OpenZeppelin

How to onboard 22 million users ~~overnight~~ using non-conventional cryptography

November 13th, 2024 | Devcon SEA, Bangkok, Thailand

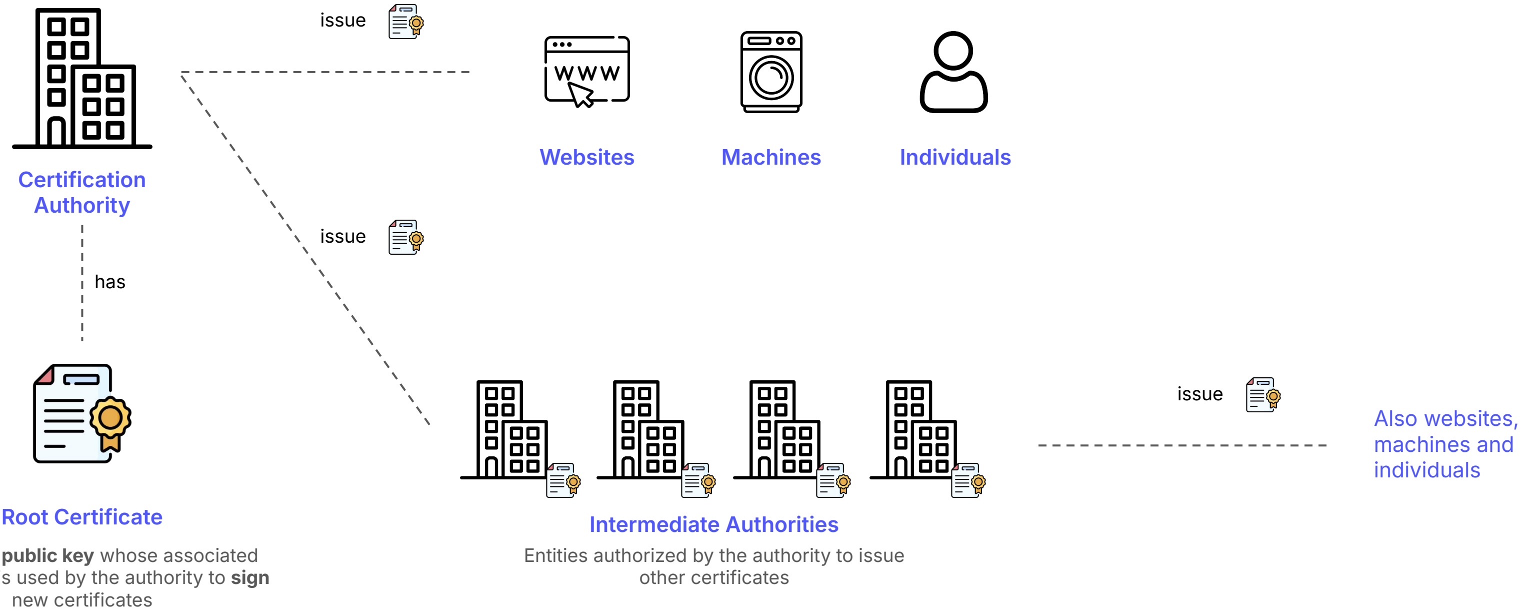
Agenda

1. A refresher on web2 cryptography
2. The Mexican case for digital signatures
3. Government cryptography in other countries

Public Key Infrastructures

A refresher on web2 cryptography

A refresher on web2 cryptography



Root Certificate

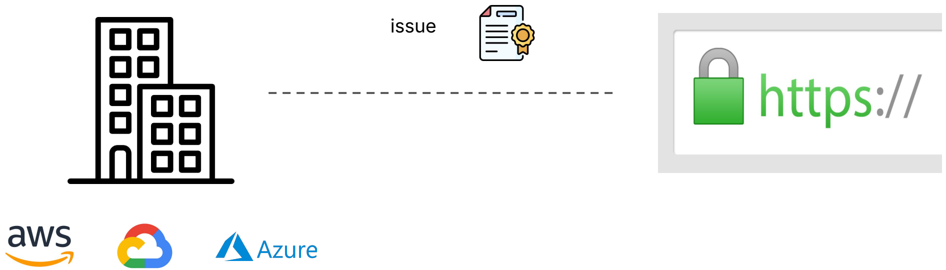
Certifies a **public key** whose associated private key is used by the authority to **sign** new certificates

