הזדהות אחידה למערכות משרד החינוך

חיבור ספקי תוכן דיגיטלי
למערכת ההזדהות
של משרד החינוך

נובמבר 2014

הגדרות - מונחים

המשרד

משרד החינוך

ספק חיצוני

ספק שאושר על ידי המשרד לספק שרותים חינוכיים טכנולוגיים

מערכת ניהול זהויות IDM

מערכת מרכזית של המשרד המספקת שרותי גישה הזדהות והרשאות למערכות ולשרותיי המשרד באינטרנט למשתמשי מערכת החינוך

משתמש מערכת החינוך (להלן "משתמש")

אדם הזכאי לשרותי גישה למערכות המשרד באינטרנט ושפרטיו מנוהלים במערכת ניהול זהויות מרכזית של המשרד

הזדהות Authentication

זיהוי המשתמש המבקש לגשת לשרותי המשרד באינטרנט באמצעות פרטי זיהוי אישיים

הרשאה Authorization

הגדרה של הפעולות המותרות למשתמש לבצע

רקע – ניהול משתמשים והרשאות במשרד החינוך

- משרד החינוך מפעיל מערכת לניהול זהויות, להלן IDM, המאפשרת למשרד לבצע ניהול מרכזי של חשבונות המשתמשים והרשאותיהם במערכות המחשוב השונות, בסביבת האינטרנט, תוך שמירה על אחידות ואכיפת נהלי 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 שרותי ההזדהות והרשאות למשתמשי מערכות הפועלות בסגמנט האינטרנט של המשרד.

זהויות במשרד החינוך

אוכלוסייה	תיאור	מקור לזהויות	כמות נוכחית	צפי גידול
תלמידים	אדם לומד או אדם הזכאי לחינוך בסיסי במערכת החינוך.	מערכת תלמידים	500,000	1.5 מיליון
עובד הוראה	אדם המוסמך ללמד במערכת החינוך	מערכת עובדי הוראה	500,000	
סגל מנהלי בית ספר	אדם המועסק בבית הספר בתפקיד מנהלי :מזכירה, לבורנט,איש תחזוקה,ספרן וכדומה	מערכת סגל מנהלי/קבצי EXCEL	10,000	
הורה/אפוטרופוס במערכת החינוך	למשרד אין כיום רישוי לניהול זהויות הורים		0	1.5
אחרים	אדם חיצוני לארגון שאינו מנוהל במערכות הליבה של הארגון ונדרש לקיים איתו קשרי מידע	מערכת גורמי קשר	20,000	
סה"כ			1.2 מיליון	כ - 5 מיליון

הצורך - הדרישה

לאור הצורך של משרד החינוך לאפשר למורים ותלמידים הזדהות אחידה לכלל יישומי מערכת החינוך החליט המשרד להרחיב את שרותי הגישה וההזדהות המרכזיים גם לספקים חיצוניים המספקים שרותים חינוכיים וטכנולוגיים לאוכלוסיות במערכת החינוך

תועלות לארגון מהרחבת השרות

- 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 שרות ותמיכה מרכזיים
- SSO – גישה לשרותי המשרד ללא צורך בהזדהות נוספת
- סיוע לספקי התוכן
- הרחבת מעגל ספקי התוכן
- קידום תכנית המחשוב הדיגיטלי בבתי הספר

תועלות לספק חיצוני

- חסכון בעלויות פיתוח תחזוקה ותפעול של ניהול מערך גישה והזדהות ליישומי הספק
  - ניהול מערך ההזדהות (חומרה , תוכנה, פיתוח תחזוקה ותפעול)
  - ניהול מערך תמיכה בסיסמאות ובמדיניות סיסמאות
  - SSO מובנה
  - ניהול ממשקים וקבצי משתמשים
  - עמידה בתקן אבטחת מידע של המשרד (מובנה)
- הפניית משאבי הספק להתמקדות בתכנים

דרישות סף לקבלת השרות

- אישור מהמשרד למתן שרותים לאוכלוסיית החינוך.
- עמידה של הספק בתקן אבטחת המידע המפורסם באתר מינהל מדע וטכנולוגיה בכתובת
- http://cms.education.gov.il/EducationCMS/UNITS/MadaTech
- אישורים ניתנים על ידי מינהל תקשוב ומדע וטכנולוגיה ובאמצעות מר נועם קוריאט

