Client-side encryption for privacy-sensitive applications on the cloud

Stefano M. P. C. Souza

stefano@stm.gov.br

Ricardo S. Puttini

puttini@unb.br

Graduate Program in Electrical Engineering
Universidade de Brasília

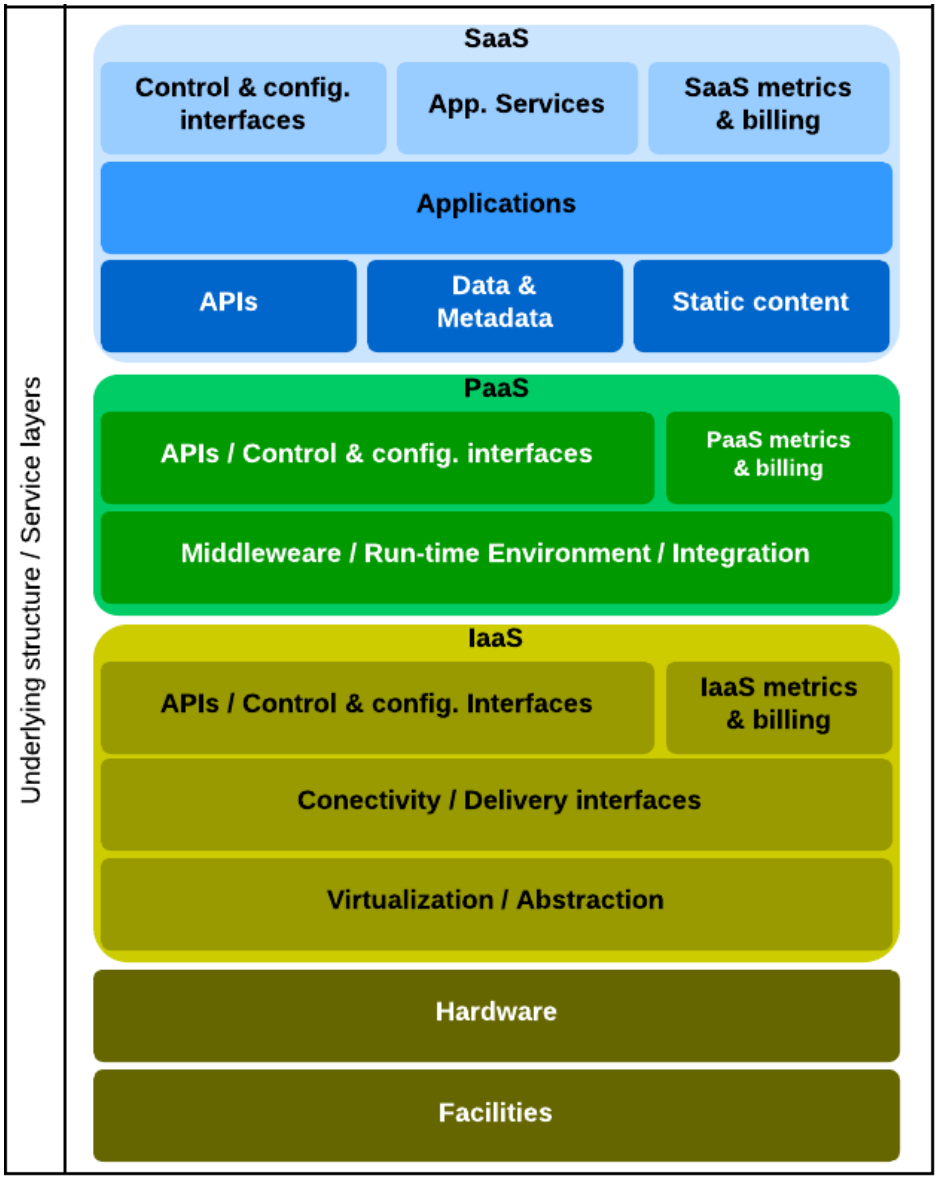
Context

- Cloud computing is the strongest trend in enterprise level computing;
- For most organizations, it means the reduction of complexity and costs of their IT infrastructure;
- A few organizations, however, handle information subject to strict legal restrictions and, thus, are not free to trust such information to third parties (e.g. health, bank accounting and tax records);

Problem

- The higher the complexity of cloud services, the lesser the effective control over the assets for the consumer;

- Improving the security and auditability of cloud infrastructures does not satisfy legal limitations on data sharing or relocation.



