

IDENTIDADE NA SOCIEDADE DIGITAL

A Abordagem UbID

Identidade Digital com Preservação da Privacidade

WHITE PAPER

Privacidade global, proteção de dados pessoais, blockchain/DLT, proteção criptográfica
Desenvolvido pela Paradigma SpA, Chile.

Preparado por

Paradigma SpA, Chile — Liderança Institucional e Tecnológica do UbID

Data de publicação: 30 de julho de 2026

Enquadramento jurídico

O UbID pode fornecer controles técnicos e evidências que apoiam de forma material a conformidade. Ele não torna, por si só, uma instituição automaticamente em conformidade. Cada implantação deve atribuir as responsabilidades de controlador, operador, emissor, serviço do titular e verificador; selecionar as bases legais; configurar os procedimentos de retenção e de atendimento aos titulares dos dados; concluir as avaliações exigidas; e obter qualquer certificação, registro ou aprovação regulatória obrigatória.

SUMÁRIO

Conteúdo

Resumo Executivo	3
Principais Conclusões	3
Escopo e Método	4
Contexto do Desenvolvedor e Institucional: Paradigma SpA Chile	5
Contribuição Estratégica da Paradigma	5
Identidade na Sociedade Digital: A Abordagem UbID	5
As limitações da identidade digital gerenciada de forma centralizada	6
Identidade descentralizada e o desafio da chave privada	6
Um novo paradigma: identidade digital autogerenciada	7
UbID: uma infraestrutura segura de identidade centrada na pessoa	8
Benefícios para as pessoas	8
Benefícios para as instituições	9
Confiança sem centralização desnecessária	10
Divulgação seletiva e verificação com preservação da privacidade	10
Custódia segura de documentos e credenciais	10
Autenticação forte sem dependência de um único fator	11
Recuperação como protocolo de segurança	11
Continuidade da identidade em múltiplos dispositivos	12
Preparando a identidade para a era pós-quântica	12
Interoperabilidade em vez de mais um silo de identidade	12
Auditabilidade, observabilidade e responsabilização institucional	13
Uma plataforma para colaboração institucional	13
Habilitando agentes digitais confiáveis	13
Uma nova distribuição de responsabilidades	14
O valor mais amplo do UbID	14
Contribuição do UbID para a Regulação e a Proteção de Dados	15
Arquitetura de Conformidade entre Jurisdições	15
Limite de Governança: O que o UbID não substitui	15
Estudo Regulatório de Blockchain e Registros Distribuídos	16
Regra de Proteção de Dados para Implantações em Blockchain	16
Regra de Implantação do UbID entre Jurisdições	16
Proteção Criptográfica, TEE e KMS	17
Arquitetura de Segurança em Camadas	17
Ambientes de Execução Confiáveis e Dados em Uso	17
Perfis TEE de Custodiante e TEE de Borda	17
Protocolo de Liberação Atestada de Chaves e Fragmentos	17
Criptografia Pós-Quântica e Criptoagilidade	18
Ancoragem em Blockchain e Segurança Criptográfica	18
Requisitos de Governança e Garantia para Produção	18
Perfil de Controles Regulatórios do UbID	19
Matriz Comparativa de Jurisdições	20
Proposta de Valor Regulatório	21
Limitações e Aviso Legal	21
Referências	22

Resumo Executivo

A identidade está se tornando uma infraestrutura reutilizável de confiança, em vez de uma coleção de contas isoladas. O UbID impulsiona essa transição ao combinar credenciais controladas pelo titular, divulgação seletiva, verificação criptográfica, autenticação forte, recuperação distribuída, continuidade em múltiplos dispositivos, custódia criptografada de documentos, governança institucional e uma trajetória progressiva rumo ao pós-quântico.

A mesma arquitetura também aborda um problema regulatório central: as organizações rotineiramente coletam e retêm mais dados pessoais do que necessitam. O UbID pode permitir que um verificador receba uma prova criptograficamente confiável de um fato sem receber o documento ou perfil completo subjacente. Isso favorece a minimização de dados, a limitação de finalidade, a privacidade desde a concepção, a redução do impacto de violações e uma responsabilização mais transparente entre jurisdições.

Principais Conclusões

- O UbID é mais bem posicionado como uma infraestrutura de identidade que amplia a privacidade e viabiliza a conformidade, e não como um produto de conformidade jurídica automática.
- A divulgação seletiva e as provas derivadas podem reduzir de forma material a quantidade de dados pessoais coletados pelas partes confiantes.
- O controle pelo titular fortalece a transparência e a autonomia, mas as instituições ainda precisam de bases legais, avisos, contratos, políticas de retenção e procedimentos de resposta aos direitos dos titulares.
- A recuperação distribuída e os controles do ciclo de vida dos dispositivos podem reduzir o risco de tomada de conta sem devolver todo o poder de recuperação a um único administrador.
- O tratamento biométrico deve ser opcional ou juridicamente justificado, isolado, vinculado a uma finalidade e regido por regras de consentimento, retenção e segurança específicas de cada jurisdição.
- A Europa e o Reino Unido oferecem estruturas formais de identidade digital que o UbID pode ter como alvo, mas o status regulado e os selos de confiança exigem certificação e registro independentes.
- A Lei chilena nº 21.719 cria uma prioridade imediata de implementação antes de sua entrada em vigor em 1º de dezembro de 2026.
- A Colômbia exige evidências robustas de autorização, limitação de finalidade, segurança e procedimentos efetivos de habeas data em seu marco atual.
- Os Estados Unidos exigem uma camada de conformidade configurável por estado e por setor, em vez de um único perfil nacional de privacidade.
- Uma única implantação global deve utilizar perfis de jurisdição versionados, em vez de tentar forçar todos os países a uma única configuração de privacidade.
- Nova York e Califórnia exigem camadas distintas nos Estados Unidos: Nova York enfatiza salvaguardas razoáveis e governança de violações, enquanto a Califórnia acrescenta amplos direitos do consumidor, controles de dados sensíveis, avaliações de risco, auditorias de cibersegurança e requisitos para decisões automatizadas.
- Os regimes latino-americanos convergem cada vez mais em responsabilização, direitos dos titulares dos dados, salvaguardas para dados sensíveis e controles de transferência, mas suas autoridades, bases legais, procedimentos e maturidade de implementação continuam específicos de cada jurisdição.
- As implantações na Ásia exigem tratamento adaptado: Hong Kong está organizado em torno de seis princípios de proteção de dados; a Coreia do Sul aplica um regime abrangente de PIPA, com expectativas rigorosas para biometria e operadores estrangeiros; e o Japão exige separação entre a conformidade com a APPI e o ecossistema especial My Number/JPKI.
- O UbID foi desenvolvido pela Paradigma SpA, Chile, cuja proposta institucional se concentra em ecossistemas de identidade digital seguros, interoperáveis e resistentes a fraudes. [35]

A análise ampliada também distingue a tecnologia blockchain da atividade regulada de criptoativos, avalia o perímetro operacional nas mesmas jurisdições e define os controles em camadas de criptografia, execução confiável e KMS necessários para proteger os dados do UbID em repouso, em trânsito e em uso. As leis de blockchain e criptoativos são tratadas como uma camada funcional separada; não se presume licenciamento, autorização ou status jurídico a partir do uso de criptografia ou de padrões de identidade descentralizada.

- A tecnologia blockchain constitui um componente estrutural do UbID, e não um recurso meramente opcional. A identidade criptográfica do usuário é vinculada a um endereço STX derivado de sua chave pública, fornecendo um identificador blockchain verificável e permitindo comprovar o controle sobre a identidade sem revelar a chave privada. A chave privada permanece sob o controle exclusivo do usuário e é armazenada em um cofre criptográfico local e criptografado. Portanto, a blockchain Stacks não criptografa nem armazena diretamente a chave privada; em vez disso, fornece o vínculo criptográfico, a verificabilidade e a rastreabilidade necessários para associar com segurança a identidade UbID à conta blockchain do titular.
- Os controles TEE e KMS fornecem defesa em profundidade para dados em uso e chaves institucionais, mas exigem atestação, privilégio mínimo, governança do ciclo de vida das chaves, garantia independente e recuperação testada.
- As funções reguladas de criptoativos devem ser segregadas da plataforma de identidade e avaliadas de forma independente em cada jurisdição.

