

קומסיין בע"מ

נהלים להסדרת פעילות הגורם המאשר (CPS)

במסגרת מתן שירותי הנפקת

תעודות אלקטרוניות העומדות בדרישות חוק חתימה אלקטרונית ותקנותיו

גרסה 5.1

תאריך אישור הרשם: 11.05.2022

תאריך פרסום: 12.05.2022

קומסיין בע"מ

ת.ד. 58077, קריית עתידים, תל-אביב 6158001

זכויות יוצרים © 2022 קומסיין בע"מ

כל הזכויות שמורות

הודעת זכויות יוצרים

כל הזכויות במסמך נהלים זה שמורות לקומסיין בע"מ.

ניתנת רשות לעשות בתוכן מסמך נהלים זה שימוש חופשי, בתנאי שיצוינו בעלי הזכויות ואתר האינטרנט המדויק שבו מופיע המסמך. אין להשתמש בתוכן לצורך שיגור "דואר זבל", אין למכור אותו, ואין לגבות תשלום בגין השימוש בו. התוכן מיועד לציבור הרחב והוא איננו בגדר מתן יעוץ משפטי.

כתובת חברת קומסיין:

כתובת למשלוח מכתבים : ת.ד. 58077, קריית עתידים, תל-אביב, 6158001 ישראל .

כתובת משרדי החברה : קריית עתידים, בניין מספר 4, 6158001, תל-אביב, ישראל .

טל : 03-6485255, פקס : 03-6474206, כתובת דואר אלקטרוני : info@comsign.co.il.

טבלת מעקב אחר גרסאות המסמך

מספר גרסה	תאריך שינוי	עיקרי העדכון
1.0	01/01/2008	
3.0	07/09/2010	בהתאם ל- RFC3647 העדכני http://www.ietf.org/rfc/rfc3647.txt
3.1	18/08/2011	- הגבלות על שימוש בתעודה (1.4.4) (4.5.9) (4.6.3) (10.7) - הוספת הגדרה לתקנות ניירות ערך (מאשר חתימה) (1.6) - שינויים במבנה התעודה למגנא, ליחיד ולתאגיד/מוסד ציבורי ותוכן השדות (7.1.1) (7.1.2) (7.1.3) - עריכת המסמך גם לפי לתקן ETSI TS 456 (1) (10.13) - החרגות למשתמשי מגנא בנושא תדירות הפרסום במאגר (2.3) (4.6.2) - זיהוי מורשה בהנפקה עבור רשות ני"ע (3.2.2.6) - פרסום CRL לרשות ני"ע (4.8.8) - הבהרת הגבלת אחריות הגורם המאשר (10.7.2.1) - משלוח הודעות לבעלי התעודות (10.11)
4.2	06/07/2020	- בהתאם ל- RFC3647 העדכני - הוספה הגבלה על כמות תעודות שניתן להנפיק לגורם מדווח אחד במערכת מגנא (3.1.1) - הוסרה ההגבלה על התקנת אמצעי חתימה למורשה על גבי מערכת חיתום מבוססת שרת (3.2.2) - התקנת אמצעי חתימה על גבי שרת חתימות המאוחסן בידי צד ג' תצויין במפורש במסמכי ההתקשרות (3.2.2) - בקשה לביטול תעודה אלקטרונית למערכת מגנא יכול ותוגש גם על ידי רני"ע (3.4.4). - דרישות זיהוי ואימות מיוחדות בהנפקה למערכת מגנא (3.2.5), (3.3.1), (4.1.2) - התאמת הנוהל להנפקת תעודה לעובד מדינה כמורשה מוסד ציבורי (4.1.2) - עדכון נוהל הנפקה במקרה של התקנת אמצעי החתימה על גבי שרת חתימות מרכזי (4.3.1) - מועדים מיוחדים למשלוח הודעת חידוש לתעודה במערכת מגנא (4.6.1) - דרישת אבטחה פיסית מוגברת לשרת חתימות (5.9) - דרישת אבטחה לוגית מוגברת לשרת חתימות (6.2.5) - משך תקופת תוקף תעודה למערכת מגנא (6.3.2)

• יידוע צד מסתמך במקרה של אמצעי חתימה השמור על גבי שרת חתימות (7.1.8) • שינוי בשדות התעודה כאשר התעודה מותקנת על גבי שרת חתימות (7.1.8-מבנה תעודה למורשה בתאגיד או מוסד ציבורי) • דרישת בדיקה וביקורת תקופתית לתוכנת שרת החתימות (8.1) • תיקון הגדרת תעודה אלקטרונית ל-"תעודה אלקטרונית מאושרת" בעקבות תיקון מס' 3 לחוק (1.6) • ביצוע חידוש מרחוק של תעודה אלקטרונית תקפה (3.3.1) • תנאים לריבוי תעודות ליחיד (3.1.1) • הרשאה לשימוש על ידי יחיד או מורשה בכינוי או בשם נעורים (3.1.3) • הנפקת תעודות אלקטרוניות ליחיד או מורשה תושב הרשות הפלסטינית (7.1.9, 3.2.3, 3.2.2) • הנפקת תעודה אלקטרונית לתושב חוץ לצורך דיווח והזדהות מול רשות המיסים (3.2.3) • הוספת אפשרות לבדיקה מקוונת של תוקף תעודה אלקטרונית (4.9.9) • הוספה האפשרות למשלוח התראות והודעות דואר אלקטרוני/ טלפוניות/ מסרונים בנושאי שירותים או מוצרים באופן ובאמצעים שאושרו על ידי בעל התעודה במועד ההנפקה או במועד מאוחר יותר. (4.6.1, 4.1.2) • התאמות לנוהל רשם מיום 17.04.2019 להגשת בקשה להנפקה על גבי התקן רשתי (3.2.2, 4.3.1, 5.9, 6.2.11, 7.1.8, 8.1) • התאמות למסמך השלמה לנוהל רשם בעניין אישור סוג הנפקה על גבי התקן רשתי (שרת חתימות) מיום 24.12.2020 כפי שעודכן ביום 21.02.2021 (9.2.3, 8.1, 3.2.2) • זיהוי תושב פלסטיני שלא לצורך שער עולמי (3.2.3) • הגבלה על משך תוקפו של אישור בדבר הרשאת מורשה לפעול בשם תאגיד (3.2.5)		5.0
---	--	-----

5.1	• הוספת מבנה תעודה לנוטריון בעל 2 תעודות (7.1.2.3)
-----	--

תוכן עניינים

14	מבוא	1.
14	הסבר כללי	1.1.
15	שם המסמך וזיהוי	1.2.
15	הגופים המשתתפים בהנפקת התעודות	1.3.
15	גורם מאשר:	1.3.1.
15	גורם רושם:	1.3.2.
15	בעל התעודה:	1.3.3.
15	צד מסתמך:	1.3.4.
15	גורמים משתתפים אחרים:	1.3.5.
16	שימוש בתעודה	1.4.
16	שימושים מותרים בתעודה:	1.4.1.
16	הגבלות על שימוש בתעודה:	1.4.2.
16	מדיניות ונהלים	1.5.
16	האחראי על יישום המדיניות ונהלים:	1.5.1.
16	איש קשר:	1.5.2.
17	הממונה על התאמת הנהלים למדיניות הגורם המאשר:	1.5.3.
17	אישור הנהלים:	1.5.4.
17	הגדרות ומונחים	1.6.
20	פרסום ומאגר מידע	2.
20	המאגר של קומסיין	2.1.
20	פרסום מידע הנוגע לתעודות באמצעות המאגר של קומסיין	2.2.
20	תדירות ומועד הפרסום במאגר	2.3.
21	בקרת גישה למאגר	2.4.
22	זיהוי ואימות	3.
22	מתן שם	3.1.
22	סוגי שמות:	3.1.1.
22	על שם בעל התעודה להיות בעל משמעות:	3.1.2.
22	שימוש בכינוי או הימנעות מציון שם:	3.1.3.
22	הוראות למתן פירוש לסוגי שמות שונים:	3.1.4.

23	ייחודיות שם בעל התעודה :	3.1.5
23	מסירת מידע לצרכי זיהוי, אימות וסימני מסחר :	3.1.6
23	אימות זיהוי ראשוני של המבקש	3.2
23	הוכחת החזקה במפתח פרטי :	3.2.1
24	אימות זהות תאגיד :	3.2.2
26	אימות זהות של מבקש יחיד :	3.2.3
27	מבקש שפרטיו לא אומתו :	3.2.4
27	ווידוא הרשאה/הסמכה :	3.2.5
27	קריטריונים להסתמכות על תעודות אלקטרוניות מארגונים חיצוניים :	3.2.6
28	זיהוי ואימות בקשות לחידוש תעודה אלקטרונית	3.3
28	זיהוי ואימות במקרה של חידוש תעודה ללא ייצור אמצעי חתימה חדש לבקשת מבקש בטרם פג תוקף תעודתו :	3.3.1
28	זיהוי ואימות לצורכי חידוש לאחר ביטול התעודה האלקטרונית :	3.3.2
28	אימות זיהוי בקשה לביטול תעודה	3.4
30	דרישות תפעוליות במחזור חייה של תעודה אלקטרונית	4
30	בקשה להנפקת תעודת אלקטרונית	4.1
30	מי יכול להגיש בקשה לתעודה אלקטרונית :	4.1.1
30	הליך הגשת הבקשה והחובות המוטלות במסגרתו :	4.1.2
33	עיבוד הבקשה להנפקת תעודה אלקטרונית	4.2
33	ביצוע פעולות זיהוי ואימות :	4.2.1
33	אישור או דחיית הבקשה :	4.2.2
34	לוחות זמנים לעיבוד הבקשה :	4.2.3
34	הנפקת תעודה אלקטרונית	4.3
34	פעולות הגורם המאשר במעמד ההנפקה :	4.3.1
35	הודעה לבעל התעודה על ביצוע ההנפקה :	4.3.2
35	קיבול התעודה האלקטרונית	4.4
35	התנהגות הנחשבת לקיבול :	4.4.1
35	פרסום התעודה על ידי הגורם המאשר :	4.4.2
35	מתן הודעה ליישויות אחרות מאת הגורם המאשר בדבר ההנפקה :	4.4.3
35	צמד המפתחות והשימוש בתעודה	4.5
35	המפתח הפרטי של בעל התעודה והשימוש בתעודה :	4.5.1
36	המפתח הציבורי והשימוש בו ובתעודה האלקטרונית על ידי צד מסתמך :	4.5.2
37	חידוש תעודה	4.6
37	הנסיבות לחידוש תעודה אלקטרונית :	4.6.1
38	מי רשאי לדרוש חידוש של תעודה אלקטרונית :	4.6.2

4.6.3.	אופן הטיפול בבקשות חידוש :	38
4.6.4.	הודעה לבעל התעודה אודות החידוש :	38
4.6.5.	התנהגות הנחשבת לקיבול של תעודה אלקטרונית שחודשה :	38
4.6.6.	פרסום התעודה המחודשת על ידי הגורם המאשר :	38
4.6.7.	מתן הודעה בדבר החידוש מאת הגורם המאשר ליישויות אחרות :	39
4.7.	החלפת צמד מפתחות לתעודה אלקטרונית (re-key)	39
4.7.1.	הנסיבות להחלפת צמד מפתחות לתעודה אלקטרונית :	39
4.7.2.	מי רשאי לדרוש החלפתו של צמד המפתחות של תעודה אלקטרונית :	39
4.7.3.	אופן הטיפול בבקשות להחלפת צמד המפתחות :	39
4.7.4.	הודעה לבעל התעודה אודות החלפת צמד המפתחות :	39
4.7.5.	התנהגות הנחשבת לקיבול של תעודה אלקטרונית שצמד מפתחותיה הוחלף :	39
4.7.6.	פרסום על ידי הגורם המאשר של התעודה שצמד מפתחותיה הוחלף :	39
4.7.7.	מתן הודעה בדבר החלפת המפתחות מאת הגורם המאשר ליישויות אחרות :	39
4.8.	ביצוע שינויים בתעודה	39
4.8.1.	הנסיבות לשינוי תעודה אלקטרונית :	39
4.8.2.	מי רשאי לדרוש שינוי של תעודה אלקטרונית :	40
4.8.3.	אופן הטיפול בבקשות לשינויה של תעודה אלקטרונית :	40
4.8.4.	הודעה לבעל התעודה אודות שינוי התעודה :	40
4.8.5.	התנהגות הנחשבת לקיבול של תעודה אלקטרונית ששונתה :	40
4.8.6.	פרסום על ידי הגורם המאשר של התעודה ששונתה :	40
4.8.7.	מתן הודעה בדבר שינוי התעודה מאת הגורם המאשר ליישויות אחרות :	40
4.9.	ביטול והתליית תעודה אלקטרונית	40
4.9.1.	הנסיבות לביטול תעודה אלקטרונית :	40
4.9.2.	מי רשאי לדרוש ביטול של תעודה אלקטרונית :	41
4.9.3.	אופן הטיפול בבקשות לביטולה של תעודה אלקטרונית :	41
4.9.4.	מתן ארכה לבעל התעודה קודם לביטולה :	41
4.9.5.	פרק הזמן העומד לרשות הגורם המאשר לביטול התעודה :	42
4.9.6.	חובת בדיקת רשימת התעודות המבוטלות על ידי צד מסתמך :	42
4.9.7.	תדירות פרסום רשימת התעודות המבוטלות :	42
4.9.8.	זמן אחזור מירבי של רשימת התעודות המבוטלות :	42
4.9.9.	בדיקה מקוונת של סטטוס אישור התעודה (OCSP) :	42
4.9.10.	דרישות מבדיקה מקוונת של הביטול :	42
4.9.11.	צורות פרסום אחרות של תעודות מבוטלות :	43
4.9.12.	דרישות מיוחדות לביטול כתוצאה מאובדן שליטה בצמד המפתחות :	43

43	נסיבות המאפשרות התליית התעודה האלקטרונית:	4.9.13
43	מי רשאי לדרוש את התליית התעודה:	4.9.14
44	אופן הטיפול בבקשת התלייה:	4.9.15
44	הגבלת משך תקופת ההתלייה:	4.9.16
44	שרותי בדיקת סטטוס תעודה אלקטרונית על ידי מסתמך	4.10
44	מאפיינים תפעוליים:	4.10.1
44	זמינות השירותים:	4.10.2
44	מאפיינים נוספים - שחרור מנעילה:	4.10.3
44	פקיעת תעודה אלקטרונית:	4.11
45	הפקדה בנאמנות (escrow) ואחזור מפתח פרטי	4.12
45	מדיניות ונהלים להפקדת מפתח פרטי ואחזורו:	4.12.1
45	מאפייני מפתח שיחה (session key) ומדיניות ונהלי אחזור:	4.12.2
46	בקורות פיזיות, ניהוליות ותפעוליות	5
46	בקורות פיזיות	5.1
46	מבנה האתר ומיקומו:	5.1.1
46	גישה פיזית:	5.1.2
46	חשמל ומיזוג אוויר:	5.1.3
47	חשיפה לנזקי מים:	5.1.4
47	הגנה מנזקי אש ומניעתם:	5.1.5
47	הגנת אמצעים לאחסון נתונים:	5.1.6
47	מניעת אובדן מידע במסגרת פינוי אשפה:	5.1.7
47	גיבוי מחוץ לאתר המאובטח:	5.1.8
47	בקורות ניהוליות	5.2
47	תפקידי אמון:	5.2.1
48	מספר העובדים הנדרש לביצוע מטלות מסויימות:	5.2.2
48	זיהוי ואימות הנדרש לכל בעל תפקיד:	5.2.3
48	תפקידים המחייבים הפרדת סמכויות:	5.2.4
48	בקורות כוח אדם	5.3
48	דרישות כשירות, ניסיון ואכשרה:	5.3.1
48	נהלים לבדיקת ואימות פרטים:	5.3.2
49	דרישות הדרכה לתפקיד:	5.3.3
49	תדירות הדרכות והכשרות:	5.3.4
49	תדירות ונוהל החלפת תפקידים:	5.3.5
49	הליכי משמעת במקרה של אי קיום הנהלים:	5.3.6
49	דרישות מקבלנים עצמאיים:	5.3.7
50	תיעוד הנמסר לצוות הגורם המאשר:	5.3.8
50	נהלי תיעוד אירועים (לוגים)	5.4

50	סוגי אירועים המחייבים תיעוד :	5.4.1
50	תדירות עיבוד לוגים :	5.4.2
50	תקופת אירכוב הלוגים :	5.4.3
50	הגנה על לוגים של הביקורת:	5.4.4
50	גיבוי לוגים של הביקורת:	5.4.5
50	מערכת איסוף רשומות הביקורת (פנימית או חיצונית):	5.4.6
51	דיווח לגורם האחראי לאירוע:	5.4.7
51	הערכת פגיעות המערכת:	5.4.8
51	אירכוב רשומות	5.5
51	סוגי רשומות הנשמרות בארכיב:	5.5.1
51	תקופת שמירת רשומות בארכיב:	5.5.2
52	הגנה על הארכיב:	5.5.3
52	נהלי גיבוי ארכיב הרשומות:	5.5.4
52	דרישה לחותמות יום ושעה של רשומות מאורכבות:	5.5.5
52	מערכת הארכוב (פנימית או חיצונית):	5.5.6
52	נהלים לאיסוף ואימות מידע ארכיוני:	5.5.7
52	החלפת מפתחות של הגורם המאשר	5.6
52	התאוששות ממצבי אסון (DRP) ופגיעה במערכת	5.7
53	נהלים להתמודדות עם ארועים בלתי צפויים ופגיעה בגורם המאשר:	5.7.1
53	פגיעה במשאבי מיחשוב, תוכנות או מידע	5.7.2
53	נהלים במקרה פגיעה במפתח הפרטי של גורם בהירארכיית הגורם המאשר	5.7.3
53	המשכיות עסקית לאחר אירוע אסון	5.7.4
53	סיום ו/או הפסקת פעילותה של קומסיין	5.8
54	אבטחה פיסית – התקן רשתי	5.9.
56	בקורות אבטחה טכנית	6.
56	חילול והתקנת צמד מפתחות	6.1
56	חילול צמד מפתחות:	6.1.1
56	מסירת המפתח הפרטי לבעל התעודה:	6.1.2
56	מסירת המפתח הציבורי של בעל התעודה לגורם המאשר:	6.1.3
56	פרסום המפתח הציבורי של הגורם המאשר לצדדים מסתמכים:	6.1.4
56	גודל מפתחות:	6.1.5
57	פרמטרים של חילול המפתח הציבורי ובקרת איכות:	6.1.6
57	Key Usages (שדה שימוש בהתאם לתקן X.509v3):	6.1.7
57	הגנה על המפתח הפרטי ובקורות קריפטוגרפיות	6.2
57	תקנים ובקורות להתקנים קריפטוגרפיים:	6.2.1
58	ביזור סמכויות (u מתוך m) בבקרה על המפתח הפרטי:	6.2.2
58	הפקדה בנאמנות של המפתח הפרטי:	6.2.3

58	6.2.4	גיבוי המפתח הפרטי:
58	6.2.5	אירכוב המפתח הפרטי:
58	6.2.6	הכנסה והוצאה של המפתח הפרטי להתקן:
58	6.2.7	איחסון המפתח הפרטי בהתקן:
59	6.2.8	הפעלת המפתח הפרטי:
59	6.2.9	סיום פעולת המפתח הפרטי:
59	6.2.10	השמדת המפתח הפרטי:
59	6.2.11	דירוג ההתקן הקריפטוגרפי:
59	6.3	היבטים אחרים בניהול צמד מפתחות
60	6.3.1	אירכוב המפתח הציבורי:
60	6.3.2	תקופת תוקף השימוש בתעודה האלקטרונית ובצמד המפתחות:
60	6.4	המידע הדרוש להפעלה:
60	6.4.1	חילול המידע הדרוש להפעלה והתקנתו:
60	6.4.2	הגנת המידע הדרוש להפעלה:
60	6.4.3	היבטים נוספים של המידע הדרוש להפעלה:
60	6.5	בקורות לאבטחת מחשב:
60	6.5.1	דרישות טכניות מיוחדות לאבטחת מחשב:
61	6.5.2	דירוג אבטחת מחשב:
61	6.6	בקורות טכניות במהלך תקופת התוקף של תעודה אלקטרונית
61	6.6.1	בקורות על פיתוחי מערכת:
61	6.6.2	בקורות על ניהול האבטחה:
61	6.6.3	בקורות אבטחה במהלך תקופת התוקף של התעודה האלקטרונית:
61	6.7	בקורות אבטחת רשת:
62	6.8	חותמת יום-שעה:
62	6.9	אבטחה לוגית – שרת חתימות
63	7	מבנה תעודה, רשימת תעודות מבוטלות ו-OCSP
63	7.1	מבנה תעודה
63	7.1.1	מספר/י גירסה:
63	7.1.2	שדות הרחבה בתעודה:
63	7.1.2.1	שדות הרחבה בתעודת השורש של הגורם המאשר (Root CA)
64	7.1.2.2	תעודת ביניים
66	7.1.2.3	מבנה תעודות למנויים
80	7.1.3	מזהי אובייקט אלגוריתמיים (OIDs – Algorithmic object identifiers):
80	7.1.4	צורות שם:
81	7.1.4.1	מידע אודות הגורם המנפיק
81	7.1.4.2	שדה Subject Information בתעודה

81	Subject Alternative Name שדה הרחבה	7.1.4.3
81	Subject Distinguished Name שדות	7.1.4.4
81	הגבלות על שמות:	7.1.5
82	מזהה אובייקט למדיניות תעודות אלקטרוניות:	7.1.6
82	מדיניות שימוש בשדות הרחבה מגבילים:	7.1.7
82	מבנה ותחביר למאפייני מדיניות תעודות אלקטרוניות:	7.1.8
	הבהרה לענין קוד המדינה המופיע על גבי תעודה אלקטרונית המונפקת ליחיד תושב הרשות	7.1.9
82	הפלסטיניות או תאגיד פלסטיני הרשום ברשות הפלסטינית:	
83	מבנה רשימת התעודות המבוטלות ("CRL")	7.2
83	מספר/י גירסה:	7.2.1
83	CRL וסיומות רישומי CRL	7.2.2
84	פרופיל מצב אישור מקוון (OCSP)	7.3
84	מספר/י גירסה:	7.3.1
84	סיומות OCSP:	7.3.2
86	ביקורות תאימות	8
86	תדירות או נסיבות עריכת ביקורות:	8.1
86	זהות עורך הביקורת:	8.2
86	עצמאות עורך הביקורת:	8.3
86	נושאים הנבדקים במסגרת הביקורת:	8.4
87	פעולות נדרשות לאור ממצאי כשל ותקלות:	8.5
87	הפצת תוצאות הביקורת:	8.6
87	עריכת ביקורת עצמית:	8.7
88	סוגיות משפטיות ועסקיות נוספות	9
88	תשלומים	9.1
88	תשלום בגין הנפקת או חידוש תעודות:	9.1.1
88	תשלום עבור גישה לרשימת התעודות האלקטרוניות:	9.1.2
88	תשלום עבור בדיקת סטאטוס התעודות האלקטרוניות:	9.1.3
88	תשלום עבור שירותים אחרים:	9.1.4
88	מדיניות החזרים:	9.1.5
88	חבות כספית	9.2
88	כיסוי ביטוחי:	9.2.1
88	בטוחות אחרות:	9.2.2
89	ביטוח או ערובה למשתמשי קצה:	9.2.3
89	הגנה על סודיות מידע עסקי	9.3
89	מידע עסקי סודי:	9.3.1
89	מידע עסקי שאיננו מוגן:	9.3.2
89	חובת ההגנה על מידע סודי עסקי:	9.3.3

89	הגנה על סודיות מידע פרטי	9.4
89	מדיניות הגנה על פרטיות המידע:	9.4.1
90	מידע הנחשב כמידע פרטי סודי:	9.4.2
90	מידע פרטי שאיננו מוגן:	9.4.3
90	חובת ההגנה על הפרטיות:	9.4.4
90	גילוי והסכמה לשימוש במידע פרטי:	9.4.5
90	גילוי מידע במסגרת הוראה שיפוטית או מנהלית:	9.4.6
90	נסיבות אחרות לגילוי מידע פרטי:	9.4.7
90	זכויות קניין רוחני	9.5
91	מצגים וחובות	9.6
91	מצגים וחובות של הגורם המאשר:	9.6.1
91	מצגים וחובות של גורמים רושמים של קומסיין:	9.6.2
91	מצגים וחובות של בעל התעודה:	9.6.3
92	מצגים וחובות של צד מסתמך:	9.6.4
92	מצגים וחובות של צדדים משתתפים אחרים:	9.6.5
92	פטור מערביות ומצגים	9.7
92	הגבלת אחריות של קומסיין ונציגיה	9.8
93	שיפוי	9.9
93	תוקף מסמך הנהלים וסיומו	9.10
94	תוקף מסמך הנהלים:	9.10.1
94	פקיעת תוקף הנהלים:	9.10.2
94	תוצאות פקיעה ושמירת תוקף:	9.10.3
94	הודעות	9.11
94	שינויים ותוספות	9.12
94	נהלים לביצוע שינויים:	9.12.1
95	אופן פרסום השינויים:	9.12.2
95	נסיבות לשינוי מזהה האובייקט (OID):	9.12.3
95	יישוב מחלוקות	9.13
95	הדין החל	9.14
95	כפיפות לחוקים	9.15
95	שונות	9.16
95	שלמות הנהלים:	9.16.1
95	המחאת זכויות וחובות:	9.16.2
96	הוראות סותרות:	9.16.3
96	אכיפה:	9.16.4

96	-----	כוח עליון:	9.16.5
96	-----	הסדרים נוספים - גורמים רשמיים	9.17.
96	-----	מבוא	9.17.1
97	-----	בקשה של גורם לפעול כגורם רשם של קומסיין:	9.17.2
97	-----	המען להגשת בקשה לקומסיין לפעול כגורם רשם של קומסיין:	9.17.3
97	-----	אחריות לפעולות גורמים רשמיים:	9.17.4

נספח - תעודות לאתרי אינטרנט

99	--	דרישות נוספות מגורם רשם של שירות הנפקת תעודות אלקטרוניות לאתרי אינטרנט	(1)
99	-----	המאגר של קומסיין	(2)
99	-----	פרסום מידע הנוגע לתעודות באמצעות המאגר של קומסיין	(3)
99	-----	שימוש בכינוי או הימנעות מציון שם בתעודות אלקטרוניות לשרתי אינטרנט:	(4)
99	-----	אימות כתובות דואר אלקטרוני הנקובות בתעודות SSL:	(5)
99	-----	אימות זהות בהנפקת תעודה אלקטרונית לשרת הנושאת את שם הארגון:	(6)
100	-----	אימות שימוש בשם עסק/שם מסחרי בתעודה אלקטרונית לשרת	(7)
100	-----	אימות ציון שם מדינה בתעודה אלקטרונית לשרת	(8)
101	-----	אימות הרשאה או שליטה בשם מתחם בתעודה אלקטרונית לשרת	(9)
102	-----	אימות כתובת IP	(10)
102	-----	אימות שימוש בתו כללי בשם מתחם	(11)
102	-----	בחינת אמינות מקור המידע	(12)
102	-----	בדיקת מרשמי גורמים מאשרים מוסמכים (CAA Records)	(13)
103	-----	הגשת בקשה לתעודה לשרת אינטרנט	(14)
103	-----	ביצוע פעולות זיהוי ואימות של בקשה לתעודה לשרת אינטרנט	(15)
104	-----	אישור או דחיית בקשה להנפקת תעודה לשרת אינטרנט	(16)
104	-----	הנסיבות לביטולה של תעודה אלקטרונית לשרת אינטרנט	(17)
104	-----	נסיבות המאפשרות התליית תעודה אלקטרונית לשרת אינטרנט	(18)
104	----	משך תקופת תוקף השימוש לתעודה אלקטרונית לשרת אינטרנט ובצמד המפתחות	(19)
104	-----	מבנה תעודה לשם מתחם SSL/TLS DV (שרתי אינטרנט)	(20)
107	-----	מבנה תעודת SSL/TLS לשרת אינטרנט של ארגון (OV)	(21)
109	-----	מזהה אובייקט למדיניות תעודות אלקטרוניות:	(22)
109	-----	נושאים הנבדקים במסגרת הביקורת על הנפקת תעודות לשרתי אינטרנט:	(23)

1. מבוא

חברת קומסיין בע"מ הינה גורם מאשר על-פי חוק חתימה אלקטרונית התשס"א 2001. כגורם מאשר מנפיקה קומסיין תעודה אלקטרונית מאושרת שהינה אישור אלקטרוני שאמצעי אימות חתימה מסוים שייך לאדם מסוים וזאת לאחר שזיהתה את מבקש התעודה האלקטרונית פנים אל פנים.

מסמך נהלים זה מסדיר את אופן מתן שירותי הנפקת התעודות האלקטרוניות של קומסיין, העומדות בדרישות החוק ואת אופן השימוש בהן, לרבות זיהוי ואימות [פרק 3]; הנפקת, ביטול וחידוש תעודות [פרק 4]; אבטחה פיזית [פרק 5]; אבטחה לוגית [פרק 6] ופרופיל תעודות ורשימת תעודות מבוטלות (CRL) [פרק 7].

קומסיין משמשת גם כמאשר חתימה מטעם רשות ניירות ערך בהתאם לתקנות ניירות ערך (מאשר חתימה), תשס"ג-2003 ומנפיקה תעודות אלקטרוניות למורשה חתימה אלקטרונית של תאגיד מדרג בהתאם לתקנות ניירות ערך (חתימה ודיווח אלקטרוני), תשס"ג-2003 ולמורשה גישה לדואר אלקטרוני מאובטח בהתאם לתקנות ניירות ערך (דואר אלקטרוני מאובטח), תשע"ג-2012.

במסגרת הנפקת תעודות אלקטרוניות למשתמשי מגנא (מערכת גילוי נאות אלקטרונית), פועלת קומסיין בהתאם לתקנות ניירות ערך ובכפוף לאישורי הנפקה שמוציאה רשות ניירות ערך. ייתכנו הסדרים מיוחדים, בנושאי הנפקה וניהול התעודות האלקטרוניות המונפקות במסגרת מערכת מגנא.

ההתקשרות בין המבקש לקומסיין כרוכה בחתימה על הסכם מנוי.

מסמך זה נערך לפי תקן RFC 3647. קומסיין מצהירה כי כללה בו גם דרישות לפי תקן ETSI TS 456 ולפי הגירסה האחרונה של ה-BaseLine Requirements. חלק מדרישות אלו כמו גם שירותים שונים אחרים, אינם חלק מהדין הישראלי ואינם נתונים לפיקוח הרשם (כהגדרתו להלן). בהתאם, הנהלים העוסקים בדרישות ושירותים אלו מופיעים בגוף מסמך הנהלים רק על דרך האזכור והפניה לנספח למסמך זה. להסרת כל ספק, הנהלים המפורטים בנספח כמו גם ההפניה לנספח בגוף מסמך הנהלים לא נבדקו ולא אושרו על ידי הרשם אולם מחייבים את קומסיין, נציגיה בעלי התעודות הרלבנטיים וצדדים מסתמכים.

1.1 הסבר כללי

שירותי הנפקת התעודות האלקטרוניות של קומסיין נועדו לתמוך במסחר אלקטרוני מאובטח ובשירותים אלקטרוניים אחרים על מנת לענות על הצרכים הטכניים, העסקיים והאישיים של המשתמשים בטכנולוגית החתימות האלקטרונית. קומסיין רשומה כגורם מאשר אצל רשם הגורמים המאשרים במשרד המשפטים בהתאם לחוק (כהגדרת מונחים אלו להלן), ומשמשת כצד שלישי נאמן אשר מנפיק, מנהל ומבטל תעודות אלקטרוניות מאושרות על פי נהלים אלה.

שירותי הנפקת התעודות כוללים הרשמה, זיהוי של המבקש, הנפקה, ביטול, ותיעוד הפעולות המבוצעות על-ידי קומסיין. ביטול של תעודות יבוצע במקרים המנויים בסעיף **Error!** **Reference source not found.** 4.9.1 למסמך נהלים זה בכפוף לחוק, לתקנות ולהוראות הרשם (כהגדרת מונחים אלו להלן).

מסמך נהלים זה מיושם על ידי קומסיין ונציגיה ומתייחס רק לתעודות אלקטרוניות מאושרות

כהגדרתן בחוק, העומדות בדרישות החוק ותקנותיו (כהגדרתם להלן).

1.2. שם המסמך וזיהוי

מסמך זה, יכונה "מסמך הנהלים" או "CPS of ComSign Ltd." או "CPS" וכך יופיע בתעודה האלקטרונית. ניתן לעיין במסמך באתר החברה <http://www.comsign.co.il/cps>.

מזהה המסמך (OID) הוא: 1.3.6.1.4.1.19389.4.1.1

1.3. הגופים המשתתפים בהנפקת התעודות

1.3.1. גורם מאשר:

קומסיין היא גורם מאשר כהגדרתו בחוק חתימה אלקטרונית והתקנות שהותקנו מכוחו. נהלי חברת קומסיין מבוססים על החוק הישראלי ותקנותיו, על התקינה הבינלאומית ככל שהיא תואמת את הוראות החוק הישראלי וכן על הנחיות רשם הגורמים המאשרים.

1.3.2. גורם רושם:

שירותי הנפקת התעודות של קומסיין מנוהלים כך ששירותים הנוגעים לטיפול בבקשות להנפקת תעודה אלקטרונית, לזיהוי המבקשים ולהרשמתם יכולים להתבצע על ידי גורם רושם שהוסמך על ידי הגורם המאשר ואושר על ידי רשם הגורמים המאשרים בהתאם לקבוע בחוק ובתקנות. הגורם הרושם מחויב לקיום נהלים אלה והנחיות הגורם המאשר. הגורם הרושם כפוף, הירארכית, לגורם המאשר, והגם שחלה עליו אחריות מוגדרת במסגרת הסמכתו, אין בכך כדי לפטור את קומסיין מאחריותה הכוללת על-פי חוק לפעילותו. באופן זה מובטחת השמירה על איכותם האחידה של השירותים אותם מספקים הגורם המאשר ונציגיו.

1.3.3. [בכל הקשור לדרישות נוספות מגורם רושם של שירות הנפקת תעודות אלקטרוניות לאתרי אינטרנט: ¹ - ראה סעיף 1.3.2.1 לנספח - (1)].

1.3.4. בעל התעודה:

ראה הגדרה בסעיף 1.6 להלן.

1.3.5. צד מסתמך:

ראה הגדרה בסעיף 1.6 להלן.

1.3.6. גורמים משתתפים אחרים:

• **פקידי רישום ואימות של קומסיין:** נציגי קומסיין שאחריותם לקבל את מבקשי התעודות, למלא את פרטי מבקשי התעודות, לוודא ולאמת את זהותם של מבקשי התעודה, לבצע את הליך הנפקת התעודה בפועל ולאחר ההנפקה לוודא כי היא פועלת כהלכה. לאחר מכן קבלת התשלום והוצאת חשבונית וקבלה. במקרים של ביטול תעודה – לוודא את זהות המבטל ולבצע את הביטול בפועל.

