מדינת ישראל
ממשלת ישראל - משרד ראש הממשלה
רשות התקשוב הממשלתי – יחידת ממשל זמין

RFI פומבי מספר 001/2015 –
בקשה לקבלת מידע –
יישומי ניהול זהויות והזדהות אחודה
(IdM ,SSO)

המידע הכלול במסמך לא יפורסם, לא ישוכפל ולא יעשה בו שימוש מלא או חלקי, לכל מטרה שהיא מלבד מענה על בקשת מידע זו

בקשה לקבלת מידע (RFI) מספר 001/2015 – יישומי ניהול זהויות והזדהות אחודה (IdM, SSO)

חלק 1 – כללי/ מנהלה

1. **כללי:** יחידת ממשל זמין ברשות התקשוב הממשלתי במשרד ראש הממשלה (להלן: "**הפונה**"), מבקשת, בהתאם להוראות תקנה 14א לתקנות חובת המכרזים, התשנ"ג - 1993, לקבל מידע מספקים ישראליים או זרים, בעלי ידע וניסיון מקומי ובינלאומי (להלן - "מוסרי המידע"), אודות מוצרים ליישומי ניהול זהויות והזדהות אחודה (IdM, SSO) (להלן: "המוצרים/ המוצר"), במסגרת בחינה להקמה ופיתוח של תשתית טכנולוגית לשימוש על ידי אזרחים, תושבים ועסקים הנמצאים בקשר מול הממשלה, מקבלים שירותים ופועלים מולה, וכן עבור עובדי הממשלה (להלן - "**הבקשה**").

2. **מהות הבקשה:**

הפונה מבקש ממוסרי המידע להגיש מענה לבקשה לקבלת מידע (RFI). המענה יכלול את הפרטים הבאים:

2.1. מידע לגבי המוצרים, כולל רכיבי חומרה, תוכנה, יישומים (אפליקציות), תקשורת ואבטחת מידע, ליישומי ניהול זהויות והזדהות אחודה והשימוש בהם (להלן: "**הפתרון**").

2.2. תיאור יכולתם וניסיונם של מוסרי המידע ליתן את הפתרון.

2.3. פרטים בדבר אופן מתן הפתרון.

2.4. **אפשרות** להדגמה - RFD (Request for Demonstration).

3. **הבהרות:**

3.1. בקשה זו הינה בקשה מוקדמת לקבלת מידע בלבד, ואין בה כדי להוות שלב בהתקשרות כזו או אחרת עם מי ממוסרי המידע המשיבים לבקשה. יודגש כי, אין בבקשה משום התחייבות של הפונה להמשיך בתהליך זה, בכל דרך שהיא, והיא איננה מהווה מכרז ו/או הזמנה להציע הצעות ו/או הקמת מאגר ספקים. כל ההוצאות הכרוכות בהגשת המידע יחולו על מוסר המידע בלבד ומוסר המידע לא יהא זכאי לכל פיצוי או שיפוי בגין הגשת המענה לבקשה.

3.2. הפונה אינו מתחייב להשתמש במידע, כולו או מקצתו, למטרת הכנת מכרז, או לכל מטרה אחרת.

3.3. העברת המידע איננה מעניקה למוסר המידע כל זכות כלפי הפונה ואינה מטילה על הפונה חובה כלשהי.

3.4. אין באמור במסמך זה משום התחייבות לפרסם מכרז בנושא כאמור, או התחייבות לגבי פרטי המכרז ככל שיפורסם כזה.

3.5. הפונה לא יישא בכל תשלום או הוצאה, שייגרמו למוסר המידע בגין בקשה זו ועקב המגעים עמו, אם יקוימו, בהקשר לבדיקת המידע, ההדגמה או בכל הקשר אחר בעניין זה.

3.6. הפונה יהיה רשאי להעביר כל מידע או נתון הקשור במידע שנמסר לכל אדם הקשור בפונה וכן לפרסם בדרך של מכרז או בדרך אחרת, מפרטים או אפיונים אשר יתבססו על המידע אשר יצטבר כתוצאה מהליך זה.

3.7. היה ויפורסם מכרז בקשר עם בקשה זו, ומבלי להתחייב לפרסום כאמור, מענה לבקשה לא יהווה תנאי להשתתפות במכרז, לא יקנה יתרון למי שנענה לבקשה רק בשל כך שנענה לבקשה, ולא יחייב שיתופו במכרז או התקשרות עמו בכל דרך אחרת.

