

הנחיות ודרישות לחיבור ספק חיצוני למערכת ההזדהות המרכזית של משרד החינוך

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

תוכן עניינים

3	מבוא	1
4	מונחים והגדרות	2
5	דרישות סף לחיבור מערכת ספק חיצוני לשירותי הזדהות מרכזיים של משרד החינוך	3
5	הנחיות כלליות להתחברות מערכת ספק לשירותי ההזדהות של משרד החינוך	4
7	שלבים בחיבור מערכת ספק חיצוני למערכת ההזדהות של משרד החינוך	5
8	תמיכה ושירות	6
9	חוסן ואמינות	7
9	הגבלת אחריות	8
9	תפעול	9
10	גורמים מעורבים	10
10	נספחים	11

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

1. מבוא

משרד החינוך (שייקרא להלן "המשרד"), באמצעות מינהל תקשוב, טכנולוגיה ומערכת מידע, מפעיל מערכת לניהול זהויות IDM, המאפשרת למשרד לבצע ניהול מרכזי של חשבונות המשתמשים והרשאותיהם במערכות המחשוב השונות, בסביבת האינטרנט, תוך כדי שמירה על אחידות ואכיפת נוהלי אבטחת המידע הנהוגים במשרד.

המערכת מאפשרת למשרד לשפר ולהרחיב את שירותי המחשוב הניתנים לאוכלוסיות השונות, ובה בעת להגביר את רמת אבטחת המידע והשמירה על צנעת הפרט, בהתאם לחוק הגנת הפרטיות.

המערכת מבוססת על מוצר Identity Management של חברת NETIQ.

במצב הקיים מערכת ניהול זהויות מספקת שירותי הזדהות והרשאות למשתמשי מערכות הפועלות בסגמנט האינטרנט של המשרד. אופי אוכלוסיית המשתמשים השונים מפורט בטבלה הבאה:

תיאור	אוכלוסייה
אדם לומד או אדם הזכאי לחינוך בסיסי במערכת החינוך	תלמידים
אדם המוסמך ללמד במערכת החינוך	עובד הוראה
אדם המועסק בבית הספר ואינו עובד הוראה: מזכירה, לבורנט, איש תחזוקה, ספרן וכדומה	סגל מנהלי בית ספר
אדם חיצוני לארגון שאינו מנוהל במערכות הליבה של הארגון ונדרש לקיים אתו קשרי מידע: עובד רשות מקומית, עובד בעלות וכדומה	אחרים
אדם המועסק על ידי משרד החינוך	עובד משרד

שירותים שהמערכת מספקת:

- ניהול מחזור חיי חשבונות המשתמשים (Provisioning) מנקודה מרכזית;
- בקרת גישה מאובטחת מבוססת הזדהות אישית למערכות המשרד באינטרנט;
- יכולת גישה בהזדהות יחידה (SSO);
- הפעלת מוקדי שירות לתמיכה בסיסמאות והרשאות;
- רישום וניהול עצמי (Self Service) לתמיכה בסיסמאות;
- אכיפת מדיניות מרכזית לאבטחת מידע.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

לאור הצורך של משרד החינוך לאפשר למורים ותלמידים הזדהות אחידה לכלל יישומי מערכת החינוך באמצעות סיסמת משרד החינוך, החליט המשרד להרחיב את שירותי הגישה וההזדהות המרכזיים גם לספקים חיצוניים המספקים שירותים חינוכיים וטכנולוגיים לאוכלוסיות במערכת החינוך. מפורסמים בזאת הנחיות ודרישות לחיבור ספק חיצוני למערכת ההזדהות המרכזית של המשרד לצורך קבלת שירותי הזדהות.

תועלות המשרד מהרחבת השירות

- הזדהות אחידה לכלל יישומי מערכת החינוך;
- מדיניות סיסמאות אחידה;
- שיפור רמת אבטחת המידע במעבר לניהול מרכזי של הזהויות ומערך ההזדהות;
- שיפור רמת השרות לאוכלוסיית מערכת החינוך;
- מוקדי שירות ותמיכה מרכזיים;
- סיסמה אחת לכלל שירותי המשרד באינטרנט;
- סיוע לספקים;
- חיסכון בעלויות פיתוח תחזוקה ותפעול של ניהול מערך גישה והזדהות;
- הפניית משאבי הספק להתמקדות בתכנים.