תפיסת הפתרון

- הפתרון הטכנולוגי להרחבת שרותי ההזדהות המרכזיים של המשרד עבור ספקים חיצוניים מבוסס על פרוטוקול עולמי פתוח הידוע בשם - Saml - Security Assertion Markup Language.
- פרוטוקול זה מאפשר החלפה של שרותי הזדהות והרשאות בין צדדים, במיוחד בין ספק הזדהות (להלן "מערכת ההזדהות של משרד החינוך- IDM") לבין ספק שרות (להלן "ספק חיצוני").
- בקרת גישה מבוססת טענת נכונות Assertion

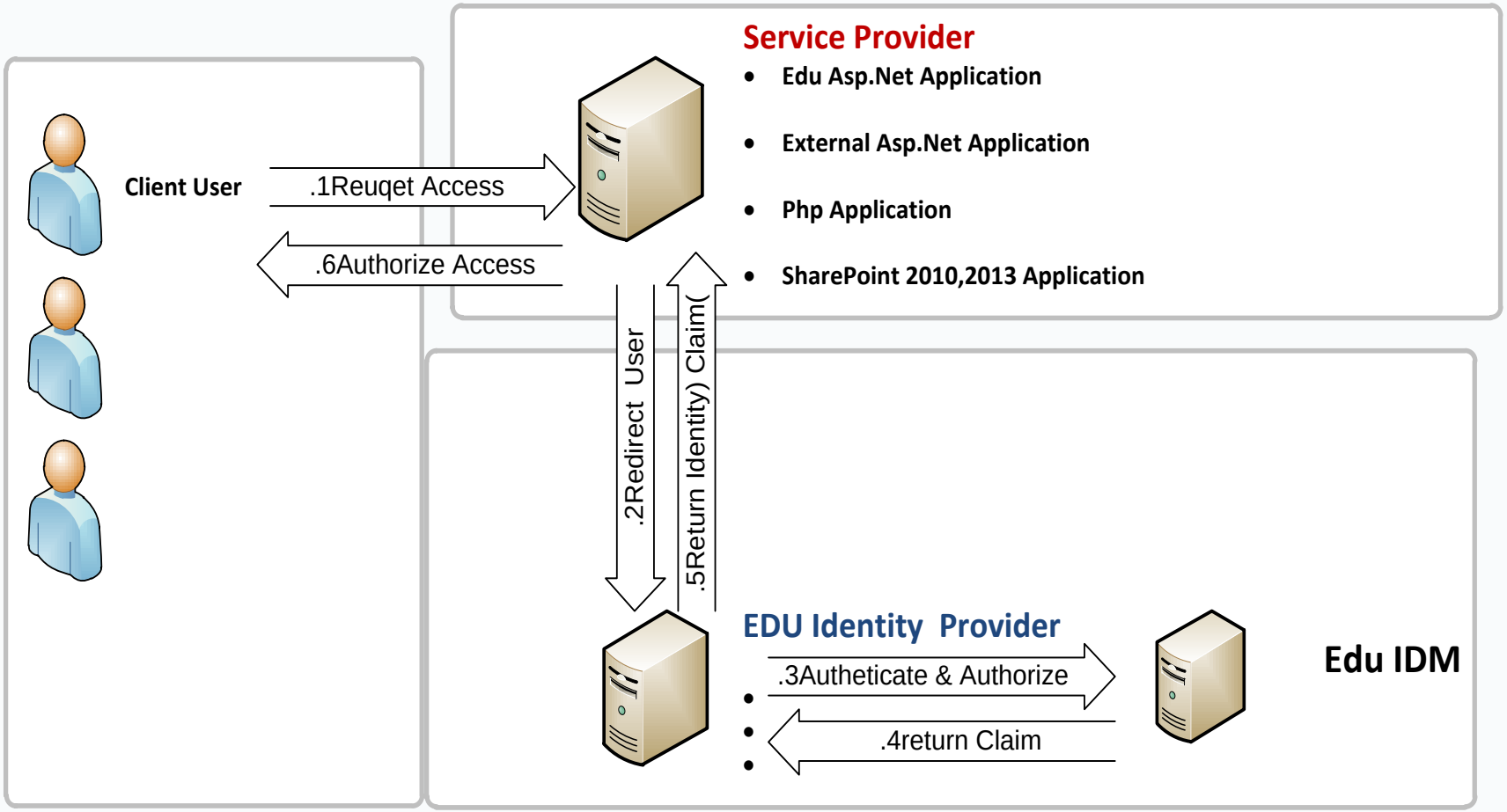
טכנולוגיה - הגדרות

- **מערכת מנוהלת** :כל מערכת אשר נתוני המשתמשים והרשאותיהם בה נשלטים ו/או מסונכרנים מול מערכת ניהול ההזדהות וההרשאות המרכזית IDM של המשרד
- **משתמש Identity Principal** : אדם המבקש לגשת לשרות ברשת, להלן, משתמש מערכת החינוך.
- **ספק שרות Service Provider:** ארגון או גוף המספק שרותי רשת (מערכת מנוהלת) למשתמשים באינטרנט, להלן, ספק חיצוני
- **ספק זהויות Identity Provider:**ארגון או גוף המוסמך לנהל זהויות (אדם או משאב) ולספק שרותי אימות לזהות. להלן, מערכת ניהול זהויות IDM

טכנולוגיה

- **חיבור מאובטח –Trust**: אבטחת ערוץ תקשורת בין הספק החיצוני לספק הזהויות על ידי תעודות והחלפת ממפתחות
- **Relaying Party**: גוף שקיים עבורו חיבור מאובטח עם המשרד
- **Token** : פיסת מידע המועברת באמצעות הדפדפן המכילה אישור ונכונות ה Identity Principal ומאפיינים על המשתמש. ה Token מוצפן וחתום על ידי ה Identity Provider וניתן לפתיחה רק על ידי SP שקיים עבורו חוזה שרות TRUST עם ספק הזהויות Identity Provider.
- **Saml Token :** Token במבנה XML המכיל מידע על המשתמש ותפקידיו. משמש את ספק השרות לאימות המשתמש ולגזירת הרשאותיו.
- **SSO:** גישה של משתמש למשאב ברשת לו קיים Token תקף ללא צורך בהזדהות נוספת