Escopo e Método

A análise regulatória baseia-se em legislação primária, orientações de autoridades supervisoras e padrões vigentes na data de corte da pesquisa. Ela se concentra na proteção geral de dados pessoais e nas obrigações de identidade digital. Requisitos setoriais específicos podem se aplicar a finanças, saúde, seguros, emprego, educação, telecomunicações, governo e infraestrutura crítica.

A palavra “alinhamento” neste documento significa que uma capacidade do UbID pode apoiar ou fornecer evidências para um requisito jurídico ou de governança. Isso não significa que toda configuração padrão satisfaça todas as jurisdições, nem que uma implementação tenha sido certificada, aprovada ou reconhecida por uma autoridade.

Princípio operacional

A conformidade deve ser expressa por meio de perfis de jurisdição e controles de política: a mesma tecnologia de credenciais pode ser utilizada globalmente, enquanto as bases legais, regras de divulgação, períodos de retenção, condições biométricas, prazos de incidentes, salvaguardas de transferência e fluxos de trabalho dos titulares dos dados são configurados para a instituição e o local em que ocorre o tratamento.

Os perfis de jurisdição são referências estratégicas de implementação. Eles identificam os principais marcos de privacidade e identidade, a contribuição técnica que o UbID pode oferecer e os controles que as instituições ainda precisam implementar. A revisão jurídica local continua necessária antes da implantação em produção, especialmente quando regulamentos, orientações de fiscalização, esquemas de certificação ou datas de entrada em vigor estiverem em evolução.

Contexto do Desenvolvedor e Institucional: Paradigma SpA Chile

O UbID foi desenvolvido pela Paradigma SpA, Chile. O site oficial da Paradigma descreve a empresa como uma organização voltada à gestão de TI e à transformação digital estratégica, com a missão de arquitetar estruturas de identidade seguras, interoperáveis e resistentes a fraudes para instituições. [35]

A Paradigma apresenta sua proposta de identidade como um ecossistema unificado Emissor–Titular–Verificador destinado a prevenir fraudes de identidade, apoiar a conformidade institucional e viabilizar interações digitais confiáveis. Seu portfólio mais amplo também faz referência à automação de infraestrutura, à nomenclatura confiável de identidades e à colaboração institucional descentralizada. [35]

Neste white paper, a contribuição da Paradigma é expressa por meio da arquitetura UbID: credenciais controladas pelo titular, divulgação seletiva, proveniência verificável, autenticação forte, custódia criptografada, recuperação distribuída, continuidade em múltiplos dispositivos, observabilidade e uma trajetória progressiva rumo ao pós-quântico. A análise regulatória não trata essas capacidades como uma certificação automática; ela explica como as instituições podem configurá-las e comprová-las de acordo com a legislação aplicável.

Contribuição Estratégica da Paradigma

- Uma plataforma de identidade desenvolvida no Chile e projetada para interoperabilidade internacional, em vez de um único silo de identidade doméstico.
- Uma arquitetura que amplia a privacidade e permite às instituições verificar alegações, reduzindo ao mesmo tempo a replicação desnecessária de documentos e a concentração de dados pessoais.
- Um modelo de governança que separa as responsabilidades de emissor, titular, verificador, custodiante e infraestrutura, favorecendo uma responsabilização mais clara.
- Uma camada de controle que viabiliza a conformidade e é capaz de aplicar políticas de jurisdição, setor, finalidade, garantia, retenção, transferência e gestão de direitos.
- Uma estratégia de segurança de longo prazo que combina a criptografia interoperável atual com uma migração controlada para proteções pós-quânticas.

Identidade na Sociedade Digital: A Abordagem UbID

Os serviços de identidade são fundamentais para as sociedades modernas. Todos os países fornecem credenciais de identidade — como cédulas nacionais de identidade, passaportes, autorizações de residência e carteiras de habilitação — que funcionam como uma raiz de confiança para pessoas que interagem com instituições públicas, empresas privadas e outras pessoas.

Essas credenciais permitem que os cidadãos demonstrem quem são em ambientes físicos. Entretanto, sua confiabilidade depende da integridade do documento, da autoridade emissora e do processo de verificação. Quando um documento de identidade é alterado, falsificado, roubado ou obtido de forma fraudulenta, as pessoas ficam expostas a roubo de identidade, personificação, crimes financeiros e danos à reputação. As instituições, por sua vez, enfrentam perdas operacionais, exposição regulatória, fraude e uma erosão progressiva da confiança em seus serviços.

O desafio se torna significativamente mais complexo em ambientes digitais. Quando a identidade precisa ser verificada remotamente, o reconhecimento físico e a inspeção direta de um documento original já não são suficientes. Uma fotografia, um documento digitalizado, uma videochamada ou uma consulta a banco de dados podem fornecer evidências, mas cada mecanismo introduz novos riscos relacionados à manipulação, identidades sintéticas, deepfakes, bancos de dados comprometidos, ataques de repetição e engenharia social.

Credenciais perdidas ou roubadas geralmente exigem reemissão pela autoridade original. Em sistemas digitais, a verificação de identidade tradicionalmente dependeu de nomes de usuário, senhas, perguntas de segurança, códigos de uso único e diferentes formas de autenticação multifator. Esses mecanismos normalmente se baseiam em algo que a pessoa sabe,

possui ou é. Embora melhorem a segurança quando combinados, todos eles já foram comprometidos em determinadas circunstâncias.

Senhas podem ser adivinhadas, reutilizadas, obtidas por phishing ou vazadas. Telefones celulares e cartões SIM podem ser roubados ou duplicados de forma fraudulenta. Contas de e-mail podem ser sequestradas. Informações biométricas podem ser capturadas, reproduzidas ou armazenadas de forma insegura. Os procedimentos de recuperação costumam ser ainda mais vulneráveis do que o método original de autenticação, transformando a recuperação de conta em um dos principais pontos de entrada para o roubo de identidade.

Esses riscos são especialmente graves em domínios de alto valor, como bancos, saúde, seguros, serviços governamentais, telecomunicações, infraestrutura crítica e administração de sistemas. Nesses setores, uma personificação bem-sucedida não apenas expõe uma conta: ela pode permitir transferências financeiras, acesso a informações médicas sensíveis, contratação fraudulenta, alterações não autorizadas em infraestrutura ou a assunção da identidade jurídica de uma pessoa.

As limitações da identidade digital gerenciada de forma centralizada

Tradicionalmente, a identidade digital reproduziu o modelo de identidade física. Uma autoridade central cria uma conta, armazena os atributos da pessoa, define os mecanismos de autenticação e decide quando o acesso deve ser concedido ou revogado. A instituição torna-se, portanto, ao mesmo tempo emissora da identidade e custodiante das informações a ela associadas.

Esse modelo possibilitou a expansão dos serviços digitais, mas também produziu grandes concentrações de informações pessoais. Cada repositório central de identidade torna-se um alvo potencialmente valioso. Uma única violação pode expor as informações de milhares ou milhões de pessoas, enquanto os indivíduos têm visibilidade ou controle limitados sobre como seus dados de identidade são copiados, tratados, compartilhados, retidos ou reutilizados.

O modelo também cria fragmentação. Uma pessoa pode ter dezenas ou centenas de identidades digitais independentes em bancos, universidades, hospitais, empregadores, portais governamentais, redes sociais e serviços comerciais. Cada organização repete processos semelhantes de identificação, armazena outra cópia das mesmas informações pessoais e assume o custo e o risco de protegê-las.

As instituições, portanto, gastam recursos consideráveis verificando repetidamente informações que podem já ter sido validadas por outra organização confiável. As pessoas são obrigadas a enviar os mesmos documentos várias vezes, divulgar mais informações do que o necessário e depender dos procedimentos de segurança e recuperação de cada provedor.

Identidade descentralizada e o desafio da chave privada

As tecnologias de criptografia e blockchain demonstraram que ativos digitais e identificadores descentralizados podem ser controlados sem depender inteiramente de um operador central. Uma pessoa que controla uma chave privada criptográfica pode autenticar operações, assinar mensagens e demonstrar controle sobre um identificador digital.

Entretanto, a adoção ampla dessas tecnologias tem sido limitada pela dificuldade de gerenciar chaves privadas com segurança. Uma chave privada pode oferecer forte proteção matemática, mas sua perda pode resultar em perda permanente de acesso. Copiá-la para um local inseguro, armazená-la em texto simples ou expô-la por meio de um dispositivo comprometido pode permitir que um invasor assuma o controle da identidade.

