Mudamos - Lawmaking

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-003	**Use Case Type:**	*Vertical*
Use Case Title:	Mudamos	**Is Use Case supporting SDGs**	*No*
		Domain:	*List 1 Appendix 1 d*
Status of Case	*Implementation*	**Sub-Domain**	*If necessary*
Contact information of person submitting/ managing the use-case	*Marco Konopacki* *Project Coordinator* *marco@itsrio.org* *+55 21 999278090* *marco@itsrio.org* *@marcoamarelo* *http://itsrio.org* *http://mudamos.org*		
Proposing Organization	*Institute for Technology and Society*		
Short Description	*Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures.*		
Long description	*Mudamos is a mobile application that enables Brazil's citizens to participate in lawmaking by proposing their own bills and signing onto one another's proposals using verified electronic signatures. Any citizen with a smartphone (Android or iOS) can download the app and register with his or her electoral ID, name and address, information which Mudamos keeps secure and verifies with Brazil's Electoral Court. The app issues what is known as a cryptographic key pair, a small piece of code used for verification. One half of the key is stored on the user's phone and the other with Mudamos, which makes it possible to authenticate a person's signature. In this way, members of the public can draft and sign petitions in a way that is verifiable and secure.*		
SDG in Focus (when applicable)	*Enter one or more number (1-17) and specific corresponding indicator/s as applicable* *See https://www.un.org/sustainabledevelopment/sustainable-development-goals/* *Goal 16: Promote just, peaceful and inclusive societies*		

Value Transfer:	*If potential solution allows to transfer any value (e.g. assets, tokens, etc.)*	**Number of Users:**	*350.000*
Types of Users:	*Voters regular registered to vote.*		
Stakeholders	*Citizens (engaged citizens in support for law making), Legislative Houses (representatives and public servants).*		
Data:	*In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks, where they can be publicly scrutinized. This ensures that signature lists are immutable, and if an interested agent wants to audit the entire signing process, from the first signature collected, they have the capability to do it without relying on Mudamos or any other agent.*		
Identification:	***Auto geranted Private key / Electoral data***		
Predicted Outcomes:	**Signature lists in support of citizens' initiative draft bills.**		

Overview of the Business Problem or Opportunity
Brazil's Constitution provides several direct democratic mechanisms, including the referendum, plebiscite, and citizens' initiatives. The initiative mechanism allows any citizen to propose a draft bill to the lower house of municipal, state or federal legislatures. If the proposal gets the requisite number of signatures from registered voters in support then the campaign organizators present the bill before the House. Once the signatures are verified, the Speaker assigns a House committee to start bill discussion that could lead (or not) to the bill becoming a law. At the federal level, the minimum amount of signatures is 1.5 million, which is problematical to organize using paper-based petitions. Popular initiatives to collect signatures are often paper-based which, apart from being costly, also present problems of transparency and integrity. In fact, no citizen bill has ever been approved at the national level due to the verification barrier and participation costs. *Thus Institute for Technology and Society (ITS Rio) created Mudamos in 2017 to reduce the high costs of creating paper-based petitions by offering a verifiable online mechanism for the creation and signing of citizen petitions and offer a robust means of participation that, in turn, should help to raise citizens' degree of trust in political institutions and contribute to the construction of participatory rules and norms.*
Why Distributed Ledger Technology?
The uniqueness of the signatures is guaranteed by the association of unique electoral ID number combined with the signature timestamp and the user's private key. The private key generates a unique hash based on the data reported for signature. Verifiability is guaranteed by publishing the user's public key along with the data given for signature and the signature hash. In order to make the whole process auditable, Mudamos publishes the signatures list periodically by registering the files in public blockchain networks.

Section 2: Current process

Current Solutions
N/A

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	Create a campaign for signature gathering	N/A. Paper-based
2.	Paper-based form download from legislative house	Access legislative house website and download form template.
3.	Signature	N/A. Paper-based signature
4.	Present signatures	N/A. Paper-based process. 1.5 million paper-based signatures have an average of 2ton weight.

