

DAL Extended Storage Mechanism

לDAL יש מגבלת זיכרון שמירה (flash), אשר מגבילה את המשתמש. אנחנו מציעים קוד ופרוטוקול עבודה אשר מתגברים על המגבלה הזו ומשתמשים בזיכרון הלא נדיף החיצוני הנגיש למערכת ההפעלה לצורך קבלת גישה לזיכרון שפחות מוגבל.

אברהם פרנקל ודויד וייס

| מערכות להרצת קוד בסביבה בטוחה – 156353.2.5780 |

15/3/2020

תוכן

[מבוא 2](#_Toc35291950)

[רקע 2](#_Toc35291951)

[תיאור הבעיה 2](#_Toc35291952)

[המטרה שלנו 2](#_Toc35291953)

[צורת החשיבה 2](#_Toc35291954)

[דרישות 2](#_Toc35291955)

[אילוצים 2](#_Toc35291956)

[אפיון 3](#_Toc35291957)

[פיצ'רים 3](#_Toc35291958)

[Applet 3](#_Toc35291959)

[Host 3](#_Toc35291960)

[תרשימים 3](#_Toc35291961)

[4](#_Toc35291962)

# מבוא

## רקע

לאינטל יש פתרון חומרתי להרצת קוד בסביבה בטוחה הנקרא Intel® Dynamic Application Loader הפתרון של אינטל משמש להרצת תהליכים בצורה מבודדת ומוגנת. אחד הפיצ'רים של DAL הוא אחסון מידע בזיכרון לא נדיף - FLASH בצורה מאובטחת.

## תיאור הבעיה

בDAL עצמו יש זיכרון מאוד מוגבל של 256B.

## המטרה שלנו

לספק פתרון אשר יאפשר למפתחי applets DAL "ספריה" שמאפשרת לשמור ולקרוא קבצים שחורגים מהמגבלה של B256.

## צורת החשיבה

נשתמש בזיכרון של DAL לשמירת מפתח הצפנה אחד בלבד, ובעזרת ה-HOST נוכל לשמור קבצים אל הזיכרון החיצוני כשההצפנה והחתימה עצמה נעשית באופן מאובטח בתוך DAL, וכן בקריאת קובץ ההצפנה והאימות נעשים ב-DAL.

תהליך זה לא מובנה במערכת הDAL, קשה לממש אותו (וקל לטעות ולממש אותו בצורה טובה שלא תיצור בעיות אבטחה או שימושיות)

### דרישות

* לספק פתרון אשר יאפשר למפתחי applets DAL "ספריה" שמאפשרת לשמור ולקרוא קבצים שחורגים מהמגבלה של B256.
* ספריה זו תספק שמירה על סודיות (Confidentiality) הקבצים (ע"י Root Of Trust המשתמש בפתרונות של אינטל)
* Authentication – בקריאת קובץ – הבטחה שהקובץ לא השתנה מאז שנשמר.
* מינימום כאב ראש למתכנת (ללא הצורך בניהול מפתחות, תקשורת עם הHOST, ואחסון).

### אילוצים

* אין לנו אפשרות ליזום שיחה מDAL. (אין לDAL גישה לממשק צדדי אחר, למשל מבוסס רשת, רק שליחת תשובה לבקשה של ה-HOST).
* ברגע שאנחנו מחזירים ערך מהDAL – כלומר מסיימים סשן כל המשתנים למעט אלו שבפלאש – נמחקים.
* בעקבות אלו הDAL לא יכול לבקש בזמן ריצה מידע נוסף מעבר למה שנשלח בעת הבקשה הראשונית אליו.