שרותי הזדהות לספקים חיצוניים



טכנולוגיות מוכחות

סוג יישום	טכנולוגיה	רשימת ספקים	פרטי חיבור	איש קשר
מערכות ניהול למידה	Modular - Moodle Object-Oriented Dynamic Learning Environment. שפת פיתוח:PHP	מכון מופ"ת		צוות מערכת הזדהות
פורטלים ארגוניים, שיתוף ידע	MS SharePoint גרסה 2013	משרד החינוך	מחייב שימוש ב ADFS	צוות מערכת הזדהות
יישומי WEB	Asp.NET	משרד החינוך	בשלב הוכחת יכולת	צוות מערכת הזדהות

הנחיות לחיבור ספק חיצוני

- השרות יינתן רק למערכות ויישומים מבוססי WEB להם קיים פתרון טכנולוגי מוכח. לקבלת הרשימה העדכנית יש לפנות לצוות מערכת הזדהות של המשרד.
- מערכת ההזדהות של המשרד מספקת שרותי הזדהות לאוכלוסיות הבאות:
- עובדי הוראה
- תלמידים
- עובדי סגל מנהלי בבתי הספר
- עובדי המשרד
- אוכלוסיות המאושרות באופן פרטני
- מערכת ההזדהות של המשרד תספק שרותי הזדהות (Authentication) בלבד.
- הרשאות (Authorization) ליישומי הספק יהיו באחריות הספק.
- הזדהות משתמשים ליישומי הספק יהיו באמצעות פרטי זיהוי אישיים שסופקו ע"י המשרד ובכפוף למדיניות הסיסמאות של המשרד באותה תקופה.

הנחיות לחיבור ספק חיצוני

- חיבור יישומי הספק למערכת ההזדהות תהיה מאובטחת ומוצפנת באמצעות תעודות דיגיטאליות. התעודות ינופקו על ידי המשרד
- חיבור יישומי הספק למערכת ההזדהות תחייב את הספק לעמוד בתקן החיבור הטכנולוגי של המשרד
- כחלק מתהליך ההזדהות מועברים ליישום הספק הפרטים הבאים אודות המשתמש: מספר זהות/קוד משתמש חד
- תמיכה במשתמשים בבעיות גישה והתחברות ליישומי הספק לרבות סיסמה יהיו באמצעות מוקדי שרות ובאמצעות שרות עצמיים אותם יעמיד המשרד לרשות המשתמשים
- תמיכה בבעיות חיבור של יישומי הספק לתשתית ההזדהות של המשרד תהיה באמצעות מוקד השרות (יפורסם) ובכפוף להסכם השרות (עתידי)

