PILOTO DE CERTIFICAÇÃO E IDENTIDADE ELETRÔNICA PARA MOÇAMBIQUE

Frederico Schardong[12], frederico.schardong@rolante.ifrs.edu.br; Lucas Mayr de Athayde[1], lucas.mayr.athayde@gmail.com; Ricardo Custódio[1], ricardo.custodio@ufsc.br

1- Universidade Federal de Santa Catarina (UFSC)
2 - Instituto Federal de Educação Ciência e Tecnologia do Rio Grande do Sul (IFRS), *Campus* Rolante

RESUMO

Infraestrutura de certificação digital e identidade eletrônica são ferramentas importantes para facilitar o acesso a serviços digitais na Internet. Este documento apresenta um piloto de Infraestrutura de Chaves Públicas (ICP), de identidade eletrônica e de assinatura de documentos eletrônicos desenvolvido em parceria entre o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) de Moçambique e o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC). O piloto foi desenvolvido para ser mostrado durante o Fórum de Governação da Internet em Moçambique 2021 (FGIMz2021). Através do piloto, todos podem criar sua identidade eletrônica, assinar documentos e experimentar com certificados digitais. O piloto pode ser acessado no endereço https://mz.labsec.ufsc.br/.

PALAVRAS-CHAVE: Infraestrutura de Chaves Públicas. Identidade eletrônica. Assinatura digital. Piloto.

1 INTRODUÇÃO

Países de todo o mundo têm implantado sistemas de gestão de identidade eletrônica e serviços de assinatura eletrônica de forma a facilitar o acesso dos seus cidadãos aos serviços de governo eletrônico. Neste trabalho desenvolvemos uma proposta de ICP e identidade eletrônica integrados para Moçambique, permitindo a seus cidadãos terem uma identidade eletrônica barata e moderna. Como estudo de caso, ofertamos um assinador de documentos eletrônicos que faz uso da identidade eletrônica e ICP para emitir certificados sob-demanda únicos para cada documento assinado. A Seção 2 detalha nosso objetivo. A Seção 3 descreve o provedor de identidade eletrônica do piloto. A Seção 4 apresenta a ICP piloto para Moçambique. A Seção 5 apresenta o assinador de documentos eletrônicos. A Seção 6 descreve o piloto propriamente dito e suas aplicações. A Seção 7 contém algumas considerações finais sobre este piloto.

2 OBJETIVOS

O objetivo deste piloto é, através de uma implementação prática, mostrar as tecnologias consagradas para implementação de sistemas de identidade eletrônica, infraestrutura de chaves públicas e assinadores de documentos eletrônicos.

3 IDENTIDADE ELETRÔNICA

No mundo físico muitas interações entre diferentes entidades (pessoas, empresas, governos) dependem das partes envolvidas serem identificadas. Da mesma forma, no mundo eletrônico, as partes que interagem precisam ter certeza de que com quem estão interagindo é de fato quem afirma ser. Nessa medida, uma identidade digital deve, sem dúvida, identificar seu titular.

Como uma identidade física, uma identidade eletrônica geralmente é definida como um conjunto de atributos que ajudam a descrever ou qualificar uma entidade em contextos específicos. Consequentemente, as identidades eletrônicas não são apenas cópias de identidades físicas, como passaporte ou carteira de motorista. Elas são criadas, usadas e destruídas de acordo com o desejo do usuário, muitas vezes contendo apenas os atributos mínimos necessários para realizar o que é necessário naquele contexto. Por exemplo, um vendedor pode ter uma identidade eletrônica no eBay sem revelar seu nome, idade ou país de residência. A única informação que preocupa outras pessoas é se este vendedor tem um histórico de transações positivas.

Atualmente, existem dois protocolos que se tornaram amplamente utilizados na Internet para lidar com identidade eletrônica, são eles o OAuth 2.0 [3] e OpenID Connect [4]. Mais especificamente, o OAuth 2.0 permite ao usuário final delegar autorização para provedores de serviço (ex: serviços de governo ou privados como alugar um carro ou fazer compras online) acessem seus dados armazenados em provedores de identidade (ex: Facebook, Google, um provedor de identidade do governo). Já o protocolo OpenID Connect permite que os provedores de serviço obtenham e armazenem informações sobre a forma que a autenticação do usuário final aconteceu (fatores de autenticação envolvidos, por exemplo) bem como seus atributos.