2. מונחים והגדרות

מונח	הגדרה
המשרד	משרד החינוך
ספק חיצוני	ספק שאושר על ידי המשרד לספק שירותים חינוכיים טכנולוגיים דיגיטליים לבתי הספר
משתמש מערכת החינוך (להלן "משתמש")	אדם הזכאי לשירותי גישה למערכות המשרד באינטרנט ושפרטיו מנוהלים במערכת ניהול זהויות מרכזית של המשרד
מערכת ניהול זהויות IDM	מערכת מרכזית של המשרד המספקת שירותי גישה, הזדהות והרשאות למערכות ולשירותי המשרד באינטרנט למשתמשי מערכת החינוך
הזדהות (Authentication)	זיהוי המשתמש המבקש לגשת לשירותי המשרד באינטרנט באמצעות פרטי זיהוי אישיים
הרשאה (Authorization)	הגדרה של הפעולות שמותר למשתמש לבצע
מטה לאישור ובקרה של ספקים חיצוניים (אוניברסיטת אריאל בשומרון)	מטה מינהלי שבאמצעותו מבצע משרד החינוך בדיקה ואישור של מערכות ספק חיצוני. תהליך הבדיקה והאישור כולל עמידה של מערכת הספק בדרישות, תקנים והנחיות שאותם קבע המשרד. בנוסף לכך מבצע הגוף מעקב, בקרה ובדיקות תקופתיות של מערכות ספק חיצוני פעילות.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

3. דרישות סף לחיבור מערכת ספק חיצוני לשירותי הזדהות מרכזיים של משרד החינוך

- 3.1** אישור הספק על ידי המשרד למתן שירותים דיגיטליים לאוכלוסיית החינוך בבתי הספר. האישור ניתן על ידי המשרד באמצעות המינהל למדע וטכנולוגיה, שמואל ברייט, בדוא"ל: shanina@ariel.ac.il.
- 3.2** על הספק להגיש טופס "בקשה לחיבור ספק חיצוני למערכת ההזדהות של משרד החינוך" לשמואל ברייט בדוא"ל: shanina@ariel.ac.il, טל': 03-7407221.

4. הנחיות כלליות להתחברות מערכת ספק לשירותי הזדהות של משרד החינוך

להלן הנחיות ודרישות כלליות לחיבור קבלן/ספק למערכת ההזדהות המרכזית של המשרד לצורך קבלת שירותי הזדהות:

- 4.1** טרם החיבור על הספק לעמוד בדרישות הסף המפורטות בסעיף 3, וברשותו טופס "בקשה לחיבור ספק חיצוני למערכת ההזדהות של משרד החינוך" מאושר וחתום.
- 4.2** יש לפנות לצוות ניהול משתמשים והרשאות במשרד החינוך באמצעות מר יוסי עמיאל בדוא"ל: yossiam@education.gov.il או בטל': 02-5603048, בבקשה לחיבור מערכת הקבלן/ספק לשירותי ההזדהות של המשרד.
- 4.3** מערכת ההזדהות של המשרד תספק שירותי הזדהות לאוכלוסיות הבאות:
- עובדי הוראה;
 - תלמידים הלומדים במערכת החינוך;
 - עובדי סגל מינהלי בבתי הספר;
 - עובדי המשרד;
 - אחר: גורמי חוץ המורשים לגשת למערכות המשרד;
 - אוכלוסיות המאושרות באופן פרטני.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

- 4.4** מערכת ההזדהות של המשרד תספק שירותי הזדהות (Authentication) בלבד.
- 4.5** הרשאות (Authorization) ליישומי הספק יהיו באחריות הספק.
- 4.6** הזדהות משתמשים ליישומי הספק תהיה באמצעות פרטי זיהוי אישיים שסופקו על ידי המשרד ובכפוף למדיניות הסיסמאות של המשרד באותה תקופה.
- 4.7** חיבור יישומי הספק למערכת ההזדהות יהיה מאובטח ומוצפן באמצעות תעודות דיגיטליות.
- 4.8** חיבור יישומי הספק למערכת ההזדהות יחייב את הספק לעמוד בתקן החיבור הטכנולוגי של המשרד התקף באותה עת.
- 4.9** עלות חיבור מערכות הספק לתשתית ההזדהות של המשרד תהיה על חשבון הספק.
- 4.10** ייתכנו מקרים חריגים שעבור חיבור היישומים לתשתית ההזדהות של המשרד יידרש הספק לעשות שימוש ברכיבי תוכנה נוספים שאינם קיימים ברשותו. אחריות רכישת הרכיב תהיה על הספק.
- 4.11** כחלק מתהליך ההזדהות מועברים ליישום הספק פרטים על המשתמש שהתחבר: פרטים כלליים על המשתמש, נתוני שיבוץ בבית ספר.
- 4.12** תמיכה במשתמשים בבעיות הזדהות ליישומי הספק, לרבות סיסמה, תהיה באמצעות מוקדי שירות ובאמצעות שירותים עצמיים שאותם יעמיד המשרד לרשות המשתמשים.
- 4.13** תמיכה בבעיות חיבור של יישומי הספק לתשתית ההזדהות של המשרד תהיה באמצעות מוקד התפעול של המשרד – **צוות IDM**.
- תמיכה ותפעול של המשרד**
מוקד סיוע של המשרד לדיווח תקלות ספקים
טל': 02-5602510
שעות פעילות המוקד: ימים א'-ה', בשעות: 07:00-17:00
- 4.14** על הספק להעמיד איש קשר מטעמו לטיפול בבעיות גישה ותפעול ליישומים שבאחריותו.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