Intermediate Authorities

Entities authorized by the authority to issue other certificates

Public Key Infrastructure

A refresher on web2 cryptography

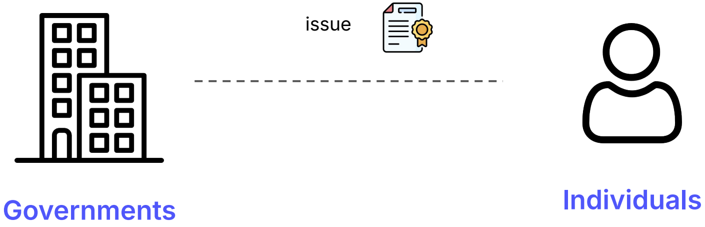


Most common Public Key Infrastructure use case is for Cloud Providers to issue TLS certificates.

These are behind the *"green lock"* and their security guarantees come from the provider.

The Mexican case for digital signatures

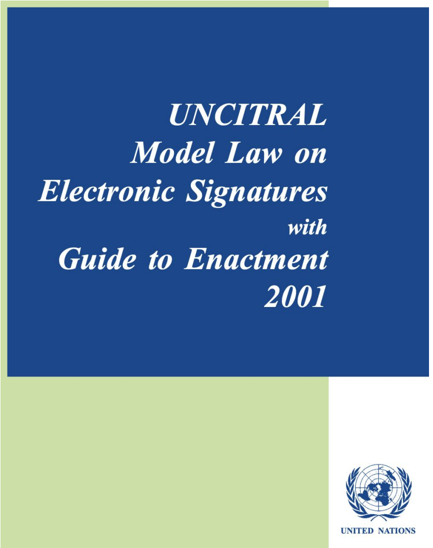
The Mexican case for digital signatures



issue

Governments

Individuals



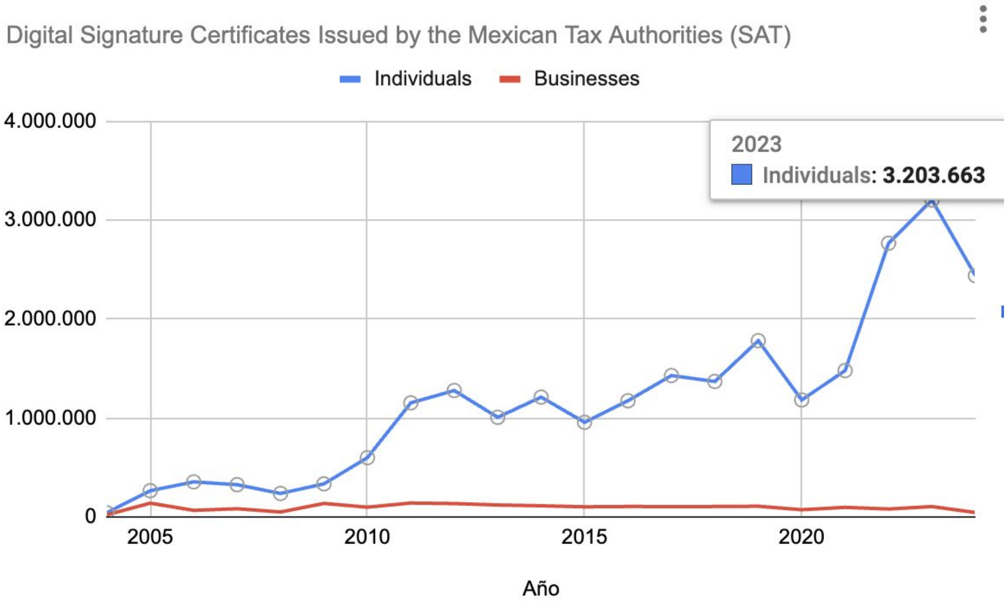
UNCITRAL
Model Law on
Electronic Signatures
with
Guide to Enactment
2001

UNITED NATIONS

Learn more

Public Key Infrastructures are used for governments to
distribute certified private keys to individuals