4 INFRAESTRUTURA DE CHAVES PÚBLICAS

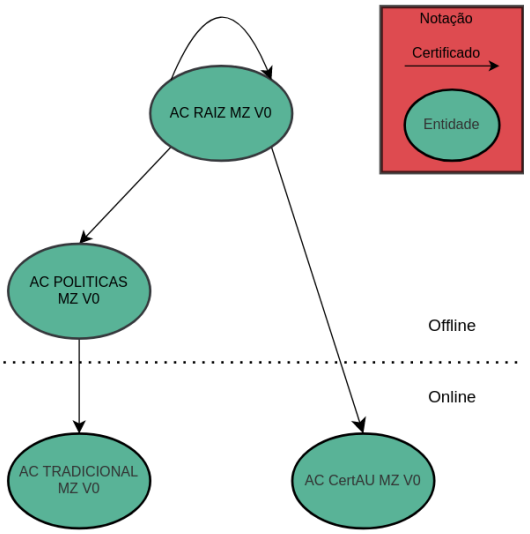
Uma infraestrutura de chaves públicas (ICP) tem como propósito o gerenciamento e a autenticação de comunicações através da Internet. Esta estrutura é baseada na criptografia de chaves públicas, que conta com uma chave privada e uma chave pública, cada uma usada na sua respectiva função de cifragem e decifragem. Certificados digitais são usados nessa infraestrutura para guardar as informações pertinentes a uma entidade e ligá-la com a sua chave pública. Estes certificados são emitidos por Autoridades Certificadoras (ACs) e sua validade pode ser verificada percorrendo a cadeia de certificados até encontrar uma AC de confiança do usuário.

Criamos este projeto piloto de uma ICP Moçambique para que os usuários possam experimentar com a assinatura de documentos e com o uso de certificados e par de chaves. Este piloto conta com duas cadeias diferentes, uma tradicional que reflete como certificados são usados normalmente e uma cadeia que faz a emissão de certificados atrelados a apenas um documento, e portanto, chamamos este certificado de assinatura única.

O piloto conta com uma AC raiz, uma AC normativa de políticas, uma AC de emissão de certificados tradicionais e uma AC emissora de certificados de assinatura única. Esta estrutura pode ser visualizada na Figura 1.

A emissão dos certificados e o preenchimento dos campos das requisições são feitos automaticamente usando as informações contidas no registro de identidade eletrônica previamente criado. A chave privada e o certificado emitido pela AC tradicional podem ser usados de modo genérico, enquanto o certificado emitido pela AC de certificados de assinatura única só tem utilidade na verificação de um único arquivo.

Figura 1 - Estrutura da ICP Moçambique piloto.



Fonte: os autores.

5 ASSINATURA DE DOCUMENTOS ELETRÔNICOS

Uma assinatura eletrônica é uma forma de assinar um documento eletrônico usando uma credencial exclusivamente associada a uma pessoa. Essa credencial é anexada ao documento, tornando-se equivalente a uma assinatura manuscrita em papel. Ele pode ser usado para autenticar o signatário e também para detectar quaisquer alterações feitas no documento após sua assinatura.

6 PILOTO

O Piloto consiste em quatro soluções:

a) Um Sistema de Gerenciamento de Identidades Eletrônicas para Moçambique.
O sistema, construído sob uma plataforma de software aberto e gratuito, utiliza os protocolos OpenID Connect e OAuth2.0. Estes são os protocolos usados por grandes empresas tais como Google, Facebook, Twitter e também por governos de vários países, incluindo o Brasil.

Todos vão poder criar sua identidade eletrônica neste sistema. Esta identidade eletrônica vai ser usada, no piloto, para que vocês se autentiquem nos serviços de emissão de certificado digital e também de assinatura de documentos eletrônicos.