• **נציג המבקש:** מגיש הבקשה כאשר מדובר בהנפקת תעודה ליחיד או נציגו המוסמך של

¹ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

היחיד או נציג מוסמך (מורשה חתימה) של התאגיד או המוסד הציבורי כאשר מוגשת בקשה להנפקת תעודה למורשה בשם תאגיד או בשם מוסד ציבורי או מורשה חתימה אלקטרונית או מורשה גישה לדואר אלקטרוני מאובטח במערכת מגנא. יש לאמת את זהותו של הנציג המוסמך בהתאם לנהלים אלו.

1.4 שימוש בתעודה

1.4.1 שימושים מותרים בתעודה:

תעודה אלקטרונית המונפקת בהתאם למסמך נהלים זה, לחוק ולתקנות היא תעודה אלקטרונית כהגדרתה בחוק, היינו: "תעודה אלקטרונית שהנפיק גורם מאשר לפי הוראות פרק ד'".

תעודה האלקטרונית יכול שתונפק כתעודה ליחיד או כתעודה למורשה מטעם תאגיד או מוסד ציבורי. השימוש בתעודה נעשה באחריותו של בעל התעודה ונועד לשימושים חוקיים בלבד.

1.4.2 הגבלות על שימוש בתעודה:

הגבלות על שימושים בתעודה לפי סעיף 19(8) לחוק יכולות להיקבע על ידי קומסיין בהתאם לסעיף 21(ב) לחוק, בהתאם להוראות כל דין, או לפי בקשה מפורשת של בעל התעודה בלבד באופן שיקבע באישור הרשם או בהתאם לאישור שהופק על ידי רשות ניירות ערך במערכת מגנא. הגבלות כאמור יופיעו בתעודה בשדה Certificate Policies. ככל שהתעודה איננה כוללת מגבלות על שימוש מותר, ניתן לעשות בתעודה כל שימוש חוקי.

בעלי התעודות בלבד אחראים לשימוש הנעשה על ידם או מטעמם בתעודות המונפקות על פי נהלים אלה, בכל תחום שיפוט בו עשויים להשתמש בתוכן התעודה או לצפות בו. לפיכך, מבקשים ובעלי תעודות צריכים להיות מודעים לקיומם של חוקים שונים בעניין העברת נתונים, ובמיוחד הצפנת נתונים, ולכך שחוקים אלה עשויים להיות שונים זה מזה באופן משמעותי ממדינה למדינה. בנוסף, על פי רוב, אין אפשרות להגביל את הפצת התוכן באינטרנט או ברשתות מסוימות אחרות שמבוססות על מיקומו של המשתמש/הצופה. דבר זה עשוי לדרוש ממבקשים ומבעלי תעודות לציית לחוקים של כל תחום שיפוט בו ניתן לצפות בתוכן התעודות או להשתמש בו.

1.5 מדיניות ונהלים

1.5.1 האחראי על יישום המדיניות והנהלים:

הגוף האחראי בקומסיין על יישום מסמך הנהלים הוא פורום האבטחה.

1.5.2 איש קשר:

האחראי על יישום המדיניות והנהלים בקומסיין הוא מנהל האבטחה. דוא"ל: security@comsign.co.il כתובת למשלוח דואר: קומסיין בע"מ, קריית עתידים, בנין 4, קומה 11 ת.ד. 58007, תל-אביב 61580 טל: 03-6443620, פקס: 03-6491092. מידע בנושא חתימה אלקטרונית מאושרת והדרכה ניתן לקבל מקומסיין לאחר פניה לדואל: support@comsign.co.il. סיוע נוסף ניתן לקבל מנציגי שירות הלקוחות של קומסיין, בדואל customer_services@comsign.co.il, טל: 03-6443620, פקס: 03-6491092.

1.5.3. הממונה על התאמת הנהלים למדיניות הגורם המאשר :

מנהל הגורם המאשר הוא הגורם הממונה על התאמת הנהלים למדיניות הגורם המאשר.

1.5.4. אישור הנהלים :

נהלים אלה נערכו בהתאם לחוק חתימה אלקטרונית ותקנותיו ואושרו לפי החוק על-ידי הרשם שהינו הסמכות הרגולטורית לעניין זה במשרד המשפטים בישראל בהתאם לסעיף 10 לתקנות חתימה אלקטרונית (גורם מאשר) (ראה הגדרות להלן).
פרטים נוספים ודרכי התקשרות לרשם ניתן למצוא בכתובת :

<http://www.justice.gov.il/Units/ilita/subjects/HatimaElectronic/Pages/OdotRasamGormimMeaasrim.aspx>

אישור הרשם למהדורה זאת של מסמך הנהלים מופיע בכותרת לנהלים אלה.

1.6. הגדרות ומונחים

למונחים המפורטים להלן תהא בנהלים אלה המשמעות המופיעה לצדם. מונחים המוגדרים בחוק ובתקנותיו יפורשו בהתאם לחוק ולתקנותיו :

אמצעי חתימה
תוכנה, חפץ או מידע ייחודיים הדרושים להפקת חתימה אלקטרונית מאובטחת. אמצעי חתימה משמש להפקת חתימה אלקטרונית מאושרת. אמצעי החתימה הינו ייחודי לבעליו, נשמר בסוד על ידי בעליו, וידוע גם כ"מפתח פרטי" בשיטת הצפנת מפתח ציבורי.

אמצעי לאימות חתימה
תוכנה, חפץ או מידע ייחודיים הדרושים על מנת לזהות שחתימה אלקטרונית מאובטחת הופקה באמצעי חתימה מסוים. אמצעי אימות החתימה הינו בעל קשר חד ערכי לאמצעי החתימה, וידוע גם כ- "מפתח ציבורי" בשיטת הצפנת מפתח ציבורי. אמצעי אימות החתימה מסוים משמש כאמצעי לזהות שחתימה אלקטרונית מאובטחת הופקה באמצעות אמצעי החתימה מסוים. ניתן להעמיד את אמצעי אימות החתימה לרשות הציבור לצורך בדיקה זו.

בעל תעודה
מבקש שהונפקה לו תעודה אלקטרונית מאושרת.

הרשמה
ההליך במסגרתו מגיש מבקש (כהגדרתו להלן) בקשה להנפקת תעודה אלקטרונית.

החוק
חוק חתימה אלקטרונית, התשס"א – 2001.

התקן או התקן חומרה
כרטיס חכם, טוקן, HSM או כל רכיב חומרה אחר המשמש ליצירת ולשמירת אמצעי החתימה.

חתימה אלקטרונית או
חתימה אלקטרונית מאושרת כהגדרתה בחוק (כהגדרתו לעיל).

חתימה אלקטרונית

מאושרת

מאגר קומסיין

בסיס נתונים של קומסיין המכיל מידע זמין לציבור הרחב ובין היתר מסמך הנהלים ורשימות תעודות מבוטלות כפי שמתפרסמות באתר קומסיין.

מאגר קומסיין כולל גם מידע נוסף שאינו זמין לכלל הציבור, למשל מאגר התעודות התקפות.

מבקש

אדם או תאגיד או מוסד ציבורי המגישים בקשה להנפקת תעודה אלקטרונית כמפורט בפרק 4 להלן.

צד מסתמך

צד ג' המקבל מסר חתום בחתימה אלקטרונית מאושרת והעושה או נמנע לעשות על יסוד חתימה אלקטרונית מאושרת ו/או על יסוד המידע המצוי במאגר קומסיין.

מפתחות (פרטי)

ציבורי או צמד

מפתחות

מפתח פרטי והמפתח הציבורי הקשור אליו קשר חד ערכי בהתאם לשיטות הצפנה מקובלות, כנדרש לפי החוק במסגרת שיטת הצפנת מפתח ציבורי.

הנהלים או נהלים אלה

הנהלים המפורטים להלן להסדרת פעילותה של קומסיין כגורם מאשר לפי החוק (כהגדרתו לעיל) ותקנותיו. נהלים אלה חלים אך ורק על התעודות (כהגדרתן להלן).

נציג קומסיין

גוף חיצוני לקומסיין אשר מונה על-ידי קומסיין כגורם רושם, באישור רשם הגורמים המאשרים, לצורך ביצוע פעולות של הרשמת מבקשים וזיהויים וטיפול בבקשות להנפקת תעודה אלקטרונית, ואשר מינויו אושר על-ידי רשם גורמים מאשרים.

צדדים

קומסיין, נציגיה והמשתמשים בתעודות, דהיינו, בעל התעודה והמסתמך.

הרשם או רשם גורמים

מאשרים

רשם גורמים מאשרים שמונה לתפקידו בהתאם לחוק.

תעודות או תעודות

אלקטרוניות

תעודות אלקטרוניות מאושרות כהגדרתן בחוק, המונפקות על-ידי קומסיין והעומדות בדרישות החוק ותקנותיו. יצוין כי קומסיין מנפיקה תעודות נוספות מסוגים שונים אשר אינן עומדות בדרישות החוק ותקנותיו אך מתאימות למטרות ולצרכים שונים. נהלים אלה חלים אך ורק על התעודות כהגדרתן לעיל. על התעודות הנוספות שמנפיקה קומסיין חלים נהלים שונים בהם ניתן לעיין ב- <http://www.comsign.co.il/cps> וכן לפנות ולבקש פרטים לגביהן.

תעודה בטלה

תעודה המופיעה ברשימת התעודות המבוטלות (CRL) במאגר קומסיין.

תעודה תקפה

תעודה אשר מופיעה ברשימת התעודות התקפות במאגר קומסיין כתעודה תקפה. מאגר זה איננו פתוח לעיון הציבור.

תקנות

תקנות שהותקנו מכוחו של החוק.

תקנות חתימה

אלקטרונית (מערכות

חומרה ותוכנה)

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

תקנות חתימה

אלקטרונית (גורם

מאשר)

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

תקנות ניירות ערך

(מאשר חתימה)

תקנות המהוות חלק מחוק ניירות ערך ותקנותיו, המסדירות את פעולת הגורם המאשר בהתייחס לחתימה אלקטרונית מאושרת על גבי מסמכים ודיווחים למערכת מגנא שרשות ני"ע מעמידה לרשות החברות הציבוריות ואשר מחייבת אותן לדווח באמצעותה ובאמצעות חתימה אלקטרונית מאושרת.

תקנות ניירות ערך

(חתימה ודיווח

אלקטרוני)

תקנות המהוות חלק מחוק ניירות ערך ותקנותיו, המסדירות את דיווחי החברות (תאגיד מדווח) באמצעות מורשה חתימה אלקטרונית מטעמן למערכת מגנא שרשות ני"ע מעמידה לרשות החברות הציבוריות ואשר מחייבת אותן לדווח באמצעותה ובאמצעות חתימה אלקטרונית מאושרת.

תקנות ניירות ערך

(דואר אלקטרוני

מאובטח)

תקנות המהוות חלק מחוק ניירות ערך ותקנותיו, המסדירות את הגישה לתיבת דואר אלקטרוני מאובטח שרשות ני"ע מעמידה לרשות החברות הציבוריות במסגרת מערכת מגנא.

2. פרסום ומאגר מידע

מטרת פרק זה הינה סקירת הדרכים בהן קומסיין מפרסמת מידע רלוונטי לציבור הרחב, לצדדים מסתמכים, לבעלי תעודה ולמבקשים לפי העניין. הפרק כולל התייחסות לסוגי המידע המפורסם, תדירות הפרסום ואופן הגישה למאגר המידע של קומסיין.

2.1. המאגר של קומסיין

לצורך פעילותה קומסיין מנהלת אוסף בסיסי נתונים המיועדים לאחסון ולשליפה של תעודות ושל מידע אחר שקשור בהן, שיכוננו להלן ביחד המאגר. המאגר של קומסיין כולל, בין היתר, את מאגרי המשנה הבאים: מאגר תעודות אלקטרוניות תקפות (לרבות התעודה של קומסיין), מאגרי תעודות בטלות, מידע על ביטול תעודות ורשימות תעודות בטלות, ומידע אחר כפי שיוחלט על ידי קומסיין מעת לעת ובכפוף להנחיות הרשם. [בכל הקשור לתעודות שהונפקו לשרתי אינטרנט (שמות מתחם²) ראה סעיף 2.1 בנספח - (2)].

רק חלק מהמידע המפורסם במאגר של קומסיין פתוח לעיון הציבור הרחב. לעיון מבוקר פתוחה רשימת התעודות הבטלות המפרטת את מספרה הסידורי ותאריך ביטול התעודה. המאגרים של קומסיין רשומים אצל רשם מאגרי המידע בהתאם לחוק הגנת הפרטיות, התשמ"א – 1981, וקומסיין תפעל בהתאם ובכפוף לחוק זה.

2.2. פרסום מידע הנוגע לתעודות באמצעות המאגר של קומסיין

במסגרת המאגר של קומסיין, תפרסם קומסיין רשימה של תעודות בטלות, עדכונים לנהלים אשר אושרו על-ידי הרשם ומידע אחר באופן המתיישב עם נהלים אלה ועם הדין החל. המידע האמור יפורסם באתר, וביחס לעדכונים למסמך הנהלים יכלול מועד כניסה לתוקף. קומסיין מאפשרת גישה מרחוק לתעודות בדיקה של קומסיין (test certificates) במאגר של קומסיין. כתובות תעודות הבדיקה הן:

(1) תעודה למנוי בתוקף: <https://fedir.comsign.co.il/test.html>

(2) תעודה למנוי מבוטלת: <https://revoked.comsign.co.uk/test.html>

(3) תעודה למנוי שפקעה: <https://expired.comsign.co.uk/test.html>

[בכל הקשור לתעודות אלקטרוניות לאתרי אינטרנט ראה סעיף 2.2 בנספח³ - (3)]

2.3. תדירות ומועד הפרסום במאגר

קומסיין תפרסם רשימת תעודות בטלות חדשה לא יאוחר מאשר כל 12 שעות או מייד לאחר ביטול תוקף של תעודה, לפי המוקדם מביניהם. תוקף רשימת התעודות הבטלות שפורסמה הוא ל-24 שעות.

החרגה למשתמשי מגנא: הפירסום (שנעשה בדחיפה לשרתי מגנא) של רשימת תעודות בטלות

² נושא זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

³ נושא זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

חדשה הוא כל שעתיים ותוקף רשימת התעודות הבטלות שפורסמה הוא ל-24 שעות.

רשימת התעודות הבטלות המעודכנת והתקפה היא הרשימה המופיעה במאגר קומסיין. על צד מסתמך לערוך בדיקה מקוונת חדשה במאגר התעודות הבטלות בכל מועד בו הוא מבקש להסתמך על תעודה על מנת להבטיח כי בדיקתו נעשית אל מול רשימת התעודות הבטלות המעודכנת ביותר. שינויים במסמך הנהלים יפורסמו בסמוך לאחר אישורם על ידי הרשם.

2.4. בקרת גישה למאגר

ניתן להיכנס באופן חופשי לאזורי המאגר הפתוחים לקהל מאתר האינטרנט של קומסיין. כתובת הגישה למאגר התעודות הבטלות של קומסיין היא: <https://www.comsign.co.il/repository>. הגישה לחלקי מאגר אחרים חסומה למעט לבעלי תפקיד שאושרו לכך בהתאם לנהלי קומסיין.

3. זיהוי ואימות

מטרת פרק זה הינה לסקור את דרישת הנוכחות הפיזית של מבקש תעודה במעמד ההנפקה הראשונה, תהליך זיהוי ואימות מבקש התעודה, המסמכים שעליו להציג, אימות הבקשה, מקרים בהם תדחה הבקשה וכן הליכים לזיהוי בעל תעודה לצורך ביטול התעודה או הנפקה מחודשת.

מסמכי מקור המשמשים לזיהוי שאינם בשפה העברית או האנגלית יוצגו בצורך תרגום לשפה העברית או האנגלית כשהתרגום מאומת על ידי נוטריון ישראלי.

3.1. מתן שם

3.1.1. סוגי שמות:

שם בעל התעודה נקוב בתעודה בהתאם להוראות תקן X.509. ניתן להנפיק מספר תעודות אלקטרוניות שונות תחת אותו שם לאותו מבקש, בתפקידיו השונים. לדוגמא: מר ראובן פלוני יקבל תעודה אחת כמדוווח במגנא, שניה כספק של משרד הביטחון ושלישית כמדוווח למערכת מרכבה של משרד האוצר. בהתאם לדרישת הרשם, במקרה של ריבוי תעודות אלקטרוניות לבעל תעודה, אחד מחובתו ליידע את הגורם הרושם במועד הנפקת כל תעודה כי בידיו יותר מתעודה אחת, לציין את כמות התעודות שברשותו ולאשר כי הוזהר על הסיכונים הנובעים מריבוי תעודות אלקטרוניות וחובתו לקיים את הדרישות הנוגעות לשליטתו הבלעדית באמצעי החתימה השונים שברשותו.

במסגרת מערכת מגנא לא ניתן להנפיק למורשה חתימה אלקטרונית יותר מאשר תעודה אלקטרונית אחת לצורכי דיווח עבור תאגיד מדוווח אחד.

3.1.2. על שם בעל התעודה להיות בעל משמעות:

על שם בעל התעודה להיות בעל משמעות במובן זה שניתן לייחס אותו לאדם או לתאגיד/מוסד ציבורי ובאופן המונע טעות בזיהוי או בייחוס התעודה לבעליה.

3.1.3. שימוש בכינוי או הימנעות מציין שם:

קומסיין לא תנפיק תעודה אלקטרונית הנושאת כינוי של בעל התעודה ושאנינה נוקבת בשמו של בעל התעודה (תעודה אנונימית). יחד עם זאת רשאית קומסיין להוסיף, לבקשתו המפורשת ובכתב של בעל התעודה, את כינויו וזאת בסוגריים ובצמוד לשמו הפרטי הרשום במסמכי הזיהוי תוך ציון כי המדובר בכינוי.

[בכל הקשור להנפקת תעודות אנונימיות לשרתי אינטרנט⁴ ראה סעיף 3.1.3 בנספח - (4)].

3.1.4. הוראות למתן פירוש לסוגי שמות שונים:

על מנת לוודא כי המידע הכלול בתעודה הינו ייחודי לבעל התעודה, לרבות השימוש בשמות ייחודיים (Distinguished Names [DN]) ומייצג ערכים ייחודיים הניתנים לאימות בהתאם

⁴ חריג זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם

לתקנים בינלאומיים, עושה קומסיין שימוש בתקן X.500 על נגזרותיו השונות.

3.1.5. ייחודיות שם בעל התעודה:

התעודה מאפשרת זיהוי ייחודי של בעל התעודה באמצעות מסמן זהות ייחודי. לגבי יחיד, מספר תעודת הזהות שהוא נושא. לגבי תאגיד, מספר הרישום של התאגיד. ייתכן, במצבים מסויימים, שימוש במסמן זיהוי נוסף על מספר תעודת הזהות, כגון מספר רישיון מקצועי, מספר עוסק מורשה וכדומה.

3.1.6. מסירת מידע לצרכי זיהוי, אימות וסימני מסחר:

מבקשים ובעלי התעודות מתחייבים כלפי קומסיין ו/או נציגיה שהמידע והפרטים הנמסרים על ידם בבקשה להנפקת תעודה אינם פוגעים או מפריים זכויות של צדדים שלישיים כלשהם, בתחום שיפוט כלשהו, ביחס לסימני המסחר, סימני השירות, השמות המסחריים שלהם או כל זכות קניין רוחני אחרת, והם אינם מבקשים להשתמש בכל פרט המופיע בבקשה להנפקת תעודה למטרה בלתי חוקית כלשהי, לרבות, בין היתר, לגרם הפרת חוזה או התערבות אסורה אחרת ביחסים חוזיים, תחרות בלתי הוגנת, פגיעה במוניטין של אחר והטעיה של אדם, תאגיד או ישות משפטית אחרת כלשהי.

קומסיין ונציגיה לא יהיו אחראים לנתונים שנמסרו לקומסיין, לנציג קומסיין, או למאגר של קומסיין או שנמסרו בדרך אחרת על ידי המבקש או בעל התעודה לצורך הכנסתם לתעודה ואשר הכנסתם או עצם מסירתם מפרה הוראת חוק או זכות צד ג' כלשהו.

כתובות דואר אלקטרוני הנמסרות על ידי המבקש לצורך צרופן לתעודה אינן נבדקות על ידי קומסיין, לא לעניין תקינותן, לא לעניין שיוכן למבקש ולא לכל צורך אחר וההסתמכות עליהן או השימוש בהן הינם באחריותו של הצד המסתמך.

[בכל הקשור בבדיקת כתובות דואר אלקטרוני הנקובות בתעודות SSL⁵ – ראה סעיף 3.1.6 בנספח - (5)]

3.2. אימות זיהוי ראשוני של המבקש

3.2.1. הוכחת החזקה במפתח פרטי:

לא תונפק תעודה אלקטרונית למי שאיננו מחזיק במפתח פרטי המקיים את הדרישות הבאות:

(א) המפתח הפרטי מבוסס על תקן מקובל, העושה שימוש באחד מאלה:

(1) מפתח RSA או DSA באורך 1,024 סיביות לפחות;

(2) מפתח elliptic curve DSA באורך 160 סיביות לפחות;

(ב) להפעלת המפתח הפרטי, או לגישה אליו, נדרש שימוש באמצעים פיזיים או הצפנתיים

⁵ שירות זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם

(קריפטולוגיים) ייחודיים, העומדים ברמת אבטחה של תקן FIPS 140-2 רמה 1, ברמת ביטחון של תקן EAL2 common criteria לפחות ;

(ג) היתה הפעלת המפתח הפרטי כרוכה בשימוש בסיסמה, תעמוד הסיסמה בדרישות אבטחה ברמה הגבוהה לפי ת"י 1495 חלק 3, או בדרישות חלופיות שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה ;

הוכחת ההחזקה במפתח הפרטי מתבצעת בהסתמך על כך שחילול צמד המפתחות על ידי המבקש מתבצע במעמד הנפקת התעודה על ידי קומסיין על גבי התקן בו מאוחסן אמצעי החתימה לגבי תנפיק קומסיין תעודה אלקטרונית מאושרת. ככל שהתקן האחסון לא סופק על ידי קומסיין, קומסיין תנפיק תעודה אלקטרונית לבעלים של אמצעי החתימה בכפוף להמצאת הצהרת מבקש התעודה בכתב ובחתימת ידו כי אמצעי החתימה והתקן האחסון מקיימים את הדרישות המפורטות לעיל.

3.2.2. אימות זהות תאגיד:

זיהוי מבקש/מורשה מטעם תאגיד כמפורט בתת פרק זה יבוצע על ידי שני פקידי רישום מטעם קומסיין, בדרך של זיהוי פנים אל פנים בלבד של המורשה, וכמפורט להלן :

• **תאגיד הרשום בישראל :** על-פי תעודת הרישום, אישור של עו"ד על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עו"ד כאמור – על-פי אימות במרשמים המתאימים, וכן על-פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד, או אישור עו"ד על מורשה חתימה כאמור בנוסח שיפורסם באתר קומסיין מעת לעת באישור הרשם.

• **תאגיד שאינו רשום בישראל :** על-פי העתק מאושר ממסמך המעיד על רישומו, אישור של עו"ד על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עו"ד כאמור – על-פי אימות במרשמים המתאימים, וכן על-פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד או אישור של עורך דין על מורשה חתימה כאמור בנוסח שיפורסם באתר קומסיין מעת לעת באישור הרשם.

• **תאגיד פלסטיני הרשום ברשות הפלסטינית :** יזוהה כמו כל תאגיד שאינו רשום בישראל ובנוסף יזוהה מורשה החתימה מטעמו בהתאם לאמור בסעיף 3.2.2.1 להלן לגבי יחיד שהוא תושב הרשות הפלסטינית.

• **מוסד ציבורי :** על-פי הצהרת המבקש באמצעות מורשה החתימה שזוהה כפי שמזוהה יחיד תושב ישראל ובנוסף באמצעות המסמכים הבאים :

- (1) מסמך מזהה שהונפק לו על ידי המדינה אשר נושא את תמונתו ומספר תעודת הזהות ;
- (2) הצהרה בכתב של עובד המדינה כי הוא מורשה חתימה מטעם המוסד הציבורי ;
- (3) מסמך המאשר כי עובד המדינה הוא מורשה חתימה מטעם המוסד הציבורי ;

לעניין פסקה זו, "מוסד ציבורי" – משרדי ממשלה, רשויות מקומיות, וכן רשויות, תאגידים

או מוסדות אחרים שהוקמו בישראל בהתאם לחוק;

לעניין תאגידים (שרשומים או שאינם רשומים בישראל) ומוסדות ציבוריים – יזהה הגורם המאשר את מורשה החתימה כפי שמזוהה יחיד תושב ישראל או תושב חוץ, לפי העניין, כמפורט בסעיף 3.2.2.1 להלן.

לעניין תאגיד שאינו רשום בישראל או מוסד ציבורי – ונדרש "העתק מאושר" – הכוונה להעתק מתאים למקור המאומת בידי אחד מאלה:

- הרשות שהנפיקה את מסמך המקור;
- עורך דין בעל רישיון לעריכת דין בישראל;
- נציג דיפלומטי או קונסולרי ישראלי בחוץ לארץ.

בהנפקה עבור הרשות לני"ע יש לבצע זיהוי מול העתק אישור הרשות (טופס 301) שהתקבל קודם לכן בקומסיין. המבקש נדרש להגיע לגורם המאשר עם אישור הרשות (מקור) שהונפק על ידי הרשות על שמו בשם התאגיד המדווח.

הנפקה למבקש על גבי התקן רשתי תתאפשר למבקש שהוא תאגיד או מוסד ציבורי בלבד. כל הנפקה כאמור מותנית בציות להנחיות הרשם כפי שיפורסמו לגורם המאשר מעת לעת. מסמכי הבקשה מטעם התאגיד/המוסד הציבורי המבקש והמורשה מטעמו יוגשו על גבי טפסים בנוסח שאושר על ידי הרשם.

3.2.2.1. בכל הקשור לאימות זהות בהנפקת תעודה אלקטרונית לשרת הנושאת את

שם הארגון⁶ ראה סעיף 3.2.2.1 בנספח - (6)

3.2.2.2. בכל הקשור באימות שימוש בשם עסק/שם מסחרי בתעודה אלקטרונית

לשרת⁷ ראה סעיף 3.2.2.2 בנספח - (7)

3.2.2.3. בכל הקשור באימות ציון שם מדינה בתעודה אלקטרונית לשרת⁸ ראה סעיף

3.2.2.3 בנספח - (8)

3.2.2.4. בכל הקשור באימות הרשאה או שליטה בשם מתחם בתעודה אלקטרונית

לשרת⁹ ראה סעיף 3.2.2.4 בנספח - (9)

3.2.2.5. בכל הקשור באימות כתובת IP¹⁰ ראה סעיף 3.2.2.5 בנספח - (10)

⁶ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

⁷ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

⁸ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

⁹ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

¹⁰ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

3.2.2.6. בכל הקשור באימות שימוש בתו כללי בשם מתחם¹¹ ראה סעיף 3.2.2.6

בנספח - (11)

3.2.2.7. בכל הקשור בבחינת אמינות מקור המידע¹² ראה סעיף 3.2.2.7 בנספח - (12)

3.2.2.8. בכל הקשור בבדיקת מרשמי גורמים מאשרים מוסמכים (CAA Records)¹³

ראה סעיף 3.2.2.8 בנספח - (13)

3.2.3. אימות זהות של מבקש יחיד:

זיהוי מבקש יחיד כמפורט בתת פרק זה יבוצע על ידי שני פקידי רישום מטעם קומסיין, בדרך של זיהוי פנים אל פנים בלבד, וכמפורט להלן:

יחיד שהוא תושב ישראל: על פי תעודת זהות (כולל ספח) בצירוף אחד מהמסמכים הבאים (נדרשות 2 תעודות שונות, נושאות תמונה, על מנת לבצע את הליך הזיהוי):

(1) דרכון ישראלי תקף; או

(2) רישיון נהיגה ישראלי תקף עם תמונה; או

(3) תעודת מעבר, כהגדרתה בחוק הדרכונים התשי"ב-1952; או

(4) מסמך מזהה שמונפק על ידי המדינה לעובד המדינה או למי שמועסק על ידה או ממלא תפקיד מטעמה או שממלא תפקיד על פי דין לצורך ביצוע עבודתו או תפקידו כאמור, ובלבד שהמסמך נושא תמונה של המבקש ואת מספר הזהות שלו. לעניין זה, "עובד מדינה" - לרבות חייל, שוטר, סוהר, וכל נושא משרה או בעל תפקיד על פי חיקוק במוסד ממוסדות המדינה; או

(5) מסמך מזהה מסוג אחר המונפק בידי רשות ציבורית לפי דין, אשר הרשם אישר לצורך עניין זה, ובלבד שהמסמך נושא תמונה של המבקש ואת מספר הזהות שלו; או -

מסמך מזהה מסוג אחר שאישר הרשם, ובלבד שהמסמך נושא תמונה של המבקש ואת מספר הזהות שלו;

או -

לעניין מי שאין בידיו מסמך מזהה לפי פסקאות משנה (1)-(5) – תצהיר על העדר המסמכים המופיעים בפסקאות משנה (1)-(5) לעיל ובנוסף אישור של עו"ד על זהותו של המבקש ועל כך שהוא מכיר את המבקש אישית, בצירוף תמונתו של המבקש החתומה בידי עורך הדין, בהתאם לנוסח שיוורה הרשם.

בנוסף לבדיקת המסמכים תתבצע בדיקת מידע זה על פי מידע שהתקבל ממשד האוכלוסין

¹¹ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

¹² סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

¹³ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

במשרד הפנים (להלן: "**מרשם האוכלוסין**") הכולל את הפרטים דלקמן: מספר זהות של המבקש, שם משפחתו ושם משפחה קודם אם ישנו, שם פרטי, שם האב, שם האם, שנת לידה, תאריך הנפקת תעודה אחרון, סיבת הנפקת תעודה, מען נוכחי, אם ישנם – סטאטוס פטירה ותאריך פטירה;

יחיד שהוא תושב חוץ: על-פי דרכון חוץ או תעודת מסע או תעודת זהות, ובצירוף מסמך זיהוי נוסף הנושא תמונה של המבקש ופרטים מזהים שלו ושל מי שהנפיק את המסמך הנוסף (נדרשות 2 תעודות שונות, נושאות תמונה, על מנת לבצע את הליך הזיהוי).

יחיד שהוא תושב חוץ לצורך דיווח והזדהות מול מערכת "שער עולמי": על-פי נוהל זיהוי יחיד תושב חוץ ובנוסף על פי "מספר יישות" שהונפק לו על ידי רשות המיסים והשוואתו למידע שהתקבל קודם ההנפקה מרשות המיסים בהתאם לנוהל עבודה פנימי. מספר הזיהוי של יחיד תושב חוץ שיופיע בתעודה האלקטרונית יהיה "מספר היישות".

יחיד שהוא תושב הרשות הפלסטינית: לצורך הנפקת תעודה אלקטרונית לתושב הרשות הפלסטינית שאינו נושא תעודת זהות ישראלית תזזה קומסיין את המבקש לפי "יחיד שהוא תושב חוץ" למעט בהנפקה לצורכי "שער עולמי" שאז הזיהוי יתבצע על פי תעודת זהות פלסטינית או דרכון חוץ וכן על ידי כרטיס כר"ח¹⁴ שהונפק על ידי המינהל האזרחי באיו"ש והנושא תמונה של המבקש ופרטים מזהים שלו.

זיהוי מורשה חתימה בשם יחיד: על-פי בקשת מבקש יחיד המסמך את מורשה החתימה לפעול בשמו ועבורו ואישור עו"ד על מורשה חתימה כאמור בנוסח שיפורסם באתר קומסיין מעת לעת באישור הרשם. הגורם המאשר יזהה את מורשה החתימה כפי שמזוהה יחיד תושב ישראל או תושב חוץ לפי העניין, כמפורט בסעיף 03.2.2.1 לעיל.

3.2.4. מבקש שפרטיו לא אומתו:

קומסיין לא תנפיק תעודה אלקטרונית למבקש שזהותו ו/או זהות בעל התעודה אינם ניתנים לאימות או לא אומתו על ידה.

3.2.5. ווידוא הרשאה/הסמכה:

קומסיין לא תנפיק תעודה למורשה בשם תאגיד בלא לוודא אצל התאגיד כי המבקש הורשה על ידי התאגיד (או היחיד בהתאם לעניין) לפעול בשמו וכי המורשה הוסמך כדין על התאגיד לפעול ולחתום בשם התאגיד. הוראה זאת לא תחול בהנפקת תעודות אלקטרוניות למערכת מגנא וקומסיין תסתפק באישור הרשות (טופס 301). תאריך האישור לא יכול שיעלה על 3 חודשים קודם מועד הנפקת התעודה האלקטרונית, אלא באישור מנהל הגורם המאשר או מי מטעמו שהוסמך לצורך זה.

3.2.6. קריטריונים להסתמכות על תעודות אלקטרוניות מארגונים חיצוניים:

¹⁴ אמצעי זיהוי ביומטרי על גבי כרטיס חכם המונפק על ידי המינהל האזרחי באיו"ש. הכרטיס מכיל מידע מודפס אודות בעל הכרטיס, תמונה, ברקוד, פס מגנטי ושבב אלקטרוני המכיל פרטי זהות התושב והמזהים הביומטריים של טביעת האצבעות שלו.

קומסיין מבצעת ומנהלת את ההנפקות במסגרת מערכת ההנפקות של קומסיין בלבד ואינה מסתמכת על הנפקות שבוצעו על ידי ארגון חיצוני כלשהו.

3.3. זיהוי ואימות בקשות לחידוש תעודה אלקטרונית

3.3.1. זיהוי ואימות במקרה של חידוש תעודה ללא ייצור אמצעי חתימה חדש לבקשת מבקש בטרם

פג תוקף תעודתו:

קומסיין תציע שירות של חידוש מרחוק של תעודה אלקטרונית שהונפקה על ידיה לבעל תעודה בטרם פג תוקפה בין ביוזמתה ובין על-פי בקשתו הטלפונית של בעל התעודה. פניית חידוש טלפונית של בעל התעודה חייבת להתבצע בטווח זמן של בין יום אחד (1) לששים (60) ימים קודם תאריך פקיעת תוקף התעודה. פניה טלפונית יזומה של קומסיין לבעל התעודה יכולה להתבצע עד 24 שעות לפני מועד הפקיעה.

חידוש תעודות אלקטרוניות למערכת מגנא קודם פקיעתן לא יחייב אישור מחודש של הרשות (טופס 301) ויתבצע במהלך שלושים (30) הימים קודם תאריך פקיעת תוקף התעודה.

