Exploring Digital Signatures Secrecy in Web-Platform:

Client-Side Cryptographic Operations

Wellington Fernandes Silvano, Gabriel Cabral, Lucas Mayr, Frederico Schardong, Ricardo Custódio

Laboratório de Segurança em Computação (LabSEC)
Departamento de Informática e Estatística (INE)
Universidade Federal de Santa Catarina – Brazil

Instituto Federal do Rio Grande do Sul (IFRS) – Brazil

Presentation

Web-signatures Platform:

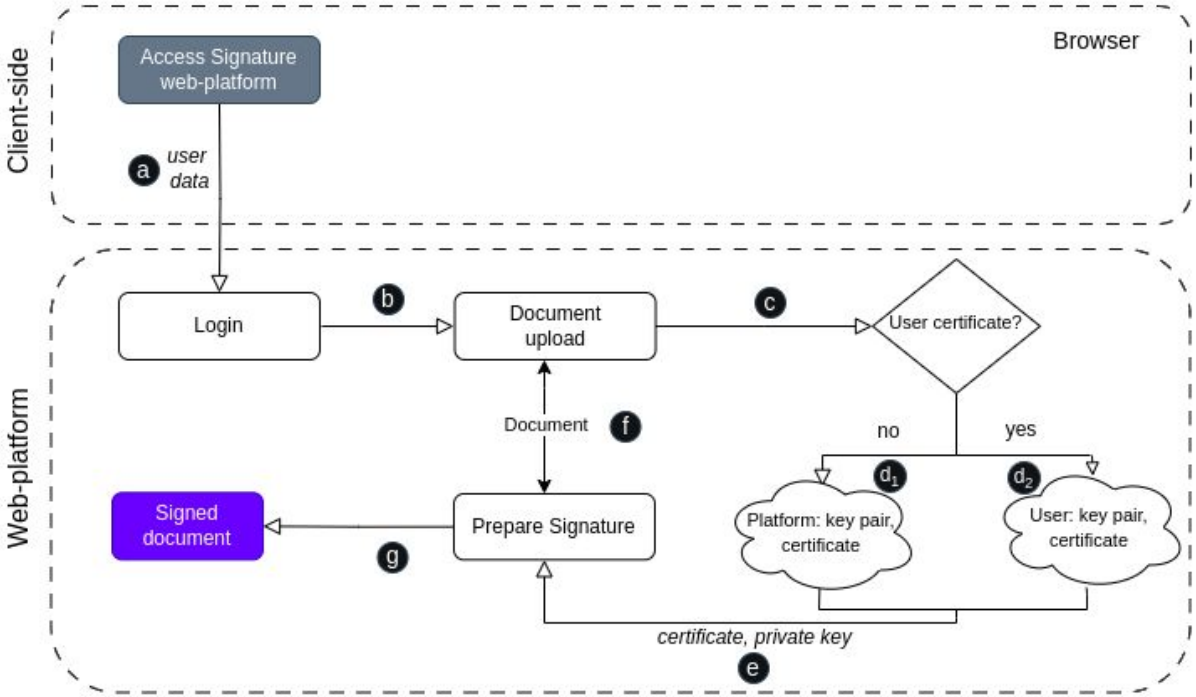
- Wide adoption
- Practicality
- Security risks (secrecy doc.)
- Data protection and secrecy law

Secrecy by Claude Shannon

- Existence of the message (SST-1)
- Equipment or techniques (SST-2)
- Concealment with cryptography (SST-3)

