודה.....	4.9.15
26.....	שירותים לבדיקת סטטוס תעודה.....	4.10
26.....	מאפיינים תפעוליים.....	4.10.1
26.....	זמינות השירות.....	4.10.2
27.....	שירותים נוספים.....	4.10.3
27.....	פקיעת תוקף התעודה.....	4.11
27.....	הפקדת מפתח בידי צד ג' ואחזורו.....	4.12
28.....	אמצעי אבטחה פיסיים, נוהלי אבטחת מידע, ותפעול.....	5
28.....	אמצעים פיזיים.....	5.1
28.....	מיקום ומבנה האתר.....	5.1.1
28.....	כניסה פיזית לאתר המאובטח.....	5.1.2
28.....	אספקת חשמל ומיזוג אוויר לאתרי פרסונל איי.די.....	5.1.3
28.....	חשיפה למים.....	5.1.4
28.....	מערכות כיבוי אש והגנה מאש.....	5.1.5
28.....	אחסנת מצעים.....	5.1.6
28.....	פינוי אשפה.....	5.1.7
28.....	גיבוי מחוץ לאתר.....	5.1.8
29.....	אמצעים נוהליים.....	5.2
29.....	תפקידי אמון.....	5.2.1
30.....	משימות המחייבות יותר מאדם אחד לביצוען.....	5.2.2
30.....	תהליכי אימות הזהות הנדרש לביצוע משימה.....	5.2.3
30.....	הפרדת תפקידים.....	5.2.4
31.....	בקרת עובדים.....	5.3
31.....	בדיקת כשירות והתאמה לתפקיד.....	5.3.1
31.....	תהליכי אימות פרטי עובדים.....	5.3.2
31.....	דרישות הדרכה.....	5.3.3
31.....	תדירות עדכון ידע מקצועי.....	5.3.4
31.....	סבב תפקידים.....	5.3.5
31.....	אמצעים משמעתיים עקב חריגה מנוהלים.....	5.3.6
31.....	דרישות מקבלנים.....	5.3.7
31.....	מסמכים המסופקים לעובדים.....	5.3.8

31.....	נוהלי בקרת אירועי אבטחת מידע.....	5.4
32.....	סוגי אירועים שנרשמים.....	5.4.1
32.....	תדירות ייצור ובדיקה של קבצי דיווח.....	5.4.2
32.....	תקופת שמירה של קבצי דיווח.....	5.4.3
32.....	הגנה על קבצי דיווח.....	5.4.4
32.....	תהליכי גיבוי של קבצי דיווח.....	5.4.5
32.....	מערכת איסוף דיווחים.....	5.4.6
32.....	מנגנוני הודעה על אירועי אבטחה.....	5.4.7
32.....	הערכת פגיעות מערכות.....	5.4.8
32.....	ארכיבאות רשומות.....	5.5
33.....	סוגי רשומות.....	5.5.1
33.....	תקופת שמירה של רשומות.....	5.5.2
33.....	הגנה על רשומות בארכיב.....	5.5.3
33.....	תהליכי גיבוי של מערכות ארכיבאות.....	5.5.4
33.....	חותמת זמן על רשומות.....	5.5.5
33.....	שמירת תוקף משפטי של מידע.....	5.5.6
34.....	אחזור רשומות מארכיון.....	5.5.7
34.....	החלפת מפתחות חתימה אלקטרונית.....	5.6
34.....	הערכות לאסון.....	5.7
34.....	טיפול באירועי DRP.....	5.7.1
34.....	שיבוש במשאבי מחשב, תוכנה ומידע.....	5.7.2
35.....	חשיפה של מפתח פרטי של ישות במערכת הגורם המאשר.....	5.7.3
35.....	המשכיות עסקית לאחר מקרה אסון.....	5.7.4
35.....	הפסקת פעילות גורם מאשר או מערך רישום.....	5.8
35.....	הפסקת פעילות גורם מאשר.....	5.8.1
36.....	הפסקת פעילות מערך רישום.....	5.8.2
37.....	אמצעי בקרה טכנולוגיים לאבטחת מידע.....	6
37.....	ייצור צמד מפתחות והתקנתם.....	6.1
37.....	ייצור צמד מפתחות.....	6.1.1
37.....	העברת מפתח ציבורי של פרסונל איי.די. לבעלי תעודות ומסתמכים.....	6.1.2
37.....	אורכי מפתחות.....	6.1.3
37.....	מאפייני חילול מפתחות.....	6.1.4
37.....	ביקורת איכות של תכונות תעודה.....	6.1.5
38.....	הגנת מפתח פרטי.....	6.2
38.....	תקנים לאמצעי אחסנה קריפטוגרפיים.....	6.2.1
38.....	דרישה לביצוע פעולה על ידי יותר מאדם אחד לצורך הפעלת מפתח פרטי.....	6.2.2
38.....	הפקדת מפתח פרטי בנאמנות.....	6.2.3
38.....	גיבוי מפתח פרטי.....	6.2.4
38.....	ארכיבאות מפתח פרטי.....	6.2.5
38.....	הכנסת מפתח פרטי לאמצעי אחסנה.....	6.2.6
38.....	אחסון מפתח פרטי ברכיב מאובטח.....	6.2.7
38.....	שיטה להפעלת המפתח הפרטי.....	6.2.8
38.....	שיטה להשבתת מפתח פרטי.....	6.2.9
38.....	שיטה להשמדת מפתח פרטי.....	6.2.10
39.....	דירוג רכיב ההצפנה.....	6.2.11
39.....	היבטים נוספים של ניהול צמדי מפתחות.....	6.3
39.....	ארכיבאות מפתח ציבורי.....	6.3.1
39.....	פרקי זמן מותרים לשימוש בצמדי מפתחות.....	6.3.2
39.....	מידע להפעלה.....	6.4
39.....	דרישות ממידע להפעלה.....	6.4.1
39.....	הגנה על מידע להפעלה.....	6.4.2
39.....	אמצעים לאבטחת מחשבים.....	6.5
40.....	אמצעי אבטחת מידע ממוחשב.....	6.5.1
40.....	תקנים לאמצעי אבטחת מידע ממוחשב.....	6.5.2
40.....	מחזור חיים של מערכת תפעולית.....	6.6
40.....	אמצעים לבקרת פיתוח המערכת.....	6.6.1
40.....	אמצעים לבקרת האבטחה במערכת.....	6.6.2
40.....	אמצעי אבטחת תקשורת מחשבים.....	6.7
40.....	חתימת זמן.....	6.8
42.....	מאפייני תעודות ורשימת תעודות מבוטלות (CRL).....	7

42	מאפייני תעודה	7.1
42	מספר גירסה	7.1.1
42	שדות הרחבה בתעודה	7.1.2
42	סוגי אלגוריתמים	7.1.3
42	צורת שמות	7.1.4
42	מגבלות על שם	7.1.5
42	מזהה עצם (OID)	7.1.6
42	הגדרת שדות הרחבה כקריטיים	7.1.7
43	רשימת שדות עם ערכים משתנים ואפיונם	7.1.8
46	פרופיל תעודה אלקטרונית לשרת הנפקה ראשי (Root CA)	7.1.9
48	פרופיל תעודה אלקטרונית לשרת הנפקה תפעולי (Operational CA)	7.1.10
50	פרופיל תעודה ליחיד לביצוע "חתימה אלקטרונית מאושרת"	7.1.11
53	פרופיל תעודה לארגון לביצוע "חתימה אלקטרונית מאושרת"	7.1.12
57	פרופיל תעודה לארגון לביצוע "חתימה אלקטרונית מאושרת" ממוכנת	7.1.13
61	מאפייני רשימת תעודות בטלות	7.2
61	גרסה	7.2.1
61	רשימת תעודות בטלות ושדות גישה אליה	7.2.2
61	פרופיל רשימת התעודות הבטלות (CRL)	7.2.3
64	פרופיל OCSP	7.3
65	מבדקי התאמה	8
65	התאמה לת"י 27001 (ISO 127001)	8.1
65	התאמה לת"י ISO 9000:2000	8.2
65	ביקורת מערכות מידע	8.3
65	ביקורת יישום נהלי עבודה	8.4
65	ביקורת לפי ת"י 27001	8.4.1
65	ביקורת לפי ת"י ISO 9002	8.4.2
65	ביקורת יישום נוהלי עבודה פנימיים	8.4.3
65	ביקורת יישום נוהלי מסמך נהלים זה	8.4.4
65	תדירות מבדקי ההתאמה	8.4.5
66	זהות והכשרה של עורך המבדק	8.4.6
66	יחסי עורך המבדק ופרסונל איי.די.	8.4.7
66	נושאים המכוסים במהלך הבדיקה	8.4.8
66	תהליכים המבוצעים כתוצאה מתוצאות מבדק	8.4.9
66	הפצת תוצאות המבדק	8.4.10
67	היבטים עסקיים ומשפטיים אחרים	9
67	תעריפים	9.1
67	תעריפי הנפקה, חידוש וביטול תעודה	9.1.1
67	תעריפי גישה לתעודה	9.1.2
67	שגיאה! הסימניה אינה מוגדרת.	9.1.3
67	תעריפי בדיקת תוקף תעודה	9.1.4
67	תעריפים לשירותים אחרים	9.1.5
67	מדיניות החזרים כספיים	9.2
67	אחריות כספית	9.2.1
67	כיסוי ביטוחי	9.2.2
67	ערובות אחרות ביטוח וערובה	9.2.3
67	כיסוי ביטוחי למשתמשי קצה	9.2.4
67	יחסי נאמנות	9.3
68	סודיות מידע עסקי	9.3.1
68	מידע עסקי הנחשב כסודי	9.3.2
68	מידע עסקי שנחשב כגלוי	9.3.3
68	אחריות להגן על מידע סודי	9.4
68	מידע פרטי הנחשב כסודי	9.4.1
68	הגנת הפרטיות	9.4.2
68	מידע עסקי הנחשב כסודי-אישי	9.4.3
68	מידע אישי הנחשב כגלוי	9.4.4
69	אחריות על מידע סודי	9.4.5
69	הסכמה לשימוש במידע אישי	9.4.6
69	גילוי לרשויות אכיפת חוק	9.4.7
69	גילוי במסגרת הליך אזרחי	

69	קניין	9.5
69	כללי	9.5.1
69	קניין בצמדי מפתחות	9.5.2
69	קניין רוחני במסמך נהלים זה	9.5.3
70	מצגים ואחריות	9.6
70	מצגים ואחריות של הגורם המאשר	9.6.1
70	מצגים ואחריות של רשות רישום	9.6.2
70	מצגים ואחריות של בעל תעודה	9.6.3
70	מצגים ואחריות של צד מסתמך	9.6.4
71	מצגים ואחריות של צדדים אחרים	9.6.5
71	העדר מצגים	9.7
71	הגבלת אחריות	9.8
71	כללי	9.8.1
71	תקרת אחריות – הגבלה בסכום	9.8.2
71	אחריות פרסונל איי.די. כלפי בעל תעודה	9.8.3
71	אחריות פרסונל איי.די. כלפי צד מסתמך	9.8.4
72	תנאים נוספים	9.8.5
72	שיפוי ופיצוי (INDEMNITIES)	9.9
72	תחולה וסיום	9.10
72	תחולה	9.10.1
72	תוקף	9.10.2
72	תוקף של מסמך נהלים	9.10.3
72	השלכות סיום תוקף	9.10.4
72	דרכי תקשורת עם בעלי תעודות	9.11
72	ניהול שינויים	9.12
73	תהליך לביצוע שינויים במסמך	9.12.1
73	מנגנון לפרסום שינויים	9.12.2
73	נסיבות לשינוי מזהה עצם	9.12.3
73	יישוב סכסוכים	9.13
73	החוק החל	9.14
73	ציות לחוק החל	9.15
73	הוראות שונות	9.16
73	הוראות כלליות לחוזי פרסונל איי.די.	9.16.1
73	מיצוי	9.16.2
74	נתיקות	9.16.3
74	כח עליון	9.16.4
74	הוראות אחרות	9.17

1. מבוא

1.1 סקירה והגדרות

1.1.1 סקירת מסמך הנהלים

מסמך נהלים זה מפרט את התהליכים, האמצעים והנהלים המיושמים על-ידי פרסונל איי.די. בקשר עם הנפקת תעודה אלקטרונית כמשמעה בחוק חתימה אלקטרונית, התשס"א-2001 ("החוק"), שהיא "תעודה ליחיד" או "תעודה לארגון". תעודה ליחיד מזהה אדם פרטי ואת אמצעי אימות החתימה שלו (המפתח הציבורי כהגדרתו להלן) אך אינה כשירה לזהות אותו כמורשה חתימה של ארגון כלשהו. תעודה לארגון מזהה ארגון, כהגדרתו במסמך זה, אשר הרשה אדם, המזוהה אף הוא בתעודה, לשמש כמורשה חתימה אלקטרונית מטעמו.

בפעילויות הנוספות בתחום התעודות האלקטרוניות, מנפיקה פרסונל איי.די. גם תעודות אלקטרוניות למטרת חתימה אלקטרונית, אשר אינן עונות על דרישות החוק והתקנות לתעודות אלקטרוניות המשמשות לביצוע "חתימה אלקטרונית מאושרת". החתימה האלקטרונית המלווה בתעודות אלה, יכולה להיחשב, לכל היותר, כ"חתימה אלקטרונית מאובטחת", כהגדרתה בחוק. מסמך נהלים זה אינו חל על תעודות אלו.

פרטים נוספים על שירותי פרסונל איי.די. ניתן למצוא באתר האינטרנט של החברה בכתובת www.personalid.co.il.

מסמך נהלים זה אושר כעומד בדרישות החוק על-ידי רשם הגורמים המאשרים במשרד המשפטים, בהתאם לסמכותו על-פי תקנות 2 ו-10 לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהול), התשס"ב-2001.

חתימה אלקטרונית המופקת באמצעות "חתימה אלקטרונית מאושרת" כהגדרתה בחוק הינה, מכוח החזקה הקבועה בסעיף 4 לחוק, גם "חתימה אלקטרונית מאובטחת".

מסמך זה נערך בהתאם להוראת RFC 3647

Practices Internet X.509 Public Key Infrastructure Certificate Policy and Certification Framework של ה- Internet Engineering Task Force (IETF).

תקן ישראלי 27001, שעניינו ניהול אבטחת מידע.	"27001"
כל אחד מאלה: תאגיד; מוסד ציבורי.	"ארגון"
הארגון או האדם הפרטי שזהותו ואחזקתו במפתח הציבורי מאומתים בתעודה.	"בעל התעודה"
חוק חתימה אלקטרונית, התשס"א-2001.	"החוק"
העתק מתאים למקור המאומת בידי אחד מאלה: הרשות שהנפיקה את מסמך המקור, עורך דין בעל רשיון לעריכת דין בישראל, נציג דיפלומטי או קונסולרי ישראלי בחוץ לארץ.	"העתק מאושר"
חוק הגנת הפרטיות, התשמ"א-1981.	"חוק הגנת הפרטיות"
הנפקה של תעודה חדשה ליחיד, על סמך תהליך זיהוי קודם, פרטי זיהוי ומפתח ציבורי שאומתו בעת הנפקת תעודה ליחיד שטרם פקעה או בוטלה.	"חידוש תעודה"
כהגדרתה בחוק.	"חתימה אלקטרונית מאובטחת"
כהגדרתה בחוק.	"חתימה אלקטרונית מאושרת"
Object Identifier (OID) – מזהה יחודי שמטרתו לאפשר זיהוי חד ערכי של אובייקט כלשהו. רשימת המזהים מנוהלת ע"י ארגון IANA (www.iana.org).	"מזהה עצם"
מידע סודי ו/או ייחודי, שאינו מפתח ציבורי או פרטי, הנדרש לצורך שימוש במפתח פרטי השמור באמצעי החתימה, בעת הפקת חתימה אלקטרונית מאושרת (כגון – מספר זיהוי אישי (PIN) או מזהה ביומטרי).	"מידע להפעלה"
כהגדרתו ב"תקנות חומרה ותוכנה", להלן.	"מידע מן המרשם"
כהגדרתו בחוק.	"מסר אלקטרוני"
"Registration Authority". ארגון או יחיד כלשהם שאינם פרסונל איי.די., ואשר קשור בחוזה מקדים עם פרסונל איי.די., באישור הרשם, לזהות באמצעות "נציגי רישום", מבקשי תעודות ולטפל בבקשות להנפקה ו/או ביטול של תעודות אלקטרוניות	"מערך רישום חיצוני"
"אמצעי חתימה" כהגדרתו בחוק. מידע ייחודי הנוצר באופן אקראי וקשור מתימטית חד-ערכית למפתח הציבורי תואם, ואשר המחזיק בו חייב לשומרו בסודיות. המפתח הפרטי משמש להפקת חתימה אלקטרונית מאובטחת.	"מפתח פרטי"
מידע ייחודי הנוצר באופן אקראי וקשור מתימטית חד-ערכית למפתח הפרטי ומהווה "אמצעי אימות חתימה" כהגדרתו בחוק..	"מפתח ציבורי"
כהגדרתו בתקנות חומרה ותוכנה.	"מוסד ציבורי"
יחיד מטעמה של פרסונל איי.די. ו/או מטעמו של "מערך רישום חיצוני", הקשור בהסכם עם פרסונל איי.די., פועל בהתאם לנהליה ומורשה על-ידה לזהות מבקשי תעודות ולטפל בבקשות להנפקה ו/או ביטול של תעודות	"נציג רישום"

אלקטרוניות, לפי הסמכות המוגדרת והמפורשת שהוקנתה לו על-ידי פרסונל איי.די., בכפוף לאישור הרשם.

פרסונל איי.די. בע"מ.

"פרסונל איי.די."

זוג תואם מתימטית באופן חד-חד ערכי של מפתח פרטי ומפתח ציבורי.

"צמד מפתחות"

קובץ מידע הערוך לפי תקן ISO/IEC 9594-8, החתום אלקטרונית על-ידי פרסונל איי.די. והמפורסם על-ידיה באופן שוטף, ובו מפורטת רשימת התעודות שבוטלו טרם פקיעתן, מועד ביטולן וסיבת הביטול, אם נרשמה. רשימת סיבות הביטול יפורסמו באתר פרסונל איי.די..

"רשימת תעודות CRL בטלות"

שרת המכיל את רשימת התעודות הבטלות העדכנית ומאפשר שאילתות בפרוטוקול http.

"שרת פרסום" "שרתי פרסום"

כמשמעותו בחוק הגנת הפרטיות.

"רשם מאגרי מידע"

כהגדרתו בחוק.

"רשם", "רשם הגורמים המאשרים"

Certificate Extension - שדה נוסף בתעודת אלקטרונית בעל מזהה עצם משלו.

"שדה הרחבה"

שרת המכיל מידע על תוקפן של תעודות אלקטרוניות ומאפשר שאילתות מקוונות בפרוטוקול OCSP (On-Line Certificate Status Protocol).

"שרת OCSP"

"Operational CA". שרת המבצע את פעולת החיתום האלקטרוני של תעודות המונפקות לפי מסמך זה.

"שרת הנפקה"

כהגדרתו בחוק הפרשנות, התשמ"א-1981 ולמעט מוסד ציבורי.

"תאגיד"

מבנה הירארכי של שרתי הנפקה שראשיתו בשרת ההנפקה הראשי וסיומו בשרת ההנפקה שחתם על תעודה ליחיד.

"נתיב אישור"

מסר אלקטרוני הערוך לפי תקן ISO/IEC 9594-8 וחתום אלקטרונית על-ידי פרסונל איי.די..

"תעודה אלקטרונית"

תעודה אלקטרונית שהנפיקה פרסונל איי.די. בהתאם להוראות פרק ד' לחוק, המאשרת כי מפתח ציבורי מסוים הוא של יחיד בעל התעודה.

"תעודה ליחיד"

תעודה אלקטרונית המאשרת כי מפתח ציבורי מסוים הוא של שרת הנפקה.

"תעודת שרת"

תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.

"תקנות חומרה ותוכנה"

תקנות חתימה אלקטרונית (רישום גורם מאשר וניהול), התשס"ב-2001.

"תקנות ניהול גורם מאשר"

הנפקה של תעודה קיימת, עם צמד מפתחות חדש

"Re-Key"

1.2 זיהוי

1.2.1 מסמך נהלי הנפקת התעודה

מסמך זה יקרא "מסמך נהלים להנפקת תעודה אלקטרונית לביצוע חתימה אלקטרונית מאושרת ליחיד" ולשם הקיצור ייקרא בגוף המסמך - "מסמך נהלים זה".

1.2.2 מזהה עצם (OID)

מזהה העצם הראשי של פרסונל איי.די. ברשת האינטרנט הוא 1.3.6.1.4.1.12440. מספר זה מוקצה על ידי Internet Assigned Numbers Authority-IANA (www.iana.org).

כל מסמך הקשור בפעילות הגורם המאשר, כמו גם שדות הרחבה ייעודיים שיוגדרו בתעודה אלקטרונית מאושרת על ידי פרסונל איי.די. מקבלים מזהי עצם הנמצאים תחת מזהה העצם הראשי.

מזהה העצם של מסמך נהלים זה הוא 1.3.6.1.4.1.12440.1.