החידוש מותנה בביצוע זיהוי בעל התעודה באמצעות שאלת זיהוי, אימות פרטי הזיהוי הרשומים בקומסיין ואימות פרטי התעודה האלקטרונית באמצעות הזדהות כלפי ההתקן עליו מותקנת התעודה. במקרה שהליך החידוש מרחוק נכשל או שאינו פועל מסיבה כלשהי עד מועד תום תוקף התעודה המוחלפת, תבוצע הנפקה חדשה לפי הליך הרישום המלא והרגיל, לרבות זיהוי המבקש כפי שמבוצע ביחס לכל הנפקה ראשונה של תעודה אלקטרונית.

3.3.2. זיהוי ואימות לצורכי חידוש לאחר ביטול התעודה האלקטרונית:

לא ניתן לחדש תעודה אלקטרונית לאחר שבוטלה ויש צורך לבצע הנפקה חדשה בנוהל זיהוי מלא.

3.4. אימות זיהוי בקשה לביטול תעודה

קומסיין תבטל תעודה על פי בקשה של בעל תעודה מייד לאחר קבלת הבקשה ולאחר שתאמת כי האדם המבקש את הביטול הוא אכן בעל התעודה או המורשה מטעמו. פעולת ביטול התעודה תתבצע על ידי שני פקידים לפחות. זיהוי בעל התעודה/המורשה המבקש לבטל את התעודה האלקטרונית שלו יבוצע באחת מהדרכים הבאות:

- באמצעות קוד הזיהוי אותו קבע בעל התעודה/המורשה בעצמו בעת הגשת הבקשה להנפקת התעודה. נציג קומסיין יוודא את אמיתות קוד הזיהוי באמצעות הקלדת הקוד למערכת הרלבנטית וקבלת חיווי "נכון"/"לא נכון".
- אם בעל התעודה/המורשה לא קבע קוד זיהוי או איננו זוכר אותו, נציג קומסיין ו/או מי מטעמה יתקשר לטלפון שבעל התעודה/המורשה ציין בבקשה להנפקת תעודה לצורך בירור אם אכן בעל התעודה/המורשה הוא המבקש את ביטולה ויאמת את פרטי מבקש ביטול התעודה על פי הפרטים האישיים אותם הזין בעת בקשת התעודה לרבות תשובות לשאלות זיהוי שניתנו על ידי בעל התעודה/המורשה במעמד ההנפקה.
- קומסיין תבטל תעודה שהונפקה למורשה חתימה בתאגיד או במוסד ציבורי או לחבר

בארגון או בגוף מוסדי אחר או למורשה בשם יחיד, לפי בקשת התאגיד, המוסד הציבורי, הארגון או הגוף המוסדי או היחיד שבשמו הוסמך לפעול. בקשת הביטול תימסר על ידי מי שהוסמך לכך על ידי התאגיד או המוסד הציבורי, הארגון או הגוף המוסדי ו/או על ידי היחיד במקרה של מורשה בשם יחיד ו/או בהתאם להסדר שנקבע בהסכם המנוי ובטפסי הבקשה להנפקת תעודה. מובהר כי ביחס למוסד ציבורי כהגדרתו בסעיף 3.2.2 לעיל תבטל קומסיין את התעודה שהונפקה למורשה מטעם המוסד הציבורי רק לאחר שזיהתה את מבקש הביטול (שאיננו המורשה) כפי שמזוהה יחיד תושב ישראל ובנוסף באמצעות המסמכים הבאים :

(1) מסמך מזהה שהונפק לו על ידי המדינה אשר נושא את תמונתו ומספר תעודת הזהות ;

(2) הצהרה של עובד המדינה כי הוא מורשה חתימה מטעם המוסד הציבורי

(3) מסמך המאשר כי עובד המדינה הוא מורשה חתימה מטעם המוסד הציבורי ;

בקשת ביטול של תעודה אלקטרונית למערכת מגנא יכול ותוגש גם על ידי רשות ניירות ערך

4. דרישות תפעוליות במחזור חייה של תעודה אלקטרונית

מטרת פרק זה הינה לפרט את תהליך הנפקת התעודה, משלב הגשת הבקשה והמסמכים הנדרשים, עובר בהליך ההנפקה הלוגי וכלה בהנפקת התעודה. בנוסף כולל הפרק הסבר על הליך חידוש וביטול התעודה, לרבות מי רשאי להגיש בקשות ביטול וחידוש. בפרק זה מפורטות גם החובות המוטלות על בעל תעודה אלקטרונית.

הליך הנפקת התעודה האלקטרונית יבוצע על ידי שני פקידים לפחות של הגורם המאשר.

יובהר כי ההנפקה על גבי שרת חתימות הינה בכפוף להנחיות הרשם בנושא זה.

4.1. בקשה להנפקת תעודת אלקטרונית

4.1.1. מי יכול להגיש בקשה לתעודה אלקטרונית:

יחיד או תאגיד (לרבות מוסד ציבורי), בין אם הוא תושב ישראל ובין אם הוא תושב חוץ, בעצמו או באמצעות מבקש שהוסמך על ידו לצורך זה, ובכפוף להמצאת המסמכים והאישורים הדרושים ועמידה בדרישות החוק והתקנות והוראות מסמך נהלים זה.

4.1.2. הליך הגשת הבקשה והחובות המוטלות במסגרתו:

קומסיין מפרסמת באתר האינטרנט שלה את הטפסים אותם יש להגיש במסגרת הבקשה לתעודה אלקטרונית. המבקש יכול, בתיאום מוקדם, למלא ולשלוח טפסים אלו למשרד קומסיין טרום הליך ההנפקה בפועל אולם עליו להגיע אישית למשרד קומסיין או למשרד מי מנציגי הרישום שלה להפעלת הליך הבקשה במועד שתואם. קומסיין רשאית, אך לא חייבת, לשלוח למבקש זימון או תזכורת למועד שתואם להנפקה, באופן ובאמצעים שקומסיין תמצא לנכון לעשות בהם שימוש באופן מידתי [הודעה טלפונית, מסרון (SMS) והודעת דואר אלקטרוני] ובלבד שאינם כוללים דבר פרסומי. הצעות לרכישת שירות או מוצר תישלחנה באמצעות הודעות דואר אלקטרוני, מסרונים (SMS) או הודעות טלפוניות רק באופן ובאמצעים שאושרו על ידי בעל התעודה במועד הגשת הבקשה או במועד מאוחר יותר.

מחובת המבקש להמציא לקומסיין מידע מלא, נכון ושלם הנדרש על ידה לצורך התחלת הליך ההנפקה. תאגידים, יחידים ומוסדות ציבוריים רשאים להגיש בקשה באמצעות מורשי חתימה.

בהנפקה ליחיד תושב ישראל ימסור המבקש את המידע והמסמכים הבאים:

(1) תעודת זהות וכן אחד מן המסמכים המזהים האלה, ובלבד שהם בתוקף:

(1) דרכון ישראלי;

(2) רישיון נהיגה ישראלי הנושא תמונה של המבקש;

(3) מסמך מזהה שמונפק על ידי המדינה לעובד המדינה, למי שממלא תפקיד או נושא משרה מטעמה או במוסד ממוסדות המדינה, או למי שממלא תפקיד על פי דין, לצורך ביצוע עבודתו או תפקידו כאמור, ובלבד שהמסמך נושא תמונה של המבקש

ואת מספר הזהות שלו; לעניין זה, "עובד המדינה" – לרבות חייל, שוטר וסוהר
מי שאין בידיו מסמך מזהה לפי פסקאות משנה (1) עד (3) והגיש תצהיר על כך, אחד
מאלה:

(1) תעודת מעבר, כהגדרתה בחוק הדרכונים, התשי"ב-1952, הנושאת תמונה של
המבקש;

(2) מסמך מזהה מסוג אחר שהרשם אישר לעניין זה ובלבד שהמסמך נושא תמונה של
המבקש ואת מספר הזהות שלו.

(3) אישור של עורך דין על זהותו של המבקש ועל כך שהוא מכיר את המבקש אישית
וכי הוא מודע לכך שאישורו נועד לתמוך בבקשה להנפקת תעודה אלקטרונית לפי
החוק, בצירוף תמונתו של המבקש החתומה בידי עורך הדין, בהתאם לנוסח שיוorra
הרשם.

(2) על מבקש המעוניין שהתעודה האלקטרונית שתונפק לו תישא על גביה את שם הנעורים
במקום שם המשפחה העדכני המופיע על גבי תעודת הזהות להודיע על כך לקומסיין
מראש ולהצטייד למעמד ההנפקה גם במסמך "תמצית רישום ממרשם האוכלוסין"
של רשות האוכלוסין וההגירה.

(3) כתובת: רחוב, עיר, מדינה, מיקוד, ארץ (המגורים).

(4) מספרי טלפון (של מקום המגורים).

(5) כתובת דואר אלקטרוני (כפי שנמסרת על ידי המבקש - אינה מאומתת).

(6) הסכם מנוי חתום.

(7) מידע אחר כפי שייקבע על ידי רשם הגורמים המאשרים ו/או הנדרש לפי החוק.

בהנפקה ליחיד תושב חוץ ימסור המבקש את המידע והמסמכים הבאים:

(1) דרכון תקף עם תמונה.

(2) תעודה רשמית נושאת תמונה.

(3) ביחס לסוחר פלסטיני לצורך הזדהות מול מערכת "שער עולמי" – על ידי תעודת זהות
פלסטינית או דרכון חוץ ובנוסף גם כרטיס כר"ח¹⁵

(4) ביחס לתושב זר (לרבות סוחר פלסטיני) לצורך דיווח והזדהות מול מערכת "שער
עולמי" גם את "מספר הישות" שהונפק לו על ידי רשות המיסים.

(5) כתובת: רחוב, עיר, מדינה, מיקוד, ארץ (המגורים).

(6) מספרי טלפון (של מקום המגורים).

¹⁵ אמצעי זיהוי ביומטרי על גבי כרטיס חכם המונפק על ידי המינהל האזרחי באיו"ש. הכרטיס מכיל מידע מודפס אודות בעל הכרטיס, תמונה, ברקוד, פס מגנטי ושבב אלקטרוני המכיל פרטי זהות התושב והמזהים הביומטריים של טביעת האצבעות שלו.

- (7) כתובת דואר אלקטרוני (כפי שנמסרת על ידי המבקש - אינה מאומתת).
- (8) הסכם מנוי חתום.
- (9) מידע אחר כפי שייקבע על ידי רשם הגורמים המאשרים ו/או הנדרש לפי החוק.
- בהנפקה למורשה של תאגיד ימסור המבקש את המידע והמסמכים הבאים:
- (1) תעודת רישום התאגיד.
 - (2) אישור עו"ד על קיום התאגיד (הכולל את שמו ומספרו) (תעודת הרישום איננה מספיקה שכן ייתכן והתאגיד חוסל בינתיים).
 - (3) העתק מאושר של החלטת הארגון המוסמך בתאגיד בדבר היות המבקש מורשה חתימה מטעם התאגיד או אישור עו"ד על מורשה חתימה כאמור.
 - (4) כל המידע והמסמכים הדרושים להנפקה ליחיד לצורך אימות זהות המורשה.
- בהנפקה למורשה של מוסד ציבורי (משרדי ממשלה, רשויות מקומיות, וכן רשויות, תאגידים או מוסדות אחרים שהוקמו לפי חיקוק):
- (1) מסמך רשמי המכיל את פרטי תיק הניכויים של המוסד.
 - (2) מסמך רשמי ומאושר על ידי נושא משרה בכירה במוסד המסמך אותו לפעול בשם המוסד.
 - (3) הצהרה של עובד המדינה כי הוא מורשה חתימה מטעם המוסד הציבורי בנוסח שנקבע על ידי הרשם.
 - (4) כל המידע והמסמכים הדרושים להנפקה ליחיד לצורך אימות זהות המורשה.
- בהנפקה למורשה של תאגיד או מוסד ציבורי שאיננו רשום בישראל:
- (1) העתק מאושר של תעודת רישום התאגיד.
 - (2) אישור עו"ד על קיומו של התאגיד (כולל את שמו ומספרו) העתק מאושר של החלטת הארגון המוסמך בתאגיד בדבר היות המבקש מורשה חתימה מטעם התאגיד או אישור עו"ד על מורשה חתימה כאמור.
 - (3) כל המידע והמסמכים הדרושים להנפקה ליחיד לצורך אימות זהות המורשה.
- בהנפקה למורשה של תאגיד פלסטיני הרשום ברשות הפלסטינית:
- יזוהה כמו כל תאגיד שאינו רשום בישראל ובנוסף תאומת זהות מורשה החתימה מטעמו שהינו תושב הרשות הפלסטינית בהתאם לאמור לעיל לגבי יחיד שהוא תושב הרשות הפלסטינית.
- בהנפקה למערכת מגנא:
- יזוהה באופן ובהתאם למסמכים הדרושים לזיהוי מבקש יחיד ובנוסף נדרש אישור (מקור) של טופס אישור הנפקה (טופס 301) של רשות ניירות ערך הכולל מספר מזהה אותו יש לציין בתעודה האלקטרונית.

"העתק מאושר" של מסמך לצורך סעיף זה הינו העתק שאושר על-ידי אחד מאלה:

(1) הרשות שהנפיקה את מסמך המקור.

(2) עו"ד בעל רישיון לעריכת דין בישראל.

(3) נציג דיפלומטי או קונסולארי ישראלי בחוץ לארץ.

4.1.3. הגשת בקשה לתעודה לשרת אינטרנט¹⁶ - ראה סעיף 4.1.3 בנספח - (14)

4.2. עיבוד הבקשה להנפקת תעודה אלקטרונית

4.2.1. ביצוע פעולות זיהוי ואימות:

הזיהוי יבוצע על ידי פקיד זיהוי ואימות הזיהוי יבוצע על ידי פקיד אימות. פקיד הזיהוי יזהה את המבקש בהתאם לדרישות החוק ותקנותיו ויחתימו על טופס הבקשה והסכם המנוי. פקיד האימות יציג בפני המבקש טופס מידע ואזהרה בנוסח שאושר על-ידי הרשם בדבר הסיכון הכרוך בשימוש בחתימה אלקטרונית והחובות המוטלים עליו ויחתימו על הצהרה כי הוזהר כאמור לעיל, בהתאם לתקנה 11(ג)(3) לתקנות רישום וניהול.

4.2.1.1. ביצוע פעולות זיהוי ואימות של בקשה לתעודה לשרת אינטרנט¹⁷ - ראה סעיף

4.2.1.1. בנספח. Error! Reference source not found.

4.2.2. אישור או דחיית הבקשה:

הושלם הליך הזיהוי, נבדקו כל המסמכים ונמצאו מלאים, תקינים וחתומים והתקיימו הדרישות הטכנולוגיות להנפקה, תועבר הבקשה למחשב ההנפקה של קומסיין. לא התקיימה מי מהדרישות האמורות, יופסק ההליך עד להשלמת/תיקון החסר/הטעון תיקון. הופסק הליך ההתקנה – יינתן על כך הסבר למבקש במעמד ההפסקה. קומסיין רשאית לסרב להנפיק תעודה למבקש כלשהו, מטעמים סבירים, כגון חשש לזהות לא נכונה, אי עמידת אמצעי החתימה בתקנות חומרה ותוכנה ו/או בהוראות הרשם, אי תשלום עבור השירות וכדומה מבלי לשאת בכל חבות או אחריות בגין הפסדים או הוצאות הנובעים מסירוב כאמור. עם סירובה של קומסיין להנפיק תעודה, קומסיין תחזיר למבקש התעודה ללא דיחוי את דמי ההרשמה ששילם, אם שילם, בגין התעודה.

קומסיין מנהלת מרשם של כל הבקשות להנפקת תעודות אלקטרוניות שנבדקו ונדחו על ידה כמו גם תעודות שבוטלו בנסיבות שמקורן בחשד לנכונות פרטים שנמסרו על ידי מבקש התעודה. המרשם הוא פנימי ומשמש את קומסיין בלבד כחלק מהליך בדיקת הבקשות.

4.2.2.1. אישור או דחיית בקשה להנפקת תעודה לשרת אינטרנט¹⁸ - ראה סעיף 4.2.2.1

¹⁶ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

¹⁷ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

¹⁸ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

4.2.3. לוחות זמנים לעיבוד הבקשה:

מידע ומסמכים שנמסרו כחלק מהליך בדיקת ועיבוד הבקשה ייבדקו בסמוך למסירתם לקומסיין. בקשה שנמסרה לקומסיין על ידי המבקש באופן אישי, ביחד עם המסמכים הדרושים, במהלך שעות העבודה של קומסיין, תיבדק במעמד המבקש. בקשה שנבדקה ונמצאה תקינה – תועבר להנפקת תעודה בלא כל דיחוי ובלבד שהדבר מתאפשר במהלך שעות העבודה של קומסיין.

4.3. הנפקת תעודה אלקטרונית

4.3.1. פעולות הגורם המאשר במעמד ההנפקה:

על מנת להבטיח את זיהוי מבקש התעודה ולאמת את הקשר שבין המבקש לבין המפתח הציבורי שלו (אמצעי לאימות חתימה), קובעת תקנה 10 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) על יחידים ו/או מורשי חתימה של תאגידים המגישים בקשה לקבלת תעודה אלקטרונית בהנפקה ראשונה להופיע אישית בפני קומסיין ו/או מי מנציגיה.

ההנפקה תתבצע במעמד המבקש על ידי פקיד האימות.

פקיד האימות יציע למבקש התקן ליצירת ושמירת אמצעי החתימה והתעודה האלקטרונית שנבדק ואושר על ידי קומסיין. במידה והמבקש מעוניין לעשות שימוש בהתקן שלא סופק לו על-ידי קומסיין, תבדוק קומסיין כי המבקש מחזיק בידיו אמצעי להפקת חתימה אלקטרונית מאובטחת וכי באמצעי החתימה ובאמצעי לאימות חתימה המזהה את אמצעי החתימה האמור מתקיימות הוראות תקנה 8 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה). לצורך הבדיקה ידרש המבקש להציג בפני קומסיין את הפרטים והתיעוד הבאים:

- שם היצרן.
- שם מוצר/דגם.
- עותק של האישור שניתן להתקן על-ידי הגורמים הבאים: NIST ו/או Common Criteria.

לעניין קיום הוראות תקנות 8(1)(ב) ו-8(ג) לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) רשאית קומסיין להסתפק בהצהרה מטעם המבקש כי הוא מסר לקומסיין פרטים נכונים למיטב ידיעתו אודות אמצעי החתימה, אופן הפעלתו והגישה אליו. בהתאם להנחיית הרשם בנסיבות שבהן התקבלה הצהרה כאמור, קומסיין לא תהיה אחראית לבדיקות נוספות של אמצעי החתימה או לגבי השימוש השוטף בו, בכפוף לאופן חילול המפתח הפרטי כמוסדר בסעיף 4.5.1 להלן.

נתוני בעל התעודה יוזנו למערכת, המבקש יחולל את אמצעי החתימה (המפתח הפרטי) ואת האמצעי לאימות חתימה (המפתח הציבורי) באמצעות סיסמה הידועה לו בלבד. במקרה של הנפקת אמצעי חתימה על גבי התקן רשתי, תזון הסיסמה בשלב איתחול המחיצה בשרת בה יאוחסן אמצעי החתימה. במקרה זה, יזין המבקש את סיסמתו לצורך יצירת אמצעי החתימה (המפתח הפרטי) והאמצעי לאימות חתימה (המפתח הציבורי) ישירות על התקן החומרה ללא אפשרות לחשיפת הסיסמה ואמצעי החתימה לעובד קומסיין. במקרה של הנפקת אמצעי

חתימה על גבי התקן רשתי המאוחסן אצל צד ג', תזון הסיסמה בשלב איתחול המחיצה בשרת בה יאוחסן אמצעי החתימה. במקרה זה, יזין המבקש את סיסמתו לצורך יצירת אמצעי החתימה (המפתח הפרטי) והאמצעי לאימות החתימה (המפתח הציבורי) ישירות על התקן החומרה ללא אפשרות לחשיפת הסיסמה ואמצעי החתימה לעובד קומסיין.

פקיד האימות יוודא את תקינות המפתחות והתעודה והימצאותם על גבי התקן החומרה (בעזרת בעל התעודה) ויציע לבעל התעודה לבדוק את תקינותה מול מערכות רלוונטיות (נט המשפט, רשות ניירות ערך וכו').

במעמד ההנפקה יקבע בעל התעודה קוד זיהוי שישמש אותו, בין היתר, לביטול התעודה במקרה הצורך. קוד זה יוזן על ידי פקיד האימות למערכת שאינה מאפשרת שיחזור הסיסמה אלא רק מתן חיווי "נכון" או "לא נכון" עם הקשת קוד הזיהוי, ראה סעיף 3.4 לעיל כמו גם קוד לחידוש תעודה מרחוק, ראה סעיף 3.33.2.5 לעיל. פקיד האימות יפרט בפני בעל התעודה את נוהל ביטול התעודה.

פקיד האימות ימסור לרשות בעל התעודה את ההתקן ויסביר לו את החובה לשמור אותו בשליטתו. פקיד האימות יסביר לבעל התעודה על חשיבות שמירת ההתקן וכן חשיבות שמירת הסיסמה ו/או רכיב הגישה להתקן במקומות שמורים ובטוחים.

יובהר כי ההנפקה על גבי התקן רשתי הינה בכפוף להנחיות הרשם ובתנאים שייקבעו על ידו.

4.3.2. הודעה לבעל התעודה על ביצוע ההנפקה:

הנפקת התעודה (למעט תעודת SSL) תתבצע בנוכחות המבקש ומסירת התעודה לידי בעל התעודה או המורשה מטעמו תתבצע במעמד סיום ההנפקה.

4.4. קיבול התעודה האלקטרונית

4.4.1. התנהגות הנחשבת לקיבול:

מסירת התעודה מקומסיין לידי בעל התעודה תחשב לקיבול בין אם אישר בעל התעודה את קבלתה ובין אם לאו, ובלבד שהמסירה תועדה ברישומי קומסיין. שימוש בתעודה על ידי בעל התעודה ייחשב גם הוא כקיבול.

4.4.2. פרסום התעודה על ידי הגורם המאשר:

עם הנפקת התעודה, תרשום קומסיין את פרטי התעודה ברשימת התעודות התקפות שבמאגר קומסיין ובמאגרים נוספים, ע"פ החוק התקנות ובכפוף להוראות הרשם. הגישה למאגר התעודות התקפות מוגבלת בהתאם לנהלי העבודה הפנימיים של קומסיין. בעלי התעודות רשאים לפרסם את התעודות שלהם במאגרים נוספים.

4.4.3. מתן הודעה ליישומים אחרות מאת הגורם המאשר בדבר ההנפקה:

קומסיין רשאית, אך לא חייבת, להודיע לצדדי ג' מסוימים על הנפקת תעודה אלקטרונית.

4.5. צמד המפתחות והשימוש בתעודה

4.5.1. המפתח הפרטי של בעל התעודה והשימוש בתעודה:

על צמד המפתחות שיצר המבקש לעמוד בדרישות תקנה 8 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) כמפורט להלן: "החתימה האלקטרונית מופקת באמצעות מפתח המבוסס על תקן מקובל, העושה שימוש באחד מאלה: (1) מפתח RSA או DSA באורך 1024 סיביות לפחות; (2) מפתח Elliptic curve DSA באורך 160 סיביות לפחות". קומסיין מנפיקה ללקוחותיה מפתחות RSA באורך 2048 סיביות. ההתקן היוצר ושומר את אמצעי החתימה יכול ויסופק על ידי קומסיין ויכול ויסופק על ידי המבקש. קומסיין לא תנפיק למבקש תעודה אלקטרונית לאמצעי אימות החתימה שאינו עומד בדרישות החוק תקנותיו והוראות הרשם כמסודר בסעיף 4.3.14.2.1 לעיל.

קומסיין תעמוד על כך שהמפתחות ייוצרו במהלך ההנפקה ולא יתאפשר מצב שהמבקש יגיע להנפקה עם אמצעי חתימה אשר יוצר בהליך מקדמי כלשהו. זאת כדי למנוע אפשרות של החדרת מפתחות השייכים לזהות אחרת אל ההתקן. במהלך הליך הבירור לא ייחשף בפני קומסיין אמצעי החתימה של המבקש.

במעמד קבלת התעודה על בעל התעודה לבדוק כי הפרטים המפורטים בה נכונים בהתאם למידע שנמסר על ידו כקבוע בסעיף 4.1.2 לעיל. במידה ומתגלה טעות בפרטי התעודה, חייב בעל התעודה, על-פי הסכם המנוי, להודיע לקומסיין מיד כשנתגלה לו דבר הטעות ולבקש את ביטול התעודה. במקרה של אי התאמה במידע שנמסר על ידי המבקש טרם ההנפקה (בין בטופס הבקשה להנפקת תעודה ו/או בטופס הפרטים האישיים ו/או הסכם המנוי) תבטל קומסיין את התעודה ותנפיק לבעל התעודה תעודה חדשה בלא תוספת תשלום. בכל מקרה אחר תבוטל התעודה ובעל התעודה יחויב בתשלום מלא בגין הנפקת התעודה החדשה. מובהר כי ביטול תעודה שלא כתוצאה מתקלה שקומסיין אחראית לה לא יזכה את בעל התעודה בהחזר כספי, בין מלא ובין חלקי.

מחובתו של בעל התעודה בלבד, במהלך כל תקופת תוקפה של התעודה, לנקוט בכל האמצעים הסבירים לשם שמירה על אמצעי החתימה שלו ולשם מניעת שימוש בו ללא הרשאתו; למסור לקומסיין הודעה מיד כשיוודע לו על פגיעה בשליטתו באמצעי החתימה, ולהשתמש בתעודה באופן המתיישב עם נהלים אלה ועם הדין.

המורשה ו/או בעל התעודה מוזהרים בזאת כי אי שמירה על אמצעי החתימה של בעל התעודה עלול לאפשר שימוש בחתימתו האלקטרונית של בעל התעודה לצורך חיוב בעל התעודה, עריכת עסקאות, ויצירת מצגים בשם בעל התעודה ולצורך ביצוע כל פעולה אחרת שניתן לבצע באמצעות החתימה האלקטרונית באופן שעלול לגרום לנזקים רבים לבעל התעודה ו/או למסתמכים על התעודה. מכאן החשיבות הרבה לשמירת אמצעי החתימה ולהגנה עליו כמפורט בנהלים אלה, בחוק ובתקנותיו.

4.5.2. המפתח הציבורי והשימוש בו ובתעודה האלקטרונית על ידי צד מסתמך:

צד מסתמך חייב לבדוק את תוקף התעודה האלקטרונית המאושרת שהנפיקה קומסיין אם ברצונו לוודא (א) שהחתימה האלקטרונית נוצרה על ידי החותם ששמו מופיע בתעודה האלקטרונית; (ב) שהמסר האלקטרוני שנחתם לא שונה מאז יצירת החתימה האלקטרונית; ו-(ג) שהשימוש בתעודה לא נמנה על ההגבלות על השימושים המותרים בתעודה, ככל שישנן.

אימות אמצעי החתימה (המפתח הפרטי) באמצעותו חותם בעל התעודה האלקטרונית בחתימתו האלקטרונית מתבצע באמצעות המפתח הציבורי (אמצעי אימות החתימה). הבדיקה מתבצעת אל מול מרשם התעודות המבוטלות (CRL) המפורסם לציבור על ידי קומסיין ושקישור אליו מופיע בגוף התעודה האלקטרונית.

בהתאם לחוק, לתקנות ולהנחיות הרשם מפרסמת קומסיין באתר האינטרנט שלה שכתובתו www.comsign.co.il את רשימת אמצעי אימות החתימה שלה המשמשים להנפקת תעודות וכן את רשימות התעודות הבטלות הקשורות לאמצעי חתימה אלה.

מסתמך שלא בדק את תוקף התעודה מסתכן בהסתמכות על תעודה אלקטרונית שאינה תקפה ועלול לשאת באחריות על פי דין לנזקים שיגרמו כתוצאה מאי בדיקת תוקף התעודה האלקטרונית. קומסיין לא תהא אחראית לנזקים כלשהם שנגרמו עקב הסתמכות על תעודה בטלה אם הוכיחה כי נקטה בכל האמצעים הסבירים לקיום חובותיה על פי החוק ומסמך נהלים זה.

בעל התעודה וקומסיין רשאים להגביל את השימושים המותרים לפי התעודה בהתאם להוראת סעיף 19(8) לחוק. הגבלות על שימוש בתעודה לבקשת בעל התעודה יעשו לבקשתו המפורשת של בעל התעודה בלבד. אופן הבקשה יקבע באישור הרשם. הגבלות אלה נקובות בתעודה או כלולות בה בדרך של אזכור ומאפשרות להזהיר את בעלי התעודות והמסתמכים לגבי השימושים המותרים בתעודות והגבלות, ככל שישנן, על היקף השימושים הנ"ל. קומסיין לא תהא אחראית לנזק שנגרם עקב שימושים החורגים מההגבלות. מומלץ למסתמכים על תעודות אלקטרוניות של קומסיין לבחון את תוכן התעודה ולחפש אזהרות והגבלות אלה.

תעודה המונפקת עבור תאגיד או מוסד ציבורי או למורשה עבור יחיד מאשרת כי האדם הרשום בה הינו מורשה חתימה מטעם אותו תאגיד או מוסד ציבורי או היחיד בשמו הוא מוסמך לפעול, אולם היא איננה מהווה ראיה לסמכותו של מורשה החתימה לבצע פעולה מסוימת בשם התאגיד או המוסד הציבורי או היחיד. המסתמכים על מסרים חתומים בחתימה אלקטרונית מאשרת אחראים בלעדית לבצע בדיקת נאותות ולהפעיל שיקול דעת סביר כנדרש ביחס לחתימות רגילות בכתב יד קודם שישתמכו על תוכנם של אותם מסרים. תעודה מהווה ערובה של קומסיין רק כקבוע בחוק בתקנות ובנהלים אלה.

4.6. חידוש תעודה

4.6.1. הנסיבות לחידוש תעודה אלקטרונית:

תנאי לחידוש תעודה הוא היות התעודה המחודשת בתוקף במועד החידוש. לא ניתן לחדש תעודה שפקעה ותידרש במקרה זה הנפקה חדשה. קומסיין רשאית, אך לא חייבת, להודיע לבעל התעודה, באופן מידתי ובאמצעים שתימצא לנכון, לרבות בהודעה טלפונית, מסרון (SMS) והודעת דואר אלקטרוני, על מועד פקיעתה הצפוי של התעודה האלקטרונית שבבעלותו ועל הצורך בחידושה. ההודעה הנ"ל נועדה אך ורק לנוחות בעל התעודה בתהליך חידוש התעודה ואין במסירתה או באי מסירתה לבעל התעודה כדי לחייב את קומסיין ו/או להטיל עליה חבות ו/או אחריות מכל סוג שהוא הנובעים ו/או הקשורים לפקיעת תוקף

התעודה ו/או לאי חידושה. הודעה כאמור לא תכלול דבר פרסומת. הצעות לרכישת שירות או מוצר תישלחנה באמצעות הודעות דואר אלקטרוני, מסרונים (SMS) או הודעות טלפוניות רק באופן ובאמצעים שאושרו על ידי בעל התעודה במועד ההנפקה או במועד מאוחר יותר.

הודעות לחידוש תעודות למערכת מגנא תישלחנה לבעל התעודה ארבעים וחמישה ימים לכל המאוחר לפני מועד סיום תוקפה, בצרף הזמנה לחדש את תוקף התעודה בתקופת שלושים הימים שלפני מועד סיום תוקפה.

4.6.2. מי רשאי לדרוש חידוש של תעודה אלקטרונית:

החידוש יכול ויתבצע לבקשת בעל התעודה או לפי הוראת רשות מוסמכת או לפי דרישת קומסיין. האחריות לחדש את התעודה חלה על בעל התעודה בלבד.

4.6.3. אופן הטיפול בבקשות חידוש:

חידוש התעודה במהלך תקופת התוקף של התעודה המתחדשת יכול ויתבצע כמוסדר בסעיף 3.3.13.2.5 לעיל. במקרה כזה צמד המפתחות של בעל התעודה יישאר זהה גם במהלך תקופת ההארכת תוקפה של התעודה המחודשת.

במקרה בו הליך החידוש הנ"ל איננו זמין ו/או שהתעודה האלקטרונית של בעל התעודה בוטלה או שפג תוקפה או שבעל התעודה לא קבע סיסמה או איננו זוכר אותה, יבוצע רישום מחדש לפי הליך הרישום המלא והרגיל לרבות זיהוי המבקש כפי שמבוצע ביחס לכל הנפקה ראשונה של תעודה.

קומסיין שומרת לעצמה זכות לתקן ולעדכן נהלי חידוש התעודה, בכפוף לאישור הרשם. נהלי חידוש עדכניים מוצגים (עם פרסומם) בדרך של גרסה מתוקנת של הנהלים בכתובת האינטרנט: <http://www.comsign.co.il/cps/>

4.6.4. הודעה לבעל התעודה אודות החידוש:

הודעה בדבר החידוש תימסר לבעל התעודה במעמד החידוש וכחלק מנוהל החידוש. בנסיבות בהן לא מתבצע חידוש כי אם הנפקה חדשה יחולו הוראות סעיף 4.3.2 לעיל.

4.6.5. התנהגות הנחשבת לקיבול של תעודה אלקטרונית שחודשה:

שימוש בתעודה שחודשה על ידי בעל התעודה ייחשב כאישורו על מסירתה לחזקתו בכפוף לתנאי ההנפקה, החידוש והשימוש.

4.6.6. פרסום התעודה המחודשת על ידי הגורם המאשר:

חידוש תוקפה של התעודה מעודכן על ידי קומסיין, במועד החידוש, ברשימת התעודות התקפות שבמאגר קומסיין ובמאגרים נוספים, ע"פ החוק התקנות ובכפוף להוראות הרשם. הגישה למאגר התעודות התקפות מוגבלת בהתאם לנהלי העבודה הפנימיים של קומסיין. בעלי התעודות רשאים לפרסם את התעודות שלהם במאגרים נוספים.

4.6.7. מתן הודעה בדבר החידוש מאת הגורם המאשר ליישויות אחרות:

תעודות שחודשו במסגרת פרויקטים המחייבים מתן הודעה למפעילי הפרויקט, בין מכוח הוראת דין ובין מכוח התקשרות חוזית שמכוחה הונפקה התעודה האלקטרונית שחודשה, יפורסמו על ידי קומסיין למרשמים המנוהלים ומצויים בשליטת ופיקוח מפעילי הפרויקטים. בנסיבות בהן לא מתבצע חידוש כי אם הנפקה חדשה יחולו הוראות סעיף 4.4.3 לעיל.