5. שלבים בחיבור מערכת ספק חיצוני למערכת ההזדהות של משרד החינוך

חיבור מערכת ספק למערכת ההזדהות של המשרד כולל את השלבים הבאים: אפיון, בנייה והקמה, בדיקות, הפעלה בייצור. להלן רשימת השלבים והפעילויות לכל שלב:

5.1 אפיון – אפיון פתרון החיבור עם צוות מערכת הזדהות של המשרד הכולל:

- א. אופי היישום וטכנולוגיית היישום של הספק;
- ב. אוכלוסיית המשתמשים;
- ג. הזדהות והרשאות;
- ד. היבטי תמיכה ותפעול.

5.2 בנייה והקמה – סביבת בדיקות (ספק):

א. הקמת חיבור מאובטח Trust בין הספק החיצוני לספק הזהויות, המשרד (שימוש בתעודות והחלפת מפתחות) – שימוש בתעודות Self Signed.

ב. לקבלת SAML2 Metadata של מערכת הזהויות של המשרד יש להיכנס לקישור:

<https://is.remote.education.gov.il/nidp/saml2/metadata>

ג. על הספק לממש במערכות שבאחריותו Service Provider SAML2 ולשלוח לצוות IDM במשרד החינוך את ה-Metadata.

ד. על הספק לפעול לחיבור המערכות לתשתית ההזדהות של המשרד בסביבת הבדיקות.

ה. הזדהות: גישה בהזדהות של משתמשי מערכת החינוך למערכת הספק תהיה באמצעות אִיקוֹן (צלמית) ייעודי של משרד החינוך. האיקון ישולב בדף הבית של הספק.

ו. כחלק מתהליך ההזדהות מועברים ליישום הספק פרטים על אודות המשתמש שהתחבר: פרטים כללים על המשתמש, נתוני שיבוץ בבית ספר.

ז. ריבוי מוסדות למשתמש: על הספק לטפל בתסריט שבו המשתמש המבקש לגשת למערכת שייך ליותר מבית ספר אחד (מורה/תלמיד המלמד/לומד בכמה בתי ספר. במקרים אלו מומלץ להציג למשתמש רשימה של בתי ספר לבחירה.

ח. הרשאות:

1) על הספק לטפל בתסריט של משתמש שעבר הזדהות בהצלחה למערכת הספק, אבל אינו רשאי להשתמש בתוכנה או שלא רכש מנוי מן הספק. בבעיית הרשאה על הספק להציג למשתמש הודעה ברורה ופרטי קשר לטיפול.

2) טיפול בהרשאות גישה לתכנים דיגיטליים לבעלי תפקידים מיוחדים במערכת החינוך.

ט. התנתקות: שילוב לחצן התנתקות בדף הבית בהתאם להנחיות המשרד.

י. להנחיות ופרטים נוספים יש לפנות לצוות IDM במשרד החינוך.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

5.3 בדיקות (ספק, משרד החינוך):

שלב זה יתמקד בבדיקה של תהליך ההזדהות וההרשאות למערכות הספק באמצעות מערכת ההזדהות של המשרד. שלב זה לא יכלול בדיקות פונקציונליות של יישום הספק לאחר תהליך ההזדהות.

- א. על הספק להעביר לצוות IDM רשימה של משתמשים לבדיקה. הרשימה צריכה לכלול משתמשים בפרופילים שונים בהתאם לאוכלוסייה המזדהה למערכת הספק ותפקידם במערכת החינוך (מחנך, מזכירה, רכז תקשוב);
- ב. בדיקות תהליכי הזדהות עבור פרופילים של משתמשים;
- ג. בדיקה של תסריטי הרשאות;
- ד. התנתקות;
- ה. SSO;
- ו. לחצן/איקון הזדהות משרד החינוך רשמי בדף הבית.

5.4 הפעלה בייצור (ספק, משרד החינוך):

- א. אישור בדיקות;
- ב. אישור תשתיות משרד החינוך וצוות IDM;
- ג. אישור הספק;
- ד. הקמת חיבור מאובטח Trust בין הספק החיצוני לספק הזהויות, המשרד (שימוש בתעודות והחלפת מפתחות).
- ה. על הספק לחתום על SAML Request באמצעות SSL CERTIFICATE חתום על ידי גוף CA חוקי.

