# eWebAPI: uma API para assinar digitalmente lotes de certificados eletrônicos utilizando o e-certsDS

Alan Schulze, Diego Kreutz

Universidade Federal do Pampa

# Gestão de Certificados Eletrônicos

| Nome | Características | Limitações |
|---|---|---|
| Certifier | API, Customização | Pago, assinaturas digitais. |
| Gerador de Certificados | Importação de CSV, Customização | Pago, assinaturas digitais, API, validação. |
| Doity | Customização, Validação. | Pago, assinaturas digitais, API. |
| SGCE | Validação, Gratuito. | Assinaturas digitais, API. |

# Gestão de Certificados Eletrônicos

| Nome | Características | Limitações |
|---|---|---|
| Certifier | API, Customização | **Pago**, assinaturas digitais. |
| Gerador de Certificados | Importação de CSV, Customização | **Pago**, assinaturas digitais, API, validação. |
| Doity | Customização, Validação. | **Pago**, assinaturas digitais, API. |
| SGCE | Validação, Gratuito. | Assinaturas digitais, API. |

# Gestão de Certificados Eletrônicos

| Nome | Características | Limitações |
|---|---|---|
| Certifier | API, Customização | Pago, **assinaturas digitais**. |
| Gerador de Certificados | Importação de CSV, Customização | Pago, **assinaturas digitais**, API, validação. |
| Doity | Customização, Validação. | Pago, **assinaturas digitais**, API. |
| SGCE | Validação, Gratuito. | **Assinaturas digitais**, API. |

# Gestão de Certificados Eletrônicos

| Nome | Características | Limitações |
|---|---|---|
| Certifier | API, Customização | Pago, assinaturas digitais. |
| Gerador de Certificados | Importação de CSV, Customização | Pago, assinaturas digitais, **API**, validação. |
| Doity | Customização, Validação. | Pago, assinaturas digitais, **API**. |
| SGCE | Validação, Gratuito. | Assinaturas digitais, **API**. |

# E-certsDS

- Permite assinaturas digitais (OpenPGP)


e-CertsDS

# E-certsDS

- Permite assinaturas digitais (OpenPGP)
- Software gratuito


e-CertsDS

# E-certsDS

- Permite assinaturas digitais (OpenPGP)
- Software gratuito
- *Open Source*


e-CertsDS

# E-certsDS

- Permite assinaturas digitais (OpenPGP)
- Software gratuito
- *Open Source*
- Ilimitado (N° de CE's)

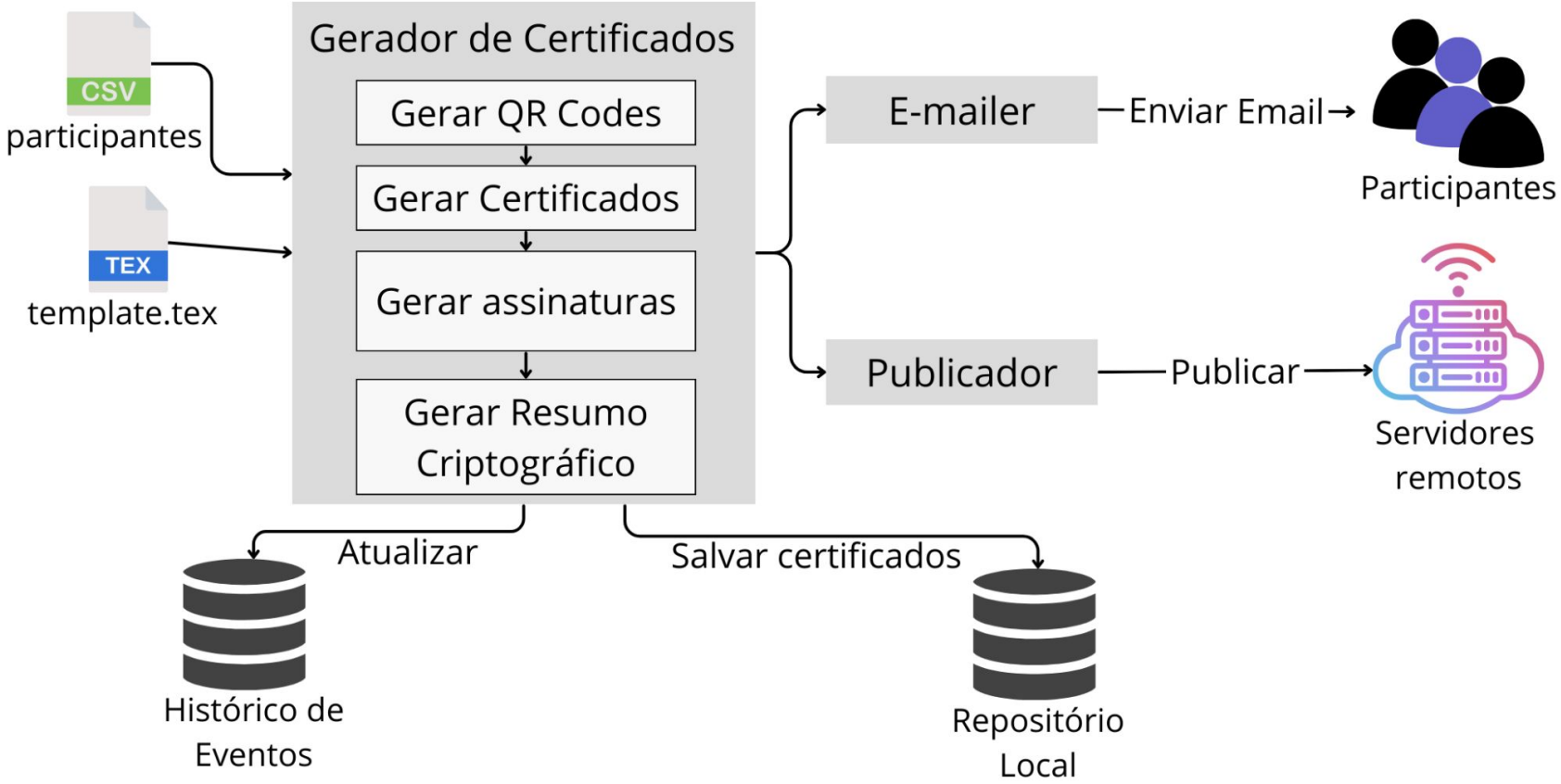

e-CertsDS

# E-certsDS

- Permite assinaturas digitais (OpenPGP)
- Software gratuito
- *Open Source*
- Ilimitado (N° de CE's)
- Customização


e-CertsDS

# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
Gerar Resumo Criptográfico
E-mailer
Enviar Email
Participantes
Publicador
Publicar
Servidores remotos
Atualizar
Salvar certificados
Histórico de Eventos
Repositório Local