4.7. החלפת צמד מפתחות לתעודה אלקטרונית (re-key)

מסמך נהלים זה איננו מאפשר החלפתו של צמד מפתחות לתעודה אלקטרונית בתוקף. בכל מקרה שבו נדרשת החלפת צמד המפתחות, למשל כתוצאה משינוי תקן, דרישות להגברת אבטחה או חשש מפריצה או אבדן שליטה במפתח הפרטי, בין בהוראת הרשם, בין ביוזמת הגורם המאשר ובין לבקשת בעל התעודה, תתבצע הנפקה של תעודה אלקטרונית חדשה ויחולל צמד מפתחות חדש במסגרת הליך ההנפקה.

4.7.1. הנסיבות להחלפת צמד מפתחות לתעודה אלקטרונית:

לא רלבנטי – ראה לעיל.

4.7.2. מי רשאי לדרוש החלפתו של צמד המפתחות של תעודה אלקטרונית:

לא רלבנטי – ראה לעיל.

4.7.3. אופן הטיפול בבקשות להחלפת צמד המפתחות:

לא רלבנטי – ראה לעיל.

4.7.4. הודעה לבעל התעודה אודות החלפת צמד המפתחות:

לא רלבנטי – ראה לעיל.

4.7.5. התנהגות הנחשבת לקיבול של תעודה אלקטרונית שצמד מפתחותיה הוחלף:

לא רלבנטי – ראה לעיל.

4.7.6. פרסום על ידי הגורם המאשר של התעודה שצמד מפתחותיה הוחלף:

לא רלבנטי – ראה לעיל.

4.7.7. מתן הודעה בדבר החלפת המפתחות מאת הגורם המאשר ליישויות אחרות:

לא רלבנטי – ראה לעיל.

4.8. ביצוע שינויים בתעודה

מסמך נהלים זה איננו מאפשר ביצוע שינוי או תיקון של תעודה בתוקף. בכל מקרה שבו נדרש תיקון או שינוי של התעודה או המלל המופיע בה, מכל סיבה שהיא, בין בהוראת הרשם, בין ביוזמת הגורם המאשר ובין לבקשת בעל התעודה, תתבצע הנפקה של תעודה אלקטרונית חדשה ויחולל צמד מפתחות חדש במסגרת הליך ההנפקה.

4.8.1. הנסיבות לשינוי תעודה אלקטרונית:

לא רלבנטי – ראה לעיל

4.8.2. מי רשאי לדרוש שינוי של תעודה אלקטרונית:

לא רלבנטי – ראה לעיל

4.8.3. אופן הטיפול בבקשות לשינויה של תעודה אלקטרונית:

לא רלבנטי – ראה לעיל

4.8.4. הודעה לבעל התעודה אודות שינוי התעודה:

לא רלבנטי – ראה לעיל

4.8.5. התנהגות הנחשבת לקיבול של תעודה אלקטרונית ששונתה:

לא רלבנטי – ראה לעיל

4.8.6. פרסום על ידי הגורם המאשר של התעודה ששונתה:

לא רלבנטי – ראה לעיל

4.8.7. מתן הודעה בדבר שינוי התעודה מאת הגורם המאשר ליישויות אחרות:

לא רלבנטי – ראה לעיל

4.9. ביטול והתליית תעודה אלקטרונית

4.9.1. הנסיבות לביטול תעודה אלקטרונית:

תעודה אלקטרונית, לרבות תעודת ביניים (Intermediate Certificate) תבוטל:

- לפי דרישה מאומתת של בעל התעודה או של המורשה מטעמו.
- אם נמסר לקומסיין על-ידי בעל התעודה, או נודע לה בדרך אחרת, כי אירע אירוע של גניבה, אובדן, שינוי, שימוש בלתי מורשה, אי עמידה בתקנים ובדרישות בחוק ובתקנות ביחס לאמצעי החתימה ואמצעי האימות של אמצעי החתימה, פגם או פגיעה אחרת באמצעי החתימה או בשליטתו של בעל התעודה באמצעי החתימה ובלבד שקומסיין השתכנעה במהימנות ההודעה.
- מיד כשנודע לקומסיין כי פרט מהפרטים המזהים את בעל התעודה המופיעים בתעודה אינו נכון, או כי נפגמה מהימנות התעודה בדרך אחרת ובלבד שקומסיין השתכנעה במהימנות ההודעה.
- מיד כשנודע לקומסיין על פגם בחתימתה האלקטרונית המאובטחת, או באמצעי החתימה שלה, או במערכות החומרה והתוכנה שלה, או באבטחת המידע של מערכות אלה באופן שיש בו כדי לפגוע במהימנות חתימתה או במהימנות התעודות האלקטרוניות שהיא מנפיקה.
- מיד כשנודע לקומסיין כי תעודה למורשה הונפקה בלא הרשאה בתוקף, כי בעל התעודה נפטר (אם מדובר באדם), או ניתן צו לפירוקו (אם מדובר בתאגיד) ובלבד שקומסיין השתכנעה

במהימנות ההודעה.

- הופסקה פעילותה של קומסיין כגורם המאשר בלא שפעילותה הועברה לגורם מאשר אחר או באם הדבר נדרש מקומסיין כדי למלא אחר הדרישות המופיעות בנהלים אלו.
- באם התגלה פגם מהותי בהליך הנפקת התעודה, בין אם מקור הפגם בקומסיין או במבקש או בכל גורם אחר המעורב בהליך ההנפקה.

4.9.1.1. הנסיבות לביטולה של תעודה אלקטרונית לשרת אינטרנט¹⁹ - ראה סעיף 4.9.1.1

בנספח - (17)

4.9.2. מי רשאי לדרוש ביטול של תעודה אלקטרונית:

בקשה לביטול תעודה תוגש על ידי בעל התעודה או מורשה או צד ג' אחר שהסמכה לכך ניתנה לו במפורש בהסכם המנוי או מכוח הוראת דין. כאשר המדובר בתעודה לתאגיד ו/או למורשה חתימה בשם תאגיד או מוסד ציבורי או למורשה של יחיד/עוסק מורשה, קומסיין תבטל תעודה לפי בקשת התאגיד, המוסד הציבורי, הארגון או הגוף המוסדי, הגורם שעבורו הונפקה התעודה למורשה או המורשה עצמו. בקשת הביטול תימסר על ידי מי שהוסמך לכך על ידי הגורם הזכאי לבטל את התעודה ו/או בהתאם להסדר שנקבע בהסכם המנוי ובטפסי הבקשה להנפקת תעודה.

פניה יכול ותבוא גם מגורם רושם לקומסיין בבקשה לביטול תעודה שהונפקה על ידי אותו גורם רושם ובתנאי שקיומה של אפשרות זו והעילות לביטול על ידי הגורם הרושם הובאו לידיעת בעל התעודה לפני הנפקתה ונכללו בהסכם המנוי של בעל התעודה.

קומסיין עצמה תיזום ביטול תעודה אלקטרונית מייד כשיוודע לה כי התקיימה נסיבה מהנסיבות המפורטות בסעיף 4.9.14.9.1.1 לעיל ושבהתקיימן על קומסיין לבטל את התעודה האלקטרונית.

4.9.3. אופן הטיפול בבקשות לביטולה של תעודה אלקטרונית:

בקשה לביטול תעודה תוגש על ידי המוסמך להגישה בין באופן טלפוני, בין בדואר אלקטרוני ובין בכתב. בקשת הביטול תטופל על ידי פקיד זיהוי בקומסיין. פקיד הזיהוי בקומסיין יאמת את זהות מבקש הביטול בהתאם לקבוע בסעיף 3.43.3.2 לעיל. במידה והאימות צלח – תבוטל התעודה על ידי אחראי רישום בקומסיין. בכל מקרה אחר – התעודה תושהה עד לבירור סופי של העניין בכפוף לנהלי העבודה הפנימיים של קומסיין. פעולת הביטול שתתבצע לא תהיה בשליטתו של אדם אחד בלבד.

4.9.4. מתן ארכה לבעל התעודה קודם לביטולה:

תעודה אלקטרונית שהתקיימו לגביה נסיבות המחייבות את ביטולה תבוטל לאלתר בלא מתן ארכה מכל סוג שהוא.

¹⁹ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

4.9.5. פרק הזמן העומד לרשות הגורם המאשר לביטול התעודה:

תעודה שיש לבטלה תבוטל לאלתר.

4.9.6. חובת בדיקת רשימת התעודות המבוטלות על ידי צד מסתמך:

מחובתו של צד מסתמך לבצע בדיקת תוקפה/תקינותה של תעודה אלקטרונית קודם ההסתמכות עליה. קומסיין מעמידה לרשות בעלי תעודות, המסתמכים וצדדים שלישיים את המאגר של קומסיין הכולל, בין השאר, רשימות של תעודות הכוללות את אמצעי אימות החתימה של קומסיין ורשימות של תעודות מבוטלות שניתן להגיע אליהן באמצעות כתובת האינטרנט: <https://www.comsign.co.il/repository>.

קישור לרשימת התעודות המבוטלות ניתן למצוא גם בגוף התעודה האלקטרונית. ראה סעיף 7.1.8 Error! Reference source not found. להלן כמו גם באתר האינטרנט של קומסיין.

הבדיקה חייבת להתבצע תמיד אל מול הרשימה המעודכנת ביותר שפורסמה של תעודות מבוטלות (CRL).

4.9.7. תדירות פרסום רשימת התעודות המבוטלות:

למעט הסדרים מיוחדים שמקורם בהתקשרות חוזית או בדרישת הדין, קומסיין תפרסם אחת ל-12 שעות רשימת תעודות בטלות (CRL) בתוקף ל-24 שעות. בוטלה תעודה על ידי קומסיין, תעודכן הרשימה בסמוך לביצוע הביטול.

CRL מעודכן יישלח לרשות לניירות ערך בהתאם לקבוע בחוק ני"ע ותקנותיו לגבי ביטול תעודה.

4.9.8. זמן אחזור מירבי של רשימת התעודות המבוטלות:

רשימת התעודות המבוטלות (CRL) זמינה בזמינות המירבית בכל עת. קומסיין מקפידה כי זמני האחזור יהיו מינימאליים בהיקף האפשרי המצומצם ביותר ובלא לגרוע מהיקף הזמינות המירבי האמור.

4.9.9. בדיקה מקוונת של סטטוס אישור התעודה (OCSP):

קומסיין מעמידה לרשות לקוחותיה בעלי תעודות אלקטרוניות מאושרות שירות המאפשר בדיקה של סטטוס התעודה האלקטרונית המאושרת באמצעות פרוטוקול מקוון לבדיקת סטטוס אישור התעודה (OCSP – Online Certificate Status Protocol).

תוצאות הבדיקה מקיימות אחר דרישת RFC6960 ו/או RFC5019 וחתומות על ידי קומסיין.

4.9.10. דרישות מבדיקה מקוונת של הביטול:

קיומו של קו תקשורת נתונים ייעודי או באמצעות האינטרנט. פירוט הדרישות ואיפיון במסגרת ההתקשרות הנפרדת בין קומסיין למנוי.

(1) קומסיין תומכת בשירות OCSP העושה שימוש בשיטת GET לתעודות מונפקות.

- (2) עבור הסטטוס של תעודות למנוי, קומסיין מעדכנת את המידע הזמין לגישה באמצעות OSCP לפחות אחת ל-4 ימים. תוקף המענה של שירות זה לעולם לא יעלה על 10 ימים.
- (3) עבור הסטטוס של תעודות ביניים, קומסיין מעדכנת את המידע הזמין לגישה באמצעות OSCP לפחות:
- a. כל 12 חודשים
 - b. בתוך 24 שעות מביטולה של תעודת ביניים
- (4) כאשר שרת ה-OCSP מקבל בקשה לבדיקת סטטוס של תעודה שלא הונפקה, התשובה שתינתן תהיה "unknown" (לא ידוע).

4.9.11. צורות פרסום אחרות של תעודות מבוטלות:

קומסיין פועלת בהתאם להוראת תקנה 15(ג) לתקנות חתימה אלקטרונית (גורם מאשר) לפיה רשימת התעודות הבטלות חייבת להיות זמינה באופן מקוון ומיידי לבדיקתו של מסתמך. כל צורת פרסום אחרת, כגון "דחיפת" ה-CRL למנוי לשירות תתאפשר, כמוסדר בתקנה 15(ד) לתקנות חתימה אלקטרונית (גורם מאשר), היינו בכפוף לאישור הרשם מראש ובכתב, או בהתאם להוראת דין. קומסיין רשאית לגבות תשלום בגין שירות זה. אין בהודעה על שינוי סטטוס כדי להוות תחליף לחובת הבדיקה של מאגרי התעודות הבטלות אלא אם הדבר נקבע לפי דין או בהסכם.

4.9.12. דרישות מיוחדות לביטול כתוצאה מאובדן שליטה בצמד המפתחות:

אובדן שליטה של בעל התעודה באמצעי החתימה (המפתח הפרטי) מחייב דיווח מיידי לקומסיין ובקשה לביטול התעודה האלקטרונית. קומסיין תבטל את התעודה מייד בסמוך לאחר קבלת ההודעה כמוסדר לעיל בנוהל הביטול הרגיל התואם את נסיבות הביטול ובלבד שקומסיין השתכנעה במהימנות ההודעה.

4.9.13. נסיבות המאפשרות התליית התעודה האלקטרונית:

כל נסיבה מכוחה יש לבטל תעודה (ראה סעיף 4.9.1 לעיל) תיחשב כנסיבה מכוחה ניתן להתלות את תוקף התעודה האלקטרונית. שיקול הדעת של הגורם המאשר באם להתלות את התעודה או לבטלה יותנה בנסיבות נוספות ובבקשת בעל התעודה או מי שהוסמך על ידו לבקש את התלייתה או ביטולה במסגרת הסכם המנוי. כך, למשל, היעלמות אמצעי החתימה בנסיבות שבהן סבור בעל התעודה כי בחיפוש סביר ניתן לאתרו, יכול וישמש נימוק סביר להתליית התעודה.

4.9.13.1. נסיבות המאפשרות התליית תעודה אלקטרונית לשרת אינטרנט²⁰ - ראה סעיף

4.9.13.1 בנספח - (17)(18)

4.9.14. מי רשאי לדרוש את התליית התעודה:

²⁰ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

הגורם הרשאי לדרוש את התליית התעודה הוא בעל התעודה או מי שהוסמך על ידו בהסכם המנוי לדרוש את ביטול התעודה או התלייתה.

4.9.15. אופן הטיפול בבקשת התלייה:

אופן הטיפול בבקשה להתליית תעודה אלקטרונית יהיה כמוסדר בסעיף 4.9.3 לעיל שעניינו אופן הטיפול בבקשה לביטול תעודה.

לאופן טיפול בבקשה להתליית תעודה אלקטרונית שהונפקה לשרת אינטרנט²¹ – ראה סעיף 4.9.15 בנספח – (19)

4.9.16. הגבלת משך תקופת ההתלייה:

התליית התעודה לא תעלה על פרק זמן בן 48 שעות שבסיומו תוסר ההתלייה או תבוטל התעודה. משך תקופת ההתליה יקבע בהתאם לנסיבות ובהתחשב בבקשת מבקש ההתליה. במהלך פרק זמן התליית התעודה תוכנס התעודה לרשימת התעודות המבוטלות (CRL).

4.10. שרותי בדיקת סטטוס תעודה אלקטרונית על ידי מסתמך

4.10.1. מאפיינים תפעוליים:

בדיקת סטטוס התעודה תתבצע על ידי המסתמך אל מול רשימת התעודות המבוטלות (CRL) באתר קומסיין.

4.10.2. זמינות השירותים:

שירות בדיקת סטטוס התעודה האלקטרונית יהיה זמין 24 שעות ביממה 7 ימים בשבוע. נפגעה זמינות השירותים מכל סיבה שהיא יפעל הגורם המאשר להשבת השירות בהקדם האפשרי. ראה גם סעיף 5.7 העוסק בהתאוששות ממצב אסון.

4.10.3. מאפיינים נוספים - שחרור מנעילה:

התקני חומרה כוללים אמצעי אבטחה לפיו הגישה להפעלת אמצעי החתימה מוגנת בסיסמה. בהתאם להנחיית הרשם יינעל התקן החומרה לאחר מספר נסיונות כושלים בהקשת הסיסמה. קומסיין תאפשר לבעלי התעודות קבלת שרות של שחרור הכרטיס מנעילה בלא שלקומסיין ניתנת אפשרות הגישה לאמצעי החתימה. זאת באמצעות מנגנון ייעודי שיאושר על ידי הרשם.

4.11. פקיעת תעודה אלקטרונית:

כל התעודות יכנסו לתוקף ביום ובשעת הנפקתן על ידי קומסיין. התעודה תהא בתוקף לפרק הזמן המופיע בהסכם המנוי ועל גבי התעודה, אלא אם תבוטל התעודה או תחודש קודם לכן.

²¹ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם

4.12. הפקדה בנאמנות (escrow) ואחזור מפתח פרטי

מסמך נהלים זה איננו מאפשר הפקדה בנאמנות של המפתח הפרטי ואחזורו.

4.12.1. מדיניות ונהלים להפקדת מפתח פרטי ואחזורו:

לא רלבנטי – ראה לעיל.

4.12.2. מאפייני מפתח שיחה (session key) ומדיניות ונהלי אחזור:

לא רלבנטי – ראה לעיל.

5. בקרות פיזיות, ניהוליות ותפעוליות

מטרת פרק זה הינה לסקור בפני המבקש, בעל התעודה והמסתמך את אמצעי הבקרה הפיזיים, אבטחת כוח האדם והגנה על רשומות בהם עושה קומסיין שימוש במסגרת פעילותה. בנוסף, ניתן בפרק זה תיאור של הרשומות אותן שומרת קומסיין וסוגי המידע המאוחסנים בהן.

קומסיין מיישמת מערכת אבטחה המבוססת על חומרת מחשבים, תוכנות ונהלי אבטחה. כל אלה מספקים רמה גבוהה של זמינות, אמינות ופעולה רציפה כמו גם מענה מספק כנגד סיכוני אבטחה.

על פי החוק והתקנות – חובה על קומסיין לעמוד בתקני אבטחה מחמירים ובבדיקות מכון התקנים הישראלי לקבלת תקני איכות. חברת קומסיין עומדת בתקן ישראלי 27001 אשר עוסק באבטחת מידע ועוברת ביקורות שנתיות של מכון התקנים הישראלי ושל מומחה מבקר אבטחה עצמאי.

נהלי העבודה הפנימיים של קומסיין, אשר עוברים בקרה ואישור של הרשם, כוללים, בין היתר, מדיניות אבטחה, הגנה על נכסים, אבטחת כח אדם, אבטחה פיזית, ניהול הפעילות, ניהול הגישה לתשתית החיתום של קומסיין, התחזוקה והמשכיות הפעילות במקרה אסון.

5.1. בקרות פיזיות

5.1.1. מבנה האתר ומיקומו:

המתקנים הקשורים בהנפקת תעודות ובניהול ביטולים פועלים בסביבה המגינה באופן פיזי על השירותים מפני פגיעה באמצעות גישה לא מורשית למערכות או לנתונים. קומסיין שומרת את חלקי המערכת החיוניים לפעילותה באתר מוגן ומאובטח, המונע חדירה וכניסה ללא הרשאה, בהתאם לאופי הפעילות של קומסיין ולהנחת דעתו של הרשם. ההגנה הפיזית מושגת באמצעות יצירת מחסומי אבטחה היקפית המוגדרים באופן ברור (כלומר מחסומים פיזיים) מסביב לשירותי הנפקת התעודות, הכנת ההתקנים וניהול הביטולים. כל חלק במתקן המשותף עם ארגון אחר ימצא מחוץ לשטח האתר המאובטח. ההגנה הפיזית מספקת מענה כנגד אסונות טבע, סכנת אש ונזקי מים, פגיעה בתשתיות תומכות כגון חשמל ותקשורת, קריסת מבנה, גניבה, פריצה וחדירה לא מאושרת.

5.1.2. גישה פיזית:

כל אדם אשר נכנס לאזור האתר המאובטח לא יישאר ללא פיקוח של אדם מוסמך. בקומסיין מוטמעות בקורות להגנה מפני הוצאה ללא רשות של ציוד, מידע, מדיות ותוכנה הקשורים בשירותי קומסיין כגורם מאשר. קומסיין מחזיקה מצאי של נכסי מידע ומקצה סיווג עבור דרישות ההגנה על הנכסים הללו, בהתאם לניתוח ניהול הסיכונים שהיא מבצעת. מנהל האבטחה מחזיק ברשותו רשימת מצאי של נכסים קריטיים ואופן ההגנה עליהם. נכסים אלו יכולים להיות נכסים פיסיים ו/או נכסי מידע לוגי.

5.1.3. חשמל ומיזוג אוויר:

מערכת אספקת החשמל ומיזוג האוויר כוללת אמצעים ובקורות לניטור סטיות ותקלות, ואספקה חלופית במקרי תקלה והפסקה בזרם החשמל לאתר המאובטח.

5.1.4. חשיפה לנזקי מים:

האתר המאובטח מנותק מרשת אספקת מים וננקטו אמצעי הגנה כנגד הצפות ונזקי מים למתקנים ולציוד.

5.1.5. הגנה מנזקי אש ומניעתם:

באתר מותקנות מערכות לאיתור וניטור אש וכיבוייה.

5.1.6. הגנת אמצעים לאחסון נתונים:

כל האמצעים לאחסון נתונים ממוקמים בתוך האתר המאובטח וכפופים להגנות הפיזיות ולבקרת גישה. מערכות הגיבוי מאוחסנות בנפרד ומוגנות אף הן באמצעים הנקוטים להגנה על אמצעי האחסון הראשיים.

5.1.7. מניעת אובדן מידע במסגרת פינוי אשפה:

קומסיין מיישמת נהלים ייעודיים המסדירים גריסה או השמדה פיזית של ניירת או מדיית קיבול הכוללת מידע סודי או מוגבל.

5.1.8. גיבוי מחוץ לאתר המאובטח:

קומסיין מיישמת מדיניות גיבוי מלא ומחזיקה במערכת התאוששות מאסונות הממוקמים בהפרדה פיזית ומיקומית מאתר הפעילות המאובטח של החברה. ראה סעיף 5.7 להלן.

5.2. בקורות ניהוליות

5.2.1. תפקידי אמון:

כל העובדים, הקבלנים והיועצים של קומסיין ו/או נציגיה אשר יש להם גישה אל, או שליטה על, פעולות רישום, הנפקה, שימוש, וביטול של תעודות מצד קומסיין, לרבות גישה לפעולות של המאגר של קומסיין שהגישה אליהן מוגבלת, ייחשבו, כממלאי תפקיד הדורש אמון מיוחד (להלן: "תפקיד אמון"). כוח אדם כאמור כולל, בין היתר, עובדי שירות לקוחות, עובדי ניהול מערכות, אנשי הנדסה ייעודיים ואנשי הנהלה שמתפקידם לפקח על תשתיות המערכת המהימנות של קומסיין. תפקידי האמון וההרשאות של כל בעל תפקיד אמון מפורטים בנהלי קומסיין. בעלי תפקידי האמון ממונים לתפקידם על ידי מנכ"ל קומסיין באישור מנהל האבטחה. בעלי תפקידי האמון בקומסיין מחויבים לסודיות ולמניעת ניגוד עניינים במסגרת ביצוע תפקידם בקומסיין.

בעלי תפקידי האמון פועלים במסגרת חוזה העסקה אישי שכולל פירוט התפקיד ומרכיביו, והתחייבות של כל עובד המוגדר כבעל תפקיד אמון כי הבין את מרכיבי התפקיד וכי הוא מתחייב לפעול על פי החוק, התקנות, הנהלים וחוזה העסקה.

קומסיין מוודאת כי לא יתקיים ניגוד אינטרסים אצל כל אנשי הסגל בתפקידי האמון וכי לא מתקיימת חפיפה בזהות אנשי הסגל הנושאים בתפקידי האמון. התפקידים המוגדרים בקומסיין כתפקידי אמון הינם: מנכ"ל קומסיין, מנהל אבטחה האחראי על יישום נהלי האבטחה, פקיד זיהוי, פקיד אימות, מנהלי מפתחות ומחזיקי מפתחות, מחזיק מפתחות לכספת, אחראי רישום ובוחן לוגים.

לכל תפקיד ישנן הגבלות גישה פיסיות ולוגיות שהינן נגזרות מהחוק, התקנות, הנחיות הרשם והנהלים הפנימיים של קומסיין. הגבלות אלו חסויות. לא ישמש בעל תפקיד אמון ביותר מאחד התפקידים הבאים: מנהל הגורם המאשר, מנהל אבטחה, פקיד רישום, מפעיל מערכת או מבקר ראה סעיף 5.2.4.

5.2.2. מספר העובדים הנדרש לביצוע מטלות מסוימות:

כל פעילות המוגדרת קריטית בקומסיין מבוצעת על ידי מינימום של שני אנשים שונים. קומסיין שומרת על יתירות כוח אדם על מנת לבצע את הנדרש על פי החוק, התקנות, הנחיות הרשם והנהלים. אין תפקיד התלוי באדם אחד ולכל אדם יש מחליף ברמתו.

5.2.3. זיהוי ואימות הנדרש לכל בעל תפקיד:

קומסיין מפעילה מדיניות בקרת גישה וניהול משתמשים העושה שימוש במערכות ביומטריות והתקני זיהוי פיזיים מתקדמים המאפשרים בקרה ושליטה הן על זהות הגורם הנכנס לאזור מאובטח מסויים או על גישתו לחלקי מערכת מאובטחים והן ניהול רשומות ביחס לזמני הכניסה והגישה כמו גם האזורים וחלקי המערכת אליהם בוצעה הגישה.

5.2.4. תפקידים המחייבים הפרדת סמכויות:

מדיניות האבטחה של קומסיין אוסרת על הענקת סמכויות אמון שונות לאותו בעל תפקיד. כך, למשל, מנהל האבטחה לא יכול לשמש בה בעת כפקיד אימות או פקיד זיהוי. בנוסף, ביצוען של מטלות מסויימות, למשל חילול צמד המפתחות של קומסיין, מחייב מעורבות של מספר בעלי תפקידים כאשר כל בעל תפקיד משלים את חלקו בפעולה, חלק שבהיעדרו הפעולה לא ניתנת להשלמה. קומסיין נוהגת בהתאם ל"נספח הפרדת תפקידים מס' 4" שהינו חלק מהנהלים של קומסיין אשר הוצג למכון התקנים הישראלי ואושר במסגרת אישור תקן ישראלי 27001 ותקן ישראלי 9001 והוצג לרשם ואושר על ידו. נספח זה כולל את תחומי ההרשאות לעובדים בקומסיין והרשאות הגישה הפיסיות למתחמים השונים בקומסיין. הנספח מציג תהליך של הפרדת תפקידים ואת היכולת לפקח כי בכל פעולה קריטית ישתתפו מינימום 2 אנשים. כל אחד מבעלי התפקידים מוגבל בגישתו הבלעדית לאזורים מסויימים בתוך מבנה קומסיין. לאזורים המוגדרים כרגישים יותר מבחינת אבטחה, מתאפשרת גישה מוגבלת של בעלי תפקידים בכירים. לא קיים בעל תפקיד אחד בעל גישה לכל האזורים באופן בלעדי.

5.3. בקורות כוח אדם

5.3.1. דרישות כשירות, ניסיון ואכשרה:

קומסיין מעסיקה כוח אדם בעל ידע, ניסיון, מומחיות וכישורים נדרשים המתאימים לדרישות התפקיד ולשירותים המסופקים על ידם לקומסיין. קומסיין מבצעת מספר בקורות לפני תחילת העסקת עובד הכוללות ראיונות אישיים, מבחן אמינות, בדיקה אל מול ממליצים ומסמכים המעידים על היכולת לבצע את התפקיד (הסמכות, השכלה, ניסיון תעסוקתי וכו'). מנכ"ל קומסיין מאשר באופן סופי את המינוי של כל מועמד לתפקיד אמון.

5.3.2. נהלים לבדיקת ואימות פרטים:

קומסיין ונציגיה עורכים בדיקה ראשונית של כל כוח האדם העובד בשרותיה. קומסיין עורכת

בדיקות מקיפות ויסודיות יותר בהתאם לנוהלי כוח האדם של קומסיין ולהנחיות הרשם בכל הנוגע לכוח האדם המיועד לשמש בתפקידי אמון. קומסיין עורכת חקירות תקופתיות של כל כוח האדם שממלא תפקידי אמון על מנת לוודא את מהימנותם ואת יכולתם המקצועית בהתאם לנוהלי כוח אדם של קומסיין ולהנחיות הרשם. לעובדים ונציגים אין גישה לאזורים רגישים ולביצוע תפקיד של בעל תפקיד אמון עד שהושלמו הבדיקות והחקירות ההכרחיות לצורך קבלתם לתפקיד. כל אדם שנכשל במהלך החקירה הראשונית או התקופתית לא יועסק בקומסיין.

קומסיין מפעילה בקורות תפעוליות הכוללות בקרה ארגונית, בקרה של משאבי אנוש, בקרה של גורמים חיצוניים ובקורות ניהוליות אחרות. בקורות אלה כוללות דרישות הנוגעות להכשרה ולהדרכה של עובדי קומסיין ו/או נציגיה, קביעת מדיניות המסדירה את חלוקת התפקידים בתוך קומסיין, דרישות לגבי תיעוד ונהלים וביקורות קבועות מראש. מנהל האבטחה מבצע ביקורות תפעוליות וביקורות אלו מוודא עבודה על פי הנהלים. עובד שנמצא כי אינו מבצע את הנדרש ממנו בהתאם להגדרת תפקידו ולנהלים יטופל משמעתית ואף תשקל האפשרות לסיים את העסקתו בקומסיין.

5.3.3. דרישות הדרכה לתפקיד:

קומסיין מקיימת הדרכות לעובדים במסגרתן מתבצע רענון ידע החוק, הנהלים והגדרות תפקיד וכן הפקת לקחים מאירועי אבטחה ואירועים אחרים. תוכנית ההדרכות השנתית מעודכנת במהלך החודש האחרון של כל שנה קלנדרית ומועברת לרשם.

5.3.4. תדירות הדרכות והכשרות:

תדירות ההדרכות נקבעת במסגרת התוכנית השנתית וכוללת סבבי הדרכה רבעוניים. תיתכן האצה בתדירות בכל מקרה של שינוי נהלים או אימוץ טכנולוגיות חדשות.

5.3.5. תדירות ונוהל החלפת תפקידים:

קומסיין איננה מפעילה מדיניות המחייבת ביצוע סבב תפקידים של עובדיה.

5.3.6. הליכי משמעת במקרה של אי קיום הנהלים:

קומסיין מקפידה על הליכי דיווח ותיחקור מקיפים בכל מקרה של תקלה או תלונה. ממצאים המצביעים על הפרת נהלי העבודה על ידי עובד או קבלן עצמאי מטופלים משמעתית עד כדי פיטורין או הפסקת התקשרות.

5.3.7. דרישות מקבלנים עצמאיים:

בכל התקשרות של קומסיין עם קבלני משנה לביצוע משימות במהלכן קבלן המשנה מקבל גישה אל, או שליטה על, פעולות רישום, הנפקה, שימוש, וביטול של תעודות מצד קומסיין, לרבות גישה לפעילויות של המאגר של קומסיין שהגישה אליהן מוגבלת, מתחייב קבלן המשנה בחוזה למול קומסיין לשמור על דרישות האבטחה המחמירות להן מחויבת קומסיין בהתאם למסמך נהלים זה, לחוק ולתקנות בקשר עם הפעילות המבוצעת על ידי קבלן המשנה ובנוסף הוא מתחייב לשפות את קומסיין בכל מקרה של נזק כתוצאה מפגיעה באבטחת המידע.

5.3.8. תיעוד הנמסר לצוות הגורם המאשר:

צוות הגורם המאשר מקבל לידי גישה מלאה, בהתאם לעניין ולהגדרת התפקיד, לנהלי העבודה הפנימיים של הגורם המאשר, למסמך נהלים זה ולהוראות אבטחה ותפעול הניתנות מעת לעת.

5.4. נהלי תיעוד אירועים (לוגים)

הפקת לוגים הינה פעולת תיעוד של אירועים המתרחשים במסגרת שירותי הנפקת התעודות האלקטרוניות באמצעות מערך המחשוב של קומסיין. התיעוד מבוצע על-ידי שמירת רשומה של האירועים באופן המונע את מחיקתה על ידי גורמים לא מאושרים.

5.4.1. סוגי אירועים המחייבים תיעוד:

קומסיין ו/או נציגיה מנהלים רשומות מהימנות, העומדות בחובת התיעוד המופיעה בתקנה 19 לתקנות חתימה אלקטרונית (גורם מאשר) ובכלל זה תיעוד של רישום כל הפעולות והאירועים הנוגעים לפעילותם, סמוך לזמן האירוע, ובכלל אלה: זמני הפעלת מערכת המחשב המשמשת לפעילות הגורם המאשר וכל אחד מיישומיה, וזמני הפסקתם, שינוי סיסמאות, ניסיונות בלתי מורשים לחדור למערכת, ייצור או שינוי מפתחות, הנפקת תעודות וביטולן והרשאות גישה למערכת המחשב.

5.4.2. תדירות עיבוד לוגים:

הרשומות נבדקות על בסיס שעתי, יומי, שבועי או חודשי בהתאם לנהלים שאושרו על ידי הרשם כאשר פעולות המוגדרות כקריטיות נבדקות ומאושרות על-ידי מנהל האבטחה. בנוסף, קומסיין בודקת את הרשומות בכל מקרה של התראה על אירוע חשוד או בלתי רגיל.

5.4.3. תקופת אירכוב הלוגים:

תקופת האירכוב בהתאם לתקנות ולהנחיות הרשם היא עד 25 שנה.

5.4.4. הגנה על לוגים של הביקורת:

הלוגים נשמרים בפורמט אלקטרוני מאובטח במסגרת מערכות המיחשוב של קומסיין וכחלק מהאתר המאובטח בהגנה פיזית ולוגית. ההגנה לרבות בקרת גישה וניהול המשתמשים הרשאים לגשת ללוגים המאורכבים.

5.4.5. גיבוי לוגים של הביקורת:

קומסיין עושה שימוש באמצעי גיבוי נאותים של הלוגים, ברמה גבוהה של זמינות, אמינות והגנה מפני אבדן מידע להנחת דעתו של הרשם.

5.4.6. מערכת איסוף רשומות הביקורת (פנימית או חיצונית):

קומסיין מיישמת מערכת פנימית לאיסוף רשומות הביקורת מהמערכות השונות הפועלות במסגרת שירותי הנפקת התעודות האלקטרוניות על ידי קומסיין. המערכת מאפשרת הן את איסוף החומר והן את איחזורו בכל רגע נתון ונתונה לביקורת המבקר בהתאם לדרישת התקנות והנחיות הרשם.