6. תמיכה ושירות

הפצה, הפקה ותמיכה בפרטי זיהוי אישיים וסיסמאות למשתמשי מערכת החינוך יהיו באחריות משרד החינוך. התמיכה במשתמשים בבעיות הזדהות וסיסמאות תתאפשר בכמה ערוצים: באמצעות מוקדי שירות, שירותים עצמיים, הפצה יזומה של פרטי זיהוי אישיים וסיסמה.

6.1 מוקד סיסמאות של המשרד

תמיכה בבעיות גישה ליישומי משרד באמצעות מוקד סיסמאות של המשרד תינתן בהתאם לזמני השירות לכלל אוכלוסיות משתמשי המשרד. המוקד ייתן מענה ראשוני לבעיות גישה ליישום הנובעות מבעיות הזדהות: העדר פרטי זיהוי אישיים, שכחה של סיסמה, איפוס סיסמה. התנאי לקבלת השירות יהיה זיהוי המשתמש על פי פרטים מזהים על ידי המוקדן וקיום **חשבון פעיל** לפונה במערכת ההזדהות של המשרד. בעיות גישה ליישום שאינן נובעות מבעיית הזדהות יועברו למוקדי השירות המקצועיים ובהתאם לתסריטי התמיכה הנהוגים באותה עת.

מוקד סיסמאות של המשרד – טל': 03-9298888

בימים א'-ה', בשעות 00:00-20:00

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

- 6.2 מערכת ניהול סיסמאות בבתי הספר**
- בבתי הספר פועלת מערכת ניהול סיסמאות המאפשרת תמיכה בסיסמאות לעובדי הוראה, תלמידים וסגל מינהלי בבית הספר. שירות זה זמין למשתמשים בזמני הפעילות של בית הספר ובכפוף להנחיות מנהל בית הספר.
- 6.3 שירותים עצמיים לתמיכה בסיסמאות**
- משרד החינוך מפעיל שירותים עצמיים לתמיכה בסיסמאות. שירותים אלו מאפשרים למשתמש להפיק סיסמה באמצעות תיבת הדוא"ל האישית או טלפון נייד. שירותים אלו זמינים בכל שעות היממה ואינם מחייבים פנייה למוקד. פרטים נוספים על שירות זה ניתן לקבל באתר משרד החינוך.
- 6.4 הפצה יזומה של סיסמאות על ידי המשרד**
- מערכת ההזדהות של המשרד מפיצה לכל משתמש חדש הודעה לתיבת הדוא"ל האישית, ובה הנחיות על אופן הפקת סיסמה וקבלת פרטי זיהוי אישיים לצורכי גישה למערכות המשרד. בנוסף לכך עובדי הוראה המקבלים את שכרם מן המדינה מקבלים את פרטי הזיהוי והסיסמה בתלש השכר.
- בעיות אחרות – הרשאות ;
- בעיות גישה ליישום הספק שאינן נובעות מבעיית הזדהות, לדוגמה: בעיות הרשאות או תפעול היישום יועברו לטיפול לאיש הקשר מטעם הספק.
- 6.5 מוקד / איש קשר ספק**
- על הספק להעמיד פרטי התקשרות למוקד שירות או לאיש קשר מטעמו לצורך טיפול בקריאות שירות הקשורות בגישה ו/או הפעלה של יישומים שבאחריותו.
- 7. חוסן ואמינות**
- 7.1** ככלל מערכת ההזדהות של המשרד זמינה 24/7.
- 7.2** מערכת ההזדהות של המשרד נבנתה בתצורת שרידות המסוגלת לתמוך בכמות גדולה של משתמשים ועומסים.
- 8. הגבלת אחריות**
- המשרד לא יהיה אחראי לפגיעה במוניטין הספק כתוצאה מהעדר שירות ללקוחותיו העלול להיגרם כתוצאה מתקלה בשירותי ההזדהות של המשרד.
- 9. תפעול**
- 9.1** תפעול מערכת ההזדהות באחריות המשרד.
- 9.2** תפעול מערכות הספק באחריות הספק.