Os mecanismos tradicionais de recuperação frequentemente reintroduzem a mesma centralização que a identidade descentralizada pretendia evitar. Ao mesmo tempo, os avanços na computação quântica criam um risco de longo prazo para algoritmos criptográficos cuja segurança depende de problemas matemáticos que computadores quânticos suficientemente capazes poderão eventualmente resolver.

O desafio, portanto, não consiste apenas em criar identificadores descentralizados. Uma arquitetura completa de identidade digital deve proteger as chaves, oferecer recuperação segura, operar em múltiplos dispositivos, permitir divulgação controlada de atributos pessoais, permanecer interoperável com sistemas institucionais e fornecer um caminho de migração crível para a segurança pós-quântica.

Um novo paradigma: identidade digital autogerenciada

Está surgindo um novo modelo no qual as pessoas podem gerenciar seus próprios identificadores descentralizados e associar a eles atributos verificáveis. Esses atributos podem ser autodeclarados ou emitidos por terceiros confiáveis, como governos, universidades, empregadores, bancos, entidades profissionais, organizações de saúde e autoridades certificadoras.

As credenciais resultantes permanecem sob o controle do titular e podem ser verificadas criptograficamente por destinatários autorizados. Em vez de consultar o emissor toda vez que uma pessoa precisa provar algo, um verificador pode validar a integridade, a proveniência, o período de validade, o status e a relação da credencial com o titular.

Isso altera fundamentalmente o modelo de identidade digital. A pessoa deixa de ser representada exclusivamente por contas mantidas por organizações externas. O indivíduo passa a possuir uma coleção reutilizável e portátil de credenciais verificáveis criptograficamente, que podem ser apresentadas em diferentes serviços e contextos.

Nesse modelo, uma pessoa nem sempre precisa revelar um documento de identidade completo. Ela pode demonstrar apenas as informações necessárias para uma transação específica — por exemplo, que possui idade superior a determinado limite, que detém uma certificação profissional válida, que está autorizada a representar uma organização ou que possui uma apólice de seguro ativa.

A divulgação seletiva reduz a exposição desnecessária de dados e apoia o princípio da minimização de dados. As instituições recebem as evidências de que necessitam sem obter automaticamente uma cópia completa do perfil de identidade da pessoa.

UbID: uma infraestrutura segura de identidade centrada na pessoa

O UbID foi projetado para transformar esse paradigma emergente em uma infraestrutura prática de identidade para pessoas e instituições. Ele combina identificadores descentralizados, credenciais verificáveis, divulgação seletiva, autenticação forte, custódia local criptografada, recuperação controlada, gestão de múltiplos dispositivos, verificação institucional e proteção pós-quântica progressiva.

Seu objetivo não é eliminar instituições confiáveis. Governos, universidades, bancos, prestadores de saúde, empregadores e organismos certificadores continuam sendo fontes essenciais de informações autoritativas. O UbID muda a forma como a confiança é criada, transportada, verificada e controlada.

As instituições continuam emitindo alegações autoritativas, mas as pessoas podem manter e reutilizar essas alegações sem exigir que cada verificador mantenha outra cópia isolada dos mesmos dados. A confiança torna-se portátil, verificável criptograficamente e sujeita ao controle explícito do titular.

Benefícios para as pessoas

Para as pessoas, o UbID oferece uma identidade digital portátil e não confinada permanentemente a um único provedor, aplicativo ou dispositivo. A pessoa pode manter o controle sobre suas credenciais de identidade e decidir quando, onde e para qual finalidade elas serão apresentadas.

Isso reduz a dependência de senhas e de procedimentos centralizados de recuperação de conta. A autenticação pode ser reforçada por passkeys, verificação biométrica, dispositivos confiáveis, provas criptográficas e combinações desses mecanismos baseadas em políticas.

O UbID também aborda um dos problemas mais difíceis da identidade autogerenciada: a recuperação segura. Em vez de depender de um único código de recuperação, administrador, conta de e-mail ou provedor de nuvem, a recuperação pode ser distribuída entre componentes protegidos de forma independente, utilizando criptografia de limiar.

Com um modelo de limiar, nenhum custodiante, servidor ou dispositivo isolado precisa possuir o segredo completo de recuperação. Um número definido de fragmentos válidos deve participar antes que a recuperação possa prosseguir. Isso reduz o risco de uma única parte comprometida assumir o controle da identidade.

A recuperação também pode ser condicionada a evidências robustas, incluindo comunicações autenticadas, aprovação de dispositivo, verificação biométrica, verificações de política, nonces, proteção contra repetição e eventos de autorização auditáveis. O objetivo é tornar a recuperação possível para a pessoa legítima e, ao mesmo tempo, tornar a recuperação fraudulenta substancialmente mais difícil.

O modelo de múltiplos dispositivos do UbID permite que uma pessoa utilize sua identidade a partir de um conjunto controlado de dispositivos autorizados. Novos dispositivos podem exigir aprovação explícita, enquanto dispositivos perdidos ou comprometidos podem ser revogados sem necessariamente invalidar toda a identidade digital da pessoa.

A pessoa também pode manter um cofre criptografado de documentos para credenciais e documentos de apoio. Informações sensíveis podem ser criptografadas localmente com chaves derivadas e protegidas por mecanismos criptográficos reforçados. O cofre tem como objetivo minimizar a exposição desnecessária de informações de identidade não criptografadas a servidores ou intermediários.

Para as pessoas, essas capacidades se traduzem em benefícios práticos:

- Menor dependência de senhas e de perguntas de segurança vulneráveis.
- Maior controle sobre informações pessoais e sobre a divulgação de credenciais.
- Menor necessidade de enviar repetidamente cópias de documentos de identidade.
- Portabilidade de credenciais entre serviços compatíveis.
- Cadastro mais seguro de dispositivos adicionais.
- Revogação controlada de dispositivos perdidos ou comprometidos.
- Proteção mais forte contra tomada de conta e recuperação fraudulenta.

- Apresentação seletiva somente dos atributos necessários para uma transação.
- Prova criptográfica da integridade e da proveniência da credencial.
- Um caminho progressivo de migração para proteção resistente a computadores quânticos.
- Maior continuidade da identidade mesmo se um determinado provedor de serviço ficar indisponível.

Mais importante, o UbID separa a identidade de qualquer conta individual. A identidade da pessoa não é apenas um registro em banco de dados pertencente a uma plataforma. Ela se torna um conjunto de relações controladas e verificáveis entre a pessoa, seus identificadores, seus dispositivos e as instituições que lhe emitiram credenciais.

Benefícios para as instituições

Para as instituições, o UbID fornece um mecanismo para receber evidências de identidade mais robustas, mais estruturadas e verificáveis criptograficamente.

Em vez de aceitar apenas fotografias, fotocópias, dados inseridos manualmente ou arquivos PDF não verificáveis, uma organização pode validar se uma credencial foi emitida por uma autoridade reconhecida, se foi alterada, se continua válida e se a pessoa que a apresenta é um titular autorizado.

Isso pode reduzir fraudes documentais, revisão manual, repetição de processos de comprovação de identidade e o custo operacional de manter grandes quantidades de dados pessoais duplicados.

As instituições podem emitir credenciais reutilizáveis além de suas próprias plataformas. Uma universidade pode emitir uma credencial acadêmica verificável digitalmente. Uma entidade profissional pode emitir uma licença ou certificação. Um empregador pode emitir uma credencial de vínculo empregatício ou função. Um banco pode atestar que um cliente concluiu um processo específico de verificação. Uma autoridade governamental pode emitir atributos de identidade ou autorizações.

Cada credencial pode ser verificada de acordo com políticas definidas sem exigir que o verificador estabeleça uma integração proprietária com cada banco de dados original.

O UbID também oferece suporte a um modelo institucional com maior preservação da privacidade. As organizações podem solicitar apenas os atributos exigidos para uma finalidade específica. Isso reduz a quantidade de informações pessoais coletadas e armazenadas, diminuindo tanto o risco de privacidade quanto o impacto de uma possível violação.

Por exemplo, um serviço pode precisar saber que uma pessoa é legalmente adulta, mas não necessariamente sua data exata de nascimento. Uma instituição pode precisar de prova de que uma licença profissional é válida, mas não do histórico educacional completo da pessoa. Uma empresa pode precisar confirmar que um indivíduo está autorizado a representar outra organização sem obter dados pessoais não relacionados.

Isso melhora a conformidade com os princípios de minimização de dados, limitação de finalidade, proporcionalidade e privacidade desde a concepção.

