



PLANO DE TRABALHO

PARTÍCIPE 1: MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
CNPJ: 00.489.828/0074-00
ENDEREÇO: SEPN 516 Bloco D lote 8
CIDADE: Brasília UF: DF CEP: 70770-524
ÁREA RESPONSÁVEL: Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos - SGD/MGI
GESTOR: ROGÉRIO SOUZA MASCARENHAS
CARGO: Secretário de Governo Digital
TELEFONE: (61) 2020-2407 EMAIL: despd@gestao.gov.br

PARTÍCIPE 2: Fundação CPQD
CNPJ: 02.641.663/0001-10
ENDEREÇO: Dr. Ricardo Benetton Martins, 1000 - Parque II
CIDADE: Campinas UF: SP CEP: 13086-902
ÁREA RESPONSÁVEL: Diretoria de Tecnologia e Novos Produtos - DTEC
GESTOR: SEBASTIÃO SAHÃO JUNIOR
CARGO: Presidente de Tecnologia
TELEFONE: (19) 3705-6200 EMAIL: tuca@cpqd.com.br

1. IDENTIFICAÇÃO DO OBJETO

Título:	Prova de Conceito da Identidade Digital Descentralizada
Descrição do Objeto:	Estabelecer uma colaboração entre a SGD/MGI e o CPQD visando a avaliação das potencialidades de uso da Identidade Digital Descentralizada nos serviços de Governo Digital.
Duração:	12 meses contados da assinatura do acordo
Área Temática:	Governo Digital

2. DAS DEFINIÇÕES

I. API: Interface de Programação de Aplicativos (*Application Programming Interface*) que contém instruções e padrões de programação definidos, para acesso por um terceiro a um aplicativo ou software de outrem. As APIs provêm pontos de entrada e documentação técnica para determinar como um programador pode realizar uma tarefa através de operações de sistemas informatizados;

II. *Decentralized Identifier* (DID)^[1] - Identificador Descentralizado: no nível mais básico, um identificador descentralizado (DiD) é simplesmente um novo tipo de identificador global, não muito diferente das URLs. DiDs são considerados como uma nova camada de identidade digital descentralizada semelhante ao que é a infraestrutura de chave pública para a Internet. Os DiDs são a contrapartida criptográfica das credenciais

verificáveis e juntos são considerados os pilares da IDD;

III. Carteira digital: consiste em software que permite que o usuário gere, armazene, gerencie e proteja chaves criptográficas, credenciais verificáveis, identificadores descentralizados (DIDs) e outros dados privados confidenciais. As carteiras podem ser instaladas em diferentes dispositivos, tais como smartphones e notebooks;

IV. Credencial verificável (VCs) ^[2]: trata-se de um conceito chave de um sistema de identidade digital descentralizada e é a representação digital de credenciais físicas, tais como uma Carteira Nacional de Habilitação (CNH), Registro Geral de Identidade (RG), diploma e certificados, dentre outros exemplos;

V. Credencial Verificável Digital Fundacional: credencial verificável emitida por órgão de governo, por exemplo, a SGD/MGI;

VI. *DID Document*: o documento DID é um conjunto de dados que descreve um Identificador Descentralizado, incluindo mecanismos, como chaves públicas e biometria, que uma entidade pode usar para se autenticar como Identificadores Descentralizados do W3C. Um Documento DID também pode conter outros atributos ou declarações que descrevem a entidade;

VII. *Distributed Ledger Technology* (DLT): tecnologia que permite a operação e uso de livro de registros (ledger) distribuídos;

VIII. *Hyperledger Besu*: rede DLT desenvolvida pela *Hyperledger Foundation*, da *Linux Foundation*, para suportar os registros de soluções de identidade digital descentralizada.

3. PRODUTOS

3.1 Realizar um teste piloto, em ambiente relevante à SGD/MGI e ao CPQD, baseada em Identidade Digital Descentralizada (IDD) e Credenciais Verificáveis, para a disponibilização dos dados de identificação do cidadão para que este, uma vez em posse dos seus dados de sua identificação, possa prová-los com privacidade e de forma segura junto à terceiros.