5.4.7. דיווח לגורם האחראי לאירוע:

מערכת בקרת הלוגים כוללת מאפיינים של התרעה מיידית בזמן אמת על סוגי אירועים מהותיים למנהל הגורם המאשר ולאחראי האבטחה. בנוסף, בהתאם לנהלי העבודה הפנימיים של קומסיין קיימים סוגי אירועי אבטחה המחייבים דיווח מיידית גם לרשם.

5.4.8. הערכת פגיעות המערכת:

הרשומות מתועדות, נשמרות ונבדקות, בין היתר, לצורך פיקוח ובדיקת רמת הפגיעות של מערכות התוכנה והחומרה של קומסיין. הערכת רמת הפגיעות של מערכות החומרה והתוכנה של קומסיין מתבצעת ונבדקת במסגרת סקר האבטחה והסיכונים השנתי בהתבסס על נתוני הרשומות. בנוסף, תתכנה הערכות סיכון על בסיס יומי, חודשי ושנתי בהתאם לדרישות נוהלי הביקורת והאבטחה של קומסיין על בסיס נתוני הרשומות העדכניים ביותר.

5.5. אירוב רשומות

קומסיין מארכבת רשומות כמסמכים בכתב או בצורת מסרים ממוחשבים, ובתנאי שהמפתוח, האחסון, השמירה והשחזור שלהם מדויקים ושלמים להנחת דעת הרשם.

5.5.1. סוגי רשומות הנשמרות בארכיב:

הרשומות המאורכבות על ידי קומסיין מתייחסות לפעולות ומידע החיוניים לכל בקשה להנפקת תעודה ולהנפקה, לשימוש, לביטול, לתפוגה או לחידוש של תעודות, כניסה ויציאה ממחשבים שמורים בתוך קומסיין, תיעוד מערכות אבטחת מידע וכיו"ב. הרשומה כוללת תיעוד של תאריך הרשומה, זהות מבצע הפעולה המתועדת ברשומה וסוג הרשומה. מטרת התיעוד היא לאפשר פיקוח ובדיקת הפעולות שבוצעו על-ידי עובדי קומסיין במהלך תהליך הנפקת התעודה וביטולה כמו גם: זהותו של בעל התעודה ששמו נקוב בכל תעודה והמסמכים שלפיהם זוהה; זהותם של האנשים המבקשים ביטול של תעודות; פרטים אחרים המפורטים בתעודה; פרטים מהותיים הנוגעים להליך הנפקת התעודות לרבות הצהרת המבקש בהתאם לתקנה 13 (ב) לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה); תיעוד פרטים הנוגעים לניהול המפתח הפרטי (אמצעי החתימה) של קומסיין לרבות, יצירת המפתח הפרטי של קומסיין, גיבוי, שמירתו, השמדתו ואופן ניהול תוכנות וחומרות ההצפנה של המפתח הפרטי; תיעוד אירועים הנוגעים לאבטחת מידע לרבות ניסיונות לפגוע בתוכנות קומסיין, ככל שנודע על כך לקומסיין, הפעולות המבוצעות על-ידי קומסיין בקשר עם אבטחת המידע, שינויים במערך אבטחת המידע של קומסיין, כשלים של חומרה ותוכנה וכיו"ב.

5.5.2. תקופת שמירת רשומות בארכיב:

קומסיין ו/או נציגיה ישמרו בדרך מהימנה רשומות הקשורות לתעודות במשך שלושים (30) שנה לפחות, לאחר מועד הביטול או התפוגה של התעודה. ניתן לשמור רשומות אלה כמסרים אלקטרוניים הניתנים לשליפה באמצעות מחשב או כמסמכים בכתב.

קומסיין תשמור מסמכים ומידע שקיבלה מבעלי התעודות והמבקשים למשך 25 שנים לפחות בהתאם לתקנה 20 לתקנות חתימה אלקטרונית (גורם מאשר).

5.5.3. הגנה על הארכיב:

הרשומות נשמרות בדוחות ביקורת אלקטרוניים וידניים. הדוחות חסויים והגישה אליהם מוגבלת באמצעים פיזיים וטכנולוגיים. הרשומות בקומסיין מוגדרות כחסויות והגישה אליהם ניתנת אך ורק לבעל תפקיד ספציפי לאחר אישור מנהל האבטחה. כל שינוי ברשומות מותר על פי הגדרת תפקיד והוא מתועד. קומסיין נוקטת באמצעים למניעת שינויים ברשומות, תוך שימוש בבקרה על הגישה לדוחות הידניים והאלקטרוניים.

הרשומות המכילות את פרטי הלקוחות נשמרות בחדר מאובטח שהכניסה אליו הינה למורשים בלבד ורק לאחר הזדהות ביומטרית וקוד אישי.

5.5.4. נהלי גיבוי ארכיב הרשומות:

מערכת הגיבוי מופעלת רק ביחס לרשומות אלקטרוניות. קומסיין עושה שימוש באמצעי גיבוי נאותים של הרשומות, ברמה גבוהה של זמינות, אמינות והגנה מפני אבדן מידע להנחת דעתו של הרשם.

5.5.5. דרישה לחותמות יום ושעה של רשומות מאורכבות:

רשומות אלקטרוניות כוללות חותמת יום ושעה המציינת את מועד יצירת הרשומה. ראה סעיף 6.8 להלן. רשומות בכתב כוללות את תאריך יצירתן שצויין באופן ידני.

5.5.6. מערכת הארכוב (פנימית או חיצונית):

קומסיין מיישמת מערכת ארכוב פנימית לאיסוף ושמירת רשומות. המערכת מאפשרת הן את איסוף החומר והן את איחזורו בכל רגע נתון ונתונה לביקורת המבקר בהתאם לדרישת התקנות והנחיות הרשם.

5.5.7. נהלים לאיסוף ואימות מידע ארכיוני:

רשומות פיזיות נשמרות בפורמט המקורי ותואמות את הנדרש בהתאם לנהלי העבודה הפנימיים של קומסיין. רשומות אלקטרוניות, לרבות מסמכים פיזיים שהומרו בסריקה לפורמט אלקטרוני, נוצרים, נשמרים ומאוחזרים בהתאם להוראת הדין המעניקה להם מעמד של מסמך מקור.

5.6. החלפת מפתחות של הגורם המאשר

בהתקיים נסיבות המחייבות את החלפת צמד המפתחות (פרטי וציבורי) באמצעות חותם הגורם המאשר על התעודה האלקטרונית של שרת ההנפקה או על התעודה האלקטרונית המונפקת לבעל התעודה מתקיים הליך חילול המפתחות המתואר בסעיף 6.1 להלן. משהוחלף צמד המפתחות, תחתמנה התעודות שיונפקו מכאן ואילך רק באמצעות צמד המפתחות החדש (המוחלף) ולא יעשה עוד כל שימוש בצמד המפתחות שהוחלף. לא כל החלפת מפתחות מחייבת ביטולן של תעודות אלקטרוניות בתוקף במועד ההחלפה ושנחתמו באמצעות צמד המפתחות הקודם. למקרה המחייב ביטול תעודה כתוצאה מפגיעה באמצעי החתימה והצורך בהחלפת צמד המפתחות ראה סעיף 4.9.1 לעיל.

5.7. התאוששות ממצבי אסון (DRP) ופגיעה במערכת

5.7.1. נהלים להתמודדות עם אירועים בלתי צפויים ופגיעה בגורם המאשר:

קומסיין ו/או נציגי קומסיין יישמו, יתעדו, ויבחנו תקופתית את התוכניות המתאימות להתמודדות עם אירועים בלתי צפויים ואת היכולות והנהלים להיערכות לאסונות, באופן המתיישב עם הוראות נהלים אלה ועם נהלי האבטחה של קומסיין (להלן: "התוכניות").

התוכניות נועדו למקרים המפורטים להלן המונעים את המשך פעילות אתר הגורם המאשר:

- נפילה כללית של מתח חשמלי וכשל של כל מערכת האל-פסק במבנה בו מצוי מערך המחשוב של קומסיין.
- השמדה פיסית של מערכות המחשוב של קומסיין ו/או של המידע המצוי בהן על-ידי כוח עליון ו/או שריפה ו/או שיטפון ו/או הפרעות מגנטיות ו/או כל סיבה אחרת שאינה בשליטת קומסיין.
- פריצת אבטחת מידע לוגית או פיזית.

5.7.2. פגיעה במשאבי מיחשוב, תוכנות או מידע

בכל אירוע שתוצאתו פגיעה בזמינות מערכות המיחשוב של הגורם המאשר יופעלו נהלי הטיפול בתקלות בניסיון להתגבר על המניעות ולהחזיר לפעילות תקינה את מערכות המיחשוב של הגורם המאשר בתוך מגבלות מועדי הזמינות בהן פועלות מערכות אלו. הובהר לגורם המאשר כי לא ניתן להתגבר על הפגיעה בתוך מגבלות הזמינות, יופעל נוהל המשך פעילות הגורם המאשר במקרה אסון כמוסדר בסעיף 5.7.4 להלן.

5.7.3. נהלים במקרה פגיעה במפתח הפרטי של גורם בהירארכיית הגורם המאשר

אבדן שליטה או פגיעה במפתח הפרטי של גורם בהירארכיית הגורם המאשר בנסיבות המחייבות את חילולו של צמד מפתחות חדש והנפקת תעודה אלקטרונית חדשה חלף התעודה שנחתמה על ידי המפתח הפרטי שנפגע יתבצע בהתאם לנהלי העבודה הפנימיים של קומסיין שאושרו על ידי הרשם, לרבות החלפת תעודות אלקטרוניות שמהימנותן נפגעה בתיאום עם בעלי התעודות ובנסיבות המתאימות גם עם צדדים מסתמכים.

5.7.4. המשכיות עסקית לאחר אירוע אסון

לקומסיין אתר התאוששות חלופי למקרה אסון (DRP) המאפשר לקומסיין להמשיך ולפרסם את רשימת התעודות הבטלות במקרה של אסון הפוגע באתר הראשי של קומסיין ומונע את תפקודו.

5.8. סיום ו/או הפסקת פעילות של קומסיין

קומסיין תסיים ו/או תפסיק את פעילותה בנסיבות המפורטות להלן:

- (1) ניתן צו פירוק חלוט המורה על פירוקה של קומסיין.
- (2) דירקטוריון קומסיין קיבל החלטה על הפסקת פעילות קומסיין כגורם מאשר. במקרה כאמור תימסר לרשם הודעה לפחות 30 יום לפני מועד הפסקת הפעילות.

3) הרשם הורה על מחיקת רישומה של קומסיין ממרשם הגורמים המאשרים בהתאם להוראת סעיף 14 לחוק.

נפסקה פעילותה של קומסיין, תנקוט קומסיין את הפעולות הבאות כמוסדר בסעיף 18(א) או 18(ב) לתקנות חתימה אלקטרונית (רישום וניהול) ובתקנות ניירות ערך (מאשר חתימה) התשס"ג – 2003 ותפעל בהתאם להנחיות הרשם:

- 1) תפסיק להנפיק תעודות אלקטרוניות חדשות.
 - 2) תבטל בהקדם האפשרי את כל התעודות האלקטרוניות התקפות שהנפיקה.
 - 3) תודיע על כך מיד לבעלי התעודות.
 - 4) תכניס את התעודות הבטלות לרשימת התעודות המבוטלות (CRL).
 - 5) תעביר לידי הרשם, בתוך 72 שעות ממועד הפסקת הפעילות או ממועד מחיקתה מרישום, את אמצעי החתימה ואת אמצעי אימות החתימה שלה וכן העתק מדויק של מאגרי התעודות האלקטרוניות שהנפיקה ומאגר התעודות המבוטלות.
 - 6) תעביר לרשם בתוך 7 ימים ממועד הפסקת הפעילות העתק מדויק של כל המסמכים שקיבלה לצורך הנפקת התעודות האלקטרוניות.
 - 7) תבטל מינוי של כל גורם רושם שהוסמך לפעול מטעמה.
 - 8) תמשיך תחזוקה של הרשומות הנדרשות לצורך אספקת הוכחת אישור למטרת הליכים משפטיים, וזאת בכפוף לקבוע בתקנה 18 לתקנות חתימה אלקטרונית (רישום וניהול).
- מקום בו הופסקה פעילות קומסיין שלא כתוצאה מהוראת רשם למחקה ממרשם גורמים מאשרים, רשאית קומסיין, בכפוף לאישור הרשם ובתנאים שייקבעו על ידו, להעביר את ניהולה לידי גורם מאשר אחר. במקרה כזה שמורה לבעל תעודה הזכות לדרוש מהגורם המאשר המחליף לבטל את תעודתו.
- מבלי לגרוע מההסדר הקבוע בהוראת כל דין, תודיע קומסיין מיד על הפסקת פעילותה לכל בעל תעודה תקפה במועד הפסקת הפעילות ותפעל למזער שיבושים פוטנציאליים מהם עלולים לסבול מנויים וצדדים מסתמכים כתוצאה מהפסקת פעילותה. ההודעה תישלח באמצעות דואר אלקטרוני וכן תפורסם בשני עיתונים יומיים.

5.9. אבטחה פיסית – התקן רשתי

תאגיד המבקש לאחסן את אמצעי החתימה על גבי התקן רשתי פנים ארגוני אחראי לנקוט באמצעי אבטחה פנים ארגוניים המונעים גישה בלתי מורשית להתקן, הוצאת אמצעי החתימה מההתקן ו/או העתקתו.

במקרה בו ההתקן הרשתי אשר בו מאוחסנים אמצעי חתימה מצוי בשליטת צד ג', הרי לפי

הנחית הרשם נדרשת עמידה ברף אבטחה גבוה יותר המחייב מיקום ההתקן הרשתי באזור מאובטח הנהנה מהגנות פיסיות ומשימוש באמצעי אבטחה פיסיים הכוללים מערכת בקרת כניסה וניהול מורשים לאזור המאובטח בו ממוקם ההתקן, מערכות ניטור ותיעוד ומערכת התרעה, לשביעות רצונו של הגורם המאשר. קומסיין תערוך ביקורת תקופתית של ההתקן הרשתי כדי לוודא עמידתו בנהלים אלו ובהנחיות הרשם.

הכול בתנאים שייקבעו על ידי הרשם ועל פי נהלי קומסיין.

במקרה בו ההתקן הרשתי מאוחסן בקומסיין, קומסיין תבטיח כי על ההתקן הרשתי יחולו כל דרישות האבטחה המוטלות על קומסיין כגורם מאשר לפי החוק.

6. בקורות אבטחה טכנית

6.1. חילול והתקנת צמד מפתחות

6.1.1. חילול צמד מפתחות:

חילול צמד המפתחות של בעל התעודה מתבצע על ידי בעל התעודה באמצעות חומרה מהימנה העומדת בדרישות התקנות ובאופן המונע גישה והתערבות בתהליך החילול. צמד המפתחות יימצא בשליטתו המלאה של בעל התעודה או מי מטעמו בכל רגע נתון.

6.1.2. מסירת המפתח הפרטי לבעל התעודה:

מסירת המפתח הפרטי לבעל התעודה תתבצע במעמד ההנפקה ובאופן מאובטח המגן על שליטתו הבלעדית של בעל התעודה, או מי מטעמו, במפתח הפרטי. חילול המפתח יתבצע בתוך התקן חומרה המונע גישה לא מורשית לאמצעי החתימה. נאסר על הגורם המאשר להחזיק ברשותו העתק המפתח הפרטי של בעל התעודה.

6.1.3. מסירת המפתח הציבורי של בעל התעודה לגורם המאשר:

מסירת המפתח הציבורי של בעל התעודה לגורם המאשר חייבת להתבצע באמצעות מנגנון המבטיח כי המפתח הציבורי יועבר בשלמות ובלא כל שינוי וכי בידי בעל התעודה מצוי המפתח הפרטי המתאים למפתח הציבורי המועבר.

6.1.4. פרסום המפתח הציבורי של הגורם המאשר לצדדים מסתמכים:

חילול צמד המפתחות של קומסיין מתבצע תחת תנאי אבטחה פיזית ולוגית באמצעות בעלי תפקידי אמון שנבחרו במיוחד לצורך ביצוע הפעולה. דרושים לפחות שישה אנשים ליצירת אמצעי החתימה של קומסיין, ולהצפנתו. לשחזור המפתח נדרשים לפחות ארבעה אנשים. כאמצעי הגנה נוסף מחולקים חלקי המפתח בין בעלי תפקידי האמון באופן שרק שילוב של כל בעלי התפקיד האוחזים ביחד בכל חלקי המפתח יאפשר את פענוח ההצפנה ושחזור המפתח.

המפתח הציבורי של הגורם המאשר פתוח לציבור המסתמכים על התעודות האלקטרוניות שמנפיק הגורם המאשר באתר האינטרנט של הגורם המאשר ובכתובת:

<https://www.comsign.co.il/repository>

6.1.5. גודל מפתחות:

גודלו של אמצעי החתימה (המפתח הפרטי) של קומסיין הוא 4096 סיביות. גודל אמצעי החתימה (המפתח הפרטי) של בעל תעודה אלקטרונית לא ייפחת מ-2048 סיביות. גודל המפתח הפרטי ימלא, בכל עת, אחר הדרישה העדכנית של תקנה 8 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) ואחר הנחיות הרשם. צמד המפתחות של קומסיין תקפים עד ליום 16/7/2036. ניתן להחליף את צמד המפתחות של קומסיין לפני התאריך הנ"ל כפוף לאישור מראש של הרשם. המפתח הציבורי החדש יתפרסם במאגר של קומסיין. כמו כן, יוחלף צמד המפתחות במקרה של שינוי התקנות או ההנחיות לפיהן הקובעות את אורך ו/או

אלגוריתם אמצעי החתימה (המפתח הפרטי) של קומסיין, וזאת באישור מראש של הרשם.

6.1.6. פרמטרים של חילול המפתח הציבורי ובקרת איכות:

המפתח הציבורי של קומסיין מחולל במסגרת טקס חילול מפתחות (key ceremony) המתבצע על-פי נהלי עבודה פנימיים שקיבלו את אישור הרשם ומיועדים לייצר סביבה מאובטחת הן מהבחינה הפיזית והן מבחינת מהימנות המשתתפים והחומרה המופעלת. התקן חומרה מהימן (FIPS 140-2 Level 3) משמש ליצירת, הגנת, והשמדת אמצעי החתימה (המפתח הפרטי) של קומסיין.

המפתח הציבורי של בעל תעודה אלקטרונית מחולל במעמד הנפקת התעודה כמוסדר בסעיף 3.2.1 לעיל וסעיף 6.2.1 להלן ובכפוף לתנאים המפורטים שם.

6.1.7. Key Usages (שדה שימוש בהתאם לתקן X.509v3):

בכל תעודה אלקטרונית הנחתמת באמצעות צמד המפתחות של הגורם המאשר מופעלים השדות: "Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing", והמפתחות משמשים אך ורק ליצירת תעודות אלקטרוניות ו-CRL's בתוך סביבת חומרה מוגנת הממלאת אחר דרישת החוק והתקנות. על מנת לקיים אחר הדרישות בתקן X.509v3 שדה השימוש בתעודות אלקטרוניות החתומות על ידי אמצעי החתימה של הגורם המאשר מכיל הגבלת שימוש בהתאם להסכם המנוי והבקשה להנפקה.

6.2. הגנה על המפתח הפרטי ובקורות קריפטוגרפיות

6.2.1. תקנים ובקורות להתקנים קריפטוגרפיים:

אמצעי החתימה של קומסיין כגורם מאשר באמצעותו היא חותמת על התעודות האלקטרוניות, נוצר על-ידי קומסיין בלבד ומצוי בשליטתה הבלעדית. אמצעי החתימה של קומסיין ו/או מי מנציגי קומסיין מוגן באמצעות אמצעי חומרה ואבטחה מהימנים ובהתאם לדרישות תקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) – היינו, אמצעי החתימה של קומסיין יעמוד בכל אלו:

- (1) הוא מבוסס על מפתח RSA או DSA באורך 2,048 סיביות לפחות;
- (2) הוא מוגן באמצעי שמתקיימות בו לפחות דרישות האבטחה של FIPS 140-2 רמה 3;
- (3) הוא מגובה באמצעים מוגנים ומאובטחים, להנחת דעתו של הרשם; הגיבוי יישמר בנפרד;
- (4) דרישות נוספות שהעמיד הרשם לשם קיום אבטחה ברמה סבירה מפני חדירה, שיבוש או שימוש לרעה.

במועד סביר קודם לביטולו או פקיעתו של אמצעי החיתום של הגורם המאשר, ידאג הגורם המאשר לייצר צמד מפתחות חיתום חדש על מנת למנוע פגיעה בפעילות השוטפת. חילול צמד המפתחות החדש יתבצע, גם הוא, בהתאם לתקן האמור או גבוה ממנו ככל שיידרש באותו מועד על-פי תנאי התקן והנחיות הרשם.

חילול ואחסון אמצעי החיתום של בעל התעודה יתבצע, גם כן, באמצעות התקן חומרה מהימן

(כרטיס חכם, טוקן, HSM וכו') המקיים את דרישות החוק ותקנותיו. ככל שהגישה למפתח הפרטי של בעל התעודה מתבצעת באמצעות סיסמה, על הסיסמה לעמוד בדרישות אבטחה ברמה הגבוהה לפי ת"י 1495 חלק 3, או בדרישות חלופיות שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה;

6.2.2. ביזור סמכויות (n מתוך m) בבקרה על המפתח הפרטי:

על מנת לבזר את יכולת ההונאה ננקטים האמצעים הבאים לצורך שמירת אמצעי החתימה (המפתח הפרטי) של קומסיין: אמצעי החתימה (המפתח הפרטי) של קומסיין מוצפן בשלמותו על כרטיס הצפנה מבוסס חומרה ומאוחסן בכספת של קומסיין. מפתח ההצפנה אשר הצפין את אמצעי החתימה (המפתח הפרטי) מחולק למספר חלקים. כל חלק מופקד בידי עובד קומסיין שאינו נמנה על העובדים אשר עוסקים באופן ישיר בשירותי הנפקת התעודות וניהולן. כל העובדים הנ"ל עוברים בדיקות מהימנות קפדניות ותקופתיות. רק חיבור כל החלקים באמצעות הליך מבוקר ומנוטר מאפשר את שיחזור מפתח ההצפנה.

6.2.3. הפקדה בנאמנות של המפתח הפרטי:

לא רלבנטי. המפתח הפרטי של קומסיין אינו מופקד בנאמנות. ההגנה מושגת כמפורט בסעיף 6.2.2.

6.2.4. גיבוי המפתח הפרטי:

קומסיין מבצעת פעילות גיבוי של כלל מערכיה, לרבות המפתח הפרטי, במסגרת ההיערכות למצבי אסון. גיבוי המפתח הפרטי מתבצע באמצעות נושאי תפקידי אמן ושמירת הגיבויים בנפרד כפופה לנהלי האבטחה הנהוגים ביחס להגנה על אמצעי החתימה של קומסיין.

6.2.5. אירכוב המפתח הפרטי:

אמצעי החתימה של קומסיין יישמר, בתנאים מאובטחים התואמים את המוסדר בנהלים אלו בכל הקשור בהגנה על המפתח הפרטי של קומסיין, לאחר ביטולו או פקיעת תוקפו והפסקת השימוש בו ולפרק זמן נוסף שלא יפחת מ-12 חודשים.

אירכוב המפתח הפרטי של בעל התעודה שתוקפו פג או שבוטל נתון לשיקול דעתו של בעל התעודה בלבד. אין כל חובה על בעל התעודה, בדין או בהסכם, לארכב את אמצעי החתימה שלו לאחר ביטולו או פקיעת תוקפו.

6.2.6. הכנסה והוצאה של המפתח הפרטי להתקן:

התקני החומרה בהם עושה קומסיין שימוש לייצור אמצעי החתימה, הן של הגורם המאשר והן של בעל התעודה, מאופיינים בכך שחילול המפתח הפרטי מתבצע בתוך התקן החומרה ולא מתאפשרת הכנסתו או הוצאתו של המפתח הפרטי מהתקן.

6.2.7. איחסון המפתח הפרטי בהתקן:

אמצעי החתימה של הגורם המאשר ושל בעל התעודה יאוחסנו בהתקן חומרה מאובטח כמפורט בסעיף 6.2.1 לעיל.

6.2.8. הפעלת המפתח הפרטי:

הגישה לאמצעי החתימה (המפתח הפרטי) והפעלתו מותרת רק לבעל אמצעי החתימה או למורשה מטעמו. הפעלת אמצעי החתימה תתאפשר רק באמצעות סיסמה או אמצעי זיהוי חד ערכי אחר (ביומטרי למשל) של בעל אמצעי החתימה או של המורשה מטעמו העומד בדרישות הדין והנחיות הרשם.

6.2.9. סיום פעולת המפתח הפרטי:

פעולת המפתח הפרטי מסתיימת בתום כל הפעלה ושימוש בו והוא חדל מלהיות פעיל.

6.2.10. השמדת המפתח הפרטי:

פועל יוצא של השמדת המפתח הפרטי הינו השמדת המידע הלוגי של אמצעי החתימה. ניתן להגשים תוצאה זאת או באמצעות מחיקה מוחלטת של המידע הלוגי האגור ברכיב החומרה בו מאוחסן המפתח הפרטי או בהשמדתו המוחלטת של אמצעי החומרה באופן המונע המשך שימוש במידע שאוחסן בו או של שיחזורו.

6.2.11. דירוג ההתקן הקריפטוגרפי:

אמצעי החתימה של הגורם המאשר ושל בעל התעודה מוגנים באמצעות תוכנת הצפנה או אסימוני חומרה (TOKEN) ומקיימים את דרישות הוראות תקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) ואת המפורט בנהלים אלה.

במקרה שבו המבקש קיבל מקומסיין את התקן החומרה המייצר והמכיל את אמצעי החתימה, נושאת קומסיין באחריות לעמידתם של אמצעי החתימה והאמצעי לאימות חתימה המזהה את אמצעי החתימה האמור בהוראות תקנה 8 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה). במקרה שבו המבקש לא קיבל מקומסיין את התקן החומרה עליו יותקן אמצעי החתימה, תנפיק קומסיין תעודה אלקטרונית למבקש רק לאחר שבדקה היטב כי המבקש מחזיק בידיו אמצעי חתימה להפקת חתימה אלקטרונית מאובטחת וכי באמצעי החתימה ובאמצעי לאימות חתימה המזהה את אמצעי החתימה האמור מתקיימות הוראות תקנה 8 לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה). לעניין קיום הוראות תקנה 8(1)(ב) ו-8(ג) לתקנות הנ"ל, רשאית קומסיין להסתפק בהצהרה מטעם המבקש בדבר אמצעי החתימה שבו הוא משתמש, אופן הפעלתו והגישה אליו. בשני המצבים אחראית קומסיין לתעודה שהונפקה לאמצעי החתימה כמוסדר בחוק ובנהלים אלו.

בהנפקה על גבי התקן רשתי יחולו, בנוסף, ההוראות הבאות:

- (1) על ההתקן הרשתי לעמוד בכל הדרישות המפורטות בהנחיית הרשם העוסקת בנוהל הגשת בקשה להנפקה על גבי התקן רשתי.
- (2) במידה וההתקן לא סופק על ידי קומסיין, רשאית קומסיין להסתפק בקבלת "הצהרה מטעם המבקש, בדבר אמצעי החתימה שבו הוא משתמש, אופן הפעלתו והגישה אליו" לפי נוסח נספח ג' להנחיית הרשם - נוהל הגשת בקשה להנפקה על גבי התקן רשתי.

6.3. היבטים אחרים בניהול צמד מפתחות

6.3.1. אירכוב המפתח הציבורי:

קומסיין מארכבת בארכיון קומסיין את המפתחות הציבוריים של שרתי החיתום שלה ומחילה לגביהם, בשינויים המתחייבים, את הוראות סעיף 5.5 לעיל.

על בעל התעודה אין מוטלת כל חובה שבדין או בהסכם לארכב את המפתח הציבורי לאחר השמדת, פקיעת או ביטול המפתח הפרטי הצמוד לו.

6.3.2. תקופת תוקף השימוש בתעודה האלקטרונית ובצמד המפתחות:

משך תקופת תוקף השימוש בתעודה האלקטרונית נקבע במועד הנפקת התעודה. משך זמן זה לא יעלה, בכל מקרה, על פרק זמן של 5 שנים או תקופה קצרה יותר ככל שיוחלט על שינוי בתקנות או בהנחיות הרשם כתוצאה מדרישה טכנולוגית או מסיבה אחרת המחייבת את החלפת צמד המפתחות והנפקת תעודה אלקטרונית חדשה. משך תקופת תוקף תעודה למערכת מגנא לא ייפחת משנתיים ולא יעלה על ארבע שנים.

לענין משך תקופת תוקף השימוש לשרת אינטרנט ראה סעיף 6.3.2 בנספח - (19)

חידוש תעודה אלקטרונית קודם מועד פקיעתה לא יחייב את החלפת צמד המפתחות.

לא ניתן להנפיק שתי תעודות אלקטרוניות תקפות לאותו צמד מפתחות. מכאן שחידוש תעודה אלקטרונית מחייב את פקיעת התוקף של התעודה הקודמת.

6.4. המידע הדרוש להפעלה:

6.4.1. חילול המידע הדרוש להפעלה והתקנתו:

חילול המידע הדרוש להפעלת אמצעי החתימה והתקנתו בהתקן החומרה המאחסן אותו (כרטיס חכם, שבב אחסון, התקן רשתי, HSM וכו') יעמדו בכל דרישות האבטחה של נהלים אלו, הוראות הדין והנחיות הרשם.

6.4.2. הגנת המידע הדרוש להפעלה:

המידע הדרוש להפעלת אמצעי החתימה יוגן באמצעים קריפטוגרפיים ויימצא בכל עת בשליטתו המוחלטת של בעל אמצעי החתימה או המורשה מטעמו האחראים להגנתו.

6.4.3. היבטים נוספים של המידע הדרוש להפעלה:

לא רלבנטי.

6.5. בקורות לאבטחת מחשב

6.5.1. דרישות טכניות מיוחדות לאבטחת מחשב:

במסגרת ביצוע השירותים המסופקים על ידם, קומסיין ונציגיה יעשו שימוש אך ורק במערכות מהימנות העומדות בדרישות הטכניות של החוק ותקנותיו.

בהתאם לתקנה 5 (א) לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה יעמדו ברמת ביטחון של תקן common criteria EAL4.

קומסיין עושה שימוש במערכות אבטחת מידע מהימנות. מערכות אלו חסויות לקהל הרחב אך מבוקרות על ידי גורמים חיצוניים. כחלק מהבקרה מבוצעת ביקורת שנתית בקומסיין על-ידי מבקר לא תלוי לבדיקת מהימנות המערכות ועבודה על פי הנהלים בהתאם לדרישות הרשם ולהנחת דעתו.

כמו כן מבוצע סקר סיכונים שנתי על-ידי מומחה אבטחת מידע חיצוני ולא תלוי לבדיקת המערכות שזהותו היא להנחת דעת הרשם. יש לציין כי קומסיין עומדת בתקני ISO 27001 בנושא אבטחת מידע ומבוקרת על ידי גורמים בלתי תלויים לצורך עמידה בתקנים אלה.

6.5.2. דירוג אבטחת מחשב:

קומסיין מיישמת את הוראות תקנה 5 (א) לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה) ועומדת בתקני אבטחת המידע הקבועים בהוראות הדין, הנחיות הרשם ובהנלים אלו.

6.6. בקורות טכניות במהלך תקופת התוקף של תעודה אלקטרונית

6.6.1. בקורות על פיתוחי מערכת:

קודם להכנסתו לשימוש של כל פיתוח או שכלול של רכיב מערכתי המשמש לפעילות הגורם המאשר, עליו לעמוד בבדיקות בקרת איכות והתאמה, לרבות דרישות הדין והנחיות הרשם. בנוסף, כל פיתוח כאמור נבחן במסגרת סקר הסיכונים השנתי על ידי מומחה חיצוני בלתי תלוי שזהותו אושרה על ידי הרשם.

6.6.2. בקורות על ניהול האבטחה:

קומסיין מפעילה, בניהולו של מנהל האבטחה של הגורם המאשר, מערכת ניטור ובקרה המנהלת באופן שוטף מעקב שמטרתו זיהוי כשלי אבטחה והגנה על שלמות המערכות והמידע של קומסיין מפני וירוסים ותוכנה זדונית ובלתי מורשה; מזעור הנזק הנגרם כתוצאה מתקריות אבטחה באמצעות השימוש בדיווח על תקריות ובוהלי תגובה; טיפול באופן מאובטח במדיה הנמצאת בשימוש קומסיין במטרה להגן עליה מפני נזק, גניבה וגנישה בלתי מורשה; יישום נוהלי ניהול המדיות המספקים הגנה מפני התיישנות ובלאי של מדיות בפרק הזמן בו יש לשמור על הרשומות; קיום נהלים עבור כל תפקידי האמון והניהול אשר משפיעים על זמינות וטיב שירותי התעודות; ניטור של דרישות הקיבולת ויצירת תחזית של דרישות קיבולת עתידיות להבטחת זמינות של עוצמת עיבוד ואמצעי אחסון; פעולה, תוך זמן סביר ותוך שיתוף פעולה, במטרה להגיב במהירות לתקריות וכדי להגביל את ההשפעה של פריצות אבטחה. כל התקריות מדווחות בהקדם האפשרי לאחר התקרית ומצויות במעקב שוטף עד להסדרתן.

6.6.3. בקורות אבטחה במהלך תקופת התוקף של התעודה האלקטרונית:

קומסיין מפעילה מערכת בקרה שוטפת שנועדה להבטיח כי תישמר שלמותן ותקינותן של מערכות חומרה העוסקות בהצפנת וחתימת מידע העוסק בתעודות אלקטרוניות ובסטאטוס התוקף שלהן, ברשימת התעודות התקפות והמבוטלות ובמידע נוסף הקשור להפעלתן או לביטולן. ראה לעניין זה סעיף 6.6.2 לעיל.

6.7. בקורות אבטחת רשת:

קומסיין מיישמת מדיניות אבטחת רשת, בקרת גישה וניהול משתמשים תוך הפרדה מוחלטת בין מערכות העוסקות בהנפקת תעודות אלקטרוניות וניהולן לבין מערכות מקוונות המחוברות לרשת האינטרנט. אותם חלקי מערכת מקוונים מוגנים באמצעי אבטחה המיועדים למנוע פריצה למערכת, החדרת ווירוסים או תוכנות זדוניות ואיתור ניסיונות חדירה לא מאושרים.