4. **<u>הדגמות:</u>**

4.1. הפונה רשאי, אולם אינו חייב, לבקש ממוסר המידע, להציג את המוצרים במסגרת הדגמה (demonstration) בפני צוות מקצועי מטעמו.

4.2. הדגמת הפתרון, אם תתקיים, תהווה חלק מהבקשה ותהיה כפופה לאמור בה.

4.3. ר׳ פירוט בחלק 2 להלן.

5. **<u>פרסום מסמכי הבקשה לקבלת מידע:</u>**

5.1. המסמכים יפורסמו באתר האינטרנט של מינהל הרכש הממשלתי באגף החשב הכללי (להלן – ״אתר האינטרנט״) בכתובת www.mr.gov.il תחת הכותרת: מכרזים / בקשה לקבלת מידע (RFI) מספר 001/2015 – יישומי ניהול זהויות והזדהות אחודה (IdM ,SSO).

5.2. המסמכים יהיו זמינים באתר החל **מיום ב׳, ה- 11/1/2016**.

6. **<u>איש קשר</u>:** איש הקשר מטעם ממשל זמין לבקשה לקבלת מידע, אליו יש להפנות את כל הבירורים והשאלות, הוא: מר דב הורוביץ, טל׳: 02-6664842, פקס׳: 02-6664650, דוא״ל: dov@gov.il.

7. **<u>נוהל העברת שאלות הבהרה לגבי הבקשה:</u>**

7.1. מוסרי מידע מעוניינים רשאים לפנות בשאלות ובקשות להבהרה לכתובת הדוא״ל של איש הקשר, כאמור בסעיף 6 לעיל.

7.2. שאלות שיגיעו עד **ליום ה׳, ה- 21.1.16, בשעה 14:00**, יענו.

7.3. מוסר המידע מתבקש להתייחס בשאלות למספר הסעיף בחלק 2.

7.4. על מוסר המידע לוודא ששאלותיו הגיעו בשלמותן לאיש הקשר.

7.5. מענה לשאלות ההבהרה יימסר עד **ליום ה׳, ה- 28.1.16**.

8. **<u>אופן מסירת המענה</u>:**

8.1. יש להעביר את המענה לבקשה לקבלת מידע בדואר אלקטרוני, לכתובת הדוא"ל של איש הקשר, עד **ליום ב', ה- 8/2/16, בשעה 15:00**.

8.2. המענה יכלול מסמכים בפורמט PDF **ובנוסף** ב- MS-WORD או ב- RTF.

8.3. מוסר המידע מתבקש לוודא קבלת המענה אצל איש הקשר.

9. **<u>תכולת המענה</u>:**

9.1. יש למסור את הפרטים המפורטים בחלק 2 של הבקשה.

9.2. יש להתייחס לשאלות הטכניות המופיעות בחלק 2 של הבקשה, על כל תת-סעיפיו, ולענות על כל תת-סעיף בהתאם לפתרון המוצע על ידי מוסר המידע, בין אם מדובר בשאלות מפורשות או בתיאור פונקציונלי.

9.3. ניתן להגיש כל חומר, מסמכים ומענה נוסף, על פי שיקול דעת מוסר המידע.

10. **<u>בעלות על המסמכים ועל המענה והשימוש בהם</u>:**

10.1. מסמך הבקשה הינו קניינו הרוחני של הפונה אשר מועבר לצורך מענה על הבקשה לקבלת מידע.

10.2. מסמך המענה הוא קניינו הרוחני של מוסר המידע. יחד עם זאת, לפונה תהא האפשרות להשתמש במידע שיינתן במסגרת המענה לכל צורך הקשור בפעילותו ולמוסר המידע לא יהיו טענות בקשר לזכויות יוצרים במידע.

בקשה לקבלת מידע (RFI) מספר 001/2015 – יישומי ניהול זהויות

והזדהות אחודה (IdM, SSO)

חלק 2 – פירוט המידע המבוקש

1. רקע:

1.1 יחידת ממשל זמין ברשות התקשוב הממשלתי במשרד ראש הממשלה (להלן – "הפונה"), מעוניינת לבחון אפשרות לרכוש ולהטמיע במסגרת תשתית התקשוב של ממשל זמין, מוצרים ליישומי ניהול זהויות והזדהות אחודה (IdM, SSO), העונים על הדרישות המקצועיות – פונקציונליות שיפורטו בחלק זה (להלן - "הפתרון"), ומזמינה בזאת ספקים של מוצרים בתחום זה להגיש מענה לבקשה לקבלת מידע זו.