Solutions in literature

- Most works in recent literature propose the use of client-side encryption for privacy-sensitive applications;
- The intuition is that, legally speaking, cloud servers never receive the actual data;
- The challenge in this approach is to find the encryption systems that will not hinder the functionalities required by the application.

Our position

- There are recurrent shortcomings of security solutions in literature, specially regarding privacy-sensitive applications;
- Client-side encryption, the most common solution, needs to be improved with the use of cryptographic primitives that allow some secure computations in the cloud;
- We propose that fellow researchers take up the task to test, further develop and disseminate such cryptographic primitives in order to foster security in the cloud environment;
- We base our proposal in the fact that other cryptographic primitives, such as digital signatures, have been successfully adopted by the general public.

Shortcomings in current solutions

- Efforts to improve security assessment and auditability of cloud services or even the accountability of CSPs do not help when the consumer is forbidden by law to trust the provider;

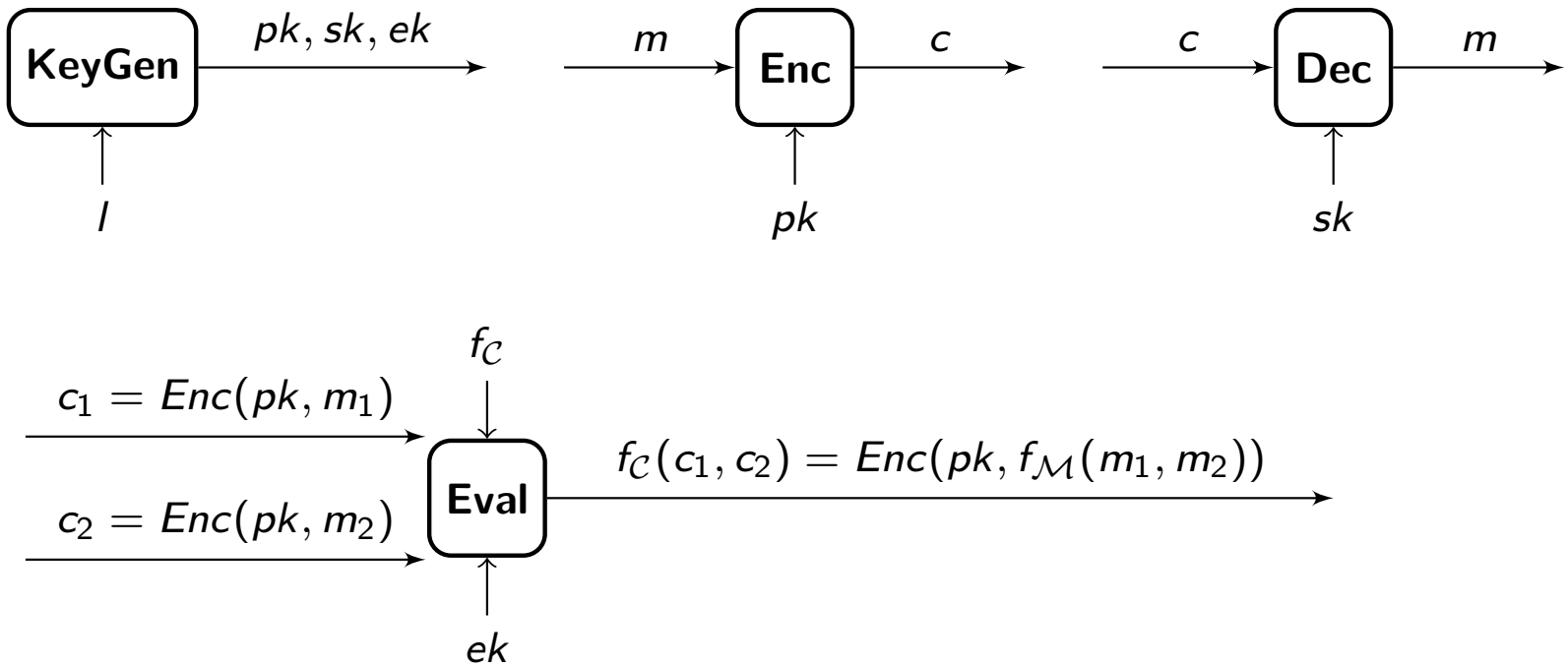
- Most works trying to address these edge cases propose client-side encryption without reasoning the nature of the data and the functional requirements of real-life applications;