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

10. גורמים מעורבים

- 10.1 צוות IDM משרד החינוך, יוסי עמיאל טל': 02-5603048
- 10.2 משרד החינוך, המינהל למדע וטכנולוגיה, שמואל ברייט טל': 03-7407221

11. נספחים

- 11.1 הזדהות אחידה – [נספח טכנולוגי](#)
- 11.2 נספח תפעול
- 11.3 [טופס אישור לחיבור מערכת ספק למערכת ההזדהות של משרד החינוך](#)
- 11.4 מדריך למשתמש למערכת ההזדהות – [לחץ כאן](#)

מדינת ישראל
 משרד החינוך
 מינהל תקשוב, טכנולוגיה ומערכות מידע
 פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

11.1 הזדהות אחידה – נספח טכנולוגי

מונח	הגדרה
מערכת מנוהלת	כל מערכת אשר נתוני המשתמשים והרשאותיהם שבה נשלטים ו/או מסונכרנים מול מערכת ניהול ההזדהות וההרשאות המרכזית IDM של המשרד
משתמש (Identity Principal)	אדם המבקש לגשת לשירות ברשת, להלן משתמש מערכת החינוך
ספק שירות (Service Provider – SP)	ארגון או גוף המספק שירותי רשת (מערכת מנוהלת) למשתמשים במערכת החינוך באינטרנט, להלן ספק חיצוני
ספק זהויות (Identity Provider – IDP)	ארגון או גוף המוסמך לנהל זהויות (אדם או משאב) ולספק שירותי אימות לזהות, להלן מערכת לניהול זהויות IDM
חיבור מאובטח (Trust)	אבטחת ערוץ תקשורת בין הספק החיצוני לספק הזהויות על ידי תעודות והחלפת מפתחות
Relaying Party	גוף שקיים עבורו חיבור מאובטח עם המשרד
Token	פיסת מידע המועברת באמצעות הדפדפן ומכילה אישור ונכונות משתמש (Identity Principal) ומאפיינים עליו. ה-Token מוצפן וחתום על ידי ספק זהויות (Identity Provider) וניתן לפתיחה רק על ידי ספק שירות שקיים עבורו חוזה שירות Trust עם ספק הזהויות.
SAML Token	Token במבנה XML המכיל מידע על המשתמש ותפקידיו – משמש את ספק השירות לאימות המשתמש ולגזירת הרשאותיו
SSO	גישה של משתמש למשאב ברשת שקיים לו Token תקף ללא צורך בהזדהות נוספת
הזדהות (Authentication)	זיהוי המשתמש המבקש לגשת לשירותי המשרד באינטרנט באמצעות פרטי זיהוי אישיים
הרשאה (Authorization)	הגדרה של הפעולות המותרות למשתמש לבצע

רקע כללי

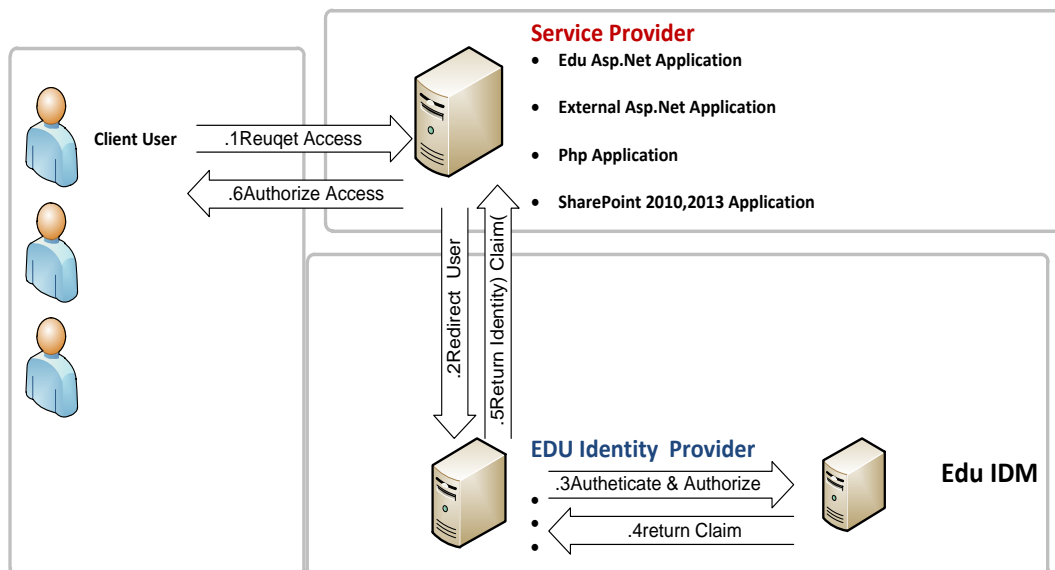
הפתרון הטכנולוגי להרחבת שירותי ההזדהות המרכזיים של המשרד עבור ספקים חיצוניים מבוסס על פרוטוקול עולמי פתוח הידוע בשם SAML (Security Assertion Markup Language). פרוטוקול זה מאפשר החלפה של שירותי הזדהות והרשאות בין צדדים, במיוחד בין ספק הזדהות (להלן "מערכת ההזדהות של משרד החינוך IDM") לבין ספק שירות (להלן "ספק חיצוני").