6.8. חותמת יום-שעה:

חותמת יום ושעה נועדה לשפר את אמינות שירותי הנפקת התעודות של קומסיין. חותמת יום ושעה מעידה על היום והשעה הנכונים של פעולה ועל זהותו של האדם או ההתקן שיצרו את החותמת. חותמת היום והשעה משקפת את שעון גריניץ' (GMT) ומאמצת את מוסכמות הזמן האוניברסאליות (UTC). חותמת יום ושעה של קומסיין מסתמכת על מקור זמן של צד ג' מהימן המספק קריאות של הזמן העולמי הרשמי בכל רגע נתון. קומסיין תטביע חותמת יום ושעה על גבי הנתונים הבאים, בין אם ישירות על גבי הנתונים ובין אם על גבי נתיב ביקורת מהימן מקביל:

• תעודות.

• רשימות תעודות מבוטלות ורשומות אחרות של בסיסי נתונים של ביטולי תעודות.

• מידע אחר, בהתאם להוראות נהלים אלה.

6.9. אבטחה לוגית – שרת חתימות

כאשר אמצעי החתימה מאוחסן בשרת חתימות נדרש כי אמצעי החתימה ייווצר וישמר במודול קריפטוגרפי שהוסמך לתקן Common Criteria EAL4, או לתקן FIPS 140-2 רמה 3 או 4 לפחות, אשר אינו מאפשר לשכפל את אמצעי החתימה לאחר ייצורו או להעתיקו (למעט לצרכי גיבוי) אל מחוץ להתקן האחסנה. הגישה לאמצעי החתימה והפעלתו תחייב זיהוי חד ערכי של בעל אמצעי החתימה ותוגבל רק למחיצה בשרת החתימות בו מאוחסן אמצעי החתימה. אופן הפעלת אמצעי החתימה והגישה אליו תספק שליטה בלעדית של החותם בחתימתו באמצעות רכיב פסי קריפטוגרפי או סיסמה ייחודית אשר עומדת בתו התקן וביתר דרישות תקנה 8(1)(ב) ו-8(1)(ג) לתקנות חתימה אלקטרונית (מערכות חומרה ותוכנה).

בהתאם לדרישת הרשם, כאשר אמצעי החתימה מאוחסן בשרת חתימות המצוי בשליטת צד ג', נדרש רף אבטחה גבוה יותר לצורך הבטחת שליטתו הבלעדית של בעל אמצעי החתימה במפתח הפרטי. דרגת אבטחה גבוהה כאמור אמורה להשיג את אותה רמת שליטה בלעדית של החותם כפי שהיתה מושגת באם אמצעי החתימה היה מאוחסן ברכיב עצמאי אשר היה מוחזק בידי המורשה. דרישה זאת מושגת באמצעות שילוב של התקן נפרד להפעלת אמצעי החתימה (כגון כרטיס חכם או התקן המפיק סיסמאות מתחלפות או טלפון סלולרי עם סיסמאות מתחלפות) בצירוף סיסמה קבועה הידועה למורשה בלבד (או בשילוב ביומטרי). רק לאחר מכן - מתאפשרת גישה להתקן האחסון האישי של החותם וזאת באמצעות סיסמה ייחודית שונה ונפרדת. רק לאחר שאושרה הגישה להתקן האחסון עצמו תתאפשר הגישה הדרושה להפעלת אמצעי החתימה בתוך המחיצה הייחודית למורשה על גבי שרת החתימות.

7. מבנה תעודה, רשימת תעודות מבוטלות ו-OCSP

7.1. מבנה תעודה

7.1.1. מספר/י גירסה:

קומסיין מנפיקה תעודות אלקטרוניות התואמות תקן 3 version X.509.

7.1.2. שדות הרחבה בתעודה:

קומסיין עושה שימוש בשדות ההרחבה הבאים:

Authority Key Identifier – OID 2.5.29.35

Subject Key Identifier – OID 2.5.29.14

Key Usage (critical) – OID 2.5.29.15

Certificate Policies – OID 2.5.29.32

Subject Alternative Name – OID 2.5.29.17

Basic Constraints (critical) – OID 2.5.29.19

Extended Key Usage – OID 2.5.29.37

CRL Distribution Points – OID 2.5.29.31

Authority Information Access – OID 1.3.6.1.5.5.7.1.1

Qualified Certificate Statement – OID 1.3.6.1.5.5.7.1.3

7.1.2.1. שדות הרחבה בתעודת השורש של הגורם המאשר (Root CA)

(i) basicConstraints:

(a) This extension appears as a critical extension.

(b) The CA field is set to true.

(c) The pathLenConstraint field is not present.

(ii) keyUsage:

(a) This extension is present and marked as critical.

(b) Bit positions for digitalSignature, keyCertSign and cRLSign are set.

(iii) certificatePolicies

(a) This extension is not present.

(iv) extendedKeyUsage

(a) This extension is not present.

(v) Subject Information

(a) The Certificate Subject contains the following:

countryName (OID 2.5.4.6). This field contains the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located = IL

organizationName (OID 2.5.4.10): This field is present and the contents contains the Subject CA's name

Common Name (OID 2.5.4.3): Comsign Global Root CA

(vi) certificate details:

Data:

Version: 3 (0x2)

Serial Number:

8f:61:71:15:ba:79:58:17:8c:7d:11:3a:ac:d6:db:ae

Signature Algorithm: sha256WithRSAEncryption

Issuer:

countryName = IL

organizationName = ComSign Ltd.

commonName = ComSign Global Root CA

Validity:

Not Before: Jul 18 10:24:54 2011 GMT

Not After : Jul 16 10:24:55 2036 GMT

Subject:

countryName = IL

organizationName = ComSign Ltd.

commonName = ComSign Global Root CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit) X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 CRL Distribution Points:

Full Name:

URI:http://fedir.comsign.co.il/crl/comsignglobalrootca.crl

Full Name:

URI:http://crl1.comsign.co.il/crl/comsignglobalrootca.crl

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:

02:45:93:D8:0D:48:62:AC:69:BA:AE:06:5B:3E:FB:AA:26:91:50:B1

X509v3 Authority Key Identifier:

keyid:02:45:93:D8:0D:48:62:AC:69:BA:AE:06:5B:3E:FB:AA:26:91:50:B1

Signature Algorithm: sha256WithRSAEncryption

תעודת ביניים .7.1.2.2

(i) certificatePolicies

(a) This extension is present and is not marked critical.

(b) certificatePolicies:policyQualifiers:qualifier:cPSuri HTTP URL for the Root CA's Certificate Policies and Certification Practice Statement.

(ii) cRLDistributionPoints

(a) This extension is present and is not marked critical. It contains the HTTP URL of the CA's CRL service.

(iii) authorityInformationAccess

(a) This extension is present. It is not marked as critical

(b) It contains the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

(c) It also contains the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(iv) basicConstraints

(a) This extension is present and is marked critical.

(b) The CA field is set to true.

(v) keyUsage

(a) This extension is present and is marked critical.

(b) Bit positions for keyCertSign and cRLSign are set.

(vi) Subject Information - Certificate Subject contains the following:

(a) countryName (OID 2.5.4.6). the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located = IL.

(b) organizationName (OID 2.5.4.10): the Subject CA's name

(c) Locality Name

(d) Common Name (OID 2.5.4.3): Comsign represents that it followed the procedure set forth in its Certificate Policy and Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

(vii) Example: ComSign Organizational CA certificate details:

Data:

Version: 3 (0x2)

Serial Number:

45:84:9b:19:72:44:10:22:14:ea:48:60:c0:3a:2b:90

Signature Algorithm: sha256WithRSAEncryption

Issuer:

countryName = IL

organizationName = Comsign Ltd.

commonName = Comsign Global Root CA

Validity

Not Before: Jun 17 13:17:32 2015 GMT

Not After : Oct 22 19:00:00 2025 GMT

Subject:
 commonName = Comsign Organizational CA
 organizationName = Comsign Ltd.
 localityName = Tel Aviv
 countryName = IL
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (4096 bit) X509v3 extensions:
 Authority Information Access:
 OCSP - URI:http://ocsp1.comsign.co.il/ocsp
 CA Issuers - URI:http://fedir.comsign.co.il/cacert/ComSignGlobalRootCA.crt
 X509v3 Basic Constraints: critical
 CA:TRUE, pathlen:0
 X509v3 Certificate Policies:
 Policy: X509v3 Any Policy
 CPS: http://www.comsign.co.il/CPS

 X509v3 CRL Distribution Points:

 Full Name:
 URI:http://fedir.comsign.co.il/crl/ComSignGlobalRootCA.crl
 Full Name:
 URI:http://crl1.comsign.co.il/crl/ComSignGlobalRootCA.crl X509v3 Key
 Usage: critical
 Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
 F5:BB:AD:EA:31:23:4B:00:5D:5B:4F:76:DE:6F:8B:02:E0:FD:DF:F0
X509v3 Authority Key Identifier:
 keyid:02:45:93:D8:0D:48:62:AC:69:BA:AE:06:5B:3E:FB:AA:26:91:50
 Signature Algorithm: sha256WithRSAEncryption

7.1.2.3. מבנה תעודות למנויים

(i) מבנה תעודה ליחיד:

שם שדה	תאור	דוגמא
גרסא Version	גרסת התעודה	"V3"
מספר סידורי Serial Number	המספר הסידורי של התעודה. מספר זה הינו ערך חד ערכי.	bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 00 ed ab"
אלגוריתם חתימה Signature Algorithm	אלגוריתם החתימה בו ישתמש בעל התעודה. אלגוריתם הגיבוב יכול להיות מסוג SHA2 או SHA1 ע"פ הנחיות הרשם	"sha1RSA"
הגורם המאשר Issuer	שדות המתארים את הגורם המאשר	Corporations שם מלא - CN שם הגורם המאשר - O מדינה C "IL"
תוקף	שדות המתארים את תוקף התעודה	

תקף מיום Valid from	יום תחילת תוקף (תאריך) (ההנפקה)	"יום שלישי 10 דצמבר 2002 06:10:33"
תקף עד ליום Valid to	יום תפוגת תוקף	"יום חמישי 08 דצמבר 2003 05:24:21"
פרטים אודות בעל התעודה Subject	פרטים אודות האינדיבידואל לו הונפקה התעודה (בעל התעודה)	
	CN (שם מלא של בעל התעודה באנגלית ומספר זהות)	" Levy Israel ID 012345678"
	שם משפחה (אנגלית) SN	Levy
	שם פרטי (אנגלית) G	Isarel
	מספר זהות Serialnumber	01-012345678
	שם הארגון – O (קוד זיהוי ומספר זהות)	07-012345678
	יחידת משנה – OU (שם מלא של בעל התעודה באנגלית)	Israel Levy
	תפקיד - T	Personal Certificate
	מדינה - C	"IL"
	אורך המפתח הציבורי של בעל התעודה	RSA (2048 Bits)
מפתח ציבורי Public Key		
הפצת CRL CRL Distribution Points	קישור לרשימת התעודות המבוטלות (CRL)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporat ions.crl
		[2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporati ons.crl

[1]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il/ocsp [2]Authority Information Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	OCSP קישור לשרת	OCSP (On- הפצת line Certificate Status Protocol)
This certificate is limited to 50,000 NIS	1.3.6.1.5.5.7.1.3	qcStatements
KeyID=93 a1 4b 84 20 bc de 68 60 9b dc 85 d5 83 51 cd 8c d9 c8 b2	Key Identifier של תעודת ביניים	Authority Key Identifier
[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Notice Number=11 Notice Text=בעל התעודה זוהה פנים אל פנים על סמך תעודות ו/או מידע מזהה אחר. על השימוש בתעודה זו יחולו נהלי קומסיין חבות ואחריות קומסיין מוגבלות כמפורט בנהלים הגבלה על השימוש בתעודה – אופציונאלי The email address in the subject alternative name field is NOT verified by the issuer and is NOT trusted	נהלים (CPS) להסדרת פעילותו של הגורם המאשר (ComSign) כתובת הדואר האלקטרוני של בעל התעודה לא אומתה על ידי הגורם המאשר לצורכי הסתמכות	מדיניות התעודה Certificate Policies
(Secure Email (1.3.6.1.5.5.7.3.4 ו/או Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)	המטרות לשמן מיועדת התעודה. מטרת אלו משתנות לפי סוג התעודה, חתימה וזיהוי בהתאמה.	Enhanced Key Usage
פרטים אודות בעל זכות החתימה		פרטים של מורשה חתימה Subject Alternative Name
"levy@israel.co.il"	כתובת דואר אלקטרוני כפי שנמסרה על ידי בעל התעודה RFC822 Name	
"IL"	מדינה C	
" 07-012345678 "	O שם הארגון (קוד זיהוי ומספר זהות)	

"ישראל לוי"	OU יחידת משנה (שם מלא של בעל התעודה בעברית)	
תעודה אישית	תפקיד T	
"לוי"	שם משפחה (עברית) - SN	
"ישראל"	שם פרטי (עברית) G	
לוי ישראל ID_012345678	CN (שם בעל התעודה בעברית ומספר זהות)	
[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2(Alternative Name: URL=http://fedir.comsign.co.il/cacert/Corporations.crt		Authority Info [1] Access
07 19 61 9a d1 4e 07 71 06 25 a3 78 71 19 bc b3 0a 83 7c 5c		Subject Key Identifier
Digital Signature, Non-Repudiation, Key Encipherment (e0)	תיאור המטרות לשמן ניתן להשתמש בתעודה	Key Usage
"sha1"	האלגוריתם לחתימה שאיתו נחתמה התעודה	אלגוריתם החתימה Thumbprint Algorithm
e2 a1 5a 40 07 e4 a3 c3 88 66 91 14 5b 9c 00 ff e4 1d 24 8e	פרטי התעודה חתומים על ידי הגורם המאשר	ערך החתימה Thumbprint
* בשלב זה – תפקידי O וOU בתעודות משהב"ט – הפוכים (שם תאגיד=O)		

(ii) מבנה תעודה לנוטריון:

שם שדה	תאור	דוגמא
גרסא Version	גרסת התעודה	"V3"
מספר סידורי Serial Number	המספר הסידורי של התעודה. מספר זה הינו ערך חד ערכי.	bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 00 ed ab"
אלגוריתם חתימה Signature	אלגוריתם החתימה בו ישתמש בעל התעודה.	"sha1RSA"

אלגוריתם הגיבוב יכול להיות מסוג SHA2 או SHA1 ע"פ הנחיות הרשם	Algorithm
שדות המתארים את הגורם המאשר	הגורם המאשר
שם מלא - CN	Issuer
Corporations	
שם הגורם המאשר - O	
" ComSign Ltd."	
מדינה C	
"IL"	
שדות המתארים את תוקף התעודה	תוקף
יום תחילת תוקף (תאריך)	תקף מיום
"יום שלישי 10 דצמבר 2002 06:10:33"	Valid from
יום תפוגת תוקף	תקף עד ליום
"יום חמישי 08 דצמבר 2003 05:24:21"	Valid to
פרטים אודות האינדיבידואל לו הונפקה התעודה (בעל התעודה)	פרטים אודות בעל התעודה
CN לנוטריון בעל 2 תעודות על רכיב יחיד (שם מלא של בעל התעודה באנגלית, מספר זהות + תפקיד נוטריון/עו"ד)	Subject
"Israel Israeli ID 111111118 Notary/Lawyer"	
שם משפחה (אנגלית) SN	
Levy	
שם פרטי (אנגלית) G	
Isarel	
מספר זהות Serialnumber	
01-012345678	
שם הארגון - O (קוד זיהוי ומספר זהות)	
07-012345678	
יחידת משנה - OU (מספר רשיון עו"ד)	
1234	
מזהה נוסף - IO (2.5.4.97) - מספר רשיון נוטריון	
4321	
תפקיד - T	
Lwayer & Notary	
מדינה - C	
"IL"	
מפתח ציבורי של בעל התעודה	מפתח ציבורי
RSA (2048 Bits)	Public Key

[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporations.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporations.crl	קישור לרשימת המבוטלות (CRL) התעודות	הפצת CRL CRL Distribution Points
[1]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il/ocsp [2]Authority Information Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	קישור לשרת OCSP	הפצת OCSP (On-line Certificate Status Protocol)
This certificate is limited to 50,000 NIS	1.3.6.1.5.5.7.1.3	qcStatements
KeyID=93 a1 4b 84 20 bc de 68 60 9b dc 85 d5 83 51 cd 8c d9 c8 b2	Key Identifier של תעודת ביניים	Authority Key Identifier

[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Notice Number=11 Notice Text=בעל התעודה זוהה פנים אל פנים על סמך תעודות ו/או מידע מזהה אחר. על השימוש בתעודה זו יחולו נהלי קומסיין חבות ואחריות קומסיין מוגבלות כמפורט בנהלים הגבלה על השימוש בתעודה – אופציונאלי The email address in the subject alternative name field is NOT verified by the issuer and is NOT trusted	נהלים (CPS) להסדרת פעילותו של הגורם המאשר (ComSign) כתובת הדואר האלקטרוני של בעל התעודה לא אומתה על ידי הגורם המאשר לצורכי הסתמכות	מדיניות התעודה Certificate Policies
(Secure Email (1.3.6.1.5.5.7.3.4 ו/או Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)	המטרות לשמן מיועדת התעודה. מטרות אלו משתנות לפי סוג התעודה, חתימה וזיהוי בהתאמה.	Enhanced Key Usage
פרטים אודות בעל זכות החתימה		
"levy@israel.co.il"	כתובת דואר אלקטרוני כפי שנמסרה על ידי בעל התעודה RFC822 Name	פרטים של מורשה חתימה Subject Alternative Name
"IL"	מדינה C	
" 07-012345678"	O שם הארגון (קוד זיהוי ומספר זהות)	
4321	OI (2.5.4.97) מזהה נוסף – מספר רשיון נוטריון	
1234	OU יחידת משנה (מספר רשיון עו"ד)	
עוד ונוטריון	T תפקיד	
"לוי"	שם משפחה (עברית) - SN	
"ישראל"	שם פרטי (עברית) G	
ID_012345678 לוי ישראל	CN (שם בעל התעודה בעברית ומספר זהות)	

[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2(Alternative Name: URL=http://fedir.comsign.co.il/cacert/Corporations.crt		Authority Info [1] Access
07 19 61 9a d1 4e 07 71 06 25 a3 78 71 19 bc b3 0a 83 7c 5c		Subject Key Identifier
Digital Signature, Non-Repudiation, Key Encipherment (e0)	תיאור המטרות לשמן ניתן להשתמש בתעודה	Key Usage
"sha1"	האלגוריתם לחתימה שאיתו נחתמה התעודה	אלגוריתם החתימה Thumbprint Algorithm
e2 a1 5a 40 07 e4 a3 c3 88 66 91 14 5b 9c 00 ff e4 1d 24 8e	פרטי התעודה חתומים על ידי הגורם המאשר	ערך החתימה Thumbprint
* בשלב זה – תפקידי O ו OU בתעודות משהב"ט – הפוכים (שם תאגיד=O)		

(iii) מבנה התעודה למורשה חתימה בתאגיד או מוסד ציבורי:

שם שדה	תאור	דוגמא
גרסא Version	גרסת התעודה	"V3"
מספר סידורי Serial Number	המספר הסידורי של התעודה. מספר זה הינו ערך חד ערכי.	bc be ac 46 8b 09 ad e5 2d 31 ed f0 8e 02 00 ed ab"
אלגוריתם חתימה Signature Algorithm	אלגוריתם החתימה בו ישתמש בעל התעודה. אלגוריתם הגיבוב יכול להיות מסוג SHA2 או SHA1 ע"פ הנחיות הרשם	"sha1RSA"
הגורם המאשר Issuer	שדות המתארים את הגורם המאשר	
	שם מלא CN	"Corporations"
	שם הגורם המאשר O -	".ComSign Ltd"
	מדינה C	"IL"
תוקף	שדות המתארים את תוקף התעודה	

יום תחילת תוקף (תאריך ההנפקה)	יום שלישי 10 דצמבר 2002 06:10:33	תקף מיום Valid from
יום תפוגת תוקף	יום חמישי 08 דצמבר 2003 05:24:21	תקף עד ליום Valid to
פרטים אודות בעל זכות החתימה בתאגיד או במוסד הציבורי		פרטים אודות מורשה החתימה בתאגיד או במוסד הציבורי Subject
שם מלא CN	"Avraham Shlomo ID_012345678"	
שם משפחה (אנגלית) SN	" Avraham "	
שם פרטי (אנגלית) G	" Shlomo"	
מספר זהות SERIALNUMBER	"01-012345678"	
O (קוד זיהוי ולאחריו מספר ח"פ)	05-519999999	
OU – שם תאגיד/מוסד ציבורי באנגלית	<u>Comda LTD.</u>	
תפקיד T	Manager	
מדינה C	"IL"	
אורך המפתח הציבורי של בעל התעודה	RSA (2048 Bits)	
מפתח ציבורי Public Key		
קישור לרשימת התעודות המבוטלות (CRL)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/Corporations.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/Corporations.crl	הפצת CRL CRL Distribution Points
קישור לשרת OCSP	[1]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il/ocsp [2]Authority Information Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	הפצת OCSP (On-line Certificate Status Protocol)

30 48 30 3c 06 08 2b 06 0H0<..+. 01 05 05 07 0b 01 30 3000 30 2e 81 29 54 68 69 73 0..)This 20 63 65 72 74 69 66 69 certifi 63 61 74 65 20 69 73 20 cate is 6c 69 6d 69 74 65 64 20 limited 74 6f 20 35 30 2c 30 30 to 50,00 30 20 4e 49 53 81 01 20 0 NIS.. 30 08 06 06 04 00 8e 46 0.....F 0b 01.	QC Statement	1.3.6.1.5.5.7.1.3
93 a1 4b 84 20 bc de 68 60 9b dc 85 d5 83 51 cd 8c d9 c8 b2	KeyID	Authority Key Identifier
[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.2.1.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ComSign Notice Number=11 פנים =Notice Text בעל התעודה זוהה פנים אל פנים על סמך תעודות ו/או מידע מזהה אחר. על השימוש בתעודה זו יחולו נהלי קומסיין חבות ואחריות קומסיין מוגבלות כמפורט בנהלים השימוש בתעודה הינו בכפוף לנוהל זכויות החתימה בתאגיד/מוסד ציבורי. הגבלות נוספות על השימוש בתעודה – אופציונאלי The email address in the subject alternative name field is NOT verified by the issuer and is NOT trusted	נהלים (CPS) להסדרת פעילותו של הגורם המאשר (ComSign) כתובת הדואר האלקטרוני של בעל התעודה לא אומתה על ידי הגורם המאשר לצורכי הסתמכות	מדיניות התעודה Certificate Policies

בתעודה למורשה מטעם מוסד ציבורי: "תעודה לחתימה אלקטרונית ל_____ (שם המוסד הציבורי) ומורשה חתימה מטעמו לתפקיד _____ (תיאור התפקיד). תעודה זאת מותקנת על גבי התקן רשתי שבידי בעל התעודה/מאוחסן אצל _____ (צד ג') – במידה והתעודה הותקנה על גבי התקן כאמור		
(Secure Email (1.3.6.1.5.5.7.3.4 נ / א Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)	תיאור המטרות לשמן מיועדת התעודה. מטרות אלו משתנות לפי סוג התעודה, חתימה וזיהוי בהתאמה.	Enhanced Key Usage
פרטים אודות בעל זכות החתימה בתאגיד או במוסד הציבורי		פרטים אודות מורשה החתימה בתאגיד או במוסד הציבורי בעברית Subject Alternative Name
"Shlomo@test.co.il"	כתובת דואר אלקטרוני כפי שנמסרה על ידי בעל התעודה RFC822 Name	
"IL"	מדינה C	
05-51999999	O קוד זיהוי ומספר ח"פ – בעברית	
קומדע בע"מ	OU – שם תאגיד/מוסד ציבורי בעברית	
"מנהל"	T תפקיד	
"אברהם"	שם משפחה (עברית) SN	
"שלמה"	שם פרטי (עברית) G	
ID_012345678	שם מלא CN שם בעל התעודה בעברית ומספר זהות	
[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2(Alternative Name: URL=http://fedir.comsign.co.il/cacert/Corporations.crt		Authority Information Access

3b a0 59 1c 5f 7c 2b 1f f0 3f df e0 25 55 09 67 10 f2 52 b6		Subject Key Identifier
Digital Signature, Non-Repudiation, Key (Encipherment (e0	תיאור המטרות לשמן ניתן להשתמש בתעודה	Key Usage
"sha1"	האלגוריתם לחתימה שאיתו נחתמה התעודה	אלגוריתם החתימה Thumbprint Algorithm
f1 36 18 f7 fe 2a 1a 34 24 47 e6 7f 85 24 " "93 40 4d d5 18 73	פרטי התעודה חתומים על ידי הגורם המאשר	ערך החתימה Thumbprint
* בשלב זה – תפקידי O וOU בתעודות משהב"ט – הפוכים (שם תאגיד=O)		

מבנה התעודה למגנא (iv)

דוגמא	תאור	שם שדה
"V3"	גרסת התעודה	גרסא Version
7f 26 0e 3c bd 8b b1 7b ea 6f ca a5 3f af 15 71	המספר הסידורי של התעודה. מספר זה הינו ערך חד ערכי.	מספר סידורי Serial Number
"sha1RSA"	אלגוריתם החתימה בו ישתמש בעל התעודה. יכול להיות מסוג SHA2 או SHA1 ע"פ הנחיות הרשם	אלגוריתם חתימה Signature Algorithm
שדות המתארים את הגורם המאשר		הגורם המאשר
"IL"	מדינה C	Issuer
"ISA"	שם הגורם המאשר - O	
"ComSign ISA Magna Issuing CA"	שם מלא CN	
שדות המתארים את תוקף התעודה		תוקף
"יום שלישי 10 דצמבר 2002 06:10:33"	יום תחילת תוקף (תאריך ההנפקה)	תקף מיום Valid from
"יום חמישי 08 דצמבר 2003 05:24:21"	יום תפוגת תוקף	תקף עד ליום Valid to
פרטים אודות בעל זכות החתימה בתאגיד או במוסד הציבורי		פרטים אודות

Amir Israeli ID#012345678@IL "000000007876"	שם מלא – CN שם מלא של בעל התעודה, מספר זהות ומספר החותם	מורשה החתימה בתאגיד או במוסד הציבורי Subject
"עמיר"	שם פרטי (עברית) G	
"ישראל"	שם משפחה (עברית) SN	
"ID#012345678@IL"	0.9.2342.19200300.100.1.1	
Magna	OU – שם יחידת משנה תאגיד/מוסד ציבורי באנגלית	
ISA	O – שם תאגיד/מוסד ציבורי באנגלית	
"IL"	מדינה C	
בעל התעודה זוהה פנים אל פנים על סמך תעודות ו/או מידע כנדרש בחוק אמצעי אימות החתימה נבדק ואושר על השימוש בתעודה זו יחולו נהלי קומסיין. חבות ואחריות קומסיין מוגבלות כמפורט בנהלי קומסיין (CPS) האחריות הכוללת של קומסיין ונציגיה כלפי כל אדם בעניין תעודה ספציפית תהא מוגבלת לעניין תעודות המונפקות למבקשי תעודות (1) הנדרשים לעשות בהם שימוש על פי חיקוק או (2) לפי דרישת רשות מרשויות המדינה לסכום שלא יעלה על סכום 500,000 (חמש מאות אלף) שח לגבי כלל החתימות האלקטרוניות ועיסקאות הקשורות לאותה תעודה השימוש בתעודה על ידי מורשה חתימה בתאגיד/מוסד ציבורי, כפוף לנהלי זכויות החתימה בתאגיד/מוסד ציבורי בהתאמה קומסיין רשומה במרשם רשם הגורמים המאשרים בישראל	2.5.4.65	
RSA (2048 Bits)	אורך המפתח הציבורי של בעל התעודה	מפתח ציבורי Public Key
Client Authentication (1.3.6.1.5.5.7.3.2(Microsoft Trust List Signing ((1.3.6.1.4.1.311.10.3.1	ייעוד התעודה	Enhanced Key Usage
KeyID=40 e6 4a 17 0c 2b dc d1 e1 0c 29 b4 ba 85 44 55 d0 2f e5 8c	Key Identifier של תעודת הביניים	Authority Key Identifier
Subject Type=End Entity Path Length Constraint=None		Basic Constraints

[1] "Certificate Policy: Policy Identifier=User Notice [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=Replace This Text Notice Number=1 Notice Text=Please Press The [More Info] Button To Access The Hebrew CPS" The email address in the subject alternative name field is NOT verified by the issuer and is NOT trusted	נהלים (CPS) להסדרת פעילותו של הגורם המאשר (ComSign) כתובת הדואר האלקטרוני של בעל התעודה לא אומתה על ידי הגורם המאשר לצורכי הסתמכות	מדיניות התעודה Certificate Policies
[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/ISA.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/ISA.crl	התעודות לרשימת קישור המבוטלות (CRL)	הפצת CRL Distribution Points
[1]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il/ocsp [2]Authority Information Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	קישור לשרת OCSP	הפצת OCSP (On-line Certificate Status Protocol)

amirisraeli@test.co.il	כתובת דואר אלקטרוני כפי שנמסרה על ידי בעל התעודה- RFC822 Name	פרטים אודות מורשה החתימה Subject Alternative Name
30 17 30 15 06 03 55 1d 0.0...U. 09 31 0e 13 0c 30 30 30 .1...000 30 30 30 30 30 37 38 37 00000787 36 6	Subject Directory Attributes	2.5.29.9
b 98 bd 66 b2 3e f5 5a bf 82 6f c7 b8 ad 4e 7c b1 1 82 91 85		Subject Key Identifier
Digital Signature, Non-Repudiation (c0(		Key Usage
"sha1"	האלגוריתם לחתימה שאיתו נחתמה התעודה	אלגוריתם החתימה Thumbprint Algorithm
"7e a2 c8 0b ed 87 1a 80 7d a8 06 77 69 c0 cd 9a 68 d6 2e da"	פרטי התעודה חתומים על ידי הגורם המאשר	ערך החתימה Thumbprint

(v) מבנה תעודה לשם מתחם SSL/TLS DV (שרתי אינטרנט)²² – ראה סעיף 7.1.2.3 (iv) בנספח -
(21)

(vi) מבנה תעודת SSL/TLS לשרת אינטרנט של ארגון (OV)²³ – ראה סעיף 7.1.2.3 (v) בנספח -
(22)

7.1.3. מזהי אובייקט אלגוריתמיים (OIDs – Algorithmic object identifiers):

קומסיין עושה שימוש באלגוריתם החתימה הבא:

SHA256 with RSA Encryption – OID 1.2.840.113549.1.1.11

7.1.4. צורות שם:

שמות שונים עשויים להופיע בתעודות המונפקות על ידי קומסיין בהתאם למתואר בסעיף 3.1.

השמות עשויים להיות מבין הבאים:

²² סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

²³ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

- שם אדם או שם ארגון כפי שהוא מופיע בתעודה המשמשת לזיהוי, כמפורט בסעיף 3.2.
- כתובת דואר אלקטרוני לפי תקן rfc822 כפי שנמסרה על ידי בעל התעודה.
- שם במבנה Distinguished name לפי תקן rfc1779, הכולל שדות כגון CN, O, OU, C, G, SN, T

7.1.4.1 מידע אודות הגורם המנפיק

תוכן Distinguished Name Field של מנפיק התעודה יהיה תואם תמיד ל- Subject DN של הגורם המאשר.

7.1.4.2 שדה Subject Information בתעודה

על ידי הנפקת התעודה מאשרת קומסיין שהיא מקיימת אחר דרישות מסמך הנהלים וכי נכון למועד הנפקת התעודה המידע בשדה ה-Subject Information הוא מדויק. קומסיין תציין שם מתחם או כתובת IP רק בהתאם לאמור בסעיפים 3.2.2.4 ו-3.2.2.5.

7.1.4.3 שדה הרחבה Subject Alternative Name

ראה סעיף 7.1.2. קומסיין לא תנפיק תעודות עבור Reserved IP Addresses או Internal Names.

7.1.4.4 שדות Subject Distinguished Name

עבור שדות אפשריים ל-Subject DN ראה סעיף 7.1.2. כל המידע הכלול יאומת בהתאם למוסדר בסעיפים 3.2.2 ו-3.2.3.

שדות ה-Subject DN יכילו רק מידע בעל משמעות המתייחס לבעל התעודה ולא מטהדטה כמו " ", "-ו-", " (רווח) או כל סימון של ערך חסר, לא שלם או לא רלוונטי.

7.1.5 הגבלות על שמות:

קומסיין אינה מיישמת מגבלה על שמות, ובלבד שהשמות יהיו תואמים לתנאים המפורטים בסעיף 3.1.

7.1.6. מזהה אובייקט למדיניות תעודות אלקטרוניות:

תעודות המונפקות על ידי קומסיין תואמות למדיניות קומסיין שהיא בעלת מזהה האובייקט הבאים:

(i) בתעודה ליחיד בהתאם לחוק: OID 1.3.6.1.4.1.19389.2.1.1

למזהה אובייקט והשימוש בהם לשרתי אינטרנט שלא בהתאם לחוק ראה סעיף 7.1.6 בנספח - (23).

לפירוט נוסף בדבר מזהה אובייקט בתעודת השורש, בתעודת הביניים או בתעודות למנויים ראה סעיף 7.1.2 לעיל.

7.1.7. מדיניות שימוש בשדות הרחבה מגבילים:

לא נעשה שימוש בשדה הרחבה להגבלת מדיניות (Policy constraints extension).

7.1.8. מבנה ותחביר למאפייני מדיניות תעודות אלקטרוניות:

קומסיין מציינת בשדה מדיניות התעודות הפניה למסמך זה ולמדיניות התעודות המפורטת בו.

קומסיין מציינת בשדה הצהרת תעודות מאושרות (QCStatement) תאימות לתקני חתימה אלקטרונית מאושרת, לפי מפרט של מספר ארגונים בין-לאומיים, כמפורט בנהלי קומסיין הפנימיים.

במקרה בו מונפקת תעודה אלקטרונית לאמצעי חתימה השמור על גבי התקן רשתי תצוין עובדה זו בתעודה האלקטרונית בשדה מדיניות התעודה (certificate policies). ככל שמדובר בהתקן רשתי המאוחסן בידי צד ג' תצוין עובדה זו בתעודה האלקטרונית בשדה מדיניות התעודה (certificate policies) **במפורש** וכך ידע המסתמך הפוטנציאלי כי אמצעי החתימה מאוחסן על גבי התקן רשתי - מאוחסן בידי צד ג' זר לבעל אמצעי החתימה ולארגון בשמו הוא חותם. יובהר כי ההנפקה על גבי התקן רשתי הינה בכפוף להנחיות הרשם ובתנאים שייקבעו על ידו.

7.1.9. הבהרה לענין קוד המדינה המופיע על גבי תעודה אלקטרונית המונפקת ליחיד תושב

הרשות הפלסטינית או תאגיד פלסטיני הרשום ברשות הפלסטינית:

קומסיין תוסיף על גבי התעודה האלקטרונית את ההבהרה הבאה בעברית ובאנגלית:

"The information provided under the "country code" section is based on the ISO-3166 Code, is for technical purposes only, and is without prejudice to the legal status of any country or territory or of its authorities."

