נספח 0.5.2 - קיצורים וראשי תיבות – תמ"ר

קיצור באנגלית	קיצור בעברית	משמעות באנגלית	משמעות בעברית
CA	ג"מ	Certification Authority	גורם מאשר
CARL	רתמג"מ	Certificate Authority Revocation List	רשימת תעודות מבוטלות של גורם מאשר
CP	ממ"ת	Certificate Policy	מדיניות מתן תעודות
CPS		Certification Practice Statement	הצהרה על נהלי מתן תעודות
CRL	רת"מ	Certificate Revocation List	רשימת תעודות מבוטלות
DN	ש"מ	Distinguished Name	שם מובדל
DSA	אח"ד	Digital Signature Algorithm	אלגוריתם חתימה דיגיטלית
DSS	תח"ד	Digital Signature Standard	תקן חתימה דיגיטלית
BCA	גמ"מ	Bridge Certification Authority	גורם מאשר מגשר
FIPS PUB		Federal Information Processing Standard Publication	פרסום תקן של ארגון הענ"א הפדרלי של ארה"ב
IFPKI	תמר"י	Israel Public Key Infrastructure	תשתית מפתח ציבורי – ישראל
IETF		Internet Engineering Task Force	כוח משימה הנדסי בנושא אינטרנט
ISO		International Organization for Standardization	ארגון התקינה הבינלאומי
ITU		International Telecommunications Union	איגוד התקשורת הבינלאומי
MOA		Memorandum of Agreement between an Agency and the IFPKI allowing interoperation between the BCA and Agency Principal CA)	מזכר הבנה בין סוכנות/ ארגון לסוכנות תמר"י המאפשרת פעילות בין-ארגונית בין הגמ"מ לגמ"ע
NIST		National Institute of Standards and Technology	המכון הלאומי לתקנים וטכנולוגיה, ארה"ב
OID	מ"י	Object Identifier	מזהה ישות
PCA	גמ"ע	Principal CA	גורם מאשר עיקרי
PIN	מז"א	Personal Identification Number	מספר זיהוי אישי
PKCS	תתמ"צ	Public Key Certificate Standard	תקן תעודת מפתח ציבורי
PKI	תמ"ר	Public Key Infrastructure	תשתית מפתח ציבורי
PKIX		Public Key Infrastructure X.509	תשתית מפתח ציבורי ע"פ תקן X.509
RA	ר"ר	Registration Authority	רשות רישום
RSA		Rivest-Shamir-Adleman (encryption algorithm)	אלגוריתם הצפנה על שם ריבסט, שמיר, אדלמן
SHA-1		Secure Hash Algorithm, Version 1	אלגוריתם Hash בטוח, גירסא 1.
S/MIME		Secure Multipurpose Internet Mail Extension	
SST		Secure Sockets Layer	
URL		Uniform Resource Locator	

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

טבלה מס' 2 – מילון מונחים ומושגים (Glossary)

עברית	אנגלית	תיאור המונח
גישה	Access	היכולת להשתמש במשאב כלשהו של מערכת מידע
בקרת גישה	Access Control	תהליך של הענקת גישה למשאבי מערכת מידע רק למשתמשים מורשים, תוכניות, תהליכים או מערכות אחרות.
הסמכה	Accreditation	הצהרה רשמית של רשות מאשרת מוסמכת, שמערכת מידע מאושרת לתפעול במצב אבטחת מידע מסויים תוך שימוש בקבוצת אמצעי הגנה מוגדרים מראש, ברמת סיכון סבירה.
סוכנות	Agency	כל מחלקה, יחידה ארגונית כפופה למחלקה, או כל ישות ארגונית עצמאית שהינה סטטוטורית ומזוהה כזרוע של ה"רשות המבצעת" בישראל.
ג"מ של סוכנות	Agency CA	ג"מ שפועל בשם סוכנות מסויימת, תחת הבקרה התפעולית של אותה הסוכנות.
מבקש	Applicant	גורם שהגיש בקשה לג"מ עבור תעודה, בסטטוס שלפני השלמת תהליך הנפקת התעודה.
ארכיון	Archive	איחסון פיזי נפרד, לטווח ארוך.
רשות אימות אפיונים	Attribute Authority	ישות רשמית מוכרת, בעלת סמכות לאמת את הקישור שבין מאפיינים לבין לישות מסויימת.
ביקורת	Audit	בדיקה עצמאית ובחינה של רשומות ופעילויות, לצורך הערכת התאמת הבקרות במערכת, על מנת להבטיח תאימות עם מדיניות מוגדרת ופרוצדורות תפעוליות, ועל מנת להמליץ על שינויים נדרשים בבקרות, במדיניות או בתהליכים.
מידע לביקורת	Audit Data	רישום כרונולוגי של פעילויות מערכת על מנת לאפשר שיחזור ובחינה של רצף אירועים ושינויים באירוע.
לוודא/ לאמת	Authenticate	לאשר ולוודא זהות של ישות, כאשר זהות זו מוצגת לבדיקה.
וידוא/ אימות	Authentication	אמצעי בטחון המתוכנן לבסס את התקפות של שידור, מסר, או מקור מידע, או אמצעים לאמת את ההרשאה והסמכות של אדם לקבל קטגוריות ספציפיות של מידע.
קשירה	Binding	תהליך של קשירת שני רכיבי מידע המתייחסים זה לזה.
ביומטרי	Biometric	מאפיין פיזיקלי או התנהגותי של בן-אנוש.