# E-certsDS


participantes.csv


template.tex

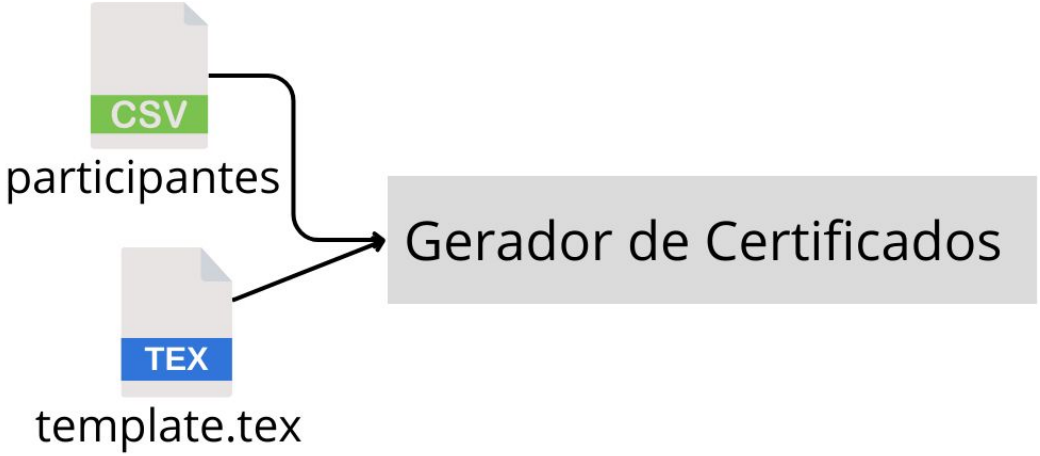
# E-certsDS


participantes.csv

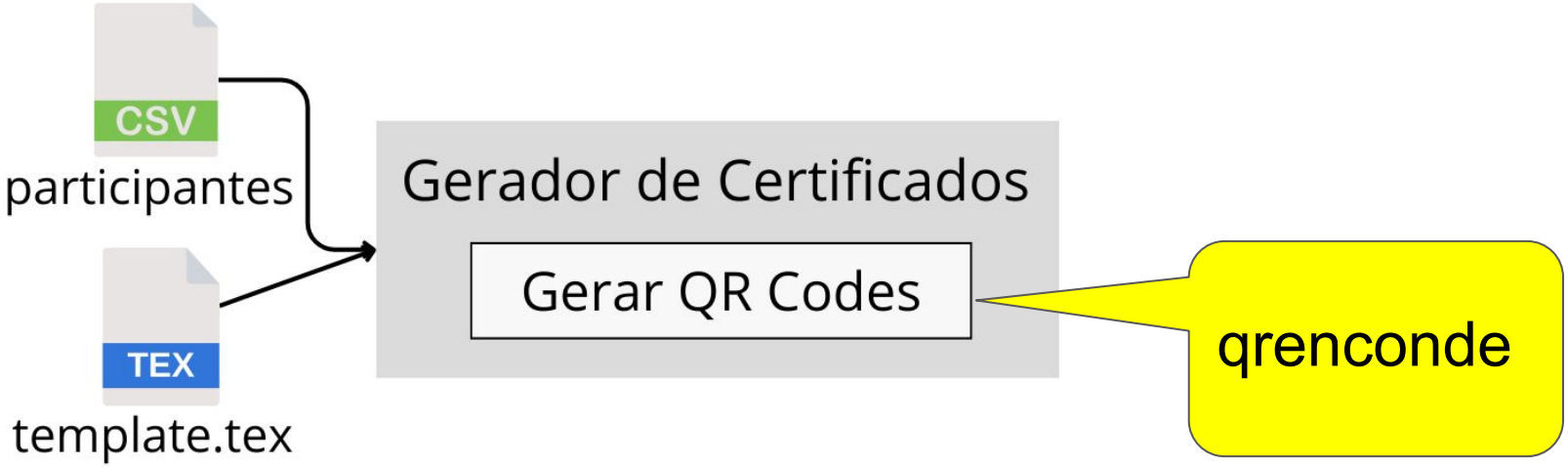

template.tex

```
Alice Silva,alice@gmail.com,Co-Organizador,1
Bob Souza,bob@gmail.com,Ouvinte,2
Eve Martins,eve@gmail.com,Ouvinte,2
Charles Pinha,charles@gmail.com,Palestrante,2
Eder Soares,eder@gmail.com,Colaborador,1
João Bento,joao@gmail.com,Co-Organizador,1
Chico Costa,chico@gmail.com,Convidado Especial,2
```

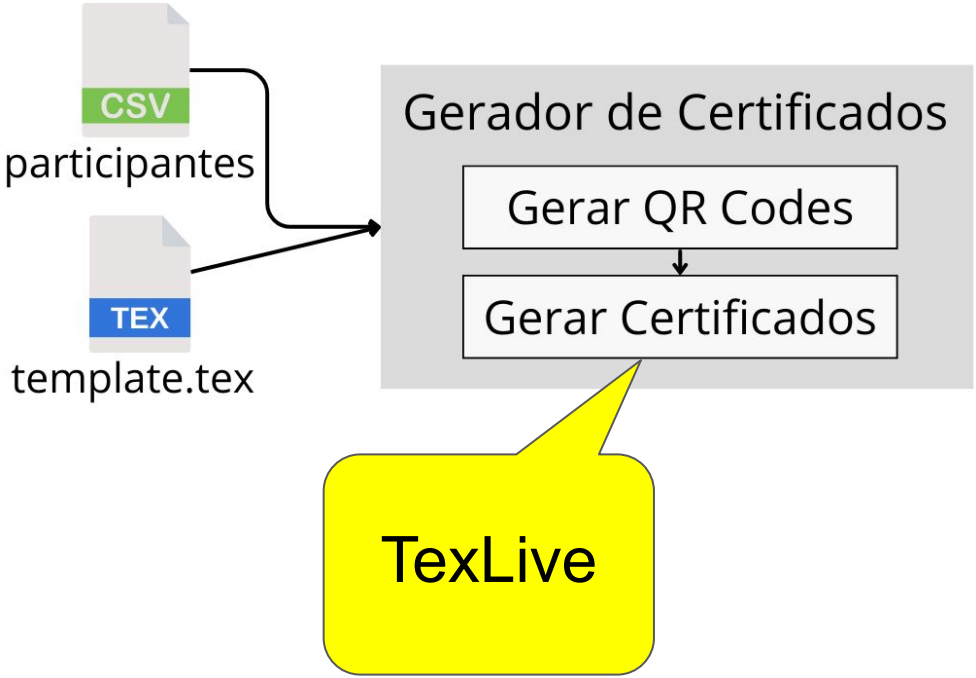
# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados

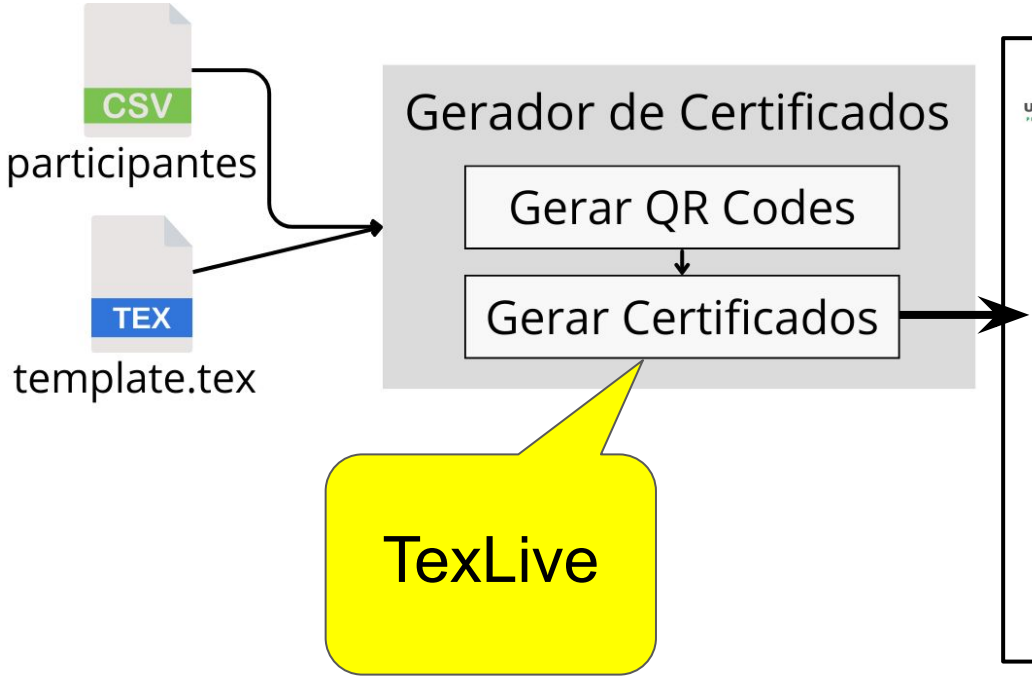
# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
qrenconde

