FICHA DE INSCRIÇÃO

Órgão/Entidade: Superior Tribunal de Justiça

Titular da Ouvidoria: Ministro Moura Ribeiro

E-mail: [redacted]

Telefones: [redacted]

Contato (pessoa): [redacted]

Município: Brasília UF: DF

Poder: ( ) Executivo ( ) Legislativo (X) Judiciário ( ) Outro

Esfera: (X) Federal ( ) Estadual ( ) Municipal

Categoria:

( ) a. Fomento à participação e ao controle social pelas populações em situação de vulnerabilidade.

( ) b. Desenvolvimento de capacidade institucional e melhoria da gestão e das entregas aos usuários de serviços públicos

( ) c. Promoção de mecanismos de tratamento da denúncia e de proteção ao denunciante de boa-fé.

(X) Tecnologia, segurança da informação e proteção de dados

Título da prática:

Uso do Login único do Governo Federal para verificação da autenticidade do usuário para atendimento das Requisições de Titulares de Dados Pessoais, baseados na LGPD

1) Descrição da prática:

A partir da vigência da Lei Geral de Proteção de Dados – LGPD, todos os órgãos tiveram de se adequar para o recebimento das requisições previstas nos arts. 18 e 19 da LGPD. No STJ, a Ouvidoria ficou responsável pelo recebimento destas requisições (art. 9º, VIII, do Regulamento da Ouvidoria). Assim, foi implementado no Sistema de Ouvidoria – SOU, o tipo de demanda "Requisições de Titulares de Dados Pessoais".

Para a apresentação dessa requisição bastava o cadastro do usuário, utilizando nome, e-mail, CPF e senha, com a possibilidade de validação, a posteriori, pela Ouvidoria, da identidade do nome informado com o nome cadastrado na Receita Federal. Entretanto, com o tempo e com o aumento do número de ataques hackers no Brasil, onde os dados são vendidos ou "sequestrados", percebemos que apenas o cadastro de senha era pouco confiável para a autenticação do usuário (a pessoa que solicita os dados pessoais é de fato a pessoa que ela diz ser?). Em especial em se tratando de um tipo de manifestação em que

o conteúdo é sensível, pois envolve dados pessoais, cuja proteção já constava na Lei n. 12.527/2011, a Lei de Acesso à Informação, e foi robustecida com a edição da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados Pessoais.

Com esta inquietação, a Ouvidoria, junto com a Secretaria de Tecnologia da Informação e Comunicação - STI e a unidade encarregada pela proteção dos dados pessoais no STJ, pesquisou os tipos de autenticação disponíveis e encontramos na "Conta gov.br" a solução mais rápida, barata e eficaz.

O que é?[1]

A Conta gov.br é um meio de acesso digital do usuário aos serviços públicos digitais. Esta Conta garante a identificação de cada cidadão que acessa os serviços digitais do governo.
Essa é a nova proposta do Governo federal, para facilitar a identificação e autenticação do cidadão, privilegiando a governança e a convergência autoritativa, e finalmente o controle de acesso unificado.
Oferece um ambiente de autenticação digital único do usuário aos serviços públicos digitais, ou seja, com um único usuário e senha você poderá utilizar todos os serviços públicos digitais que estejam integrados com a Conta gov.br. Fornece um nível de segurança compatível com o grau de exigência, natureza e criticidade dos dados e das informações pertinentes ao serviço público solicitado.

Por quem foi criado?
Foi criado pelo Ministério da Economia (ME) em parceria com o Serviço Federal de Processamento de Dados (Serpro).
O projeto da Plataforma de Cidadania Digital foi instituído pelo Decreto n° 8.936, de 19 de dezembro de 2016 site externo, que contempla diversas diretrizes para a prestação de serviços públicos digitais, das quais fazem parte a convergência autoritativa e a federação dos processos de autenticação dos serviços digitais, tendo por base:

- Presidência da República, por meio da Casa Civil;
- Compartilhamento de base de dados constante no Decreto n° 8.789, de 29 de junho de 2016 site externo;
- Política de Governança Digital, por meio do Decreto n° 8.638 de 15 de janeiro de 2016 site externo;
- Políticas de Governo Digital com enfoque no cidadão.