שלבים בחיבור ספק החיצוני

- פניה של המשרד אל הספק (סדר העדיפות יקבע על ידי המשרד)
- סבב אישורים
  - בדיקה כי הספק עומד בדרישות הסף
  - אישור מנהל תשתיות ומנהל מינהל תקשוב לחיבור הספק
  - תכנית עבודה לחיבור
- מענה משרד לבקשת הספק
- אפיון פתרון החיבור עם צוות מערכת הזדהות של המשרד: אופי היישום וטכנולוגיית היישום, אוכלוסיית משתמשים, היבטי תמיכה ותפעול
- הקמה:
  - הקמת חיבור מאובטח TRUST בין הספק החיצוני לספק הזהויות,המשרד (שימוש בתעודות והחלפת מפתחות)
  - חיבור מערכות הספק לתשתית ההזדהות של המשרד
  - בדיקות
  - אישור התשתית
  - תמיכה ותפעול שוטף: על הספק להעמיד איש קשר מטעמו לטיפול בבעיות גישה ליישומים שבאחריותו

תמיכה בסיסמאות

אין לי סיסמה !!
נתקלת בבעיה ?

תמיכה בסיסמאות

שרות עצמי לקבלה ואיפוס סיסמה באמצעות דוא"ל (שרות 7/24 מחייב כתובת דוא"ל עדכני במאגרי המשרד). בעתיד יורחב השרות גם לטלפון סלולרי שברשות המשתמש

תמיכה בסיסמאות

- ✓ מערכת ניהול סיסמאות בבית הספר – גישה למערכת היא באמצעות הזדהות חזקה והרשאה באחריות מנהל בית ספר
- ✓ קישור

תמיכה בסיסמאות

מוקד סיסמאות של המשרד

- ✓ שרות לעובדי הוראה, סגל מנהלי בית ספר,אחרים ונבחני בגרות
- ✓ המשרד פועל להרחבת שרתי התמיכה גם לתלמידים.
- ✓ השרות בהתאם לשעות הפעילות של המוקד

<u>מוקד סיסמאות של המשרד</u>

ימים א'-ה': שעות 8-16

טלפון: 03-9298888

זמינות מערכת ההזדהות של המשרד

- מאז הפעלת מערכת ההזדהות בשנת 2010 לא הייתה השבתת שרות
- מוקם DR בימים אלו .סיום דצמבר 2014
- למרות האמור לעיל המשרד מתחייב שבמידה ויהיה צורך בהורדת המערכת לצרכי תחזוקה הדבר יעשה בתאום עם הספקים

אוכלוסיות משתמשים שאינם קיימים במאגרי המשרד

- אישור על פי דרישה במסגרת אפיון הדרישות עם הספק
- קיים ערוץ להוספה של משתמשים

רשות או חובה

- להתחבר או לא להתחבר ?
- החיבור הוא רשות אבל בעתיד הקרוב יוגדר כחובה

תכנית עבודה לחיבור הספקים

שלב 1

- עדיפות לחיבור תינתן לספקי תוכן וספרים דיגיטליים שאושרו במכרז התוכן
  - סדר החיבור ייקבע על פי גודל הגוף (כמות משתמשים) ורמת הזמינות של הספק לביצוע החיבור
  - תואמו פגישות אל מול סנונית, מט"ח ועת הדעת
  - סיום חיבור עד ה 1.9.2015

שלב 2

- חיבור ספקי תוכן שלא אושרו

שלב 3

- חיבור יתר הספקים, לא רק מעולם התוכן

תפעול

- <u>תפעול</u>
  - תפעול מערכת ההזדהות באחריות המשרד
  - תפעול מערכות הספק באחריות הספק

גורמים מעורבים

שם	תפקיד	הערות
נעמי בוסטין	מנהל חטיבת תשתיות	
נועם קוריאט	מנהל תחום ארגון ופיתוח ניהול ידע	ניהול הקשר אל מול ספקי התוכן
יוסי עמיאל	מנהל פרויקט ניהול זהויות	ניהול פרויקט הזדהות אחידה yossiam@education.gov.il
אורנית יהושע, רונית מורגנשטרן, אוד פרץ	צוות מערכת הזדהות, משרד החינוך	
חברת EDP - דורון אלמליח, תומר עזרן	אינטגרטור של המוצר IDM במשרד החינוך	
שאול בן שושן	אבטחת מידע,משרד החינוך	
אביאור ניסים,זיו בר	צוות חממה, משרד החינוך	
קובי היין	תשתיות WEB משרד החינוך	