הצורך המרכזי שעליו עונה השימוש בפרוטוקול SAML הוא היכולת לאפשר שירותי הזדהות מאובטחים מרכזיים ו-SSO לגישה של משתמשים באמצעות דפדפן למערכות **אינטרנט** של הארגון ולמערכות **אינטרנט** של ספקי צד שלישי **מחוץ לארגון**, יכולת שעד אז הייתה אפשרית רק לשירותים הניתנים למשתמש ברשת הפנים הארגונית. ממצב שבו גישה מאובטחת לשירות של ספק שירות חיצוני חייבה את הספק בניהול המשתמשים והרשאותיהם, יתאפשר עכשיו לספק להתחבר למערכת ההזדהות המרכזית של המשרד (**IDM**) ולחסוך מעצמו את הצורך בניהול המשתמשים ובניהול גישה מאובטחת (**Authentication**).

ככלל, עולם ה-IT צועד לכיוון בקרת גישה מבוססת **טענת נכונות** (Assertion). מודל זה מציג שלוש הגדרות עיקריות – **משתמש** (Principal), **ספק זהויות** (IDP), **ספק שירות** (SP), ונותן מענה לתסריט העיקרי הבא: **המשתמש** פונה לשירות של **ספק שירות** כלשהו. ספק השירות מעוניין לאמת ולאשר את נכונות **המשתמש מספק הזהויות**. על בסיס טענת נכונות זו יכול ספק השירות לאפשר גישה למשתמש לשירות המבוקש. ספק הזהויות מאשר את נכונות **המשתמש** באמצעות פרטי זיהוי אישיים, למשל קוד משתמש וסיסמה (**Authentication**), שאותם מעביר המשתמש לספק הזהויות. בתום ההזדהות מועבר המשתמש יחד עם Token חזרה לשירות שביקש. ספק השירות בודק את ה-Token (Assertion) של המשתמש ומאשר לו את הגישה למשאב שביקש.

התרשים הבא מתאר את תהליך ההזדהות של משתמש לשירות של ספק חיצוני:

שרותי הזדהות לספקים חיצוניים



1. בקשה של משתמש להפעלת שירות של ספק שירות חיצוני – המשתמש ניגש באמצעות דפדפן לשירות של ספק שירות (Service Provider), למשל <https://sp.example.il/myresource>. ספק השירות מבצע בדיקת זיהוי למבקש השירות. אם המבקש מזוהה, יש לדלג על שלבים 2 עד 5.
2. הפניה של המשתמש לספק הזהויות לצורכי זיהוי ואימות – ספק השירות מפנה את המשתמש לספק הזהויות (משרד החינוך) שהוגדר לצורכי זיהוי ואימות, למשל <https://lgn.edu.gov.il/nidp/wsfed/ep?wa=wsignin1.0&wtrealm=https://inet.org.il>.
3. זיהוי ואימות פרטי המשתמש מבקש השירות על ידי ספק הזהויות – ספק הזהויות פונה למשתמש ומבקש ממנו לעבור בדיקת הזדהות.
4. זיהוי המשתמש ויצירת Token על ידי ספק הזהויות – אם ההזדהות מוצלחת, ספק הזהויות מחזיר את ה-Token שמכיל את ה-Identity של המשתמש.
5. המשתמש מועבר חזרה לכתובת השירות של ספק השירות המבוקש יחד עם ה-Token. ספק השירות מגדיר את הרשאות הגישה בהתאם ל-Token.
6. המשתמש מקבל גישה למשאב.

11.2 נספח תפעול

א. הרשאות לסביבות תוכן לבעלי תפקידים בבית הספר ובמשרד החינוך בתחום התקשוב

המעבר להזדהות האחידה לסביבות התוכן מבטל את הצורך בניהול רשימות של בעלי תפקידים מיוחדים, כגון מדריכי תקשוב, מפקחי תקשוב ומטמיעי תקשוב, על ידי הספקים לצורך יצירת סיסמאות ומתן הרשאות גישה.

ההזדהות וההרשאות יהיו מעתה באופן הבא:

הזדהות – לכלל בעלי התפקידים והתלמידים יש קוד וסיסמה של משרד החינוך, ובאמצעותם הם מזדהים למערכות המשרד לרבות תכנים של ספקי התוכן.