Process scheme (as-is)

Data and information (as-is)		
Data	**Type**	**Description**
1	*Documents*	Electoral Personal Data (Name, Electoral ID, ZIP Code) and signature written down on paper-base forms.
2	*Payment transactions*	N/A

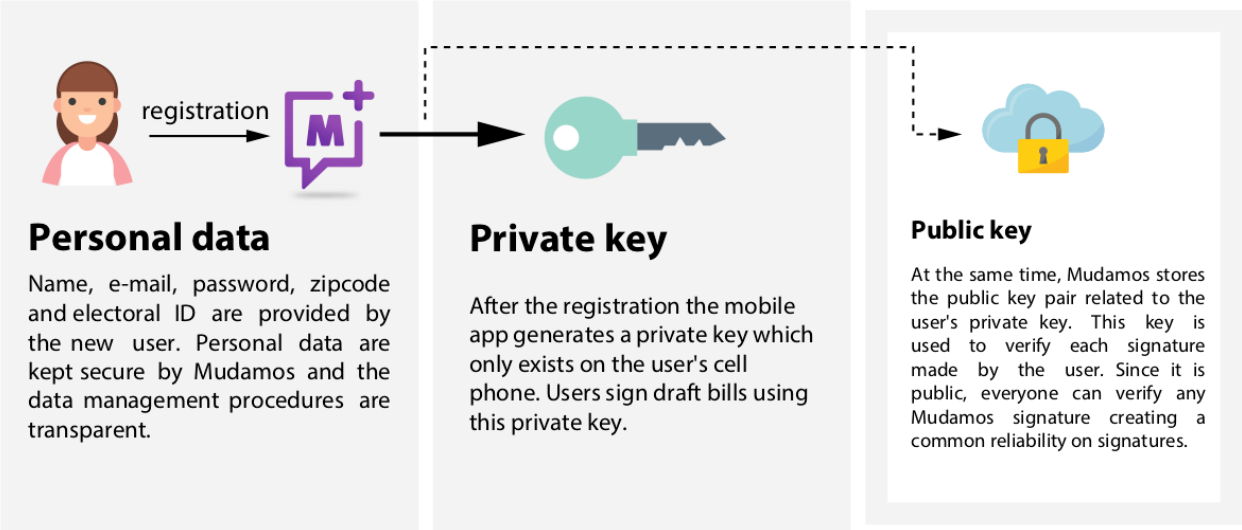
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	*Legislative houses*	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
2	*Signature campaign leaders*	People who decide organize campaigns in support for a drat bills and manage all logistics for that.
3	*Signers*	People how sign in support for a draft bill.

Other Notes
Any assumptions, issues

Section 3: Expected process

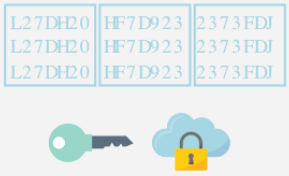
Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Register on Mudamos	Generate key pair
2.	User signature	Electoral data hashing based on private key
3.	Signature verification	Checking electoral data against signature hash and user's public key
4.	Check public signature lists	PDF signature list hashes checking on public Blockchains
5.	Reach signatures threshold	Present lists into a flash drive to legislative house speaker to start bill discussion

Process scheme (to-be)



Sign a draft bill

Personal data is compiled based on the legal Brazilian standard. In addition, Mudamos adds some metadata to strengthen the signature and make it reliable (i.e. timestamp).



Hashing data

The data is hashed by user's private key and the outcome is a cyphered word. This word is the evidence of the user's act in order to support a draft bill.

Signature storage

All the signatures hashes are stored on Mudamos' servers. These signatures can be verified how many times are necessary using the public keys related for each user registration.

Regular publishing

Mudamos regularly compile each draft bill campaign signatures in a single document and make it public to allow every one follow the ongoing process.

Blockchain register

Every signatures document is registered on public Blockchains to ensure its authenticity and integrity, in other words, ensure they were not modified during the signature gathering campaign.

Presenting to a legislative house

The signatures document can be independently verified by the legislative house. In fact, every stakeholder can do your own signature verification without any special resources from Mudamos.

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*System Manager*	ITS Rio. Responsible to support Mudamos and make it online.
2	*Mudamos users*	Brazilian citizens registered to vote who can propose draft bills or sign for existing ones.
3	*Legislative houses*	Brazilian legislative houses in any different level (city, state and national) where draft bills and signature are addressed for.
4	*Draft bill proponents*	People who propose draft bills to be supported through Mudamos platform.

Data and information		
Data	**Type**	**Description**
1	*Documents*	Electoral Personal Data (Name, Electoral ID, ZIP Code) PDF list containing signatures compilation
2	*Payment transactions*	N/A

Security and privacy

1. Verification process can be automatized

2. On going campaigns lists have personal data anonymized

3. Signature information can be changed by man in the middle attacks due to its verifiability by its signature hash and public key.