"המידע המופיע תחת סעיף "country code", הינו בהתאם לתקן ISO-3166, הינו טכני בלבד ואין בו כדי להוות אמירה כלשהי ו/או להשליך על המעמד המשפטי של מדינה, טריטוריה, רשות או

7.2 מבנה רשימת התעודות המבוטלות ("CRL")

7.2.1 מספר/י גירסה:

קבצי ה-CRL הם בגרסה 2.

7.2.2 CRL וסיומות רישומי CRL

פרופיל רשימת CRL

שם שדה	תיאור	דוגמא
גרסא		V2
הגורם המאשר	שדות המתארים את הגורם המאשר (O, OU, CN)	
	שם הגורם המאשר CN	לדוגמא "Corporations"
	שם הארגון O	"Comsign Ltd."
	מדינה	"IL"
תוקף	שדות המתארים את תוקף ה-CRL	
	מועד פרסום ה-CRL	"יום שלישי 10 דצמבר 2002 06:10:33"
	מועד פרסום ה-CRL הבא (לכל המאוחר)	"יום רביעי 11 דצמבר 2002 06:10:33"
אלגוריתם חתימה	אלגוריתם החתימה בו נחתם קובץ ה-CRL	sha256
תעודות מבוטלות	שדות המתארים את התעודות המבוטלות	
	המספר הסידורי של התעודה. חד ערכי.	"bc be ac 46 8b 09 ad e5 2d 31 ed f0 00" "8e 02 ed ab"
	התאריך שבה בוטלה התעודה	"יום שלישי 10 דצמבר 2002 02:10:33"
	תאריך תחילת הבטלות (אי-תוקף) של התעודה	"יום שלישי 10 דצמבר 2002 02:10:33"

unspecified	(0)	סיבת ביטול התעודה	
keyCompromise	(1)		
cACompromise	(2)		
affiliationChanged	(3)		
superseded	(4)		
cessationOfOperation	(5)		
certificateHold	(6)		
removeFromCRL	(8)		
privilegeWithdrawn	(9)		
aACompromise	(10)		
למשל: 1e		מספר סדרתי של רשימת ה – CRL	מספר סידורי

7.3 פרופיל מצב אישור מקוון (OCSP)

7.3.1 מספר/י גירסה:

גרסת מענה לפניות OCSP הינה 1.

7.3.2 סיומות OCSP:

שם שדה	תיאור	דוגמא
Responder ID	מזהה המאפשר לזהות את משיב OCSP. המזהה יכול לעשות שימוש בשם או ב-HASH של המפתח הציבורי של המשיב.	byKey: f39bbeb80201bbdb8d7f9bebe5f4011a3dac25b5
Produced At	תאריך ושעת החתימה על מענה OCSP	2016-12-07 12:04:25 (UTC)
Cert ID	פרטי זיהוי של התעודה שתקפותה נבדקת אל מול משיב OCSP. הפרטים כוללים: 1. אלגוריתם גיבוב, 2. ערך גיבוב של שם השרת המנפיק, 3. ערך גיבוב של המפתח הציבורי של השרת המנפיק, 4. מספר סידורי של התעודה	hashAlgorithm (SHA-1) Algorithm Id: 1.3.14.3.2.26 (SHA-1) issuerNameHash: 7b7f618dd153e1d2f7ad862f000cc6f0a116bcb0 issuerKeyHash: f5bbadea31234b005d5b4f76de6f8b02e0fddff0 serialNumber: 0x00e8d3baab1b84226459fb12378cd6f459
Cert Status	סטטוס התוקף של התעודה	יכול לקבל את הערכים הבאים: [0] good [1] revoked

[2] unknown		
thisUpdate: 2016-12-07 08:00:17 (UTC) nextUpdate: 2016-12-08 08:00:18 (UTC)	תחילת וסוף התוקף של מקור המידע המשמש את מגיב OCSP לצורך המענה	This Update Next Update
sha256WithRSAEncryption	אלגוריתם חתימה על מענה OCSP	Signature Algorithm
1c12e794f305b2ca183f1da117c465deb4fc21667146a 2ae...	חתימת המשיב על המענה	Signature
signedCertificate version: v3 (2) serialNumber: 0x0e2bcda4aa4f8f..... signature (sha256WithRSAEncryption) Algorithm Id: 1.2.840.113549.1.1.11 issuer: validity: subject: subjectPublicKeyInfo: extensions:	התעודה המשמשת לחתימה על תשובת OCSP	Certificate

8. ביקורות תאימות

8.1. תדירות או נסיבות עריכת ביקורות:

קומסיין כפופה לנהלי עבודה פנימיים המאושרים על ידי הרשם ובמסגרת הסמכות שהוקנתה לרשם גם להליכי ביקורת ובדיקה בהתאם לחוק ולתקנות. כמו כן נערכות בקומסיין ביקורות בהתאם לתקנה 4 לתקנות חתימה אלקטרונית (גורם מאשר) ולצורך הגשת חוות דעת של מבקר לרשם כנדרש בחוק ובתקנותיו.

הביקורת האמורה מתבצעת על בסיס שנתי ובמידת הצורך או על פי דרישת הרשם, גם בתדירות גבוהה מכך.

כמו כן, לצורך עמידה בתקנים ת"י 27001 ו- ISO 9000/9001, יערכו ביקורות כנדרש בתקנים הנ"ל על-ידי גופים שיש להם רישיון לערוך ביקורות כנדרש על-פי התקנים.

על קומסיין לבצע דיווח שנתי הכולל פירוט ההנפקות של תעודות אלקטרוניות מאושרות על גבי התקן רשתי ודיווח חציוני בדבר בדיקות אבטחת מידע שבוצעו להתקנים רשתיים עליהם בוצעו הנפקות מכוח אישור סוג שניתנו על ידי הרשם. במקרה בו יונפקו תעודות אלקטרוניות מאושרות על גבי אמצעי חתימה המאוחסן על גבי התקן רשתי המצוי בשליטתו של צד ג' נדרשת, קודם להנפקת התעודות האלקטרוניות, בדיקה של התוכנה שמותקנת על גבי שרת החתימות באמצעות מומחה אבטחת מידע אפליקטיבי וכן בדיקת התצורה הכוללת באמצעות יועץ אבטחת מידע ובאמצעות המבקר. ככל שמבוצע שימוש חוזר באותה תוכנה ובאותה תצורה אצל לקוחות שונים – אין צורך בביקורת חוזרת.

קומסיין מקיימת אחר כל דרישות ה-CAB Forum, לרבות דרישת עריכת ביקורות תקופתיות ודיווחים.

8.2. זהות עורך הביקורת:

עורך הביקורת בהתאם לחוק ולתקנות הוא איש מקצוע מוסמך בתחום אבטחת מידע להנחת דעתו של הרשם.

עורך הביקורת בהתאם לדרישת ה-CAB Forum הוא איש ביקורת המקיים את דרישות ההסמכה של WEBTRUST ו/או ETSI.

8.3. עצמאות עורך הביקורת:

עורך הביקורת הוא קבלן עצמאי אשר אינו עובד קומסיין ואינו כפוף לקומסיין בכל צורה שהיא.

8.4. נושאים הנבדקים במסגרת הביקורת:

נושאי הביקורת מפורטים בהנחית רשם גורמים מאשרים 2/2015.

8.4.1. לנושאים הנבדקים במסגרת הביקורת על הנפקת תעודות לשרתי אינטרנט²⁴ - ראה סעיף

8.4.1 בנספח - (24)

8.5. פעולות נדרשות לאור ממצאי כשל ותקלות:

קומסיין תבחן את דוחות הביקורת ותדאג לתקן את הטעון תיקון, אם בכלל, בהקדם האפשרי.

8.6. הפצת תוצאות הביקורת:

ממצאי הביקורת נחשבים למידע סודי שאיננו מיועד להפצה למעט הבאתו לידיעת רשם גורמים מאשרים, הנהלת הגורם המאשר והגורמים האחראים על התחומים הרלבנטיים בהם נמצאו ממצאים הדורשים טיפול ותיקון במסגרת הגורם המאשר.

קומסיין כן מפרסמת את ממצאי ביקורת ה-WebTrust וניתן לעיין בהם במאגר של קומסיין ב-

www.comsign.co.il/repository

8.7. עריכת ביקורת עצמית:

קומסיין עורכת ביקורת עצמית רבעונית במהלכה מבוקרת פעילותה והתאמתה למסמך הנהלים, לנהלי העבודה הפנימיים ולדרישות ה-CAB Forum. הביקורת מתבצעת באופן מדגמי ביחס ללא פחות מ-3% מהתעודות שהונפקו במהלך תקופת הביקורת.

²⁴ סעיף זה איננו מיושם בהליך הנפקת תעודה אלקטרונית מאושרת במסגרת החוק ולא נבדק/אושר על ידי הרשם.

9. סוגיות משפטיות ועסקיות נוספות

9.1. תשלומים

9.1.1. תשלום בגין הנפקת או חידוש תעודות:

קומסיין גובה תשלום עבור שירותי הנפקת וחידוש תעודות אלקטרוניות. תעריפי קומסיין משתנים מעת לעת ומושפעים מהיקף השירות הניתן וסוג התעודות. למען הסר ספק מובהר בזאת כי שינויים במחירי שירותי קומסיין לא יחולו רטרואקטיבית.

9.1.2. תשלום עבור גישה לרשימת התעודות האלקטרוניות:

קומסיין איננה גובה תשלום עבור גישה לתעודות אלקטרוניות מכל סוג אחר, ככל שהדבר אפשרי.

9.1.3. תשלום עבור בדיקת סטאטוס התעודות האלקטרוניות:

קומסיין איננה גובה תשלום עבור גישה לרשימת התעודות המבוטלות (CRL) לצורך בדיקת הסטאטוס שלהן.

9.1.4. תשלום עבור שירותים אחרים:

קומסיין זכאית לגבות תשלום עבור שירותים שונים להם תתבקש וזאת בהתאם לתעריפיה כפי שייקבעו מעת לעת.

9.1.5. מדיניות החזרים:

בכפוף להוראת כל דין, תעודה שבוטלה לבקשת בעל התעודה או מכל סיבה אחרת שאין מקורה בקומסיין, לרבות תעודה שחודשה קודם מועד פקיעתה ביחס לפרק הזמן שבין מועד החידוש לתאריך הפקיעה המקורי – לא תזכה את בעליה בהחזר, לרבות לא בהחזר חלקי/יחסי.

9.2. חבות כספית

9.2.1. כיסוי ביטוחי:

קומסיין מבטחת את אחריותה המקצועית בסכום ובתנאים בהתאם להוראות הדין ולהנחת דעתו של הרשם.

9.2.2. בטוחות אחרות:

קומסיין העמידה את כל הבטוחות והערבויות הנדרשות לפעילותה כגורם מאשר במסגרת החוק.

9.2.3. ביטוח או ערובה למשתמשי קצה:

קומסיין תעמיד ערבות בנקאית או ערובה אחרת או ביטוח, כמתחייב מסעיפים 11(א)(3) ו-15(ב) לחוק ומפרק ג' לתקנות חתימה אלקטרונית (גורם מאשר) ולפי קביעת הרשם, וזאת לשם הבטחת פיצויו של מי שנפגע עקב מעשה או מחדל הנובע מאי עמידת קומסיין בהתחייבויותיה על פי נהלים אלו. סכום הערבות הינו סכום שנקבע על ידי הרשם מעת לעת על פי שיקול דעתו הבלעדי של הרשם ומשקף, בין היתר, את הסיכון שמקורו בהנפקת תעודות אלקטרוניות מאושרות על גבי התקן רשתי

9.3. הגנה על סודיות מידע עסקי

9.3.1. מידע עסקי סודי:

מובהר לבעל התעודה כי כל מידע המופיע בשדות התעודה, גם ככל היותו נחשב מידע עסקי סודי בעיני בעל התעודה, לא ייחשב ככזה ולא ייהנה מהגנה. מומלץ, לכן, לבעל התעודה להימנע מהכללתו בשדות התעודה של מידע שאיננו נדרש ושעשוי להיחשב כמידע עסקי סודי.

בה בעת ייתכן כי בעל התעודה יידרש על ידי קומסיין להעמיד לרשותו מידע הנוגע לעסקו ולאופן ניהולו, בין לצורכי זיהוי, בין לצורכי חיוב וגביה ובין לצורך זכאותו של מבקש לתעודה מסוג מסוים. מידע כאמור, שאיננו נכלל בשדות התעודה, יישמר בארכיב קומסיין כמידע סודי שהגישה אליו מוגבלת למורשים בלבד ועל בסיס צורך ישיר בגישה אליו לשם מילוי תפקידם במסגרת שירותי הנפקת התעודות האלקטרוניות של קומסיין.

יובהר כי מידע עסקי שאיננו נמנה על המידע הנקוב בשדות התעודה האלקטרונית או ברשימת התעודות המבוטלות ובאופן רגיל היה נחשב כמידע סודי, אך פורסם ברשות הרבים על ידי הרשאי לפרסמו ככזה – לא ייחשב עוד כמידע סודי עסקי.

9.3.2. מידע עסקי שאיננו מוגן:

תוכן שדות התעודה האלקטרונית ורשימת התעודות המבוטלות, גם בהיותם מידע עסקי, לא ייחשבו כמידע סודי הזכאי להגנה.

9.3.3. חובת ההגנה על מידע סודי עסקי:

למעט במסגרת המידע המתפרסם בשדות התעודה האלקטרונית, קומסיין מתחייבת לשמור בסודיות את המידע הסודי העסקי של בעל התעודה ולא לגלותו לצד ג' כלשהו אלא כקבוע ובכפוף לכל דין.

9.4. הגנה על סודיות מידע פרטי

9.4.1. מדיניות הגנה על פרטיות המידע:

מאגרי המידע של קומסיין רשומים אצל רשם מאגרי המידע ובהתאם לחוק הגנת הפרטיות, התשמ"א-1981 וקומסיין תפעל בהתאם ובכפוף לחוק האמור ובהתאם להנחיות ודרישות הרשם בעניינים אלו, כפי שיהיו מעת לעת.

קומסיין מיישמת מדיניות הגנה על פרטיות שאת הוראותיה המעודכנות ניתן לקבל בכל עת.

9.4.2. מידע הנחשב כמידע פרטי סודי:

כל מידע הקשור לזהותו של בעל התעודה ולרשומות העוסקות בהליך הנפקת התעודה האלקטרונית, למעט מידע שפורסם בשדות התעודה האלקטרונית, או ברשימת התעודות המבוטלות או שנחשף, ככזה, ברשות הרבים על ידי מי שהיה מוסמך לפרסמו – ייחשב כמידע פרטי סודי.

9.4.3. מידע פרטי שאיננו מוגן:

תוכן שדות התעודה האלקטרונית ורשימת התעודות המבוטלות, גם בהיותם מידע אישי פרטי סודי, לא ייחשבו כמידע סודי הזכאי להגנה.

9.4.4. חובת ההגנה על הפרטיות:

קומסיין מתחייבת לשמור בסודיות את המידע האישי הסודי של בעל התעודה ולא לגלותו לצד ג' כלשהו אלא כקבוע ובכפוף לכל דין.

9.4.5. גילוי והסכמה לשימוש במידע פרטי:

קומסיין לא תעשה כל שימוש במידע פרטי של בעל התעודה שנמסר לידיה במסגרת הליך הנפקת התעודה האלקטרונית והנחשב לסודי ללא אישור והסכמה מפורשת של בעל התעודה.

9.4.6. גילוי מידע במסגרת הוראה שיפוטית או מנהלית:

מובהר בזאת כי קומסיין תמלא אחר כל הוראה מחייבת של רשות שיפוטית או מנהלית המורה לה לחשוף מידע, פרטי או עסקי, שנמסר לידיה על ידי המבקש או בעל התעודה, לרבות מידע הנחשב כסודי. במידת האפשר ובכפוף לכל הגבלה או איסור שיוטלו על קומסיין על ידי הגוף המוסמך הדורש את חשיפת המידע, תביא קומסיין לידיעת בעל המידע את דבר גילוי בהתאם לדרישה האמורה.

נדרשה קומסיין לגלות מידע סודי של בעל התעודה במסגרת הליכים שהיא איננה צד ישיר להם או במקרה בו ביקש בעל התעודה למנוע את גילוי של המידע וכתוצאה מכך נגרמו לקומסיין הוצאות משפטיות ואחרות, ישיב לה בעל התעודה את מלוא ההוצאות בהן חבה.

9.4.7. נסיבות אחרות לגילוי מידע פרטי:

ההגבלות על גילוי של מידע סודי לא יחולו במקרה של עריכת ביקורות מטעמו של רשם גורמים מאשרים או רשם מאגרי מידע.

9.5. זכויות קניין רוחני

זכויות הקניין במידע ובנתונים שבמסמך זה ובמבנה התעודה האלקטרונית המונפקת על ידי קומסיין נחשבים קניינה של קומסיין ואין לעשות בהם כל שימוש בלא אישורה המפורש, מראש ובכתב, של קומסיין.

9.6. מצגים וחובות

9.6.1. מצגים וחובות של הגורם המאשר:

קומסיין מצהירה כי במהלך פעילותה כגורם מאשר תוודא כי אין בתעודה האלקטרונית מצגי שווא עובדתיים הידועים לקומסיין; כי אין כל טעויות תעתיק בנתונים כפי שהתקבלו על ידי קומסיין ממבקש התעודה, הנובעים מהימנעותה של קומסיין לנקוט זהירות סבירה ביצירת התעודה; כי התעודה עומדת בכל הדרישות המהותיות של נהלים אלה ובדרישות החוק ותקנותיו; כי כל המידע המובא בתעודה או הכלול בה בדרך של אזכור, למעט כתובת הדואר האלקטרוני של בעל התעודה כפי שנמסרה על ידו ולא אומתה על ידי קומסיין, אומת על-ידי קומסיין באופן סביר; כי לאחר הנפקת תעודה, לא תחול על קומסיין חובה נמשכת לחקור ולבדוק את מידת הדיוק והנכונות של המידע הכלול בבקשה להנפקת תעודה, אלא אם נמסרה לקומסיין הודעה מפורשת כי פרט מהפרטים המופיעים בתעודה אינו נכון וקומסיין השתכנעה באופן סביר ממהימנות ההודעה. במקרה בו יוברר כי התעודה כוללת מצגי שווא עובדתיים, תבוטל התעודה וניתן יהיה, לבקשת בעל התעודה, להנפיק לו תעודה חדשה הכוללת את המידע המעודכן.

קומסיין לא תהא אחראית לנזק שנגרם עקב הסתמכות על תעודה אלקטרונית שהנפיקה, אם הוכיחה כי נקטה את כל האמצעים הסבירים לקיום חובותיה על פי החוק ומסמך הנהלים. אחריותה של קומסיין לנזק כאמור כפופה להגבלות כמפורט בפרק זה להלן. מבלי לגרוע מהאמור לעיל, קומסיין מחויבת לספק את התשתית ואת שירותי הנפקת התעודות, ובכלל זה הקמת, פרסום ותפעול המאגר של קומסיין באופן זמין ואמין כנדרש בחוק וכמפורט בנהלים אלה; לספק את הבקורות והבסיס של תשתית המפתח הציבורי (PKI) של קומסיין, ובכלל זה הגנה על המפתחות של קומסיין וקיום נהלים לשותפות סוד, כפי שאלה מוצגים בנהלים אלה; לבצע את נהלי האימות של הבקשות לתעודות, כמפורט בנהלים אלה; להנפיק תעודות בהתאם לנהלים ולכבד את המצגים השונים הניתנים לבעלי התעודות ולצדדים המסתמכים בנהלים אלה; לפרסם מאגר תעודות בטלות באופן זמין, מקוון ומיידית למי שמבקש להסתמך על תעודה אלקטרונית מסויימת כמפורט בנהלים; לבצע את התחייבויותיו של גורם מאשר ולשמור על זכויות בעלי התעודות והצדדים המסתמכים המשתמשים בתעודות, בהתאם לנהלים ובהתאם לחוק ולתקנותיו; לבטל תעודות כנדרש בנהלים; לטפל בחידוש של תעודות כקבוע בנהלים.

9.6.2. מצגים וחובות של גורמים רושמים של קומסיין:

האמור בסעיף 9.6.1 לעיל יחול על גורמים רושמים של קומסיין ככל שרלוונטי לפעולות המבוצעות על ידם. ראה גם סעיף 9.17 להלן.

9.6.3. מצגים וחובות של בעל התעודה:

על בעל התעודה חלה החובה למסור לקומסיין מידע מלא, נכון ועדכני הדרוש לזיהויו או לזיהוי המורשה מטעמו ולהנפקת התעודה האלקטרונית לאמצעי החתימה שלו לרבות המידע הכלול בה; לנקוט במשך כל תקופת תוקף התעודה האלקטרונית בכל האמצעים הסבירים כדי לשמור את אמצעי החתימה בשליטתו המלאה ולמנוע את הגישה אליו ואת השימוש בו על ידי אחרים;

לדווח לקומסיין מייד לכשהובא לידיעתו על פגיעה בשליטתו באמצעי החתימה או שימוש לא מורשה בו או שינוי במידע או בפרטים מכוחם הונפקה לו התעודה האלקטרונית לרבות מידע הכלול בתעודה ולקיים את כל החובות, ההוראות והאזהרות הנקובות בהסכם המנוי.

9.6.4. מצגים וחובות של צד מסתמך:

צד מסתמך מצהיר ומתחייב כי קודם להסתמכות על תעודה אלקטרונית או על המידע הכלול בה הוא יבדוק ויוודא כי התעודה האלקטרונית בתוקף, יבדוק את הגבלות השימוש בתעודה האלקטרונית וכי הגבלות אלו אינן חלות על המסר האלקטרוני החתום וכי המורשה בשם תאגיד או מוסד ציבורי אכן הוסמך לחתום בשם התאגיד או המוסד הציבורי ולחייבו בחתימתו האלקטרונית המאושרת על המסר האלקטרוני.

צד מסתמך שלא יקיים חובותיו אלו יישא בעצמו ולבדו בכל נזק או הוצאה שייגרמו לו או למי מטעמו או לצד ג' אחר כתוצאה מהסתמכותו של הצד המסתמך על התעודה האלקטרונית וקומסיין לא תישא בכל אחריות ולא תשפה או תפצה מי מהאמורים על כל נזק או הוצאה שנגרמו להם.

9.6.5. מצגים וחובות של צדדים משתתפים אחרים:

לא רלבנטי.

9.7. פטור מערבויות ומצגים

קומסיין ו/או נציגיה אינם ערבים לכך שבעלי התעודות לא יתכחשו לתעודה או למסר כלשהו (יובהר כי נושא ההתכחשות או אי התכחשות לחתימה מוסדרים על פי דין); אינם ערבים לתוכנה כלשהי למעט הטכנולוגיה והתוכנות המשמשות את קומסיין להנפקת התעודות ולהתקן עליו שמור אמצעי החתימה אם סופק על ידי קומסיין; אינם אחראים לנזקים כלשהם שנגרמו עקב הסתמכות על תעודה בטלה אשר פרטיה פורסמו כחוק ברשימת התעודות הבטלות קודם להסתמכות כאמור ובלבד שהוכיחו כי נקטו בכל האמצעים הסבירים לקיום חובותיהם על פי החוק ומסמך נהלים זה; לא יחובו בגין כל נזק עקיף, הנובע ו/או הקשור לשימוש כלשהו ולכל מטרה שהיא בתעודות האלקטרוניות ו/או בחתימות האלקטרוניות וחבותם של קומסיין ו/או נציגיה תחול על נזקים ישירים בלבד הנובעים באורח טבעי ובמהלכם הרגיל של הדברים מאי קיום חובותיה של קומסיין על-פי החוק.

התעודות האלקטרוניות אינן מיועדות לשימושים בצידוד בקרה בנסיבות מסוכנות ו/או לשימושים הדורשים ביצועים חסיני כשל, כגון הפעלת מתקנים גרעיניים, ניווט כלי טייס או מערכות תקשורת, מערכות לבקרת תנועה אווירית ו/או מערכות בקרת נשק ו/או מקום שכשל עלול להוביל במישרין למוות או לנזק גוף או לגרום נזק סביבתי.

9.8. הגבלת אחריות של קומסיין ונציגיה

אחריותה של קומסיין נקבעת על פי דין ומוגבלת על פי סעיף 21 לחוק ועל-פי דין. קומסיין רשאית להגביל את אחריותה על-פי הוראות סעיף 21 (ב) לחוק, לרבות לעניין סוגי השימושים בתעודה או סכומי העסקאות שלגביהן ניתן לעשות שימוש בתעודה.

פורטו הגבלות כאמור על גבי התעודה האלקטרונית, לא תהיה קומסיין אחראית לנזק שנגרם עקב שימוש החורג מההגבלה. כמו כן קומסיין רשאית להגביל את אחריותה כלפי בעל תעודה בהסכם המנוי, ובלבד שהסכם כאמור אינו סותר את הוראות החוק או את הוראות מסמך זה.

הגבלות על שימוש בתעודה לבקשת בעל התעודה יעשו לבקשתו המפורשת של בעל התעודה בלבד. אופן הבקשה יקבע באישור הרשם.

קומסיין רשאית להגביל את אחריותה הכוללת בגין שימוש בחתימה אלקטרונית, והמגבלה תופיע באופן בולט בתעודה ותמסר למבקש תעודה טרם הנפקתה. קומסיין תפרסם במקום בולט באתר האינטרנט שלה את מדיניות הגבלת האחריות שלה ביחס לסוגי תעודות שונות.

בכל מקרה שהוא, האחריות הכוללת של קומסיין ו/או נציגיה כלפי כל הצדדים (לרבות, בין היתר, מבקש, בעל תעודה או צד מסתמך) לא תעלה על תקרת החבות הרלוונטית, כמפורט להלן:

1) בכל הקשור לתעודות המונפקות למבקשי תעודות (א) הנדרשים לעשות בהן שימוש למילוי דרישות חתימה לפי חוק, או (ב) לפי דרישת רשות מרשויות המדינה, לא תעלה על סך של 500,000 ₪ לגבי חתימה בודדת אחת כמו גם כלל החתימות האלקטרוניות שבוצעו וכלל העסקאות הקשורות לאותה תעודה.

2) האחריות הכוללת המשולבת של קומסיין ונציגיה כלפי כל אדם בגין כל תעודה אחרת תהא מוגבלת לסכום שלא יעלה על סך של 50,000 (חמישים אלף) ₪ לגבי כלל החתימות האלקטרוניות שבוצעו וכלל העסקאות הקשורות לאותה תעודה ולסך של 10,000 (עשרת אלפים) ש"ח, לגבי ביצוע חתימה אלקטרונית בודדת אחת והעסקאות הקשורות לאותה חתימה בודדת.

ההגבלה על נזקים ודמי הנזק כאמור לעיל חלה על אובדן ונזק מכל מין שהוא, לרבות, נזקים ישירים, פיצויים, נזקים עקיפים, מיוחדים, תוצאתיים, פיצויים לדוגמא או נזקים נלווים, הנגרמים לאדם כלשהו לרבות, מגיש בקשה, בעל תעודה, צד מסתמך או צד ג' כלשהו, ואשר נגרמים בשל הסתמכות על תעודה, או שימוש בתעודה, שקומסיין מנפיקה או מנהלת אותה, משתמשת בה או משעה או מבטלת אותה, או בשל הסתמכות על תעודה שפגה או שימוש בתעודה שפגה. הגבלה זו על נזקים ודמי נזק חלה גם על חבות חוזית, נזיקית ועל כל תביעת חבות. בכפוף לאמור לעיל, תקרת החבות לגבי כל תעודה תהא זהה מבלי להתייחס למספר החתימות האלקטרוניות, העסקאות, או התביעות בקשר לאותה תעודה. במידה וסכום התביעות עולה על תקרת החבות, תקרת החבות הקיימת תוקצה תחילה לתביעות המוקדמות יותר על מנת להגיע ליישוב סופי של המחלוקת, אלא אם בית משפט מוסמך יורה אחרת. בשום מקרה, קומסיין לא תהא מחויבת לשלם סכום העולה על תקרת החבות הכוללת לגבי כל תעודה, מבלי להתייחס לשיטת חלוקת תקרת החבות בין מספר תובעים.

9.9. שיפוי

חובת שיפוי, ככל שתוטל, לא תחרוג מההגבלה הנקובה בסעיף 9.8 לעיל.

9.10. תוקף מסמך הנהלים וסיומו

9.10.1. תוקף מסמך הנהלים:

מסמך נהלים זה, וכל שינוי או תיקון בו, ייכנס לתוקף ויבטל את גרסתו הקודמת, מיד עם אישורו על ידי רשם גורמים מאשרים ופרסומו בכתובת הגורם המאשר:
<http://www.comsign.co.il/cps>

9.10.2. פקיעת תוקף הנהלים:

נהלי קומסיין, כפי שישתנו מעת לעת, יישארו בתוקפם עד להחלפתם בגרסה חדשה של הנהלים שאושרה על ידי הרשם.

9.10.3. תוצאות פקיעה ושמירת תוקף:

תעודות אלקטרוניות תונפקנה רק בהתאם למסמך הנהלים בתוקף במועד ההנפקה. לא תונפקנה תעודות אלקטרוניות הכפופות להוראותיו של מסמך נהלים שפקע, והוראות מסמך הנהלים שפקע תמשכנה לחול על התעודות האלקטרוניות שהונפקו במהלך תקופת תוקפו.

9.11. הודעות

כל עת שצד כלשהו לנהלים אלה מעוניין או נדרש למסור הודעה, דרישה או בקשה בנוגע לנהלים אלה, המסר האמור יינתן תוך שימוש במסרים חתומים אלקטרונית באופן המתיישב עם דרישות נהלים אלה, או בכתב. מסרים אלקטרוניים יהיו תקפים כאשר השולח יקבל מן הנמען אישור קבלה תקף. אישור הקבלה האמור חייב להתקבל בתוך חמישה (5) ימים, אחרת יש לשלוח הודעה בכתב. מסרים בכתב לקומסיין חייבים להימסר באמצעות שירות בלדרות שמאשר מסירה בכתב או באמצעות דואר רשום, לכתובת קומסיין.

מקומסיין או מגורם רושם לאדם אחר: אל הכתובת הרשומה המעודכנת ביותר. כל גורם רושם של קומסיין יודיע מיידית לקומסיין על כל הודעה משפטית שנמסרה לו ואשר עלולה להשפיע על קומסיין.

האמור לא יחול על:

- 1) הודעה לביטול תעודה כאמור בסעיף 4.9 Error! Reference source not found. לעיל.
- 2) הודעה לתיאום מועד הנפקה כאמור בסעיף 4.1.2 לעיל.
- 3) הודעה על מועד פקיעת תעודה ואפשרות לחידוש טלפוני כאמור בסעיף 4.6 לעיל.

9.12. שינויים ותוספות

9.12.1. נהלים לביצוע שינויים:

תיקון למסמך הנהלים יכול שיעשה בדרך של עדכון חלקי. בוצע 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 היא בתוקף. ניתנת אורכה של 60 יום מיום פרסום עותק מעודכן של מסמך הנהלים, לציבור מחזיקי התעודות, להציע התנגדויות, תיקונים או השגות - על מנת שקומסיין תוכל לשקול אותם ואף להעבירם להתייחסות הרשם במידת הצורך. כל מי שיפנה – יקבל תשובה בכתב לפנייתו מקומסיין. לא תהיה התייחסות להערות שיתקבלו לאחר 60 יום מיום פרסום מסמך נהלים מעודכן.

9.12.2. אופן פרסום השינויים:

נוסח מעודכן של מסמך הנהלים יפורסם באתר הגורם המאשר בכתובת <http://www.comsign.co.il/cps>.

9.12.3. נסיבות לשינוי מזהה האובייקט (OID):

הכנסת שינויים למסמך הנהלים לא תחייב שינוי מזהה האובייקט (OID).

9.13. יישוב מחלוקות

קודם להפעלת מנגנון כלשהו ליישוב סכסוכים (לרבות התדיינות משפטית או בוררות) לגבי מחלוקת המערבת היבט כלשהו של נהלים אלה או תעודה שהונפקה על ידי קומסיין, גורמים שנפגעו יודיעו על כך לקומסיין, לגורם הרושם ולכל צד אחר למחלוקת, על מנת לנסות לפעול ליישוב המחלוקת בינם לבין עצמם.

9.14. הדין החל

נהלים אלו נוסחו בהתאם לדיני מדינת ישראל מבלי להתייחס להוראות דינים ו/או כללים הנוגעים לברירת הדין וללא דרישה להוכחת קשר מסחרי לישראל. על נהלים אלו יחולו דיני מדינת ישראל. ברירת הדין נקבעה על מנת להבטיח נהלים אחידים ופרשנות אחידה לכל המשתמשים, בלא קשר למקום מגוריהם או למקום בו הם משתמשים בתעודות שלהם.

קומסיין מצהירה כי נהלים אלו נערכו בהתאמה לתקן ETSI TS 456 ודרישות ה-CAB Forum.

9.15. כפיפות לחוקים

נהלים אלה כפופים לדיני מדינת ישראל, להוראות החוק ותקנותיו ולהנחיות הרשם.

9.16. שונות

9.16.1. שלמות הנהלים:

נוסחם של נהלים אלה מחליף כל נוסח אחר אשר היה קיים קודם לכן, ולא יהיה כל תוקף לכל נוסח אחר, בין אם בכתב ובין אם בע"פ, בין במפורש ובין במשתמע, אלא כאמור בנהלים אלו, כפי שיתוקנו מעת לעת.

9.16.2. המחאת זכויות וחובות:

קומסיין תהא רשאית להמחות זכויותיה ו/או חובותיה כמפורט בנהלים אלו לכל גורם אחר בכפוף לקבלת אישור הרשם מראש ובכתב.

9.16.3. הוראות סותרות:

בכל מקרה של סתירה בין הוראות החוק והתקנות והנחיות הרשם ובין הוראות מסמך זה – יגברו הוראות החוק והתקנות והנחיות הרשם. בכל מקרה של סתירה בין הוראות הסכם המנוי ובין הוראות מסמך זה – יגברו הוראות מסמך זה בכל מקרה של סתירה בין מסמך נהלים מעודכן למסמך נהלים קודם – יגברו הוראות מסמך הנהלים המעודכן.

9.16.4. אכיפה:

נהלים אלו מחייבים את הגורם המאשר וכל הפועל מטעמו וכן את בעל התעודה, המורשה מטעמו, צד מסתמך וכל הפועל מטעמו ותנאיהם יהיו ניתנים לאכיפה על כל אחד מהם.

שום ויתור, הנחה, דחייה, מתן ארכה או הימנעות מפעולה במועד מצד קומסיין ו/או בעל התעודה לא יפורש כוויתור מצדם על זכויותיהם כפי שמופיעות בנהלים אלו ולא ישמשו כטענה או כמניעה לתביעה מצדם.

