

# תקן WEB SERVICE לממשל זמין

גרסה 6.3

**מסמך זה כולל מידע השייך לממשל זמין, רשות התקשוב הממשלתי. כל חשיפה, שימוש או העתקה של מסמך זה או חלקים ממנו – ללא קבלת אישור בכתב ממנהל מערך סייבר ואבטחת מידע בממשל זמין – אסורה בהחלט. מסמך זה מיועד לעובדי ממשל זמין ולקוחותיו**

## מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1	19.3.2008	ישי כהן	מסמך מקור גרסת תוכנה 2.0.0
2	24.2.2011	ישי כהן	שינוי עם המעבר למשרד ראש הממשלה. מתן אפשרות לכותרת ללא מעבר לדף חדש.
3	10.4.2011		עדכון מסמך
4	1.2.2013		עדכון מסמך
5	17.6.2015		עדכון מלא של המסמך והעברה לתבנית חדשה של ממשל זמין.
6	2.9.2015	ישי כהן	עדכון מלא של המסמך + הוספת תמונות.
6.1	11.10.2015	אופיר יהב	החלפת השם ל-XML Firewall
6.2	12.10.2015	אופיר יהב	תיקון התרשים ותוספת לפרק כללי תיקון כל מילות הריפוש.
6.3	29.11.2015	יוני ארוך	שינוי לוגו והוספת נתוני גרסת המסמך

## נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	PMO	אופיר יהב	19.3.2008	(חתימה)
נבדקה ע"י	מוביל טכנולוגיות במערך סייבר ואבט"מ	אלעד פז	19.3.2008	(חתימה)
אושרה ע"י	מנהל מערך סייבר ואבט"מ	אברהם זרוק	19.3.2008	(חתימה)

## תוכן עניינים

4.....	כללי	.1
5.....	יעדי המסמך	.2
6.....	הסתייגויות	.3
7.....	שרטוט מבנה ה-Gateway	.4
8.....	תקן	.5
8.....	הגדרות ותיחום התקן	5.1
8.....	מקורות מידע	5.2
9.....	דוגמא למבנה מסר	5.3
12.....	גבול אחריות	5.4
12.....	מבנה מסר	5.5
14.....	אופן מימוש החתימה	5.6
15.....	הערות	5.7
16.....	דיאגנוסטיקה	.6
16.....	טכנולוגיית WSE - End of Life	.7
17.....	טכנולוגיית WCF	.8
18.....	בדיקות לביצוע טרם העברת אפליקציה לסביבת ייצור	.9
18.....	תאימות שעונים	.11
18.....	הרשאות	.13
19.....	רענון (Refresh) של שירותים	.15
19.....	נספחים	.14

## 1. כללי

בממשל זמין קיים שירות המאפשר פרסום שירותים (אפליקציות) על ידי המשרדים השונים. שירות זה הוא יצירת Gateway ממשלתי. ה-Gateway יאפשר למשרדים לפרסם שירותים משרדיים בין המשרדים לבין עצמם ובין האזרחים (internet) למשרדים. תקן ws.gov.il מבוסס על התקן העולמי ws-security המפרט כיצד ניתן לאבטח web services ע"י הזדהות ואימות המסרים העוברים בין השרת ללקוח. בעוד ותקן ws-security מאפשר מספר מנגנוני הזדהות, תקן ws.gov.il מאפשר הזדהות ע"י חתימה דיגיטלית בעזרת X.509 v3 certificate בלבד. במהותו תקן ws.gov.il מחייב כל צד (שרת ולקוח) לחתום דיגיטלית כל מסר יוצא, ולוודא (verify) כל מסר נכנס. בנוסף, לכל צד יש רשימה של ישויות המורשות לפנות אליו, כך שבתהליך הווידוי, בנוסף לוודא החתימה נבדק כי הפונה רשאי לפנות לצד זה. שירות זה יאפשר למשרד לשמור על מאגרי המידע ששייכים לו ונמצאים ברשותו בצורה מעודכנת ולהימנע מהפצה לא רצויה של מאגרי מידע. מסמך זה כתקן GOVIL, נועד ליצור שפה אחידה ותיאום ציפיות בין ממשל זמין ללקוחותיו. ממשל זמין שם לעצמו למטרה לאפשר ללקוחותיו, וכלל המשתמשים, שירותים מאובטחים ורציפים. מסמך זה כולל, בין היתר, הנחיות אבטחת מידע ודרישות טכניות הנגזרות מהן. רק הקפדה על הנחיות ודרישות אלו תיצור מעטפת הגנה מיטבית על השירותים ותשמור על רציפותם של השירותים.