- These solutions are usually built around the access control requirements, resorting to complex Public Key Encryption systems, such as Identity-based Encryption, Attribute-Based Encryption and Hierarchical Public Key Encryption;

- In practice, these schemes completely hinder the use of the cloud's computing power, reducing consumer's options and benefits in adopting the cloud;

Homomorphic cryptography

The computing power of the cloud must be used at least for the extraction of anonymous/aggregate information (e.g. totals, means, modes) and for the selection of records of interest in a given interaction with the cloud application.



Recent results with client-side encryption (NOT PEER REVIEWED)

- We have used Additively Homomorphic and Order-preserving schemes to perform efficient searches over millions of health records of the Brazilian National Electronic Health Record;

- These searches allow sanitarians and policy-makers to identify records featuring specific medical observations (e.g. high blood pressure, high cholesterol) in documents produced in the nation-wide public health system - while preserving patient's privacy;

- Encryption and key management happens at client-side, and patients are able to use digital signatures to grant doctors read/write authorizations over their records;

Cryptographic primitives in “everyday computing”

Brazil has an official Public Key Infrastructure (PKI), with legislation governing the use of digital signatures in health data and in the communication with the justice system and with the Revenue Authority;

Many countries have PKIs dedicated to health or fiscal data (German e-Health, French SESAM, Spanish TASS, Italian CIE, Taiwan TMT *etc*).