על פי מסמך מדיניות זה מונפקות שתי תעודות:

- תעודה אלקטרונית מאושרת ליחיד, מזהה עצם: 1.3.6.1.4.1.12440.1.1
- תעודה אלקטרונית מאושרת לארגון, מזהה עצם: 1.3.6.1.4.1.12440.1.2

1.3 ישויות משתתפות

1.3.1 מערך הנפקה

מערך פרסונל איי.די. כולל שרת הנפקה ראשי (Root CA) ושרתי הנפקה. צמד המפתחות של שרת ההנפקה הראשי, והתעודה המאשרת את זיהויו נחתמו אלקטרונית על ידו (Self-Signed) נוצרים בתהליך חיתום מתועד בנוכחות גורמי ביקורת חיצוניים (עו"ד, רו"ח, מומחה אבטחת מידע) ובנוכחות רשם גורמים מאשרים או נציגו.

שרת ההנפקה הראשי חותם בחתימה אלקטרונית מאובטחת תעודות אלקטרוניות המזהות שרתי הנפקה.

1.3.2 מערך רישום

מערך הרישום מעביר בקשות להנפקת תעודות וביטולן. על מערך הרישום לעשות זאת תוך יישום נהלים ואמצעים המפורטים במסמך נהלים זה.

מערך רישום משמש כזרוע ביצועית לצורך זיהוי מבקשי התעודות, רישום פרטי הבקשות, הגשתן למערך ההנפקה לצורך הנפקת תעודה והפצת התעודות המונפקות לבעליהן.

על-פי הוראות מסמך נהלים זה אפשר שפרסונל איי.די. תעשה שימוש במערך רישום חיצוני. הפעלת מערך רישום חיצוני על-פי מסמך נהלים זה חייבת על-פי תקנה 10(1) לתקנות חומרה ותוכנה באישור הרשם.

מערך רישום חיצוני ונציגי רישום קשורים בחוזה מקדים עם פרסונל איי.די., שבו מוסדרות סוגיות כגון בקרת עובדים, מערכות מידע, אחריות נזיקית לתוצאות פעולות מערך הרישום החיצוני וכד'.

1.3.3 בעלי תעודות

בעל תעודה הינו יחיד או ארגון אשר זוהה על פי מסמך נהלים זה וקיבל אמצעי לחתימה אלקטרונית.

1.3.4 ישויות נוספות

אין

1.4 שימושי תעודה מאושרת

בעלי תעודה ליחיד יכולים להיות יחידים בלבד. תעודה ליחיד אינה יכולה לזהות ארגון כלשהו ו/או להעיד על היותו של בעל התעודה מורשה חתימה אלקטרונית בשם הארגון, אף אם הארגון שילם עבור התעודה.

על בעל התעודה חלות חובות כמפורט בסעיף 4.5.1.

על בעל התעודה חלות, בנוסף, חובות שונות מכוח חוזה התקשרותו עם פרסונל איי.די., בתאום עם הרשם.

1.4.1 שימושים הולמים בתעודה

באמצעות צמד מפתחות ותעודה רשאי בעל התעודה (בתעודה ליחיד), או מורשה החתימה מטעם בעל התעודה (בתעודה לארגון), לחתום מסרים אלקטרוניים ב"חתימה אלקטרונית מאושרת", כהגדרתה בחוק.

בהתאם ובכפוף למדיניות הרשם, פרסונל איי.די. תהא רשאית, אך אינה חייבת, לאפשר לבעל התעודה לעשות שימוש בצמד המפתחות ובתעודה להזדהות באופן מקוון בפני מערכות מחשב (Client Authentication). ככל שהתעודה מתירה זאת, ייאמר בה הדבר במפורש, ואם לא נאמר במפורש – אין היא מתירה שימוש כזה.

1.4.1.1 שימושים מותנים או מוגבלים בתעודה

לשימושים ההולמים בתעודה המונפקת עלפי מסמך זה אפשר שיוספו תנאים ו/או מגבלות לגבי הנושאים הבאים:

□ סוג היישומים (applications), מערכות הפעלה (Operating Systems), חומרה (Hardware) ותוכנה (Software) באמצעותן ניתן להשתמש בתעודה;

□ הגבלה על אחריותו של הגורם המאשר בגין נזקים שנגרמו בשל שימוש בתעודה;

□ סכום העסקאות שניתן להתחייב בהן באמצעות התעודה;

□ הגבלות נוספות על השימושים המותרים בתעודה;

הגבלות על שימוש בתעודה ייעשו לבקשתו המפורשת של מבקש תעודה בלבד. אופן הבקשה יקבע באישור הרשם.

פרסונל איי.די. רשאית להגביל את השימוש ואת אחריותה הכוללת, כלפי כל אדם, בגין או בקשר עם שימוש ו/או הסתמכות על תעודה שהנפיקה, ביטלה, השתמשה, ו/או ניהלה, לרבות בגין או בקשר עם תעודה שהותלתה, או פגה. הגבלת האחריות תחול על נזק מכל סוג שהוא, לרבות נזקים ישירים, עקיפיים ותוצאתיים מכל סוג וכן תשלום והוצאה מכל סוג. פרסונל איי.די. תפרסם את מדיניות הגבלת האחריות במקום בולט באתר האינטרנט שלה ותציב קישור לפרסום זה בכל תעודה שתנפיק. אחריותה הכוללת של פרסונל איי.די. וכל מי מטעמה בכל הקשור לתעודות המונפקות לא תעלה על 500,000 ₪, בגין או בקשר עם תעודה, ללא תלות בהיקף העסקאות ולמספר הפעולות שנעשו באמצעות, או בקשר עם התעודה. בכל הקשור לתעודות המונפקות למבקשי תעודות (1) הנדרשים לעשות בהן שימוש למילוי דרישות חתימה לפי חיקוק, או (2) לפי דרישת רשות מרשויות המדינה, לא תגביל פרסונל איי.די. את אחריותה הכוללת בגין התעודה, כאמור לעיל, לפחות מ-500,000 ₪.

פירוט ההתניה או ההגבלה יעשה באמצעות תיאור טקסטואלי של המגבלה בשדה Certificate Policies בגוף התעודה וכן ההתניה או ההגבלה, אם קיימות, יירשמו בטופס שיצורף כנספח לחוזה ההתקשרות עם בעל התעודה.

1.4.2 שימושים אסורים בתעודה

אין לעשות בצמד המפתחות ובתעודה שימושים שאינם הולמים על-פי סעיף 1.4.1 לעיל. שימושים אסורים כאמור יעשו באחריותו המלאה והבלעדית של בעל התעודה והגורם המאשר לא ישא בכל אחריות לשימושים אסורים כאמור.

1.5 ניהול מסמך המדיניות

1.5.1 אחראי על מסמך המדיניות

בעל התפקיד האחראי על מסמך נהלים זה בפרסונל איי.די. הוא מנהל הגורם המאשר.

1.5.2 פרטי התקשרות

מנהל הגורם המאשר

פרסונל איי.די. בע"מ

רח' בן גוריון 34

רמת-גן

ישראל 52573

טל' 073-2900047

פקס 073-2900379

דוא"ל office@personalid.co.il

מוקד שירות לקוחות

טל' 073-2900047

פקס 073-2900379

דוא"ל support@personalid.co.il

1.5.3 אישור מסמך המדיניות

מסמך נהלים זה אושר כעומד בדרישות החוק על-ידי רשם הגורמים המאשרים במשרד המשפטים, בהתאם לסמכותו על-פי תקנות 2 ו-10 לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001 בתאריך _____.

2. חובות פרסום ואחסון

2.1 ארכיון

פרסונל איי.די. מקיימת ארכיון המחזיק נתונים בדבר תעודות וקבצי CRL שתוקפם פג. תעודות שפקעו מבלי שבוטלו קודם לכן מסיבה כלשהי, מועברות לארכיון בסמוך לאחר פקיעתן. מהארכיון ניתן, על ידי מי שמורשה לכך בפרסונל איי.די., לאחזר מידע הנוגע לתעודות ולסטטוס התעודות במועדים מן העבר. משך החזקת תעודות בארכיון יהיה כאמור בסעיף 5.5.2 להלן. השימוש בארכיון כפוף לתשלום, על-פי התעריפים שפרסונל איי.די. תקבע מעת לעת. יכול שתעריפים כאמור ייקבעו בחוזה ההתקשרות שבין פרסונל איי.די. לבין בעל התעודה או בינה לבין צד מסתמך. עם פרסום מסמך נהלים חדש, מועבר לארכיון מסמך הנהלים הישן והוא יהיה זמין לבדיקה מקוונת לצורך בחינה של תעודות שהונפקו על-פי מסמך הנהלים הישן. המסמך יישמר בארכיון לפרק הזמן המקביל לחובת השמירה של מסמכים של תעודה ספציפיות על-פי תקנות ניהול גורם מאשר.

2.2 פרסום מסמכי פרסונל איי.די.

- מסמך זה, בגרסתו המעודכנת ביותר ומועד תחולתו מפורסמים באתר האינטרנט של הגורם המאשר בכתובת הבאה :
<http://www.personalid.co.il/repository/cps/>
ניתן לגשת לדף זה גם מתוך קישור אשר יופיע בתעודה ובנוסף דרך דף הבית של הגורם המאשר. גרסאות קודמות של מסמך זה יפורסמו באותה הכתובת, לצד מועד התחולה. המסמך זמין לעיון בפורמט Adobe Acrobat.
הגרסה האלקטרונית התקפה, לכל דבר ועניין, היא רק זו שפורסמה בפורמט Adobe Acrobat מהדורה מודפסת של מסמך זה או של גרסאות קודמות של מסמך זה תשלחנה בדואר חוזר לפונים אל פרסונל איי.די. תמורת סכום שפרסונל איי.די. תקבע מעת לעת.
- תעודות שרתי ההנפקה יפורסמו באתר האינטרנט של הגורם המאשר בכתובת הבא :
<http://www.personalid.co.il/repository/certificates>
- רשימות תעודות בטלות יתפרסמו, בין היתר, בכתובת :
<http://www.personalid.co.il/crl>
- הוראות על מגבלות בתעודה
<http://www.personalid.co.il/repository/cps/limitations.pdf>
- רשימת קודים לסיבות ביטול
<http://www.personalid.co.il/repository/cps/RevokeReasonList.pdf>
- רשימת עדכונים למסמך הנהלים
http://www.personalid.co.il/repository/cps/CPS_versions.pdf

2.3 זמן ותדירות פרסום

- שינויים במסמך המדיניות מתפרסמים בהתאם למדיניות השינויים, כמפורט בסעיף 9.12.
- רשימות תעודות בטלות מתפרסמות בהתאם למדיניות הפרסום שנקבעה במסמך זה, בסעיף 4.9.7.
- פרסום תעודה של שרת הנפקה יתבצע בסמיכות להקמתו.

2.4 בקרת גישה

פרסונל איי.די. תאפשר גישה לעיון במסמכי נהלים להנפקת התעודות שאושרו על-ידי הרשם בגרסותיהם השונות, כמפורט בסעיף 2.2 לעיל.

פרסונל איי.די. מיישמת אמצעי בקרת גישה פיזיים ולוגיים על מאגרי המידע שלה, המיועדים למנוע עיון ו/או שימוש ו/או שינוי בלתי מורשה בהם, הכל בכפוף למדיניות הגנת הפרטיות ו/או הנחיות הרשם ו/או מדיניותה העסקית ו/או מדיניות אבטחת המידע שלה.

3. זיהוי והזדהות

3.1 מתן שמות

3.1.1 סוגי שמות ייחודיים

התעודה לשרתי ההנפקה של פרסונל איי.די. כוללת שמות ייחודיים, כמפורט בפרופיל התעודות בסעיפים 7.1.9, 7.1.10 למסמך נהלים זה.

תעודה המונפקת עלפי מסמך זה, כוללת שמות ייחודיים, כמפורט בפרופיל התעודה בסעיפים 7.1.11 ו- 7.1.12 למסמך נהלים זה.

בשדה ה-Common Name יופיע שם בעל התעודה (או מורשה החתימה בתעודה לארגון) בשפה האנגלית, כפי שמופיע באחד ממסמכי הזיהוי, ואחריו סוג תעודת הזיהוי, מספר תעודת הזיהוי וארץ הנפקת תעודת הזיהוי בפורמט המתואר בפרופיל התעודה כאמור. לאחר שם בעל התעודה או מורשה החתימה ותיאור מסמכי הזיהוי שלו, כאמור לעיל, אפשר ויתווספו פרטי מידע נוספים, העשויים להיות הכרחיים לצורך זיהוי החד-ערכי של בעל התעודה בבסיס נתונים כלשהו.

שמו הפרטי בעברית של בעל התעודה או מורשה החתימה, כפי רישומו במסמך הזיהוי יופיע בשדה Given Name (G). שם משפחתו בעברית של בעל התעודה או מורשה החתימה, כפי רישומו במסמך הזיהוי יופיע בשדה Surname (Sn).

שמו של בעל התעודה בתעודה לארגון כפי רישומו במסמכי הרישום, יופיע בשדה OU, ומספר המזהה של התאגיד (לדוגמא ח.פ.) יופיע בשדה O.

פרסונל איי.די. רשאית, אך לא חייבת, לכלול ב-CN את שם האדם בשפות נוספות.

פרסונל איי.די. רשאית להוסיף פרטי זיהוי נוספים לשדה ה-CN על-פי מסמך נהלים זה.

3.1.2 דרישת היות שם בעל התעודה אמיתי

על-פי מסמך נהלים זה לא תונפק תעודה אלא אם היא כוללת את שמו של אדם, ובתעודה לארגון, גם את שם הארגון כפי שמופיעים במסמכים הדרושים לזיהויים על-פי התקנות. כל עוד לא נקבע אחרת בתקנות ו/או בהנחיות הרשם, התעודה הראשית לזיהוי של אדם הינה תעודת זהות שהונפקה לו על-ידי משרד הפנים של מדינת ישראל (ביחיד שהוא תושב ישראל) ודרכון (ביחיד שהוא תושב חוץ).

בתעודה לארגון יהיה שם בעל התעודה בעברית ו/או באנגלית, בהתאם למסמכים שהוצגו לזיהוי. לא היה לארגון שם עברי רשמי, יתורגם שמו בתרגום סביר לעברית.

3.1.3 מנויים אנונימיים

על-פי מסמך נהלים זה לא תונפק תעודה לגורם אנונימי.

3.1.4 כללי פירוש של צורות שם שונות

אין.

3.1.5 ייחודיות השם

שיטת בניית שם התעודה למנויים, כפי שמפורטת בסעיף 3.1.1, מבטיחה שלכל בעל תעודה שהוא יחיד, ולכל מורשה חתימה בארגון יקבע CN ייחודי. בתעודה ליחיד, הייחודיות נקבעת באמצעות תעודת הזהות של המבקש המצוינת ב-CN. בתעודה לארגון, הייחודיות נקבעת באמצעות המספר המזהה של הארגון, המצוין בשדה OU.

3.1.6 הכרה ואימות החזקה בשם מסחר.

חל איסור להשתמש בשמות ובסימנים המפרים זכויות של צדדים שלישיים, במסגרת הבקשה לתעודה. פרסונל איי.די. איננה בודקת אם המבקש רשאי להשתמש בשם או סימן מסוים, אם לאו והיא לא תשמש כבורר, מגשר או כל מנגנון אחר לשוב סכסוך בעניין שימוש בשם או סימן כאמור. פרסונל איי.די. רשאית

להשעות, לפי שיקול דעתה, בקשה לקבלת תעודה בשל סכסוך על שם או סימן הכלול בה ולא תישא בכל אחריות בשל כך.

3.2 אימות זיהוי ראשוני

צמד המפתחות לחתימה אלקטרונית יחולל בנוכחות ו/או על-ידי נציג רישום ובמעמד מסירת צמד המפתחות והתעודה האלקטרונית לידי בעל התעודה

3.2.1 שיטה להוכחת החזקה במפתח פרטי

צמד מפתחות החתימה האלקטרונית מיוצר בנוכחות ו/או על ידי נציג הרישום ובמעמד מסירתם לבעל התעודה בלבד בהתאם להנחיות הרשם, וכך מבוצעת הוכחת החזקה במפתח הפרטי.

3.2.2 אימות זהות של ארגון

אימות הזהות של ארגון יתבצע בהתאם להוראות תקנה 10(2) לתקנות חומרה ותוכנה, על פי הכללים הבאים.

3.2.2.1 ארגון הרשום בישראל –

- תעודת הרישום
- אישור עורך דין על קיומו של תאגיד, שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור - על פי אימות במרשמים המתאימים
- מורשה החתימה מטעם הארגון יזוהה ע"פ האמור בסעיף 3.2.3.
- ארגון המשתמש בשרת חתימות, יאשר באמצעות ארגון מוסמך, בהתאם לטופס שקבע הרשם, כי נמסרו לו פרטים אודות אופן הפעלת השרת והוא מכיר את הסיכונים הקשורים בשימוש בשרת. תעודה כאמור, תכלול פרטים אודות היותה לשימוש ממוכן.

3.2.2.2 ארגון שאינו רשום בישראל –

- על פי העתק מאושר ממסמך המעיד על רישומו
- אישור של עורך דין על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור - על פי אימות במרשמים המתאימים

3.2.3 אימות זהות של אדם

אימות זהות של אדם המקבל תעודה ליחיד נעשית על-פי הוראות החוק, על-פי תקנות חומרה ותוכנה ועל-פי הנחיות הרשם ו/או על-פי החלטות פרסונל איי.די. (ככל שאינן סותרות את הוראות החוק, התקנות והנחיות הרשם). בגורם המאשר מיושמים נהלי בדיקה פנימיים שתפקידם להקטין את הסיכון בכשל באימות הזהות. נבדקים הפרטים הבאים:

- זהותו של מבקש התעודה.
- נכונות הפרטים המפורטים בבקשה להנפקת התעודה.

3.2.3.1 אימות זהות של תושב ישראל

יחיד שהוא תושב ישראלי יזוהה על פי אלו:

- תעודות זהות ומידע מן המרשם
- וכן לפי אחד מן המסמכים האלו ובלבד שהם בתוקף:
- דרכון ישראלי
- רישיון נהיגה הנושא תמונה של המבקש

- מסמך מזהה שמונפק ע"י המדינה, כאמור בתקנות ובהנחיות הרשם.
- למי שאין בידיו אחד מאלו, והגיש תצהיר על כך, אחד מאלו:
 - תעודות מעבר
 - מסמך מזהה מסוג אחר שהרשם אישר לעניין זה, כאמור בתקנות חומרה ותוכנה
 - אישור עורך דין על זהותו, כאמור בתקנות חומרה ותוכנה ועל פי נוסח שהינחה הרשם

3.2.3.2 אימות זהות תושב חוץ

יחיד שהוא תושב חוץ יזוהה על פי אחד מאלו:

- דרכון חוץ
- תעודת מסע
- תעודת זהות

וכן על פי מסמך זיהוי נוסף הנושא תמונה של המשתמש ופרטים מזהים שלו ושל מי שהנפיק את המסמך הנוסף.

בנוסף לאמור בסעיפים 3.2.3.1 ו- 3.2.3.2 לעיל: בתעודה לארגון או למוסד ציבורי, יזוהה מורשה החתימה על פי העתק מאושר של החלטת הארגון המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד, או אישור של עורך דין על מורשה החתימה כאמור.

3.2.4 מבקש תעודה שפרטיו לא אומתו

לא תונפק תעודה אלקטרונית למי שפרטיו לא אומתו כנדרש.

3.2.5 הסתמכות על זיהוי שביצעו גורמים מאשרים אחרים

לא תונפק תעודה ליחיד בהסתמך על זיהוי שבוצע על-ידי גורם מאשר שאינו פרסונל איי.די. ו/או נציג רישום מטעמה.

3.3 אימות זהות בחידוש תעודה

3.3.1 אימות זהות בחידוש תעודה

חידוש תעודה נעשה לאחר אימות החזקת בעל התעודה במפתח הפרטי לפי התהליך המתואר בסעיף 3.2.1 לעיל, כשהמסר החתום אלקטרונית מכיל את פרטי המפתח הציבורי החדש, אם נוצר כזה, ונחתם על אלקטרונית על ידי המפתח הפרטי התקף.

בנוסף, מתבצע אימות של זהות שולח המסר על סמך הוכחת ידיעת פרטי מידע ייחודיים שסופקו על ידי פרסונל איי.די. לבעל התעודה, או שסופקו על-ידי בעל התעודה לפרסונל איי.די., בתהליך הרישום הראשוני. אימות הפרטים יכול שיעשה באופן מקוון או בטלפון ובלבד שהרשם אישר את הפרוצדורה הטכנולוגית של האישור מרחוק.

הוראות סעיף זה אינן חלות על אימות זהות בחידוש תעודה שלא הונפקה על ידי פרסונל איי.די.. במקרה זה יש לזהות את בעל התעודה בתהליך זיהוי ראשוני, כאמור בסעיף 3.2 לעיל.

3.3.2 אימות זהות בחידוש תעודה שבוטלה

אין חידוש לתעודה שבוטלה.