הכותרות וכותרות המשנה בנהלים אלה תואמות את תקן RFC 3647, מובאות למען הנוחות והאזכור בלבד ולא ייעשה בהן שימוש בפרשנות, בפירוש או באכיפה של הוראות כלשהן של נהלים אלה. הנספחים, לרבות ההגדרות לנהלים אלה, מהווים לכל מטרה ועניין חלק בלתי נפרד ומחייב מהנהלים.

אלא אם נקבע אחרת, נהלים אלה יפורשו באופן המתיישב עם הוראות החוק והתקנות ועם הסביר מסחרית באותן נסיבות. בפירוש נהלים אלה, יש להתייחס להיקף וליישום הבינלאומי שלהם, ליתרונות הטמונים בעידוד אחידות ביישומם ולשמירה על תום לב.

9.16.5. כוח עליון:

קומסיין ונציגיה לא יהיו אחראים בגין כל הפרת חבות, עיכוב או הימנעות מביצוע על פי נהלים אלה, הנובעים מאירועים שמעבר לשליטתם כגון, כוח עליון, מלחמות, תקופות חירום משקי, מגפות, הפסקות חשמל, שריפות, רעידות אדמה, ואסונות אחרים, ובלבד שלא היה באפשרות קומסיין להיערך לקראת אירועים אלה באופן סביר.

9.17. הסדרים נוספים - גורמים רשמיים

9.17.1. מבוא

חלק משירותי הנפקת התעודות הניתנים על ידי קומסיין יכול שינתנו באמצעות נציגים מטעמה. נציגי קומסיין יאשרו על ידי הרשם בטרם מינוים לתפקיד גורם רשם. הנציגים מופעלים על פי שיקול דעתה של קומסיין ובכפוף לאישור הרשם מראש ובכתב לאחר שקומסיין הגישה לו בקשה מפורטת. נציגי קומסיין ייטלו חלק בשירותי קומסיין, בכל הנוגע לטיפול בקבלת הבקשות לתעודות אלקטרוניות וזיהוי ורישום המבקשים. נציגי קומסיין מתחייבים לפעול בהתאם לחוק, תקנותיו והנחיות הרשם ולעמוד בכל הדרישות השונות המפורטות בנהלים אלה.

קומסיין אחראית לפעילות נציגיה בהתאם לקבוע בחוק.

הפעולות המפורטות בסעיף 3.2.2.4 אינן בגדר סמכותו של גורם רושם של קומסיין.

9.17.2. בקשה של גורם לפעול כגורם רושם של קומסיין:

כל אדם ו/או תאגיד ו/או מוסד ציבורי המעוניין לפעול כגורם רושם של קומסיין יגיש לקומסיין בקשה חתומה שאומתה ואושרה על-ידי עו"ד. לא תטופל בקשה לא מאומתת ו/או שאיננה מכילה את כל המידע הנדרש. הבקשה תכלול, בין היתר, את הפרטים הבאים:

- שם, כתובת, מספרי פקסימיליה וטלפון, כתובת(ות) דואר אלקטרוני של מגיש הבקשה, אנשי הקשר האדמיניסטרטיביים שלו ונציגיו המוסמכים.
- פירוט כל מידע שיש בו כדי להצביע על מהימנותו של מגיש הבקשה (לדוגמא, חדלות פירעון בהווה או בעבר) ושעשוי להשפיע מהותית על יכולתו של מגיש הבקשה לפעול כגורם רושם של קומסיין.
- העתקים מאושרים של תעודת התאגדות, מסמכי היסוד של התאגיד, פרוטוקולי החלטות המוסדות המתאימים של התאגיד להתמנות ולפעול כגורם רושם של קומסיין וכן פרוטוקול המסמך את מי שמונה מטעם התאגיד לפעול כנציג התאגיד ולהתחייב בשמו בכל הנוגע למינוי התאגיד כגורם רושם של קומסיין.
- אישור עו"ד בדבר תחום פעילות התאגיד, זהות נציג התאגיד המוסמך להתחייב בשמו ומטעמו וכן אישור כי ההחלטות של המוסדות המתאימים של התאגיד להתמנות ולפעול כגורם רושם של קומסיין תקפות ומחייבות את התאגיד וכי התקבלו בהתאם למסמכי ההתאגדות של התאגיד ולהחלטותיו.
- התחייבות לקיים בדווקנות את כל הוראות החוק ותקנותיו.
- הצהרה של מגיש הבקשה לפיה יש ביכולתו לקיים את דרישות הנהלים, וכן התחייבות מגיש הבקשה למלא בדווקנות אחר הוראות הנהלים.
- כל מידע אחר הנדרש על ידי קומסיין, על-ידי רשם הגורמים המאשרים או לפי החוק ותקנותיו.
- הנציג שמגיש את הבקשה יעשה את כל הפעולות הנדרשות ויחתום על כל המסמכים הנדרשים לצורך קבלת אישור רשם הגורמים המאשרים למינוי כגורם רושם של קומסיין.

9.17.3. המען להגשת בקשה לקומסיין לפעול כגורם רושם

של קומסיין:

בקשות לפעול כגורם רושם של קומסיין, המכילות את כל המידע והמסמכים הנדרשים על-ידי קומסיין ולפי החוק ותקנותיו ומאושרות ומאומתות על ידי עו"ד (וכוללות מידע משלים כפי הנדרש) יוגשו למשרדי קומסיין אשר תעביר את הבקשות לאחר שאושרו על ידה לרשם הגורמים המאשרים לצורך קבלת אישורו הסופי.

9.17.4. אחריות לפעולות גורמים רושמים:

קומסיין אחראית לפעולות גורמים רושמים מטעמה בהתאם לקבוע בחוק.

נספח

הנהלים המפורטים בנספח זה מתייחסים לדרישות שמקיימת קומסיין ולשירותים שמספקת קומסיין ושאינם חלק מהדין הישראלי ואינם נתונים לפיקוח הרשם. להסרת כל ספק, הנהלים המפורטים בנספח זה לא נבדקו ולא אושרו על ידי הרשם.

(1) 1.3.2.1 דרישות נוספות מגורם רושם של שירות הנפקת תעודות אלקטרוניות לאתרי אינטרנט

קומסיין רשאית לבצע את הפעולות המפורטות בסעיף 3.2 למסמך הנהלים והעוסקות בהנפקת תעודות אלקטרוניות לאתרי אינטרנט באמצעות גורם רושם ובלבד שהתקיימו כל הדרישות של סעיף 3.2 כמו גם יתר הנהלים במסמך זה, בשינויים המתחייבים.

(2) 2.1 המאגר של קומסיין

לצורך פעילותה קומסיין מנהלת אוסף בסיסי נתונים המיועדים לאחסון ולשליפה של תעודות ושל מידע אחר שקשור בהן, שיכונן להלן ביחד המאגר. המאגר של קומסיין כולל, בין היתר, את מאגרי המשנה הבאים: מאגר תעודות אלקטרוניות תקפות (לרבות התעודה של קומסיין) בכל הקשור לתעודות שהונפקו לשרתי אינטרנט (שמות מתחם) גם פירוט בדיקות האימות שביצעה קומסיין עובר להנפקת התעודה האלקטרונית ביחס לכל שם מתחם וכל כתובת IP, מאגרי תעודות בטלות, מידע על ביטול תעודות ורשימות תעודות בטלות, ומידע אחר כפי שיוחלט על ידי קומסיין מעת לעת ובכפוף להנחיות הרשם.

רק חלק מהמידע המפורסם במאגר של קומסיין פתוח לעיון הציבור הרחב. לעיון מבוקר פתוחה רשימת התעודות הבטלות המפרטת את מספרה הסידורי ותאריך ביטול התעודה.

(3) 2.2 פרסום מידע הנוגע לתעודות באמצעות המאגר של קומסיין

קומסיין מקיימת את הדרישות המעודכנות של ה-CAB Forum המתפרסמות ב- <http://www.cabforum.org> ובכל מקרה של אי התאמה בין נהלים אלו וה- Baseling Requirements for the Issuance and Management of Publicly-Trusted Certificates, אלו יגברו על נהלים אלו.

(4) 3.1.3 שימוש בכינוי או הימנעות מציון שם בתעודות אלקטרוניות לשרתי אינטרנט:

קומסיין רשאית להנפיק תעודה אלקטרונית לשרתי אינטרנט הנושאת שם כינוי של בעל התעודה ושאיננה נוקבת בשמו של בעל התעודה (תעודה אנונימית).

(5) 3.1.6 אימות כתובות דואר אלקטרוני הנקובות בתעודות SSL:

בנוסף לאמור בסעיף 3.1.6 למסמך הנהלים, ביחס לתעודות SSL, כתובות דואר אלקטרוני הנמסרות על ידי המבקש לצורך צרופן לתעודה נבדקות על ידי קומסיין, לעניין תקינותן ושיכון למבקש.

(6) 3.2.2.1 אימות זהות בהנפקת תעודה אלקטרונית לשרת הנושאת את שם הארגון:

קומסיין תאמת את זהות הארגון ואת כתובתו באמצעות אחד מהאמצעים הבאים, לפחות:

(i) מרשם ממשלתי המתנהל במקום הקמת הארגון או פעילותו.

(ii) מאגר מידע המעודכן באופן שוטף ומנוהל על ידי צד ג' אמין.

(iii) ביקור פיזי באתר הפעילות על ידי עובד קומסיין או נציגה.

(iv) מכתב אישור המידע חתום על ידי עו"ד, רואה חשבון או נושא תפקיד ממשלתי.

לחילופין, קומסיין רשאית לוודא את כתובת הארגון (אך לא את זהותו) באמצעות חשבון צריכת מים, חשמל וכדומה, דף חשבון בנק או כל אמצעי אחר הנחשב כאמין בעיני קומסיין.

במקרה בו הארגון מבקש כי בנוסף לשדה ה-CommonName תכיל התעודה גם מידע על מיקומו, קומסיין תוודא את זהות מדינת הארגון כמוסדר בסעיף 3.2.2.3 בנספח זה להלן ותוסיפו לשדה ה-Country.

במקרה בו הארגון מבקש כי בנוסף לשדה ה-CountryName תכיל התעודה גם מידע על זהותו, קומסיין תוודא את זהות הארגון ואת אמינות הבקשה כמוסדר בסעיף זה.

כל מסמך המוגש במסגרת סעיף זה ייבחן על ידי קומסיין לשלילת אפשרות של שינוי או זיוף.

(7) 3.2.2.2. אימות שימוש בשם עסק/שם מסחרי בתעודה אלקטרונית לשרת

אם המידע הכלול בתעודה אמור לכלול שם עסק/שם מסחרי, קומסיין תאמת את זכאות האתר לעשות שימוש בשם העסק/שם מסחרי באמצעות אחד, לפחות, מהאמצעים הבאים:

(v) תיעוד מטעם או התכתבות עם גוף ממשלתי במקום רישום האתר או פעילותו.

(vi) הסתמכות על מאגר מידע אמין.

(vii) על בסיס אישור של גוף ממשלתי האחראי לרישום שמות עסק או שמות מסחריים.

(viii) מכתב אישור המידע חתום על ידי עו"ד, רואה חשבון או נושא תפקיד ממשלתי.

(ix) חשבון צריכת מים, חשמל וכדומה, דף חשבון בנק או כל אמצעי אחר הנחשב כאמין בעיני קומסיין.

(8) 3.2.2.3. אימות ציון שם מדינה בתעודה אלקטרונית לשרת

אם מבקשים לציין את שם המדינה בהקשר לשרת בשדה subject:CountryName, קומסיין תאמת את המידע באמצעות אחד, לפחות, מהאמצעים הבאים:

(x) בדיקת כתובת ה-IP של השרת ביחס לטווח הכתובות המוקצות על ידי המדינה או כתובת ה-IP של המבקש.

(xi) ה-ccTLD של שם המתחם המבוקש.

(xii) מידע שסופק על ידי מנהל מרשם שמות המתחם, או

(xiii) אמצעי המפורט בסעיף 3.2.2.1 בנספח זה לעיל.

קומסיין תנסה לסנן שרתי proxy כדי למנוע הסתמכות על כתובות IP שהוקצו במדינה שונה ממדינת הפעילות של התאגיד.

(9) 3.2.2.4. אימות הרשאה או שליטה בשם מתחם בתעודה אלקטרונית לשרת

במסגרת הנפקת תעודות SSL לארגונים, קומסיין תאמת את זהות בעל שם המתחם או איש הקשר מטעמו כדי למנוע התחזות הומוגרפית של IDNs. קומסיין מבצעת סריקות של אתרים שונים כדי לאתר את הבעלים של שם מתחם מסוים. במקרה של ממצא שלילי, פקיד הרישום ידחה בקשה של שם מתחם הנחזה להכיל מספר סקריפטים במסגרת שם המתחם.

הזמנות שמקורן בתאגידים גדולים, שמות מסחר מפורסמים ומוסדות פיננסיים ייבדקו באופן מדוקדק והנפקת התעודה האלקטרונית תושהה עד להשלמת הבדיקה. במקרים אלו, איש הקשר חייב להיות עובד קבוע של הארגון. שיטות האימות במקרה זה יכללו אחד מהבאים:

(i) אימות הזיקה של איש הקשר לשם המתחם

הבדיקה תתבצע ישירות מול רשם שמות המתחם ביחס ל-FQDN המבוקש. במסגרת זאת קומסיין תאמת את זהות המבקש כמוסדר בסעיף 3.2.2.1 ואת הרשאתו כמוסדר בסעיף 3.2.5 להלן.

(ii) אימות הזיקה של איש הקשר לשם המתחם באמצעות דוא"ל, פקס, מסרון או דואר

קומסיין תאשר את שליטת המבקש על ה-FQDN באמצעות משלוח תוכן בעל ערך אקראי באמצעות דוא"ל, פקס, מיסרון או דואר רגיל שישלחו לכתובת הקשר של שלם המתחם וקבלת תשובה המכילה את התוכן בעל הערך האקראי מהכתובת הנשגרת. התוכן האקראי ישתנה בכל פעם ותוקפו לא יעלה על 30 יום.

(iii) אימות שליטת המבקש בשם המתחם באמצעות דוא"ל מובנה

הדוא"ל יישלח לכתובת שתיווצר על ידי שימוש בביטויים: "admin", "administrator", "webmaster", "hostmaster" or "postmaster" כשלאחריו סימן כרוכית (@) ושם המתחם. הדוא"ל יכיל תוכן בעל ערך אקראי ויידרש מענה המכיל את התוכן בעל האופי האקראי. התוכן בעל האופי האקראי יוחלף בכל הודעת דוא"ל וישאר בתוקף לא יותר מאשר 30 יום לצורך מענה.

(iv) אימות זיקת המבקש לכתובת המתחם באמצעות תעודה מאשרת

ניתן לאמת את זיקת המבקש ל-FQDN המבוקש על ידי בדיקת הרשאתו של המבקש לקבל תעודה אלקטרונית כמוסדר במסמך הרשאה שמקורו ברשם שמות המתחם או בבעל הרשום של המתחם. תאריך מסמך ההרשאה חייב להיות לא לפני יום הגשת הבקשה לקומסיין או במקרה בו הוא נושא תאריך מוקדם – לא חל שינוי במידע הנוגע למרשם שם המתחם.

(v) אימות זיקת המבקש לכתובת המתחם באמצעות שינוי מוסכם לאתר

הבדיקה תתבצע באמצעות אימות אחד מהבאים תחת ספריית `/.well-known/pki-validation` או תחת נתיב אחר הרשום אצל IANA לצורכי אימות שמות מתחם שקומסיין תערוך באמצעות HTTP/HTTPS:

- איתורו באתר של ערך אקראי המכיל לפחות 112 ביטים שנמסר על ידי הגורם המאשר למבקש התעודה לצורך הוספתו בתוך קובץ או בעמוד ווב בצורה של תגית מטה. או,
- איתורו של ערך המחולל באופן שקבע הגורם המאשר והמקשר אותו למפתח של הבקשה לתעודה אלקטרונית. הערך יכול ויכיל חותמת יום-שעה כמו גם מידע אחר המצביע על ייחודו.

(vi) אימות זיקת המבקש לכתובת המתחם באמצעות שינוי DNS

הבדיקה תאתר תוכן בעל ערך אקראי או ערך המחולל באופן שקבע הגורם המאשר כמוסבר לעיל ב-DNS TXT או רישום CAA לאימות שם מתחם או כזה שתחילתו עם תגית המתחילה בסימן עם קו תחתי.

(vii) אימות זיקת המבקש לכתובת המתחם באמצעות כתובת IP

בדיקה לוודא שתשובה מחיפוש DNS לרישומי A או AAAA תואמת את הקבוע בסעיף 3.2.2.5 בנספח זה להלן.

(viii) אימות זיקת המבקש לכתובת המתחם באמצעות ערך אקראי

הבדיקה תאתר קיומו של ערך אקראי, כמוסבר לעיל, בתעודה של הרשאת שם המתחם הנגישה לגורם המאשר באמצעות TLS.

3.2.2.5 (10) אימות כתובת IP

על קומסיין לוודא שכל כתובת IP הרשומה בתעודה האלקטרונית נשלטת על ידי מבקש התעודה במועד ההנפקה. הבדיקה באמצעות:

(i) דרישה מהמבקש להוכיח שליטה מעשית בכתובת ה-IP באמצעות עריכת שינוי מוסכם

מראש בתוכן דף אינטרנט מקוון שהגישה אליו כוללת את כתובת ה-IP.

(ii) הצגת תיעוד מ-IANA או מרשם אינטרנט אזורי (RIPE, APNIC, ARIN, AfriNIC)

LACNIC המאשר את הקצאת כתובת ה-IP.

(iii) ביצוע חיפוש-לאחור של כתובת ה-IP ולאחר מכן ווידוא שליטה בשם המתחם שהתקבל

בחיפוש כמוסדר בסעיף 3.2.2.4.

3.2.2.6 (11) אימות שימוש בתו כללי בשם מתחם

קודם להנפקת תעודה הכוללת תו כללי (wildcard character) בשדה ה-CN או subjectAltName מסוג DNS-ID כאשר התו הכללי מופיע כתו ראשון משמאל ב-registry-controlled או בסיומת ציבורית, קומסיין תדרוש מהמבקש להוכיח בעלות בכל ה-Domain Namespace. כדי להבחין בין registry-controlled לבין החלק של ה-country code Top Level Domain Namespace, קומסיין תסתמך על מאגרי סיומות ציבוריות כגון <http://publicsuffix.org>.

3.2.2.7 (12) בחינת אמינות מקור המידע

קודם להסתמכות על מקור מידע, קומסיין תבחן את מהימנותו, דיוקו, אמינותו וחסינותו מפני שינויים לא מורשים. הבחינה תכלול את השיקולים הבאים:

(i) רמת העדכניות של המידע.

(ii) תדירות העדכון של מקור המידע.

(iii) זהות ספק המידע ולצורך מה נאסף המידע.

(iv) מידת הנגישות הציבורית לבסיס המידע.

(v) הקושי היחסי בשינוי או זיוף המידע.

3.2.2.8 (13) בדיקת מרשמי גורמים מאשרים מוסמכים (CAA Records)

קומסיין תבדוק במרשמי גורמים מאשרים המוסמכים להנפיק תעודות לשמות מתחם כל dNSName בסיומת ה-subjectAltName של התעודה אותה מבקשים להנפיק וזאת בהתאם לנוהל ב-RFC 6844.

תעודות יונפקו על ידי קומסיין במסגרת זמן החיים (TTL) של ה-CAA Record או בתוך 8 שעות, לפי הממושך יותר.

קומסיין לא תנפיק תעודה שממצאי הבדיקה לגביה העלו סימון קריטי.

קומסיין לא תנפיק תעודה אלא אם כן :

- (i) תוכן הבקשה לתעודה תואם את מרשמי ה-CAA Record. או,
- (ii) קיימת החרגה ב-CP או ב-CPS הרלבנטיים. החרגה זאת יכול שתהיה רק אחת מהבאות :
 - a. במקרה בו נוצרה תעודת בדיקה (pre-certificate) וזאת נרשמה לפחות בשני מרשמי לוגים של Certificate Transparency שה-CAA שלהם נבדק.
 - b. וויתור על בדיקת CAA במקרה בו התעודה היא תעודת ביניים המוגבלת טכנית (technically constraint) המונפקת על ידי גורם מאשר כפוף בעל סמכות מוגדרת וויתור על הצורך בבדיקת CAA מופיע במפורש בהסכם עם הלקוח.
 - c. וויתור על בדיקת CAA כאשר קומסיין או חברת בת שלה הינם מפעיל ה-DNS (כמוגדר ב-RFC 7719) של שם המתחם.

במקרה של כשל בביצוע הבדיקות, קומסיין תנפיק תעודה רק בהתקיים כל אלו :

- a. מקור הכשל מחוץ לתשתית של קומסיין.
 - b. בוצעה לפחות בדיקה חוזרת אחת.
 - c. לתחום שם המתחם אין אישור DNSSEC בשרשור לשורש ה-ICANN.
- קומסיין תתעד אירועים פוטנציאליים שנמנעו בעקבות בדיקת CAA Rrecord לצורך העברת דיווח ל-CA/Browser Forum.

4.1.3 (14) הגשת בקשה לתעודה לשרת אינטרנט

בקשה להנפקת תעודה אלקטרונית לשרת אינטרנט תכיל את המידע והמסמכים הבאים :

- (i) בקשה להנפקת תעודה. הבקשה יכול ותוגש באופן אלקטרוני.
 - (ii) חתימה על הסכם מנוי. החתימה וההסכם יכול ויוגשו באופן אלקטרוני.
- קומסיין רשאית לדרוש מסמכים ותיעוד נוסף בהתאם לדרישת הנהלים וה-CA/Browser Forum.

4.2.1.1 (15) ביצוע פעולות זיהוי ואימות של בקשה לתעודה לשרת אינטרנט

- (i) קומסיין תשאב את כל המידע הדרוש לה מהבקשה, מהמבקש עצמו או ממקור מידע אמין ועצמאי שמקורו בצד ג'. קומסיין מפעילה נהלים ומדיניות שמטרתם לאמת את כל המידע הכלול בתעודה לפי דרישת הלקוח. על המבקש לספק לקומסיין, בין היתר, לפחות שם מתחם מאושר ורשום אחד, או כתובת IP לצורך הכללתם בשדה ה-SubjectName בתעודה.

- (ii) מידע ומסמכים הנמסרים לקומסיין בהתאם לסעיף 3.2 יכולים לשמש גם הם לצורך הנפקת התעודה ובלבד שלא חלפו יותר מאשר 825 יום מקבלתם.
- (iii) קומסיין מיישמת נוהל מתועד המזהה ודורשת אימות נוסף במקרה של בקשות המסומנות כבקשות בסיכון מוגבר והמקיים אחר דרישות ה-CAB Forum.
- (iv) קומסיין מאמתת קיום ותוכן CAA records קודם להנפקת התעודה האלקטרונית. קומסיין פועלת בהתאם ל-CAA Records, ככל שקיימים כמוסדר בסעיף 3.2.2.8. שמות המתחם בשימוש קומסיין הם : comsign.co.il, comsign.co.uk, comsigneurope.com.

4.2.2.1 (16) אישור או דחיית בקשה להנפקת תעודה לשרת אינטרנט

- (i) קומסיין תנפיק תעודות רק לשמות מתחם עם סיומות ציבוריות שאושרו על ידי ICANN ולא תנפיק תעודות לשמות מתחם עם סיומות פנימיות.
- (ii) קומסיין לא תנפיק תעודות המכילות gTLD חדש המצוי בבדיקה על ידי ICANN. קומסיין תנפיק תעודה למבקש רק לאחר שוודאה את זכותו הבלעדית בשם המתחם כמוסדר בסעיף 3.2.2.4 בנספח זה לעיל.

4.9.1.1 (17) הנסיבות לביטולה של תעודה אלקטרונית לשרת אינטרנט

קומסיין תבטל תעודה אלקטרונית שהונפקה לשרת אינטרנט בכל אחד מהנסיבות המנויות בסעיף 4.9.1 במסמך הנהלים ובנוסף לכך כאשר בידי קומסיין יימצאו ראיות לפיהן לא ניתן להוסיף ולהסתמך על בדיקת הבעלות בשם המתחם או בשליטה ב-FQDN או בכתובת ה-IP שבתעודה או שהמשך השימוש בהם נאסר בצו שיפוטי או בהוראת חוק.

4.9.13.1 (18) נסיבות המאפשרות התליית תעודה אלקטרונית לשרת אינטרנט

כל נסיבה מכוחה יש לבטל תעודה שהונפקה לשרת אינטרנט (ראה סעיף 4.9.1.1 לנספח זה) תיחשב כנסיבה מכוחה ניתן להתלות את תוקף התעודה האלקטרונית. שיקול הדעת של הגורם המאשר באם להתלות את התעודה או לבטלה יותנה בנסיבות נוספות ובבקשת בעל התעודה או מי שהוסמך על ידו לבקש את התלייתה או ביטולה במסגרת הסכם המנוי.

4.9.15 (19) אופן הטיפול בבקשת התלייה לתעודה אלקטרונית שהונפקה לשרת אינטרנט:

אופן הטיפול בבקשה להתליית תעודה אלקטרונית לשרת אינטרנט יהיה כמוסדר בסעיף 4.9.3 לעיל שעניינו אופן הטיפול בבקשה לביטול תעודה.

6.3.2 (20) משך תקופת תוקף השימוש לתעודה אלקטרונית לשרת אינטרנט ובצמד המפתחות

משך תקופת תוקף השימוש לתעודה אלקטרונית לשרת אינטרנט לא יעלה, בכל מקרה, על 825 ימים.

7.1.2.3 (21) מבנה תעודה לשם מתחם SSL/TLS DV (שרתי אינטרנט)

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. This number is single-value	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"

Signature algorithm	The signature algorithm used by the certificate owner. The hash algorithm is of SHA2 type.	“sha256RSA”
Issuer (CA)	Fields describing the CA	
	Full name – CN	ComSign Organizational CA
	CA name – O	“ComSign Ltd”
	Locality – L	“Tel Aviv”
	Country -C	“IL”
Validity	Fields describing the certificate’s validity	
Valid from	Date the certificate becomes valid (issue date)	“Tuesday, November 04 06:10:33 2014”
Valid to	Expiration date	“Thursday, November 02 05:24:21 2017”
Subject	Details of the Individual Certificate Owner	
	CN – A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	“www.test.com”
	OU – A fixed description of the certificate type.	“Domain Control Validated”
Public Key	Public key of the certificate owner length	RSA 2048 Bits
Authority Information Access	indicates how to access information and services for the issuer: [1] OCSP Service location. [2] Certification Authority Issuer Certificate	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cacert/ComsignOrganizationalCA.crt
Authority Key Identifier	Key Identifier of an intermediate certificate	KeyID=f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0
Certificate policies	Specifies the regulations for operations of the CA (ComSign Organizational CA): [1] ComSign CPS – DV Section [2] Domain validated with Compliance to the Baseline Requirements of the CA/Browser Forum – No entity identity asserted	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.3.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1

CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/ComsignOrganizationalCa.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/ComsignOrganizationalCa.crl
Enhanced Key Usage	purposes for which the certified public key may be used	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Identification of the certificate according to its particular public key	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"
Subject alternative name	A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	"www.test.com"
Key Usage	Description of the purposes for which it is permissible to use the certificate. This field is marked as CRITICAL.	Digital Signature, Key Encipherment (a0)

(i) השדה להלן שמור בתעודה לשימוש הגורם המאשר (CA) כדי לקיים את דרישות ה-

: CA/Browser Forum

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1).

(ii) התעודה תואמת את דרישות ה-CA/Browser Forum ואינה כוללת Subject

.DomainName authorization Identity Information למעט

(iii) תעודות DV-SSL כוללות גם הפניה ב-certificatePolicies extension למסמך

הנהלים של קומסיין המבהירה כי התעודה מקיימת אחר דרישת ה-CAB Forum

Policy Identifier=1.3.6.1.4.1.19389.3.1.1

[1,1]Policy Qualifier Info:

Policy Qualifier Id=CPS

Qualifier:

<http://www.comsign.co.il/CPS>

(iv) תעודות DV-SSL לא כוללות בשדה ה-Subject את : ,streetAddress ,organizationName

,state Or ProvinceName או PostalCode. לאור זאת כוללות התעודה את השדה הבא

subject:organizationalUnitName: OU = "Domain : הני"ל : שנועד להבהיר את היעדר הני"ל :

"Control Validated". כמו כן שדה ה-OU לא יכיל כל שם, שם מסחרי, כתובת, מיקום או תוכן אחר המתייחס לאדם או לישות חוקית.

(22) 7.1.2.3 (v) מבנה תעודת SSL/TLS לשרת אינטרנט של ארגון (OV)

Field Name	Description	Example
Version	Certificate Version	"V3"
Serial number	The certificate's serial number. This number is single-value	"f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0"
Signature algorithm	The signature algorithm used by the certificate owner. The hash algorithm is of SHA2 type.	"sha256RSA"
Issuer (CA)	Fields describing the CA	
	Full name – CN	ComSign Organizational CA
	CA name – O	"ComSign Ltd"
	Locality – L	"Tel Aviv"
	Country – C	"IL"
Validity	Fields describing the certificate's validity	
Valid from	Date the certificate becomes valid (issue date)	"Tuesday, November 04 06:10:33 2014"
Valid to	Expiration date	"Thursday, November 02 05:24:21 2017"
Subject	Details of the Individual Certificate Owner	
	CN – A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	"www.test.com"
	O – Organization Name	O = Test Ltd.
	L – Locality	"Tel Aviv"
	S – State	"IL"
	C – Country	"IL"
Public Key	Public key of the certificate owner length	RSA 2048 Bits
Authority Information Access	indicates how to access information and services for the issuer: [1] OCSP Service location. [2] Certification Authority Issuer Certificate	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp1.comsign.co.il [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://fedir.comsign.co.il/cacert/ComsignOrganizationalCA.crt
Authority Key Identifier	Key Identifier of an intermediate certificate	KeyID=f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0

Certificate policies	Specifies the regulations for operations of the CA (ComSign Organizational CA): [1] ComSign CPS – OV Section [2] Organization validated with Compliance to the Baseline Requirements of the CA/Browser Forum – Subject identity validated	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.19389.3.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.comsign.co.il/CPS [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2
CRL Distribution Points	Link to the CRL	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://fedir.comsign.co.il/crl/ComsignOrganizationalCa.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.comsign.co.il/crl/ComsignOrganizationalCa.crl
Key Usage	purposes for which the certified public key may be used	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Key Identifier	Identification of the certificate according to its particular public key	“f5 bb ad ea 31 23 4b 00 5d 5b 4f 76 de 6f 8b 02 e0 fd df f0”
Subject alternative name	A DNS Name containing the Fully-Qualified Domain Name or an IP Address containing the IP address of a host to be covered by the certificate	“www.test.com” Enhanced
Key Usage	Description of the purposes for which it is permissible to use the certificate. This field is marked as CRITICAL.	Digital Signature, Key Encipherment (a0)

(xiv) השדה להלן שמור בתעודה לשימוש הגורם המאשר (CA) כדי לקיים את דרישות ה-

: CA/Browser Forum

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies
baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1).

התעודה תואמת את דרישות ה-CA/Browser Forum וכוללת Subject Identity Information כמפורט בס"ק (3).

(xv) תעודות OV-SSL כוללות גם הפניה ב-certificatePolicies extension למסמך

הנהלים של קומסיין המבהירה כי התעודה מקיימת אחר דרישת ה-CAB Forum

Policy Identifier=1.3.6.1.4.1.19389.3.1.1

[1,1]Policy Qualifier Info:

Policy Qualifier Id=CPS

Qualifier:

<http://www.comsign.co.il/CPS>

(xvi) (תעודות OV-SSL כוללות בשדה ה-Subject את : streetAddress , organizaionName , localityName state Or ProvinceName , countryName או PostalCode בהתאם למידע המאומת שנמסר לקומסין במסגרת הבקשה להנפקת תעודה אלקטרונית).

(xvii) אטריבוטים אופציונאליים אחרים שיוספו לשדה ה- subject יכילו מידע שאומת על ידי הגורם המנפיק בקומסיין. אלו לא יכללו תווים מסוג " ", "- " ו- " " (רווח) כמו גם סימון אחר לערך חסר, לא שלם או לא ישים.

7.1.6 (23) מזהה אובייקט למדיניות תעודות אלקטרוניות:
תעודות המונפקות על ידי קומסיין תואמות למדיניות קומסיין שהיא בעלת מזהה האובייקט הבאים :

(i) בתעודה לשרתי אינטרנט DV : OID 1.3.6.1.4.1.19389.3.1.1

(ii) בתעודה לשרתי אינטרנט OV : OID 1.3.6.1.4.1.19389.3.1.2

קומסיין עשויה לעשות שימוש במזהה אובייקט נוספים כגון : OID 2.23.140.1.2.1, OID 2.23.140.1.2.2 כפי שמוסדר בסעיפים 7.1.2.3 (iv) ו- 7.1.2.3 (v) (1) לנספח זה.

8.4.1 (24) נושאים הנבדקים במסגרת הביקורת על הנפקת תעודות לשרתי אינטרנט:
בכל הקשור בהנפקת תעודות אלקטרוניות לשרתי אינטרנט תורחב הביקורת לכלול לפחות את אחת מתבניות הביקורת הבאות :

(i) WebTrust for Certification Authorities v2.1 and up

(ii) WebTrust for SSL Certificates V2.3 and up

(iii) תבנית ביקורת התואמת את ETSI EN 319 411 / ETS ITS 102 042

הביקורת תיערך באמצעות מבקר מורשה כמוסדר בסעיפים 8.2 ו- 8.3 למסמך הנהלים.
קודם להנפקת תעודה אלקטרונית, קומסיין תוודא שהליך אימות שם המתחם והשליטה בו הנדרש בסעיף 3.2.2.4 לנספח זה או אימות כתובת ה-IP כנדרש בסעיף 3.2.2.53.2.2.5 לנספח זה שבוצע על ידי צד ג' המשמש כנציג או כגורם רושם של קומסיין –

(i) נעזר בלפחות אדם אחד (בן אנוש ולא מכונה) בביצוע הבדיקות, או

(ii) שחלק מהבדיקה העוסק באימות השליטה בשם המתחם בוצע ישירות על ידי קומסיין.

במידה ונציג קומסיין איננו גורם רושם שהוסמך לכך על ידי קומסיין, תכלול הביקורת בחינה של פעילות צד ג' ואישור שפעילותו מקיימת אחר דרישת נהלים אלו. בכל מקרה שבו

ממצאי הביקורת על צד ג' הם שליליים, קומסיין תפסיק לאלתר כל קשר עם צד ג' בנושא
הנפקת תעודות לשרתי אינטרנט.
תוקף הביקורת לא יעלה על 12 חודשים.