

שליבים לחישוב Hash מסוג SHA-512

מסמך זה מיועד ללקוחות מס"ב המשתמשים באתר התשלומים לצורך שידור קבצים למס"ב ומעוניינים לוודא התאמה בין הקובץ שיצרו לקובץ שהתקבל במס"ב.
לצורך כך, על הלקוח לחשב את ה- Hash של הקובץ שיצר ולהשוותו לערך ה Hash המוצג באתר התשלומים.
ערך ה Hash המוצג באתר הינו חלקי, העתקת ערך ה Hash מאתר התשלומים והדבקתו במקום אחר, תאפשר להציג את הערך המלא לצורך השוואתו.

להלן הסבר לחישוב ערך ה Hash המופיע באתר התשלומים של מס"ב :

1. הכנת ה Salt עבור ה Hash

יש לשרשר את ערכי השדות הבאים לפי הסדר בו הם מופיעים בטבלה :

מס' סידורי	שדה	אורך
1	מוסד/נושא	8
2	מספר התנועות	7
	סה"כ	15

רשומה באורך 15.

2. הכנת הנתונים ליצירת ה Hash

יש לשרשר את ערכי השדות הבאים לפי הסדר בו הם מופיעים בטבלה :

מס' סידורי	שדה	אורך
1	מוסד/נושא	8
2	קוד בנק	2
3	מספר סניף	3
4	מספר חשבון	9
5	סכום לתשלום	13
6	סוג תנועה	3
	סה"כ	38

כל רשומה בשורה אחת, באורך 38 ומשורשרת לשורה הבאה.

3. חישוב Hash עם ה Salt :

$\text{Hash} = \text{SHA512}(\text{salt}) + 2 \text{ סעיף}$

[illegible]

1. חישוב שדות בסעיף 1 ליצירת Salt :

78363306	מוסד/נושא :	1
0000002	מספר התנועות :	2

שדות לחישוב : 783633060000002

2. חישוב שדות בסעיף 2 ליצירת Hash :

#	שם שדה	רשומה 1	רשומה 2
1	מוסד/נושא :	78363306	78363306
2	קוד בנק :	12	10
3	מספר סניף :	778	001
4	מספר חשבון :	000474720	000219916
5	סכום לתשלום :	0000000005000	00000000020000
6	סוג תנועה :	006	006

שדות לחישוב :

7836330612778000474720000000000500000678363306100010002199160000000020000006

3. חישוב Hash :

סעיף 1 (Salt)	סעיף 2
7836330600000002	7836330612778000474720000000000500000678363306100010002199160000000020000006

$$\text{Hash} = \text{SHA512} ((\text{Salt})^1 + 2^{\text{סעיף}})$$

4. תוצאת חישוב ה Hash :

6966936CF3714C074ED9E1CFCB5D1DC8B752DA014C485FA3BF49D9359AA779AA596F
221601817626A6FE1F245CEE4BE6C82D8A5EE050475206D2719EA8DC5D78