3.4 אימות זהות בעת בקשה לביטול תעודה

ביקש בעל תעודה (או אדם אחר הרשאי לבטל את התעודה על-פי החוזה בין בעל התעודה לבין פרסונל איי.די.) או אדם המוסמך לכך על פי דין, לבטל תעודה שהונפקה לו על-פי מסמך נהלים זה, תאומת זהות המבקש באמצעות מידע ייחודי שסיפק מורשה הביטול לפרסונל איי.די. או למערך הרישום החיצוני בעת שהונפקה התעודה נשוא בקשת הביטול – או, לפי העניין, באמצעות הוכחת ידיעת מידע ייחודי שפרסונל איי.די. או מערך הרישום החיצוני סיפקו לו לצורך אימות זהותו במקרים כאלה בעת הנפקת התעודה. אימות הפרטים יכול שייעשה באופן מקוון או בטלפון, לפי החלטת פרסונל איי.די. בתהליך שאושר ע"י הרשם.

היה ולא ניתן לזהות את מבקש הביטול באמצעות מידע ייחודי שסיפקה פרסונל איי.די. (למשל, אם פרט המידע נשכח או רישומו אבד), תפעל פרסונל איי.די. לזהות את המבקש באמצעים מקובלים אחרים להנחת דעתה, באישור מנהל הגורם המאשר ועל פי נוהל שאושר ע"י הרשם.

4. היבטים תפעוליים במחזור חיים של תעודה אלקטרונית

4.1 בקשה להנפקת תעודה חדשה

4.1.1 מי יכול להגיש בקשה לתעודה

תעודה ליחיד - כל יחיד, שהוא אזרח במדינת ישראל או תושב חוץ, או ארגון ובלבד שיש ברשותו המסמכים הדרושים לזיהוי על פי סעיף 3.2.3.

תעודה לארגון – כל תאגיד הרשום בישראל או שאינו רשום בישראל, או מוסד ציבורי ובלבד שיש ברשותו המסמכים הדרושים לזיהוי לפי סעיפים 3.2.2 ו-3.2.3.

4.1.2 תהליך רישום

הגשת בקשה למערכת החיתום להנפקת תעודה לאדם על-פי מסמך נהלים זה תעשה רק לאחר השלבים הבאים:

- מסירה של מסמכי הזיהוי הנדרשים לפי חוק והסמכת פרסונל איי.די. לשמור עותק מהם;
- זיהוי פנים אל פנים ואימות הפרטים של מבקש התעודה כמפורט בסעיף 3.2 למסמך נהלים זה;
- חתימה של מבקש התעודה על הצהרה בנוסח שנקבע על ידי הרשם בדבר הסיכון הכרוך בשימוש בחתימה אלקטרונית והחובות המוטלות עליו, בהתאם לתקנה 11(3) לתקנות רישום וניהול;
- במידה ואמצעי האחסנה המיועד לייצור ואחסנת צמד המפתחות והתעודה אינו מסופק על ידי פרסונל איי.די., יידרש המבקש להצהיר בפני פרסונל איי.די. לפי תקנה 13(ב) בדבר אמצעי החתימה בו משתמש, אופן הפעלתו, הגישה אליו והמידע הנדרש להפעלתו, בהתאם להנחיות הרשם;
- במידה ואמצעי האחסנה המיועד לייצור ואחסנת צמד המפתחות הוא מחשב-שרת ארגוני, הרי שעל מבקש התעודה לציין זאת בפני פרסונל איי.די. והתעודה שתונפק למבקש תכלול הוראה המעידה על כך, בהתאם לנוסח המופיע בסעיף 7.1.11 להלן.
- חתימה על חוזה התקשרות עם פרסונל איי.די.;
- סיסמא לביטול;
- סיסמא לשחרור מנעילה במידה שאישר הרשם הפעלת תכונה זו באמצעי האחסנה ובהתאם לתנאים שאישר.

4.1.3 חובותיו של מבקש התעודה בתהליך הרישום

מבקש התעודה ליחיד חייב -

4.1.3.1 מסירת פרטי זיהוי מסמכי זיהוי נכונים

למסור לפרסונל איי.די., לפי בקשתה, מידע שהוא למיטב ידיעתו נכון ומלא, הדרוש לפרסונל איי.די. לשם ביצוע תפקידיה לפי החוק. מבלי לגרוע מכלליות האמור לעיל, ימסור מבקש התעודה לפרסונל איי.די. העתק של המסמכים שעל-פיהם היא נדרשת לזיהויו לפי הוראות החוק, התקנות, הנחיות הרשם ומסמך נהלים זה.

מבקש התעודה ימסור מידע שיאפשר לפרסונל איי.די. לזהות בפניה מרחוק אל פרסונל איי.די. את בעל התעודה ו/או את מורשה הביטול לצורך תהליכי ביטול תעודה או חידושה. הוראות בעניין הליך חידוש וזיהוי לצורך חידוש יקבעו באישור הרשם.

4.1.3.2 חתימה על מסמך אזהרה

לחתום על מסמך, בנוסח התואם את הנחית הרשם, המאשר כי בעל התעודה הוזהר בדבר הסכנות הכרוכות בשימוש בתעודה והחובות המוטלות עליו מכוח החוק

4.1.3.3 חתימה על הצהרה בדבר שימוש באמצעי חתימה

אם אמצעי החתימה ו/או אמצעי האחסנה לא סופקו על ידי פרסונל איי.די. - לחתום על הצהרה בנוסח התואם את תקנה 13(ב) לתקנות חומרה בתוכנה וכן את הנחיית הרשם, בדבר אמצעי החתימה בו הוא משתמש, אופן הפעלתו והגישה אליו כאמור בדרישות תקנה 18(ב) ו/או 81(ג) לתקנות חומרה ותוכנה.

4.2 טיפול בבקשה להנפקת תעודה ועיבודה

4.2.1 אופן תהליך אימות הזהות

אימות זהות המבקש יתבצע על ידי שני נציגים של הגורם המאשר או של גורם רישום שהוסמך ואושר על פי סעיף 1.3.2. הנציגים יאמתו את זהותו של המבקש כמפורט בסעיף 3.2.

4.2.2 אישור או דחייה של בקשה לתעודה

היה ואומתו הפרטים ומולאו התנאים המוקדמים להגשת הבקשה כאמור בסעיף 4.1.2, תוגש הבקשה אל שרתי ההנפקה לאישור. היה ולא אומתו הפרטים, או לא מולאו התנאים להגשת הבקשה כאמור, לא תוגש הבקשה אל שרתי ההנפקה והבקשה תידחה.

4.2.3 משך זמן להנפקת התעודה

תעודה המונפקת על-סמך מסמך נהלים זה תונפק במעמד הזיהוי.

4.3 הנפקת התעודה

4.3.1 פעולות הגורם המאשר בזמן הנפקת התעודה

הגורם המאשר יבדוק אם הפרטים המופעים בבקשה תואמים לתבנית התעודה המבוקשת.

4.3.2 יידוע בעל התעודה על הנפקתה

פרסונל איי.די. תודיע לבעל התעודה על הנפקת התעודה במעמד ההנפקה.

4.4 מסירת תעודה וקבלתה על-ידי בעל התעודה

4.4.1 מסירת התעודה לבעליה

4.4.1.1 מסירה בעת תהליך הזיהוי

התעודה תימסר לבעל התעודה לאחר הנפקתה בסמוך למועד תהליך זיהוי בעל התעודה על-ידי מערך הרישום. נציג הרישום יתעד את מועד ועצם מסירת התעודה. סרב בעל התעודה לקבל את התעודה, תבוטל התעודה מיידית על ידי נציג הרישום ו/או פרסונל איי.די..

4.4.1.2 סיסמאות לביטול ושחרור מנעילה

עם מסירת התעודה לבעליה, ימסרו גם המידע ייחודי לזיהוי בעל התעודה בעת בקשה לביטול התעודה וסיסמה לשחרור אמצעי החתימה מנעילה. מבלי לגרוע מהצורך באישור הרשם, פרסונל איי.די. מתחייבת כי היא מיישמת טכנולוגיות שמטרתן שמירה כי לא תפגע שליטתו הבלעדית של בעל אמצעי החתימה באמצעי החתימה בשל שימוש בסיסמת שחרור מנעילה, וכי ססמת שחרור מנעילה לא תשמר על ידה.

4.4.2 פרסום התעודה ע"י הגורם המאשר

הגורם המאשר יהיה רשאי, אך לא חייב, לפרסם את התעודה לכלל הציבור ו/או לצדדים שלישיים מסוימים – בין אם במסגרת ארכיב ציבורי ובין אם בכל דרך אחרת שיבחר.

4.4.3 יידוע גורמים חיצוניים על הנפקת התעודה

הגורם המאשר יהיה רשאי, אך לא חייב, ליידע את כלל הציבור ו/או צדדים שלישיים מסוימים על עצם הנפקת התעודה.

4.5 שימוש בתעודה אלקטרונית ובצמד מפתחות

4.5.1 חובותיו של בעל התעודה בעת שימוש במפתח הפרטי

4.5.1.1 הגנה על מפתח פרטי של בעל תעודה

לנקוט בכל האמצעים הסבירים לשם שמירה על אמצעי החתימה ולשם מניעת שימוש בו ללא הרשאה כאמור בסעיף 7 (א) (1) לחוק. היה ואמצעי האחסנה ואמצעי החתימה סופק ע"י פרסונל איי.די., יסופקו הנחיות מתאימות לאופן השמירה על אמצעי החתימה כאמור.

4.5.1.2 הודעה על חשיפה של מפתח פרטי

מיד כשנודע לו כי נפגעה השליטה במפתח הפרטי יתקשר בעל התעודה אל פרסונל איי.די. בטלפון או יגיע פיזית למשרדי פרסונל איי.די. ויודיע על החשיפה. פרטי התקשרות עדכניים יתפרסמו באתר האינטרנט של הגורם המאשר בכתובת www.personalid.co.il.

במידה וההודעה על הפגיעה בשליטה במפתח הפרטי נעשתה מרחוק, נידרש המבטל להזדהות בעזרת המידע הייחודי לזיהוי אשר נמסר לו בתהליך ההנפקה.

4.5.1.3 מגבלות על שימוש בעל תעודה במפתח פרטי

להשתמש במפתח הפרטי אך ורק לשימושים שלא הוגבלו או הותנו בתעודה או במסמך זה (סעיף 1.4).

4.5.1.4 חובת שמירתו של מידע ייחודי בסודיות

לנקוט בכל האמצעים הסבירים הדרושים לשמירת סודיות המידע הייחודי המשמש להפעלת אמצעי החתימה, או לזיהוי מרחוק לצורכי תפעול, כגון ביטול תעודה ושחרור מנעילה.

4.5.2 השימוש של הצד המסתמך במפתח הציבורי והתעודה

כדי להסתמך על תעודה, על צד מסתמך לבדוק את סטאטוס התעודה, לרבות סטאטוס התעודה של שרת החיתום של התעודה (בהתאם לסעיף 4.9.6) וכן ואת תקינות החתימה האלקטרונית לצורך הסתמכות על החתימה. כמו כן צד מסתמך חייב לקיים את הוראות ההסכם בינו לבין פרסונל איי.די., אם קיים וכן את הוראות הדין הכללי ו/או החוק החלות (ככל שחלות) על הסתמכותו.

4.6 חידוש תעודה אלקטרונית

4.6.1 נסיבות חידוש תעודה אלקטרונית

חידוש תעודה אלקטרונית יכול שיתבצע באחד מהמקרים הבאים:

- תוקף התעודה עומד לפוג.
- הנחיית רשם, או מקרה מיוחד באישורו.

פרסונל איי.די. רשאית, אך אינה חייבת, לשלוח לבעל התעודה תזכורת לפני מועד פקיעת התעודה.

4.6.2 מי רשאי לבקש חידוש תעודה

רשאי לבקש חידוש תעודה, מי שהונפקה עבורו תעודה על פי מסמך נהלים זה, והתעודה עודנה בתוקף.

4.6.3 תהליך העיבוד של בקשות לחידוש תעודה אלקטרונית

בתהליך הבקשה לחידוש התעודה, תזוהה פרסונל איי.די. את מבקש החידוש בהתאם לנוהל המפורט בסעיף 3.3.1.

4.6.4 יידוע בעל התעודה על הנפקה

יידוע בעל התעודה על הנפקתה, יתבצע כאמור בסעיף 4.3.2

4.6.5 מסירת התעודה לבעליה

מסירת תעודה שחודשה תתבצע כאמור בסעיף 4.4.1

4.6.6 פרסום תעודה שחודשה

פרסום תעודה שחודשה יתבצע כאמור בסעיף 4.4.2.

4.6.7 הודעה לישויות חיצוניות

יידוע גורמים חיצוניים על הנפקה התעודה יתבצע כאמור בסעיף 4.4.3.

4.7 הנפקה של תעודה קיימת, עם צמד מפתחות חדש (re-Key)

עבור תעודות שהונפקו על פי מסמך נהלים זה, לא יתבצע תהליך של re-Key.

4.8 שינויים בתעודה

בתעודה שהונפקה לפי מסמך נהלים זה לא יתבצעו שינויים כלשהם. במידה ונדרש לבצע שינוי, תונפק תעודה חדשה עם הפרטים החדשים, ולפי כל הכללים להנפקת תעודה או חידושה.

4.9 ביטול תעודה או התלייתה

4.9.1 עילות לביטול תעודה

תעודה שהונפקה על פי מסמך זה תבוטל במקרים הבאים:

4.9.1.1 בקשת בעל התעודה

על-פי בקשת בעל התעודה, לאחר וידוא זהות המבקש כבעל התעודה כאמור בסעיף 3.4.

4.9.1.2 מידע לא נכון בתעודה

אם נודע לפרסונל איי.די. כי פרט מהפרטים המופיעים בתעודה אינו נכון.

4.9.1.3 מות בעל התעודה, או פירוק התאגיד

עם מותו של בעל התעודה (או מורשה החתימה בתעודה לארגון), לאחר קבלת הודעה על כך בגורם המאשר ואימות ההודעה מול המידע מן המרשם, ובתעודה לארגון – אם יצא צו לפירוק התאגיד.

4.9.1.4 פגיעה בשליטה באמצעי חתימה של גורם מאשר

אם נודע לגורם המאשר על פגם בחתימה האלקטרונית המאובטחת שלו, או במערכות החומרה והתוכנה שלו, שיש בו כדי לפגוע במהימנות חתימתו או במהימנות התעודות האלקטרוניות שהוא מנפיק, או עם חשיפת המפתח הפרטי של הגורם המאשר.

4.9.1.5 הפרת התחייבות בעל התעודה

הגורם המאשר רשאי לבטל תעודה כאשר בעל התעודה מפר אחת או יותר מההתחייבויות המפורטות להלן -

- כל התחייבות כספית, או שוות ערך של המשתמש לגורם המאשר ו/או למי מטעמו, שלא שולמה או בוצעה במועדה.
- בכל מקרה אחר, בכפוף לאישור הרשם.

4.9.1.6 פירוק גורם מאשר

פורסמה הודעה על פירוק הגורם מאשר, או החליט הגורם המאשר על הפסקת פעילותו כגורם מאשר, או הודיע הרשם לגורם מאשר כי בכוונתו למחוק את רישומו מן המרשם לפי הוראות סעיף 14 לחוק (לפי סעיף 5.8.1).

4.9.1.7 פסלות דין של בעל תעודה

עקב הכרזת בעל התעודה כפסול דין על-פי חוק הכשרות המשפטית והאפוטרופסות, התשכ"ב-1962.

4.9.1.8 צו בית משפט

עם קבלת צו מחייב כדין מבית משפט במדינת ישראל המורה לפרסונל איי.די. לבטל תעודה מסוימת.

4.9.1.9 הוראת ביטול אחרת

עם קבלת הוראת ביטול ממי שהורשה בהסכם עם בעל התעודה להורות כך או על פי דין.

4.9.2 זהות הרשאים לבקש ביטול תעודה

4.9.2.1 בעל התעודה

בעל התעודה רשאי לבקש ביטול תעודה שהונפקה עבורו.

4.9.2.2 מנהל הגורם המאשר בפרסונל איי.די.

מנהל הגורם המאשר בפרסונל איי.די., או מי שהורשה מטעמו, רשאי לבטל את התעודה במקרים המפורטים בסעיפים 4.9.1.2, 4.9.1.3, 4.9.1.4, 4.9.1.5, 4.9.1.6. במקרה המפורט בסעיף 4.9.1.6, נדרש גם אישורו של הרשם.

4.9.2.3 אפוטרופוס של בעל תעודה

במקרה המפורט בסעיף 4.9.1.7, רשאי לבקש את ביטול התעודה האפוטרופוס שמונה לבעל התעודה.

4.9.2.4 מי שהורשה על ידי בעל תעודה

במקרה המפורט בסעיף 4.9.1.9 רשאי לבקש את ביטול התעודה מי שהורשה בהסכם עם בעל התעודה לעשות כן, והרשאה זו הודעה לפרסונל איי.די. על-ידי בעל התעודה או על פי דין.

4.9.3 תהליך לביטול תעודה

4.9.3.1 בעל התעודה

במקרה המפורט בסעיף 4.9.2.1 לעיל, יתקשר בעל התעודה אל פרסונל איי.די. או אל מערך הרישום שהנפיק לו את התעודה בטלפון או יגיע פיזית למשרדי פרסונל איי.די. או מערך הרישום. לאחר שאומתה זהות המבקש בהתאם לתהליך המפורט בסעיף 3.4, תבוטל התעודה מיידית (תהליך ביטול התעודה לא יהא בשליטתו של אדם אחד בלבד בגורם המאשר).

במידה והבקשה לביטול התעודה נעשתה מרחוק, נידרש המבטל להזדהות בעזרת המידע הייחודי לזיהויו אשר נמסר לו בתהליך ההנפקה.

4.9.3.2 מנהל הגורם המאשר

במקרים המפורטים בסעיף 4.9.1 לעיל יורה מנהל הגורם המאשר בפרסונל איי.די., או מי שהוסמך מטעמו, לאחר שנוכח כי קיימת עילה לכך ובהמשך לברור טלפוני, ככל שהדבר רלוונטי, על ביטול התעודה. הודעה על ביטול התעודה תישלח לבעל התעודה לפי כתובת הדואר האלקטרוני המופיעה בתעודה, ואם אין מופיעה כתובת כזו - באמצעות הטלפון ו/או בדואר לכתובת בעל התעודה כפי שמופיעה במסמכי הרישום.

4.9.3.3 בעל התעודה הוכרז פסול דין

במקרה המפורט בסעיף 4.9.1.7 יגיע האפוסטרופוס למשרדי פרסונל איי.די., או יעביר אל מנהל הגורם המאשר מידע מאומת המעיד על פסלות הדין של בעל התעודה.

4.9.3.4 מי שהורשה על-ידי בעל התעודה

במקרה המפורט בסעיף 4.9.1.9 יתבצע תהליך הביטול בדומה לביטולה על-ידי בעל תעודה כמצוין בסעיף 4.9.2.1, באמצעות בקשה על ידי נציג מוסמך של בעל התעודה, או על ידי אדם הרשאי לכך על פי דין ושאינו מורשה על ידי בעל התעודה.

4.9.4 תקופת חסד עד לביטול תעודה

במקרים המפורטים בסעיף 4.9.1.5 רשאי מנהל הגורם המאשר בפרסונל איי.די., או מי שהורשה על ידו, לתת לבעל התעודה פרק זמן לפי שיקול דעתו להסדיר את ענייניו. בכל מקרה אחר, תבוטל התעודה מיד לאחר אימות זהות המבקש ו/או אימות העובדות המשמשות יסוד לביטול.

4.9.5 פרק הזמן שבו הגורם המאשר מחויב לבצע את הביטול

בכל מקרה שבו לא ניתנה תקופת חסד כאמור בסעיף 4.9.4, תבוטל התעודה מיידית.

4.9.6 בדיקת רשימת התעודות הבטלות ע"י צד מסתמך

בדיקת תוקף תעודה שהנפיקה פרסונל איי.די. על פי מסמך נהלים זה יכולה להיעשות בדרכים הבאות:

□ פניה של צד מסתמך לאתר אינטרנט בפרוטוקול HTTP (Hyper Text Transfer Protocol) לקובץ בסיומת CRL.

□ פניה של צד מסתמך בפרוטוקול OCSP (On-line Certificate Status Protocol) לשרת OCSP בפרסונל איי.די. (אם קיים).

המידע על הכתובות של שרתי המחשבים בהם נמצאת רשימת התעודות הבטלות מופיע בשדה – CDP (CRL Distribution Point) בתעודה.

ניתן להוריד את רשימות התעודות הבטלות באופן ידני בכתובת: <http://www.ica.co.il/crl>. קישור לדף זה ניתן למצוא בדף הראשי של אתר האינטרנט של הגורם המאשר.

על הצד המסתמך לוודא שהבדיקה מתבצעת מול רשימת התעודות הבטלות המעודכנת ביותר, ולא מול רשימה ישנה יותר (כגון, רשימה השמורה בזיכרון מטמון), גם אם הרשימה המצויה בידו הינה בתוקף שהוגדר לה.

פרסונל איי.די. רשאית, לפי שיקול דעתה המוחלט, לאפשר לצדדים מסתמכים לקבל באופן מקוון עותק עדכני של רשימת התעודות הבטלות לשימוש הפנימי, וזאת במקביל לפרסום רשימת התעודות הבטלות בשרתי הפרסום. הזכות לבדיקה מרוכזת זו של תוקף תעודות טעונה התקשרות בהסכם בכתב ומראש עם פרסונל איי.די.. במקרה כזה יחולו כל הכללים בעניין תדירות הפרסום כאמור בסעיף 4.9.7.