Conclusion

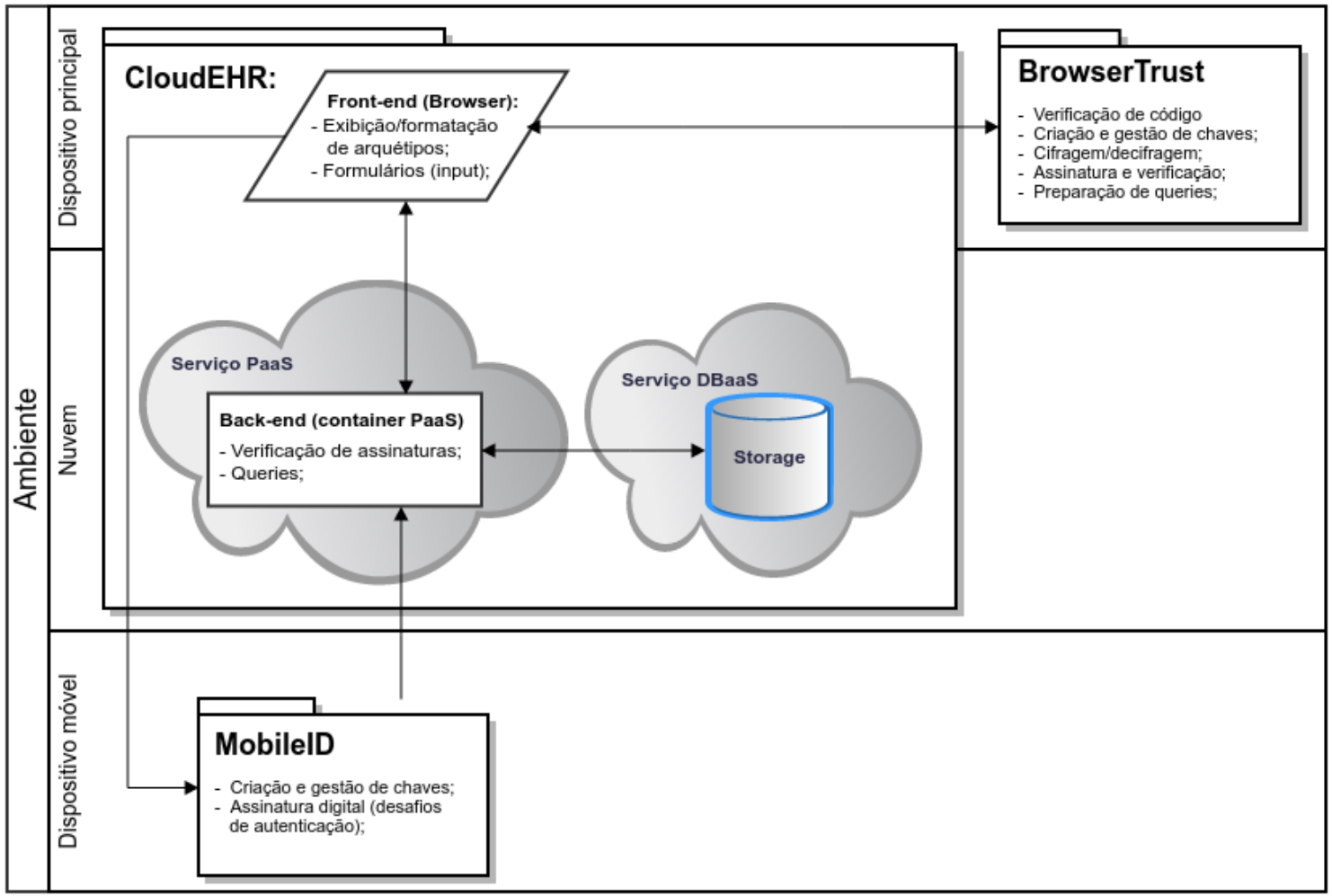
- Some applications will have client-side encryption as a prerequisite for cloud deployment;

- The future of cloud computing must, therefore, include cryptographic primitives fit for client-side encryption, such as Homomorphic and Order-Preserving encryption systems;