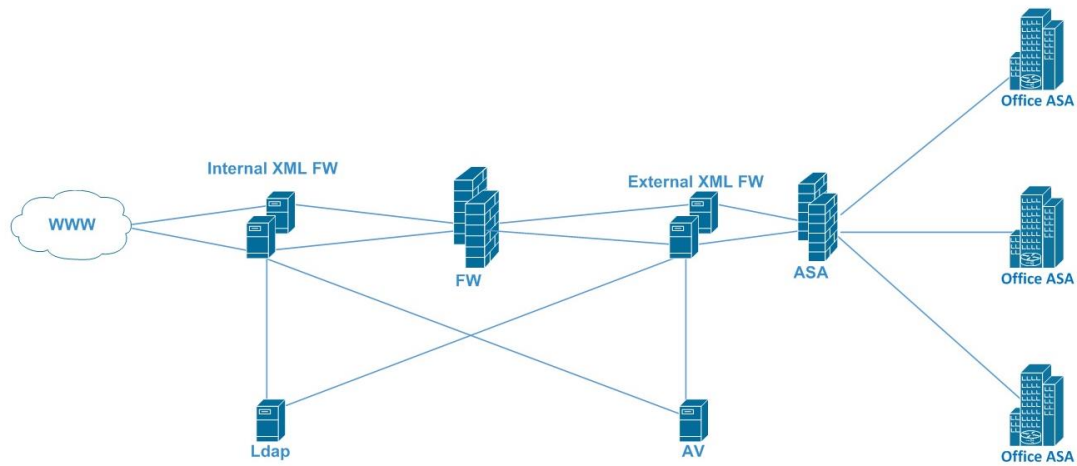
## 2. יעדי המסמך

- 2.1 מטרת המסמך היא לספק למשרדי הממשלה דרך וסטנדרט לספק שירותי מידע בין משרדי באופן שיאפשר קבלת מידע (שאליות ספציפיות) בין משרד למשרד או בין ממשל זמין למשרד.
- 2.2 שירות המידע יינתן ע"י מקור המידע וממקום אחד בלבד. האחריות על תקינות ועדכניות המידע היא על מקור המידע אשר בתחום סמכותו גם לקבוע מי הם הזכאים לקבלת שירותי מידע אלה.
- 2.3 אופי התקן יתבסס על הגדרת "Schema for the SOAP/1.1 envelope" מותאמת עבור שירותים אלה אשר כל שירות באשר הוא ממשלתי, יחויב לעמוד בה. אף על פי שהגדרות אלו מבוססות על SOAP 1.1, הגדרות אלו תקפות גם ל-SOAP 1.2.
- 2.4 ממשק המידע יסתמך על טכנולוגית ה-web service (ע"י מימוש ב-WCF) ובמבנה SOAP (מעטפת המסר בגרסאות 1.1 ו-1.2).
- 2.5 רק שירותי מידע אשר יעמוד בסטנדרטים אלה יפורסם בשרת הפורטל של ממשל זמין .

## 3. הסתייגויות

- 3.1 המסמך אינו מתיימר לספק דרך להעברת מאגרי מידע בין משרדים (חיתוכים).
- 3.2 המסמך אינו מגדיר את תקן ורמת השירות הבסיסית הנדרשת מספק השירות (SLA וכו').
- 3.3 המסמך מתייחס לפרוטוקול התקשורת TCP/IP . לא תתאפשר עבודה עם פרוטוקולי תקשורת אחרים.
- 3.4 המסמך מתייחס לסביבת Microsoft Windows כמערכת הפעלה ול MS IIS כשרת אפליקציה, אם כי ניתן לעבוד גם בסביבת לינוקס.

