

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

“SAGE IIOT” – O SAGE INTEGRADO À INTERNET INDUSTRIAL

MARCELO ROSADO DA COSTA(1); RUY MAGALHÃES BRITTO(1); PAULO STEIN(1); NIVALDO LAMBERT
CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA CEPEL (1)

RESUMO

Este trabalho tem por objetivo apresentar a incorporação do protocolo MQTT na arquitetura de solução do OPC UA disponível no SAGE (Sistema Aberto de Gerenciamento de Energia) de modo possibilitar a utilização de diversos *softwares* disponíveis gratuitamente no mercado para construção de *Dashboards* em plataformas *WEB* e *Smartphones* para a visualização de dados de tempo real. O acesso aos dados considera aspectos de segurança cibernética, incluindo autenticação em duas etapas. Alguns exemplos de uso dos *softwares* para configuração de Painéis IIoT através do protocolo MQTT no SAGE são apresentados neste trabalho.

PALAVRAS-CHAVE

MQTT, OPC UA, SCADA, SAGE

1.0 INTRODUÇÃO

Atualmente a sociedade, em geral, vem utilizando diariamente as redes de computadores sob requisitos que, cada vez mais, exigem mobilidade para diferentes necessidades, tais como: acesso a notícias, informações bancárias, compras de produtos, acesso e-mail, etc., demandando de forma crescente o uso de dispositivos móveis nessas atividades.

Adicionalmente, com o surgimento dos conceitos da “Indústria 4.0” e “Internet das Coisas aplicada na Indústria” (IIoT, do inglês *Industrial Internet of Things*), uma mudança significativa vem ocorrendo na indústria, no que tange a interoperabilidade para troca de informações de maneira segura, confiável e contínua entre dispositivos de diferentes fornecedores.

O OPC UA (*Open Platform Communications Unified Architecture*), formalizado como padrão internacional através da publicação da norma IEC 62541, tem sido adotado como um dos principais protocolos padronizados para uso na Indústria 4.0 e na IIoT.

Considerando este cenário, o CEPEL (Centro de Pesquisa de Energia Elétrica) empreendeu esforços para a implementação nativa do padrão OPC UA no sistema SAGE [1]. Esta implementação abriu novas fronteiras para a integração padronizada e segura de aplicativos, sistemas e fontes de dados aos sistemas de supervisão e controle suportados pelo SAGE.

Dando continuidade aos dois trabalhos publicados no XXV SNTPEE, sobre o desenvolvimento do protocolo OPC UA no sistema SAGE (Sistema Aberto de Gerenciamento de Energia) [2], e sobre o desenvolvimento de um aplicativo móvel nativo do SAGE [3], este trabalho tem por objetivo apresentar o desenvolvimento do Adaptador MQTT (*Message Queuing Telemetry Transport*) integrado ao OPC UA, nativo ao SAGE, de modo que venha a possibilitar a exportação de dados e utilização pelos diferentes *softwares* disponíveis gratuitamente no mercado para construção de Painéis (*Dashboards*) em plataformas *Desktop WEB* e *Smartphones*.

A incorporação do protocolo MQTT ao OPC UA foi definida nas normas do protocolo OPC UA (Parts 1 e 14 da IEC 62541 [4][5]), possibilitando assim esta integração OPC UA – MQTT no contexto da IIoT.

A partir deste desenvolvimento do Adaptador MQTT, o SAGE passou a se integrar na IIoT, permitindo a exibição de *Dashboards* contendo quaisquer dados existentes na base de dados de tempo real do sistema SAGE, tanto para os

dados (tópicos MQTT) do modelo SCADA (*Supervisory Control And Data Acquisition*), quanto para os do modelo EMS (*Energy Management System*).

Este trabalho descreve como o OPC UA e o MQTT foram inseridos na arquitetura original do SAGE, considerando aspectos tais como: a integração com a base de dados de tempo real, a exposição do modelo de dados para acessos externos e integração com os mecanismos de autorização e autenticação exigidos pelos atuais requisitos de segurança da informação. Este trabalho não aborda a aquisição de dados em MQTT pelo SAGE, somente a exportação de dados.