Existing/traditional Model

For Signature Web-platforms



The problem

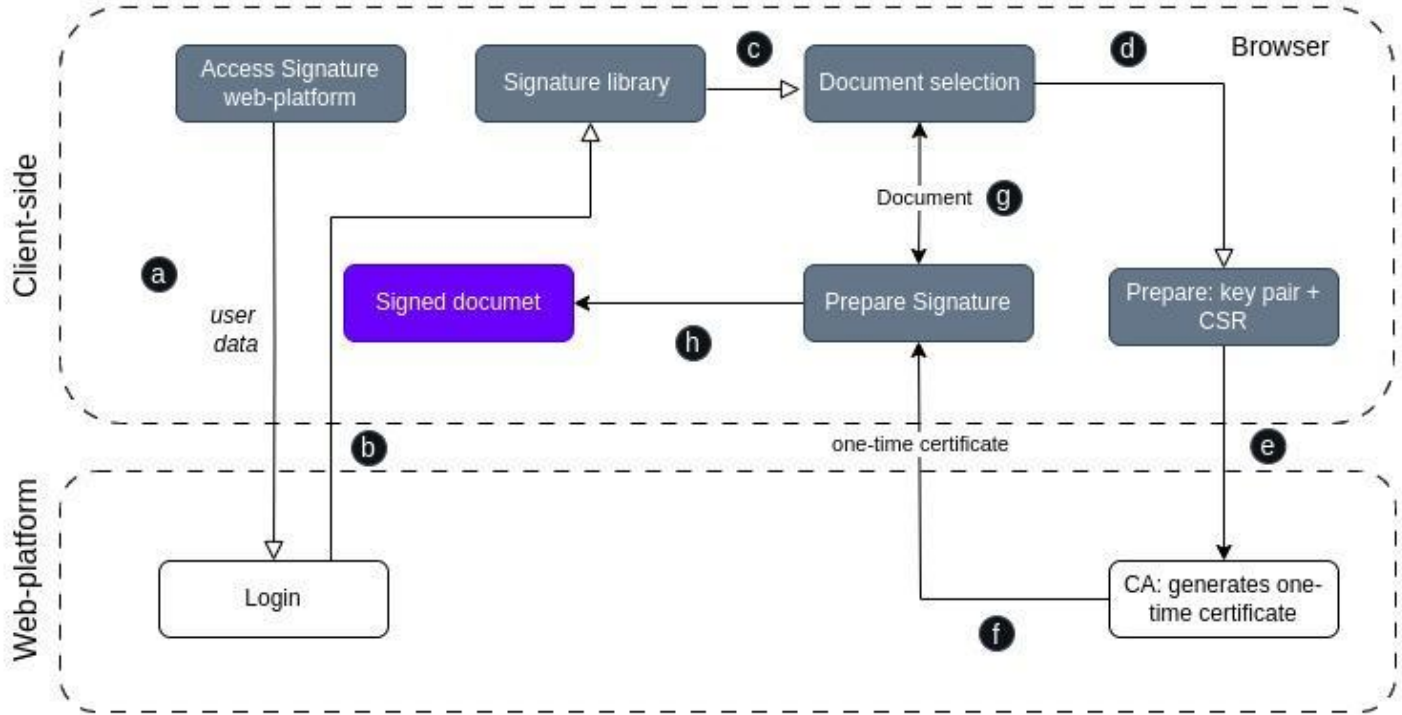
- Exposure of “Sensitive” Documents;

- Compromise of Private Keys (new paradigm?!);

- Compliance with Regulations:
  - GDPR and LGPD;
  - Industrial Property;
  - Professional secrecy;
  - Espionage Law;
  - Freedom of Information Act (FOI).

Proposed Model

For Signature Web-platforms



Model Implementation

- Javascript
- Webcrypto library

Legacy Compatible:

- ISO-32000
- PAdES
- x.509 certificate
- RFC 5280 certificate standards

Application Flow

Algorithm 1: Signing PDF documents in the client's browser using One-Time Certificate

```
1:  function SIGN(BytesPDF, userIdentity)
2:      BytesPDF ← PrepareDocumentForSignature(BytesPDF)
3:      Hash ← CalculateHashOfBytesToBeSigned(BytesPDF)
4:      KeyPair ← GenerateKeyPair()
5:      CSR ← CreateCSR(KeyPair, Hash, userIdentity)
6:      PKCS7 ← SendCSRToCA(CSR)
7:      PKCS12 ← CreatePKCS12(KeyPair.private, PKCS7)
8:      SignedBytes ← SignPDF(BytesPDF, PKCS12)
9:      return SignedBytes
10: end function
```