Concebeu o conceito da Plataforma de Autenticação Digital do Cidadão, o projeto Conta gov.br.

Formas de Autenticação
Existem quatro formas de autenticação:

1. Usar o aplicativo gov.br, por meio da leitura de QR-CODE
2. Usar o seu login de usuário e senha, em que o usuário será o CPF informado na criação da conta;
3. Usar uma Conta de Banco Credenciado;
4. Usar um Certificado Digital de Pessoas Físicas ou Jurídicas dos tipos A1 ou A3 compatíveis com ICP-Brasil;

[1] Informações retiradas do FAQ: http://faq-login-unico.servicos.gov.br/en/latest/_perguntasdafaq/oquee.html

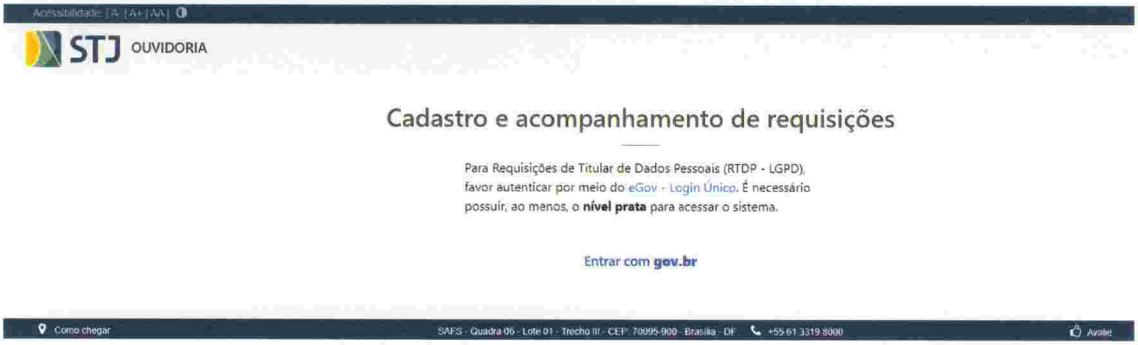
5. Usar um Certificado Digital em Nuvem.

É seguro?
Sim, pois utiliza os mesmos recursos e protocolos (OPENID CONNECT e OAUTH2) de segurança de empresas renomadas, respaldados por uma especificação consolidada da indústria de software para identificação, autenticação e autorização de usuários.

Assim, a Ouvidoria solicitou à STI a implementação da funcionalidade de verificação da autenticidade do usuário, conhecida como "Login único", dentro do SOU, para as requisições dos titulares de dados pessoais. A implementação decorreu com a realização das seguintes ações:

- estudos para implantação do login único como forma alternativa de acesso ao SOU;
- implantação de modalidade de verificação de meio de acesso ao sistema (login único ou SOU)
- implantação de modalidade de verificação de nível de acesso do usuário (bronze, prata ou ouro)
- possibilidade de solicitação de migração de um tipo de manifestação para outro com solicitação de uso do login único ou mudança de nível (de bronze para prata, por exemplo)

Em novembro de 2021 a funcionalidade foi publicada no site da Ouvidoria (https://www.stj.jus.br/ouvidoria) e no site sobre a LGPD no STJ, se apresentando da seguinte forma:



2) Histórico da implementação:

Da solicitação à STI até a publicação no site da Ouvidoria, em novembro de 2021, decorreram 2 meses, durante os quais houve a negociação com o Ministério da Economia e as adaptações no sistema de ouvidoria para a implantação final da ferramenta.