2.0 PROTOCOLO MQTT

O Protocolo MQTT (*Message Queuing Telemetry Transport*) é um protocolo de mensagens leve, projetado para comunicação entre dispositivos em redes com largura de banda limitada ou com conexões instáveis. Ele foi desenvolvido em 1999 pela IBM para ser usado em redes de sensores e atuadores, especialmente em ambientes de Internet das Coisas (IoT).

O MQTT é baseado em um modelo de *publish/subscribe*, onde os dispositivos se comunicam por meio de um intermediário chamado de *broker* [6]. Os dispositivos podem publicar mensagens em tópicos específicos, enquanto outros dispositivos podem se inscrever nesses tópicos para receber as mensagens. Algumas características importantes desse protocolo são:

- O protocolo é projetado para ser eficiente em termos de largura de banda e recursos computacionais. Isso o torna adequado para dispositivos com restrições de energia e processamento.
- Os dispositivos podem se conectar ao *broker* de forma assíncrona, o que significa que não precisam manter uma conexão constante.
- O nível de qualidade do serviço pode ser configurado individualmente para cada mensagem, de acordo com a importância e a confiabilidade desejadas.
- Os dispositivos podem publicar e subscrever tópicos específicos numa estrutura hierárquica, o que permite uma filtragem eficiente das mensagens.
- O protocolo tem baixa sobrecarga em relação ao conteúdo das mensagens, o que o torna eficiente em termos de largura de banda.

3.0 PROTOCOLO OPC UA

O protocolo OPC UA surgiu a partir da identificação de limitações do OPC Clássico, que é restrito ao uso basicamente em plataforma MS Windows, em decorrência do uso das tecnologias COM (*Component Object Model*) e DCOM (*Distributed Component Object Model*) da Microsoft. Dessa forma, o OPC UA foi lançado com as seguintes metas estabelecidas:

- Equivalência funcional com o OPC Clássico: para preservar o investimento de quem já possuía o OPC Clássico e que desejasse migrar para o OPC UA;
- Uma arquitetura orientada a serviços;
- Independência de plataforma: sendo utilizável tanto em um microcontrolador embarcado quanto em uma infraestrutura em nuvem;
- Segurança: com ferramentas de criptografia, autenticação e auditoria;
- Extensibilidade: permitindo a adição de novas funcionalidades sem prejudicar as aplicações existentes;
- Modelagem de informação abrangente: para permitir a definição de informação complexa.

O desenvolvimento do OPC UA contou também com o envolvimento de outras organizações de padronização, como a IEC e a ISA, que estavam interessadas em usar o OPC como mecanismo de transporte. Dessa forma, coube à OPC Foundation a definição de como descrever e transportar dados, enquanto às outras organizações coube definir quais dados deveriam ser descritos e transportados de acordo com os modelos de informação desejados [7].

O OPC é um padrão de fato, desenvolvido pela OPC Foundation para a troca de dados na área de automação industrial incluindo os sistemas elétricos. A especificação OPC UA estendeu este padrão para uma arquitetura orientada a serviços (SOA – *Service Oriented Architecture*), que objetiva ser independente de plataforma, escalável e extensível.

De fato, esta nova arquitetura traz vários benefícios quando comparada com o padrão OPC Clássico e tem tido grande aceitação entre os fabricantes de sistemas de automação e software afins, incorporando no seu conjunto de serviços recursos para:

- Comunicação segura entre os sistemas, através do uso de certificados X509 (para segurança das mensagens), assinaturas e criptografia baseada em algoritmos padronizados como PKCS (*Public Key Cryptography Standards*), DSS (*Digital Signature Standard*) e AES (*Advanced Encryption Standard*).
- Autenticação de usuários que se registram nos sistemas utilizando Username+passwords, *WebServices Security Tokens* ou Certificados X509 (específicos para identificação do programa de aplicação ou do usuário interativo).
- Exportação e importação dos modelos de dados utilizados pelos sistemas que se comunicam, incluindo modelos proprietários, como os modelos SCADA e EMS do SAGE, modelos proprietários de outros fabricantes, e modelos padronizados, como o modelo CIM (*Common Information Model*) definido na norma IEC 61970.