Do ponto de vista operacional, as instituições se beneficiam de:

- Maior garantia quanto à origem e à integridade das credenciais.
- Menor exposição a documentos falsificados, alterados ou reproduzidos.
- Menores custos de verificação de identidade e de revisão manual.
- Menos repositórios duplicados de informações pessoais sensíveis.
- Maior segurança no onboarding e na recuperação de contas.
- Tratamento mais claro de status, expiração, suspensão e revogação de credenciais.
- Políticas de verificação reutilizáveis para múltiplos tipos de credenciais.
- Melhor auditabilidade dos eventos de emissão, apresentação, verificação e recuperação.
- Maior interoperabilidade entre organizações públicas e privadas.
- Menor dependência de silos proprietários de identidade.
- Um caminho controlado para introduzir proteção criptográfica pós-quântica.
- A capacidade de automatizar a verificação sem automatizar integralmente decisões finais sensíveis.

O UbID também pode apoiar modelos de governança institucional nos quais ações de alto impacto seguem uma sequência controlada, como preparar, validar, aprovar e executar. Um sistema automatizado pode preparar e validar tecnicamente uma solicitação de credencial, enquanto a emissão final, a revogação, a recuperação ou o acesso de alto risco permanecem sujeitos a uma decisão institucional autorizada.

Esse equilíbrio permite que as instituições se beneficiem da automação, mantendo a responsabilização, a segregação de funções e a supervisão humana.

Confiança sem centralização desnecessária

O UbID não pressupõe que toda alegação de identidade seja igualmente confiável. A confiança depende do emissor, do tipo de credencial, do método de verificação, do status atual da credencial, da política aplicável e do contexto em que a credencial é apresentada.

Uma declaração autoemitida pode ser adequada para uma preferência pessoal ou um atributo de perfil de baixo risco. Uma credencial emitida pelo governo pode ser necessária para identidade legal. Uma credencial emitida por uma universidade pode comprovar um grau acadêmico. Uma entidade profissional regulada pode atestar uma licença. Um processo de verificação biométrica pode demonstrar que a pessoa que apresenta uma credencial corresponde ao titular cadastrado.

O UbID permite que esses diferentes níveis e fontes de confiança coexistam em uma arquitetura comum. O verificador pode decidir quais emissores, formatos de credencial, níveis de garantia, algoritmos criptográficos e condições de apresentação são aceitáveis para uma transação específica.

Isso cria um modelo descentralizado sem eliminar a governança. A confiança permanece mensurável, contextual e orientada por políticas.

Divulgação seletiva e verificação com preservação da privacidade

Um princípio central do UbID é que a verificação não deve exigir divulgação irrestrita.

Por meio de mecanismos de credenciais com divulgação seletiva, um titular pode revelar apenas as alegações necessárias para uma finalidade específica, mantendo ocultas as informações não relacionadas. Provas criptográficas permitem ao verificador confirmar que as alegações divulgadas pertencem a uma credencial emitida por uma entidade confiável e que não foram modificadas.

Isso estabelece uma distinção importante entre identificar uma pessoa e verificar um direito ou atributo. Muitas transações não exigem identificação completa. Elas exigem prova de uma condição específica.

O UbID pode, portanto, oferecer suporte a interações como:

- Comprovar a maioridade legal sem revelar a data de nascimento completa.
- Demonstrar residência sem divulgar atributos de identidade desnecessários.
- Confirmar status profissional sem compartilhar registros de emprego não relacionados.
- Comprovar que uma credencial está ativa sem apresentar o documento original.
- Demonstrar autoridade organizacional sem expor informações pessoais além do necessário.
- Confirmar que uma verificação de identidade foi concluída por uma instituição confiável sem repetir todo o processo.

Esse modelo melhora a privacidade e, ao mesmo tempo, reduz a responsabilidade institucional. Dados que nunca são coletados não podem vazar dos sistemas do verificador.

Custódia segura de documentos e credenciais

As credenciais de identidade frequentemente coexistem com documentos de apoio: cédulas de identidade, passaportes, certificados, contratos, licenças, registros acadêmicos, documentos de seguro e qualificações profissionais.

O UbID incorpora o conceito de um cofre criptografado de documentos no qual esses materiais podem ser protegidos e, ao mesmo tempo, permanecer associados à identidade do titular.

Os documentos podem ser classificados, processados por reconhecimento óptico de caracteres, examinados em busca de dados estruturados e submetidos a diferentes níveis de verificação. A verificação pode incluir validação de códigos QR, análise de assinatura digital, verificações de domínio institucional, verificações de consistência documental e confirmação junto a emissores reconhecidos ou fontes externas.

O resultado não é apenas armazenamento de documentos. É um ambiente controlado no qual documentos podem evoluir de arquivos não verificados para evidências estruturadas de identidade, com status de verificação e proveniência explícitos.

Isso oferece às pessoas um repositório mais útil e seguro, enquanto as instituições recebem informações mais claras sobre a confiabilidade das evidências apresentadas.

Autenticação forte sem dependência de um único fator

O UbID reconhece que nenhum fator de autenticação é infalível. A segurança, portanto, depende da combinação de fatores de acordo com o risco e o contexto.

As passkeys podem fornecer autenticação resistente a phishing. A biometria pode reforçar a prova de que o titular legítimo está presente. O registro de dispositivos pode limitar o acesso a endpoints conhecidos. Chaves criptográficas podem demonstrar controle sobre um identificador descentralizado. Políticas institucionais podem exigir aprovação adicional para ações de alto risco.

A combinação adequada pode variar. Uma apresentação de credencial de baixo risco pode exigir apenas uma prova válida do titular. Um evento sensível de recuperação pode exigir múltiplos dispositivos registrados, verificação biométrica, aprovação por limiar e validação criptográfica por desafio-resposta.

Essa abordagem baseada em políticas evita tratar todas as transações de forma idêntica e permite que os controles de segurança sejam proporcionais ao impacto potencial.

Recuperação como protocolo de segurança

Em muitos sistemas, a recuperação é tratada como uma exceção administrativa. No UbID, a recuperação é tratada como um protocolo criptográfico e de governança de primeira classe.

A recuperação deve estabelecer que o solicitante tem legitimamente o direito de recuperar o controle. Deve impedir repetição, personificação, acesso unilateral de administrador e substituição silenciosa de chaves ou dispositivos. Também deve produzir evidências que possam ser auditadas sem expor desnecessariamente o segredo recuperado.

A criptografia de limiar permite distribuir a autoridade de recuperação. Custodiantes confiáveis, componentes de infraestrutura protegidos, dispositivos aprovados ou ambientes de execução seguros podem participar sem controlar individualmente a identidade completa.

Ambientes de execução confiáveis no lado do servidor podem liberar um fragmento autorizado de acordo com uma política definida, sem reconstruir o segredo completo. Ambientes de execução confiáveis de borda podem proteger localmente operações sensíveis em dispositivos compatíveis. Comunicações criptografadas podem transportar mensagens de recuperação, enquanto evidências assinadas registram as decisões e condições que permitiram a operação.

O objetivo não é apenas recuperar o acesso. É recuperar o acesso de uma forma que preserve a credibilidade da identidade após a recuperação.

Continuidade da identidade em múltiplos dispositivos

Os usuários modernos não interagem por meio de um único dispositivo permanente. Telefones são substituídos, computadores são atualizados, dispositivos são perdidos e diferentes contextos exigem diferentes endpoints.

O UbID oferece suporte a uma identidade controlada em múltiplos dispositivos, em vez de sincronização irrestrita. Um novo dispositivo deve ser associado ao titular legítimo e pode exigir aprovação de um dispositivo já confiável ou de outro mecanismo de recuperação autorizado.

Cada dispositivo pode ter um ciclo de vida explícito: pendente, aprovado, ativo, suspenso, revogado ou substituído. Instituições e usuários obtêm visibilidade sobre quais dispositivos estão autorizados a interagir com a identidade.

Esse modelo fornece continuidade prática sem tratar todos os dispositivos como igualmente confiáveis. Ele também permite excluir rapidamente um endpoint comprometido, preservando a validade da identidade mais ampla e de suas credenciais.

Preparando a identidade para a era pós-quântica

A maioria dos sistemas atuais de identidade digital depende de criptografia clássica de chave pública. Esses algoritmos continuam essenciais para a interoperabilidade, mas a longa vida operacional das informações de identidade exige preparação para futuras transições criptográficas.