As unidades envolvidas, após a aprovação da solução pela administração do STJ, preencheram o documento de adesão disponibilizado pelo Ministério da Economia e, após o envio, o STJ recebeu os códigos fontes para o desenvolvimento da solução de integração do Sistema de Ouvidoria – SOU ao login único.

A solução tecnológica pode ser descrita da seguinte maneira:

O sistema de Ouvidoria, para requisições de titulares de dados pessoais, pode ser subdividido em duas funções, quais sejam: a autenticação via "Login Único" e o efetivo acesso às demandas do titular dos dados pessoais.

Conforme o exposto anteriormente, todo o sistema possui como pré-requisito primordial a garantia de autenticidade do titular dos dados dos quais a requisição é realizada (art. 2º da Lei 13.709/2018). Garantindo a autenticidade do cidadão, é possível respeitar a sua privacidade e inviolabilidade da sua intimidade, honra e imagem. Cabe notar que ambas funcionalidades foram construídas sobre o alicerce da solução GovBR, disponibilizada pelo Ministério da Economia.

Dando prosseguimento à análise técnica, a primeira funcionalidade, a autenticação via "Login Único", deve se iniciar com o cadastro da conta no sistema GovBr. A cada cidadão é possível, a criação de uma conta GovBr, que pode possuir três níveis de confiabilidade, do menor para o maior: bronze, prata ou ouro. Cada nível exige um conjunto de critérios que visam aumentar a confiança na autenticidade do usuário. Estão disponíveis diversos critérios, como, validação facial, certificação digital ou selos das instituições financeiras. Considerando que a partir do nível prata a validação facial já é um dos possíveis meios de validação de autenticidade e pela criticidade dos dados pessoais, esse nível foi o menor exigido para acesso a requisições de dados pessoais no Sistema SOU.

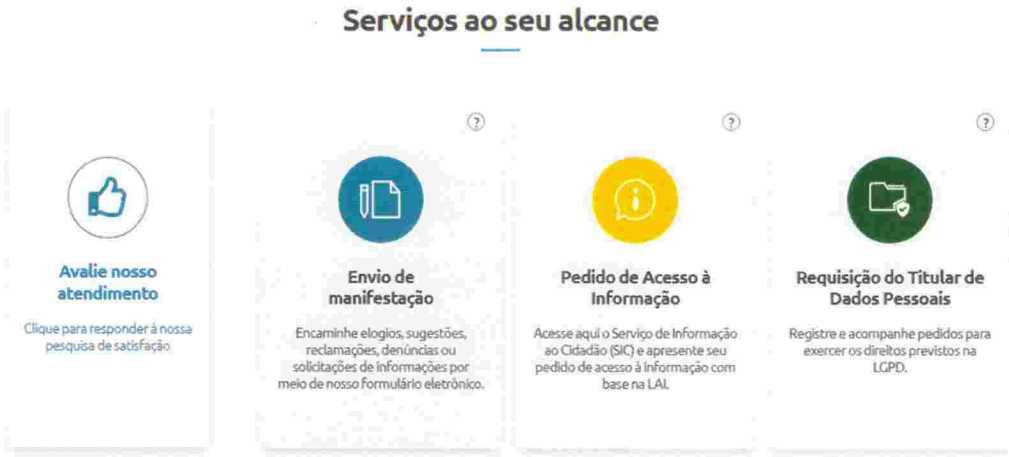
Em termos tecnológicos, a solução envolveu a utilização de uma arquitetura baseada em Angular no *FrontEnd*, Java no *BackEnd* e Banco de Dados SQL Server. O sistema ainda possui funções para garantir a acessibilidade e responsividade. No que tange à segurança, o protocolo HTTPS é o único aceito, bem como toda a comunicação realizada entre as camadas do sistema é feita por intermédio do uso de *access token*, conforme estabelecem os padrões OAUTH2 e OpenID Connect. A arquitetura da solução, em conjunto com o Ministério da Economia, envolveu, além do *Resource* Server, o *Authorization Server* dessa entidade governamental, cujo papel é essencial para garantir a segurança criptográfica dos *access tokens*.