Quanto aos protocolos, o OPC UA pode ser mapeado em uma variedade de protocolos de comunicação ao longo dos 7 níveis do modelo OSI / ISO, sendo que os dados trafegados podem ser codificados de várias maneiras para aumentar a portabilidade e a eficiência, conforme ilustrado no stack [7] de protocolos mostrados na Figura 1.

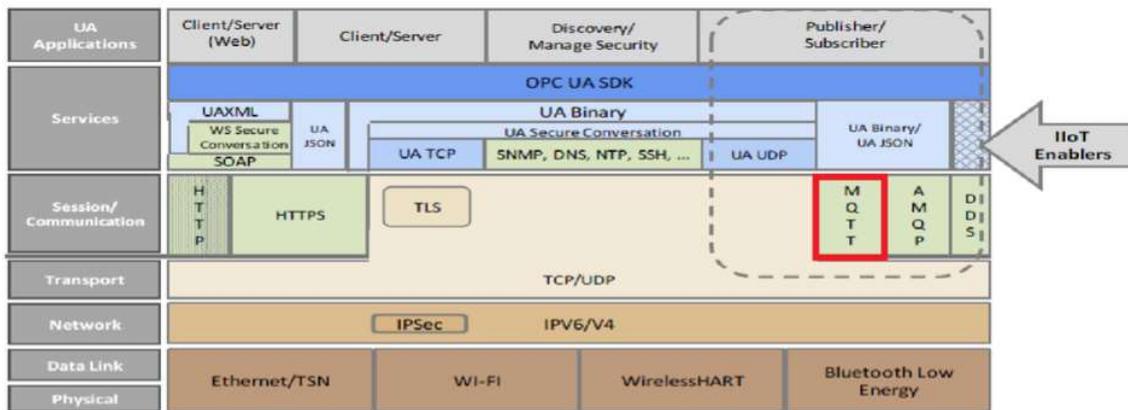


Figura 1 - Protocolos utilizados no OPC UA (Fonte: OPC Foundation [7])

O CEPEL desenvolveu nativamente o padrão OPC UA no sistema SAGE de modo a permitir que sistemas externos disponíveis no mercado ou desenvolvidos por usuários possam ser integrados ao SAGE utilizando padrões internacionais, sem que haja dependência ou necessidade de participação do CEPEL.