Main Success Scenario + expected time line

Description of DLT-based solution, which potentially will be created

Conditions (pre- or post-)

1.

Performance needs

What potential performance specs (frequency of use, transactions per second, confirmation time, sync time, etc.) are expected. What scalability, interoperability, reliability, accessibility needs exist.

Legal considerations

Currently, thanks to the Internet and other technologies, it is possible to collect signatures throughout Brazil and verify them automatically. Digital signatures already had their relevance recognized and used in common civic procedures, as instituted by the Presidency Act MPV 2200/2001, and in legal acts, as instituted by Law 11419/06. However, since the cost of obtaining official digital certificates is prohibitive, they did not gain widespread adoption and a mere .005% of Brazilians have them.

Digital signatures based on certificates issued by the Brazilian government have the advantage that they are legally binding, meaning any documents signed using those certificates are recognized by any authority as authentic for any purpose, from the recognition of a debt to real estate transactions. However, when we talk about political rights, we do not need signatures to be that strong because people's support of causes are the expression of their political desire, not legal intent. Signature campaigns need only ensure that signatories have the constitutional right to sign the draft bill and signatures only need to allow for public scrutiny to audit the political support given to the bill.

Taking this into account, Mudamos created a way to allow people to sign draft bills using self-issued certificates using their own smartphones. The technology stack used by Mudamos is the same used by certificate authorities to issue certificates, excluding the fact Mudamos is not a recognized authority to issue legally-binding certificates. That is to say, while Mudamos issued certificates cannot be used to authenticate a contract in court, nonetheless the signatures are technically unbreakable and verifiable and well-suited to the purpose of ascertaining citizen wishes but without the cost of doing through one of a handful of monopoly legal certificate providers. In short, Mudamos created a secure and affordable way for people to express themselves politically through digital means.

Risks

Despite all it has to offer, Mudamos's electronic signature is not a national standard and the major risk to the Mudamos project is the contesting of the validity of its signatures by legislative bodies or in courts. Actually, Mudamos is facing a challenge from the legislative house of the Federal District, where Mudamos signatures were not accepted in support of a citizen's initiative draft bill, which called for reducing the House budget. Since an electronic signature standard is not established by law or even by a House of Representatives rule, the decision whether or not to accept Mudamos signatures is discretionary. To mitigate this scenario, ITS drafted a report about citizen initiatives bills arguing that electronic signatures should be accepted based on the current legislation. In addition, the Mudamos team has been talking to congressmen and other leaders, pushing for legislation to standardize electronic signatures. The Mudamos legal framework is another approach to build dialogue bridges between technicians, activists, and legislative houses to support local and national legislative change.

Another risk faced by Mudamos is the adoption rate of the app (350,000 active users) in relation to the number of signatures required to propose a national level draft bill (1.5 million). Despite the fact that Mudamos had at least 4 viral waves since its launch, new user registrations are not growing at a substantial rate. Continuous engagement on Mudamos requires fostering internal variables, such as better user experience and strategic communication for action, and external variables, such as the participatory will of the people which leads to more interest in collaboration and representation in the political process. Mudamos launched its second major version (2.0) in January 2019, seeking user experience improvements, especially features to make campaigns sharing easier.

Mudamos started using public Blockchain as part of its technical architecture, aiming to create a completely transparent and accountable system for verifying signatures. However, after almost 2 years running, the Mudamos team realizes that the availability of this secure infrastructure where anyone can "look under the hood" does not de facto mean anyone is actually doing so. As with the volunteer lawyers, there is a need to develop an independent, crowdsourced technical governance mechanism to ensure that the system maintains its legitimacy.

Finally, the populist, right-wing president, Jair Bolsonaro elected in 2018, has expressed authoritarian tendencies. It is, thus far unknown, how changes in politics will impact political culture in Brazil in the near and longer-term. One can surmise that the trend in government toward more autocratic behavior could end up depressing political mobilization and participation. Or, to the contrary, Mudamos may become more popular than ever if it escapes legal challenge.

Special Requirements

Business and technical requirements of use case

External References and Miscellaneous

For a complete reference of Case Mudamos see: http://congress.crowd.law/case-mudamos.html

Other Notes

Any assumptions, issues

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)