## 4. שרטוט מבנה ה-Gateway



- 4.1 כיוון זרימת המידע של השירותים שיתפרסמו לעולם, יהיה מהעולם לכיוון ממשל זמין ומשם למשרדי הממשלה. כך שצרכני השירותים יהיו מתשתית האינטרנט לכיוון ממשל זמין.
- 4.2 לא תתאפשר כיוון זרימת נתונים כך שתשתיות ממשל זמין יצרכו שירותים מהעולם. וכמובן, משרדי ממשלה לא יפנו ל Web service בעולם.
- 4.3 לצורך כך הוקמה תשתית שרידה של SOA בייצור ותשתית נפרדת לחלוטין לכלל שירותי הטסט הפיתוח וכו'.
- 4.4 אין עירבוב סביבות עבודה של ייצור בשום סביבה אחרת שאינה ייצור.
- 4.5 הדרישה מהלקוחות שלנו שגם להם תהיה סביבה נפרדת לייצור, כך שההפרדה בסביבות העבודה תהיה מלאה לכל אורך התשתית.
- 4.6 כל שירות חייב לשלוח מסרים חתומים אל ממשל זמין, וכל שירות חייב לקבל מסרים חתומים מממשל זמין.
- 4.7 ממשל זמין מהווה תוך מאובטח ואין רשות לשנות תוכן המסר.

## 5. תקן

### 5.1 הגדרות ותיחום התקן

- 5.1.1. הצעה לפורמט אחיד למבנה המסר שהינו בקשה למידע ותשובה לבקשה.
- 5.1.2. המסמך יתייחס לתקן SOAP על גבי תקשורת HTTP.
- 5.1.3. הצעה לסכמה מוסכמת שתהווה בסיס ותקינה לכל שירות WS.
- 5.1.4. התקן לא יגע ב- HTTP-Header אלא רק ב- Envelope Header שב- Message עצמו.
- 5.1.5. הצעה לפורמט מבנה המידע המוחזר מהשירות (מבנה טבלאי - רב נתונים, סקלארי - נתון חוזר בודד).
- 5.1.6. טיפול ב- Authorization + Authentication תקן וגבולות אחריות.
- 5.1.7. התקן יציע שמות ומבנה מאפיינים מוסכמים.

### 5.2 מקורות מידע

- 5.2.1. אינפורמציה נוספת על טכנולוגית WCF ניתן למצוא ב:
  - 1. <http://msdn.microsoft.com/en-us/netframework/aa663324>
  - 2. <http://msdn.microsoft.com/en-us/library/dd456779.aspx>
- 5.2.2. אינפורמציה נוספת עבור NET. ניתן למצוא ב:
  - 1. <http://www.microsoft.com/net/>
  - 2. <http://msdn.microsoft.com/net/>

## 5.3 דוגמא למבנה מסר

Envelope

```
<?xml version="1.0" encoding="utf-8" ?>  
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"  
  xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-  
  open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
```

הסטנדרטים הממומשים בהודעת ה-SOAP



Body

```
<soap:Body wsu:Id="Id-d2a3e783-6565-47e6-868b-02c494319a26">
  <isTipulBeRami xmlns="heterBniyaWcf">
    <oBakashaDetailsIn xmlns:a="http://schemas.datacontract.org/2004/07/HeterBniyaWcf">
      <a:mahutBakasha>1</a:mahutBakasha>
      <a:misBakasha>1</a:misBakasha>
      <a:nechesList>
        <a:Neches>
          <a:chelka i:nil="true"/>
          <a:gush i:nil="true"/>
          <a:messageDetailsList xmlns:b="http://schemas.datacontract.org/2004/07/HeterBniyaWcf">
            <a:misTik>52366532?</a:misTik>
            <a:semelYisuv i:nil="true"/>
            <a:tatChelka i:nil="true"/>
            <a:teudatZehut i:nil="true"/>
          </a:messageDetailsList>
        </a:Neches>
      </a:nechesList>
      <a:sugBakasha>1</a:sugBakasha>
    </oBakashaDetailsIn>
  </isTipulBeRami>
</soap:Body>
```

## 5.4 גבול אחריות

5.4.1. השירות יינתן מאתרו הפיזי של נותן השירות (מפרסם השירות) או כשירות מתארח בממשל זמין. נותן השירות יהיה אחראי לתקינות השירות ועדכונו. האחריות על הגנת ותחזוקת השירות הינה באחריות מקום האירוח של השירות. היה והשירות יתארח בממשל זמין, השירות יטופל באותה מתכונת של כל אתר מתארח אחר.