4.9.7 תדירות הנפקת רשימת תעודות מבטלות (CRL)

תדירות ההנפקה של רשימת תעודות מבטלות במערך פרסונל איי.די. היא:

□ רשימת תעודות בטלות של שרת ה-Root CA - כל שלושה חודשים או מיידית עם ביטול תעודה של שרת הנפקה שנחתמה על-ידי שרת ה-Root CA.

הרשימה תונפק עם תוקף של 3 חודשים.

❑ רשימת תעודות מאושרות בטלות שהונפקו על-ידי שרת הנפקה (OCA) – מיד עם ביטול תעודה שהונפקה על-ידי שרת הנפקה זה או כל 12 שעות, או לפי שיקול דעתה הבלעדי של פרסונל איי.די., לפי המוקדם מביניהם.

הרשימה תונפק עם תוקף של 24 שעות (היות הרשימה בתוקף, אינו פותר את הצד המסתמך מלודא שהרשימה היא העדכנית ביותר).

4.9.8 זמינות בדיקה מקוונת של תוקף תעודה

שרתי הפרסום של תעודות מבטלות יהיו זמינים לבדיקה מקוונת של תוקף תעודה של מי שזכאי להיות צד מסתמך עליהן, במידת האפשר בכל עת. על-פי הנחיות הרשם, על פרסונל איי.די. להיות זמינה לבדיקת תוקף תעודה ב-99% משעות היממה.

4.9.9 דרישות מקדימות לבדיקה מקוונת של תוקף תעודה

לצורך בדיקה מקוונת של תוקף התעודה, הצד המסתמך נדרש להיות בעל גישה לשרתי פרסום רשימת התעודות הבטלות באמצעות תקשורת נתונים, דרך רשת האינטרנט או דרך רשת ייעודית שהוקמה לצורך העניין.

4.9.10 צורות אחרות של פרסום תוקף תעודה

פרסונל איי.די. מאפשרת לצדדים מסתמכים לקבל אליהם באופן מקוון ומיידי עותק עדכני של רשימת התעודות הבטלות ו/או רשימת התעודות התקפות, לשימוש פנימי. יכולת בדיקה מרוכזת זו של תוקף תעודות מחייב התקשרות מקדימה עם פרסונל איי.די..

פרסונל איי.די. רשאית להנפיק, לשימוש של גוף המעוניין בכך, על-פי דרישה ולאחר התקשרות מקדימה, רשימת תעודות בטלות חלקית (Partial CRL) המכילה מידע על קבוצה מוגדרת של תעודות בטלות, כגון תעודות שהונפקו עבור מערכת מסוימת או לקוח מסויים.

פרסום באופן השונה מהקבוע בתקנה 15(ג) לתקנות ניהול גורם מאשר מותנה באישור מראש ובכתב של הרשם, ואם ייעשה יצוין אופן הפרסום באתר האינטרנט של פרסונל איי.די. ובתעודות הרלוונטיות, כנדרש בחוק.

4.9.11 דרישות מיוחדות בעת חשיפת מפתח פרטי של תעודה

למעט הכנסת תעודה לרשימת תעודות בטלות ופרסומה על פי מסמך נהלים זה, וזאת בסמוך לאחר קבלת הודעה מבעל תעודה כי נשללה שליטתו במפתח החתימה הפרטי, אין על פרסונל איי.די. חובה נוספת לפעול.

4.9.12 נסיבות להתליית תעודה

התליית תוקף תעודה על-פי מסמך נהלים זה יכולה להיעשות:

❑ בעקבות בקשה לביטול התעודה, במקרים בהם מתעורר חשד שמבקש הביטול אינו מוסמך לעשות זאת.

❑ לבקשת בעל התעודה.

4.9.13 זהות הרשאי לבקש התליית תוקף תעודה

אם הוסכם על כך בהסכם ההתקשרות עם בעל התעודה, רשאי בעל התעודה לבקש את התלייתה.

4.9.14 תהליך התליית תוקף תעודה

בהתקיים אחת הנסיבות המפורטות בסעיף 4.9.12, מנהל הגורם המאשר, או מי שהוסמך על ידו יורה על התליית התעודה.

4.9.15 מגבלות על התליית תוקף תעודה

תהליך ההתלייה לא יהיה בשליטתו של אדם אחד.

4.10 שירותים לבדיקת סטטוס תעודה

4.10.1 מאפיינים תפעוליים

בדיקת סטטוס תעודה אלקטרונית תהיה אפשרית באמצעים המצויינים בסעיפים 4.9.6 עד 4.9.10.

4.10.2 זמינות השירות

השירות לבדיקת סטטוס תעודה יהיה זמין במשך 24 שעות ביממה, 7 ימים בשבוע (24X7). הפרסום יתבצע באמצעות מספר שרתים וספקי אינטרנט שונים להבטחת זמינות גבוהה של רשימת התעודות המבוטלות.

4.10.3 שירותים נוספים

פרסונל איי.די. רשאית להציע שירותים נוספים לבדיקת תוקף תעודות, כגון שירותי OCSP.

4.11 פקיעת תוקף התעודה

תוקף התעודה יפוג באחד משני המקרים הבאים :

- סיום מועד תוקף התעודה, כפי שנרשם בתעודה במועד הנפקתה.
- התעודה בוטלה בהתאם לסעיף 4.9.

4.12 הפקדת מפתח בידי צד ג' ואחזור

עבור תעודות המונפקות על-פי מסמך זה לא יינתנו שירותים של גיבוי המפתח הפרטי ולא תהיה אפשרות לאחזור מפתח זה.

5. אמצעי אבטחה פיסיים, נוהלי אבטחת מידע, ותפעול

5.1 אמצעים פיזיים

5.1.1 מיקום ומבנה האתר

תשתיות החיתום וההנפקה של הגורם המאשר ומערכות הניהול של מערך הגורם המאשר ממוקמים פיזית באתר מאובטח, מוגן ומנוטר באמצעי אבטחת מתקדמים ובמספק שכבות הגנה, הכוללות אמצעי בקרת גישה, ניטור וטלוויזיה במעגל סגור.

5.1.2 כניסה פיזית לאתר המאובטח

הכניסה לאתר המאובטח מוגנת במספר מעגלי אבטחה פיזית. גישה לאזורים קריטיים מחייבת זיהוי של שני אנשים מורשים לפחות, המזדהים באמצעי זיהוי חזקים (כגון זיהוי ביומטרי).

פרסונל איי.די. הוסמכה לתקן ישראלי 27001, "טכנולוגית מידע: טכניקות אבטחה - מערכות לניהול אבטחת מידע - דרישות". בהתאם לכך פרסונל איי.די. מנטרת באופן שוטף סיכונים לפעילותה ויש לה תהליכים ונהלים להתמודדות עם סיכונים אלה ובכלל זה מנגנוני אבטחה פיזית.

מערך הכניסה ובקרת הכניסה לאתר המאובטח פועל בהתאם לתקן 27001 ואושר על-ידי הרשם במסגרת רישום פרסונל איי.די. על-פי החוק.

5.1.3 אספקת חשמל ומיזוג אוויר לאתרי פרסונל איי.די.

האתר המאובטח מקבל מתח חשמל ממערכת UPS בעלת מצברים פנימיים אשר ניוזנה מרשת החשמל הארצית. מערכת ה-UPS מספקת הגנה מפני שינויים פתאומיים במתח ומספקת מתח לתשתית המחשוב באתר המאובטח במקרה של הפסקת חשמל ממושכת.

באתר מותקנות שתי מערכות מיזוג אוויר נפרדות אשר מגבות האחת את השנייה ומותקן חיפון לזיהוי והתראה על טמפרטורת קיצוניות (חום וקור).

5.1.4 חשיפה למים

כדי למזער את החשיפה לנזקי מים, לא קיימת אספקת מים באתר המאובטח מערכת כיבוי האש באתר מבוססת על פיזור גז לכיבוי שרפות.

5.1.5 מערכות כיבוי אש והגנה מאש

מערך הגילוי באתר מבוסס על מערכות דגימה. במקרה של גילוי שריפה, מופעלת מערכת כיבוי בגז.

5.1.6 אחסנת מצעים

כל מצע (Storage Media), אלקטרוני ואו ופיסי, המכיל מידע שיש להגן אל הגישה אליו, מאוחסן באתר שמור בתוך פרסונל איי.די.. על המידע מיושמים אמצעים פיסיים ולוגיים אשר מונעים שימוש בלתי מורשה בו.

5.1.7 פינוי אשפה

כל המצעים, אלקטרוניים ופיסיים, המכילים מידע החייב במניעת נגישות ללא מורשים מפונה מאתרי פרסונל איי.די. בהתאם לנוהל מוגדר המבטיח כי מידע הדורש חיסיון יושמד.

5.1.8 גיבוי מחוץ לאתר

פרסונל איי.די. מגבה מידע קריטי עבורה, כגון מפתחות פרטיים שלה, רשומות, בסיסי נתונים וכד' גם באתר מרוחק בנוסף לגיבוי מקומי. הגיבוי המרוחק מאוחסן באמצעי אחסנה מאובטחים והולמים, תוך יישום שיטות למזעור הסיכון הנובע מגיבויים כאמור. רמת ההגנה על מידע קריטי באתר גיבוי היא באותה הגנה הקיימת באתר המרכזי.

5.2 אמצעים נוהליים

5.2.1 תפקידי אמון

תפקיד במערך פרסונל איי.די. מוגדר כתפקיד אמון אם יש באפשרות האדם המבצע את התפקיד לבצע את הפעולות הבאות:

- ☐ הזנה ואימות מידע של בקשה להנפקת תעודה
- ☐ הזנה ואימות מידע של בקשה לביטול, התליה או חידוש של תעודה
- ☐ הרשאת כניסה לאזורים מוגבלים בכניסה בגורם המאשר, או מתן אישור לאחר להיכנס
- ☐ הגדרה של ישויות במערך פרסונל איי.די.

המשמעות של הגדרת אדם כנושא תפקיד אמון היא יישום של מערך בקרה ואישוש מידע בתהליך הגיוס, ההכשרה והפעילות השוטפת של העובד בתפקידו בגורם המאשר של פרסונל איי.די..

תפקידים הפרדת תפקידים לפחות בתפקידים הבאים:

- ☐ אחראי אבטחת מידע
- ☐ נציג רישום
- ☐ מנהל מערכות מידע
- ☐ אחראי גיבויים

בכל מקרה לא ישמש בעל תפקיד אמון ביותר מאחד התפקידים הבאים: מנהל אבטחה, פקיד רישום, אדימיניסטרטור, מפעיל מערכת או מבקר.

5.2.1.1 תפקידי אמון בפרסונל איי.די.

התפקידים הבאים מוגדרים כתפקידי אמון, ומילויים מחייב יישום של נוהלי גיוס כ"א ווידוא כשירות כאמור:

- מנכ"ל פרסונל איי.די.
- אחראי (אחראי אבטחת המידע)
- אחראי הסיסטם
- מנהל מערכות מידע
- אחראי משמרת
- תורן משמרת
- נציג רישום
- אחראי גיבויים

אפשר שתפקידים נוספים יוגדרו כתפקידי אמון.

5.2.1.2 הפרדת תפקידים

תפקידים הפרדת תפקידים לפחות בתפקידים הבאים:

- אחראי האבטחה
- נציג רישום
- מנהל מערכות מידע
- אחראי גיבויים

בכל מקרה לא יישמש בעל תפקיד אמון ביותר מאחד התפקידים הבאים: מנהל אבטחה, פקיד רישום, אדימניסטרטור, מפעיל מערכת או מבקר.

5.2.2 משימות המחייבות יותר מאדם אחד לביצוען

לביצוע משימות קריטיות או רגישות בגורם המאשר של פרסונל איי.די. נדרשת נוכחותם של, לכל הפחות, שני אנשים מורשים בעת ביצוע הפעולה, וזאת בין היתר בהתאם להוראות סעיפים 5 ו-7 לתקנות חומרה ותוכנה. טרם ביצוע הפעולה, כל מורשה מזוהה על סמך שני אמצעי זיהוי לפחות מבין האמצעים הבאים: אחזקה בכרטיס חכם, ידיעת סיסמא ייחודית והזדהות ביומטרית.

בין היתר, נדרשים שני אנשים או יותר לביצוע הפעולות הבאות:

□ זיהוי מבקש תעודה, הנפקה, ביטול או התלייה של תעודה אלקטרונית שהונפקה לפי מסמך נהלים זה (להלן פעולות חיוניות).

□ הגדרה, או שינוי הגדרה, של ישות במערך פרסונל איי.די., לרבות שינוי בהרשאות הנוגעות לפעולות חיוניות

□ ביטול או התליה של תעודה לגורם במערך התפעולי של פרסונל איי.די.

□ חתימה אלקטרונית של תעודת שרת הנפקה, או של ישות אחרת במערך פרסונל איי.די.

□ זיהוי או מסירה של תעודה שהונפקה לפי מסמך זה

בכל מקרה לא יישמש בעל תפקיד אמון ביותר מאחד התפקידים הבאים: מנהל אבטחה, פקיד רישום, אדימניסטרטור, מפעיל מערכת או מבקר.

5.2.3 תהליכי אימות הזהות הנדרש לביצוע משימה

לצורך אימות זהותו של מי שמבצע פעולה הדורשת הרשאה מיוחדת, מיושמים במערך פרסונל איי.די. אמצעי אימות זהות הבאים, כולם או חלקם – וזאת לפי הצורך והעניין:

אמצעים ביומטריים, כגון מערכת זיהוי מבנה כף היד, טביעת אצבע וכד'.

אמצעים פיזיים כגון כרטיסים חכמים.

מידע להפעלה ייחודי הנמצא בחזקת מורשה הפעולה בלבד.

בכל פעולה הדורשת אימות זהות כאמור לעיל, יתבצע האימות באמצעות שניים לפחות מהאמצעים המפורטים לעיל.

5.2.4 הפרדת תפקידים

תתקיים הפרדת תפקידים לפחות בתפקידים הבאים:

□ אחראי אבטחת מידע

□ נציג רישום

□ מנהל מערכות מידע

□ אחראי גיבויים

ובנוסף – ביצוען של המשימות שלהלן מחייבים את מעורבותם ונוכחותם של שני בעלי תפקידי אמון שונים בכל שלבי הביצוע:

□ ייצור של מפתחות פרטיים של שרת הנפקה

□ גיבוי ואחזור של מפתחות פרטיים המשמשים שרתי הנפקה של פרסונל איי.די. לחתימה אלקטרונית של תעודות אלקטרוניות

□ הוספה או הסרה של יישומים בשרתי הנפקה וניהול מערך פרסונל איי.די.

בכל מקרה לא יישמש בעל תפקיד אמון ביותר מאחד התפקידים הבאים: מנהל אבטחה, פקיד רישום, אדימניסטרטור, מפעיל מערכת או מבקר.

5.3 בקרת עובדים

5.3.1 בדיקת כשירות והתאמה לתפקיד

כל עובד בפרסונל איי.די. עובר תהליכי מיון, המוודאים את התאמתו וכשירותו לתפקיד. מי שנושא בתפקיד אמון, עובר תהליכי בדיקה נוספים לוידוא התאמה לתפקיד. בין היתר, נבדקים הרישום הפלילי שלו, הרקע המקצועי, התאמת האישיות לתפקיד וכד'. הליכים אלה נבדקו על-ידי הרשם כחלק מרישום פרסונל איי.די. כגורם מאשר על-פי החוק.

5.3.2 תהליכי אימות פרטי עובדים

בטרם קבלתם של עובדים בתפקידי אמון נערכות לפחות הפעולות הבאות:

- נערכים שני ראיונות עבודה לפחות, (לפחות אחד מהם עם גורם בכיר)
- מתבצעת שיחת רקע עם ממליץ
- נבדקת תעודת יושר ממשטרת ישראל - בהתאם לחוק המרשם הפלילי ועל פי הסייגים הקבועים בו
- מבוצעים בדיקות מהימנות

5.3.3 דרישות הדרכה

עבודה במערך פרסונל איי.די. מותנית במעבר מבחן מקצועי המוודא את ידיעתו של העובד את הנושאים המהותיים לתפקודו בגורם המאשר.

5.3.4 תדירות עדכון ידע מקצועי

מתבצעת הדרכה תלת-חודשית בנושאים הקשורים לעבודתו הספציפית של העובד במערך.

5.3.5 סבב תפקידים

החברה רשאית לבצע סבב תפקידים בין העובדים בחברה. זכות זה כפופה לביצוע בדיקות כשירות, התאמה לתפקיד והכשרה כנדרש על פי מסמך המדיניות ובכפוף לכך שמעבר כאמור לא יסכן את עיקרון הפרדת התפקידים שתואר בסעיף 5.2.1 לעיל. עם סיום העסקה יבוטלו הרשאות עובד במערכת ויוחלפו הסמאות שלו.

5.3.6 אמצעים משמעתיים עקב חריגה מנהלים

בגורם המאשר מיושמת מערכת משמעתית קפדנית המטפלת בחריגות מהוראות נוהלי עבודה של פרסונל איי.די.. הסנקציות הננקטות כלפי מפירי משמעת היא יחסית למהות החריגה, ועשויה להגיע עד כדי פיטורין.

5.3.7 דרישות מקבלנים

קבלנים המספקים שירותים מהותיים לגורם המאשר, חתומים על חוזים המסדירים נושאים כגון שמירה על פרטיות, קניין רוחני, מידע סודי של פרסונל איי.די. ולקוחותיו וכד' – ככל שאינם מחויבים בכך מכוח הוראות הדין החלות עליהם ובהתאם לנוהלי החברה לעניין התקשרות עם צד שלישי. ביקורת על הנושאים הללו מתבצעת באופן תקופתי על ידי גורמי הביקורת בגורם המאשר בהתאם לנוהלי הביקורת של הגורם ותקני הבטחת איכות ואבטחת מידע בהם עומד הגורם המאשר.

5.3.8 מסמכים המסופקים לעובדים

המסמכים הנמסרים לעובדים עם תחילת עבודתם בגורם המאשר הינם:

- התחייבות לשמירת סודיות
- הוראות אבטחת מידע ובטחון
- כל הנהלים הרלוונטיים לעבודתם בגורם המאשר

5.4 נוהלי בקרת אירועי אבטחת מידע

פרסונל איי.די. מחזיקה אמצעי רישום וגיבוי של מידע הנוגע לפעילותה.

5.4.1 סוגי אירועים שנרשמים

פרסונל איי.די. מתעדת בקבצי דיווח את האירועים הבאים כחלק מתהליך העבודה השגרתי של פעולתה כגורם מאשר:

- שינויים בתצורה של מערכות המידע של פרסונל איי.די..
- אירועי אבטחת מידע שזוהו על-ידי מערך פרסונל איי.די..
- זהות הנכנסים לאזורים מאובטחים של פרסונל איי.די..
- זהות המבצעים כניסה לוגית למערכות ההפעלה של רכיבי פרסונל איי.די..
- פעולות הקשורות במחזור החיים של התעודות המונפקות לפי מסמך נהלים זה.

5.4.2 תדירות ייצור ובדיקה של קבצי דיווח

קבצי דיווח מתעדכנים באופן מיידי בסמוך לאירוע אותו הם מתעדים.

קבצי הדיווח נבדקים באופן ידני ובאופן אוטומאטי באמצעות מערכת בקרה, בתדירות שנקבעה בנהלי אבטחת המידע.

5.4.3 תקופת שמירה של קבצי דיווח

קבצי דיווח נשמרים לתקופה של חצי שנה בפורמט זמין מיידי. לאחר מכן, הם מועברים לארכיון לתקופות הקבועות בתקנות ניהול גורם מאשר והנחיות הרשם למשך 12 חודשים נוספים. בנוסף, קבצי דיווח לא יימחקו בטרם קבלת אישור הרשם שעשוי להורות על שמירה לתקופה ארוכה יותר.

5.4.4 הגנה על קבצי דיווח

בעת קיומם בפורמט אלקטרוני, קבצי הדיווח מוגנים במסגרת ההגנה הכללית על מערכות פרסונל איי.די.. לאחר העברתם למדיום גיבוי, הם מוגנים באמצעי אחסנה שמורים המונעים גישה בלתי מורשית אליהם (כלומר מי שלא קיבל הרשאת קצין בטחון).

5.4.5 תהליכי גיבוי של קבצי דיווח

קבצי דיווח מגובים באופן שגרתי באופן יומי, שבועי וחודשי. עותקים של אמצעי הגיבוי מאוחסנים באופן מאובטח בכספות.

5.4.6 מערכת איסוף דיווחים

בגורם המאשר מיושמת מערכת מידע המרכזת את המידע מהמערכות השונות המשמשות לתפעול פרסונל איי.די. וניהולו. מערכת זו מציגה ושומרת את המידע באופן מרוכז לצורך מעקב שוטף ואפשרות תחקור אירועים.

5.4.7 מנגנוני הודעה על אירועי אבטחה

בגורם המאשר מיושמת מערכת בקרה המדווחת באופן אוטומטי על אירועי אבטחה מסוגים מסוימים. בנוסף, קיימים נוהלי עבודה מוגדרים לטיפול באירועי אבטחה מסוגים מסוימים ובכלל זה דיווח מיד לרשם.