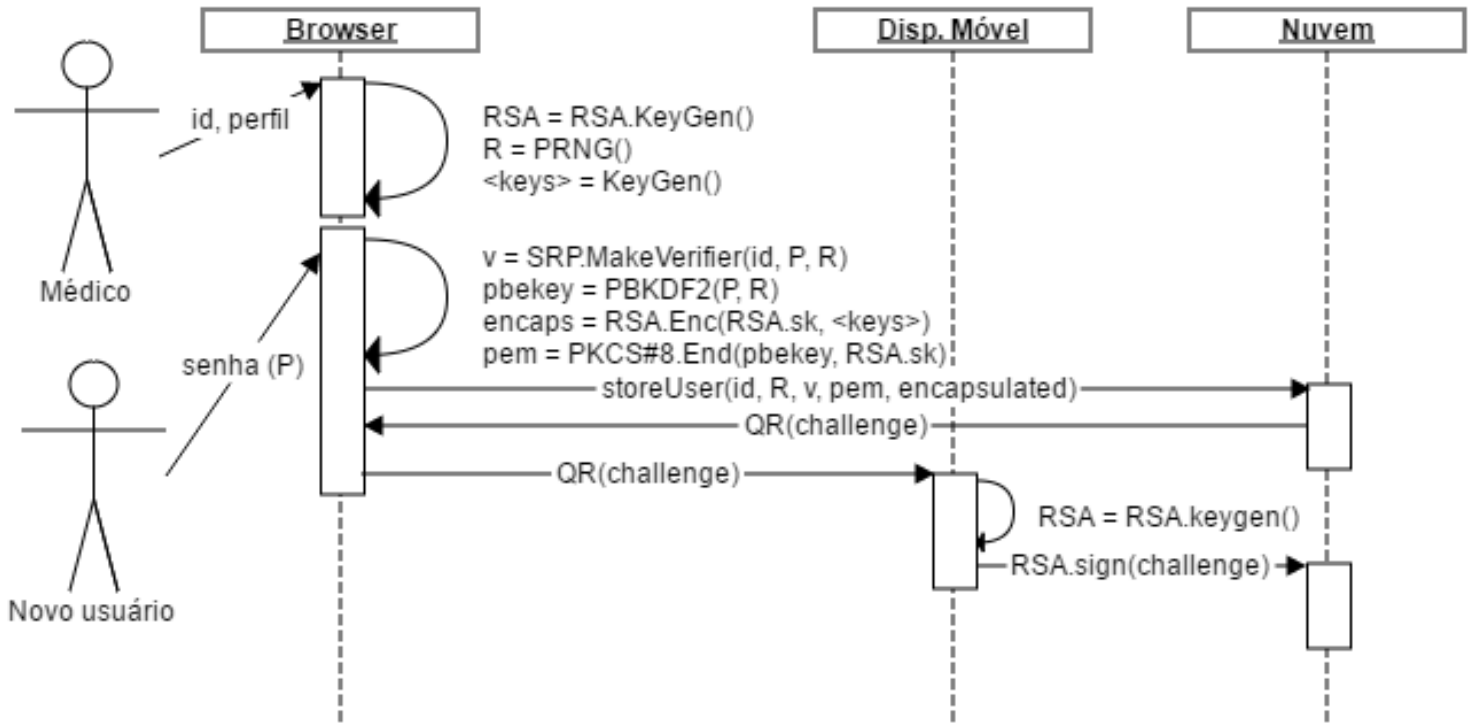
- Further research and development on client-side encryption, specially the presence of mature, well tested, and simple open software libraries featuring such cryptographic primitives, could help bridge the gap between them and real-life cloud applications (and, consequently, the general public).