A identidade eletrônica poderia, por exemplo, ser usada pelo cidadão moçambicano para se autenticar nas aplicações de governo eletrônico. De forma a facilitar a geração e o uso da identidade, optamos por um registro aberto, livre, sem qualquer checagem de dados. Mas, pode-se facilmente incluir checagem por e-mail, controle manual, e também adicionar segundo fator de autenticação.

b) Uma Infraestrutura de Chaves Públicas para Moçambique.
Construímos uma infraestrutura de Chaves Públicas contento uma AC Raiz, uma Autoridade de Gestão de Políticas de Certificação e duas ACs emissoras de certificados digitais para os usuários. Essa infraestrutura também foi construída usando software aberto e gratuito.

c) Um Assinador Universal de Documentos Eletrônicos.

Também colocamos à sua disposição um sistema de assinatura de documentos no formato Portable Document Format (PDF) [1], usando os certificados da ICP de Moçambique. O usuário, ao se autenticar usando sua identidade eletrônica, pode submeter um documento PDF para ser assinado à aplicação. O documento é assinado e retornado ao usuário.

Note que usamos uma tecnologia inovadora, no sentido de que o usuário não precisa dispor, de antemão, de um certificado digital. Ao submeter o documento ao sistema assinador, um certificado digital é emitido automaticamente. Então o documento é assinado. E após assinado, o certificado é descartado. Esta solução é muito interessante, pois ao mesmo tempo que permite que documentos eletrônicos sejam assinados de forma segura com certificados digitais, não requer que os usuários tenham smartcards ou tokens, Lembramos que o documento PDF assinado pode ser visualizado em qualquer leitor de documento PDF. E aqueles leitores que dispõem de verificação de assinatura, mostram os detalhes da assinatura. Por exemplo, o Adobe Reader.

d) Um Sistema de Emissão de Certificados de Propósito Geral
Este sistema permite que o usuário emita um certificado digital genérico. O arquivo contendo o certificado e sua chave privada (formato PKCS #12 [4]), pode ser instalado em qualquer aplicação do usuário. Por exemplo, pode ser instalado no repositório do sistema operacional do Windows. O objetivo deste é propiciar ao usuário um certificado com chave privada para experimentar nos mais diversos sistemas e aplicações e assim adquirir experiência no trato de certificação digital e aplicações.

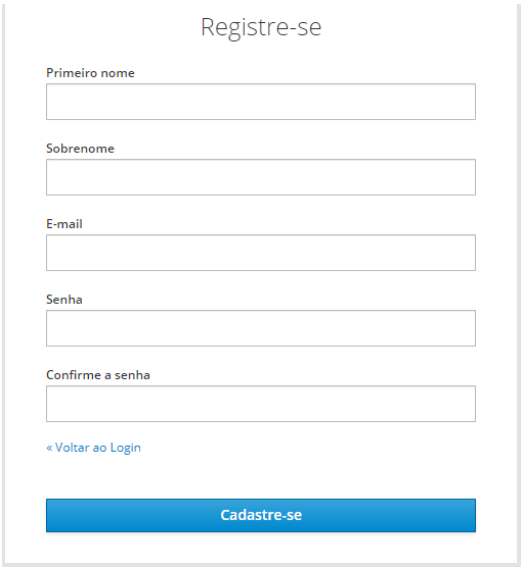
Nosso piloto está disponível em https://mz.labsec.ufsc.br livremente para todos utilizarem. O código-fonte será disponibilizado para o INTIC, que poderá continuar o projeto como desejar. A seguir, detalhamos o piloto.

5.1 Identidade Eletrônica de Moçambique
Identidade eletrônica permite que as pessoas se identifiquem na Internet, desta forma tendo acesso a serviços personalizados. Neste protótipo/demo oferecemos aos participantes do FGIMz2021 a possibilidade de criarem uma identidade eletrônica em nosso provedor de identidade. Com ela, o usuário tem acesso a dois serviços: (i) emissão de certificados digitais; e (ii) assinatura de documentos eletrônicos.

Nós criamos este provedor de identidade eletrônica utilizando Keycloak [2], uma solução de código aberto e gratuita mantida pela Red Hat. Os dois serviços que disponibilizamos foram construídos em Python 3 e se conectam ao provedor de identidade através dos protocolos OAuth 2.0 e OpenID Connect, que são os padrões *de facto* utilizados internacionalmente para lidar com identidade eletrônica.

A Figura 2 mostra o processo de criação de uma identidade eletrônica em nosso provedor de identidade. Para criar uma identidade eletrônica, o usuário precisará informar seu nome, e-mail e uma senha.