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

עברית	אנגלית	תיאור המונח
תעודה	Certificate	ייצוג דיגיטלי של מידע שהינו לפחות: (1) מזהה את הגורם שהנפיק אותו; (2) קורא בשם או מזהה את המנוי; (3) כולל את המפתח הפומבי של המנוי; (4) מזהה את תקופת התפעול התקיפה; (5) נחתם אלקטרונית על ידי הג"מ שהנפיק אותו. הגדרה טכנית וספציפית יותר, מייחסת מונח זה לתעודות שבהן נרשם בצורה מפורשת התייחסות למזהה האובייקט של "מדיניות הרישוי" (CP) בשדה "Certificate Policies" בתעודה ע"פ תקן X.509 מהדורה 3.
גורם מאשר	Certification Authority (CA)	רשות אשר משתמש אחד או יותר בוטחים בה, לצורך הנפקה וניהול של תעודות מפתח פומבי לפי X.509, ורשימת תעודות מבוטלות.
רשימת תעודות מבוטלות של ג"מ	Certification Authority Revocation List (CARL)	רשימה חתומה, כולל חתימת זמן, של מספרים סדרתיים של מפתחות ציבוריים של תעודות, כולל תעודות-צולבות, אשר בוטלו.
מתקן ג"מ	CA Facility	אוסף של ציוד, כוח אדם, תהליכים ומבנים, בהם עושה ג"מ שימוש, על מנת לבצע הנפקה של תעודות וביטולן בעת הצורך.
רשות ניהול תעודות	Certificate Management Authority (CMA)	גורם מאשר או רשות רישום.
תוכנת גורם מאשר	Certification Authority Software	תוכנות לניהול מפתחות וקריפטוגרפיה, שבהן נעשה שימוש להנפקת תעודות למנויים.
מדיניות הנפקת תעודות	Certificate Policy (CP)	סוג מיוחד של מדיניות מינהלית, המכוונת לטרנזקציות אלקטרוניות ומבוצעת במהלך ניהול תעודות. המדיניות מתייחסת לכל ההיבטים הקשורים בחילול, ייצור, הפצה, תימחור, התאוששות מפגיעה ומינהל של תעודות דיגיטליות.
הצהרת נוהל הנפקת תעודות	Certification Practice Statement (CPS)	הצהרה על הנהלים והנוהגים אשר גורם מאשר מיישם בהנפקה, השעיה, ביטול וחידוש של תעודות ומתן הגישה אליהן, בהתאמה לדרישות מסוימות.
מידע קשור לתעודה	Certificate - Related Information	מידע, כגון כתובת הדואר של המנוי, שאינה כלולה בתעודה עצמה. עשוי לשמש לצורכי ניהול על ידי הגורם המאשר.
רשימת תעודות מבוטלות	Certificate Revocation List (CRL)	רשימה המנוהלת על ידי גורם מאשר, של כל התעודות שהוא הנפיק ואשר בוטלו לפני מועד פג התוקף המקורי שהוגדר עבורן.
רשות לסטטוס תעודות	Certificate Status Authority	ישות נאמנה, אשר מספקת מידע מקוון לאימות, לגורם המסתמך על אמינות תעודה של אדם מסוים, ואשר יכולה לספק גם מידע נוסף על מאפייני המידע עבור אותו אדם מסוים.