Thank you

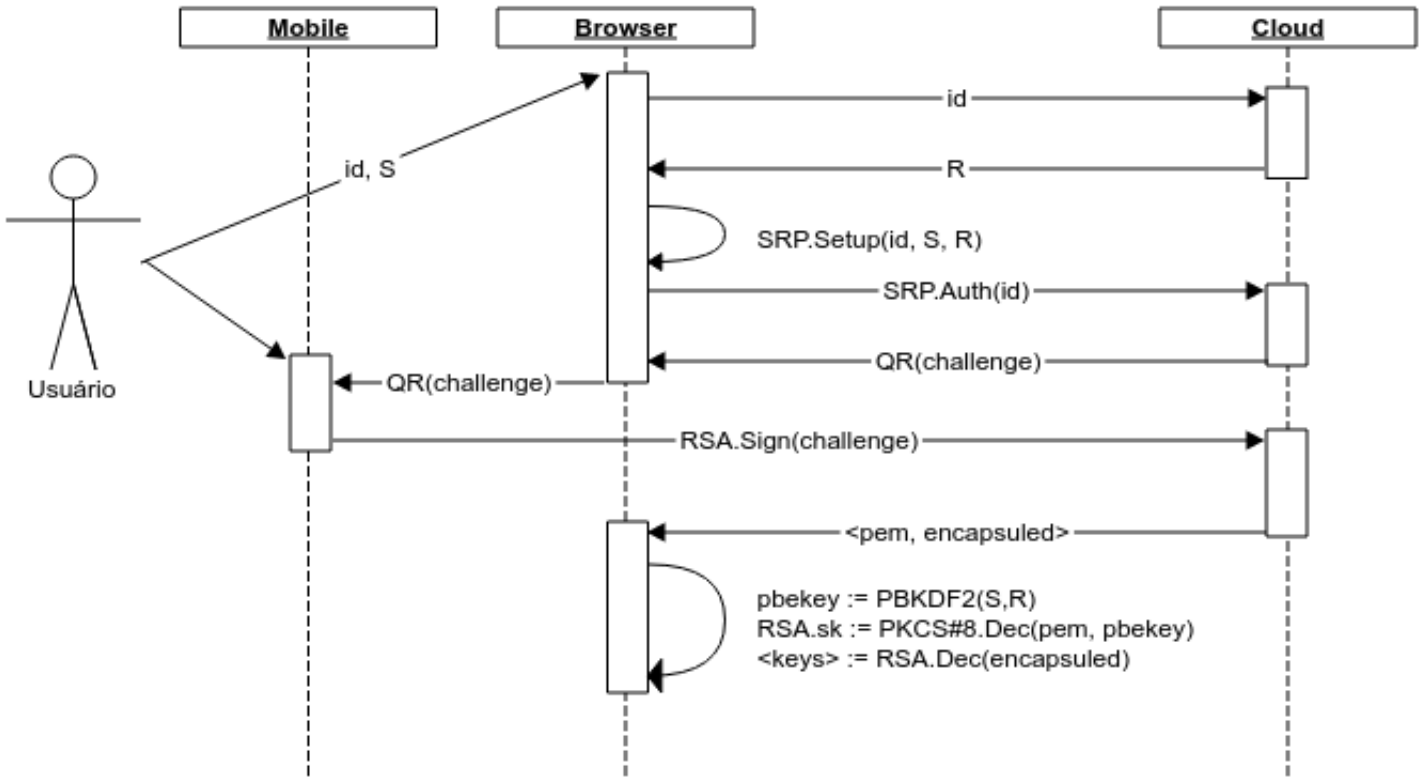
Safe-Record: architecture



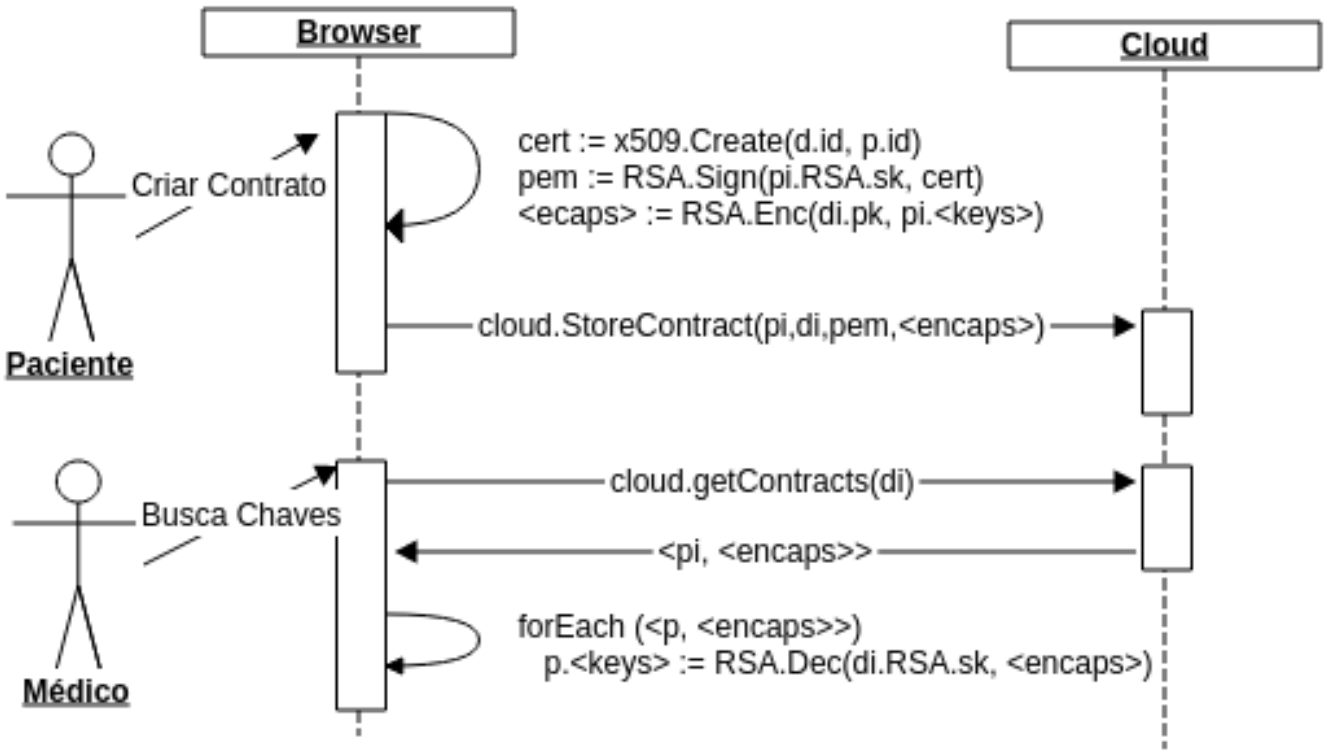
Safe-Record: user registration



Safe-Record: authentication

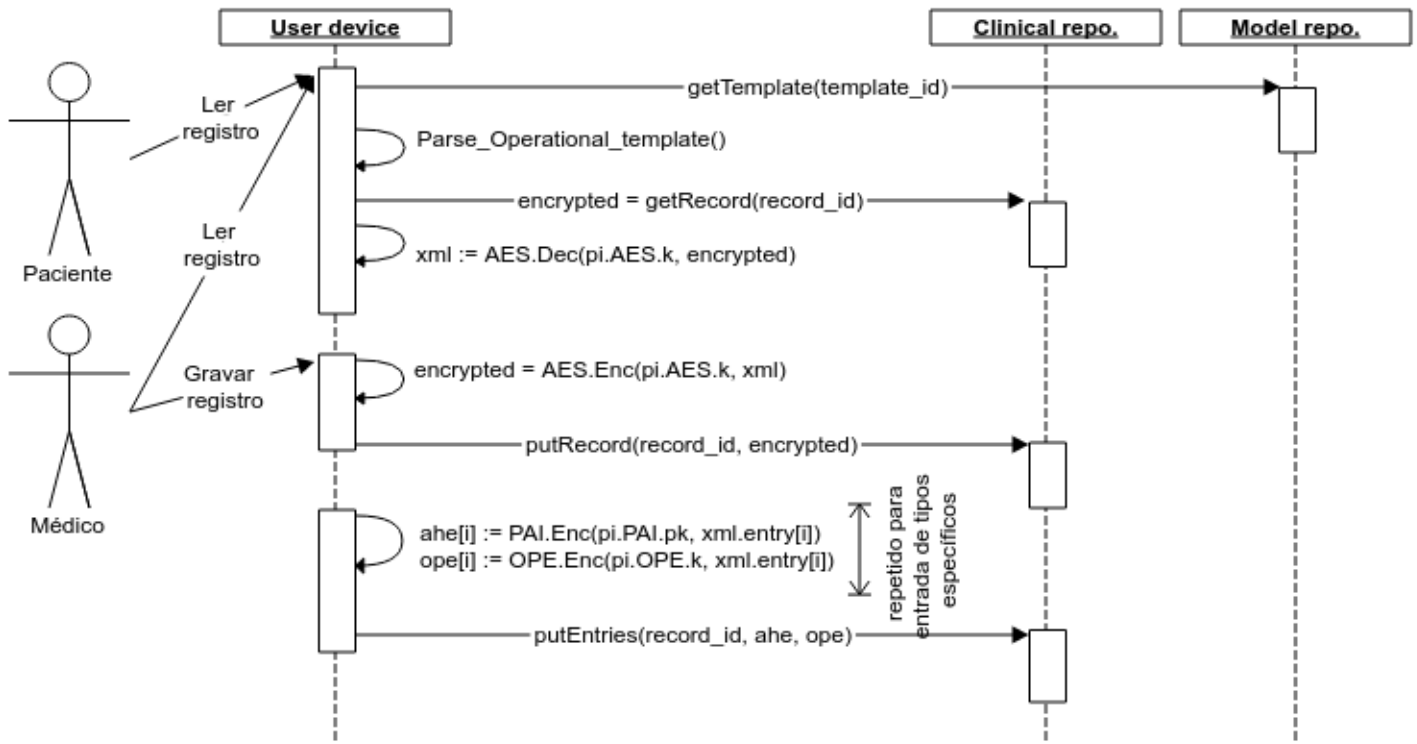