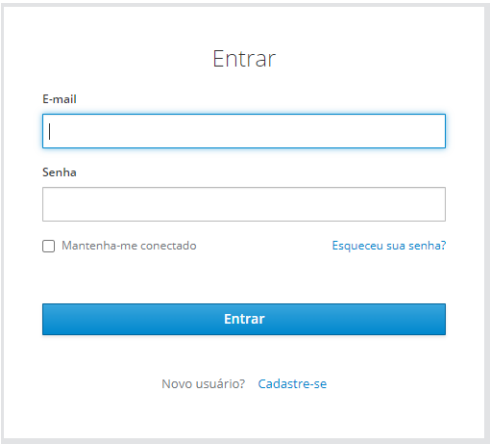
Figura 2 - Registro da Identidade Eletrônica.



Fonte: os autores.

Caso já tenha criado sua identidade eletrônica em nosso provedor de identidade mas não esteja autenticado, deverá fornecer seu e-mail e senha previamente cadastrados, conforme mostrado na Figura 3.

Figura 3 - Autenticação do Usuário no Provedor de Identidade.



Fonte: os autores.

Após se autenticar, o usuário é redirecionado para a página inicial e poderá acessar os dois serviços que disponibilizamos (emissão de certificado e assinatura digital de documentos PDF).

5.2 ICP Moçambique

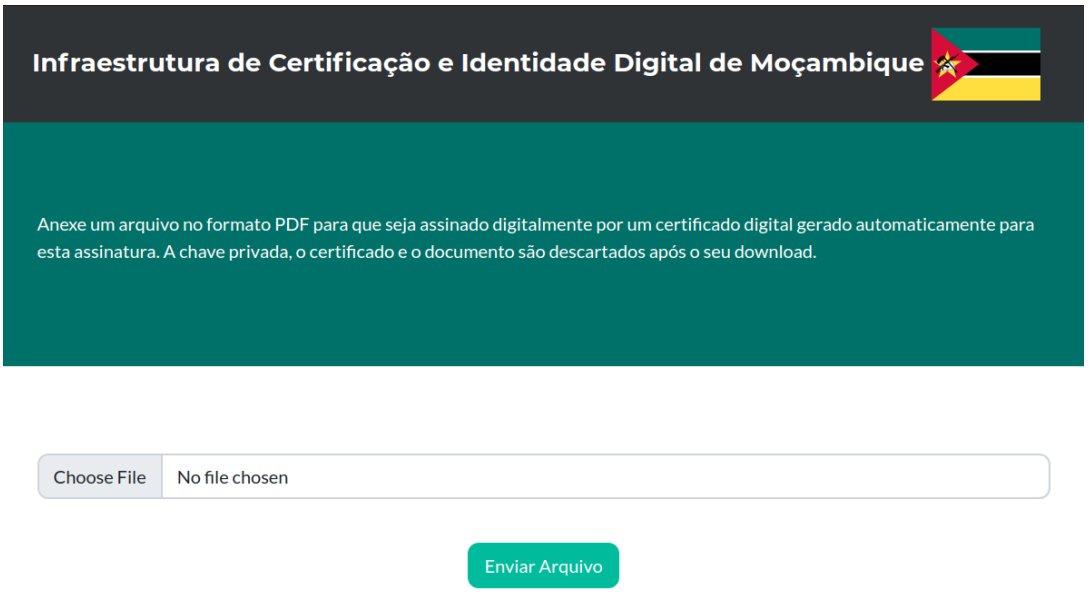
A ICP do piloto foi implementada usando Python3 para a interface com usuário e Openssl para a criação e gerenciamento das ACs. A AC emissora de certificados tradicionais emite certificados com duração de 5 anos e o par de chaves utilizado na criação da requisição pode ser usado múltiplas vezes. A AC de certificados de assinatura única, entretanto, difere do uso tradicional, podendo ser usada para confirmar a validade de apenas um documento. O sistema

que cria a requisição e faz a assinatura do documento descarta o par de chaves após a assinatura, assim o usuário não precisa se preocupar em manter a sua chave privada segura.

