

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

Lack of
standardized
interface
between
browser and
token

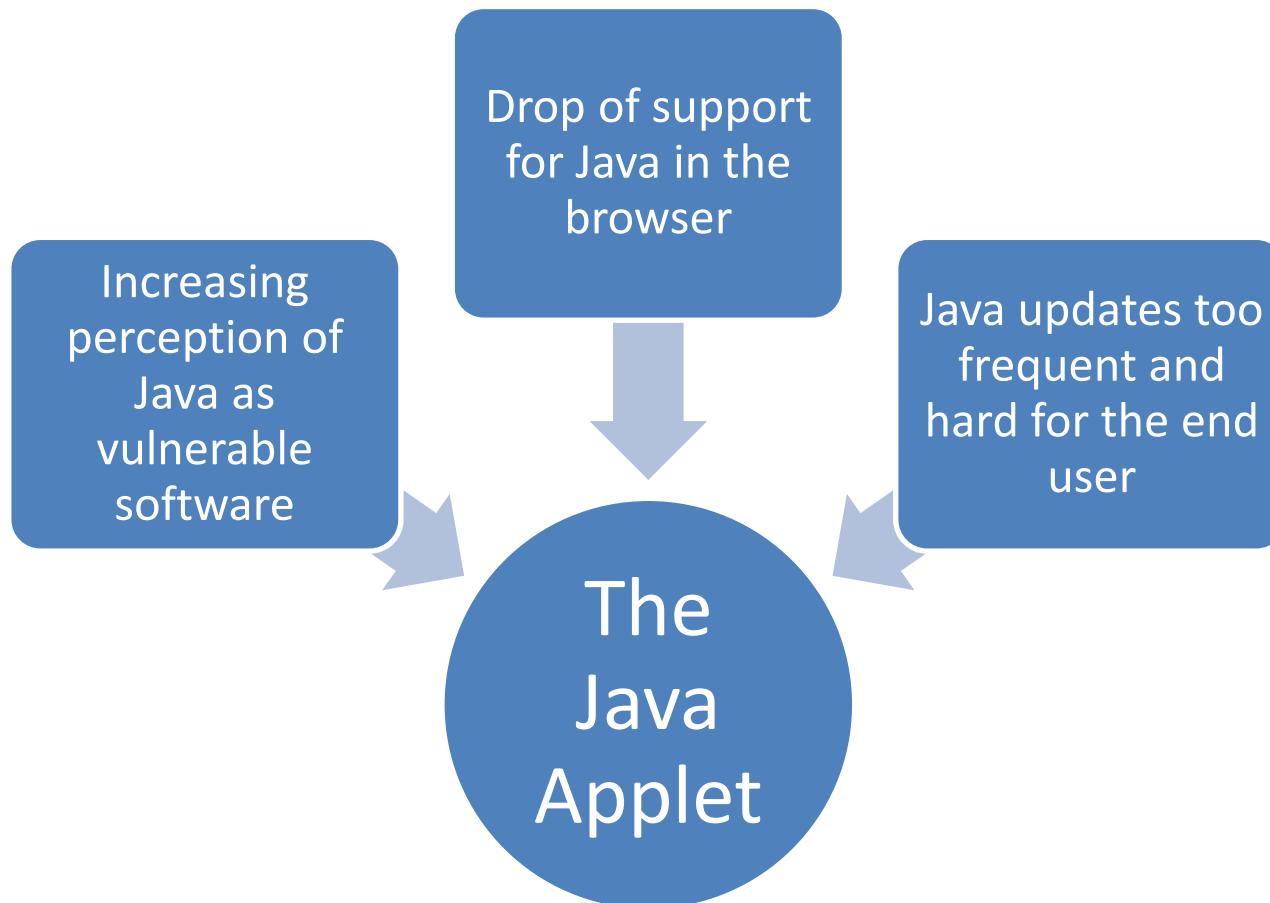


Java applet the
only method to
access token

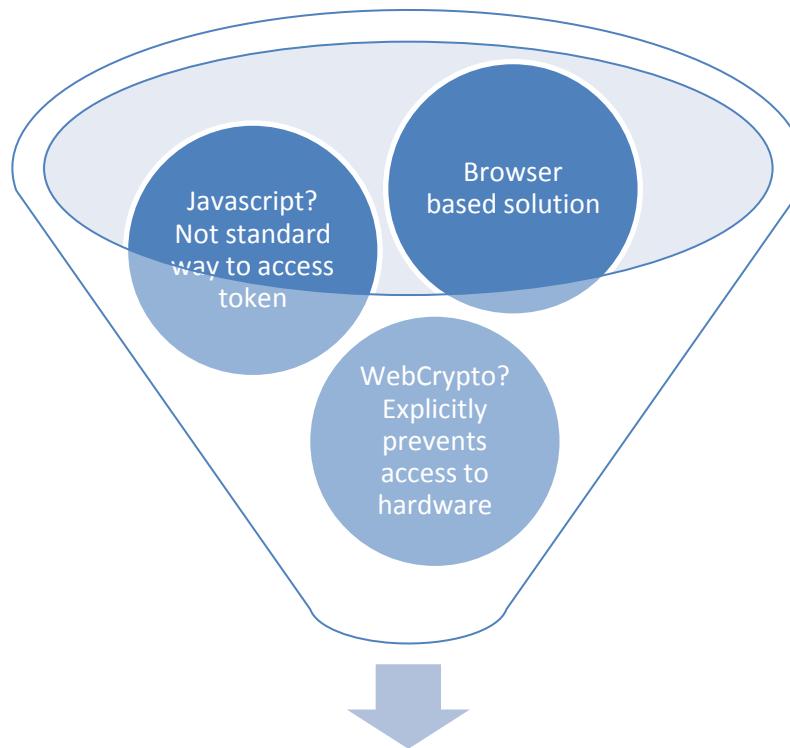