3.2 Emitir uma Credencial Verificável extra a partir da credencial fundacional GOV.BR

3.3 Disponibilizar proposta de Infraestrutura Pública Digital de Credenciais Verificáveis.

3.4 Realizar um teste piloto com usuários da credencial extra em ambiente relevante.

4. DIAGNÓSTICO

A conta gov.br é uma iniciativa do governo brasileiro que visa fornecer uma identificação digital única e segura aos cidadãos brasileiros, facilitando o acesso a serviços públicos de forma eficiente e confiável. A necessidade de uma plataforma de autenticação mais abrangente surgiu com a demanda de simplificar a interação digital entre os cidadãos e o governo. Atualmente a Plataforma gov.br conta com mais de 155 milhões de usuários cadastrados, sendo considerada uma das maiores plataformas de autenticação do mundo.

A identidade digital do usuário vai além da sua autenticação. Ela pode ser usada pelo cidadão para solicitar serviços não só do governo, mas também de entidades privadas, sem a necessidade de comprovar seus dados ou sua condição a cada pedido. Para que isso seja implementado, o cidadão precisa ter o controle dos seus dados para poder compartilhar com quem deseje.

O governo, como um todo, possui muitos dados dos cidadãos, mas de forma espalhada nos diversos órgãos. A integração desses dados não é uma tarefa fácil, devido a questões legais e custos. A adoção da tecnologia *blockchain* pode ajudar nessa tarefa.

IDD é uma tecnologia emergente no cenário internacional e é considerada uma nova geração de sistemas de identidade digital para pessoas físicas, jurídicas e coisas. A tecnologia está sendo desenvolvida desde 2016 e possui as seguintes características: (I) o usuário faz gestão dos seus dados, (II) ausência de uma autoridade central, (III) o uso de *Blockchain* como forma de registro para a maioria das soluções atualmente implantadas, (IV) elevados níveis de segurança e privacidade e (V) conformidade com as leis gerais de proteção de dados, como o GDPR europeia e a LGPD no Brasil. Iniciativas internacionais vêm sendo realizadas visando o desenvolvimento da tecnologia, da padronização e a realização de testes pilotos em diferentes setores da economia e governos.

5. ABRANGÊNCIA

A abrangência do projeto é nacional, para todo o público usuário da conta gov.br. Para a realização da prova de conceito, os partícipes podem definir um grupo mais restrito, com usuários que possuem acesso ao aplicativo gov.br.

6. JUSTIFICATIVA

Com a expansão dos serviços digitais, a tendência é que os governos adotem a identidade digital descentralizada, que permita reunir as informações sobre o usuário em um local, mas sem a necessidade de centralizar os dados do usuário em um único banco de dados. Para isso, a Identidade Descentralizada fará uso de uma rede *blockchain permissionada* para registro de eventos em uma plataforma composta por APIs que permitem definir, emitir e fazer provas de credenciais do cidadão.

Como benefícios para os cidadãos, citam-se transações mais confiáveis, rápidas e sem intermediários; controle de todas as transações e informações pelo próprio usuário; ausência de um ponto único de falha; simplificação do ecossistema de identificação. além de trazer mais transparência ao processo.

7. ATIVIDADES A SEREM REALIZADAS

Para a realização deste Plano de Trabalho, estão previstas as seguintes atividades:

Atividade	Descrição
A.1 Implantação da rede <i>Hyperledger Besu</i>	Nesta atividade, estão previstas a continuidade da implantação e da configuração de uma rede DLT baseada no framework <i>open-source Hyperledger Besu</i> , para que sirva de infraestrutura para emissão e verificação de Credenciais Verificáveis.
A.2 Mapeamento do Caso de Uso	Nesta atividade, está prevista o detalhamento da jornada do caso de uso.
A.3 Disponibilização da Credencial Verificável Fundacional gov.br	Nesta atividade, está prevista a disponibilidade da Credencial Verificável Fundacional gov.br, por parte da SGD.
A.4 Desenvolvimento de aplicação para emissão de Credencial Verificável	Nesta atividade, está previsto o desenvolvimento da aplicação responsável por emitir uma credencial verificável a partir da verificação da credencial fundacional gov.br.
A.5 Adaptação do App gov.br para Gestão das Credenciais Verificáveis	Nesta atividade, estão previstas as adaptações necessárias do aplicativo gov.br, por parte da SGD, para suportar o armazenamento e gestão das Credenciais Verificáveis.
A.6 Teste em ambiente relevante	Nesta atividade, está prevista a realização de testes em ambiente relevante, que visam validar e comprovar a entrega da Credencial Verificável Fundacional gov.br, para o cidadão, assim como o uso da credencial verificável extra.
A.7 Proposta de Infraestrutura Pública Digital de Credenciais Verificáveis	Nesta atividade, está prevista a realização de estudos e proposta de Infraestrutura Pública Digital de Credenciais Verificáveis.
A.8 Análise dos resultados	Nesta atividade, está prevista a elaboração de um relatório contendo a análise dos resultados gerados.

