

A browser-based digital signing solution over the web

Fotis Loukos
Charalampos Tsipizidis
Dimitris Daskopoulos

Contents

The problem

Proposed solution

- Architecture
- Native Messaging Host
- Native Messaging App
(browser plugin)

UX and Use cases

Conclusion

The need

Goal:

- High assurance digital identity in applications
- Non-repudiation of actions/documents



Means:

- Digital signatures on crypto devices (tokens)



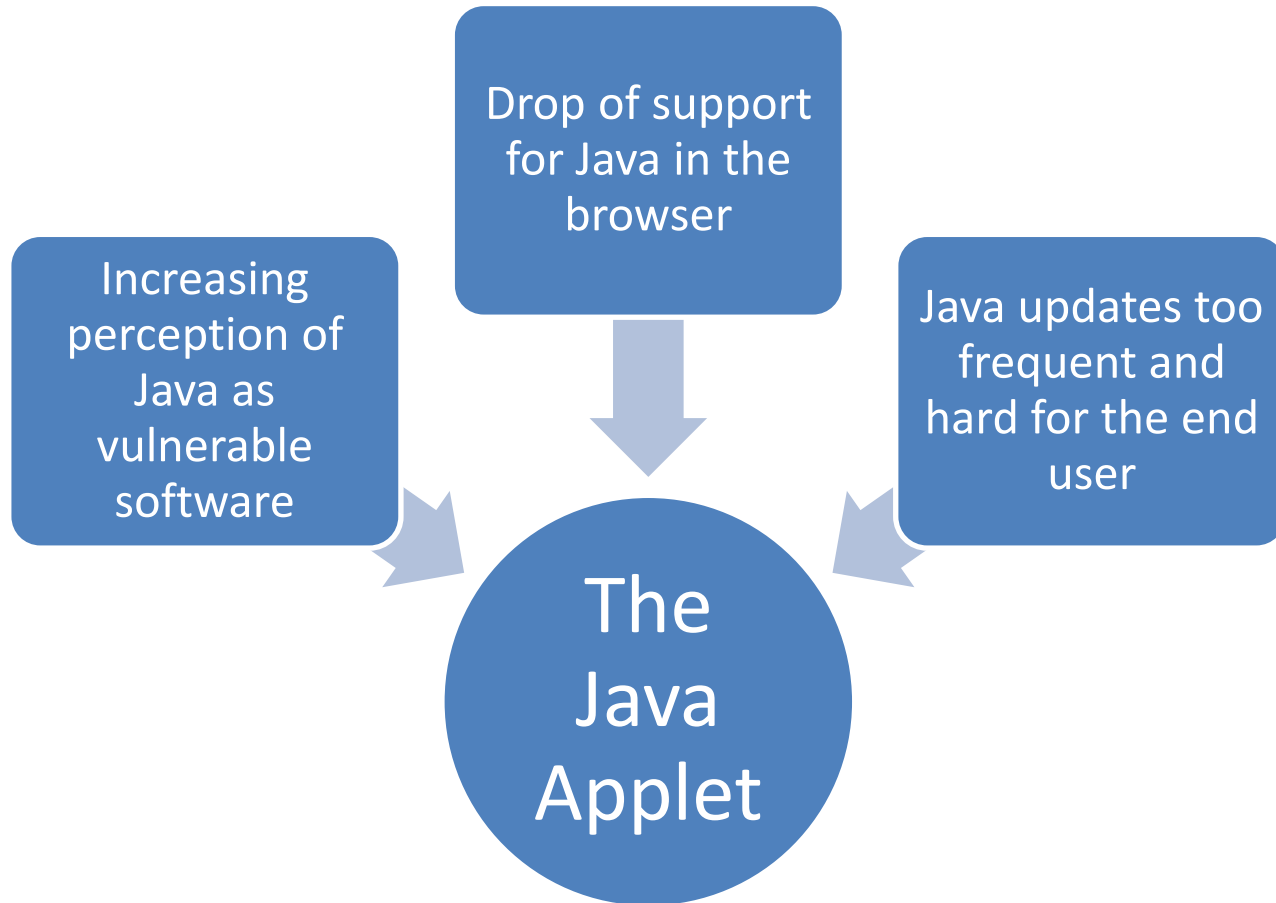
Requirements:

- Seamless digital signing on the web
- Ease of use, rapid installation, minimal maintenance