5.3 Assinador de Documentos Eletrônicos

Uma das possíveis aplicações dos certificados emitidos por uma ICP é a assinatura digital de documentos. Em nosso protótipo, unimos a assinatura digital de documentos em PDF com a nossa proposta de ICP e identidade eletrônica. Nossa ICP é composta por duas ACs que estão sempre online emitindo certificados, a AC Tradicional MZ V0 e a AC Certificado Assinatura Única MZ V0. Enquanto a primeira é utilizada para emissão de certificados tradicionais para usos quaisquer e de duração de 5 anos, a segunda emite certificados de duração de 30 anos e deve ser usada para propósitos específicos, como a assinatura digital de documentos. A Figura 4 mostra a página onde os usuários podem fazer o envio de um documento PDF para ser assinado digitalmente.

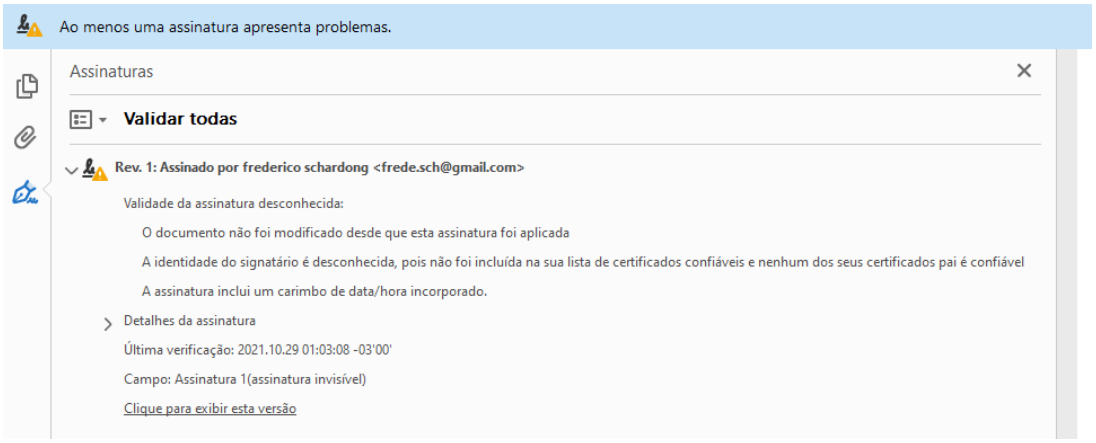
Figura 4 - Aplicativo de Assinatura de Documentos Eletrônicos.



Fonte: os autores.

Nosso sistema emite um certificado de assinatura única utilizando as informações provenientes da identidade eletrônica do usuário autenticado, assina o documento enviado com este certificado e descarta a chave-privada, certificado e o documento após o navegador fazer o download do documento assinado. O usuário pode verificar a assinatura digital com, por exemplo, o Adobe Reader. Entretanto, como nossa ICP é desconhecida pelo dispositivo do usuário quando usado pela primeira vez, o Adobe Reader não confiará na assinatura de imediato, conforme mostrado na Figura 5.