# E-certsDS

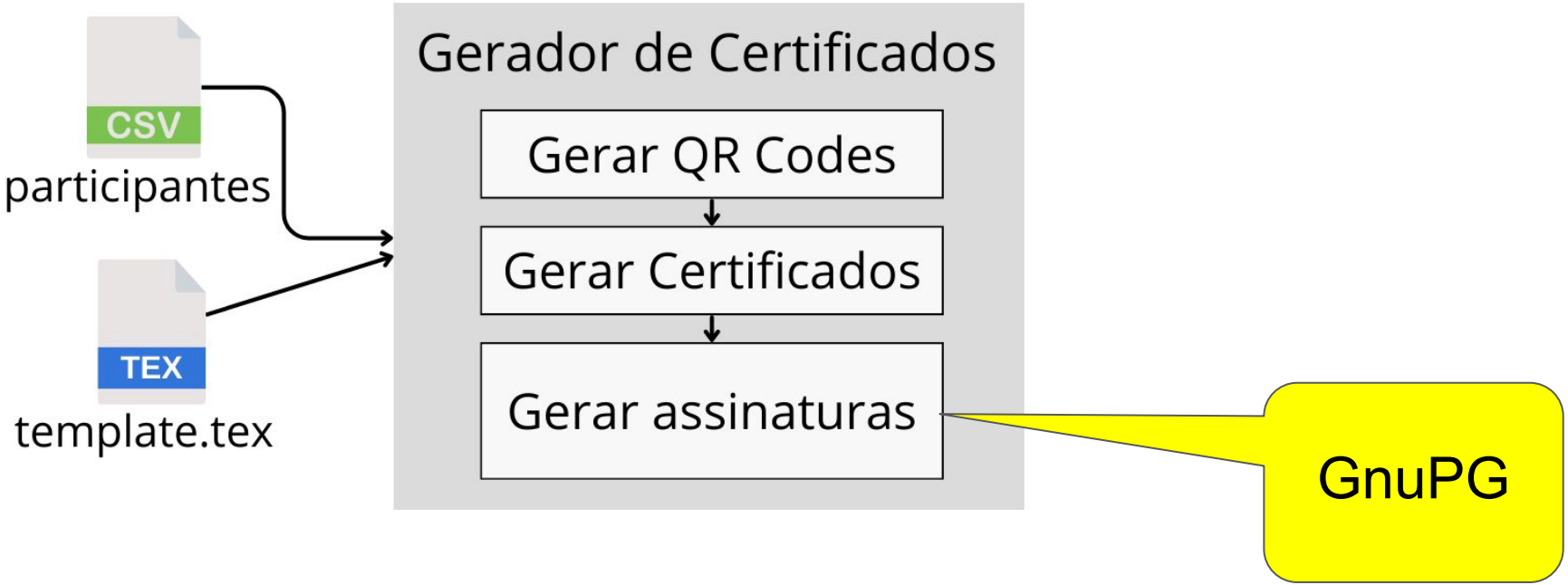

CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
TexLive

# E-certsDS

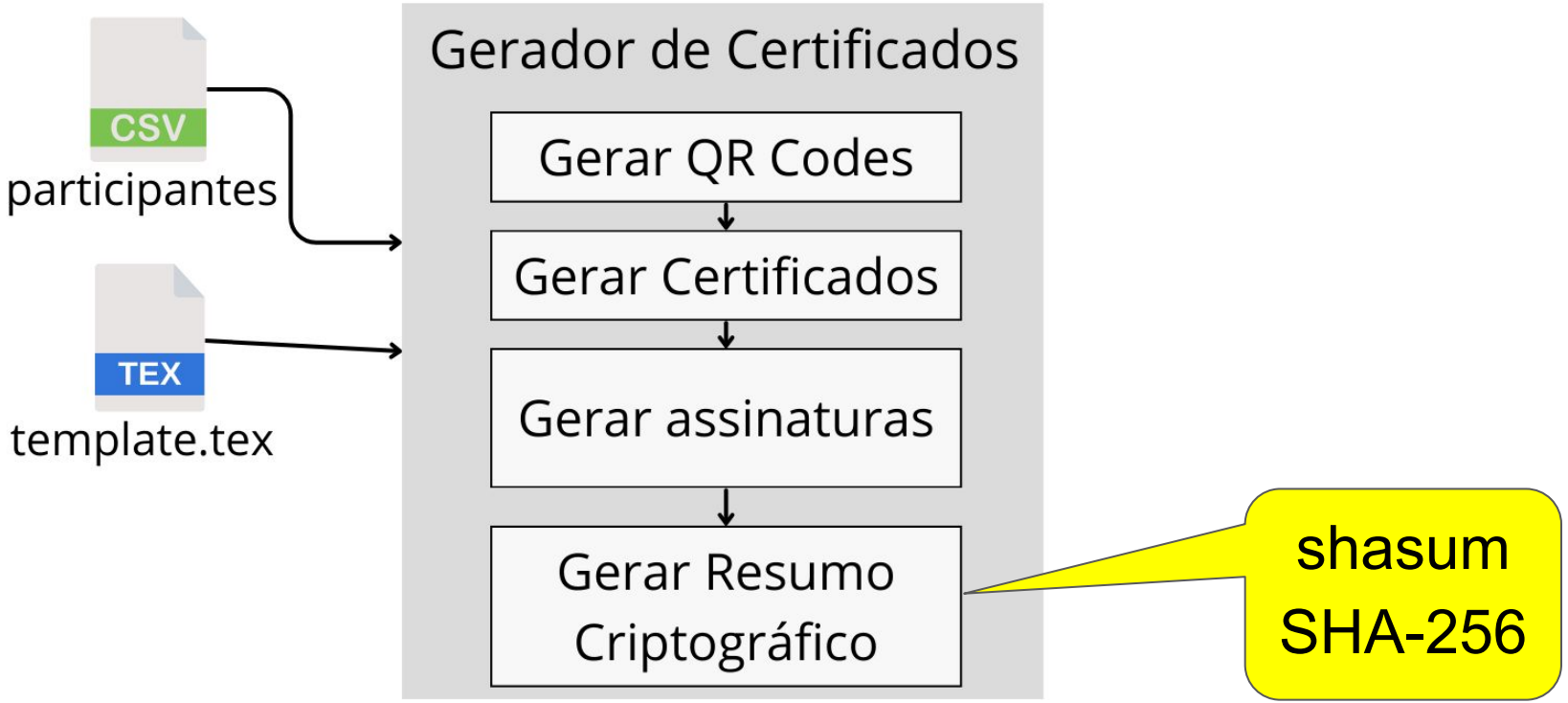

CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
TexLive


UNIHACKER.CLUB
Clube Universidade Hacker
UNIHACKER.CLUB
Série TechTalks: 2a DevApps (Design, Prototipação e Usabilidade de Apps Mobile), em
parceria com o Programa UniHacker.Club, realizada dia 11/06/2020, às 19:00.
Certificado de PARTICIPANTE
para Maurício Mendonça El Uri
(2 hora(s) de atividades)
Diego Kreutz
Organizador
kreutz@unipampa.edu.br
Brandow Buenos
Colaborador
brandowbuenos@gmail.com
E-mail: info@unihacker.club Web: https://unihacker.club

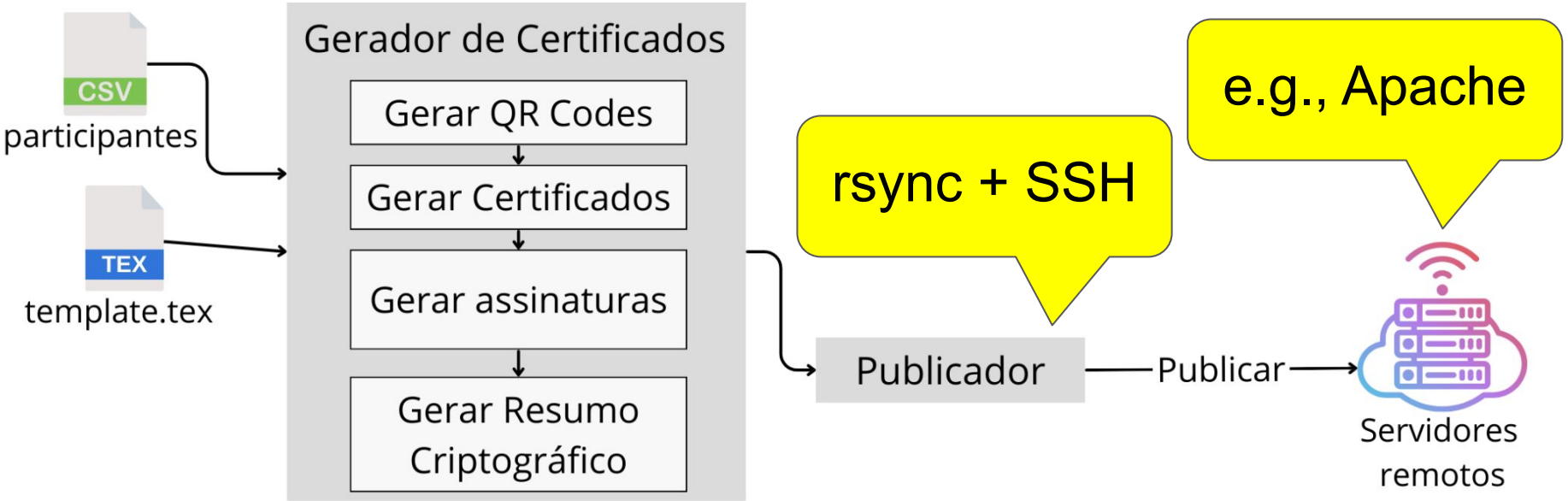
# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
GnuPG