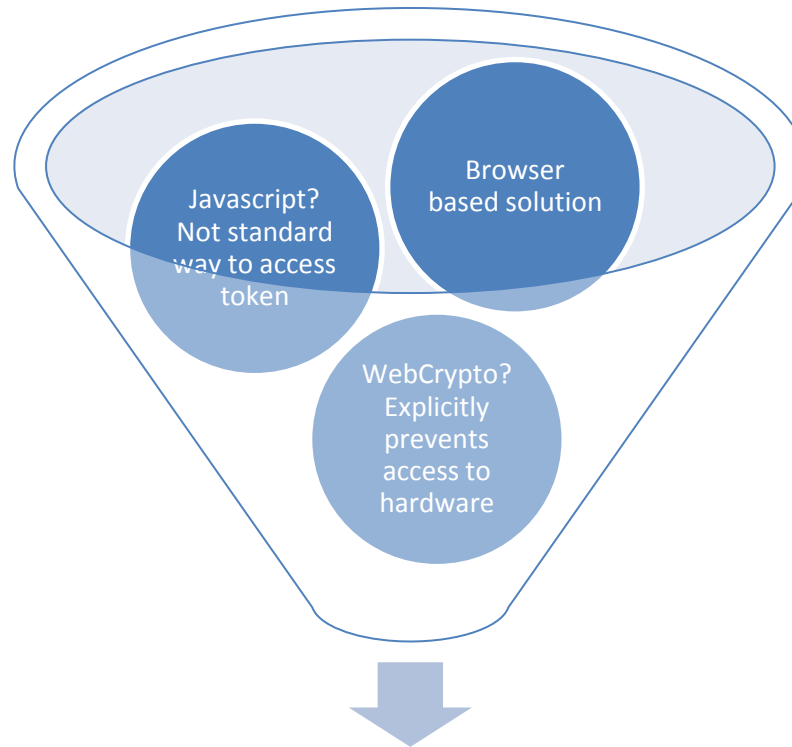
Legacy solution



The problem with legacy solutions

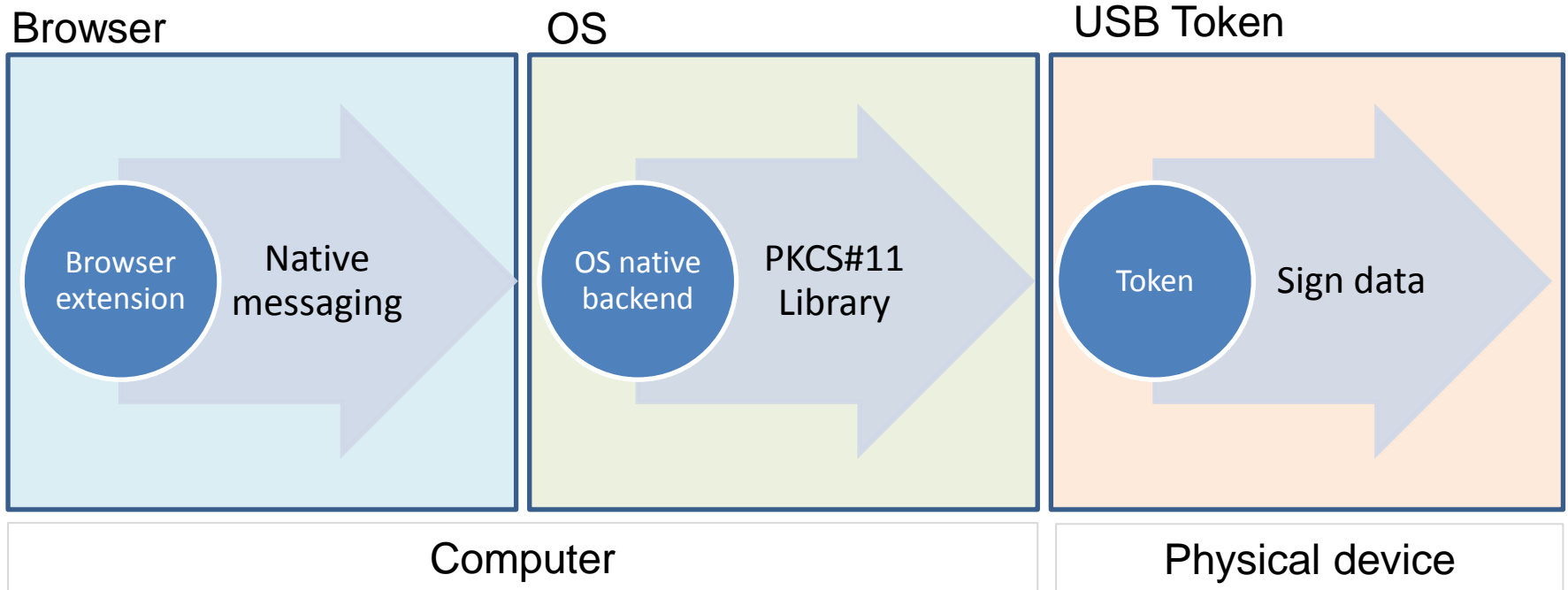


Proposed solution



Browser extension with native components!