Safe-Record: authorization

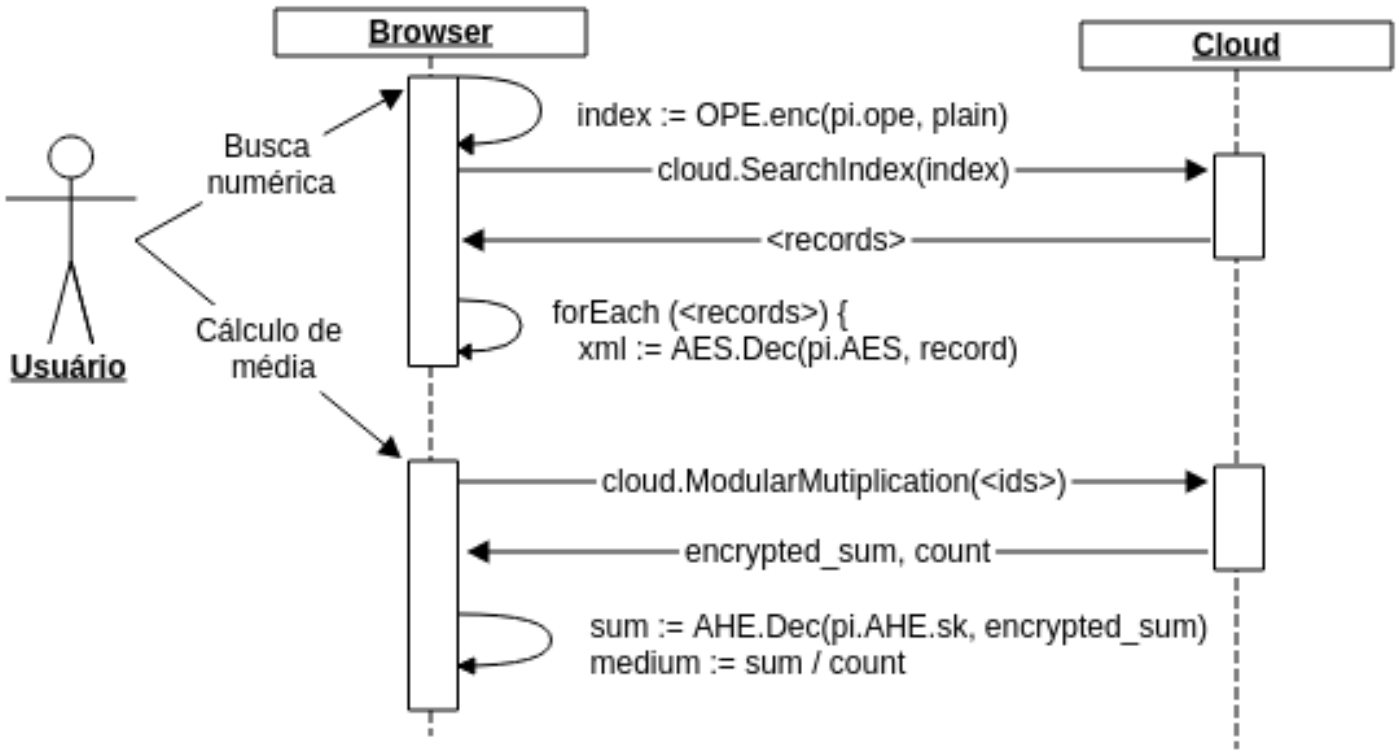


EHR handling

Pacientes apenas lêem os registros. Médicos adicionam ou alteram registros.



Search


Browser
Cloud
Usuário
Busca numérica
Cálculo de média
index := OPE.enc(pi.ope, plain)
cloud.SearchIndex(index)
<records>
forEach (<records>) {
xml := AES.Dec(pi.AES, record)
cloud.ModularMutiplication(<ids>)
encrypted_sum, count
sum := AHE.Dec(pi.AHE.sk, encrypted_sum)
medium := sum / count