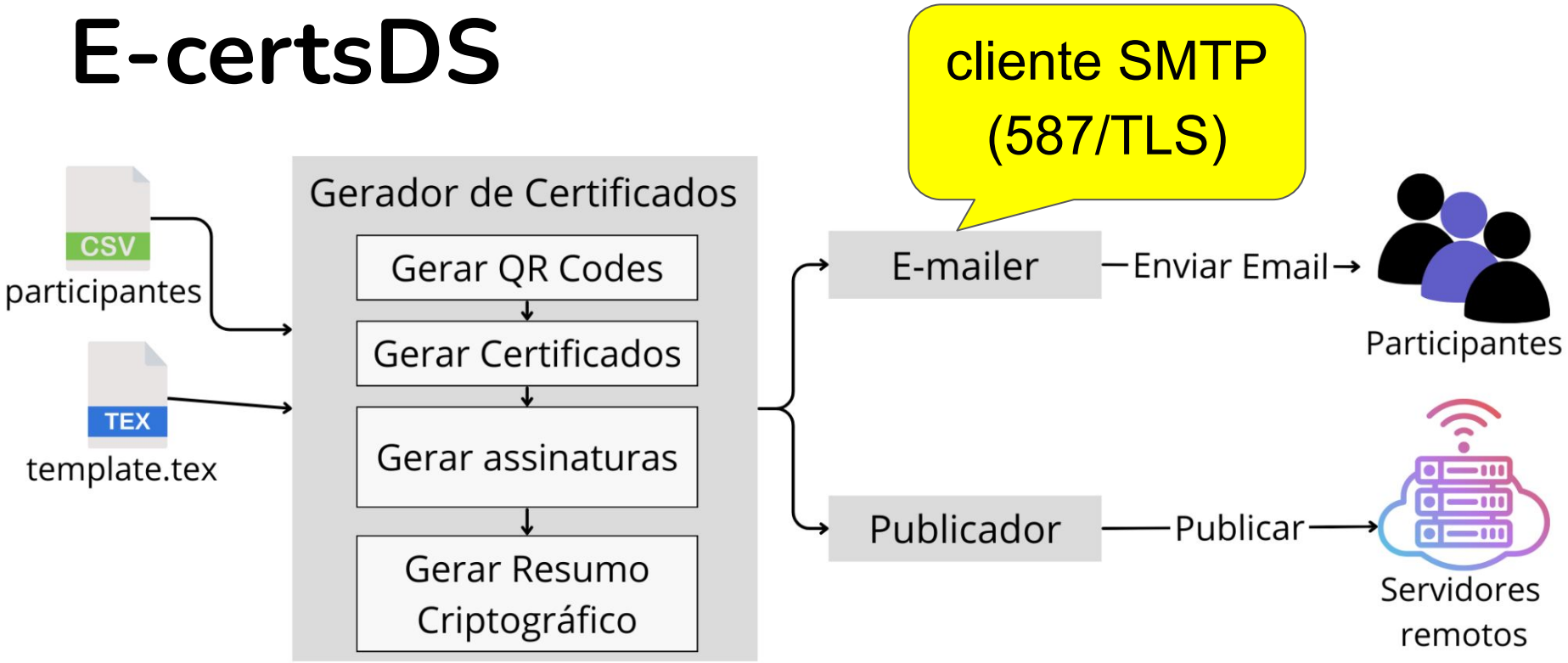
# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
Gerar Resumo Criptográfico
shasum
SHA-256

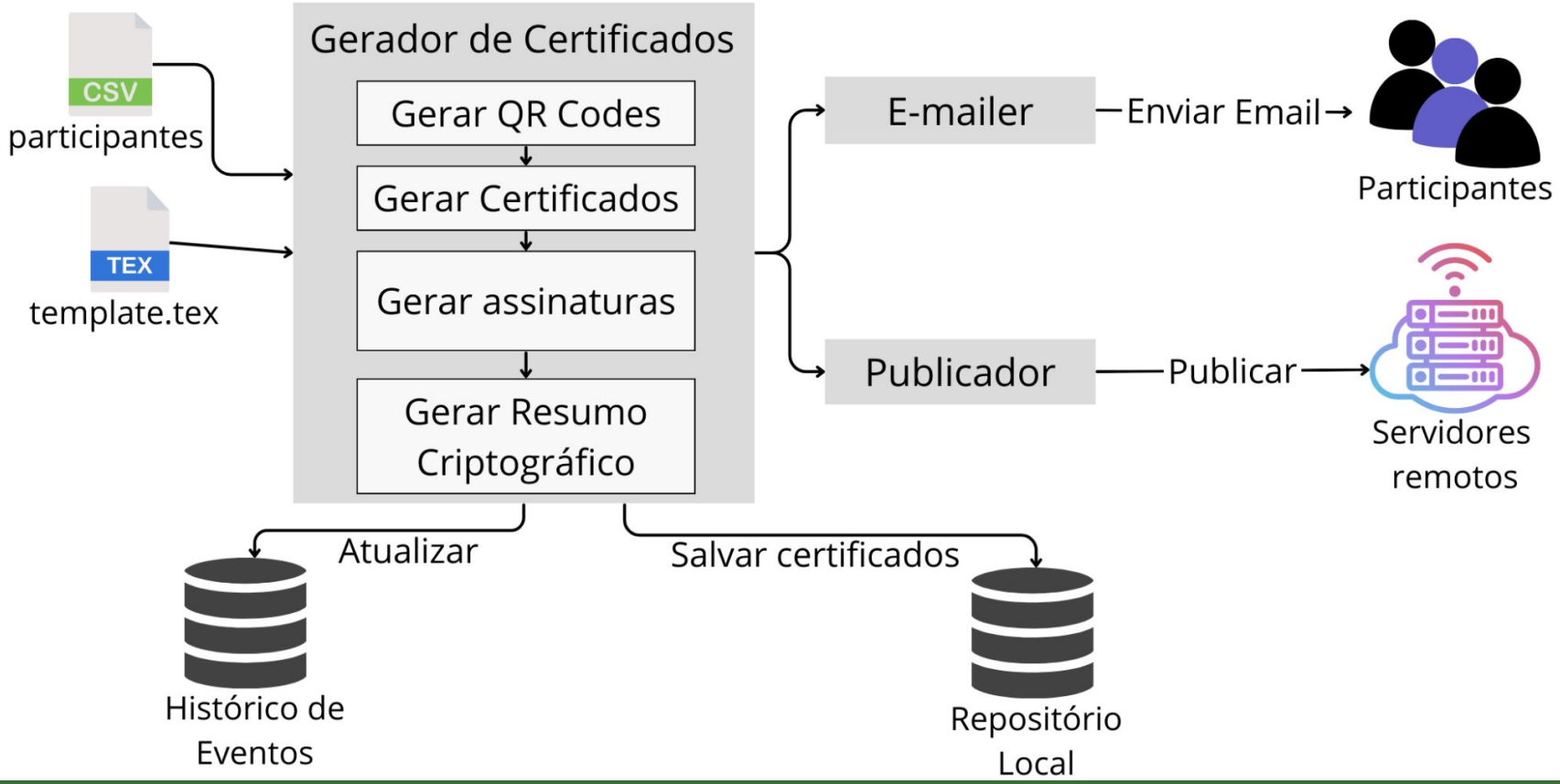
# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
Gerar Resumo Criptográfico
rsync + SSH
e.g., Apache
Publicador
Publicar
Servidores remotos

# E-certsDS


cliente SMTP
(587/TLS)
CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
Gerar Resumo Criptográfico
E-mailer
Enviar Email
Participantes
Publicador
Publicar
Servidores remotos

# E-certsDS


CSV
participantes
TEX
template.tex
Gerador de Certificados
Gerar QR Codes
Gerar Certificados
Gerar assinaturas
Gerar Resumo Criptográfico
E-mailer
Enviar Email
Participantes
Publicador
Publicar
Servidores remotos
Atualizar
Salvar certificados
Histórico de Eventos
Repositório Local

# E-certsDS - Limitações

- Usabilidade e complexidade

# E-certsDS - Limitações

- Usabilidade e complexidade
  - linha de comando

# E-certsDS - Limitações

- Usabilidade e complexidade
  - linha de comando
  - dependências: ferramentas
    - gnupg, qrencode, shasum, ssh, ...