Architecture



Browser extension

WebExtensions API

- Currently runs on Google Chrome, Chromium and Opera
- Will be supported at Firefox and Edge

Responsible for launching OS native component

- Acts as a Native Messaging Host
- Launches the OS native component
- It can supply it with either local files or data from the web server

OS native component

Written in python

- Portability (Windows, Linux, MacOSX)!
- Uses the PyKCS11 library

Responsible for signing

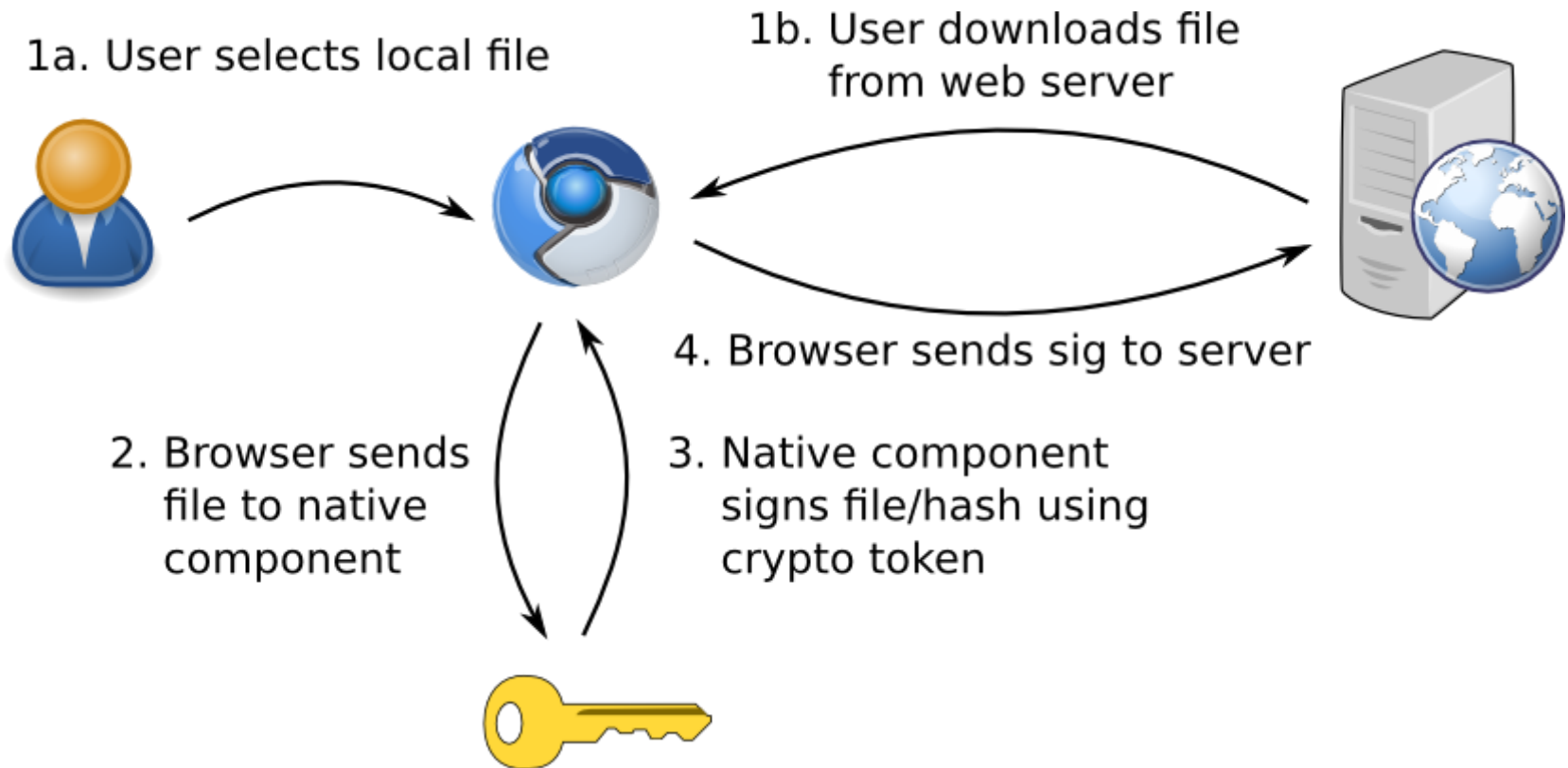
- It receives a JSON formatted message from the web extension with the text to be signed
- The component can either sign the text or its checksum (md5/sha1/sha2 supported)
- It supports multiple encodings for input message and signature