## 5.5 מבנה מסר

5.5.1. **המעטפה (envelop):** כל מסר ממשלתי בין אם הוא בקשה או תשובה לשירות יכיל את תוכן הבקשה ואת מעטפת הבקשה. מעטפה זו תכיל תוספות שחלקם חובה וחלקם רשות. המעטפה תציע תקן לזיהוי מאובטח חד ערכי של מבקש השירות וכן תקן לזיהוי ספק השירות ומאפייני השירות. תוכן המעטפה יכלול גם מידע על האובייקטים ותכונותיהם.

5.5.2. **ראשית (header):** כרגע, התשתית הקיימת בממשל זמין תומכת (במסגרת טכנולוגיות WCF) בסטנדרטים הבאים:

5.5.2.1 WS-Security

5.5.2.2 WS-Addressing

5.5.2.3 WS-Security : SOAP Message Security

5.5.2.4 WS-Security : X.509 Certificate Token Profile

**לגבי שימוש בפרוטוקולים אחרים ו/או אובייקטים ו/או תכונה אחרת יש לברר עם צוותי SOA ואבט"מ של ממשל זמין.**

**הערה חשובה:** אין להעביר שדות תוכן ב header.

אין בדיקת schema validation על ה header (רק על ה-body).

5.5.3. **תוכן (body):** תוכן ההודעה יכיל את הפרמטרים שעוברים אל השירות ובחזרה. כל הפרמטרים צריכים להיות מוגדרים בסכמה של השירות, אשר מגדירה את אורך והתוכן של אותה הפרמטר.

5.5.4. אין לשלוח בבקשה (request) סכימת XML או HTML כאובייקט בתוך ה body.

5.5.5. אין להחזיר בתשובה (response) סכימת XML או HTML כאובייקט בתוך ה-body.

5.5.6. יש להקשיח את הסכמה לפי נספחי תקן WS-gov.il ולהעביר לבדיקות צוות אבטחת המידע של ממשל זמין. רק שירות שיעבור בהצלחה בבדיקות אבט"מ יאושרו לפירסום בתשתיות הטסט \ ייצור של ממשל זמין.

הערות והסברים	חובה	תקן	תכונה	אובייקט
תקן ה-soap	כן	http://schemas.xmlsoap.org/soap/envelope/	xmlns:soap	soap:Envelope
תקן ה-xml	כן	http://www.w3.org/2001/XMLSchema-instance	xmlns:xsi	
תקן ה-addressing	כן	http://schemas.xmlsoap.org/ws/2004/03/addressing	xmlns:wsa	
סכימת security	כן	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	xmlns:wsse	
סכימת security-utility	כן	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	xmlns:wsu	
ה-header של מעטפת ה-soap	כן			soap:Header
שם הפעולה (המסר)	כן		ws-addressing	wsa:Action
מס' ייחודי להודעה	כן		ws-addressing	wsa:MessageID
namespace לתשובה	בבקשה		ws-addressing	wsa:ReplyTo
לאיזה messageID התשובה מיועדת	בתשובה			wsa:RelatesTo
ה-endpoint של הבקשה	כן		ws-addressing	wsa:To

אובייקט	תכונה	תקן	חובה	הערות והסברים
	wsse:Security	ws-security	כן	תוספת security header ל
	wsu:Timestamp	ws-security	כן	חובה גם תאריך יצירה וגם תאריך פקיעת ההודעה
	Signature	ws-security - ממומש בסטנדרט: http://www.w3.org/2000/09/xmldsig עם X509v3 לפי: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3	כן	חובה לשלוח Public cert של החותם (לפי הסטנדרט). תמיכה רק ב-X509v3
soap:Body			כן	תוכן ההודעה

## 5.6 אופן מימוש החתימה

5.6.1 המינימום הנדרש על מנת לעבוד עם רשת ה-gateway הממשלתי מגדיר כי כל מסר (הן בקשה והן תשובה) שעובר דרך ה-gateway הממשלתי יהיה חתום על ידי צוות PKI של ממשל זמין (נספח ג' – סרטיפיקטים).