1.2 הפונה מבקשת לקבל מידע ממוסרי המידע, שהינם בעלי ידע ומומחיות מתאימים, בדבר ניסיונם בפיתוח, שיווק והטמעת מוצרים ליישומי ניהול זהויות והזדהות אחודה (IdM, SSO).

2. פרטי מוסר המידע:

2.1 שם מוסר המידע: _____

2.2 מספר רישום התאגיד: _____

2.3 מקום רישום התאגיד: בישראל/ בחו"ל (יש לציין את שם המדינה): _____

2.4 כתובת משרדי התאגיד: _____

2.5 טלפון משרדי התאגיד: _____

2.6 פקס' משרדי התאגיד: _____

2.7 כתובת דואר אלקטרוני: _____

2.8 כתובת אתר אינטרנט (אם קיים): _____

2.9 שנת הקמה: _____

2.10 פרטי נציג/איש קשר למענה לבקשה לקבלת מידע:

2.10.1 שם: _____

2.10.2 תפקיד: _____

2.10.3 טלפון נייד: _____

2.10.4 טלפון במשרד: _____

2.10.5 דוא"ל: _____

3. פרטי המוצר המוצע:

3.1. על מוסר המידע לפרט את עיסוקיו, התמחותו וניסיונו בפיתוח, שיווק והטמעת מוצרים בתחום ניהול זהויות והזדהות אחודה (IdM, SSO) (להלן – המוצר, המוצרים).

3.2. ככל שמדובר במוצרים קיימים, על מוסר המידע להציג אישור בעלות מוכחת על זכויות היוצרים או רישיון לשיווק המוצרים.

3.3. על מוסר המידע לצרף תיאור מקיף של המוצרים.

3.4. יובהר כי ניתן להציג יותר ממוצר אחד הרלבנטי לתחום זה.

3.5. יש לפרט **לגבי כל מוצר בנפרד** את הפרטים הבאים, תוך התייחסות לדרישות ולצרכים של הפונה מהמוצר כמפורט בסעיף 4 להלן:

3.5.1. שם המוצר:_____

3.5.2. שם היצרן:_____

3.5.3. מהדורה נוכחית של המוצר:_____

3.5.4. שנת תחילת הפצה:_____

3.5.5. תיאור אופן השימוש במוצר (מומלץ להרחיב בנספח נפרד): _____

3.5.6. רשימת מדינות ופרויקטים בהם מיושם המוצר (מומלץ להרחיב בנספח נפרד):

_____

3.6. <u>תיאור טכני של המוצר</u>: יש לצרף תיאור טכני של המוצר.

3.7. <u>תיאור הפתרון המוצע</u>: יש לצרף הסבר לגבי הארכיטקטורה המוצעת וכיצד ניתן לשלבה בתשתיות קיימות על בסיס ממשקים ותקנים.

3.8. <u>תמיכה בתקנים</u>: יש לציין מהם התקנים הישראליים, התקנים הבינלאומיים, הפרוטוקולים המקובלים והתקנים של ארגונים וולונטאריים בהם המוצר תומך.

3.9. <u>בדיקות לגבי עמידה בתקנים</u>: ככל שנערכו בדיקות עמידה בתקנים (על פי הפירוט בסעיף 3.8 דלעיל), יש לצרף פירוט של בדיקות אלו, לצורך הוכחת עמידה בתקנים.

3.10. <u>בדיקות אבטחת מידע</u>: בהמשך לסעיף הקודם, יש לציין בפרט עמידה בתקני אבטחת מידע ובבדיקות חדירות (PT).

3.11. <u>ביצועים</u>: יש לציין את עמידת המוצר בביצועים על פי פרמטרים רלבנטיים והפניה לבדיקות עומסים שנערכו על ידי גורמים מוסמכים.

3.12. <u>יישומים קודמים וקיימים במוצר</u>: יש לפרט דוגמאות למדינות ולפרויקטים בהם נעשה שימוש במוצר, בהמשך לאמור בסעיף 3.5.6 לעיל, תוך פירוט **היקף הזהויות שהמערכת מנהלת**, מספר טרנזקציות ליחידת זמן ואנשי קשר לצורך פניה בפרויקטים אלו, ובפרט תוך התייחסות לשימוש בתקנים שצוינו בסעיף 3.8 לעיל.

3.13. פרטים נוספים:

3.13.1. ניתן למסור פרטים נוספים כלשהם, על פי שיקול דעת מוסר המידע.