הרשאות – יש לעדכן את מנגנון ההרשאות של כל ספק באופן הבא:

יש להתייחס למאפיין OrgRolesSimple שמתקבל ב-SAML Token שמגיע ממשרד החינוך. כל משתמש שה-OrgRolesSimple מכיל אחד מהתפקידים הארגוניים שלהלן יקבל הרשאה מלאה לכל התכנים של הספק:

793 – מפקח תקשוב מחוזי

794 – מטמיע תקשוב רשותי

795 – מדריך תקשוב **במוסד 110110**

החל משנת הלימודים תשע"ז לא יועברו רשימות של בעלי תפקידים במוסד, ולא ייעשה שימוש במוסדות פיקטיביים לצורך מתן הרשאות. הדרך היחידה לתמוך בהרשאות לבעלי תפקידים היא באמצעות התפקיד הארגוני (OrgRolesSimple), כפי שהוסבר לעיל.

ב. הגדרת אנשי תמיכה ב-IDM עבור ספק

רקע – כדי לאפשר לצוות הספק להזדהות לתכנים שלו באמצעות הזדהות אחידה של משרד החינוך, יש להגדיר את אנשי צוות הספק ב-IDM:

1. להגדרת איש תמיכה מטעם הספק יש לפנות לתמר צימרינג בדוא"ל:

tamarcim@education.gov.il, באמצעות מילוי טופס הצהרת סודיות.

2. איש התמיכה יוגדר על ידי תמר צימרינג בתפקיד ארגוני תומך בישות ארגונית של הספק, בהתאם לטבלת הספקים בסעיף 3) להלן.

3. לכל ספק מאושר מוגדר במשרד החינוך קוד ספק ייחודי: (קוד הספק ניתן במעמד מילוי טופס לאישור חיבור ספק למערכת ההזדהות).

שם הספק	קוד הספק
בריינפופ	8800000001

מדינת ישראל
 משרד החינוך
 מינהל תקשוב, טכנולוגיה ומערכות מידע
 פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

שם הספק	קוד הספק
המרכז הישראלי למצוינות בחינוך	88000000002
אלנט (Lnet)	88000000003
סנונית	88000000004
מטח	88000000005
הלומדה	88000000006
עת הדעת	88000000007
ממשק	88000000008
אלמוסתקבל ספרים דיגיטליים	88000000009
פור אי די (4ID)	88000000010
חילין מערכות	88000000011
מלינגו	88000000012
גמרא ברורה	88000000013

אם פרטי הספק אינם מופיעים ברשימה, יש לפנות לצוות תפעול IDM – לרונית מורגנשטרן

בדוא"ל: ronitmo@education.gov.il.

4. הספק רשאי להחליט לנהל הרשאות עבור איש תמיכה מטעמו. הספק ייצוק תוכן לתפקיד התמיכה על פי החלטתו. כאשר איש תמיכה מטעם הספק גולש לתכנים של הספק, ידע הספק להבחין שמדובר באיש תמיכה מטעמו על פי הנתונים ב-Token: איש תמיכה מטעם הספק הוא בתפקיד ארגוני תומך עם סמל ישות של הספק (ראו למעלה טבלת קודי ספק).

ג. תוקף תעודות (SSL CERTIFICATE)

בתהליך חיבור הספק למערכת ההזדהות של המשרד נעשה שימוש בתעודת SSL בצד הספק לצורכי אבטחת מידע. באחריות הספק לדאוג להחלפת תעודות שפג תוקפן. החלפת התעודות תהיה בתיאום עם המשרד.

מדינת ישראל
 משרד החינוך
 מינהל תקשוב, טכנולוגיה ומערכות מידע
 פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

11.3 טופס אישור לחיבור מערכת חיצונית לשירותי ההזדהות של משרד החינוך

פרטי הספק/הארגון/החברה (למילוי על ידי הספק)

	קוד ספק (למילוי) על ידי צוות IDM:		שם הספק/ ארגון/חברה:		תאריך הבקשה:
					תיאור המוצר:
	טלפון נייד:		טלפון:	שם איש קשר מטעם המערכת:	
			כתובת דוא"ל:		
	טלפון נייד:		טלפון:	שם איש קשר טכנולוגי:	
			כתובת דוא"ל:		