5. RESULTADOS ESPERADOS

Ao final de sua vigência, este Plano de Trabalho deverá ter como entrega:

- I. Aplicação para emissão de credencial a partir da Credencial Fundacional gov.br;
- II. Infraestrutura para emissão e verificação de Credenciais Verificáveis;
- III. Proposta de Infraestrutura Pública Digital de Credenciais Verificáveis;
- IV. Relatório com resultados dos testes em ambiente relevante e respectiva análise dos resultados.

6. CRONOGRAMA DE EXECUÇÃO DAS ATIVIDADES E RESPONSÁVEIS

Segue o cronograma das atividades e respectivos PARTÍCIPES responsáveis:

Atividade / mês	1	2	3	4	5	6	7	8	9	10	11	12	Responsável
A.1 Implantação da rede Hyperledger Besu	x	x	x	x	x	x	x	x	x	x	x	x	CPQD
A.2 Mapeamento do Caso de Uso	x	x	x										CPQD e SGD/MGI
A.3 Disponibilidade da Credencial Verificável Fundacional gov.br	x	x	x	x	x	x	x	x	x	x	x	x	CPQD e SGD/MGI
A.4 Desenvolvimento de aplicação para emissão de Credencial Verificável extra				x	x	x	x	x					CPQD e SGD/MGI
A.5 Adaptação do App gov.br para Gestão das Credenciais Verificáveis		x	x	x	x	x	x	x					CPQD e SGD/MGI
A.6 Teste em ambiente relevante								x	x	x	x		CPQD e SGD/MGI
A.7 Proposta de Infraestrutura Pública Digital de Credenciais Verificáveis							x	x	x	x	x	x	CPQD
A.8 Análise dos resultados											x	x	CPQD e SGD/MGI

7. METODOLOGIA DE INTERVENÇÃO E OBRIGAÇÕES DAS PARTES

Para o presente Acordo de Cooperação não está prevista qualquer transferência de recursos ou

compartilhamento de bens.

Caberá ao CPQD:

- Disponibilizar as bibliotecas e APIs de *backend* necessárias para a adaptação do aplicativo da SGD;
- Desenvolver a aplicação para a emissão das credencial extra;
- Disponibilizar uma rede *Hyperledger Besu*.

Caberá à SGD/MGI:

- Disponibilizar a credencial fundacional gov.br para a emissão da credencial extra;
- Adaptar o aplicativo gov.br para gestão das Credenciais Verificáveis.

8. DA PROPRIEDADE INTELECTUAL

Os componentes desenvolvidos no contexto da atividade A.4 serão disponibilizados em código fonte e poderão ser utilizados por ambas as partes, de forma independente, em futuras iniciativas relacionadas ao objeto deste acordo.

9. MECANISMOS DE ACOMPANHAMENTO E FISCALIZAÇÃO

A execução será acompanhada pelos gestores designados pelos partícipes.

Ao final da execução, deverá ser encaminhado Relatório de Cumprimento do Objeto, com o detalhamento da execução, dificuldades encontradas, metas cumpridas e resultados alcançados.

Aprova-se o presente Plano de Trabalho.

ROGERIO SOUZA MASCARENHAS

Secretário de Governo Digital

Ministério da Gestão e da Inovação em Serviços Públicos

SEBASTIÃO SAHÃO JUNIOR

Presidente da Fundação CPQD

[1] <https://www.w3.org/TR/did-core/>

[2] <https://www.w3.org/TR/vc-data-model/>



Documento assinado eletronicamente por **Sebastião Sahão Junior, Usuário Externo**, em 26/06/2026, às 09:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Rogério Souza Mascarenhas, Secretário(a)**, em 26/06/2026, às 17:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://colaboragov.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **62333343** e o código CRC **9191FBD0**.

Referência: Processo nº 19974.101582/2023-66.

SEI nº 62333343