A browser-based digital signing solution over the web

Fotis Loukos
Charalampos Tsipizidis
Dimitris Daskopoulos

Contents

The need

Goal:

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

Means:

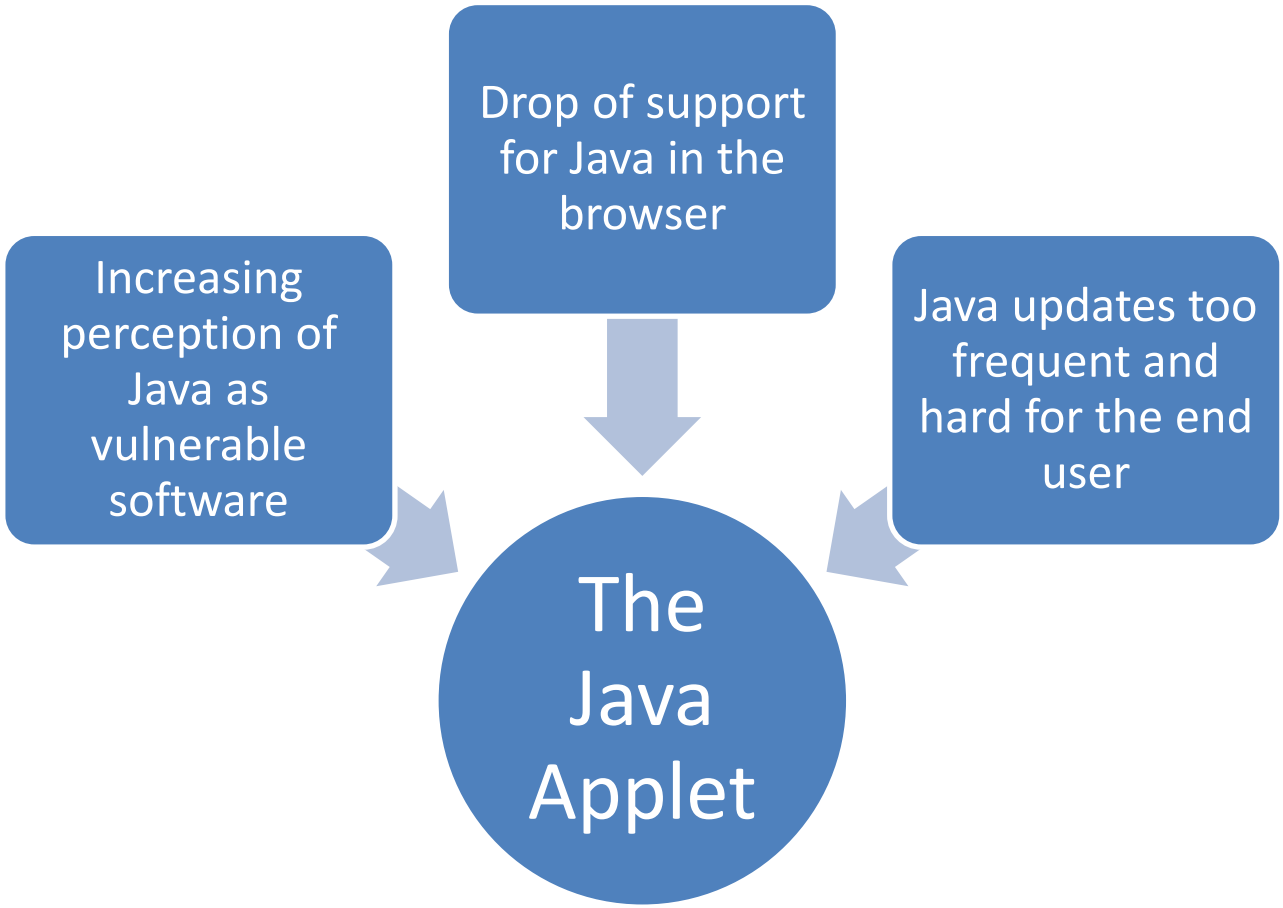
- Digital signatures on crypto devices (tokens)

Requirements:

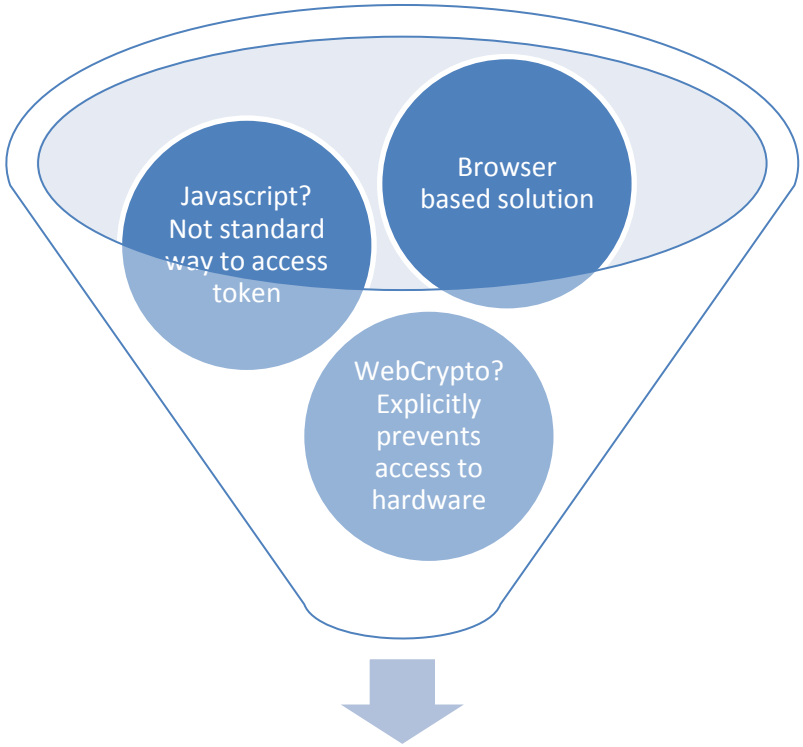
- Seamless digital signing on the web
- Ease of use, rapid installation, minimal maintenance