Credenciais de identidade, registros de recuperação, documentos jurídicos e atestações institucionais podem permanecer sensíveis ou valiosos por muitos anos. Informações capturadas hoje podem ser armazenadas por um invasor e visadas posteriormente, quando capacidades computacionais mais fortes estiverem disponíveis.

O UbID, portanto, incorpora uma abordagem progressiva para a segurança pós-quântica. Algoritmos clássicos podem continuar garantindo compatibilidade com wallets, verificadores e padrões atuais, enquanto assinaturas pós-quânticas adicionais, mecanismos de estabelecimento de chaves ou evidências criptográficas podem ser introduzidos em paralelo.

Uma abordagem híbrida permite que uma operação se beneficie tanto da criptografia clássica consolidada quanto de algoritmos pós-quânticos mais recentes. Isso evita uma migração abrupta que isolaria a plataforma do ecossistema existente, ao mesmo tempo em que reduz a dependência de uma única família criptográfica.

Para as instituições, isso fornece uma estratégia de migração controlada. Para as pessoas, reforça a proteção de longo prazo das chaves de identidade, dos mecanismos de recuperação e das credenciais de alto valor.

Interoperabilidade em vez de mais um silo de identidade

Uma plataforma de identidade digital gera valor limitado se as credenciais só puderem ser utilizadas dentro de seu próprio aplicativo.

O UbID é orientado a padrões reconhecidos de identidade descentralizada e credenciais, incluindo identificadores descentralizados, credenciais verificáveis, credenciais baseadas em JWT com divulgação seletiva, fluxos de emissão e apresentação de credenciais baseados em OpenID e comunicações seguras baseadas em DIDComm.

A interoperabilidade baseada em padrões permite que uma instituição emita credenciais compreendidas por sistemas externos compatíveis. Também permite que o UbID receba e valide credenciais emitidas por outras organizações confiáveis, sujeitas a políticas.

O objetivo é criar uma camada de identidade capaz de interagir com wallets, emissores, verificadores, aplicações institucionais, serviços públicos e agentes de software autorizados sem obrigar todos os participantes a adotar a mesma pilha tecnológica interna.

A interoperabilidade protege as instituições contra dependência excessiva de fornecedores e dá às pessoas maior confiança de que suas credenciais permanecerão portáteis.

Auditabilidade, observabilidade e responsabilização institucional

Uma infraestrutura de identidade confiável exige mais do que algoritmos criptográficos. As instituições precisam compreender se os serviços estão funcionando corretamente, se as políticas estão sendo aplicadas e se há atividades suspeitas em curso.

O UbID incorpora observabilidade operacional, monitoramento de integridade, métricas, alertas e evidências auditáveis. Emissão de identidade, verificação, registro de dispositivos, alterações de status de credenciais e operações de recuperação podem produzir registros estruturados adequados à investigação e à governança.

Segredos sensíveis não precisam aparecer nesses registros. Em vez disso, o sistema pode registrar as referências criptográficas, decisões de política, atores, carimbos de tempo, desafios, resultados de verificação e evidências de autorização necessários para demonstrar o que ocorreu.

Isso oferece às instituições maior capacidade para detectar anomalias, investigar incidentes, atender controles internos e demonstrar conformidade.

Uma plataforma para colaboração institucional

O UbID cria a base para que instituições cooperem sem exigir acesso irrestrito aos bancos de dados umas das outras.

Uma organização pode emitir uma credencial que outra organização verifica. O verificador não precisa necessariamente de acesso contínuo aos sistemas internos do emissor, e o emissor não precisa conhecer todos os contextos em que o titular apresenta a credencial.

Essa separação reduz a vigilância institucional desnecessária e a complexidade de integração. A confiança é transportada pela credencial, por sua prova criptográfica, por suas informações de status e pela política de verificação aplicável.

Esse modelo pode oferecer suporte a ecossistemas intersetoriais envolvendo governo, educação, finanças, saúde, emprego, seguros, telecomunicações e acreditação profissional.

Uma pessoa pode manter uma identidade digital coerente enquanto recebe diferentes credenciais de diferentes autoridades. Cada instituição continua responsável pelas alegações que emite, enquanto o titular permanece responsável por decidir como essas alegações são utilizadas.

Habilitando agentes digitais confiáveis

À medida que sistemas de inteligência artificial e agentes autônomos de software se tornam mais ativos nos processos institucionais, a identidade também precisará se estender além das sessões humanas de login.

Os agentes devem ser capazes de descobrir quais credenciais são exigidas, compreender políticas de verificação, preparar solicitações, validar condições técnicas e apresentar informações a tomadores de decisão autorizados. Entretanto, não devem receber automaticamente autoridade irrestrita para emitir credenciais, recuperar identidades ou executar ações de alto impacto.

O UbID pode fornecer interfaces controladas por meio das quais agentes autorizados acessam capacidades de identidade, esquemas de credenciais, status de emissores, políticas de recuperação, requisitos de verificação e informações operacionais.

Aplica-se o mesmo princípio: a automação pode preparar e validar, mas ações sensíveis devem continuar regidas por políticas explícitas, aprovações, autorização criptográfica e evidências de auditoria.

Isso cria um caminho para operações de identidade assistidas por máquinas sem sacrificar a responsabilização institucional nem o controle individual.

Uma nova distribuição de responsabilidades

O UbID altera a distribuição de responsabilidades na identidade digital.

A instituição continua responsável pela veracidade e pela governança das alegações que emite. A pessoa passa a controlar a custódia e a apresentação dessas alegações. O verificador continua responsável por decidir quais evidências são suficientes para uma transação. A plataforma fornece os mecanismos criptográficos, operacionais e de interoperabilidade que permitem que essas responsabilidades funcionem em conjunto.

Esse modelo reduz a expectativa de que uma única organização deva armazenar, controlar e proteger permanentemente todos os componentes da identidade de uma pessoa.

Ele também evita colocar todo o ônus sobre a pessoa. Identidade autogerenciada não deve significar que um dispositivo perdido ou um segredo esquecido resulte em exclusão permanente. Recuperação segura, continuidade em múltiplos dispositivos, credenciais institucionais, custódia criptográfica protegida e governança auditável são necessárias para tornar o controle individual viável.

O valor mais amplo do UbID

Para as pessoas, o UbID oferece autonomia, privacidade, portabilidade, continuidade e proteção mais forte contra personificação.

Para as instituições, oferece evidências de identidade de maior qualidade, menor exposição a fraudes, menor duplicação de dados sensíveis, verificação mais eficiente, melhor auditabilidade e uma base de colaboração orientada por padrões.

Para a sociedade, oferece uma alternativa ao acúmulo crescente de bancos de dados de identidade fragmentados e mecanismos de autenticação inseguros. Ele viabiliza um modelo no qual a confiança pode ser estabelecida criptograficamente, divulgada de forma proporcional, verificada de maneira independente e governada com transparência.

O UbID não trata a identidade como um documento estático, um nome de usuário ou uma senha. Trata-a como um conjunto continuamente gerenciado de relações verificáveis entre pessoas, instituições, credenciais, dispositivos, chaves criptográficas e políticas.

O objetivo final é permitir que as pessoas se representem com segurança no mundo digital, possibilitando ao mesmo tempo que as instituições confiem nas evidências recebidas — sem exigir dados desnecessários, sem depender exclusivamente de intermediários vulneráveis e sem abrir mão da segurança ou da interoperabilidade de longo prazo.

Nesse modelo, a identidade digital se torna mais do que um mecanismo de acesso. Ela se torna uma infraestrutura reutilizável de confiança para a sociedade moderna.

Contribuição do UbID para a Regulação e a Proteção de Dados

A regulação de dados pessoais não prescreve uma única arquitetura universal de identidade digital. Ela estabelece deveres relativos à licitude, equidade, transparência, finalidade, proporcionalidade, segurança, retenção, direitos individuais e responsabilização. O UbID contribui convertendo muitos desses deveres em padrões técnicos aplicáveis e evidências operacionais verificáveis.

O maior valor regulatório do UbID não está em armazenar dados de identidade com mais segurança em um novo repositório central. Seu valor está em permitir que instituições verifiquem credenciais e atributos coletando menos dados subjacentes, que titulares controlem as apresentações, que as credenciais permaneçam portáteis e que a plataforma registre as políticas e evidências criptográficas necessárias para explicar por que uma operação de identidade foi permitida.