5.6.2 החתימה בכל הודעה תהיה לפחות על החלקים הבאים במסר:

1. ה-body של מעטפת ה-soap - wsp:Body()
2. ה-To של פרוטוקול ws-addressing (נמצא ב-header) - wsp:Header(wsa:To)
3. ה-Action של פרוטוקול ws-addressing (נמצא ב-header) - wsp:Header(wsa:Action)
4. ה-MessageID של פרוטוקול ws-addressing (נמצא ב-header) - wsp:Header(wsa:MessageID)
5. ה-Timestamp של ההודעה, מתוך פרוטוקול ws-security (נמצא ב-security שבתוך ה-header) - wse:Timestamp()

5.6.3 על מנת ליצור שפה משותפת וכדי למנוע בלבולים כל משרד החושף web service יחשוף את צורת העבודה איתו באמצעות קובץ web config.

- 5.6.4. המשרד יעביר את קבצי WSDL ו XSDs לממשל זמין כולל איפיון השירות ובאחריותו לעמוד בתנאים אותם המסמך מפרט. ממשל זמין יערוך בדיקות על הקבצים הנ"ל ויאשר או לא יאשר אותם לעלייה לייצור.
- 5.6.5. לאחר אישור אבט"מ למוכנות השירות לעלייה לאויר, אין לערוך שינויים בקבצים הנ"ל ללא ידיעה ואישור של צוותי אבט"מ ו SOA.

## 5.7 הערות

- 5.7.1. כל חריגה מדרישות המינימום דורשת אישור של צוות צומת השירותים.
- 5.7.2. הדרישה הנ"ל היא למעשה ברירת המחדל של חתימה/אימות בעבודה עם קובץ web config.
- 5.7.3. השירותים בממשל זמין עובדים בצורה סינכרונית.
- 5.7.4. התקשורת בין ממשל זמין את משרדי הממשלה יהיו בפורטים 80 ו 443 בלבד.
- 5.7.5. גודל המסר המקסימלי המאושר הינו 4MB אלא אם הוגדר אחרת ע"י צוות צומת השירותים.
- 5.7.6. כל הצרופות שישולבו בתוכן של המסר, צריכות לעבור בדיקה של AntiVirus.
- 5.7.7. עבור כל הודעה, יוגדר TimeOut של 120 שניות, שאחריו ההודעה תיכשל.
- 5.7.8. זיהוי הסרטיפיקט יתבצע מול המפתח הציבורי של ה CA ובמקרים מיוחדים מול המפתח הציבורי של הסרטיפיקט של המשרד נותן השירות.

## 6. דיאגנוסטיקה

6.1 WCF תומכות ביכולות דיאגנוסטיקה (Diagnostic) שונות, אשר יכולות לעזור למפתח לנתח ולהבין את הגורם לשגיאות אפליקציות שרצות. באופן כללי היכולות מבוססות על היכולת לעקוב אחרי הודעות ה-SOAP ולנתח נתונים שונים בזמן שגיאות.

## 7. טכנולוגיית WSE - End of Life

- 7.1 שירותי Web Services Enhancements (WSE) הגיעו לסיומ מחזור החיים שלהם ואינם נתמכים עוד במיקרוסופט End of Life.
- 7.2 ממשל זמין מנחה להאיץ את תהליכי ההסבה של שירותים אלה לשירותים עדכניים מסוג Windows Communication Foundation (WCF). לתשתית ה-WCF יתרונות רבים, ביניהם: אמינות וגמישות, מהירות תגובה וניצול משאבים טוב יותר ביחס לתשתית ה-WSE.
- 7.3 ממשל זמין ימשיך לספק תמיכה בשירותי ה-WSE עד 31 ליולי 2016.
- 7.4 שירותים שלא יוסבו עד לתאריך זה, לא ייתמכו ע"י ממשל זמין ולא יטופלו תקלות הקשורות בשירותים אלה.
- 7.5 שירותים שלא יוסבו ל WCF, יעבדו כל עוד הם עובדים עד 31 ליולי 2017.
- 7.6 בתאריך 1 באוגוסט 2017 שירותי ה-WSE ייצאו משימוש בממשל זמין.