# E-certsDS - Limitações

- Usabilidade e complexidade
  - linha de comando
  - dependências: ferramentas
    - gnupg, qrencode, shasum, ssh, ...
  - dependências: bibliotecas
    - várias dezenas de pacotes

# E-certsDS - Limitações

- Usabilidade e complexidade
  - linha de comando
  - dependências: ferramentas
    - gnupg, qrencode, shasum, ssh, ...
  - dependências: bibliotecas
    - várias dezenas de pacotes
- Diagnóstico de erros

# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

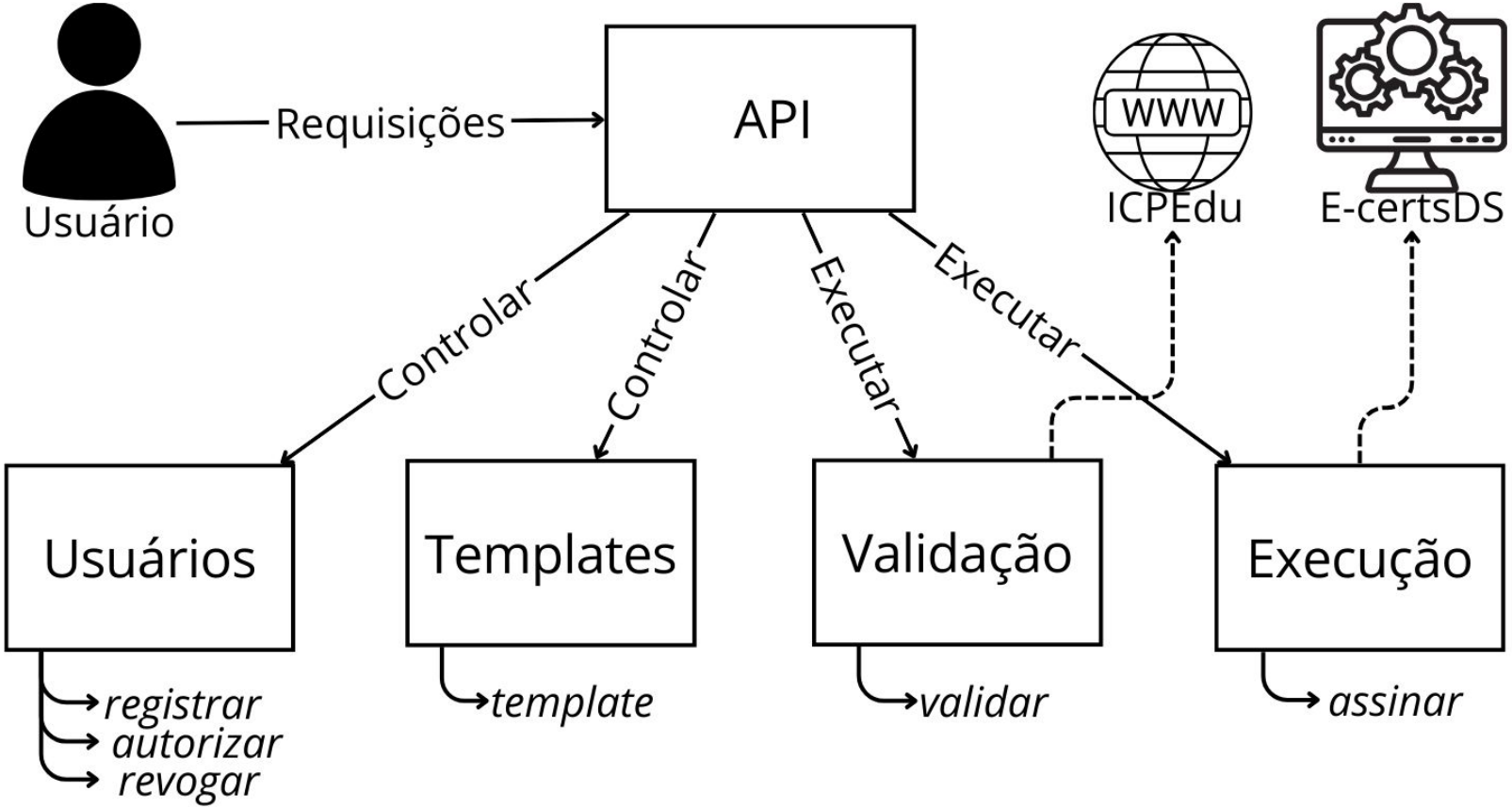
# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

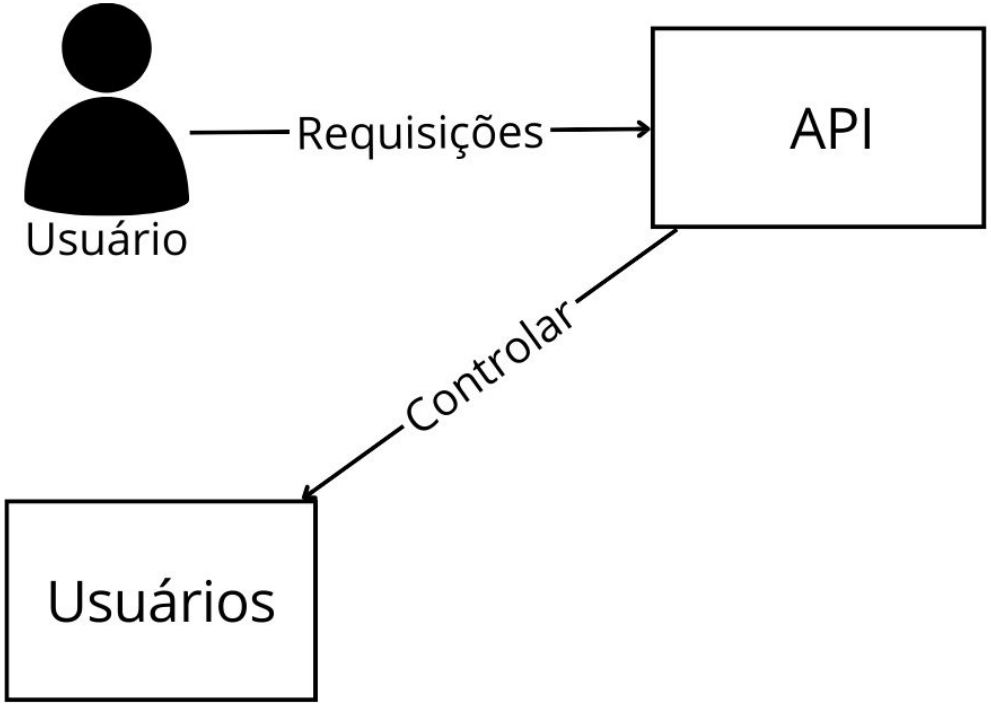
# Proposta: eWebAPI

- e-certsDS como um serviço
- Simplificar a utilização
- Viabilizar a integração com sistemas
- Utilizar certificados PKCS (e.g., ICPEdu)
- Disponibilizar novos recursos
  - e.g., validação de certificados
- Facilitar diagnóstico de erros