Arquitetura de Conformidade entre Jurisdições

Objetivo regulatório	Contribuição do UbID
Minimização de dados	Divulgação seletiva, alegações derivadas e apresentações específicas para cada verificador podem revelar apenas os atributos exigidos para uma transação.
Limitação de finalidade	As solicitações de credenciais podem ser vinculadas a uma finalidade declarada, parte confiável, audiência, nonce, transação e decisão de política.
Autonomia do titular	A pessoa pode autorizar explicitamente a emissão e a apresentação, inspecionar o que é solicitado e controlar os dispositivos registrados.
Redução da duplicação	Os verificadores podem validar evidências assinadas sem reter uma cópia completa de cada documento ou perfil de origem.
Segurança desde a concepção	Criptografia, passkeys, vinculação de dispositivos, recuperação por limiar, rotação de chaves, execução segura e migração pós-quântica reduzem o risco de identidade.
Responsabilização	Eventos de emissão, apresentação, verificação, status, dispositivo e recuperação podem criar evidências auditáveis sem registrar material secreto em logs.
Viabilização de direitos	Índices de credenciais e do cofre podem apoiar fluxos de trabalho de acesso, retificação, supressão, revogação, restrição e portabilidade.
Controles de jurisdição	As políticas podem controlar residência de dados, transferência internacional, uso de biometria, retenção, base legal, tratamento de incidentes e limites para decisões automatizadas.

Limite de Governança: O que o UbID não substitui

- Determinação e documentação da base legal para cada finalidade de tratamento.
- Avisos de privacidade, linguagem de consentimento e políticas institucionais adequadas à jurisdição e ao setor.
- Contratos controlador–operador, emissor–verificador e com fornecedores, incluindo cláusulas de transferência internacional.
- Avaliações de impacto à proteção de dados, avaliações de legítimo interesse e avaliações de risco específicas do setor, quando exigidas.
- Autorização de pessoal, segregação de funções, treinamento e controles disciplinares.
- Cronogramas legais de retenção, retenções legais, deveres de gestão de registros e obrigações relativas a registros públicos.
- Registros regulatórios, certificação, avaliação de conformidade, selos de confiança ou status de serviço de confiança qualificado.
- Notificação de violações, comunicação com reguladores e medidas de reparação para pessoas afetadas.

Nenhuma alegação falsa de conformidade

Os materiais de marketing e contratuais do UbID devem distinguir entre “apoia a conformidade”, “configurado para um perfil regulatório”, “avaliado de forma independente”, “certificado” e “legalmente reconhecido”. Esses termos não são intercambiáveis.

Estudo Regulatório de Blockchain e Registros Distribuídos

A regulação de blockchain não constitui uma única categoria jurídica. Um registro distribuído pode ser utilizado como mecanismo interno de integridade, registro público, trilho de pagamento, infraestrutura de mercado, plataforma de emissão de tokens ou sistema de custódia. A legislação aplicável acompanha a função, os direitos representados, as partes atendidas e os riscos criados — e não o simples uso da palavra “blockchain”. De forma semelhante, o NIST trata blockchain como uma família técnica de registros distribuídos e vinculados criptograficamente, e não como sinônimo de criptomoeda. [36]

O cofre de identidade do UbID não deve ser descrito como uma wallet de criptoativos, a menos que efetivamente forneça serviços de criptoativos. A custódia das credenciais de identidade e das chaves de autenticação de uma pessoa é jurídica e operacionalmente diferente da custódia de valor financeiro transferível. A linguagem do produto, a separação de chaves, as APIs, os contratos, a contabilidade e os procedimentos de incidentes devem preservar esse limite. Se um módulo futuro adicionar funções de token ou de valor, será necessária uma avaliação regulatória separada, e ele não deverá herdar a aprovação da plataforma de identidade.

Regra de Proteção de Dados para Implantações em Blockchain

A análise de privacidade se aplica mesmo quando um registro armazena apenas identificadores, endereços, hashes ou valores criptografados, se esses elementos puderem ser razoavelmente vinculados a uma pessoa. As diretrizes finais sobre blockchain do European Data Protection Board, de julho de 2026, enfatizam a seleção da arquitetura, a atribuição de papéis, a proteção de dados desde a concepção, a minimização e os direitos efetivos, e alertam contra a colocação de dados pessoais on-chain quando isso conflitar com princípios de proteção de dados. O mesmo princípio de engenharia é prudente em todas as jurisdições abordadas neste documento.

- Manter credenciais, alegações, biometria, imagens de documentos, identificadores de dispositivos, dados de recuperação e históricos de apresentação fora da blockchain (off-chain).
- Se a ancoragem for justificada, publicar apenas um compromisso não reversível gerado com separação de domínio, um salt secreto ou uma construção com chave; um hash simples de dados pessoais previsíveis não constitui anonimização.
- Não presumir que criptografar dados pessoais on-chain resolve a eliminação. Texto cifrado, chaves, metadados e o risco futuro de criptoanálise devem ser avaliados durante todo o período de retenção.
- Preferir governança permissionada quando a responsabilização institucional, a localização dos nós, o controle de acesso, os procedimentos de correção e a resposta a incidentes precisarem ser aplicáveis e fiscalizáveis.
- Documentar operadores de nós, papéis de controlador e operador, governança de consenso, autoridade para alterações de software, jurisdição, retenção e o procedimento para registros contestados ou ilícitos.

Regra de Implantação do UbID entre Jurisdições

Em todas as jurisdições, a posição institucional mais segura é a separação de capacidades. O produto principal UbID deve emitir, manter e verificar evidências de identidade; uma extensão financeira ou de criptoativos deve constituir um módulo governado separadamente, com chaves, registros, operadores, licenças, avaliações de risco e procedimentos de incidentes distintos. Isso impede que um futuro recurso de token contamine as premissas de conformidade da plataforma de identidade e permite que cada instituição demonstre com precisão qual função regulada desempenha.

- Nenhum dado pessoal, payload de credencial, template biométrico ou fragmento de recuperação em uma blockchain pública.
- Nenhum valor transferível ou direito de investimento em uma credencial de identidade.
- Nenhuma capacidade institucional de movimentar ativos do titular apenas porque a instituição pode ajudar a recuperar o acesso à identidade.
- Entidades jurídicas, descrições de serviço e hierarquias de chaves separadas quando forem adicionados serviços regulados de criptoativos.

- Um perfil de jurisdição versionado deve registrar o perímetro jurídico, o regulador, a licença, a data de vigência, as atividades permitidas e as funções proibidas.

Proteção Criptográfica, TEE e KMS

O modelo de proteção do UbID deve ser avaliado nos três estados da informação: dados em repouso, dados em trânsito e dados em uso. A criptografia de um banco de dados protege apenas um desses estados. Uma infraestrutura de identidade robusta exige separação criptográfica de funções, liberação controlada de chaves, execução respaldada por hardware ou confidencial para as operações mais sensíveis, capacidade de recuperação sem um segredo universal de administrador e evidências de que o código e a política autorizados — e não apenas um usuário autenticado — permitiram uma operação.

Arquitetura de Segurança em Camadas

A arquitetura deve preservar uma hierarquia na qual os titulares controlam as credenciais, os aplicativos recebem apenas serviços criptográficos com escopo restrito, o KMS governa as chaves institucionais e as TEEs protegem a computação de alto risco em uso. Nenhuma camada substitui as demais: uma TEE sem gerenciamento sólido de chaves pode receber o segredo errado; um KMS sem execução atestada pode liberar um segredo correto para código comprometido; e algoritmos robustos não corrigem privilégios excessivos, recuperação fraca ou governança de auditoria deficiente.