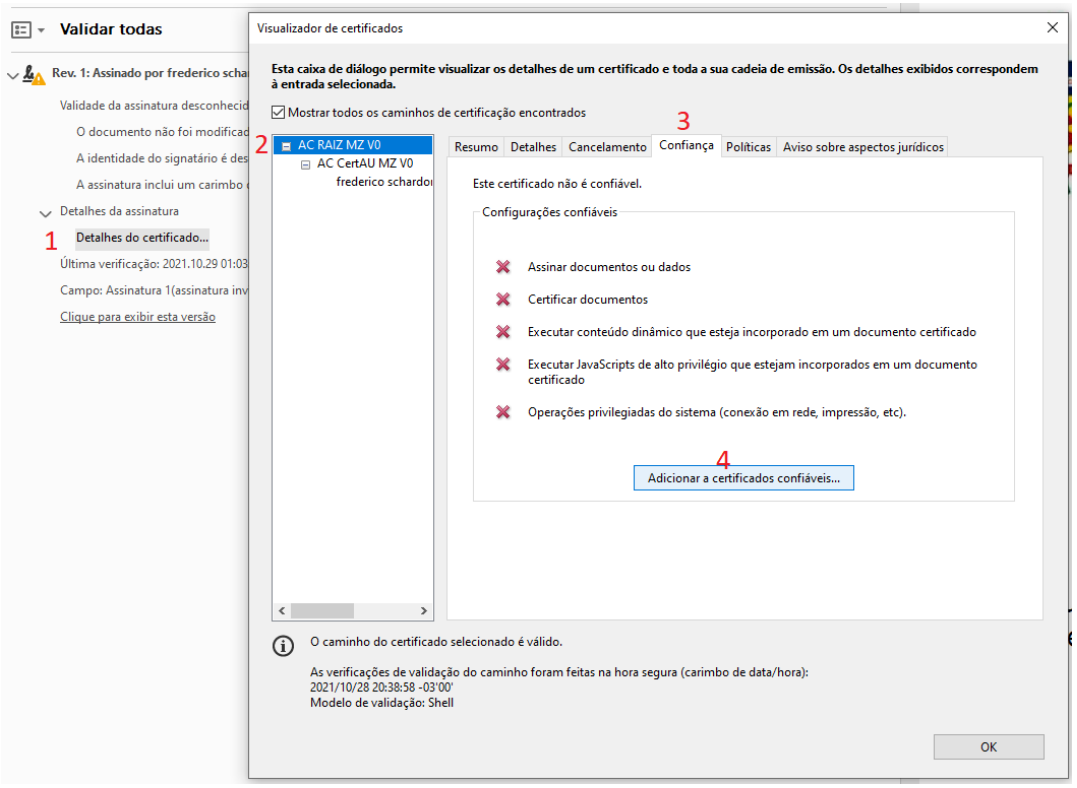
Figura 5 - Verificação da Assinatura Digital.



Fonte: os autores.

É necessário que o usuário adicione nossa AC RAIZ MZ V0 como uma entidade confiável. Ele pode fazer isso diretamente no Adobe Reader seguindo os passos anotados em vermelho na Figura 6.

Figura 6 - Cadeia de Certificados da ICP Moçambique.



Fonte: os autores.

6 CONCLUSÃO

Este documento descreve um sistema piloto de certificação digital e identidade eletrônica para Moçambique. Foi implementada uma infraestrutura de chaves públicas consistindo de uma AC raiz, uma autoridade gestora de políticas e duas ACs de emissão online de certificados digitais. Também foi implementado um provedor de identidade eletrônico, permitindo que cidadãos moçambicanos possam emitir suas identidades eletrônicas. Com o uso da identidade eletrônica, os usuários podem emitir certificados digitais para experimentar nas mais diversas

aplicações em sistemas computacionais. Finalmente, implementou-se uma aplicação universal de assinatura de documentos eletrônicos.

Mostra-se, através deste piloto, que os usuários não precisam se preocupar com seus certificados digitais para que possam assinar documentos eletrônicos. Ao acessar o aplicativo de assinatura de documentos eletrônicos, um certificado digital é automaticamente emitido, usado para assinar o documento e, em seguida, descartado. Sempre que for necessário assinar um novo documento, um novo certificado digital é emitido. Esta técnica inovadora evita enormes custos de manutenção de chaves privadas por parte dos usuários, além de simplificar muito o processo de assinatura eletrônica de documentos eletrônicos.

AGRADECIMENTOS:
O presente trabalho foi realizado com apoio do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS).

Referências

1. BIENZ, T., COHN, R., & Adobe Systems (Mountain View, Calif.). *Portable document format reference manual*. Boston MA: Addison-Wesley, 1993.
2. CHRISTIE, M. A., BHANDAR, A., NAKANDALA, S., MARRU, S., ABEYSINGHE, E., PAMIDIGHANTAM, S., & PIERCE, M. E. Using keycloak for gateway authentication and authorization, 2017.
3. HARDT, D. The OAuth 2.0 authorization framework, 2012.
4. MORIARTY, K., NYSTROM, M., PARKINSON, S., RUSCH, A., & SCOTT, M. PKCS# 12: Personal Information Exchange Syntax v1. 1. *Internet Engineering Task Force (IETF)*, 2014.
5. SAKIMURA, N., BRADLEY, J., JONES, M., DE MEDEIROS, B., & MORTIMORE, C. Openid connect core 1.0. *The OpenID Foundation*, S3, 2014.