3.13.2. בפרט, ניתן למסור פרטים, על פי שיקול דעת מוסר המידע, לגבי מחירי רישיונות לשימוש במוצר ושיטת התמחור, גם ברמת סדרי גודל (לדוגמה - לפי משתמש, לפי שימוש, לפי התקנה ארגונית חד פעמית, הנחת כמויות, שיטה אחרת).

3.14. הדגמה:

3.14.1. ככל שתידרש הדגמה, יימסרו הנחיות ספציפיות לגבי מיקום ההדגמה, משך ההדגמה ואופן ביצועה.

3.14.2. מקום ההדגמה יכול להיות במשרדי הפונה, במשרדי מוסר המידע או בטכניקה של הדגמה מרחוק באמצעות שיחת וידאו, בהתאם לשיקול הפונה ובתיאום עם מוסר המידע.

3.14.3. ההדגמה תכלול לפחות שלושה תסריטים:

3.14.3.1. תסריט של חווית המשתמש בשלב ההרשמה (enrolment), בשלב הנפקת אמצעי הזדהות (credentials) ובשלב האימות המקוון עצמו.

3.14.3.2. תסריט של תפעול המוצר על ידי מנהל המערכת (administrator) והאפשרויות שהמוצר מעמיד לרשותו.

3.14.3.3. תסריט של ממשקים חיצוניים עם מערכות אחרות.

3.14.3.4. תסריטים נוספים כפי שיוצגו על ידי מוסר המידע לפי שיקול דעתו.

4. דרישות הפונה מהמוצר:

4.1. מטרות ויעדים - כללי:

4.1.1. מטרת הפונה היא לגבש דרך פעולה לגבי אופן מימוש מערך ניהול זהויות והדהות אחודה (SSO, IdM), בממשל זמין, בפרט עבור אזרחים, תושבים ועסקים הפונים לקבלת שירותי ממשלה, אך גם עובדי הממשלה, מערוצי גישה ומתן שירות שונים, כולל גלישה לאתרי אינטרנט, גישה ממכשירים ניידים בכלל ומאמצעים "לבישים" בפרט.

4.1.2. כוונת הפונה הינה לפתח תשתית של הזדהות אחודה עבור אזרחים, תושבים ועסקים, וכן גם עבור עובדי הממשלה, לצורך קבלת שירותים. הכוונה לאפשר לנותן השירות (service provider) להגדיר רמות הבטחת אימות[1] (Levels of assurance) שדרושות לשירות זה או אחר בתהליך האימות (Authentication), ובהמשך להגדיר הרשאות למשתמשים ככל שהדבר יידרש (Authorization).

4.1.3. דוגמה למערך הרשאות היא לאפשר כניסה לבלוג פנימי מסוים, ל- X אנשים מסוימים בלבד, או לאפשר דיווח בשירות מסוים רק למי שנרשם בצורה ספציפית קודם לכן לשירות זה.

4.1.4. יש להציג כיצד מוגדרת רמת הבטחת האימות עבור כל שירות וכן כיצד מופעל מערך ההרשאות.

4.1.5. אחד מרכיבי המערכת יאפשר לחולל ו/או לנפק אמצעי הזדהות (credentials) על בסיס פרמטרים מוגדרים מראש לכניסה למערכת, שהם נגזרת של רמת הבטחת האימות. כדוגמה – סיסמה אחת שתשמש לכל שירותי הממשלה.

4.2. **<u>חווית המשתמש הצפויה (User Experience)</u>:**

4.2.1. המשתמש ייכנס לאתר ממשלתי כלשהו, לצורך ביצוע / קבלת שירות כלשהו, על ידי לחיצה על הקישור המתאים.

4.2.2. השירות יבדוק את רמת הבטחת האימות של המשתמש. אם אינו רשום עדיין במערכת, הוא יופנה לתהליך ההרשמה. לאחר מכן תיבדק זהות המשתמש מול ספק ההזדהות (Identity Provider). כמו כן תיבדק התרמת רמת הבטחת האימות של המשתמש מול השירות.

4.2.3. אם קיימת התאמה והזהות אומתה, ניתן יהיה להתקדם לשירות עצמו.

4.2.4. הכוונה היא שאפשר יהיה לנתב כל משתמש, בהתאם לתהליכים שיאופיינו (Work Flow ו"חוקה לוגית"), בהתאם לנתונים שייקלטו.

4.2.5. בתהליך ההרשמה, יש להציג את המענה הניתן לאופן ניהול הרשומות לכל תושב להזדהות מול הממשלה, כולל מענה לאפשרות ניהול שמות משתמש וסיסמאות באופן מרכזי בממשלה.