A partir da autenticidade verificada dos usuários, a segunda funcionalidade estará disponível. Essa segunda etapa reúne duas ações, a primeira é a verificação de autorização baseada em perfis de acesso. Esta permite dividir o acesso à requisição de dados pessoais das demais opções existentes no sistema. Pelo fato de que dados pessoais sejam considerados mais críticos, por motivos já expostos, somente aqueles que possuírem os perfis de autenticação prata ou ouro via GovBr poderão visualizar as requisições de dados pessoais. Ademais a autorização ainda é reforçada por um segundo nível de *tokens* criados internamente dentro da própria estrutura de autenticação/autorização do STJ.

Prosseguindo com o fluxo, uma vez realizada a autorização, o cidadão poderá visualizar, modificar e remeter requisições de dados pessoais. Nesse momento, os dados cadastrais complementares do usuário são exigidos, como, por exemplo, Unidade Federativa e confirmação do e-mail de contato. Essa etapa se torna primordial por questões do negócio, na medida em que tais dados contribuem para o retorno das informações, bem como para composição de dados estatísticos.

Cabe lembrar que o Sistema SOU ainda possui outras duas funcionalidades, o envio de manifestação e o pedido de acesso à informação. Essas duas funcionalidades requerem um nível mais brando de acesso, uma vez que são dados de conhecimento público. Para essas funcionalidades, a abordagem de integração com o GovBR, "Login Único", não foi utilizada. No entanto, a composição de *access tokens* e o Sistema de Autenticação do STJ ainda são exigidos, bem como os protocolos de segurança HTTPS e OAUTH2.

A adoção dessa solução foi acompanhada da reformulação da página da Ouvidoria para que essa passasse a apresentar os tipos de manifestação admissíveis, com uma explicação sucinta de cada uma delas para os usuários.



3) Relevância da prática em relação aos critérios do regulamento:

A solução se mostra **criativa e inovadora** pois através de uma ferramenta pré-existente e de larga utilização pela população solucionou um importante problema da instituição que era garantir que estava entregando informações sobre o tratamento de dados pessoais à pessoa a qual eles se referem.

Em termos de **custo-benefício** a solução mostra-se adequada pois não envolveu contraprestação pecuniária entre os órgãos que, por meio do trabalho de seus próprios servidores conseguiram desenvolver, compartilhar, adaptar e implementar a ferramenta do login único.

Os **impactos da iniciativa** no processo de trabalho da Ouvidoria foram relevantes do ponto de vista da segurança, e para o cidadão trouxe segurança e facilidade, pois agora ele tem diante de si uma ferramenta já conhecida, pois já utilizada em larga escala pelo Poder Executivo. Além disso, a adoção do login único contribuiu para a **efetividade** da ferramenta de requisição dos titulares de dados pessoais, eis que possibilita que o órgão tenha todas as informações necessárias sobre a autenticidade do usuário para atendê-lo.

E, por fim, a solução se mostrou de uso simples e intuitivo para o usuário e de implementação simples para a unidade, podendo facilmente ser reaplicada em outros sistemas de ouvidoria ou mesmo por meio da adoção do SOU STJ por outros órgãos, já com a integração ao login único, eis que se trata de sistema web.

Por fim, vê-se que a solução é capaz de garantir a autenticidade do requerente, numa ferramenta gratuita, tanto para o cidadão quanto para os órgãos públicos, e é de simples desenvolvimento, facilitando a possibilidade de ser **replicada** por outros órgãos ou esferas do Governo.

Brasília-DF, 31 de janeiro de 2022.

Declaro que tomei conhecimento do Regulamento do V Concurso de Boas Práticas da Rede Nacional de Ouvidorias

Tatiana A Estanislau de Souza

Ouvidora auxiliar do STJ

Tatiana A. Estanislau de Souza
Analista Judiciário Mat. S056302
Superior Tribunal de Justiça