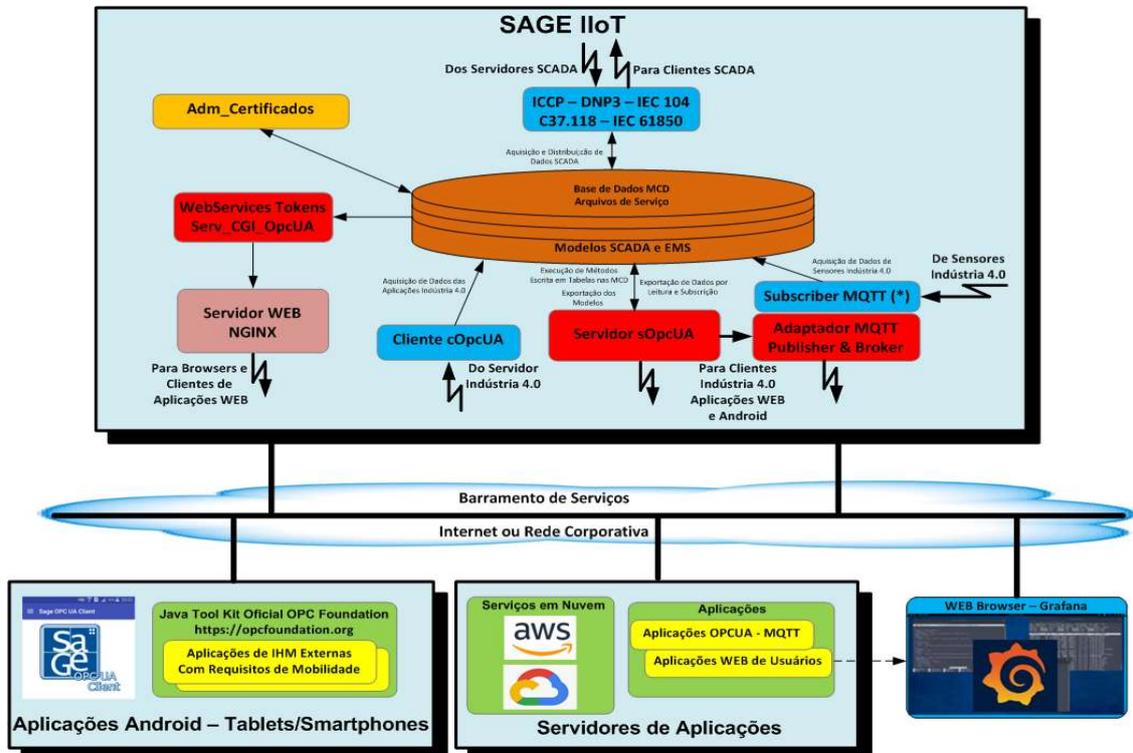


Figura 2 - Arquitetura OPC UA do SAGE

A Figura 2 mostra o servidor OPC UA do SAGE disponibilizando informações e serviços em tempo real, proporcionando uma integração segura com os sistemas externos de terceiros e/ou desenvolvidos pelos usuários, atendendo aos mais diversos requisitos de acesso via redes locais, de longa distância, públicas e privadas. Da mesma forma, essa integração pode ser estabelecida na direção oposta com o cliente OPC UA do SAGE obtendo dados de servidores externos, para uso das aplicações SCADA e EMS do SAGE.

4.0 INTEGRAÇÃO OPC UA COM MQTT NO SAGE

A Figura 1 mostra o mapeamento de protocolos utilizados no contexto do OPC UA, com a incorporação do protocolo MQTT no nível de transporte do seu Stack de protocolos, possibilitando assim esta integração do MQTT ao OPC UA do SAGE no contexto da IIoT.

Diferentemente da norma do OPC UA, que especifica diferentes formatos para codificação dos dados transportados, a norma da versão do MQTT implementada no SAGE (versão 3.1.1) [6] não especifica formatos a serem usados para os dados trafegados. Ela especifica que o formato de dados é livre, podendo ter codificação binária ou ASCII, ser baseado em estruturas de dados ou ser de um tipo primitivo (inteiro, *float*, *booleano*, ..), dentre outras variações para codificação dos dados trafegados no MQTT.

Mesmo não sendo a responsável pelas normas do MQTT, a Organização "OPC Foundation" incluiu o protocolo MQTT dentro da especificação das normas do OPC UA, por ser o MQTT um protocolo do tipo *Publish-Subscribe* bastante difundido na IIoT. A Figura 3 abaixo reproduz trechos dos volumes 1 e 14 da norma do OPC UA que fazem referência ao MQTT.