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

עברית	אנגלית	תיאור המונח
לקוח (יישום)	Client (application)	ישות מערכתית, בדר"כ תהליך ממוחשב הפועל מטעם משתמש אנושי, שעושה שימוש בשירות המסופק על ידי השרת.
סיכון ופגיעה	Compromise	גילוי של מידע לאנשים בלתי מוסמכים, או פגיעה במדיניות אבטחת המידע של מערכת, שכתוצאה מכך נגרמה פגיעה מכוונת או בלתי מכוונת, שינוי, מחיקה או אובדן במידע.
סודיות	Confidentiality	בטחון שמידע לא נמסר לישויות או לתהליכים בלתי מאושרים.
תעודה צולבת	Cross-Certificate	תעודה שנעשה בה שימוש ליצירת קשרי אימון בין שני גורמים מאשרים.
שלמות מידע	Data Integrity	בטחון שמידע לא השתנה מאז יצירתו ועד לקבלתו.
חתימה דיגיטלית	Digital Signature	התוצאה של טרנספורמציה של מסר על ידי שימוש במערכת קריפטוגרפית המשתמשת במפתחות כך שגורם המסתמך על החתימה יכול לקבוע: (1) האם הטרנספורמציה נוצרה תוך שימוש במפתח הפרטי שמתאים למפתח הפומבי שנמצא בתעודה הדיגיטלית של החותם; ו- (2) האם המסר שונה על ידי מישהו, מאז שבוצעה הטרנספורמציה.
משך	Duration	שדה בתוך תעודה שמורכב משני שדות משנה: "תאריך הנפקה" ו"תאריך פג תוקף".
מסחר אלקטרוני	E-commerce	שימוש בטכנולוגיית תקשורת (בעיקר אינטרנט) לקנות או למכור סחורות ושירותים.
עובד/ מועסק	Employee	כל אדם שמועסק על ידי סוכנות כמוגדר לעיל.
שלמות	Integrity	הגנה כנגד שינוי או השמדה לא מורשית של מידע. מצב שבו מידע נשאר ללא שינוי מהנקודה שבה נוצר על ידי המקור, במשך השידור, האיחסון והקבלה על ידי היעד.
גורם מאשר ביניים	Intermediate CA	גורם מאשר שהינו כפוף לג"מ אחר, ושיש לו ג"מ שכפוף אליו.
הפקדת מפתחות	Key Escrow	הפקדה של מפתח פרטי של מנוי ומידע רלבנטי אחר, בהתבסס על הסכם הפקדה או חוזה אחר, הקובע עבור המנוי, את התנאים שבהם נדרש סוכן אחד או יותר, להחזיק את המפתח הפרטי של המנוי לתועלת המנוי, עובד/ מועסק או צד אחר, בהתאם לתנאים המוגדרים בהסכם.
החלפת מפתחות	Key Exchange	תהליך של החלפת מפתחות ציבוריים במטרה לבסס תקשורת בטוחה.
חומרי יצירת מפתחות	Key Generation Material	מספרים אקראיים, כעין-מספרים אקראיים ופרמטרים קריפטוגרפיים שבשימוש בתהליך יצירת מפתחות קריפטוגרפיים.