5.4.8 הערכת פגיעות מערכות

הכנת פרסונל איי.די. לת"י 27001 כללה סקר סיכונים מפורט לכל מערכות פרסונל איי.די.. סקר זה מתבצע אחת לשנה, על ידי גורם מומחה בלתי תלוי בהתאם למתודולוגיה מוכרת במסגרת הביקורת התקופתית לעמידה בהוראות התקן והנחיות הרשם.

5.5 ארכיבאות רשומות

מטרת הארכיבאות היא לשמר את התיעוד המעיד על פעולותיה של פרסונל איי.די. כ"גורם מאשר" וגוף אמון לרבות לצורך הגשת תעודות גורם מאשר, כמשמעותן בסעיף 5 לחוק.

5.5.1 סוגי רשומות

בתהליך הטיפול בתעודה, פרסונל איי.די. מייצרת רשומות בפורמט אלקטרוני או פיסי לכל אירוע מהותי המתרחש בגורם המאשר. בין היתר, מופקות הרשומות הבאות:

- פרטי הבקשה להנפקת תעודה של מבקש תעודה
- העתק ממסמכי הזיהוי של מבקש תעודה
- אזהרות שהוזהרו מי שמבקש לקבל תעודה
- מידע לאימות הזהות של בעל תעודה בעת בקשה לביטולה
- מחזור החיים של התעודה – הנפקה, ביטול, פקיעה וחידוש של תעודות. מתועדים גם נסיונות שלא צלחו לבקשות להנפקת תעודה, כגון הגשת בקשה לא מלאה.
- קבצי דיווח, כמפורט בסעיף 5.4.1 לעיל

5.5.2 תקופת שמירה של רשומות

רשומות שתקופת שמירתן נקבעה בחוק, התקנות או בהוראות הרשם, נשמרות לתקופות שנקבעו:

- העתקי המסמכים על-פי הם זוהה מקבל התעודה נשמרים למשך הזמן הנקוב בתקנה 11 לתקנות תוכנה וחומרה (שמירת מסמכי זיהוי) – 15 שנה מיום הנפקת התעודה האחרונה שהונפקה על בסיס מסמכי זיהוי אלה.
- מסמכים ומידע שקיבל הגורם המאשר לפי תקנות ניהול גורם מאשר ישמרו למשך 25 שנים לפחות.
- קבצי דיווח – כמפורט בסעיף 5.4.3.

רשומות שאינן חייבות בשמירה על-פי החוק, נשמרות לפרק הזמן בו יידרשו, בהתאם לנוהלים הפנימיים של פרסונל איי.די.. הנהלים קובעים כי רשומות העשויות לשמש בהליכים אזרחיים, נשמרות לתקופה של שבע שנים לפחות.

5.5.3 הגנה על רשומות בארכיב

רשומות בארכיב יהיו מוגנות בפני גישה לשינוי או מחיקה של בלתי מורשים, ומפני נזקי זמן, שריפה ורטיבות. לצידן של רשומות בפורמט דיגיטליות ישמרו הכלים הדרושים לצפייה במידע, במקרים של שינויים טכנולוגיים תתבצע המרה של הנתונים באופן שתשמר היכולת לצפות במידע (כגון שינויים בפורמט הקבצים, מדיה וכד').

5.5.4 תהליכי גיבוי של מערכות ארכיבאות

רשומות אלקטרוניות מגובות באופן שגרתי באופן יומי, שבועי וחודשי. עותקים של אמצעי הגיבוי מאוחסנים באופן מאובטח בכספות מחוץ למתחם פרסונל איי.די..

חלק מהרשומות בפורמט נייר נסרקות למערכת ארכיבאות אלקטרונית, ולאחר מכן מטופלות כרשומות אלקטרוניות.

5.5.5 חותמת זמן על רשומות

עבור רשומות בפורמט אלקטרוני, תוצמד לכל רשומה חותמת זמן אשר מוטבעת מתוך המערכת המייצרת את הרשומה בעת יצירתה. למערכת מקור זמן אמין המשקף את שעון גריניץ' (GMT) ומאמץ את מוסכמות הזמן האוניברסאליות (UTC). עבור רשומות בפורמט פיסי, ירשם באופן ידני תאריך קבלת המסמך ע"י הנציג התפעולי המתאים לצד שם הנציג.

5.5.6 שמירת תוקף משפטי של מידע

פרסונל איי.די. מיישמת נוהל המיועד להבטיח שלרשומותיה, הנוגעות לתעודות אלקטרוניות, יהיה תוקף משפטי מחייב.

תקינותן של הרשומות נבדקת בעת ארכובן ובאופן תקופתי במסגרת ביקורת ת"י 27001.

אחזורה של רשומה ספציפית אינו מידי, אך ניתן לאחזר רשומות לצורך הצגתה בהליך משפטי.

5.5.7 אחזור רשומות מארכיון

אחזור רשומות מארכיון יתבצע בהתאם לצורך, באופן הבא:

- למטרות תפעוליות לניהול מחזור החיים של תעודה או תעודות שהונפקו על ידי הגורם המאשר – יתבצע ע"י נציגי רישום.
- למטרות ביקורת על ידי גוף מבקר – יתבצע ע"י מנהל הגורם המאשר, או מנהל אבטחת המידע של הגורם המאשר.
- בכל מקרה אחר – אחזור רשומות מהארכיון יתבצע באישור מנהל הגורם המאשר בלבד.

5.6 החלפת מפתחות חתימה אלקטרונית

פקיעת תעודה של שרת הנפקה מחייבת החלפת מפתחות החתימה האלקטרונית של אותו שרת, וגוררת את ביטולן של כל התעודות שהונפקו על ידו.

החלפת מפתחות לחתימה אלקטרונית של שרת הנפקה מתבצעת בתהליך מתועד בנוכחות גורמי ביקורת חיצוניים (עו"ד, רו"ח, מומחה אבטחת מידע).

למרות האמור לעיל, פרסונל איי.די. רשאית, אך לא חייבת, לחדש תעודה של שרת הנפקה ללא החלפת צמד המפתחות שלו לתקופה נוספת בכפוף לסעיף 6.3.2 למסמך נהלים זה.

פקיעת תעודה המונפקת על פי מסמך נהלים זה מחייבת החלפת צמד מפתחות החתימה, והנפקת תעודה חדשה. פרסונל איי.די. רשאית, אך לא חייבת, לחדש תעודה שהונפקה על-פי מסמך נהלים זה ללא החלפת צמד המפתחות, בכפוף לקבוע בסעיף 6.3.2 למסמך נהלים זה. חידוש תעודה יעשה על-פי הנוהל המפורט בסעיף 4.3.

5.7 הערכות לאסון

5.7.1 טיפול באירועי DRP

במערך פרסונל איי.די. קיימת תוכנית המשכיות עסקית למקרה אסון (DRP) שאושרה במסגרת קבלת ת"י 27001. תפישת הפעולה של פרסונל איי.די. מיועדת בראש ובראשונה למזער למינימום האפשרי את האפשרות שיתרחש אירוע המשכיות עסקית. תפיסה זו מיושמת באמצעים שיושמו בעת בניית מערך פרסונל איי.די.. תוכנית ההמשכיות העסקית מטפלת במקרה בו על אף האמצעים שנקטו נפגע השירות שנותן פרסונל איי.די. באופן מהותי.

תוכנית ההערכות לאסון מטפלת ונותנת פתרונות למקרים הבאים וזאת מבלי לפגוע ברמת אבטחת המידע של המערכת:

- מפתח פרטי של שרת הנפקה ראשי או תפעולי נחשף
- משאבי מחשוב, תוכנה, תקשורת ו/או מידע נפגעו באופן המשבית את פעולת הגורם המאשר
- אתר מאובטח נפגע כתוצאה מאסון טבע, אירוע מלחמתי או אירוע אסון אחר
- התגלתה הונאה של מערך הזיהוי של פרסונל איי.די.
- התגלה כשל מהותי בטכנולוגיה עליה מבוסס מערך פרסונל איי.די.

התוכנית מזהה את השפעות התממשות המקרים המתוארים לעיל על שירות פרסונל איי.די., קובעת את התהליכים המפורטים שייעשו במקרה התממשותם ואת אמצעי הבקרה והתרגול שנועדו לשימור האפקטיביות שלה. בהתאם לתוכנית מסוגלת פרסונל איי.די. לקיים את תקנות 3 עד 5 לתקנות חתימה אלקטרונית גם בעת אירוע המפורט בסעיף זה.

5.7.2 שיבוש במשאבי מחשוב, תוכנה ומידע

ככלל, במקרה של תקלה בזמינות המידע החיוני לפעולת הגורם המאשר עקב שיבוש במשאבי מחשב, תתבצע פעילות שעיקרה החזרת מערכות המידע לתקינות בסביבה התפעולית הראשית. על פי שיקול דעתו של מנהל הגורם המאשר, ובהסתמך על חוות הדעת של הגורמים הטכניים תישקל הפעלת תוכנית ה-DRP כאמור בסעיף 5.7.1.

5.7.3 חשיפה של מפתח פרטי של ישות במערך הגורם המאשר

במקרה שבו יאומת חשד לחשיפה של מפתח פרטי של ישות במערך הגורם המאשר, ינקטו הפעולות הבאות:

- ביטול מיידי של התעודה אשר מהימנותה נפגעה עקב חשיפת המפתח הפרטי.
 - הפעלת נוהל "אירוע אבטחת מידע" כמפורט בנהלי התפעול של הגורם המאשר.
 - הודעה לרשם.
 - ביטול כל התעודות האלקטרוניות אשר קיים חשד לפגיעה במהימנותן בעקבות החשיפה תוך תאום עם הרשם, הודעה לבעלי התעודות על הביטול ופרסום רשימת תעודות מבוטלות עדכנית בהתאם. הנפקת תעודות חדשות שתוקפן יהיה עד למועד הפקיעה של התעודות שבוטלו, ללא תשלום, ומסירת הודעה לבעלי התעודות על כך.
 - יישקל פרסום בערוצי פרסום ציבוריים במידת הצורך.
- הוראות סעיף זה יחולו, בשינויים המחויבים לפי העניין, גם במקרה שבו תפגע שליטתו של נציג רישום באמצעי החתימה שלו ובכלל זה אם יאומת חשד לחשיפת המפתח הפרטי של נציג הרישום.

5.7.3.1 חשיפה של מפתח פרטי של שרת חיתום במערך הגורם המאשר

במקרה שבו תפגע שליטתה של פרסונל איי.די. באמצעי החתימה של שרת חיתום, ינקטו בנוסף לעיל הפעולות הבאות:

- פרסום דבר הפגיעה באתר האינטרנט באופן מובלט למשך 30 יום לפחות או לתקופה ארוכה יותר כפי שיוורה הרשם.
- מתן הודעה לציבור על הפסקת הפעילות והשלכותיה בשני עיתונים יומיים לפחות.

5.7.4 המשכיות עסקית לאחר מקרה אסון

תוכנית ה-DRP של החברה למקרה אסון, מטפלת בהפעלת היכולות הנדרשות באתר חלופי, בין היתר בכל הדרוש למימוש של תהליכים מהותיים ושימור היכולת התפעולית של הגורם המאשר ובפרט תהליכים הקשורים בהפקה ובפרסום רשימות תעודות בטלות.

5.8 הפסקת פעילות גורם מאשר או מערך רישום

5.8.1 הפסקת פעילות גורם מאשר

הפסקת פעילות כגורם מאשר המנפיק תעודות אלקטרוניות מאושרות מוסדרת בסעיף 14 לחוק ובתקנה 18 לתקנות ניהול גורם מאשר.

במקרה בו תפורק פרסונל איי.די., או שיחליטו בעלי מניותיה על התפרקותה מרצון, או על הפסקת הפעילות של הגורם המאשר, או שהרשם יבטל את הרישיון שניתן לחברה להיות גורם מאשר, מתחייבת פרסונל איי.די.:

- במקרה של החלטת פרסונל איי.די. על פירוק או הפסקת פעילות: להודיע לרשם על כוונת החברה בעניין;
- להימנע מלהנפיק תעודות אלקטרוניות מאושרות;
- לבטל את כל התעודות האלקטרוניות המאשרות התקפות שהנפיקה לאחר תיאום ואישור של הרשם, ולהודיע על כך מיד לבעליהן, ולהכניסן לרשימת התעודות הבטלות;

- להעביר לידי הרשם את אמצעי החתימה ואמצעי אימות החתימה שלה, באופן שיוכל למלא את חובותיה של פרסונל איי.די. בהתאם לסעיף 5 לחוק, וכן העתק מדויק של מאגרי התעודות האלקטרוניות המאושרות שהנפיקה, ומאגר התעודות הבטלות, בתוך 72 שעות ממועד הפסקת פעילות או ממועד מחיקת הרישום, לפי הענין;
- להודיע לרשות ני"ע, בהתאם לתקנות ניירות ערך;
- להעביר לידי הרשם העתק מדויק של כל המסמכים שקיבלה לצורך הנפקת תעודות אלקטרוניות מאושרות, בתוך 7 ימים ממועד הפסקת הפעילות או מחיקת הרישום, לפי הענין, באופן שהרשם יוכל למלא את חובותיה של פרסונל איי.די. בהתאם לסעיף 5 לחוק, להנחת דעתו;
- כל עוד לא קיבלה פרסונל איי.די. הודעה מאת הרשם בדבר הכוונה למחקה מן המרשם, רשאית פרסונל איי.די. להעביר את ניהולה לידי גורם מאשר אחר הרשום במרשם ("גורם מאשר מחליף") באישור הרשם.
- אם הפסיקה פרסונל איי.די. את פעילותה כאמור, חובה עליה להודיע על כך מיד לכל מי שהיא הנפיקה לו תעודה התקפה בעת הפסקת הפעילות. הודעות כאמור יימסרו בדואר אלקטרוני ומתן הודעה לציבור על הפסקת הפעילות והשלכותיה בשני עיתונים יומיים לפחות..
- הגורם המאשר המחליף ימלא את כל זכויותיה וחובותיה של פרסונל איי.די. מהמועד שהוסכם בין הצדדים ואושר ע"י הרשם.

5.8.2 הפסקת פעילות מערך רישום

הפסקת פעילותה של מערך רישום תתבצע כתוצאה מאחד או יותר מהמקרים להלן:

- החלטה עסקית של מערך הרישום ו/או הגורם המאשר
 - אי עמידה בתנאי הרישיון שקיבל מערך הרישום מהגורם המאשר
 - הנחיית רשם גורמים מאשרים
- עם הפסקת פעילותה של מערך רישום ינקטו הפעולות הבאות:
- יחדל מערך הרישום מביצוע של פעולות זיהוי, הנפקה וניהול של תעודות אלקטרוניות מאושרות
 - ביטול האמצעים הדיגיטאליים ואמצעי ההתקשרות אל מול מערכות הגורם המאשר
 - יוחזרו אמצעי זיהוי וכל אמצעי אחר אשר הונפק ע"י הגורם המאשר ונמסר למערך הרישום ומי מטעמו
 - יועברו לידי הגורם המאשר כל מסמך או תיעוד לגבי אימות זהויות אשר בוצעו על ידי הגורם רושם

6. אמצעי בקרה טכנולוגיים לאבטחת מידע

6.1 ייצור צמד מפתחות והתקנתם

6.1.1 ייצור צמד מפתחות

צמדי מפתחות של שרתי ההנפקה במערכת פרסונל איי.די. מופקים באמצעי חומרה קריפטוגרפיים (HSM) המייצרים את המפתחות בעצמם. המפתח הפרטי אינו עוזב את רכיב החומרה, גם בעת שימוש בו.

ייצור צמדי מפתחות של בעל תעודה יתבצע בנוכחות פקיד הרישום על גבי חומרה מהימנה כנדרש מכח החוק, התקנות ומהנחיות הרשם, או בתהליך שאושר ע"י הרשם.

כנדרש בתקנה 13 לתקנות ניהול גורם מאשר, פרסונל איי.די. לא תקבל לידיה ולא תחזיק פרסונל איי.די. אצלה עותק מצמד מפתחות לחתימה אלקטרונית של בעל תעודה, או כל מידע המאפשר שחזור או יצירה של צמד מפתחות עבור או במקום בעל התעודה.

6.1.2 העברת מפתח ציבורי של פרסונל איי.די. לבעלי תעודות ומסתמכים

המפתחות הציבוריים של כל נתיב האישור של פרסונל איי.די. (שרת ה-RCA ושרת ה-OCA) נמצאים בתעודות שרתי ה-RCA וה-OCA, ובכל תעודה.

פרסונל איי.די. מאפשרת להוריד מכתובת מזהה בתעודה אלקטרונית (בשדה AIA) ובאתר האינטרנט שלה את התעודות לשרתי ה-RCA וה-OCA לכל מי שמעוניין להסתמך על תעודות שהנפיקה, בכתובת:

www.personalid.co.il/repository/certificates

הצד המסתמך רשאי להתקין את תעודות שרתי ה-OCA וה-RCA בכל יישום האמור להשתמש בה לשם זיהוי פרסונל איי.די., כגון ברשימת האמון (Trust list) בדפדפן.

6.1.3 אורכי מפתחות

המפתחות המשמשים את יחידות פרסונל איי.די. להזדהות, חתימה אלקטרונית והצפנה במסגרת מערך פרסונל איי.די., הם מפתחות RSA באורך מינימלי של 2048 סיביות.

אורך המפתח המינימלי לחתימה אלקטרונית המלווה בתעודה מאושרת נקבעים בתקנה 8 לתקנות חומרה ותוכנה ובהנחיות הרשם. לאלגוריתם חתימה מסוג RSA, אורך המפתח המינימלי המותר הוא 2048 סיביות. לאלגוריתם מסוג ECDSA (Elliptic Curve DSA) אורך המפתח המינימלי המותר הוא 224 סיביות.

6.1.4 מאפייני חילול מפתחות

אין דרישות מיוחדות.

6.1.5 ביקורת איכות של תכונות תעודה

טקס יצירת התעודה המזהה את פרסונל איי.די. ושרתי ההנפקה השונים נעשה על-פי נוהל ספציפי (Key Ceremony) והוא מפקח על-ידי גורמים חיצוניים כגון מבקר מערכות מידע, מומחה אבטחת מידע, ר"ח ואו עו"ד.

היישום המשמש לניהול מערך פרסונל איי.די. כופה תהליך איכות, וביקורת שלה, לגבי היבטים מסוימים של תכונות התעודה, כגון פרטי המידע שחייבים להיות ממולאים, אורך מפתח מותר על-פי מסמך נהלים זה וכד'. בנוסף, נוהלי הנפקת התעודות מחייבים את נציגי הרישום, בכפוף למדיניות הנפקה ספציפית, לוודא כי המידע בתעודה תואם את מסמך הנהלים ואת פרטי בעל התעודה.

איכות התעודה והתאמתה למסמך הנהלים נבדקים באופן אוטומטי על-ידי תוכנת ניהול מערך PKI.

6.2 הגנת מפתח פרטי

6.2.1 תקנים לאמצעי אחסנה קריפטוגרפיים

שרת ה-Root-CA ושרת ה-OCA- מבוססים על אמצעי ייצור, אחסנה וחתימה קריפטוגרפי (HSM) העומד בתקן FIPS 140-2 level 3. שאר אמצעי האחסנה של מפתחות הפרטיים במערך פרסונל איי.די. עומדים בתקן FIPS 140-2 level 2 או דומה לו.

6.2.2 דרישה לביצוע פעולה על ידי יותר מאדם אחד לצורך הפעלת מפתח פרטי

הפעולות המפורטות בסעיף 5.2.2 במערך פרסונל איי.די. דורשות שימוש של לפחות שני בני-אדם המחזיקים בחלקי מפתח פרטי הנמצאים על אמצעי אחסנה שונים (Key split).

6.2.3 הפקדת מפתח פרטי בנאמנות

מפתחות פרטיים של מערך פרסונל איי.די. אינם מופקדים בנאמנות. לא ניתן להפקיד מפתח פרטי של תעודה מאושרת בנאמנות אצל פרסונל איי.די. או אצל מערך רישום חיצוני כלשהו.

6.2.4 גיבוי מפתח פרטי

המפתחות הפרטיים של שרתי ההנפקה מגובים בתהליך הקמת השרתים והם נשמרים באופן מאובטח למטרות של הערכות לאסון ובאופן שאינו מפחית מהרשאות הגישה אליהם. המפתחות הפרטיים של רכיבים חיוניים במערך פרסונל איי.די., מגובים בעת יצירתם, ומוחזקים באופן מאובטח ונפרד ובאופן שאינו מפחית מהרשאות הגישה אליהם או רמת ההגנה עליהם.

6.2.5 ארכיבאות מפתח פרטי

ארכיבאות מפתח פרטי, אם אפשרית על-פי תהליך ההנפקה וסוג אמצעי האחסנה, היא באחריותו הבלעדית של בעל התעודה.

6.2.6 הכנסת מפתח פרטי לאמצעי אחסנה

כל אמצעי האחסנה של צמדי מפתחות במערך פרסונל איי.די. מייצרים את צמד המפתחות בעצמם, ואינם מקבלים מפתחות ממקור חיצוני.

6.2.7 אחסון מפתח פרטי ברכיב מאובטח

מפתחות פרטיים של שרתי ההנפקה, יצורו וישמרו על גבי רכיב מאובטח כאמור בסעיף 6.2.1. מפתחות פרטיים של בעלי תעודות, יוחזקו באמצעי חומרה כאמור בסעיף 6.1.1.