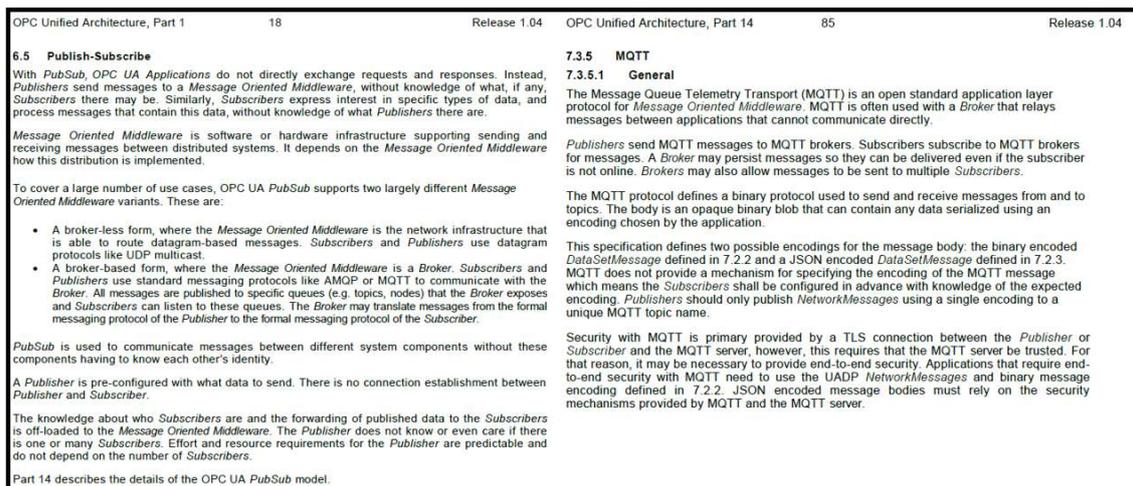


Figura 3 – Normas do OPC UA Incorporando o MQTT (Fonte: *OPC Foundation* [4], [5])

Com essa incorporação do MQTT ao OPC UA apresentada na Figura 2, o principal benefício obtido no SAGE foi o de permitir a sua integração com diferentes aplicações que implementam o MQTT, como por exemplo aplicativos IIoT para *Smartphones* e o Grafana, uma aplicação cliente *Desktop WEB* gratuita bastante difundida no mercado.

Utilizando essas aplicações que implementam o protocolo MQTT, o usuário do SAGE passou a dispor de mais recursos para a construção de *Dashboards* que podem exibir quaisquer dados EMS e SCADA residentes na base de dados tempo-real do SAGE.

Na norma do MQTT esses dados são denominados "tópicos", sendo que na implementação do MQTT no SAGE esses tópicos são mapeados em *strings* codificadas em ASCII, podendo conter valores numéricos de medições SCADA e EMS, textos de estado de variáveis booleanas e discretas, textos de alarmes, anotações (*tags*) feitas por operadores, etc.

5.0 CASOS DE USO

Dentre os diversos *softwares* para configuração de Painéis IIoT MQTT existentes no mercado, alguns serviram para a realização de testes de integração dos dados do SAGE através do protocolo MQTT.

A Figura 4 mostra um *Dashboard* Grafana onde o servidor (*Publisher/Broker*) do SAGE foi conectado pelo cliente Grafana através do seu "MQTT *Data Source*", permitindo assim que os tópicos MQTT incluídos no *Dashboard* desenhado pelo usuário, e subscritos pelo Grafana, sejam visualizados em *Web Browsers* (Chrome, Firefox, Edge).



Figura 4 - *Dashboard* em Aplicação *WEB Browser* - Grafana com MQTT *DataSource*

No caso dos aplicativos para *Smartphones*, foram testados os produtos MQTT *Dash* e IoT MQTT *Panel*, que também disponibilizam um amplo conjunto de tipos de painéis a serem utilizados pelos usuários na composição dos seus *Dashboards*, incluindo os gráficos de tendências, botões, chaves, *sliders*, indicadores *leds*, indicadores de progresso, gráficos de barra, gráficos de pizza, sendo alguns deles mostrados na Figura 5 abaixo.