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

עברית	אנגלית	תיאור המונח
צמד מפתחות	Key Pair	שני מפתחות מתמטיים הקשורים זה לזה, בעלי התכונות (1) ניתן להשתמש במפתח אחד להצפין מסר כך שניתן לפענחו רק באמצעות המפתח השני, ו- (2) אפילו שמפתח אחד ידוע, לא ניתן ואין זה מעשי לגלות בצורה חישובית את המפתח השני.
רשות רישום מקומית	Local Registration Authority (LRA)	רשות רישום שאחראית על קהילה מקומית.
אימות הדדי	Mutual Authentication	תהליך המתרחש כאשר שני הצדדים בשני קצות התקשורת, מבצעים וידוא פעיל האחד לשני.
רשות שמות	Naming Authority	ישות ארגונית האחראית על הקצאת שם מובדל (DN) ולהבטיח שכל DN הינו משמעותי וחד-ערכי בתוך התחום (DOMAIN).
אי-הכחשה	Non-Repudiation	בטחון שלשולח מספקים הוכחה לאישור המשלוח ולמקבל מסופקת הוכחה על זהות השולח כך שאף אחד מהם לא יכול להכחיש שהוא עיבד את המידע.
רשות לניהול מדיניות	Policy Management Authority (PMA)	גוף שמיוסד לראיה כוללת של יצירה ועדכון של מדיניות הנפקת תעודות, לבחינה של הצהרות נהלי הנפקת תעודות, לבחון תוצאות ביקורת על עמידה בהצהרת מדיניות, ופיקוח וניהול מדיניות תעודות PKI. עבור התמ"ר הממשלתי בישראל, נכון לעכשיו, זהו צוות תמ"ר.
גורם מאשר עיקרי	Principal CA	גורם מאשר שממונה על ידי סוכנות להיות בקשר עם גורם מאשר מגשר.
מפתח פרטי	Private Key	(1) המפתח בצמד המפתחות שבו משתמשים ליצירת החתימה הדיגיטלית. (2) המפתח של צמד מפתחות הצפנה שבו נעשה שימוש לפענח מידע סודי. בשני המקרים, מפתח זה חייב להישמר סודי.
מפתח ציבורי	Public Key	(1) המפתח מתוך צמד מפתחות לחתימה דיגיטלית, שנועד לאמת חתימה דיגיטלית. (2) המפתח של צמד מפתחות הצפנה שנועד להצפנת מידע סודי. בשני המקרים, המפתח בדרך כלל זמין לציבור בצורה של תעודה דיגיטלית.
תשתית מפתח ציבורי	Public Key Infrastructure (PKI)	אוסף של מדיניות, תהליכים, פלטפורמות שרתים, תוכנה ועמדות עבודה, שבהם נעשה שימוש לניהול תעודות וצמדי מפתחות פרטי-ציבורי, כולל היכולת להנפיק, לתחזק, לנהל ולבטל תעודות מפתח ציבורי.
רשות רישום	Registration Authority (RA)	גורם שאחראי על זיהוי ווידוא של נושאי תעודות, אולם אינו חותם ומנפיק תעודות בעצמו.

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

עברית	אנגלית	תיאור המונח
מיפתוח מחדש של תעודה דיגיטלית	Re-Key (a certificate)	שינוי של ערך מפתח קריפטוגרפי שנעשה בו שימוש במערכת קריפטוגרפית. בדרך כלל, משמעות הדבר היא הנפקת תעודה חדשה על המפתח הציבורי החדש.
גורם מסתמך	Relying Party	אדם או סוכנות שמקבלים מידע שכולל תעודה וחתימה דיגיטלית שניתנת לאימות בהתייחס למפתח פומבי המפורט בתעודה, ונמצא במצב שהוא מסתמך עליהם.
חידוש תעודה	Renew (a certificate)	הפעולה או התהליך של הארכת תוקף המידע הקשור לתעודת מפתח ציבורי, על ידי הנפקת תעודה חדשה.
מאגר	Repository	בסיס נתונים הכולל מידע המתייחס לתעודות. ניתן להגדרה גם כ"ספריה" (directory).
ביטול תעודה	Revoke a Certificate	לסיים באופן קבוע את תקופת ההפעלה של תעודה, בזמן ספציפי.
גורם מאשר "שורש"	Root CA	בארכיטקטורה היררכית של PKI, זהו הגורם המאשר שהמפתח הפומבי שלו משמש כמידע הנאמן ביותר שניתן לסמוך עליו (כלומר – תחילת מסלול האמון), עבור תחום אבטחת מידע.
תעודת חתימה	Signature Certificate	תעודת מפתח ציבורי שכוללת מפתח ציבורי שמיועד לאימות חתימות דיגיטליות, ולא להצפנת מידע או לביצוע פונקציות קריפטוגרפיות אחרות.
גורם מאשר כפוף	Subordinate CA	במסגרת PKI היררכי, זהו גורם מאשר אשר מפתח החתימה של תעודותיו, מאושר על ידי גורם מאשר אחר, ואשר פעולותיו מוגבלות על ידי גורם מאשר אחר זה.
מנוי	Subscriber	ישות אשר (1) היא שם נושא התעודה או שמזוהה בתעודה המונפקת לאותה ישות, (2) מחזיק במפתח פרטי שמקביל למפתח הציבורי הרשום בתעודה, ו- (3) לא מנפיק בעצמו תעודות לכל גורם אחר.
גורם מאשר בכיר	Superior CA	ב- PKI היררכי, זהו גורם מאשר שאישר את תעודת החתימה של גורם מאשר אחר, ואשר מגביל את פעילות הגורם המאשר האחר.
עדכון תעודה	Update (a certificate)	פעולה או תהליך לפיהם פריטי מידע הקשורים לתעודת מפתח פומבי קיימת, ובפרט הרשאות הניתנות לנושא התעודה, משתנים על ידי הנפקת תעודה חדשה.

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