6.2.8 שיטה להפעלת המפתח הפרטי

לצורך הפעלת מפתח פרטי של שרת הנפקה, יש להציג בפני השרת אמצעי חומרה, כגון כרטיס חכם, שמאשר את אתחול השימוש ברכיב האחסנה הנפרד (HSM). לאחר מכן, נדרש לספק מידע להפעלה. לצורך הפעלת מפתח פרטי של ישות במערך פרסונל איי.די. שאינה שרת הנפקה, יש להציג בפני השרת את אמצעי החומרה עליו מאוחסן המפתח הפרטי. לאחר מכן, נדרש לספק מידע להפעלה. הפעלת מפתח פרטי של תעודה מאושרת מחייב שימוש במידע להפעלה –סיסמא, זיהוי ביומטרי של בעל התעודה או כל אמצעי אחר הקושר בין בעל התעודה למפתח הפרטי.

6.2.9 שיטה להשמדת מפתח פרטי

מפתח פרטי ממערך פרסונל איי.די. אותו יש להשמיד, מושמד מאמצעי האחסנה באופן ובאמצעים שלא מאפשרים לשחזר אותו לאחר מכן. השמדת מפתח פרטי של בעל תעודה מאושרת הינה באחריותו. במידה שאמצעי האחסנה סופק על ידי פרסונל איי.די. היא תמסור לבעל התעודה המלצות בנושא זה, וכן תכלול מידע זה באתר האינטרנט שלה.

פקעה תעודה, ישמיד בעל התעודה את המפתח הפרטי המלווה את התעודה בסמוך לפקיעתה.

השמדת מפתח טרם פקיעת התעודה המלווה אותו מחייבת הפעלת תהליך ביטול תעודה מקביל בגורם המאשר או במערך הרישום שהנפיק אותו.

6.2.10 **זירוג רכיב ההצפנה**

ראה סעיף 6.2.1.

6.3 **היבטים נוספים של ניהול צמדי מפתחות**

6.3.1 **ארכיבאות מפתח ציבורי**

המפתחות הציבוריים של שרתי החיתום, ישויות פרסונל איי.די. ובעלי התעודות מגובים בתהליך שגרתי יום-יומי של גיבוי שרת אחסנת התעודות.

פרסונל איי.די. שומר ארכיון של התעודות שהונפקו על ידו, כולל המפתחות הציבוריים שלהם.

6.3.2 **פרקי זמן מותרים לשימוש בצמדי מפתחות**

צמד מפתחות לחתימה אלקטרונית המשמש בשרת הנפקה ישמש יותר מפרק הזמן שנותר עד לפקיעת צמד המפתחות של השרת החותם את התעודה.

במידה ותשוננה התקנות הקובעות את אורך ו/או אלגוריתם המפתח של גורם מאשר, או שתתקיים סיבה אחרת המחייבת שינוי מפתחות, יוקם שרת הנפקה חדש בעל צמד מפתחות חדש העונה על הדרישות. תהליך זה ייעשה תוך אישור הרשם מראש, ובאופן שבו לא ייפגע תוקפן של תעודות החתומות על ידי המפתח הפרטי התקף של פרסונל איי.די..

צמדי מפתחות של בעל תעודה מותרים לשימוש לתקופות הבאות :

□ אם אוחסנו באמצעי אחסון פיזי קריפטוגרפי, כגון כרטיס חכם, העומד בתנאי תקנות חומרה ותוכנה – עד חמש שנים.

בפרק הזמן המותר לשימוש, רשאית פרסונל איי.די. לחדש את התעודה מבלי לדרוש את ייצורם של צמדי מפתחות חדשים. מעבר לפרקי הזמן המותרים, חייב בעל התעודה לייצר צמד מפתחות חדש עם חידוש התעודה.

במפתח פרטי של תעודה מאושרת מותר להשתמש רק כאשר התעודה המאשרת אותם תקפה. במפתחות ציבוריים לאימות חתימה ניתן להשתמש בכל עת מרגע כניסת התעודה לתוקף.

6.4 **מידע להפעלה**

6.4.1 **דרישות ממידע להפעלה**

דרישות להפעלת אמצעי חתימה של שרתי ההנפקה :

□ שימוש בכרטיס חכם שקודד במעמד התקנת אמצעי החתימה

□ תיקבע הסיסמא להפעלת הכרטיס החכם המיועד להפעלה

□ הסיסמא תקבע באופן רנדומאלי, תהיה באורך של 12 תווים לפחות ותורכב מספרות ומאותיות.

□ דרישות מידע להפעלת אמצעי חתימה במקרה של בעל תעודה או של בעל תפקיד במערך התפעול של הגורם המאשר (בהתאם להנחיית הרשם מספר 1/2010).

6.4.2 **הגנה על מידע להפעלה**

הגנה על מידע להפעלה של אמצעי חתימה של בעל תעודה היא באחריות בעל התעודה.

6.5 אמצעים לאבטחת מחשבים

6.5.1 אמצעי אבטחת מידע ממוחשב

תקנה 5(א) לתקנות חומרה ותוכנה קובעת "א) מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה (להלן – פעולות חיוניות) יעמדו ברמת ביטחון של תקן Common Criteria EAL4 או לפי תקן מקובל אחר, המבטיח רמת אבטחה מקבילה, להנחת דעתו של הרשם".
הרשם פרסם הנחייה 2-2010 הקובע דרישות בנושא זה.

חברת פרסונל איי.די. נבדקה על ידי קסלמן פתרונות בניהול סיכונים PricewaterhouseCoopers בע"מ, שאושרה על ידי הרשם לביצוע הבדיקה לפי ההנחיה, לעמידה בהנחייה זו.

6.5.2 תקנים לאמצעי אבטחת מידע ממוחשב

תקנה 5(א) לתקנות חומרה ותוכנה קובעת כי מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה ולביטולה יעמדו ברמת בטחון של תקן common criteria EAL4 או תקן CWA 14167-1 ותקן תומך CWA 14172-3 או לפי תקן מקובל אחר, המבטיח רמת אבטחה מקבילה, להנחת דעתו של הרשם. המערכת המשמשת בפרסונל איי.די. נבחנה ונמצא עומדת בדרישות המפורטות בהנחיית רשם מספר 2-2010, לעניין "תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר" ואושרה ע"י הרשם.
ראו בנוסף סעיף 6.2.1 לעיל.

6.6 מחזור חיים של מערכת תפעולית

6.6.1 אמצעים לבקרת פיתוח המערכת

יישומים ושירותים חדשים במערך פרסונל איי.די. מוכנסים לשירות מבצעי במערכות התפעוליות של פרסונל איי.די. לאחר שנבחנו במערכת ניסוי.

בנוסף, קיים נוהל מסודר להערכה של מידת ההשפעה של הכנסת האמצעי או היישום החדש על תפקוד מערכות פרסונל איי.די. על אמצעים שנמצאים במסגרת הרכיבים המנויים בתקנה 5 או בהנחייה 2-2010, לעבור את הבקרה המפורטת בסעיף [6.5.1](#) לעיל. פרסונל איי.די. מדווחת לרשם על כל שינוי כאמור לפי סעיף 13 לחוק.

6.6.2 אמצעים לבקרת האבטחה במערכת

במערך פרסונל איי.די. מיושמת מערכת לניטור ובקרה של התרעות על אירועי החשודים כאירועי אבטחת מידע.

במערך פרסונל איי.די. מיושם נוהל המחייב את האחראי על אבטחת המידע של המערך לבחון בפרקי זמן קבועים (על בסיס יומי, שבועי ותקופתי) את תקינות מערכות אבטחת המידע.

6.7 אמצעי אבטחת תקשורת מחשבים

פרסונל איי.די. בכלל ומערכות ניהול הגורם המאשר עומדים בתקן מת"י 27001. בהתאם לכך מערכות התקשורת הקשורות במערכת הניהול מוגנות באמצעים ובנהלי אבטחת מידע מחמירים. פרסונל איי.די. מפרידה בהיקף ובמידה האפשריים, בין מערכות המשמשות לביצוע פעולות חיוניות לבין מערכות מחשוב אחרות.

מערכות פרסונל איי.די. מחוברות לרשת האינטרנט או לרשת ציבורית אחרת רק באמצעות אמצעי הגנה המקנים רמה גבוהה של אמינות מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב. מידע המועבר ממערכות פרסונל איי.די. ברשת ציבורית או באינטרנט הינו מוצפן.

6.8 חתימת זמן

תעודות אלקטרוניות ורשימות תעודות בטלות (CRL), יכללו מידע אודות מועד הפקתן. מידע זה ייחתם בחתימתו של שרת ההנפקה כחלק בלתי נפרד.

רשומות מערכת (לוגים) יכללו חתימת זמן בעת מועד יצירתן. חתימת הזמן יכולה, אך לא חייבת להתבצע באמצעות מודול קריפטוגרפי, בהתאם לתקן מקובל.

למערכת חיתום הרשומות מקור זמן אמין המשקף את שעון גריניץ' (GMT) ומאמץ את מוסכמות הזמן האוניברסאליות (UTC)

7. מאפייני תעודות ורשימת תעודות מבוטלות (CRL)

7.1 מאפייני תעודה

7.1.1 מספר גירסה

התעודות המזהות את שרתי הנפקת התעודות של פרסונל אי.די. הן תעודות מסוג X509 version 3. פרופילי תעודות שרתי RCA ו-OCA מפורטים בסעיפים 0 ו-0 להלן.

תעודות אלקטרוניות המונפקות על-ידי פרסונל אי.די. על-פי מסמך נהלים זה אף הן מגרסה 3 של תקן X509. השדות המופיעים בתעודה מפורטים להלן בסעיף 7.1.11.

7.1.2 שדות הרחבה בתעודה

בתעודה המונפקת על פי מסמך נהלים זה ניתן להגדיר שדות הרחבה (Certificate Extensions). לשדה הרחבה שאין לו מזהה עצם מוכר, יוגדר מזהה עצם של פרסונל אי.די. על פי המבנה המתואר בסעיף 1.2.2.

7.1.3 סוגי אלגוריתמים

האלגוריתמים הבאים מותרים לשימוש בתעודה המונפקת על-פי מסמך נהלים זה :

שיטת גיבוב (HASH)

מועד	שיטת גיבוב	אורך פלט
עד סוף 2012	SHA-224, RIPEMD-160 (עם פלט מקוצר)	160
ללא הגבלה	SHA-224 ומעלה	224 ומעלה

שיטות חתימה

DSA, RSA ו-ECDSA באורכי מפתחות כאמור בסעיף 6.1.3

7.1.4 צורת שמות

ראו סעיף 3.1.1 לעיל.

7.1.5 מגבלות על שם

אין.

7.1.6 מזהה עצם (OID)

מזהה העצם של מסמך נהלים זה OID 1.3.6.1.4.1.12440.1, והפניה לכתובת האינטרנט בה ניתן לעיין בו מצורפים לכל תעודה המונפקת על-פי מסמך נהלים זה בשדה מדיניות אישור (Certificate Policies).

7.1.7 הגדרת שדות הרחבה כקריטיים

על פי מסמך נהלים זה ניתן להגדיר שדה הרחבה כקריטי, הגדרת שדה הרחבה כקריטי תגרום לכך שיישום שאינו תומך בשדה הרחבה זה לא יאפשר שימוש בתעודה.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

7.1.8 רשימת שדות עם ערכים משתנים ואפיונים

שם שדה	Type	מבנה	תיאור התוכן	דוגמא
<Cert_Hash>	Hex	Hash 160 bit	ערך גיבוב (Hash) של התעודה	7727 D14E A002 3CC3 AB6C 662F BB75 2A85 0E6F BE9A
<Cert_Ser_Num>	Hex	Integer	מספרה הסידורי של התעודה בשרת ההנפקה על פי RFC 2459	3E51 0398
<Country>	אלפא- נומרי אנגלית	Free Text	קוד דו-ספרתי של מדינה על פי תקן ISO 3166 http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html	IL US FR
<Fam_Name>	אלפא- נומרי אנגלית	Free Text	שם משפחה באנגלית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	Israeli
<ID_Doc_Det>	אלפא נומרי אנגלית מורכב	<ID_Doc_Type>#<ID_Num>@<Country>	התיאור המפורט (סוג מסמך הזיהוי, מספרו וארץ הנפקתו) של המסמך על פיו זוהה מבקש התעודה	ID#012345678@IL P#3496as95@US TR#ART2356Vi@FR
<ID_Doc_Type>	אלפא נומרי אנגלית	Free Text	סוג מסמך הזיהוי על פיו זוהה מבקש התעודה, לפי הרשימה הבאה: ID – תעודת זהות P – דרכון TR – תעודת מסע	ID
<ID_Num>	אלפא נומרי	Free Text	מספר תעודת הזיהוי הראשית על פיה זוהה מבקש התעודה. בתושב ישראל – 9 ספרות. אזרח זר – על	012345678 3496as95



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

שם שדה	Type	מבנה	תיאור התוכן	דוגמא
			פי מסמך הזיהוי.	ART234456Vi
<Key_Hash>	Hex	Hash160 bit	ערך גיבוב (Hash) של מפתח ציבורי של בעל התעודה או של השרת שהנפיק	KeyID=2DF8 7A35 E360 9CE3 5DCD B709 4964 7007 E24A FC36
<Key_length>	נומרי	1024/2048/4096	אורך המפתח של שדה ה Public Key.	1024
<Opt_Inf>	אלפא-נומרי עברית/אנגלית	Free Text	מידע נוסף על בעל התעודה שהוספתו נדרשת לצורך הבדלה בין תעודות שונות שהונפקו לאותו אדם על פי מדיניות הנפקה זו	00023 M=234096
<Pri_Name>	אלפא-נומרי אנגלית	Free Text	שם פרטי באנגלית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	Israel
<Public_Key>	Hex	RSA_Key	המפתח הציבורי RSA המזוהה בתעודה	3081 8902 8181 00C1 34D2 4F96 DD3F 22FC 36AC 2052 D121 FDF9 94DC F893 E9DD EECE EA61 A9E9 1B27 2EDB 1587 D456 C7F6 374A 7AB2 051E 933F 0CC0 A7ED 784A BD51 50E4 321D B0B1 6278 FCEF FCB5 F18A 0B49 ADE4 0BDE 628D C8D0 1D02 3734 18FA D649 1F1E



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

שם שדה	Type	מבנה	תיאור התוכן	דוגמא
				A2B6 3E16 5A9C 5065 8261 3294 0A3F 000C AF0E BF29 43F4 1DFB 82E2 5F7C 9E2B 1BDC DE48 538B 2E80 D502 0301 0001
<Valid_from>	Date	DD/MM/YY hh/mm/ss	שדה תאריך המציין את תחילת תוקף התעודה	6/2/2003 12:00
<Valid_To>	Date	DD/MM/YY hh/mm/ss	שדה תאריך המציין את סיום תוקף התעודה	6/2/2004 11:59
<שם_משפחה_ערבית>	ערבית	Free Text	שם משפחה בערבית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	زيرة
<שם_משפחה>	אלפא-נומרי עברית	Free Text	שם משפחה בעברית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	ישראלי
<שם_פרטי_ערבית>	ערבית	Free Text	שם פרטי בערבית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	احمد
<שם_פרטי>	אלפא-נומרי עברית	Free Text	שם פרטי בעברית של מבקש התעודה כפי הופעתו במסמכי הזיהוי	ישראל



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

7.1.9 פרופיל תעודה אלקטרונית לשרת הנפקה ראשי (Root CA)

קבוצה	שם שדה	ערכים
גרסה (Version)		V3
מספר סידורי (Serial Number)		<Cert_Ser_Num>
אלגוריתם חתימה (Signature Algorithm)		Sha2RSA
שם ייחודי של מנפיק התעודה Issuer Distinguished Name	Country (C)	IL
	Organization (O)	PersonalIDLtd
	Organizational Unit (OU)	Ceritfication Servers
	Common Name (CN)	PersonalID Trustworthy RootCA 2011
תקף מ : (Valid from:)		<Valid_From>
תקף עד : (Valid To:)		<Valid_To>
שם ייחודי של בעל התעודה Subject Distniguated Name	Country (C)	IL
	Organization (O)	PersonalID Ltd
	Organizational Unit (OU)	Ceritfication Servers



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

PersonalID Trustworthy RootCA 2011	Common Name (CN)	
<Public_Key> <4096>		מפתח ציבורי (Public Key)
[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.12440.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf		מדיניותות אישור Certificate Policies
<Key Hash>		גיבוב מפתח של נשוא התעודה Subject Key Identifier
<Key Hash>		גיבוב מפתח של מנפיק התעודה Authority Key Identifier
Subject Type=CA Path Length Constraint=2		מגבלות בסיסיות Basic Constraints
Sha1		אלגוריתם גיבוב Thumbprint Algorithm
<Cert_Hash>		גיבוב Thumbprint



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

7.1.10 פרופיל תעודה אלקטרונית לשרת הנפקה תפעולי (Operational CA)

קבוצה	שם שדה	ערכים
גרסה (Version)		V3
מספר סידורי (Serial Number)		<Cert_Ser_Num>
אלגוריתם חתימה (Signature Algorithm)		Sha2RSA
שם ייחודי של מנפיק התעודה Issuer Distinguished Name	Country (C)	IL
	Organization (O)	PersonalIDLtd
	Organizational Unit (OU)	Ceritfication Servers
	Common Name (CN)	PersonalID Supervisted Operationa CA 2011
תקף מ : (Valid from:)		<Valid_From>
תקף עד : (Valid To:)		<Valid_To>
שם ייחודי של בעל התעודה Subject Distinguished Name	Country (C)	IL
	Organization (O)	PersonalIDLtd
	Organizational Unit (OU)	Ceritfication Servers



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

PersonalID Supervised Operational CA, PersonalID Supervised Operational CA 2011 וכד'	Common Name (CN)	
<Public_Key> <2048>		מפתח ציבורי (Public Key)
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl01.ica.co.il/cdp/PersonalID Trustworthy RootCA 2011.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl02.ica.co.il/cdp/ PersonalID Trustworthy RootCA 2011.crl	CRL Distribution Point (CDP)	מקום הפצת CRL CRL Distribution Point ¹
[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.12440.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf		מדיניות אישור Certificate Policies
<Key_Hash>		גיבוב מפתח של נושא התעודה Subject Key Identifier

¹ עשויים להיות יותר מ-CDP אחד. אפשר ועותק CRL ימוקם באתר אשר אינו זמין לקהל הרחב, אך יהיה זמין.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<Key_Hash>		גיבוב מפתח של מנפיק התעודה Authority Key Identifier
Subject Type=CA Path Length Constraint=1		מגבלות בסיסיות Basic Constraints
Sha1		אלגוריתם גיבוב Thumbprint Algorithm
<Cert_Hash>		גיבוב Thumbprint

7.1.11 פרופיל תעודה ליחיד לביצוע "חתימה אלקטרונית מאושרת"

קבוצה	שם שדה x509	ערכים
גרסה (Version)	Version	V3
מספר סידורי (Serial Number)	Serial Number	<Cert_Ser_Num>
אלגוריתם חתימה (Signature Algorithm)	Signature Algorithm	Sha2RSA or Sha1RSA
שם ייחודי של מנפיק התעודה	Country (C)	IL
	Organization (O)	PersonalIDLtd



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

Ceritification Servers	Organizational Unit (OU)	Issuer
PersonalID Supervised Operational 2011	Common Name (CN)	
<Valid_From>	Valid From	תקף מ : (Valid from:)
<Valid_To>	Valid To	תקף עד : (Valid To:)
IL	Country (C)	בעל התעודה Subject
PesonalID Ltd ברירת מחדל : אפשר שיוגדרו שמות ארגון (O) אחרים, בהתאם ללקוחות ו/או פרוייקטים וכד'.	Organization (O)	
ILESLOW Certificates ברירת מחדל : אפשר שיוגדרו שמות יחידות ארגוניות (OU) נוספים, בהתאם ללקוחות ו/או פרוייקטים וכד'.	Organizational Unit (OU)	
תעודה לחתימה אלקטרונית מאושרת ליחיד	Description	
<Pri_Name> <Fam_Name> <ID_Doc_Det> <Opt_Inf> דוגמא : <i>Israel Israeli ID#1234567@IL 00234</i>	Common Name (CN)	
<שם פרטי> דוגמא : <i>Israel</i>	Given Name (G)	



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<שם משפחה> דוגמא:	Surname (Sn)	
Israeli		
<Public_Key> <2048>	Public Key	מפתח ציבורי (Public Key)
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl01.ica.co.il/cdp/PersonalID Supervised Operational CA 2011.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl02.ica.co.il/cdp/PersonalID Supervised Operational CA 2011.crl	CRL Distribution Point (CDP)	מקום הפצת CRL CRL Distribution Point
[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.12440.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= פרסונל איי.די. בע"מ, בן-גוריון 34, רמת-גן 52573; גורם מאשר רשום לפי חוק החתימה האלקטרונית התשס"א-2001; בעל התעודה זוהה פנים אל פנים על סמך תעודות ו/או מידע כנדרש בחוק; אמצעי אימות חתימה נבדק; מגבלות שימוש בתעודה: <תיאור המגבלה או הפניה למסמך הנהלים>; מגבלות על אחריות וכיסוי ביטוחי ³ : <תיאור המגבלה או הפניה למסמך הנהלים>; [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf	Certificate Policies	מדיניות אישור Certificate Policites

² עשויים להיות יותר מ-CDP אחד. אפשר ועותק CRL ימוקם באתר אשר אינו זמין לקהל הרחב, אך יהיה זמין.