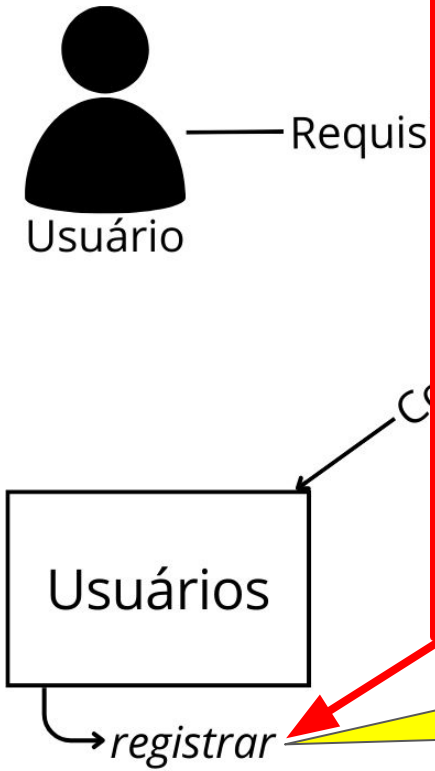
# eWebAPI: visão geral



# eWebAPI



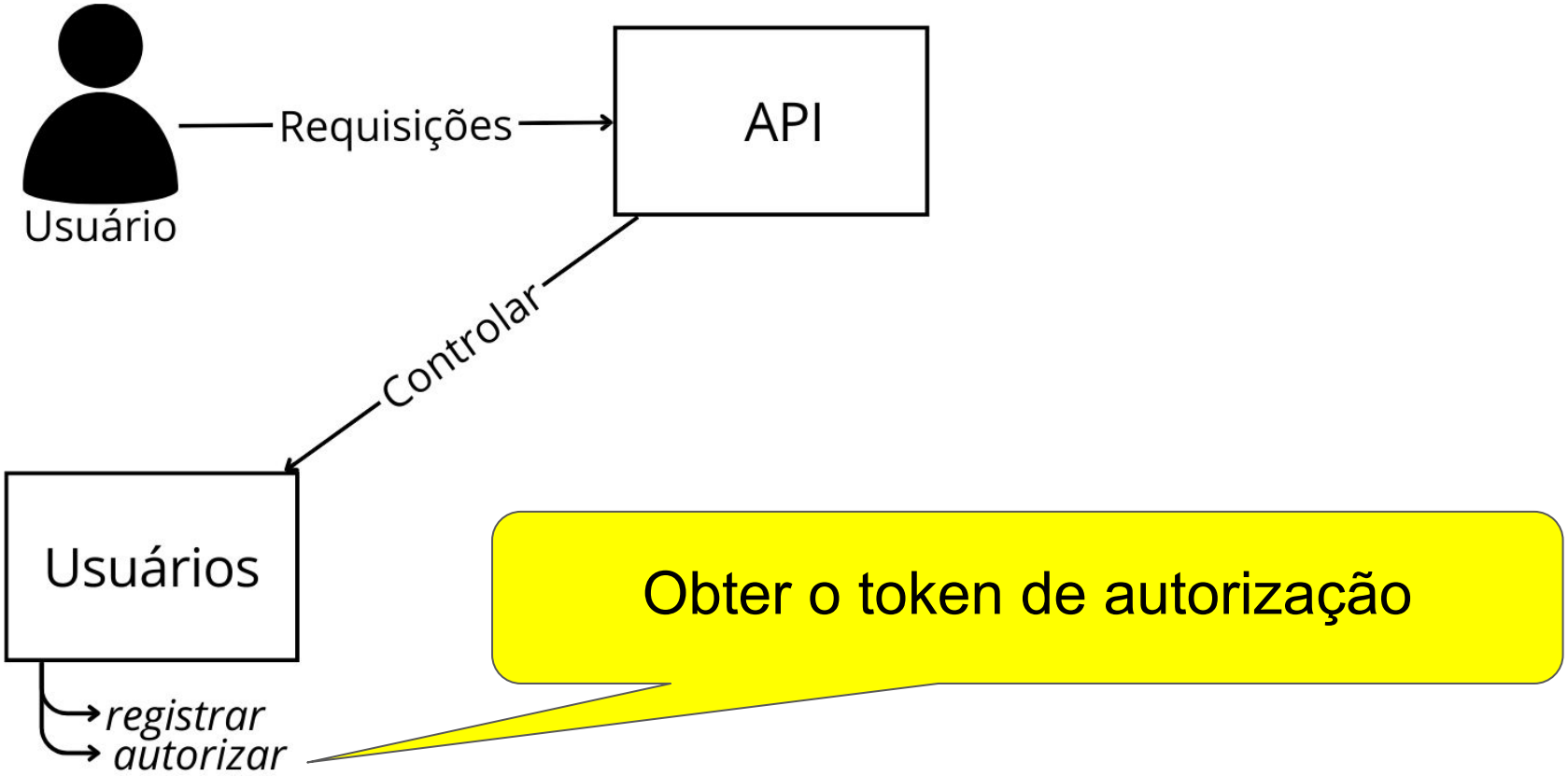
# eWebAPI



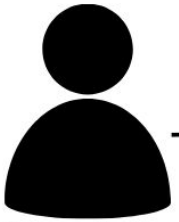

```
{
  "token": "1t53HGaF64Ok1WKsL2jxb1J",
  "dados": {
    "nome": "Adm 1",
    "email": "adm@gmail.com"
  },
  "chave-publica": "MEgCQQCo9+BpMRYQ/
    /Qp8eFhnii7NT7fELilKUSnxS30WAvQCC
}
```

Cadastrar novos usuários

# eWebAPI


Usuário
Requisições
API
Controlar
Usuários
registrar
autorizar
Obter o token de autorização

# eWebAPI



Usuário

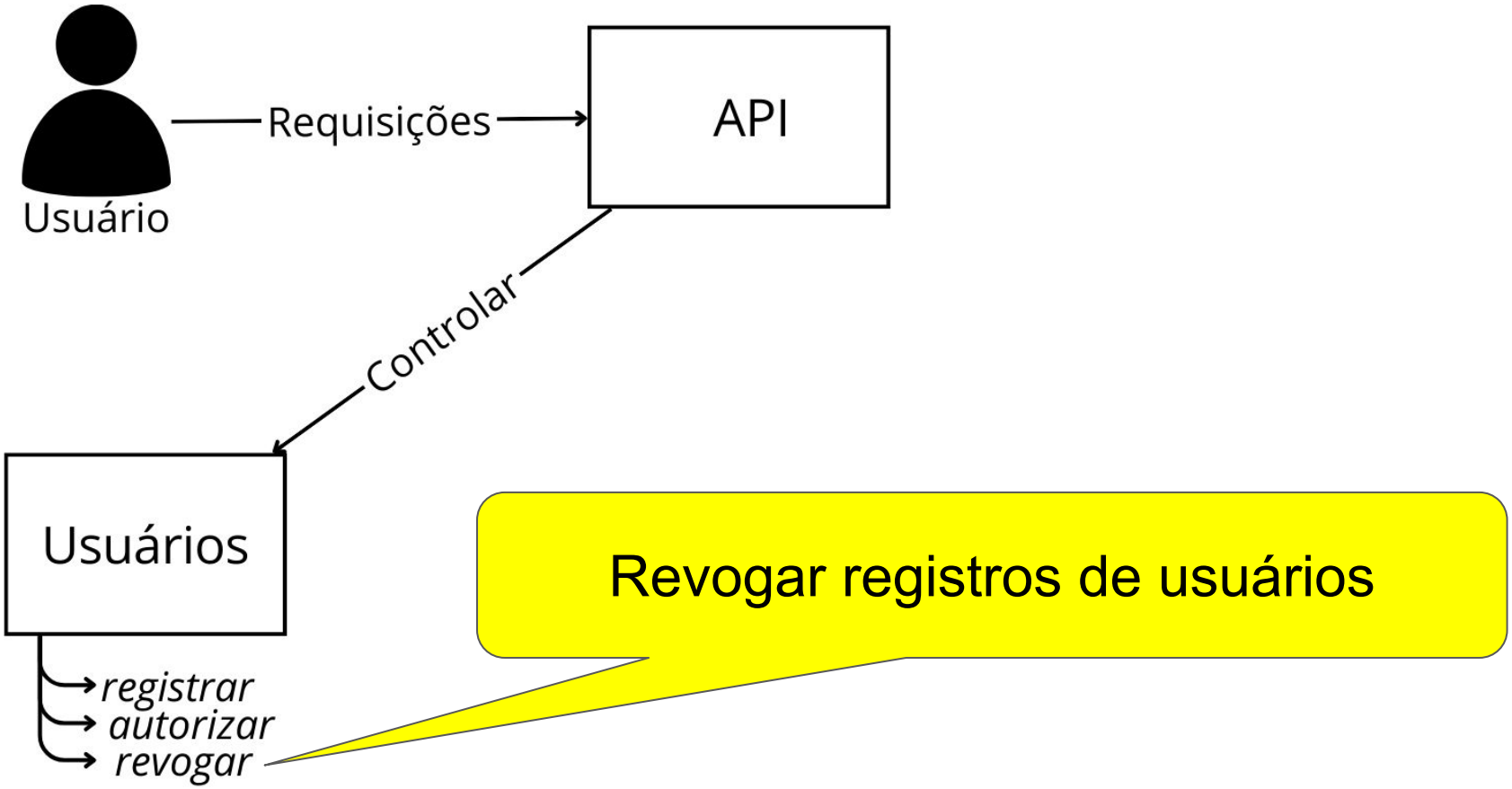
```
{
    "id": "adm@gmail.com",
    "nonce": "4smdj10z91zh",
    "assinatura": "gjq8c8192nd291nA912AZ0"
}
```