Ambientes de Execução Confiáveis e Dados em Uso

Uma TEE cria um ambiente de execução isolado por hardware destinado a proteger código e dados enquanto são processados. A propriedade relevante para o UbID é a atestação remota: um componente dependente pode verificar as medições da plataforma e da carga de trabalho antes de liberar um fragmento ou uma chave. O AMD SEV-SNP protege máquinas virtuais confidenciais e adiciona proteções de integridade de memória; o Intel TDX isola domínios de confiança respaldados por hardware; o AWS Nitro Enclaves fornece computação isolada com atestação; e o OP-TEE é um ambiente complementar baseado em Arm TrustZone para Linux não seguro. [37] [38] [39] [32]

Uma TEE não torna código arbitrário confiável, não elimina vulnerabilidades de software nem substitui secure boot, aplicação de patches, controle de acesso, logging e revisão independente. As evidências de atestação devem ser verificadas em relação a uma medição e política aprovadas, incluindo requisitos de firmware e versão de segurança. Segredos não devem ser liberados para builds de depuração, bases de computação confiável desatualizadas ou medições que não possam ser vinculadas a uma versão assinada. O TEE Protection Profile da GlobalPlatform fornece uma referência de avaliação para TEEs móveis, mas continuam necessárias certificação específica do produto e garantia da implantação. [40]

Perfis TEE de Custodiante e TEE de Borda

O Perfil TEE de Custodiante do UbID é um worker de infraestrutura executado em um ambiente de computação confidencial de classe servidor, como SEV-SNP, TDX ou Nitro Enclaves. Ele valida a solicitação DIDComm autenticada, o desafio, o nonce, o contexto da transação, a janela de repetição, a decisão de política e o estado de atestação e, em seguida, libera apenas um fragmento de recuperação autorizado. Ele nunca reconstrói o segredo completo do titular e produz evidências assinadas e minimizadas da decisão.

O Perfil TEE de Borda do UbID utiliza OP-TEE ou um ambiente confiável comparável em um dispositivo Arm, gateway ou plataforma IoT adequados. Ele pode receber três fragmentos autorizados, reconstruir localmente, utilizar o segredo recuperado para a operação estritamente aprovada e zerar com segurança o material transitório sem exportar o segredo completo para o sistema operacional normal. O OP-TEE complementa as TEEs de servidor: protege a computação final na borda, enquanto as TEEs custodiantes protegem a liberação independente dos fragmentos.

Protocolo de Liberação Atestada de Chaves e Fragmentos

- O titular inicia a recuperação e recebe um identificador de transação, um desafio criptograficamente aleatório, um nonce e uma janela curta de validade.
- A TEE de borda ou de destino produz uma atestação vinculada a uma chave pública efêmera, à medição aprovada da carga de trabalho, à versão de segurança e à transação de recuperação.
- Cada custodiante valida de forma independente a autenticação do titular, a política de dispositivo e recuperação, o frescor do nonce, o estado de repetição, os controles de jurisdição e a atestação da TEE.

- O KMS autoriza apenas a operação criptográfica necessária ou encapsula um fragmento para a chave efêmera atestada; o fragmento nunca é devolvido em texto simples ao serviço comum.
- Três fragmentos são reconstruídos somente dentro da TEE de borda aprovada ou do ambiente designado do titular. O segredo completo não é registrado em logs, persistido nem exposto por diagnósticos.
- O ambiente executa a ação aprovada de rekey, abertura do cofre ou recuperação, zera com segurança os valores transitórios e emite evidências assinadas contendo identificadores e resultados, mas nenhum material secreto.

Criptografia Pós-Quântica e Criptoagilidade

O NIST FIPS 203 padroniza o ML-KEM para estabelecimento de chaves pós-quântico, e o FIPS 204 padroniza o ML-DSA para assinaturas digitais. [29] [30] O modelo de migração apropriado para o UbID é híbrido e consciente do formato: utilizar criptografia clássica para a interoperabilidade atual, adicionar ML-KEM-768 para proteger recuperações e trocas com custodiantes de longa duração contra o risco de “coletar agora, descriptografar depois” e anexar evidências ML-DSA-65 onde verificadores e formatos consigam validá-las.

O SD-JWT compacto e interoperável não deve receber uma segunda assinatura ad hoc que rompa a compatibilidade com wallets e verificadores externos. Até que os formatos consumidores padronizados ofereçam suporte a assinaturas pós-quânticas, o UbID pode manter a credencial interoperável e expor uma prova PQC vinculada separadamente ou utilizar um contêiner de múltiplas assinaturas apenas em ecossistemas controlados. Todo artefato deve indicar se o PQC é experimental, evidência paralela ou verificação obrigatória; o fallback silencioso da validação híbrida para apenas clássica deve ser proibido em fluxos que aleguem garantia pós-quântica.

Ancoragem em Blockchain e Segurança Criptográfica

Um hash em blockchain prova, no máximo, que uma determinada sequência de bytes ou compromisso existia em relação a um evento do registro; ele não prova que o documento de origem era autêntico, obtido licitamente, preciso, atual ou vinculado à pessoa correta. Essas propriedades decorrem da governança do emissor, da comprovação de identidade, das assinaturas, do status, da vinculação ao titular e da política do verificador. Portanto, o UbID deve tratar a ancoragem em blockchain como evidência opcional de carimbo de tempo ou integridade, nunca como substituto da validação da credencial.

Se a ancoragem for adotada, cada credencial deve utilizar um compromisso aleatorizado ou uma construção Merkle que impeça recuperação por dicionário e correlação entre contextos. A blockchain não deve conter DID que resolva diretamente para dados pessoais, hash de documento derivado de campos previsíveis, material biométrico, motivo de revogação ou histórico de apresentações. Os sistemas off-chain devem manter a base legal, a finalidade, a retenção e o fluxo de direitos, enquanto a governança do registro deve oferecer suporte a defeitos de software, chaves de assinatura comprometidas e entradas contestadas.

Requisitos de Governança e Garantia para Produção

- Manter uma lista de materiais criptográficos assinada que cubra algoritmos, bibliotecas, tamanhos de chaves, protocolos, perfis de certificados, raízes de confiança em hardware e datas de descontinuação.
- Classificar cada chave por proprietário, finalidade, ambiente, sensibilidade, exportabilidade, rotação, backup, revogação e procedimento de destruição.
- Utilizar mounts, chaves e políticas KMS separados para assinatura JWT, emissão de credenciais, criptografia de documentos, encapsulamento de recuperação, integridade de auditoria e ambientes de teste.
- Exigir controle duplo para geração de token root, elevação de política, operações de seal/unseal e operações com fragmentos de recuperação; preservar evidências sem registrar os fragmentos.
- Verificar a atestação da TEE, o status do firmware, a medição da carga de trabalho, a versão de segurança e as informações de revogação antes de cada liberação sensível.
- Exercitar restauração do KMS, seal/unseal, revogação de tokens, rotação de chaves, resposta a comprometimento de chave de emissor, atualização de medição da TEE e recuperação completa pelo menos em uma periodicidade definida com base em risco.
- Contratar modelagem de ameaças e testes de penetração para canais laterais, repetição, rollback, cenários de confused deputy, custodiantes mal-intencionados, comprometimento da cadeia de suprimentos e vazamento de observabilidade.
- Representar com precisão o status da implementação: objetivo de arquitetura, prova de conceito, controle testado em staging e controle com garantia para produção são alegações distintas.

Esses controles fortalecem confidencialidade, integridade, disponibilidade e responsabilização, mas não criam, por si só, conformidade jurídica ou certificação formal. As instituições continuam responsáveis pela atribuição de papéis, tratamento lícito,

regras setoriais, aceitação de riscos, garantia independente, notificação de incidentes e adequação da TEE e do módulo criptográfico selecionados a cada jurisdição e caso de uso.

Perfil de Controles Regulatórios do UbiD

Uma implantação em produção deve traduzir obrigações regulatórias em um perfil de controle versionado e legível por máquina. O perfil deve ser avaliado nos pontos de emissão, apresentação, verificação, recuperação, registro de dispositivo, ingestão de documentos e exceções administrativas. Deve oferecer suporte a camadas por país, estado ou província, setor e papel institucional, mantendo a versão exata da política utilizada em cada transação histórica.