The Mexican case for digital signatures



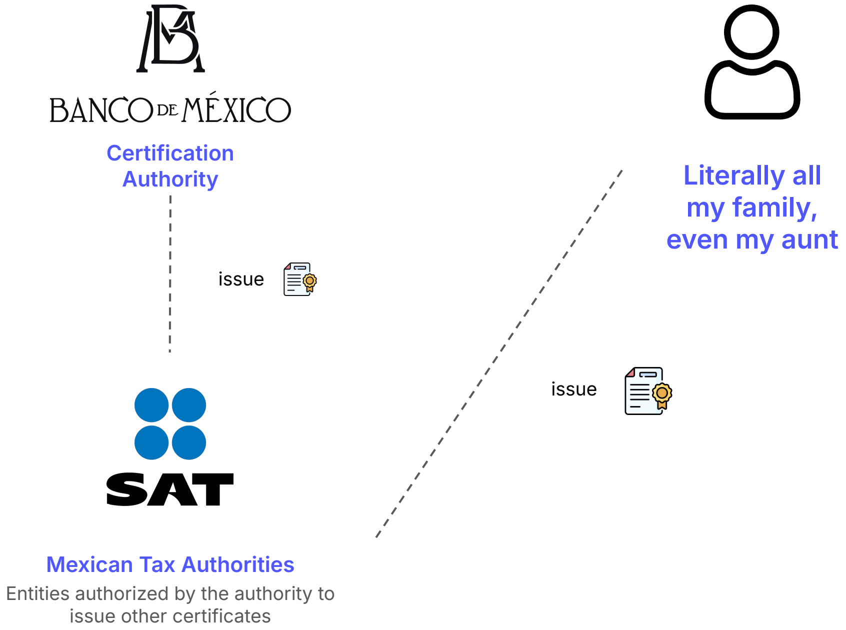
24,594,880

"Physical Person" Certificates

2,206,854

"Business Person" Certificates

The Mexican case for digital signatures



BANCO DE MÉXICO

Certification Authority

issue

SAT

Mexican Tax Authorities

Entities authorized by the authority to issue other certificates

issue

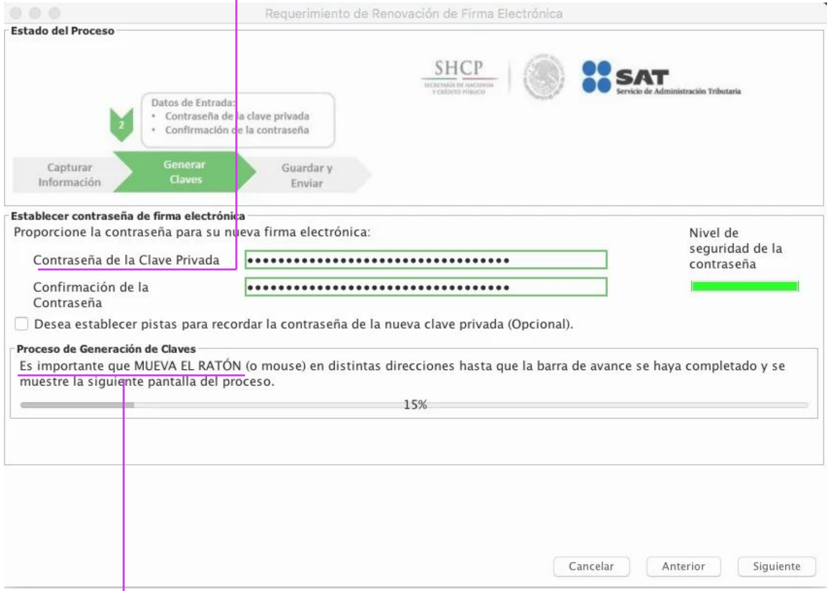
Literally all my family, even my aunt

Mexican learnt basic private key management with these keys.

Mostly misused, there are no tools to enable them to use them as **identity wallets**.

The Mexican case for digital signatures

Passphrases?!