Legacy solution

The problem with legacy solutions

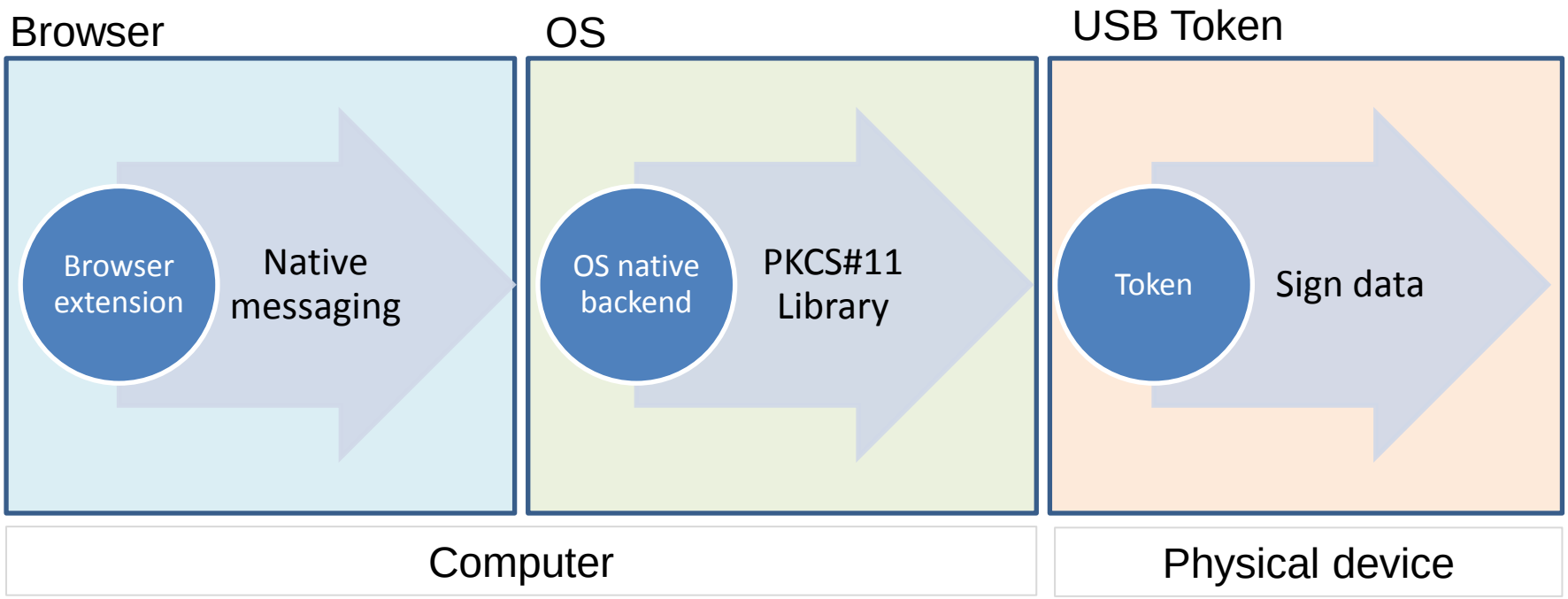


Proposed solution



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

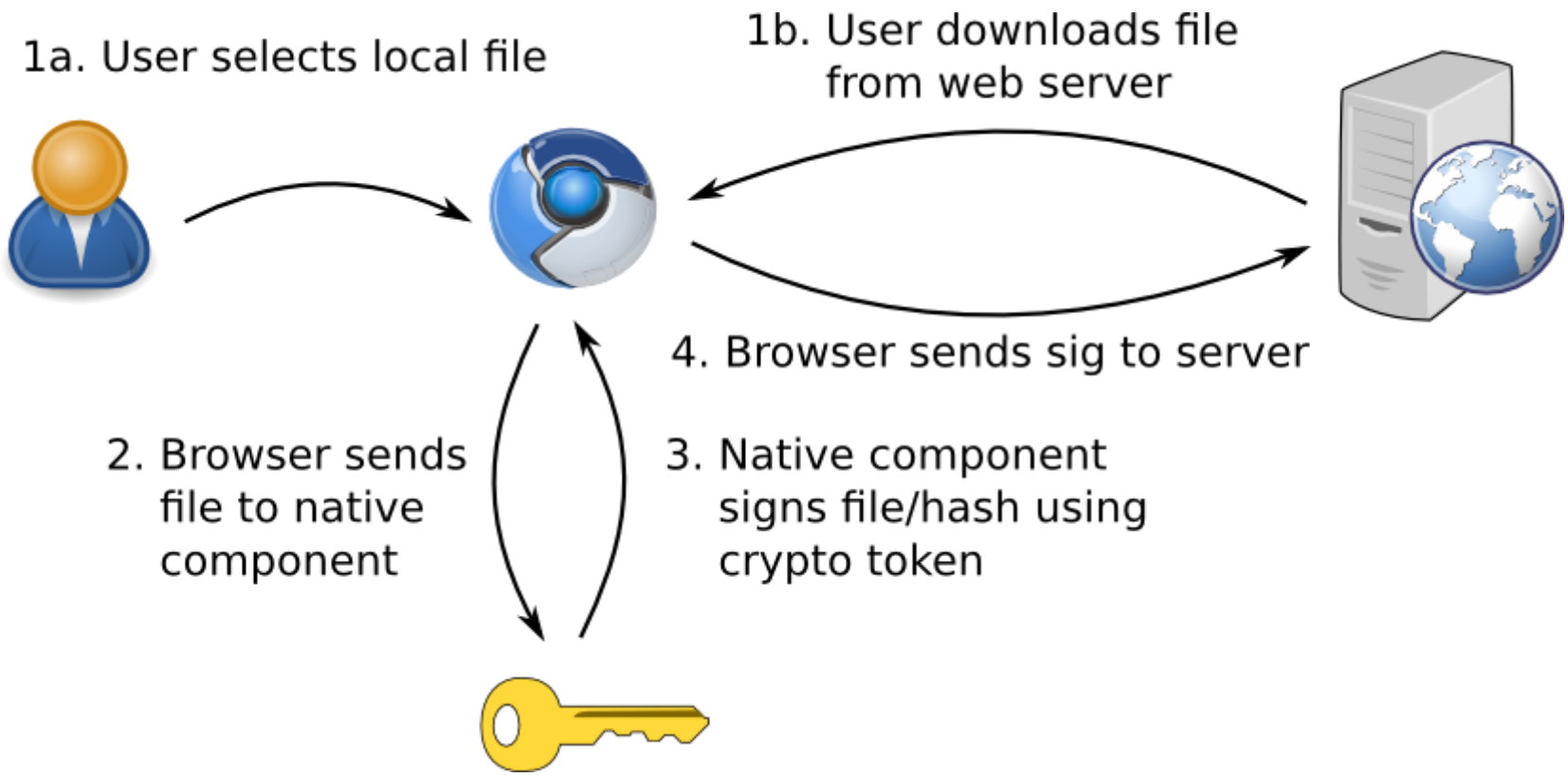
- It receives a JSON formatted message from the web extension with the text to be signed
- The component can either sign the text or its checksum (md5/sha1/sha2 supported)
- It supports multiple encodings for input message and signature