Usuários

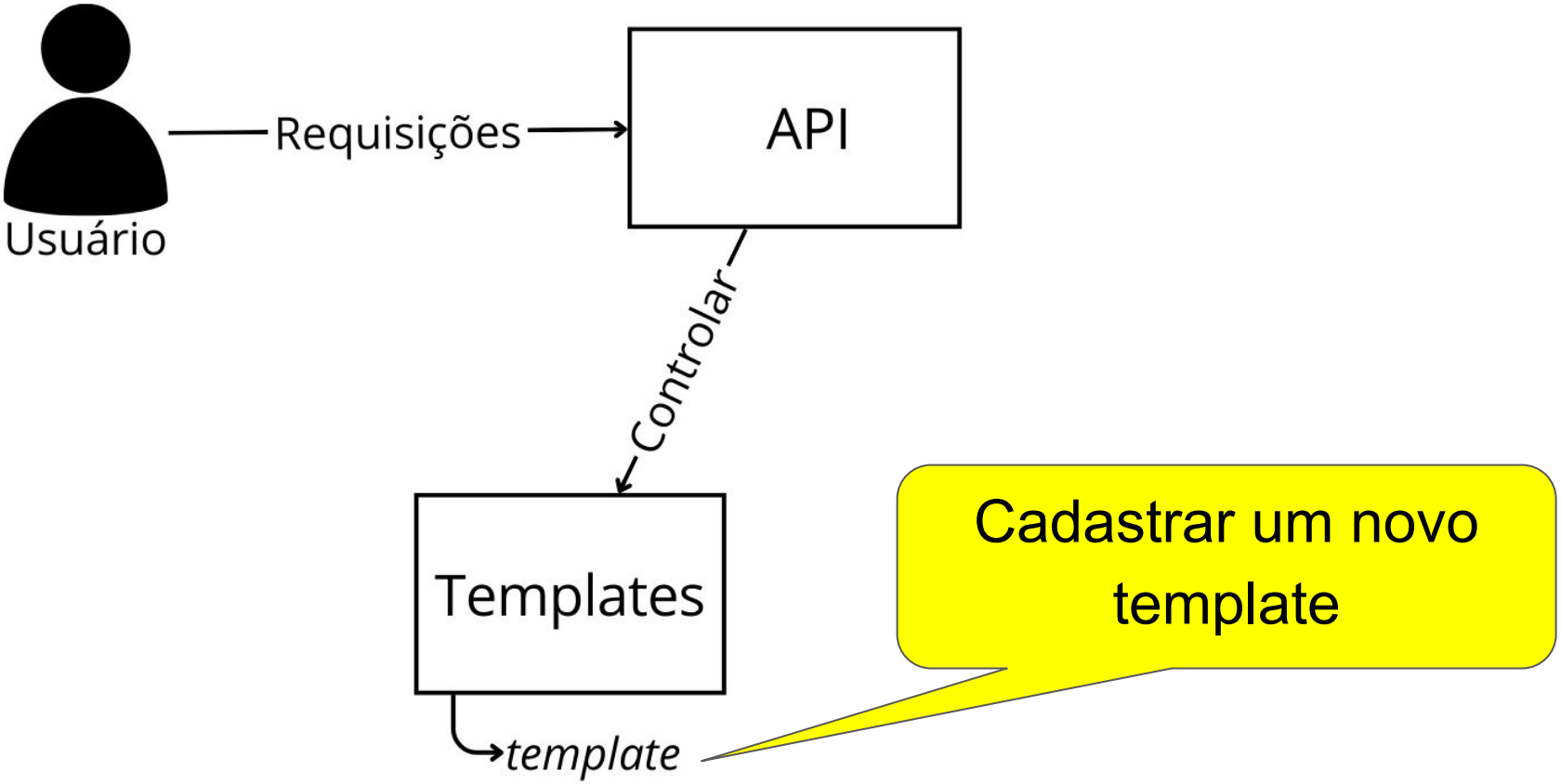
*registrar*
*autorizar*

Obter o token de autorização

# eWebAPI


Usuário
Requisições
API
Controlar
Usuários
registrar
autorizar
revogar
Revogar registros de usuários