Signature Interoperability (1/3)

Results and Discussion

```
pdfsig example_assinado.pdf
Digital Signature Info of: example_assinado.pdf
Signature #1:
- Signer Certificate Common Name: Alice Silva
- Signer full Distinguished Name: E = alice.silva@secrecy.com, CN =
   Alice Silva, C = BR
- Signing Time: Feb 09 2024 16:25:07
- Signing Hash Algorithm: SHA-384
- Signature Type: adbe.pkcs7.detached
- Signed Ranges: [0-23448], [43450-44167]
- Total document signed
- Signature Validation: Signature is Valid.
```

Figure 3. *pdfsig* tool usage example to verify PDF digital signatures.

Execution Times: Client-Side Signature (2/3)

Results and Discussion

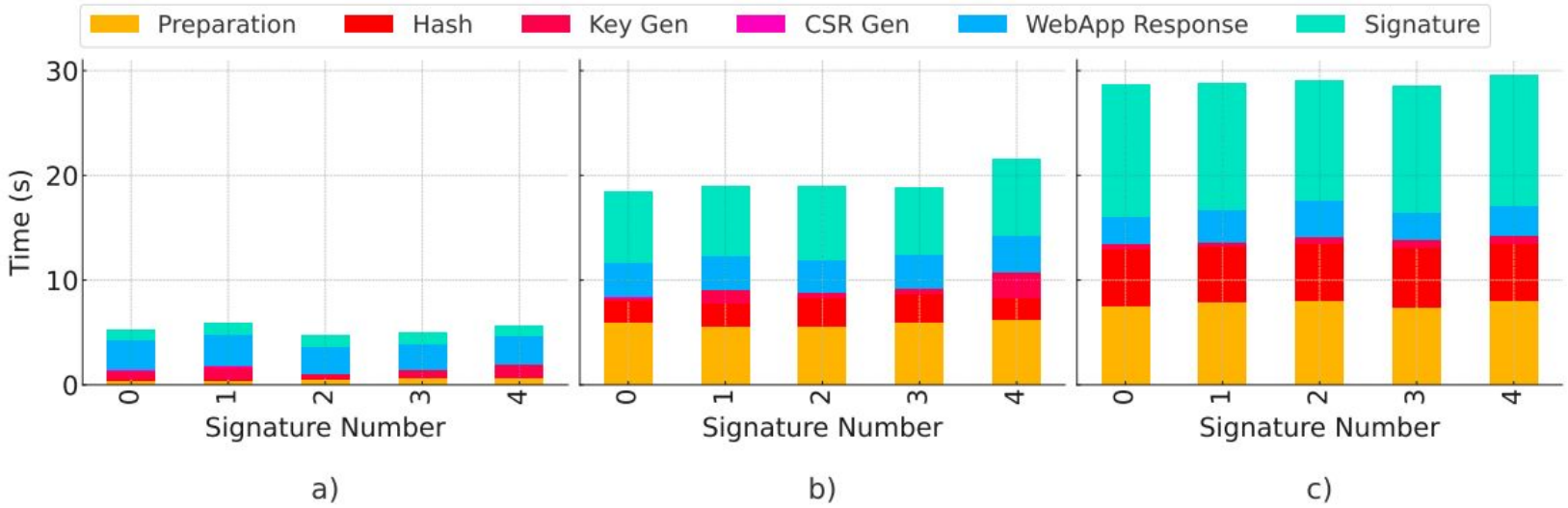


Figure 4. Total signature time for multiple signatures. Document sizes: a) 1.12 MB, b) 32.16 MB, c) 60 MB.