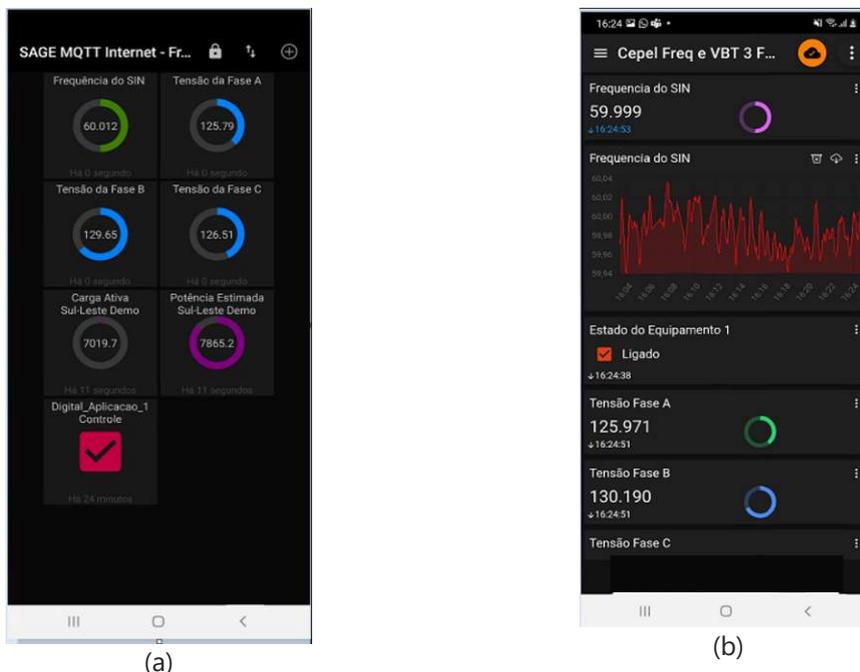


Figura 5 - *Dashboards* em Aplicativos de *Smartphones* - MQTT *Dash* (a) e IoT MQTT *Panel* (b)

De forma comparativa com a criação de *Dashboards* no Grafana, a execução dessa visualização em aplicativos de *Smartphones* pode ser considerada bem mais simples de ser realizada, provavelmente devido ao público-alvo desses

aplicativos ser constituído na sua maioria por inexperientes, diferentemente do que ocorre com o Grafana, que é normalmente utilizado por técnicos ou engenheiros especialistas.

Considerando o fato de que o protocolo MQTT não permite ao cliente subscritor consultar a árvore de objetos existentes em um servidor (*NodeIds* OPC UA que são tópicos MQTT), é bastante útil ao usuário de um *Smartphone* usar esses aplicativos MQTT em conjunto com o aplicativo SageOpcUaClient [3], visto que ele permite a navegação na árvore de tópicos dos modelos SCADA e EMS do SAGE em OPC UA para fazer a escolha dos tópicos que deseja visualizar.

Além disso, o aplicativo [3] permite efetuar operações de controle supervisão seguro, protegidas pela verificação de certificados digitais e credenciais de login do usuário no aplicativo, como também do endereço IP de origem dependente da localização do *Smartphone*.

Para exemplificar o uso integrado no *Smartphone* dos protocolos OPC UA e MQTT em um ambiente IIoT seguro, a Figura 6 mostra a execução de controle em tempo real no aplicativo SageOpcUaClient e com o resultado do ponto de supervisão do controle visualizado no MQTT Dash.