4.2.6. המערכת תאפשר התחברות למערכות חיצוניות לצורך וידוא פרטי המשתמש (כגון מול מאגרים ממשלתיים אחרים, בכפוף להרשאה חוקית מתאימה כמובן).

4.2.7. המערכת תאפשר מחיקת פרטי משתמש מסוים, כפעולה יזומה של המשתמש ו/או של מנהל המערכת.

[1] ר' גם סעיף 4.3 להלן

4.2.8. המערכת תתמוך בכל רמות הבטחת האימות, ושימוש באמצעי הזדהות מתאימים, כולל שם משתמש וסיסמה, OTP, כרטיס חכם או token אחר מותנה בתהליך ההרשמה, ובהתאם להנחיות ונהלים שייקבעו.

4.2.9. יש לציין מהי התמיכה במערכת לגבי קביעת חוזק סיסמה או בדיקתה במקרה של בחירה על ידי המשתמש.

4.3. **<u>רמות הבטחת אימות</u>:**

4.3.1. הכוונה שתהיה הגדרה גנרית במסגרת מדיניות לאומית להזדהות בטוחה, של "רמות הבטחת אימות" (Level of assurance).

4.3.2. כל גוף/ משרד, יהיה אחראי להגדרת רמת הבטחת האימות של השירותים שהוא מספק.

4.3.3. במקביל, תהיה הגדרה מהם הפתרונות הטכנולוגיים שעונים על כל רמת הבטחת אימות, בהקשר לתהליכי ההרשמה (enrolment), ניהול אמצעי ההזדהות (credentials) וטרנזקציות האימות עצמן.

4.4. **<u>אמצעי הזדהות</u>:**

4.4.1. יידרש מענה לסוגים שונים של כרטיסים חכמים, tokens, וכן לגישה מאמצעים ניידים/ לבישים (כגון - "שעון חכם").

4.4.2. יש להתייחס בפרט לתמיכה בתעודת זהות אלקטרונית (eID) ובמערך תשתית מפתח פומבי (PKI).

4.4.3. יובהר שלא מדובר רק על שירותים ואתרים שיתארחו בחוות השרתים בממשל זמין, אלא גם בשירותים שיתארחו בתשתית חיצונית, ובמקרה כזה יש להציג כיצד יווצר האמון ביניהם.

4.5. **<u>דרישות מיוחדות - כללי</u>:**

4.5.1. <u>"אימות מתמשך"</u>: יתאפשר "אימות מתמשך" במהלך טרנזקציה, כלומר – מעבר לאימות בתחילת הטרנזקציה, גם אימות בנקודות זמן מסוימות במהלך הטרנזקציה, כגון – במעבר לטרנזקציה מקוננת (nested), או לפי פרופיל אחר.

4.5.2. <u>Work flow</u> : יתאפשר להגדיר work flow של תהליך ההרשמה, הנפקת אמצעי ההזדהות והאימות המקוון עצמו.

4.6. **<u>SSO - דרישות מיוחדות</u>:**

4.6.1. נדרשת תמיכה מלאה ב- SAML 2.0. ניתן להתייחס גם לתמיכה בפרוטוקולים נוספים כמו OAuth ו- OpenID Connect.

4.6.2. נדרשת אפשרות ל- federation של credentials, כלומר – אפשרות מעבר בין-גופים תוך כדי תהליך ה- SSO הגם שלא יהיו מותקנים פיזית בחוות השרתים של ממשל זמין.

4.6.3. הנפקת ה- token עם ה- credentials למשתמש באופן שניתן יהיה להעבירו בין סביבות שונות.

4.6.4. תמיכה בפלטפורמות שונות (multi-platform) בצד נותני השירות (Service Providers) לצורך העברת tokens/ credentials.

4.6.5. <u>הפקת דוחות ובקרה</u>: אפשרות לקבלת דוחות מפורטים לגבי ביצועי המערכת ותפעולה, כגון – איזה שירות נצרך, מי ניגש לשירות, שעות זמינות לשרות, עומסים, ניסיונות כושלים (היבטי אבטחת מידע).

4.6.6. <u>אבטחת מידע</u>: דיווח אירועי אבטחת מידע לרבות העברת נתונים ולוגים למערכת SIEM חיצונית.

4.6.7. <u>זמינות ושרידות</u>:

4.6.7.1. תמיכה בזמינות גבוהה (High Availability) וביתירות (redundancy).

4.6.7.2. אפשרות לאתר גיבוי והתאוששות בחירום (DR), כולל ביזור במספר אתרים פיזיים, במתכונת של ACTIVE-ACTIVE.