Requerimiento de Renovación de Firma Electrónica
SHCP
SAT
Servicio de Administración Tributaria
Capturar Información
Generar Claves
Guardar y Enviar
Cancelar
Anterior
Siguiente

Estado del Proceso

Datos de Entrada:
- Contraseña de la clave privada
- Confirmación de la contraseña

Establecer contraseña de firma electrónica

Proporcione la contraseña para su nueva firma electrónica:

Contraseña de la Clave Privada	•••••••••••••••••••••••••••••••••••
Confirmación de la Contraseña	•••••••••••••••••••••••••••••••••••

Nivel de seguridad de la contraseña

□ Desea establecer pistas para recordar la contraseña de la nueva clave privada (Opcional).

Proceso de Generación de Claves

Es importante que MUEVA EL RATÓN (o mouse) en distintas direcciones hasta que la barra de avance se haya completado y se muestre la siguiente pantalla del proceso.

15%

IT IS IMPORTANT TO ***MOVE THE MOUSE****... to generate randomness locally*

Let's onboard people to crypto
Actually, In Mexico government cryptography is the most understood and widely accepted yet still self-sovereign enough to use with technologies like Account Abstraction

Go build it, anon

Government cryptography in other countries

Government cryptography in other countries

- Afghanistan
- Antigua and Barbuda (a,c)
- Barbados
- Bhutan
- Botswana
- Cabo Verde
- China
- Colombia
- Costa Rica (a)
- Gambia
- Ghana
- Grenada
- Guatemala
- Honduras
- India (a)
- Jamaica
- Libya (a)
- Madagascar
- Maldives
- Mexico
- Nicaragua (a)
- Oman (a)
- Papua New Guinea
- Paraguay (a,c)
- Peru (a)
- Qatar
- Rwanda
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent and the Grenadines
- San Marino
- Saudi Arabia (a)
- Thailand
- Timor Leste
- Trinidad and Tobago
- Uganda
- United Arab Emirates
- United Kingdom of Great Britain and Northern Ireland
    - Anguila (b)
    - British Virgin Islands (b)
    - Montserrat (b)
- Viet Nam
- Zambia

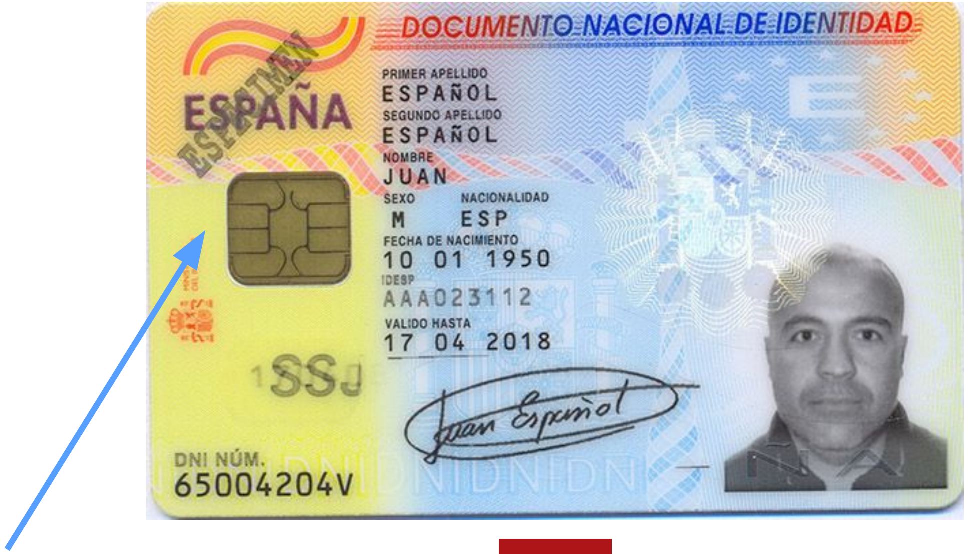
(a) The legislation is influenced by the Model Law and the principles on which it is based.
(b) Overseas territory of the United Kingdom of Great Britain and Northern Ireland.
(c) The legislation amends previous legislation based on the Model Law.