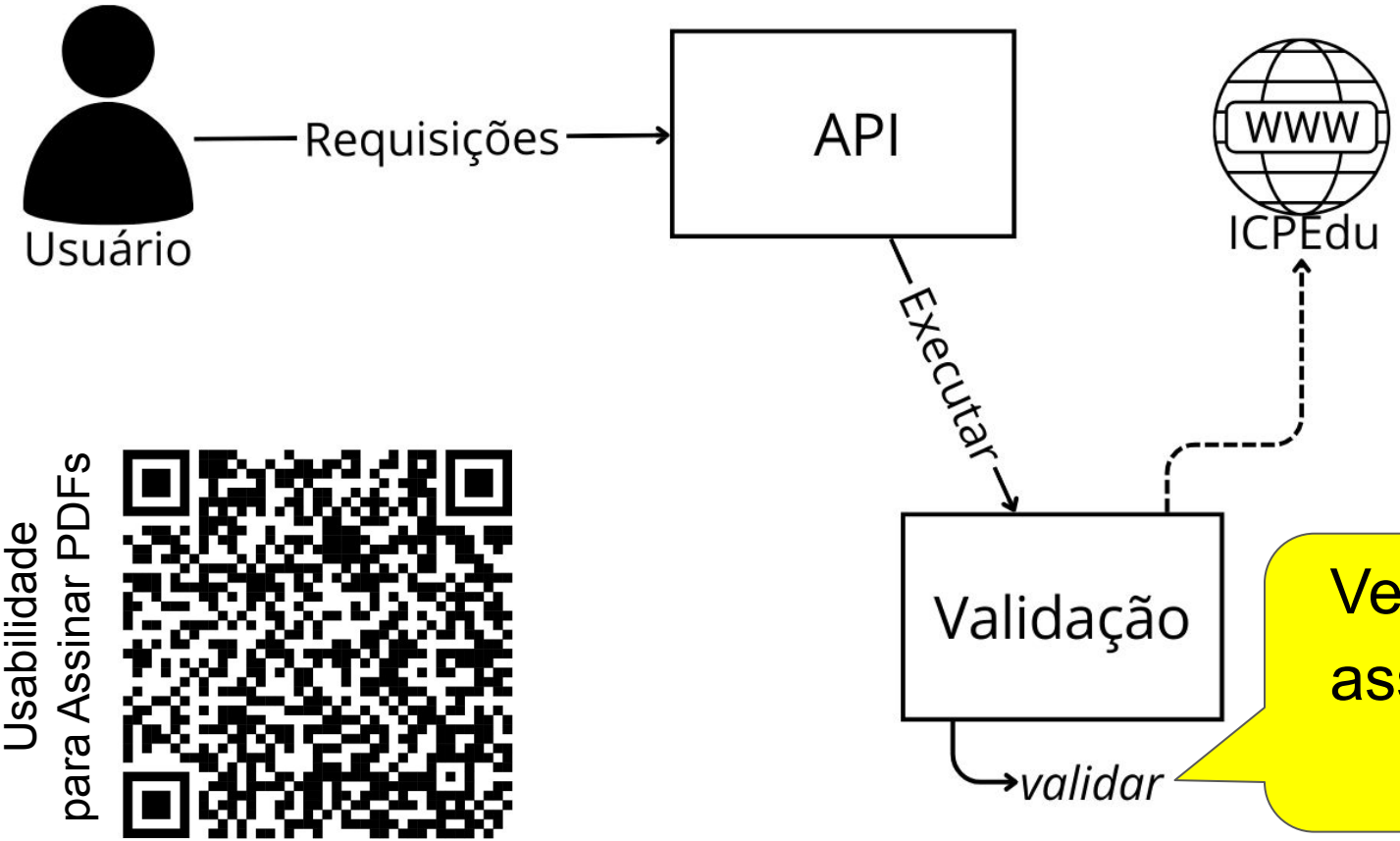
# eWebAPI


Usuário
Requisições
API
Controlar
Templates
template
Cadastrar um novo template

# eWebAPI

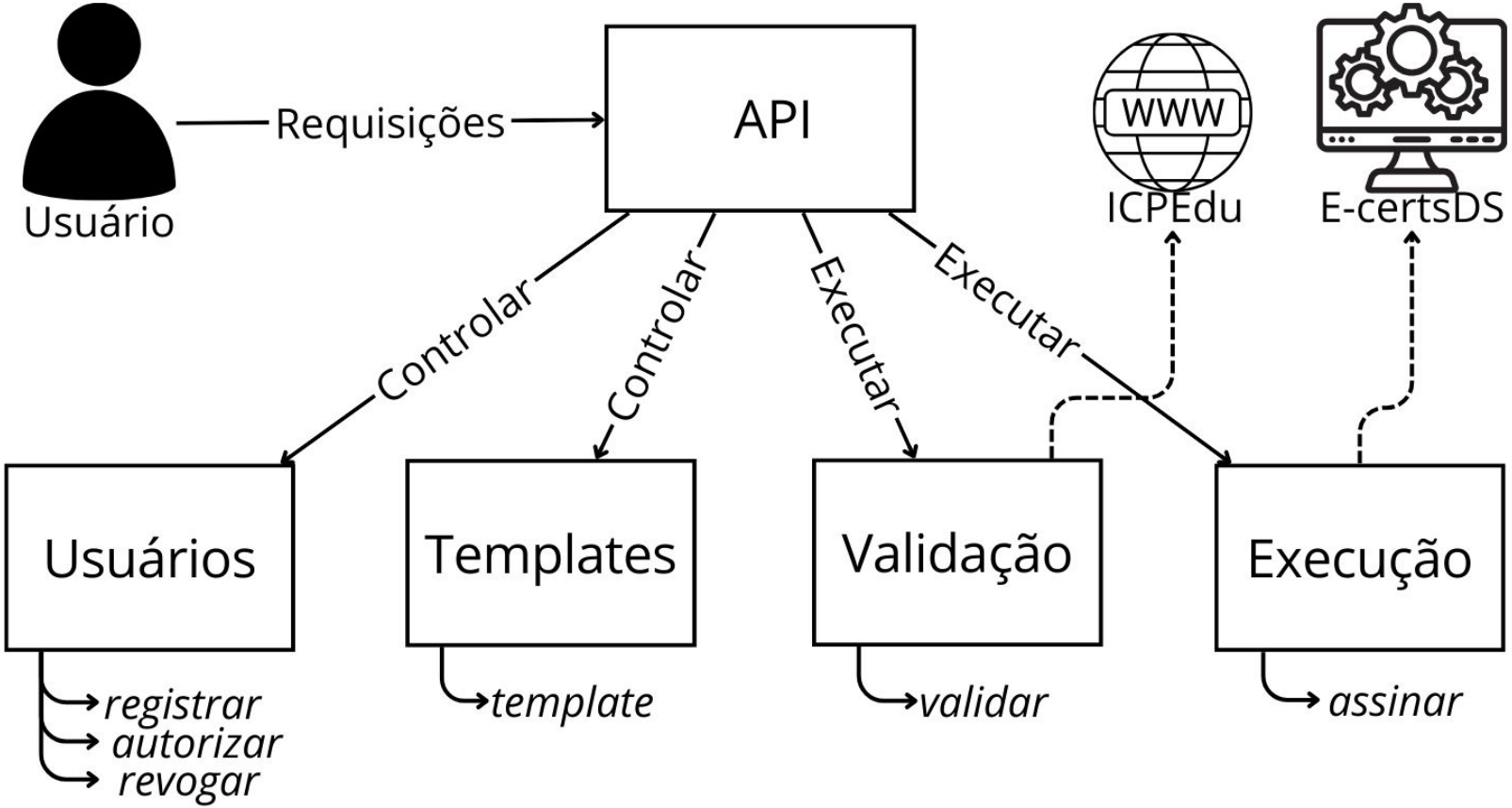

```
{
  "token": "A5bR1fG9KtP2zN7xM3d",
  "participantes": [
    {
      "nome": "Participante 1",
      "email": "part1@gmail.com",
      "tipo": "ouvinte",
      "horas": 2.5
    }
  ],
  "evento": "WRSeg 2023",
  "template": "template_wrseg.tex"
}
```

# eWebAPI




Usabilidade para Assinar PDFs

# eWebAPI: visão geral



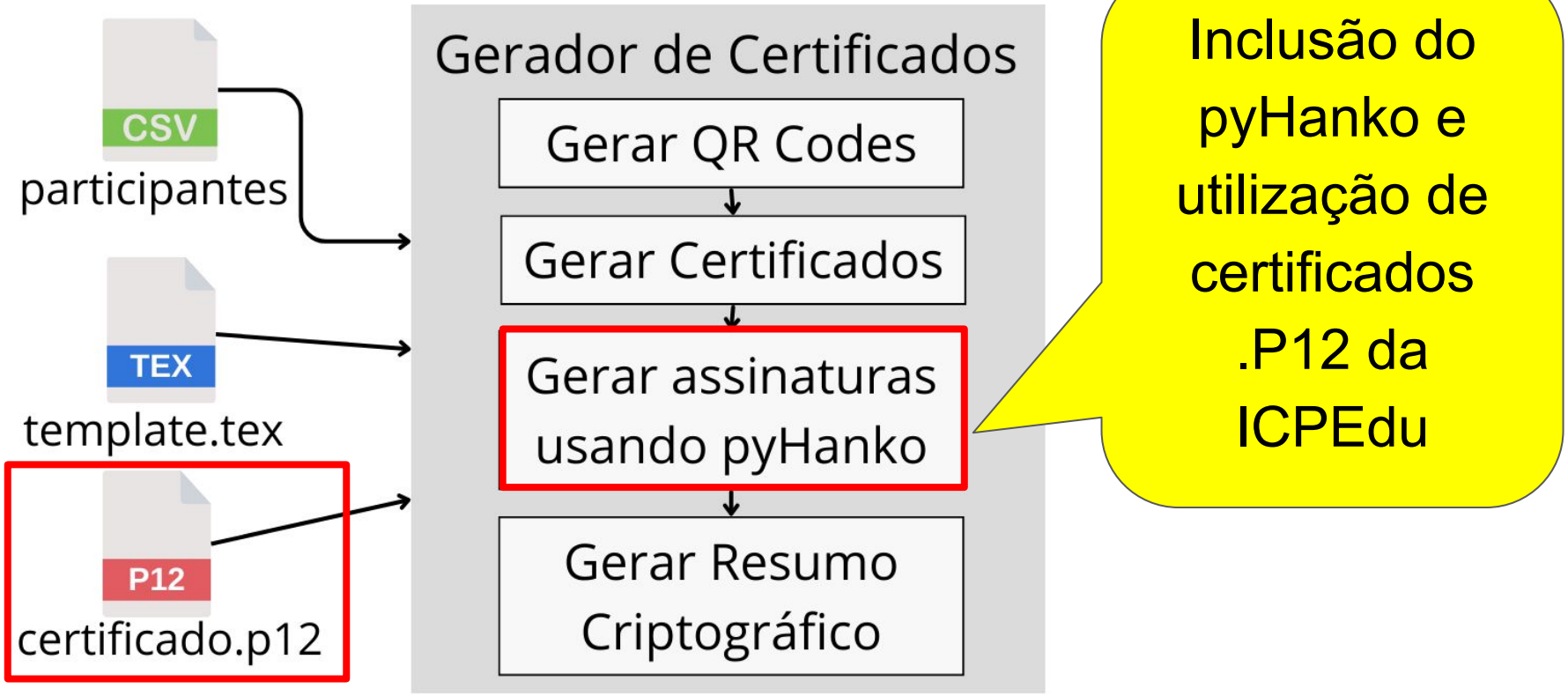
# E-certsDS: adaptação

- Suporte a certificados digitais ICPEdu



pyHanko

# E-certsDS - Adaptação



# Considerações finais

## eWebAPI

- Simplifica a utilização do e-certsDS

# Considerações finais

## eWebAPI

- Simplifica a utilização do e-certsDS
- Viabiliza integração com sistemas

# Considerações finais

## eWebAPI

- Simplifica a utilização do e-certsDS
- Viabiliza integração com sistemas
- Possibilita uso de certificados digitais

# Considerações finais

## eWebAPI

- Simplifica a utilização do e-certsDS
- Viabiliza integração com sistemas
- Possibilita uso de certificados digitais
- Permite utilizar o e-certsDS como serviço

# Trabalhos Futuros

- *Endpoints* para integração com sistemas específicos

# Trabalhos Futuros

- *Endpoints* para integração com sistemas específicos
- Análise de segurança da API

# Trabalhos Futuros

- *Endpoints* para integração com sistemas específicos
- Análise de segurança da API
- Segurança assistida por hardware para proteger os Certificados Digitais

# Trabalhos Futuros

- *Endpoints* para integração com sistemas específicos
- Análise de segurança da API
- Segurança assistida por hardware para proteger os Certificados Digitais
- Testes de usabilidade com usuários diversos

unipampa
Universidade Federal do Pampa


LEA
Laboratório de Estudos Avançados em Computação

PPGES
Programa de Pós-Graduação em Engenharia de Software

# Obrigado!

Alan Miguel Dorr Schulze

alanschulze.aluno@unipampa.edu.br