Execution Times: Client-Side Signature (2/3)

Results and Discussion

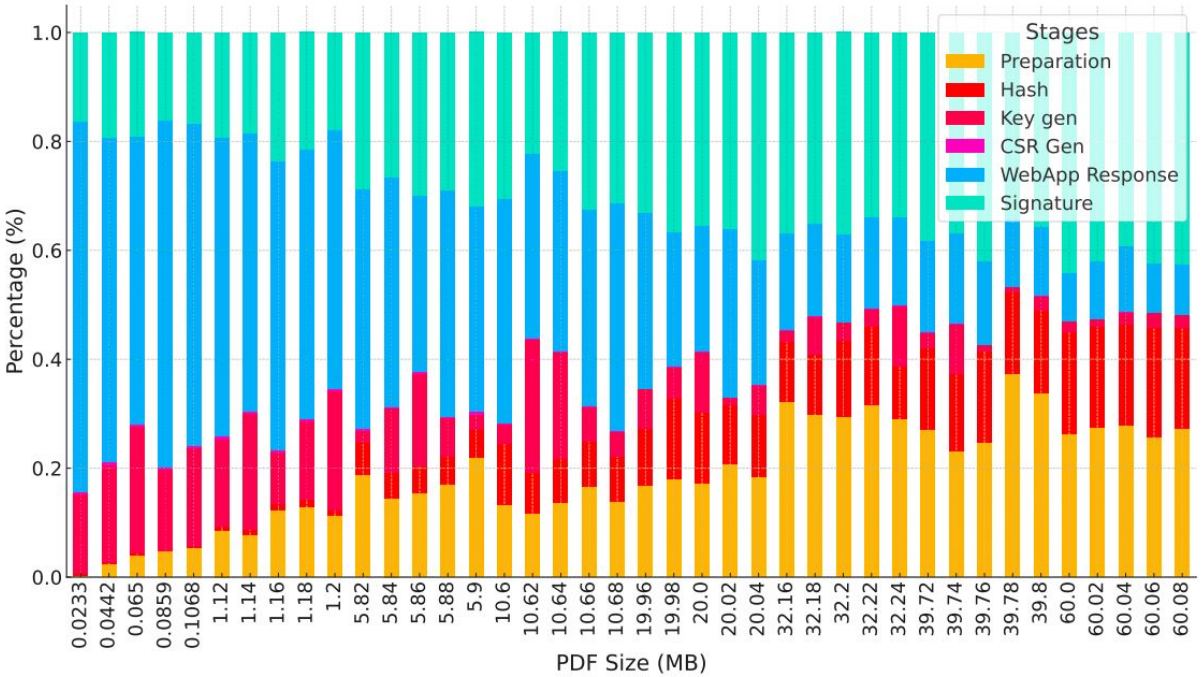


Figure 5. Percentage of Total Time by Process and Document Size.

General Analysis (3/3)

Results and Discussion

Table 1. Comparison between traditional signature web-platforms with our model

Feature	Traditional Web Platforms	Our model
Document Secrecy	Conditional	Unconditional
Private Key Secrecy	Conditional	Unconditional
Private Key Management	Complex	Simplified
Certificate Handling	Resource-Intensive	Streamlined
Multiple Signers	Link-Based	Out-of-Band
Signature Performance	Server Power Dependency	Client Machine Dependency
Large documents performance	Slower	Faster
Small documents performance	Faster	Slower

Final Consideration

Enhancing document secrecy and eliminating private key exposure.

Improved Security: No document uploads, secure key management.

User-Friendly: Seamless browser integration, simplified certificate handling.

Compliance with GDPR/LGPD, reduces platform liabilities.

Future Work

- Multi-signature processes (doc. Share/secret share);
- Optimizing performance;
- Browser security study

Obrigado!

SBSeg24 SÃO JOSÉ DOS CAMPOS

LabSEC
Laboratório de Segurança em Computação

UNIVERSIDADE FEDERAL DE SANTA CATARINA

RCPN
Operador Nacional | Registro Civil do Brasil

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

CAPES

Contato

Wellington Fernandes Silvano
wellington.fernandes@posgrad.ufsc.br