Government cryptography in other countries

Several countries use some sort of cryptographic signatures already KYC'd

All these people can use Ethereum and connect to a global financial system **now.**

Issue? Most are RSA keys, an algorithm no longer recommended by the NSA



DOCUMENTO NACIONAL DE IDENTIDAD

ESPAÑA

ESPECIMEN

PRIMER APELLIDO
ESPAÑOL

SEGUNDO APELLIDO
ESPAÑOL

NOMBRE
JUAN

SEXO M

NACIONALIDAD ESP

FECHA DE NACIMIENTO
10 01 1950

IDESP
AAA023112

VALIDO HASTA
17 04 2018

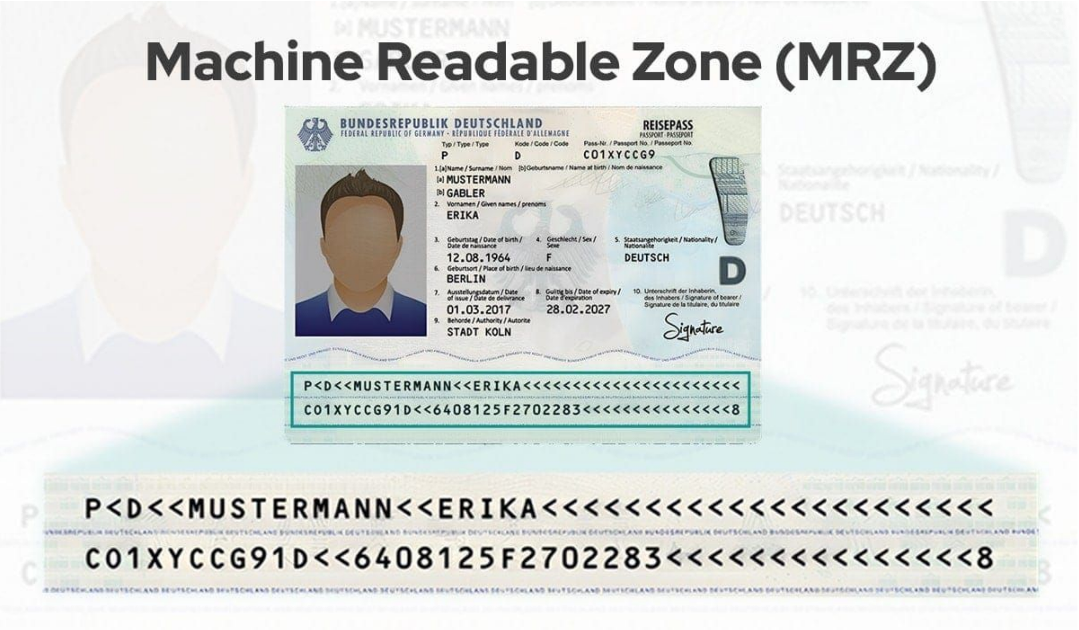
Juan Español

DNI NÚM.
65004204V

Private Key and Certificate

Government cryptography in other countries

Instead, we'd been AI-scanning MZR codes instead of just **using the cryptography.**



Machine Readable Zone (MRZ)

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY · RÉPUBLIQUE FÉDÉRALE D'ALLEMAGNE

REISEPASS
PASSPORT · PASSEPORT

Typ / Type / Type: P
Kode / Code / Code: D
Pass-Nr. / Passport No. / Passeport No.: C01XYCCG9

1. [a] Name / Surname / Nom [b] Geburtsname / Name at birth / Nom de naissance
[a] MUSTERMANN
[b] GABLER

2. Vornamen / Given names / prenoms
ERIKA

3. Geburtstag / Date of birth / Date de naissance
12.08.1964

4. Geschlecht / Sex / Sexe
F

5. Staatsangehorigkeit / Nationality / Nationalite
DEUTSCH

D

6. Geburtsort / Place of birth / lieu de naissance
BERLIN

7. Ausstellungsdatum / Date of issue / Date de delivrance
01.03.2017

8. Gultig bis / Date of expiry / Date d'expiration
28.02.2027

9. Behorde / Authority / Autorite
STADT KOLN

10. Unterschrift der Inhaberin, des Inhabers / Signature of bearer / Signature de la titulaire, du titulaire
Signature

```
P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<
C01XYCCG91D<<6408125F2702283<<<<<<<<<<<<<<<8
```

```
P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<
C01XYCCG91D<<6408125F2702283<<<<<<<<<<<<<<<8
```

Use the cryptography

Thank You.

Ernesto García

ernesto@openzeppelin.com

OpenZeppelin