OS native component

Sample message

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

Workflow


1a. User selects local file
1b. User downloads file from web server
4. Browser sends sig to server
2. Browser sends file to native component
3. Native component signs file/hash using crypto token

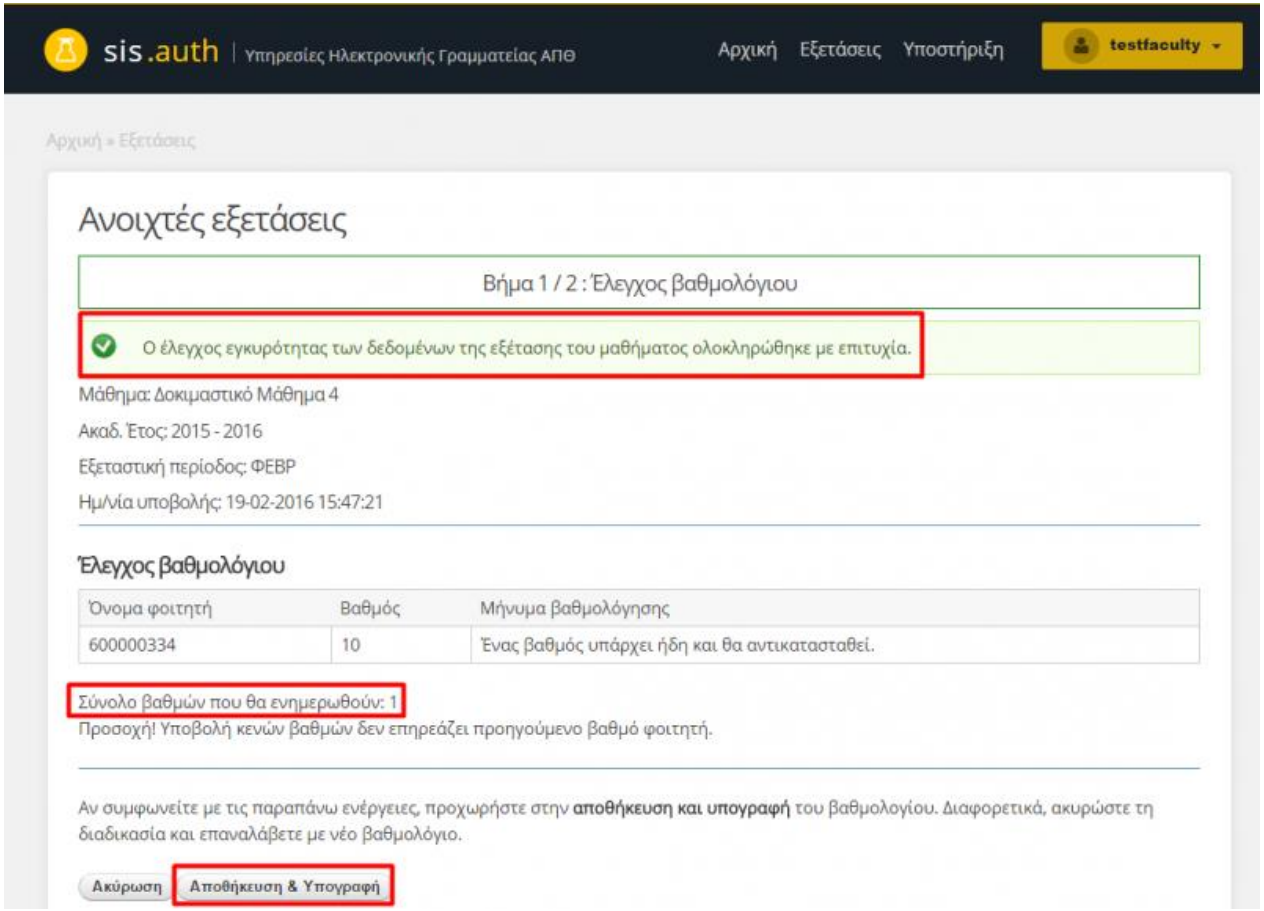
Installation experience

Installer for native app backend

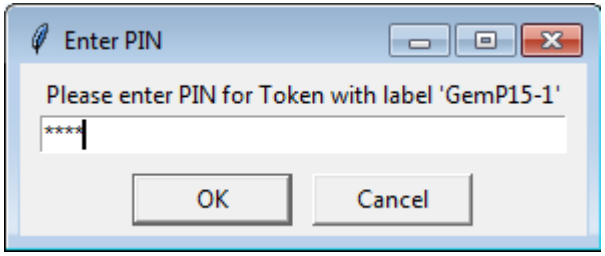
- Also includes drivers for the AcademicID, an ID given to all Greek members of the academic community