³ מגבלות שימוש, כיסוי ביטוחי ומגבלות על סכום עשויות להיות מיושמות בנוסף בשדה X509 ייעודי שיסומן קריטי, והכל בהתאם להוראות מהותיות בנושא זה במסמך זה.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

Sha1		אלגוריתם גיבוב Thumbprint Algorithm
<Cert_Hash>		גיבוב Thumbprint

7.1.12 פרופיל תעודה לארגון לביצוע "חתימה אלקטרונית מאושרת"

קבוצה	שם שדה x509	ערכים
גרסה (Version)	Version	V3
מספר סידורי (Serial Number)	Serial Number	<Cert_Ser_Num>
אלגוריתם חתימה (Signature Algorithm)	Signature Algorithm	Sha2RSA or Sha1RSA
שם ייחודי של מנפיק התעודה Issuer	Country (C)	IL
	Organization (O)	PersonalIDLtd
	Organizational Unit (OU)	Ceritification Servers
	Common Name (CN)	PersonalID Supervised Operational CA2011
תקף מ : (Valid from:)	Valid From	<Valid_From>
תקף עד : (Valid To:)	Valid To	<Valid_To>



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

IL	Country (C)	בעל התעודה Subject
<Company_Name_English> <Company_Type>#<Company_Reg_Number>@<Country> דוגמא: <u>Securenet Ltd PRC#512835059@IL</u>	Organization (O)	
<שם_חברה> <סוג חברה>#<מספר חברה>@<קיצור_שם_מדינה> דוגמא: <u>פרסונל איי.די. בע"מ חפ"מ #512835059@IL</u>	Organization (O)	
תעודה לחתימה אלקטרונית מאושרת לארגון ומורשה חתימה מטעמו	Description	
<Pri_Name> <Fam_Name> <ID_Doc_Det> <Opt_Inf> דוגמא: <u>Israel Israeli ID#1234567@IL 00234</u>	Common Name (CN)	
<שם פרטי> דוגמא: <u>Israel</u>	Given Name (G)	
<שם משפחה> דוגמא: <u>Israeli</u>	Surname (Sn)	
<מספר תעודת זיהוי> דוגמא: <u>1234567</u>	Serial Number (SN)	



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<תפקיד_אנגלית> דוגמא: CFO	Title (T)	
<מספר_חפ(אופציונלי)> דוגמא: 512835059	UID	
<Public_Key> <2048>	Public Key	מפתח ציבורי (Public Key)
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl01.ica.co.il/ PersonalID Supervised Operational CA 2011.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl02.ica.co.il/ PersonalID Supervised Operational CA 2011.crl	CRL Distribution Point (CDP)	מקום הפצת CRL CRL Distribution P ⁴ oint

⁴ עשויים להיות יותר מ-CDP אחד. אפשר ועותק CRL ימוקם באתר אשר אינו זמין לקהל הרחב, אך יהיה זמין.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.12440.2.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= פרסונל איי.די. בע"מ, בן-גוריון 34, רמת-גן 52573; גורם מאשר רשום לפי חוק החתימה האלקטרונית התשס"א-2001; בעל התעודה זוהה ואומת קיומו על סמך תעודות ו/או מידע כנדרש בחוק; מורשה החתימה מטעם בעל התעודה זוהה פנים אל פנים ואומתה הרשאתו לקבל תעודה אלקטרונית עבור בעל התעודה כנדרש בחוק; אמצעי אימות חתימה נבדק; מגבלות שימוש בתעודה: <תיאור המגבלה או הפניה למסמך הנהלים>; <מגבלות על אחריות וכיסוי ביטוחי ⁵ : <תיאור המגבלה או הפניה למסמך הנהלים>; <סכום עסקה מותר: <סכום בש"ח> [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf Sha2	Certificate Policies	מדיניות אישור Certificate Policies
		אלגוריתם גיבוב Thumbprint Algorithm
<Cert_Hash >		גיבוב Thumbprint
יהיו שדות הרחבה ייעודיים של פרסונל איי.די. בהם יוכנסו, אופציונלית, הנתונים הבאים: שם החברה, מספר הרישום שלה, ארץ הרישום, סוג החברה, מספר תעודת זהות של מורשה החתימה, ארץ הנפקת התעודה המזהה וכד'.		שדות הרחבה
Digital Signature; Non-Repudiation		שימוש במפתחות Key Usage

⁵מגבלות שימוש, כיסוי ביטוחי ומגבלות על סכום עשויות להיות מיושמות בנוסף בשדה X509 ייעודי שיסומן קריטי, והכל בהתאם להוראות מהותיות בנושא זה במסמך זה.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<Key_Hash>		מזהה מפתח גורם מאשר Authority Key Identifier
<Key_Hash>		מזהה מפתח בעל תעודה Subject Key Identifier

7.1.13 פרופיל תעודה לארגון לביצוע "חתימה אלקטרונית מאושרת" ממוכנת

קבוצה	שם שדה x509	ערכים
גרסה (Version)	Version	V3
מספר סידורי (Serial Number)	Serial Number	<Cert_Ser_Num>
אלגוריתם חתימה (Signature Algorithm)	Signature Algorithm	Sha2RSA or Sha1RSA
שם ייחודי של מנפיק התעודה Issuer	Country (C)	IL
	Organization (O)	Pesonal Ltd
	Organizational Unit (OU)	Ceritifcation Servers
	Common Name (CN)	PersonalID Supervised Operational CA 2011



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<Valid_From>	Valid From	תקף מ : (Valid from:)
<Valid_To>	Valid To	תקף עד : (Valid To:)
IL	Country (C)	בעל התעודה Subject
<Company_Name_English> <Company_Type>#<Company_Reg_Number>@<Country> דוגמא : <u>Securenet Ltd PRC#512835059@IL</u>	Organization (O)	
<שם_חברה> <סוג חברה>#<מספר חברה>@<קיצור שם מדינה> דוגמא : <u>פרסונל איי.די. בע"מ חפ#512835059@IL</u>	Organization (O)	
תעודה לחתימה אלקטרונית מאושרת לארגון ומורשה חתימה מטעמו תעודה זו מותקנת על שרת חתימות לשימוש ממוכן בהתאם לסעיף <u>3.2.2.1</u> למסמך הנהלים.	Description	
<Pri_Name> <Fam_Name> <ID_Doc_Det> <Opt_ Inf> דוגמא : <u>Israel Israeli ID#1234567@IL 00234</u>	Common Name (CN)	
<שם פרטי> דוגמא : <u>Israel</u>	Given Name (G)	



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<שם משפחה> דוגמא: Israeli	Surname (Sn)	
<מספר_תעודת_זיהוי> דוגמא: 1234567	Serial Number (SN)	
<תפקיד_אנגלית> דוגמא: CFO	Title (T)	
<מספר_חפ(אופציונלי)> דוגמא: 512835059	UID	
<Public_Key> <2048>	Public Key	מפתח ציבורי (Public Key)
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl01.ica.co.il/ PersonalID Supervised Operational CA 2011.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl01.ica.co.il/ PersonalID Supervised Operational CA 2011.crl	CRL Distribution Point (CDP)	מקום הפצת CRL CRL Distribution Point ⁶

⁶ עשויים להיות יותר מ-CDP אחד. אפשר ועותק CRL ימוקם באתר אשר אינו זמין לקהל הרחב, אך יהיה זמין.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.12440.2.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= פרסונל איי.די. בע"מ, בן-גוריון 34, רמת-גן 52573; גורם מאשר רשום לפי חוק החתימה האלקטרונית התשס"א-2001; בעל התעודה זוהה ואומת קיומו על סמך תעודות ו/או מידע כנדרש בחוק; מורשה החתימה מטעם בעל התעודה זוהה פנים אל פנים ואומתה הרשאתו לקבל תעודה אלקטרונית עבור בעל התעודה כנדרש בחוק; אמצעי אימות חתימה נבדק; מגבלות שימוש בתעודה: <תיאור המגבלה או הפניה למסמך הנהלים>; <מגבלות על אחריות וכיסוי ביטוחי>: <תיאור המגבלה או הפניה למסמך הנהלים>; מגבלה על סכום עסקה מותר: <סכום בש"ח> [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: : http://www.ica.co.il/repository/cp/PersonalID_Practice_Statement.pdf	Certificate Policies	מדיניות אישור Certificate Policites
Sha1		אלגוריתם גיבוב Thumbprint Algorithm
<Cert_Hash >		גיבוב Thumbprint
יהיו שדות הרחבה ייעודיים של פרסונל איי.די. בהם יוכנסו, אופציונלית, הנתונים הבאים: שם החברה, מספר הרישום שלה, ארץ הרישום, סוג החברה, מספר תעודת זהות של מורשה החתימה, ארץ הנפקת התעודה המזהה וכד'.		שדות הרחבה
Digital Signature; Non-Repudiation		שימוש במפתחות Key Useage

⁷מגבלות שימוש, כיסוי ביטוחי ומגבלות על סכום עשויות להיות מיושמות בנוסף בשדה X509 ייעודי שיסומן קריטי, והכל בהתאם להוראות מהותיות בנושא זה במסמך זה.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

<Key_Hash>		מזהה מפתח גורם מאשר Authority Key Identifier
<Key_Hash>		מזהה מפתח בעל תעודה Subject Key Identifier

7.2 מאפייני רשימת תעודות בטלות

7.2.1 גרסה

רשימת התעודות הבטלות (CRL) המונפקת על-ידי פרסונל איי.די. על-פי מסמך נהלים זה ערוכה לפי תקן X509 גרסה 3.

7.2.2 רשימת תעודות בטלות ושדות גישה אליה

בנוסף למידע הבסיסי על תאריך ושעת הכנסת תעודה מסוימת לסטטוס מבוטל, רשאת פרסונל איי.די., אך אינה חייבת לפרט את סיבת ביטול התעודה.

7.2.3 פרופיל רשימת התעודות הבטלות (CRL)

קבוצה	שם שדה x509	ערכים
גרסה (Version)	Version	V2
שם ייחודי של מנפיק התעודה	Country (C)	IL
	Organization (O)	PersonalIDLtd.



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

Ceritification Servers	Organizational Unit (OU)	Issuer
PersonalID Supervised Operational CA 2011	Common Name (CN)	
<DD/MM/YY hh/mm/ss>	Effective Date	תקף מ : (Effective Date:)
<DD/MM/YY hh/mm/ss> 24+ שעות מזמן התוקף	Next Update	תקף עד : (Next Update:)
Sha2RSA	Signature Algorithm	אלגוריתם חתימה (Signature Algorithm)
Integer	Crl Number (OID 2.5.29.20)	מספר סידורי של CRL (CRL Number)
KeyID=Integer (HEX) Certificate Issuer: Directory Address: CN= PersonalID Supervised Operational CA 2011 OU=Certification Servers O=PersonalID Ltd. C=IL Certificate SerialNumber=Integer (Hex)	Authority Key Identifier	מזהה מפתח של מנפיק (Authority Key Identifier)
כתובת ה-CRL (הפניה בקופ)	Issueing Distribution Point (OID 2.5.29.28)	מקום הנפקת CRL Issueing Distribution Point
	Serial No.	רשימת תעודות מבוטלות
	Revocation Date	



פרסונל איי.די. בע"מ

מסמך נהלים להנפקת תעודה אלקטרונית ליחיד

תקפה לפי סעיף 2 לחוק החתימה האלקטרונית, התשס"א-2001

One of the following:	Details	
(0) Unspecified (1) Key Compromise (2) CA Compromise (3) Affiliation Changed (4) Superseded (5) Cessation of Operation		

7.3 פרופיל OCSF

החברה רשאית, אך לא חייבת לספק שירותי OCSF לבדיקת תקפות תעודה, בהתאם לאפיון נהלים שיקבעו בעתיד, באישור הרשם.

8. מבדקי התאמה

8.1 התאמה לת"י 27001 (ISO 127001)

פרסונל איי.די. עומדת בת"י 27001 (ISO 127001) ומקיימת מערכת ניהול אבטחת מידע (מנא"מ) כנדרש בו. במהלך שנה קלנדרית מבוצעים בפרסונל איי.די. תהליכי בדיקה עצמיים לזיהוי עמידת המנא"מ בדרישות התקן.

במסגרת הכנת פרסונל איי.די. לעמידה בת"י 27001 ייושם נוהל פעולה מתקנת, המטפל במקורותיו של כל אירוע אבטחת מידע ומתקן את הדרוש תיקון.

8.2 התאמה לת"י ISO 9000:2000

פרסונל איי.די. עומדת בת"י ISO 9000:2000 ומקיימת מערכת אבטחת איכות.

[נכון למועד כתיבת המסמך, לא הסתיים תהליך ההסמכה. ת"ל 15/4/2010]

8.3 ביקורת מערכות מידע

מערכות המידע של פרסונל איי.די. נבדקות על בסיס שנתי בהתאם לדרישות הרשם והקבוע בתקנות ניהול גורם מאשר. במסגרת זו, עורך בודק בלתי תלוי, להנחת דעת הרשם, בדיקות אבטחה שנתיות בהתאם לתקנה (8)2 לתקנות, ולהנחיות הרשם הכוללות גם מבדקי חדירות בהתאם לכללים מקובלים.

8.4 ביקורת יישום נוהלי עבודה

ביקורת יישום נוהלי העבודה של פרסונל איי.די. נעשית במסגרות הבאות:

8.4.1 ביקורת לפי ת"י 27001

בהליך הביקורת לפי ת"י 27001 נבדק גם יישום נוהלי העבודה בנושאי אבטחת מידע המשמשים כבסיס לעמידה בתקן.

8.4.2 ביקורת לפי ת"י ISO 9002

בהליך הביקורת לפי ת"י ISO 9002 נבדק גם יישום נוהלי העבודה בנושאי אבטחת איכות השירות המשמשים כבסיס לעמידה בתקן.

8.4.3 ביקורת יישום נוהלי עבודה פנימיים

פרסונל איי.די. מקיימת מערכת ביקורת פנימי לעמידה בנהלי העבודה הפנימיים שלה. מערך הביקורת פועל בהתאם לתוכנית העבודה השנתית של פרסונל איי.די..

8.4.4 ביקורת יישום נוהלי מסמך נהלים זה

פרסונל איי.די. מקיימת מערכת ביקורת פנימית לעמידה בהוראות הנפקת התעודות על-פי מסמך נהלים זה. מערך הביקורת פועל בהתאם לתוכנית העבודה השנתית של פרסונל איי.די..

8.4.5 תדירות מבדקי ההתאמה

מבדקי ההתאמה לעמידה בתקנים מבוצעים על בסיס חצי שנתי. ביקורת מערכות המידע נעשית באופן שנתי, כנדרש בתקנות.

ביקורת יישום נהלי עבודה נעשית לפי תוכנית עבודה שנתית של פרסונל איי.די..

8.4.6 זהות והכשרה של עורך המבדק

מבדקי ההתאמה לתקני ISO 9000:2000 ו-27001 מבוצעים על-ידי מעבדה מאושרת, בהתאם לדרישת תקנות ניהול גורם מאשר.

מבדקי מערכות המידע של פרסונל איי.די. נעשים על-ידי מבקר מערכות מוסמך, כנדרש בתקנות ניהול גורם מאשר והנחיות הרשם, להנחת דעתו של הרשם.

מבדקי עמידת מערך פרסונל איי.די. במסמך נהלים זה נעשה על-ידי המבקר הפנימי של פרסונל איי.די..

8.4.7 יחסי עורך המבדק ופרסונל איי.די.

אין קשר עסקי, לבד מזה הקשור בהזמנת ביצוע הביקורות לעמידה בתקנים, בין המעבדה המאושרת ופרסונל איי.די..

אין קשר עסקי, לבד מזה הקשור בהזמנת הבדיקה, בין מבקר המערכות המוסמך ובין פרסונל איי.די..

בדיקת עמידת פרסונל איי.די. בנהלים הפנימיים שלה מתבצעת על-ידי מבקר הפנים בפרסונל איי.די..

8.4.8 נושאים המכוסים במהלך הבדיקה

במהלך הבדיקות מכוסים כל הנושאים המפורטים בתקנים הרלוונטים.

ביקורת מערכות המידע בודקת את עמידת מערכות המידע של פרסונל איי.די. בהוראות החוק והתקנות.

8.4.9 תהליכים המבוצעים כתוצאה מתוצאות מבדק

נמצא במבדק כי תהליך מסוים בפרסונל איי.די. מחייב טיפול, יבוצעו, בהתאם למהות הבעיה ועל-פי הצורך, התהליכים הבאים:

- תיקון הטעון בדיקה;
- יישום אמצעים משמעותיים;
- הפעלת נוהל פעולה מתקנת;

8.4.10 הפצת תוצאות המבדק

תוצאות המבדקים ותהליכי התיקון בעקבותיהם נחשבים כמידע סודי כמפורט בסעיף 2.8 להלן.

תיקון הליקויים שנמצאו בתוצאות מבדקי ההתאמה לתקן מהווה תנאי לחידוש תוקף תעודת העמידה בתו התקן והם יתוקנו מיידיית בפיקוח הנהלת פרסונל איי.די..

9. היבטים עסקיים ומשפטיים אחרים

9.1 תעריפים

פרסונל איי.די. רשאית לגבות תשלומים עבור שירותיה השונים, בין השאר כאמור להלן במסמך נהלים זה.

9.1.1 תעריפי הנפקה, חידוש וביטול תעודה

פרסונל איי.די. רשאית לגבות תשלום עבור הנפקה של תעודה מאושרת ועבור חידושה. המחירים יכול שיקבעו בחוזה ההתקשרות בין בעל התעודה לפרסונל איי.די., או מי מטעמה.

9.1.2 תעריפי בדיקת תוקף תעודה

פרסונל איי.די. רשאית, אך אינה חייבת, לגבות תשלום עבור גישה לרשימת התעודות הבטלות לשם בדיקת תוקף של תעודה בודדת או קבוצה של תעודות אלקטרוניות. בהעדר חוזה בין פרסונל איי.די. לצד המסתמך, מחיר הבדיקה יפורסם לציבור.

9.1.3 תעריפים לשירותים אחרים

פרסונל איי.די. לא תגבה כסף עבור מידע אחר שהיא חייבת לפרסמו על-פי חוק, כגון מסמך זה. פרסונל איי.די. זכאית לגבות תשלום עבור שירותים אחרים הניתנים על ידו בהקשר התעודות האלקטרוניות, דוגמת אחזור מסמכי הרשמה לצורך הליך משפטי, תדפיסי רשומות וכד'. תעריפי השירותים יפורסמו באתר האינטרנט של פרסונל איי.די..

9.1.4 מדיניות החזרים כספיים

פרסונל איי.די. לא תחזיר תשלום עבור תעודה שהונפקה על-פי מסמך נהלים זה ובוטלה טרם מועד פקיעתה, אם התקיימו אחד מאלה –

(1) הביטול לא בוצע על ידי פרסונל איי.די.;

(2) הביטול הוא בנסיבות המנויות בסעיף [4.9.1.5](#).

9.2 אחריות כספית

9.2.1 כיסוי ביטוחי

אחריותה של פרסונל איי.די. מבוססת על ידה בפוליסת ביטוח. נוסח פוליסת הביטוח, שיעור הפיצוי בה והיקף הביטוח נערכו בהתאם לדרישות החוק, התקנות והנחיות הרשם.

פרסונל איי.די. אחראית לשנות את הכיסוי הביטוחי שלה בהתאם לכמות התעודות שהונפקו כנדרש בתקנות.

9.2.2 ערובות אחרות בביטוח וערובה

פרסונל איי.די. הפקידה בידי הרשם, על פי הוראתו (ככל שניתנה) ערבות בנקאית בשיעור שנקבע בתקנות. מימוש ערבות זו כפוף להוראות החוק.

9.2.3 כיסוי ביטוחי למשתמשי קצה

ראה סעיף 9.2.1

9.2.4 יחסי נאמנות

הנפקת תעודות אלקטרוניות, או השתתפות בהנפקת תעודות תחת הוראות מסמך נהלים זה אין בה כדי ליצור יחסי נאמנות, שליחות, שותפות, עובד-מעביד, אפטרופסות או כל צורה אחרת של ייצוג בין פרסונל איי.די. לבין צד מסתמך, או בין פרסונל איי.די. לבין בעל התעודה.

9.3 סודיות מידע עסקי

9.3.1 מידע עסקי הנחשב כסודי

מידע הנחשב סודי-עסקי בגורם המאשר הינו מידע תפעולי ו/או מידע עסקי ו/או מסחרי של פרסונל איי.די.. בין היתר, מידע סודי הוא המידע המפורט להלן:

- ☐ מפתחות פרטיים של רכיבי מערך פרסונל איי.די.;
- ☐ הגדרות, הרשאות ומידע להפעלה של מערכות פרסונל איי.די.;
- ☐ אמצעי ותוכניות אבטחה של פרסונל איי.די.;
- ☐ תוכניות הערכות לאסון של פרסונל איי.די.;
- ☐ נהלי תפעול פנימיים;

9.3.2 מידע עסקי שנחשב כגלוי

המידע להלן נחשב גלוי-עסקי בפרסונל איי.די.. פרסומו וגישת אליו יהיו כמפורט במסמך נהלים זה:

- ☐ מסמך נהלים זה;
 - ☐ מסמך מדיניות הגנת פרטיות של פרסונל איי.די.;
 - ☐ מסמך מדיניות אבטחת מידע של פרסונל איי.די.;
- מידע אשר לא הוגדר במפורש בסעיף זה לא יחשב כגלוי וכל עיון ו/או שימוש במידע בו חייב בהרשאה מפורשת מראש ובכתב של פרסונל איי.די., שתינתן או תישלל לפי שיקול דעתה המוחלט של החברה

9.3.3 אחריות להגן על מידע סודי

פרסונל איי.די. מיישמת אמצעים וכללים הולמים לשם שמירתו של מידע עסקי הנחשב לסודי בהתאם לנוהלי אבטחת המידע.