Creation of a
Java Applet that
will sign
anything

The problem with legacy solutions



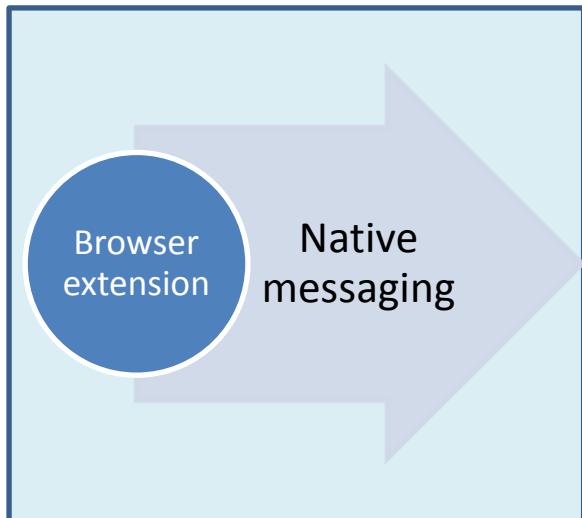
Proposed solution



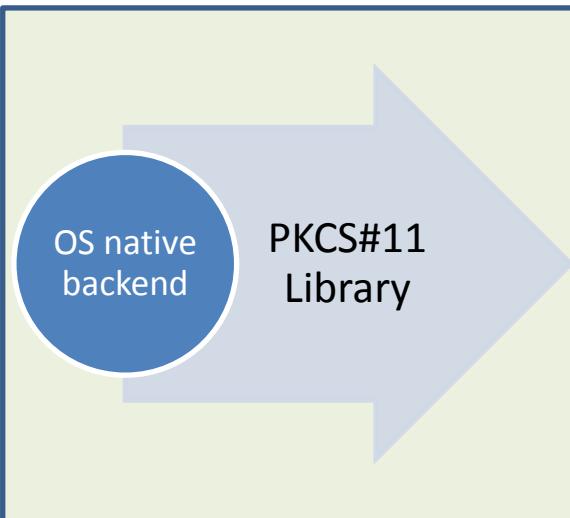
Browser extension with native
components!