# אפיון

## פיצ'רים

### Applet

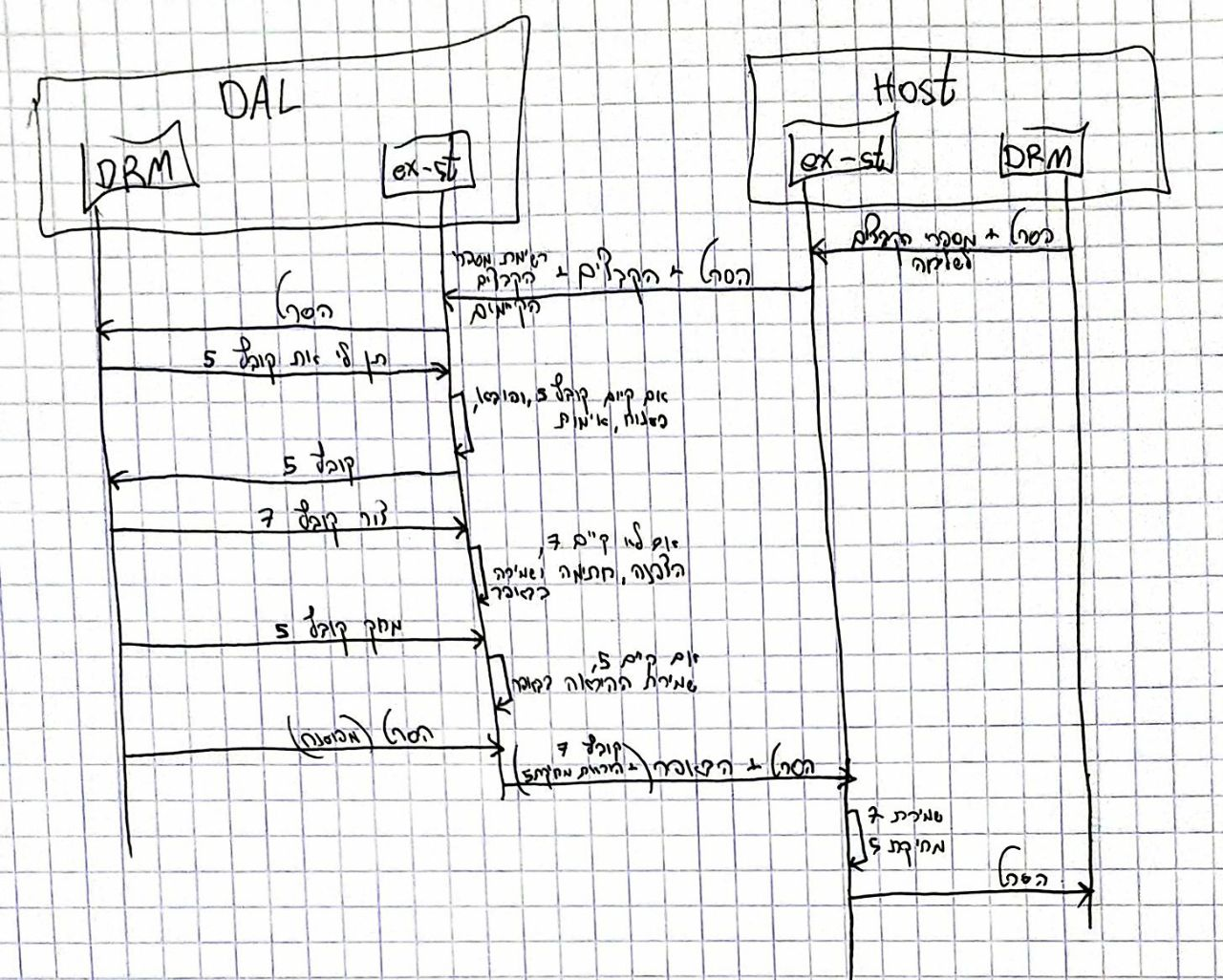
* בתחילת SendAndRecv - חילוץ המידע שנשלח מה-HOST על הקבצים, בצורה שקופה למשתמש (שחזור הבאפר המקורי של המשתמש)
* טיפול בבקשת כתיבת קובץ (מאחורי הקלעים – הצפנה וחתימה).
* טיפול בבקשת קריאת קובץ (מאחורי הקלעים – פענוח ואימות החתימה).
* טיפול בבקשת מחיקת קובץ.
* בסוף SendAndRecv - ליידע את הHost בנוגע לקבצים שמצריכים שינוי (ע"י הכנסת המידע על הקבצים אל הבאפר).

### Host

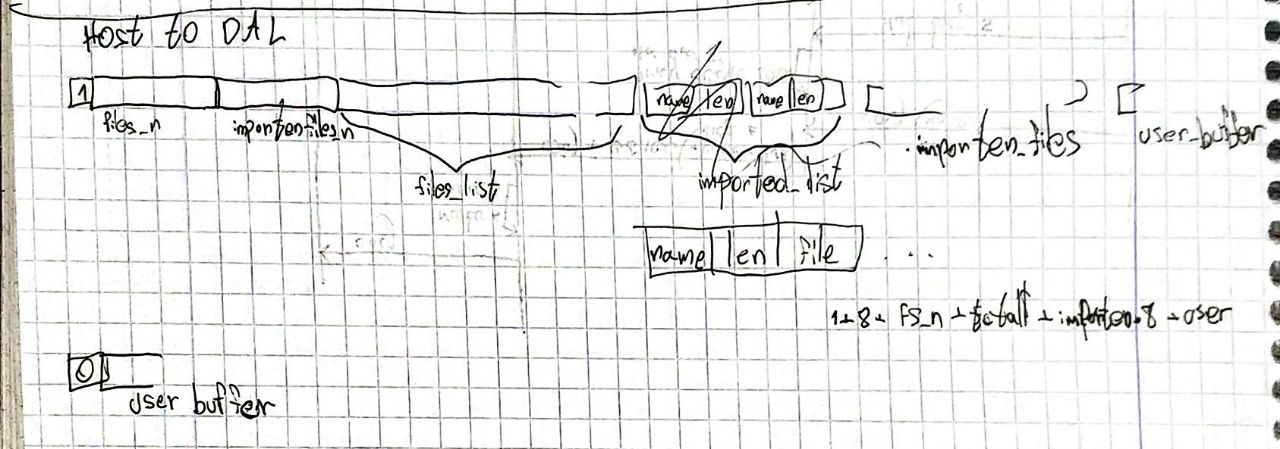
* בתחילת SendAndRecv – שליחת רשימת הקבצים הקיימים והקבצים שיהיו ניתנים לקריאה – הקבצים שייטענו בקריאה זו (ע"י הכנסת מידע זה אל הבאפר).
* בסוף SendAndRecv - קבלת רשימת קבצים למחיקה/יצירה וביצוע הפעולות המתאימות.

## תרשימים

תרשים לפעולה טיפוסית:



תיאור פרוטוקול התקשורת מצד ה-HOST:



תיאור פרוטוקול התקשורת מצד ה-DAL:

## 