## 8. טכנולוגיית WCF

- 8.1 טכנולוגיית WCF הינה עשירה יותר ביכולות הדיאגנוסטיקה שלה ומביאה איתה יכולות נוספות כגון:
- 8.1.1 יכולות Trace מתקדמות המאפשרות ניתוח ללא שימוש ב-debugger.
  - 8.1.2 ניתוח הודעות לפני ואחרי שליחה.
  - 8.1.3 יכולות כתיבה ל-Event Log.
  - 8.1.4 שעוני ביצועים שונים.
- 8.2 מידע נוסף לגבי הפעלת יכולות דיאגנוסטיקה ניתן לקרוא בנספח ב' – מצגת בנושא WCF – הגדרות לעמידה בתקן WS-gov.il.
- 8.3 למידע נוסף לגבי היכולות השונות של מנגנון הדיאגנוסטיקה ניתן לקרוא באתר MSDN - <http://msdn.microsoft.com/en-us/library/ms731055.aspx>
- 8.4 יש לציין, כי בטכנולוגיית WCF בלבד ניתן לבצע הקשחות אבטחת המידע המתוארות בנספח א' על ידי שימוש ב-DLL הקשחות של ממשל זמין אותו ניתן לקבל על פי דרישה, ובו ניתן להשתמש בכדי לבצע את ההקשחות ברמת קוד השירות.
- 8.5 לחילופין, ניתן לבצע ה"קשחות ידניות" שלא באמצעות ה-DLL הנ"ל ואז הקבצים יוטענו לוקאלית במכונת ה-XML Firewall. רענונים (Refresh) משמעותם, תיקון הקבצים לוקאלית.

---

## 9. בדיקות לביצוע טרם העברת אפליקציה לסביבת ייצור

- 9.1. טרם העברת אפליקציה מסביבת פיתוח לסביבת ייצור יש לבצע בדיקות שונות כדי להימנע משגיאות אשר קשורות להגדרת הסביבה ולא בגלל שגיאות באפליקציה עצמה. לאור ניסיון העבר בעבודה מול פרויקטים רבים, נציין מספר בדיקות שיכלו למנוע פעמים רבות עיכוב בעלייה לאוויר.
- 9.2. לפני עלייה לייצור, אישור לקוח שכל הפונקציות המוכלות בשירות נבדקו כהלכה.
- 9.3. אישור אבט"מ לגבי תקינות ההגדרות, כאמור.

---

## 11. תאימות שעונים

- 11.1. נדרש לבצע התאמה בין השעונים של המכונה עליה רץ ה-client והמכונה עליה רץ ה-web service. במידה והשעונים אינם מסונכרנים ניתן להגדיר הפרשי זמן מקובלים מתוך ה-configuration tool בלשונית של security בשדה Time Tolerance In Seconds.
- 11.2. מומלץ ללקוחותינו לחבר את השרתים הפונים לתשתית SOA לשרת NTP.

---

## 13. הרשאות

- 12.1. יש לוודא הרשאות קריאה RO של המשתמש ב-application pool עבור ה-process שמשתמש ב-WCF על ה-private key של המכונה שנמצא בספרייה:  
C:\Documents and Settings\all users\application data\microsoft\crypto\rsa\machine keys  
פעולה זו יש לבצע עבור ה-client ובנוסף עבור web service.

---

## 15. רענון (Refresh) של שירותים

- 13.1. דינו של ריענון (Refresh) שירות כמוהו כדין שירות ששונה בהגדרותיו.
- 13.2. לפיכך, לפני כל בקשת ריענון נבקש לקבל הסברים לגבי מהות השינוי.

---

## 14. נספחים

- 14.1. כפי שהוגדר בסעיפים הקודמים, מסמך זה מרכז הנחיות כלליות לעמידה בתקן WS-gov.il. הסעיפים למטה מפרטים את הנספחים הטכנאים אשר מגדירים במדויק את ההגדרות השונות אשר נדרש להגדיר בכדי לעמוד בתקן בטכנולוגיות השונות.
- 14.2. הנספחים אשר משלימים תקן זה הינם:
  - 14.2.1. נספח א' – הקשחת סכמות וסוגי נתונים.
  - 14.2.2. נספח ב' – מצגת בנושא WCF – הגדרות לעמידה בתקן WS-gov.il.
  - 14.2.3. נספח ג' – סרטיפיקטים.