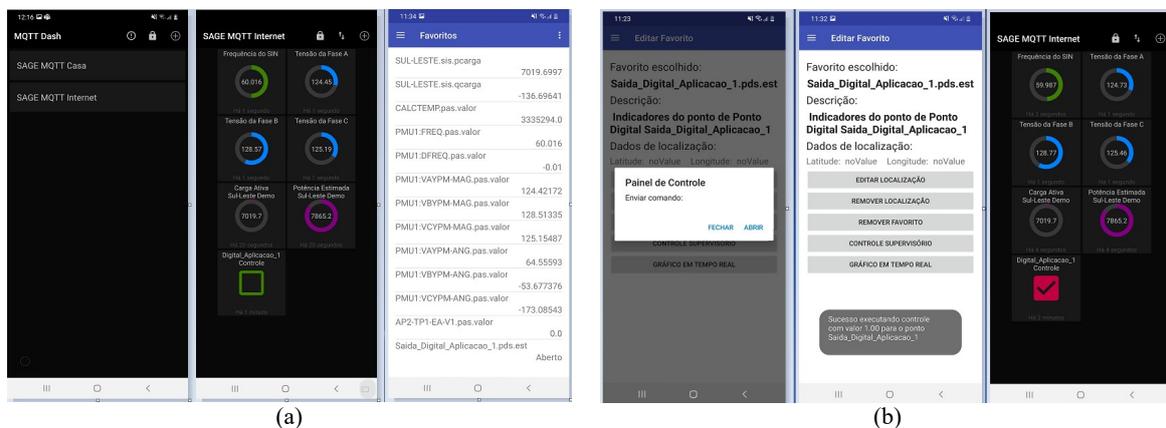


Figura 6 - Operação integrada OPCUA - MQTT Utilizando o SageOpcUaClient no Ambiente IIoT, (a) antes da efetivação do controle e (b) após a efetivação do controle

6.0 AUTENTICAÇÃO MQTT EM 2 ETAPAS COM O GOOGLE-AUTHENTICATOR E WEB TOKENS

A Figura 2 mostra quatro elementos ativos no SAGE que estão relacionados com a autenticação em 2 Etapas dos usuários MQTT de plataformas *Desktop WEB*, como o Grafana, e de aplicativos de *Smartphones*, como o MQTT Dash e IoT MQTT Panel.

Esses elementos são o (1) Servidor WEB Nginx, em conjunto com o (2) Servidor de WebTokens *Serv_Cgi_OpcUA*, o próprio (3) Adaptador MQTT, realizando as funções de *Publisher* e *Broker* MQTT, e o (4) programa *AdmCertificados*, que o Administrador do SAGE usa para cadastrar usuários e seus certificados digitais pessoais, assim como gerar as “Google-Authenticator secrets” associadas a esses usuários, como também conceder privilégios de operações que eles poderão, ou não poderão, realizar no SAGE.

Essa autenticação é processada de forma concomitante tanto para os usuários cadastrados no “Acesso Legado” do SAGE quanto para os usuários cadastrados nos “Servidores AD Corporativo e ou Operativo” da empresa.

Na autenticação dos usuários MQTT nas plataformas *Desktop WEB*, como o Grafana, o servidor Nginx deve estar configurado com a exigência do certificado digital pessoal do usuário (gerenciado pelo *AdmCertificados*) e o servidor de WebTokens *Serv_cgi_OpcUA* deve estar configurado com a exigência do código de acesso do Google-Authenticator naquele site (também gerenciado pelo *AdmCertificados*). Sendo assim, quando o usuário se conectar à URL do SAGE através do seu *Browser*, algumas informações de acesso serão necessárias como a digitação do *username/password* e código de acesso gerado pelo Google-Authenticator, conforme Figura 7. Quando o usuário está autenticado e todos os requisitos/etapas de segurança do site satisfeitos, ele pode usufruir desse *Single-Sign-On* em todas as aplicações WEB utilizadas nele. Caso o usuário não possua o certificado digital pessoal instalado no seu *Browser*, o seu acesso será negado.

Ao se autenticar cumprindo, nesse caso, todos os 3 requisitos exigidos (certificado digital, *username/password*, código do Google-Authenticator), o *Browser* do usuário recebe um WebToken JWT do servidor *serv_cgi_OpcUA*, que será atualizado a cada período de 60 segundos, enquanto esse *Browser* estiver conectado ao SAGE.

Por opção de configuração no SAGE, este token pode ser compartilhado com o Adaptador MQTT do SAGE para aceitar conexões de subscritores MQTT de *Smartphones*, cujo usuário esteja mantendo atualizado esse WebToken JWT pelo seu *Desktop WEB*.