Architecture

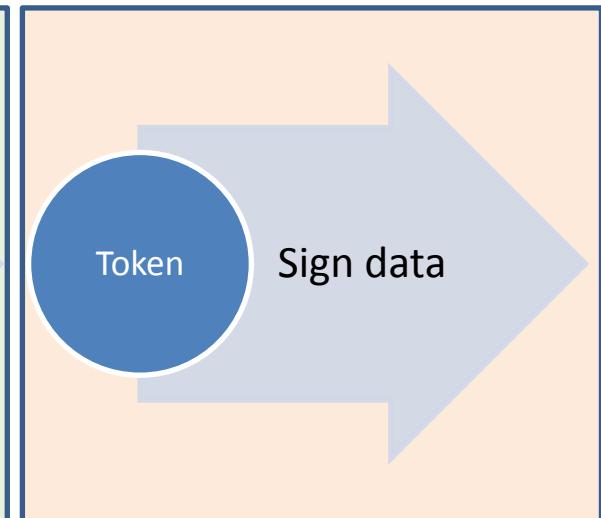
Browser



OS



USB Token



Computer

Physical device

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

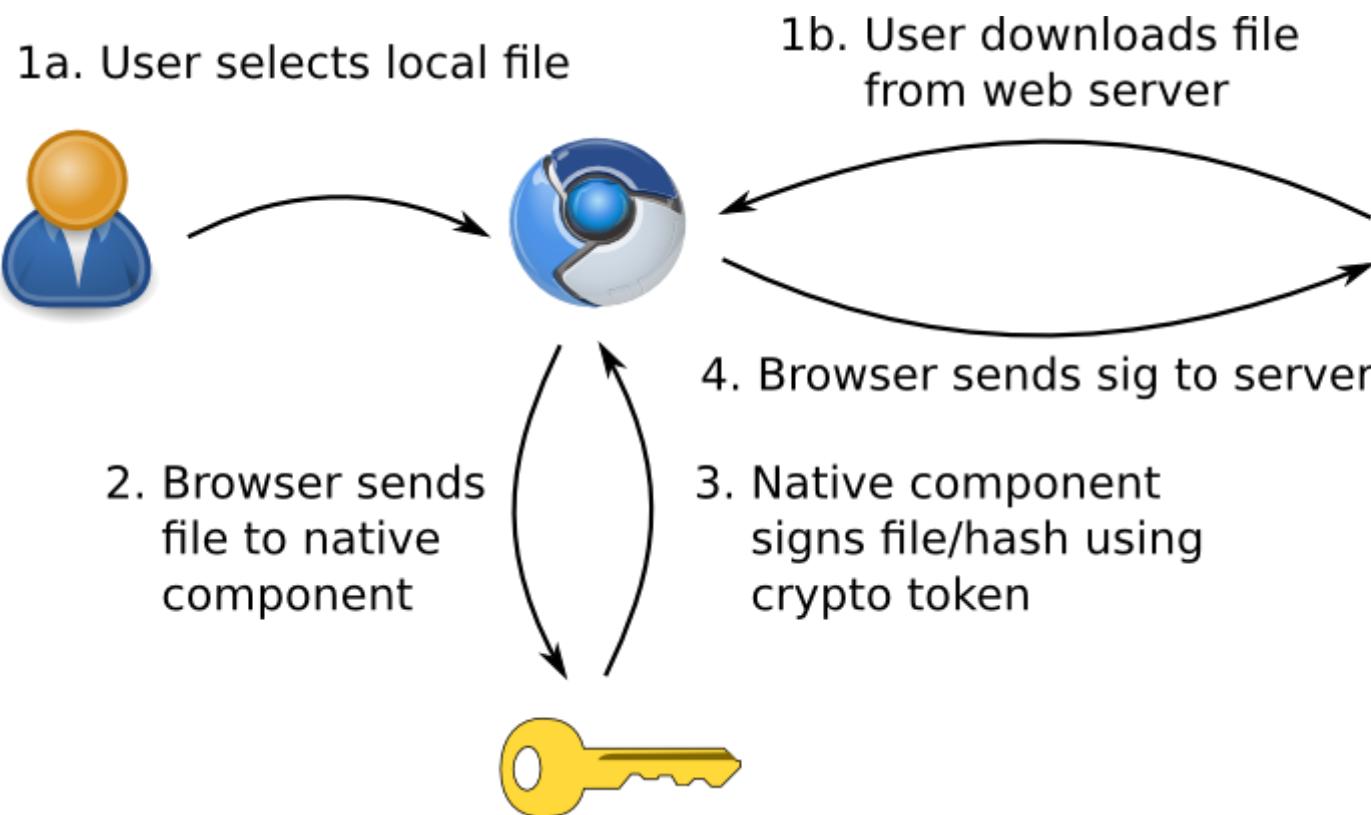
- It receives a JSON formatted message from the web extension with the text to be signed
- The component can either sign the text or its checksum (md5/sha1/sha2 supported)
- It supports multiple encodings for input message and signature