פרטי הלקוח במשרד החינוך – הגורם המאשר חיבור ספק תוכן

קישור לאישור בענן החינוכי	מס' אישור	תאריך אישור	יחידה	תפקיד	פרטי הגורם

נספח בדיקות

להלן תסריטי בדיקות שיש לבצע בסביבת טסט לפני עלייה לייצור

1. הוספת כפתור הזדהות משרד החינוך – מערכת של ספק חיצוני תוסיף כפתור "הזדהות משרד החינוך" שתפנה לדף הזדהות של משרד החינוך
2. הזדהות תקינה עם פרטי קוד משתמש וסיסמה
3. מימוש הרשאות
 - משתמש מורשה – משתמש שהזדהה בהצלחה ומורשה להיכנס למערכת, יש להציג את שמו המלא בצד שמאל או ימין במסך
 - משתמש לא מורשה - במידה ומשתמש עבר הזדהות בהצלחה אך אינו מורשה (אין לו תפקיד במערכת) יש להציג הודעה מתאימה: " אינך מורשה למערכת, נא וודא מול מנהל מערכת כי הינך מוגדר כמורשה למערכת "
4. הוספת כפתור יציאה /התנתקות – מימוש: לחיצה על כפתור יציאה/ התנתקות מנתק את פרטי היוזר ממערכת ההזדהות, המימוש יהיה בהתאם לטכנולוגיה של המערכת
5. ריבוי תפקידים ומוסדות – משתמש יכול להיות משויך למספר תפקידים ארגוניים במספר מוסדות ובסוגי מוסדות שונים כגון (רשות, בעלות, בית ספר וכו') יש להתייחס לתפקידים וסוגי ישויות הרלוונטיים, ההמלצה להציג למשתמש קומבו עם המוסדות המשויכים אליו
6. יש להוסיף לתפריט צדדי במערכת קישור ל"חשבון שלי" החשבון שלי משמש את המשתמש לעדכון שוטף של פרטי הזדהות ופרטי קשר לצרכי אימות ותמיכה בסיסמאות בפניות למוקד סיסמאות ולשימוש בשרותים העצמיים להפקת סיסמה

<http://appslimud.education.gov.il/EduLogin/myaccount.aspx> - TEST

<https://apps2.education.gov.il/EduLogin/myaccount.aspx> - - PROD

דגשים למעבר לייצור:

יש להעביר certificate (חוקי) לצורך הגדרת המערכת בייצור

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0

החלפת תעודה עבור הזדהות ב- Federation

התעודה שבשימוש היום היא: lgn.edu.gov.il – תוקף התעודה עד 22-06-2017
אנו מחליפים לתעודה - signingfds.edu.gov.il תוקף התעודה עד 3-07-2020

תוכנית עבודה:

1. התקנת תעודה חדשה בשרתי ה Access Manager.
2. הכנת קבצים \ הסבר עבור ספקי התוכן
3. תיאום יום לביצוע ההחלפה, תהיה השבתה, עד שהספק יעדכן בצד שלו.
4. שליחת מסמך הסבר לספקי התוכן.
5. החלפת התעודה ב Access Manager ביום המעבר.
6. כל ספק יבצע את השינוי לפי ההנחיות המתאימות למערכת שלו.

להלן פעולות שנדרש ספק התוכן לבצע עבור עדכון התעודה, כל אחד ושיטת החיבור שלו.

שיטת חיבור - .Net

להחליף את ה Thumbprint

את הערך: 0e78303234e4347a482fdcedd60bca0883c1ac71
להחליף ב: d2bb771913a4214179f6eddb5fe3cf9b63385856

```
<trustedIssuers>  
  <add thumbprint="d2bb771913a4214179f6eddb5fe3cf9b63385856"  
    name="https://lgn.edu.gov.il/nidp/saml2/metadata" />  
</trustedIssuers>
```

שיטת חיבור - SimpleSAMLphp

להחליף את הקובץ saml20-idp-remote.php הקיים בקובץ הזה:



saml20-idp-remote.php

שיטת חיבור - ADFS

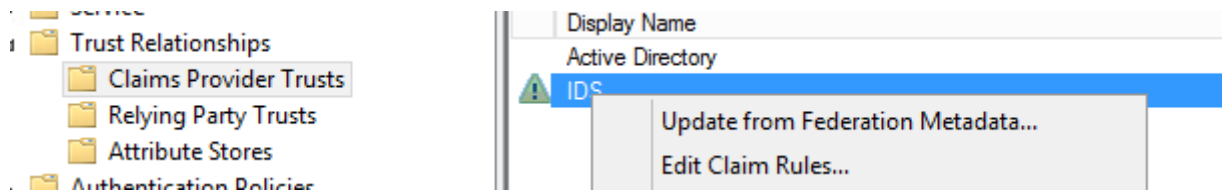
להיכנס לניהול של ה ADFS

Trust Relationships → Claims Provider Trust → right click on IDS → Update from Federation MetaData

מדינת ישראל
משרד החינוך
מינהל תקשוב, טכנולוגיה ומערכות מידע
פרויקט ניהול זהויות IDM – הזדהות אחידה

מאי 2016

גרסה 2.0



שיטת חיבור - Python

לערוך את הקובץ settings.json לשנות את הערך של x509cert תחת ה IDP, להחליף את הטקסט שמכיל את התעודה, בטקסט הקיים בקובץ המצורף settings.json בשורה x509cert. לשים לב שזה בא בשורה אחת, לפתוח את הקובץ ב Notepad++ .



settings.json