9.4 מידע פרטי הנחשב כסודי

9.4.1 הגנת הפרטיות

בהתאם להוראות החוק, פרסונל איי.די. רשמה את מאגר המידע שלו אצל רשם מאגרי המידע. מאגר המידע של פרסונל איי.די. כפוף לפיקוחו של רשם מאגרי מידע בהתאם להוראות חוק הגנת הפרטיות, וזאת בנוסף לפיקוח שחל עליו במסגרת חוק החתימה האלקטרונית.

במערכות פרסונל איי.די. מיושמים אמצעים למניעת חשיפתו של מידע הפוגע בפרטיות, כהגדרת החוק הגנת הפרטיות.

מדיניות הגנת הפרטיות של פרסונל איי.די. מפורטת במסמך המפורסם באתר האינטרנט של החברה

9.4.2 מידע עסקי הנחשב כסודי-אישי

מידע הנחשב סודי-אישי בגורם המאשר הינו מידע הפוגע בפרטיות של בעל תעודה. בין היתר, מידע סודי-אישי הוא המידע המפורט להלן:

- ☐ פרטי הזדהות ורישום של מבקשי תעודות;
 - ☐ מאגר התעודות האלקטרוניות שהונפקו על-פי מסמך נהלים זה;
- על מידע הנחשב לסודי בפרסונל איי.די., מיושמים אמצעים וכללים הולמים לשם שמירתו

9.4.3 מידע אישי הנחשב כגלוי

המידע להלן נחשב גלוי-אישי בפרסונל איי.די.. פרסומו וגישת אליו יהיו כמפורט במסמך נהלים זה:

- ☐ מאגר רשימת התעודות הבטלות;

9.4.4 אחריות על מידע סודי

פרסונל איי.די. מיישמת אמצעים וכללים הולמים לשם שמירתו של מידע פרטי הנחשב לסודי בהתאם לנוהלי אבטחת המידע.

9.4.5 הסכמה לשימוש במידע אישי

בהעדר הסכמה מבעל המידע, פרסונל איי.די. לא תשתמש במידע פרטי של בעל התעודה הנחשב סודי אלא לפי דרישות החוק או לצורכי תפעול של הגורם המאשר.

מידע אשר לא הוגדר במפורש בסעיף 9.4.2. לא יחשב כגלוי וכל עיון ו/או שימוש במידע בו חייב בהרשאה מפורשת מראש ובכתב של פרסונל איי.די., שתינתן או תישלל לפי שיקול דעתה המוחלט של החברה.

9.4.6 גילוי לרשויות אכיפת חוק

מידע שאינו מוגדר כגלוי והשייך לפרסונל איי.די., או מוחזק על ידה, יימסר לרשויות אכיפת חוק על פי דין. בהעדר הגבלה משפטית על כך, ובמידת האפשר, תדווח פרסונל איי.די. לבעל המידע על דבר צו שניתן בקשר עם גילוי מידע, טרם פעולת הגילוי.

אין בהתחייבות פרסונל איי.די. על-פי סעיף זה כדי למנוע, באופן כלשהוא, פעולות ביקורת של הרשם או של רשם מאגרי מידע של מערכות פרסונל איי.די..

פרסונל איי.די. תהיה רשאית לתבוע מבעל המידע החזר הוצאות משפטיות ו/או אחרות שנגרמו לו עקב הטיפול בבקשת הגילוי.

9.4.7 גילוי במסגרת הליך אזרחי

מידע שאינו מוגדר כגלוי ושייך לפרסונל איי.די., או מוחזק על ידה, יימסר רק על פי דין.

פרסונל איי.די. תהיה רשאית להתנות מתן מידע כאמור בהחזר הוצאות משפטיות ו/או אחרות שנגרמו לה עקב הטיפול בבקשת הגילוי.

9.5 קניין

9.5.1 כללי

כל זכויות הקניין הרוחני – לרבות זכויות היוצרים, הזכויות המוסריות, סימני המסחר, המדגמים, הפטנטים וסודות המסחר – במבנה התעודה הייחודי שיצרה פרסונל איי.די. וזאת במובחן מהתקנים שעל בסיסם יצרה פרסונל איי.די. את מבנה התעודה, שייכות לפרסונל איי.די. בלבד. האמור לעיל חל גם על כל מידע בתעודה, שאינו פרטיו האישיים של בעל התעודה או המפתח הציבורי בלבד. בכלל זה חל האמור לעיל על כל סימן מסחר של פרסונל איי.די. ונוסח של מגבלות ותנאים לשימוש בתעודה.

אין להעתיק את מבנה התעודה או כל מידע בה, שהזכויות בו הינן של פרסונל איי.די. כאמור לעיל, בלא קבלת הרשאה מפורשת בכתב ומראש מפרסונל איי.די.. פרסונל איי.די. רשאית, אך אינה חייבת, ליתן זכויות שימוש בתבנית התעודה או במידע בהסכמים שתחתום עם בעלי תעודות, מערכי רישום חיצוניים או צדדים מסתמכים.

9.5.2 קניין בצמדי מפתחות

כל זכויות הבעלות מכל מין וסוג, לרבות (אך לא רק) זכויות הקניין הרוחני ובכללן זכויות היוצרים, הזכויות המוסריות, סימני המסחר, המדגמים, הפטנטים וסודות המסחר, בצמדי המפתחות המשמשים את פרסונל איי.די. לשם ניהול מערכי הגורם המאשר ו/או הנפקת התעודות האלקטרוניות על-פי מסמך נהלים זה, שייכות לפרסונל איי.די. בלבד. פרסונל איי.די. מתירה בזאת להשתמש אך ורק במפתח הציבורי, שבאמצעותו ניתן לאמת את חתימתה האלקטרונית על גבי תעודות אלקטרוניות – וזאת לצורך אימות כאמור ולצורך זה בלבד.

אין לפרסונל איי.די. זכויות קנייניות כלשהן בצמדי המפתחות המשמשים את בעל התעודה.

9.5.3 קניין רוחני במסמך נהלים זה

כל זכויות הקניין הרוחני - לרבות זכויות היוצרים והזכויות המוסריות, סימני המסחר וסודות המסחר - במסמך נהלים זה שייכות לפרסונל איי.די.. אין להעתיק, להפיץ, לשכפל, לצלם, להקליט, לתרגם, להציג, לאחסן במאגר מידע, לשדר או לשנות מסמך זה, בכל אמצעי שהוא - לרבות בכל אמצעי אלקטרוני, אופטי, מכאני או אחר - ללא אישור מפורש בכתב ומראש מפרסונל איי.די..

מותר לעיין במסמך זה, לקוראו, להדפיסו ולשומרו בפורמט אלקטרוני לכל תכלית הקשורה במישרין בתעודה מאושרת שפרסונל איי.די. מנפיקה, או במסגרת כל הליך משפטי שבו נדרש לעשות שימוש במסמך נהלים זה, על פי דין. אין לעשות במסמך כל שימוש אחר, לרבות כל שימוש מסחרי בו.

9.6 מצגים ואחריות

9.6.1 מצגים ואחריות של הגורם המאשר

פרסונל איי.די. מצהירה ומאשרת כדלקמן:

- אין מצגים בתעודה המהווים טעות מהותית בעובדה, הידועים או הנובעים מהגורמים בפרסונל איי.די. המאשרים את הבקשה לתעודה, או המנפיקים את התעודה;
- אין טעויות במידע המופיע בתעודה ושנגרמו על ידי הגורמים בפרסונל איי.די. המאשרים את הבקשה לתעודה או המנפיקים את התעודה כתוצאה מכישלונם לפעול בסבירות בטיפול בבקשה או בהנפקה של התעודה;
- התעודות שפרסונל איי.די. מפקה עומדות בכל הדרישות המהותיות של מסמך נהלים זה;
- ביטול התעודות והשימוש בארכיון תואמים באופן מהותי להוראות הרלבנטיות במסמכי הנהלים הרלבנטיים להם;
- החוזה שבין פרסונל איי.די. לבין בעל התעודה עשוי לכלול מצגים והתחייבויות נוספות של פרסונל איי.די. כלפי בעל התעודה.

9.6.2 מצגים ואחריות של רשות רישום

רשות רישום מצהירה ומאשרת כדלקמן:

- אין מצגים בתעודה המהווים טעות מהותית בעובדה, הידועים או הנובעים מהגורמים ברשות הרישום המאשרים את הבקשה לתעודה, או המנפיקים את התעודה;
- אין טעויות במידע המופיע בתעודה ושנגרמו על ידי הגורמים ברשות הרישום המאשרים את הבקשה לתעודה כתוצאה מכישלונם לפעול בסבירות בטיפול בבקשה;
- התעודות שרשות הרישום מפקה עומדות בכל הדרישות המהותיות של מסמך נהלים זה;
- ביטול התעודות, ככל שרלבנטי, והשימוש בארכיון תואמים באופן מהותי להוראות במסמכי הנהלים הרלבנטיים להם;
- החוזה שבין פרסונל איי.די. לבין בעל התעודה עשוי לכלול מצגים והתחייבויות נוספות של רשות הרישום כלפי בעל התעודה.

9.6.3 מצגים ואחריות של בעל תעודה

בעל התעודה מצהיר ומאשר כדלקמן:

- כל המצגים שהציג בעל התעודה בבקשה שהגיש לקבלת התעודה, הם אמת;
- כל המידע שסיפק בעל התעודה והמצוין בתעודה, הוא אמת;
- בעל התעודה משתמש בתעודה למטרות מאושרות וחוקיות בלבד ובהתאם למסמך נהלים זה;
- בעל התעודה הוא משתמש קצה ולא גורם מאשר והוא איננו משתמש במפתח הפרטי התואם למפתח הציבורי המצוין בתעודה לשם חתימה אלקטרונית של כל תעודה או פורמט אחר של מפתח ציבורי, או כל רשימת תעודות מבוטלות, כגורם מאשר או ככל גורם אחר;

9.6.4 מצגים ואחריות של צד מסתמך

צד מסתמך מצהיר ומאשר כדלקמן:

- יש בידיו מידע מספק כדי לקבל החלטה מודעת ביחס להיקף ההסתמכות שלו ולפי בחירתו, על מידע בתעודה;
- הצד המסתמך אחראי באופן בלעדי להחלטתו אם להסתמך על מידע כאמור;
- הצד המסתמך נושא באחריות לכשלונו לבצע את התחייבויותיו בהתאם למסמך נהלים זה;
- החוזה שבין פרסונל איי.די. לצד המסתמך עשוי לכלול מצגים והתחייבויות נוספות של הצד המסתמך כלפי פרסונל איי.די..

9.6.5 מצגים ואחריות של צדדים אחרים

אין

9.7 העדר מצגים

ראה סעיף 9.6 לעיל.

9.8 הגבלת אחריות

9.8.1 כללי

סעיף 21(א) לחוק קובע כי גורם מאשר לא יהיה אחראי לנזק שנגרם עקב הסתמכות על תעודה אלקטרונית שהנפיק, אם הוכיח כי נקט את כל האמצעים הסבירים לקיום חובותיו לפי חוק זה. פרסונל איי.די. לא תהיה אחראית לכל נזק מכל מין וסוג, ובכלל זה נזק ישיר או עקיף, ממוני או שאינו ממוני, שייגרם לכל אדם עקב שימוש אסור (כאמור בסעיף 1.4).

פרסונל איי.די. לא תהיה אחראית לכל נזק מכל מין וסוג, ובכלל זה נזק ישיר או עקיף, ממוני או שאינו ממוני, שייגרם לכל אדם, בהתאם להגבלת האחריות המפורטת בפרק זה.

9.8.2 תקרת אחריות – הגבלה בסכום

מבלי לגרוע מן ההוראות שלעיל ולהן - בכל מקרה, אחריות פרסונל איי.די. בגין נזק שייגרם עקב הסתמכות סבירה ובתום-לב על תעודה מאושרת, או עקב הסתמכות סבירה ובתום-לב על מידע בדבר תוקף תעודה שהונפקה כאמור, לא תעלה על סכום מצטבר של 500,000 שקלים חדשים לתעודה. פרסונל איי.די. רשאית לקבוע תקרת אחריות נמוכה יותר. גובה תקרת האחריות יצוין בתעודה. האמור לעיל לא יחול על נזק שגרמה פרסונל איי.די. בזדון.

בכל הקשור לתעודות המונפקות למבקשי תעודות (1) הנדרשים לעשות בהן שימוש למילוי דרישות חתימה לפי חיקוק, או (2) לפי דרישת רשות מרשויות המדינה, לא תגביל פרסונל איי.די. את אחריותה הכוללת בגין התעודה, כאמור לעיל, לפחות מ- 500,000 ₪.

9.8.3 אחריות פרסונל איי.די. כלפי בעל תעודה

בנוסף לאמור בסעיף 9.8.1 לעיל, אחריות פרסונל איי.די. כלפי בעל תעודה נקבעת בחוזה שבין פרסונל איי.די. לבין בעל התעודה, ובלבד שחוזה כאמור אינו סותר את הוראות החוק או את הוראות מסמך נהלים זה. בהעדר חוזה כאמור, או אם אין בחוזה כאמור התייחסות לאחריות פרסונל איי.די., יחול רק האמור בסעיף 9.8.1 לעיל.

9.8.4 אחריות פרסונל איי.די. כלפי צד מסתמך

בנוסף לאמור בסעיף 9.8.1 לעיל ובהוראות כל דין, היה חוזה בין פרסונל איי.די. לבין הצד המסתמך, הכולל הוראות בדבר אחריות פרסונל איי.די. כלפי הצד המסתמך, תיקבע אחריותה כלפי צד מסתמך כאמור בחוזה, ובלבד שחוזה כאמור אינו סותר את הוראות החוק, התקנות והנחיות הרשם או את הוראות מסמך נהלים זה. בהעדר חוזה כאמור, יחול האמור בסעיף 9.8.1 לעיל וכן יחול האמור להלן.

9.8.5 תנאים נוספים

9.8.5.1 כוח עליון

לפרסונל איי.די. נהלים קפדניים אשר חלקם מפורט במסמך נהלים זה. נהלי פרסונל איי.די. נועדו ליתן מענה, בין השאר, למקרים של שיבושים, תקלות ואסון. בכפוף לכך ולהוראות כל דין, פרסונל איי.די. לא תישא באחריות כלשהי לכל הפסד, אובדן רווח, תשלום, הוצאה או נזק שהם תוצאת כוח עליון או נסיבות שאינן בשליטת פרסונל איי.די., ואשר לא ניתן היה להיערך לקראתן באופן סביר.

לעניין סעיף זה - "כוח עליון" לרבות- מצב מלחמה והנובע ממנו; כל שיבוש, תקלה, עיכוב או קלקול הנובעים מרשויות ממשלתיות ו/או אחרות ו/או מחברות המספקות שירותי תשתית, חשמל ותקשורת לגורם המאשר וכן כל שיבוש, תקלה, עיכוב או קלקול שהם תוצאת שביתה והשבתה שלא אצל פרסונל איי.די. בלבד, והמצב הביטחוני או המדיני של מדינת ישראל.

9.9 שיפוי ופיצוי (Indemnities)

כאמור בסעיף 9.8 לעיל.

9.10 תחולה וסיום

9.10.1 תחולה

מסמך זה תקף מרגע אישורו על רשם גורמים מאשרים במשרד המשפטים ופרסומו באתר האינטרנט של הגורם המאשר בכתובת <http://www.ica.co.il/repository/cps/>

9.10.2 תוקף

מסמך נהלים זה תקף ממועד תחילת תוקפו כאמור לעיל וכל עוד לא שונה, הותלה או בוטל.

9.10.3 תוקף של מסמך נהלים

מסמך נהלים חל על תעודות שהונפקו בעת שהיה בתוקף. אושר ופורסם מסמך נהלים חדש, המחליף מסמך נהלים קודם, יחול מסמך הנהלים החדש על כל התעודות שהונפקו מיום אישורו ופרסומו ואילך. מסמך הנהלים הישן יישלח לארכיון פרסונל איי.די., ויהיה זמין לעיון בכתובת הבאה: <http://www.personalid.co.il/repository/cps>

תיקון למסמך הנהלים יכול שיעשה בדרך של עדכון חלקי. לצד כל תיקון במסמך הנהלים, יפורסם מועד אישורו המחייב בידי הרשם, באופן שיאפשר מעקב אחר תחילת תוקפו וסיום תוקפו של המסמך או הפרק הקודם. תחולת התיקון תהיה מעת מועד הפרסום לאחר אישור הרשם, אולם אין בכך כדי להוסיף חובות למי שהונפקה לו תעודה לפי מסמך נהלים תקף קודם, כל עוד התעודה שהונפקה לו בתוקף.

9.10.4 השלכות סיום תוקף

לא תונפקנה תעודות אלקטרוניות על פי מסמך נהלים זה מרגע סיום תוקפו. הכללים שיחולו על תעודה שהונפקה על פי המסמך, אם לא בוטלה יהיו הכללים הנהוגים בו, עד לסיום תוקף התעודה.

9.11 דרכי תקשורת עם בעלי תעודות

פרסונל איי.די. תפנה אל בעלי התעודות האלקטרוניות באמצעות דואר אלקטרוני כפי שנמסר במעמד הרישום. כמו כן, רשאית פרסונל איי.די., לפי שיקול דעתה המוחלט, ליתן הודעה כאמור גם על ידי פרסום בעיתון יומי.

9.12 ניהול שינויים

9.12.1 תהליך לביצוע שינויים במסמך

החברה תוכל לבצע שינויים למסמך באישור מנהל הגורם המאשר, ובאישור מנכ"ל החברה בתיאום עם הייעוץ המשפטי. השינוי יכנס לתוקף רק לאחר אישור הרשם לשינוי.

9.12.2 מנגנון לפרסום שינויים

המסמך יפורסם באתר האינטרנט של החברה, בכתובת <http://www.personalid.co.il/repository/cps/> מייד עם כניסתו לתוקף.

9.12.3 נסיבות לשינוי מזהה עצם

שינויים ועדכונים במסמך זה לא יהיו סיבה לשינוי מזהה עצם, אלא אם הדבר הוחלט ע"י מנכ"ל החברה ומנהל הגורם המאשר ואושר ע"י רשם גורמים מאשרים.

9.13 יישוב סכסוכים

הוראות חוזי ההתקשרות שבין פרסונל איי.די. לבין בעל התעודה ו/או המסתמך יכול שיכללו הוראות בדבר יישוב סכסוכים.

9.14 החוק החל

הדין החל על פעולות פרסונל איי.די. על-פי מסמך זה הוא דין מדינת ישראל בלבד (למעט כללי ברירת הדין הבינלאומיים). בשום תנאי לא יחולו על פעולות פרסונל איי.די. על-פי מסמך נהלים זה דיניהן של מדינות אחרות כלשהן.

9.15 ציות לחוק החל

הגורם המאשר יפעל לפי הוראות החוק, התקנות, הנחיות הרשם ודיני מדינת ישראל החלים עליו.

9.16 הוראות שונות

9.16.1 הוראות כלליות לחוזי פרסונל איי.די.

מסמך נהלים זה אינו ממצה את ההסדרים החוזיים שבין פרסונל איי.די. לבין בעלי תעודות ו/או צדדים מסתמכים. פרסונל איי.די. רשאית להסכים בכל חוזה שבינה לבין בעל תעודה ו/או בינה לבין צד מסתמך על הסדרים נוספים על האמור במסמך נהלים זה. מובהר כי הסדרים נוספים כאמור לא יתנו על הוראות מסמך נהלים זה.

חוזי פרסונל איי.די. עם בעלי תעודות אלקטרוניות וצדדים המסתמכים על תעודות אלקטרוניות מכילים סעיפי נתיקות, המשכיות, מיצוי והודעות.

סעיף נתיקות ("כלל העפרון הכחול") קובע כי אם תנאי בחוזה יוכרז כבטל או בלתי אכיף, לא יפגע הדבר בתוקפן של שאר הוראות החוזה. עוד מורה הסעיף כי ככל שניתן לקיים בקירוב הוראה שהוכרזה כבטלה או בלתי-אכיפה, היא תקום כך.

סעיף המשכיות קובע את ההוראות בחוזה שנשארות בתוקף לאחר סיום החוזה או ביטולו.

סעיף מיצוי קובע כי כל ההסכמות בין הצדדים מגולמות בחוזה הכתוב, ואין תוקף להסכמה שלא נכנסה לחוזה הכתוב

9.16.2 מיצוי

ראה סעיף 9.16.1

9.16.3 נתיקות

ראה סעיף 9.16.1

9.16.4 כח עליון

ראה סעיף 9.8.5.1.

9.17 הוראות אחרות

אין.