OS native component

Sample message

```
• {  
    "message": "Hello world!",  
    "srcenc": "plain",  
    "dstenc": "base64",  
    "hash": "sha256",  
    "includecert": 1  
}
```

Workflow



Installation experience

Installer for native app backend

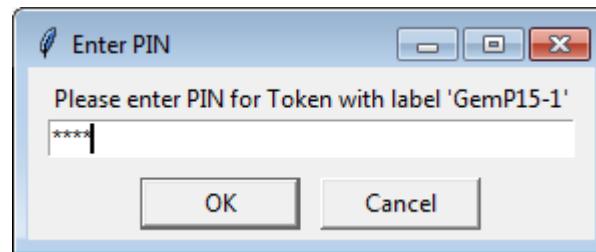
- Also includes drivers for the AcademicID, an ID given to all Greek members of the academic community

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

User experience (1) - prepare

The screenshot shows a web-based application interface for academic evaluations. At the top, there is a header bar with the logo 'sis.auth' and the text 'Υπηρεσίες Ηλεκτρονικής Γραμματείας ΑΠΘ'. On the right side of the header, there are links for 'Αρχική', 'Εξετάσεις', 'Υποστήριξη', and a user profile icon labeled 'testfaculty'. Below the header, the main content area has a breadcrumb navigation 'Αρχική > Εξετάσεις'. The main title is 'Ανοιχτές εξετάσεις'. A green box highlights 'Βήμα 1 / 2 : Έλεγχος βαθμολόγου'. A red box highlights a success message: 'Ο έλεγχος εγκυρώτητας των δεδομένων της εξέτασης του μαθήματος ολοκληρώθηκε με επιτυχία.' Below this message, there are details: 'Μάθημα: Δοκιμαστικό Μάθημα 4', 'Ακαδ. Έτος: 2015 - 2016', 'Εξετασική περίοδος: ΦΕΒΡ', and 'Ημ/νία υποβολής: 19-02-2016 15:47:21'. A section titled 'Έλεγχος βαθμολόγου' contains a table with three columns: 'Όνομα φοιτητή', 'Βαθμός', and 'Μήνυμα βαθμολόγησης'. The table row shows '600000334' in the first column, '10' in the second, and 'Ένας βαθμός υπάρχει ήδη και θα αντικατασταθεί.' in the third. A red box highlights the note 'Σύνολο βαθμών που θα ενημερωθούν: 1'. Below this, a note says 'Προσοχή! Υποβολή κενών βαθμών δεν επηρεάζει προηγούμενο βαθμό φοιτητή.'. At the bottom, there is a note: 'Αν συμφωνείτε με τις παραπάνω ενέργειες, προχωρήστε στην αποθήκευση και υπογραφή του βαθμολογίου. Διαφορετικά, ακυρώστε τη διαδικασία και επαναλάβετε με νέο βαθμολόγιο.' Two buttons are at the bottom: 'Ακύρωση' and 'Αποθήκευση & Υπογραφή', with the latter being highlighted by a red box.

User experience (2) – unlock crypto device



User experience (3) - signed

The screenshot shows a web application interface for 'sis.auth' (Services of the Electronic Government of the Ministry of Education and Religious Affairs). The top navigation bar includes links for 'Αρχική', 'Εξετάσεις', 'Υποστήριξη', and a yellow 'Συνδεθείτε' button.

The main content area displays a section titled 'Τρέχουσες εξετάσεις' (Current Exams) with a sub-section 'Βήμα 2 / 2 : Παραλαβή αποδεικτικού'. A green box contains two items:

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

Below this, there is a note: Μάθημα: Λαζαρεανά και θεωρητικά σύστασης, Ακαδ. Έτος: 2015 - 2016, Εξεταστική περίοδος: ΣΕΠΤ, and Ημ/νία υπογραφής: 03/09/2016 09:22:00.

A section titled 'Αποτελέσματα Βαθμολόγησης' lists one result:

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

At the bottom, it says Σύνολο βαθμών που ενημερώθηκαν: 1.

Two red boxes highlight specific text: 'Μοναδικός αριθμός ελέγχου αποστολής: Stj4QMNC9X2ANozBQWyw1/lgnQ=' and 'Εκτύπωση αποδεικτικού βαθμολόγησης'. A red arrow points from the second box towards the right.

At the very bottom left is a 'Επιστροφή' button.

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