OS native component

Sample message

- {
 “message”: “Hello world!”,
 “srcenc”: “plain”,
 “dstenc”: “base64”,
 “hash”: “sha256”,
 “includecert”: 1
}

Workflow



Installation experience

Installer for native app backend

- Also includes drivers for the AcademicID, an ID given to all Greek members of the academic community

Plugin auto-installed on the browser when first visiting app page

User experience (1) - prepare

sis.auth | Υπηρεσίες Ηλεκτρονικής Γραμματείας ΑΠΘ Αρχική Εξετάσεις Υποστήριξη testfaculty

Αρχική » Εξετάσεις

Ανοιχτές εξετάσεις

Βήμα 1 / 2 : Έλεγχος βαθμολόγιου

✔ Ο έλεγχος εγκυρότητας των δεδομένων της εξέτασης του μαθήματος ολοκληρώθηκε με επιτυχία.

Μάθημα: Δοκιμαστικό Μάθημα 4
 Ακαδ. Έτος: 2015 - 2016
 Εξεταστική περίοδος: ΦΕΒΡ
 Ημ/νία υποβολής: 19-02-2016 15:47:21

Έλεγχος βαθμολόγιου

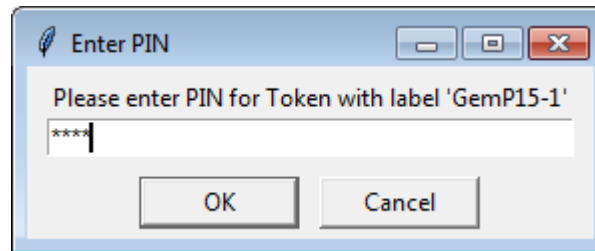
Όνομα φοιτητή	Βαθμός	Μήνυμα βαθμολόγησης
600000334	10	Ένας βαθμός υπάρχει ήδη και θα αντικατασταθεί.

Σύνολο βαθμών που θα ενημερωθούν: 1
 Προσοχή! Υποβολή κενών βαθμών δεν επηρεάζει προηγούμενο βαθμό φοιτητή.

Αν συμφωνείτε με τις παραπάνω ενέργειες, προχωρήστε στην **αποθήκευση και υπογραφή** του βαθμολογίου. Διαφορετικά, ακυρώστε τη διαδικασία και επαναλάβετε με νέο βαθμολόγιο.

Ακύρωση **Αποθήκευση & Υπογραφή**

User experience (2) – unlock crypto device



User experience (3) - signed

sis.auth | Υπηρεσίες Ηλεκτρονικής Γραμματείας ΑΠΘ Αρχική Εξετάσεις Υποστήριξη

Αρχική » Εξετάσεις

Τρέχουσες εξετάσεις

Βήμα 2 / 2 : Παραλαβή αποδεικτικού

- ✓ Το βαθμολόγιο αποθηκεύτηκε με επιτυχία.
- ✓ Η διαδικασία υπογραφής ολοκληρώθηκε με επιτυχία.

Μάθημα: Διακριτική και Εφαρμοσμένη Λογική
 Ακαδ. Έτος: 2015 - 2016
 Εξεταστική περίοδος: ΣΕΠΤ
 Ημ/νία υπογραφής: 08/02/2016 15:22:08

Αποτελέσματα Βαθμολόγησης

Όνομα φοιτητή	Βαθμός	Μήνυμα βαθμολόγησης
Διακριτική	9	Ο βαθμός του φοιτητή αποθηκεύτηκε με επιτυχία.

Σύνολο βαθμών που ενημερώθηκαν: 1

Μοναδικός αριθμός ελέγχου αποστολής: Stj4QMNC9X2ANorzBQWYw1/IgnQ=

Εκτύπωση αποδεικτικού βαθμολόγησης

Επιστροφή

Where is it used?

Already in production at AUTH

- Signed course grading data in Student Information System (custom)
- Future work for document signing in document management system (Alfresco)

Interested? Contact us!

Conclusion

The benefits of a method to securely sign using a hardware token

- The future on the web will certainly include digital signing. In a more standardized way.
- But this is a working solution, today.
- Sign actions (signed data stored on server)
- Sign documents (signed docs submitted to services)

Questions