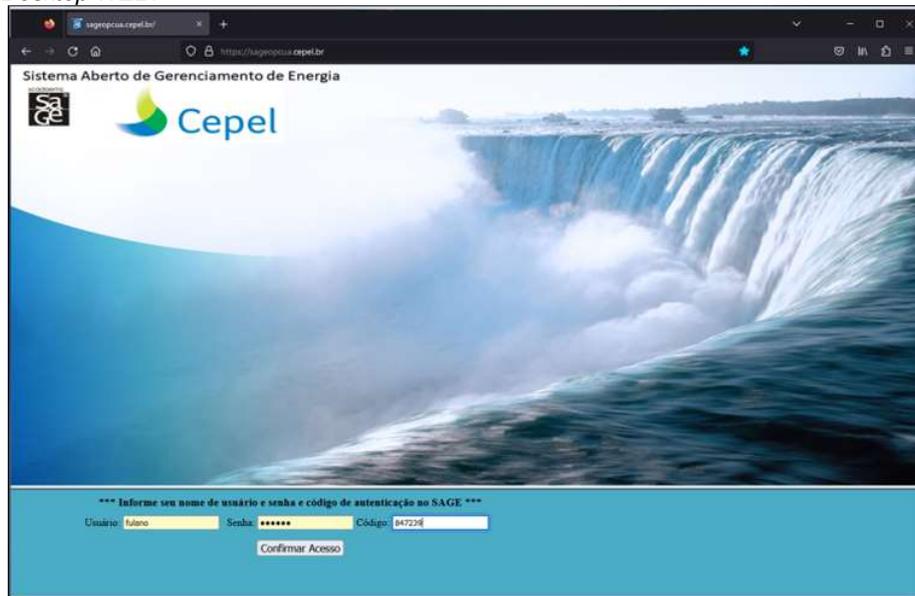


Figura 7 – Autenticação com certificado digital, *username/password*, *Google-Authenticator*

Com essa estratégia, a autenticação simples feita nos aplicativos IIoT de *Smartphones* do mercado, que utilizam apenas *username/password* no passo de autenticação, passam a compartilhar a verificação do código do *Google-Authenticator*, mantida por uma plataforma *Desktop WEB* do próprio usuário.

7.0 CONSIDERAÇÕES FINAIS

A integração do MQTT com o OPC UA do SAGE oferece uma solução robusta e eficiente para a comunicação em tempo real de dados. Ao combinar a leveza e escalabilidade do MQTT com a modelagem de dados e recursos avançados do OPC UA do SAGE, as empresas podem realizar uma comunicação eficiente, escalável e segura com *softwares* de visualização das informações em tempo real por meio de dashboards e interfaces gráficas que proporcionam uma visão abrangente e facilitam a tomada de decisões.

Como trabalho futuro, o protocolo MQTT para aquisição e controle será desenvolvido e incorporado a arquitetura do SAGE de forma a possibilitar a realização da comunicação do SAGE com os dispositivos distribuídos de IIoT e sistemas de controle. Com a contínua evolução da automação industrial e IIoT, a integração do MQTT com o OPC UA tem um papel crucial na criação de sistemas interconectados, para melhorar a eficiência operacional e impulsionar o progresso tecnológico.

8.0 REFERÊNCIAS

- [1] OLIVEIRA FILHO, A. L., SANTOS, H. T., PEREIRA, L. A. C., LIMA, L. C., LAMBERT, N., CRUZ, D., SCHIO, G. R., GOMES, D. B., LAMEIRÃO, A. M. M. S., “Soluções para a Rede de Gerenciamento de Energia do ONS – REGER”, XXI SNPTEE, Florianópolis, SC, Brasil, 2011.
- [2] BRITO, R. M., LAMBERT, N., OLIVEIRA FILHO, A. L., “Desenvolvimento e Utilização da Arquitetura OPC UA no Sistema Aberto de Gerenciamento de Energia - SAGE”, XXV SNPTEE, GOP, Belo Horizonte, MG, Brasil, 2019
- [3] BASTOS, R. L. R., BORGES, C. L. T., COSTA, M. R., DURVAL, F. V. , “Uso da Tecnologia Móvel para o Acesso a Dados de Tempo Real do Sistema Elétrico”, XXV SNPTEE, GTL, Belo Horizonte, MG, Brasil, 2019
- [4] OPC Foundation: OPC Unified Architecture Part 1 : Overview and Concepts, Release 1.04, November 2017
- [5] OPC Foundation: OPC Unified Architecture Part 14 : PubSub, Release 1.04, February 2018