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

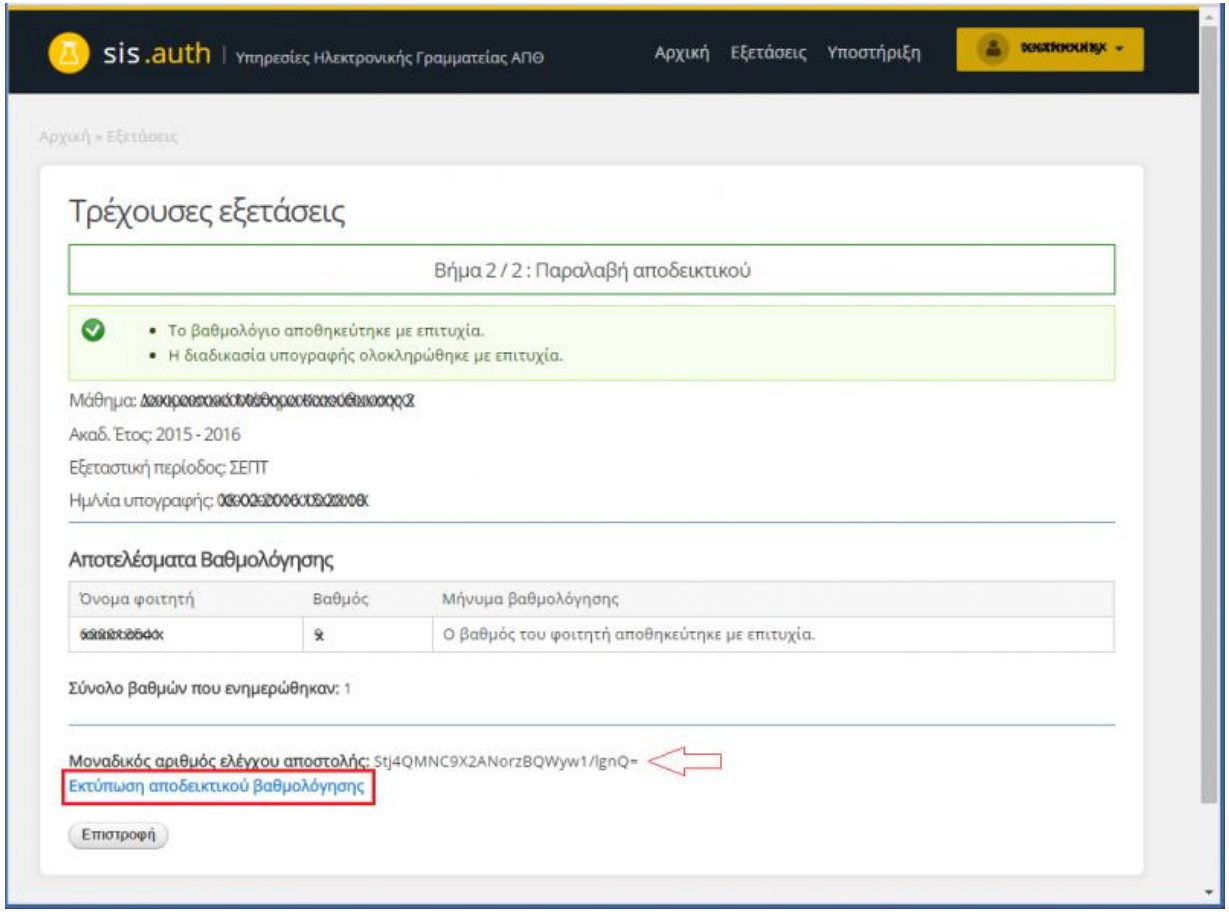
User experience (1) - prepare



User experience (2) – unlock crypto device



User experience (3) - signed



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