Campo de controle	Configuração e evidências exigidas
Jurisdição e setor	País, estado ou região; setor público/privado; finanças, saúde, educação, emprego, seguros ou outro domínio.
Papel institucional	Controlador, operador, emissor, verificador, provedor de serviço do titular, custodiante, provedor de orquestração ou provedor de serviço de confiança.
Base legal	Consentimento, contrato, obrigação legal, tarefa pública, legítimos interesses ou outro fundamento autorizado, com condições para categorias especiais.
Finalidade e audiência	Finalidade declarada, instituição solicitante, audiência pretendida, identificador da transação e usos secundários proibidos.
Minimização de alegações	Alegações permitidas, provas derivadas, combinações proibidas e regras de retenção do verificador.
Garantia de autenticação	Passkey, biometria, dispositivo, desafio criptográfico, aprovação por limiar e condições de autenticação reforçada (step-up).
Tratamento de direitos	Fluxos de trabalho de acesso, correção, exclusão, supressão, oposição, restrição, portabilidade, reclamação e recurso.
Retenção e status	Validade da credencial, revogação, retenção de evidências, retenção legal, exclusão do cofre e períodos de destruição de biometria.
Transferências e residência	Regiões permitidas, operadores, mecanismos de transferência, localizações de custodiantes e restrições de telemetria.
Obrigações relativas a incidentes	Prazos de detecção, escalonamento e notificação ao regulador e às pessoas, preservação de evidências e recuperação.
Decisões automatizadas	Limites para aprovação humana, explicação, contestabilidade, monitoramento de vieses e ações automatizadas proibidas.
Status de garantia	Avaliação interna, auditoria externa, certificação, inclusão em registro, selo de confiança ou status qualificado.
Versão legal e data de vigência	Lei promulgada, data de vigência, disposição transitória, regulamento, orientação da autoridade e data de aprovação interna.
Modelo de consentimento e aviso	Linguagem de aviso exigida, granularidade do consentimento, tratamento da revogação, fundamentos legais alternativos e formato das evidências.
Dados sensíveis e biométricos	Classificação, teste de necessidade, alternativas, localização do template, acesso, retenção, destruição e requisitos antirrepetição.
Transferências internacionais	Origem, destino, destinatário, mecanismo jurídico, regra de localização, condições de transferência subsequente e controles de acesso remoto.
Fluxo de incidentes e regulador	Limites de detecção, padrão de avaliação, prazos de notificação, autoridade competente, comunicação à pessoa afetada e retenção de evidências.
Controles de decisões automatizadas	Regras aplicáveis de profiling ou ADMT, explicação, revisão humana, objeção, opt-out e requisitos de avaliação de risco.
Monitoramento de mudanças legais	Responsável, periodicidade de revisão, eventos disparadores, aprovação jurídica, substituição do perfil e migração de operações pendentes.

Matriz Comparativa de Jurisdições

Jurisdição	Marco principal	Ênfase regulatória	Contribuição do UbiD	Obrigações institucionais residuais
União Europeia	GDPR; EUDI/eIDAS 2.0	Base legal, minimização, direitos, DPIA, transferências, papéis regulados de wallet/confiança	Divulgação seletiva, controle do titular, proveniência, evidências de política	DPIA, mapeamento de papéis, transferências, conformidade/status qualificado
Reino Unido	UK GDPR; DPA 2018; DUAA 2025; DVS TF	Privacidade desde a concepção, reclamações, garantia DVS e certificação	Serviço do titular, passkeys, nível de confiança e metadados de auditoria	Deveres perante a ICO, certificação CAB, registro OfDIA
Canadá	PIPEDA; Privacy Act; regimes provinciais	Finalidades apropriadas, consentimento, salvaguardas, acesso, registros de violações, estruturas de confiança	Provas minimizadas, evidências de consentimento, roteamento de direitos, interoperabilidade de garantia	Aplicabilidade federal/provincial, PIAs, controles de violações e fornecedores
Estados Unidos — federal	FTC; HIPAA; GLBA; COPPA; leis setoriais	Práticas injustas/enganosas, segurança e deveres setoriais	Camadas configuráveis, autenticação forte, evidências de auditoria	Mapeamento setorial, contratos, procedimentos de solicitação e incidentes
Estado de Nova York	SHIELD Act; NYDFS Part 500	Salvaguardas razoáveis, notificação de violações, cibersegurança financeira	MFA/passkeys, ciclo de vida dos dispositivos, logs, recuperação distribuída	Aplicabilidade do DFS, programa de cibersegurança, testes e relatórios
Califórnia	CCPA/CPRA; regulamentações de 2026; Delete Act	Direitos, dados sensíveis, risco, auditorias de cibersegurança, ADMT e opção de exclusão (opt-out)	Divulgação seletiva, orquestração de direitos, evidências de avaliação	Análise de papéis, opt-outs, avaliações de risco, implementação gradual de auditorias
México	Leis de dados dos setores privado/público de 2025	Legalidade, finalidade, consentimento, proporcionalidade, ARCO, segurança, transferências	Comprovantes de autorização, minimização, encaminhamento ARCO, criptografia	Autoridade, avisos, controles de dados sensíveis e de transferências
El Salvador	Decreto 144/2024; lei de cibersegurança	Governança abrangente emergente de privacidade e segurança	Credenciais minimizadas, evidências de consentimento, segurança e auditoria	Verificar regulamentações/autoridade, direitos, transferências e incidentes
Colômbia	Lei 1581; Decreto 1074; Lei 527	Autorização, finalidade, circulação restrita, habeas data	Aprovação do titular, minimização, evidências de reclamações	Políticas, RNBD, incidentes perante a SIC e transferências
Peru	Lei 29733; DS 016-2024-JUS	Consentimento, ARCO, bancos de dados, segurança, dados sensíveis, transferências	Comprovantes de consentimento, encaminhamento de direitos, retenção e auditoria	Registro, regras de 2025, incidentes e tratamento transfronteiriço
Brasil	LGPD; regulamentações da ANPD	Bases legais, direitos, dados sensíveis/de crianças, responsabilização, transferências	Perfis de finalidade, minimização, direitos e evidências de impacto	Mapeamento de papéis, DPO/contato, RIPD, incidentes e transferências
Chile	Lei 19.628; Lei 21.719; lei de cibersegurança	Direitos modernizados, supervisão, segurança, transferências	Arquitetura de pré-conformidade, fluxos de direitos, observabilidade	Transição de 2026, procedimentos da ADPP, biometria e transferências
Paraguai	Lei 7593/2025	Novo marco abrangente; transição de implementação	Perfil versionado, minimização, direitos e evidências de auditoria	Verificar regulamentações, autoridade, procedimentos e transferências
Argentina	Lei 25.326; Decreto 1558/2001	Consentimento, habeas data, segurança, bases de dados, transferências	Aprovação do titular, índice de direitos, criptografia e proveniência	Registro na AAIP, prazos de direitos, salvaguardas de transferência
Hong Kong	PDPO e seis DPPs	Coleta, retenção, uso, segurança, transparência, acesso/correção	Provas vinculadas à finalidade, retenção, segurança, IDs pseudônimos	PICS, compatibilidade de uso, operadores, marketing e plano de resposta a violações
Coreia do Sul	PIPA; orientações da PIPC	Consentimento granular, IDs sensíveis, biometria, transferências, segurança	Minimização, comprovantes de política, isolamento biométrico	Operador estrangeiro, representante, obrigações ISMS-P/setoriais
Japão	APPI; My Number Act/JPKI	Finalidade, segurança, transferências, direitos; controles especiais de My Number	Claims minimizados, complemento JPKI, perfil separado de My Number	Separação APPI/My Number, regras da PPC, uso autorizado de JPKI

Proposta de Valor Regulatório

Para as pessoas, o UbID pode reduzir a exposição repetida de documentos de identidade, melhorar o controle sobre a divulgação, fortalecer a continuidade e a recuperação e tornar o uso institucional das evidências de identidade mais visível e passível de contestação.

Para as instituições, o UbID pode reduzir a coleta desnecessária de dados, melhorar a integridade das credenciais, fortalecer a garantia de identidade, automatizar verificações de políticas, reter evidências verificáveis e limitar as consequências de uma violação.

Para reguladores e auditores, o UbID pode produzir uma cadeia de responsabilidade mais clara: quem emitiu a credencial, quem a controlou, o que o verificador solicitou, o que foi divulgado, qual política permitiu a operação, quais controles de segurança foram aplicados e como a instituição respondeu a direitos ou incidentes.

A contribuição estratégica, portanto, não é apenas a descentralização. É a minimização responsável: comprovação de identidade confiável com menor concentração desnecessária de dados pessoais, combinada com uma governança suficientemente robusta para que as instituições confiem no resultado.

Limitações e Aviso Legal

Este white paper é uma análise estratégica e técnica, e não constitui aconselhamento jurídico. Leis, regulamentações, orientações de autoridades supervisoras, esquemas de certificação e práticas de fiscalização mudam ao longo do tempo. Cada instituição deve concluir seu próprio mapeamento de papéis, análise de base legal, relatório de impacto à proteção de dados, revisão contratual, análise setorial e interação regulatória antes da implantação no Canadá, nos Estados Unidos, no Estado de Nova York, na Califórnia, no México, em El Salvador, na Colômbia, no Peru, no Brasil, no Chile, no Paraguai, na Argentina, no Reino Unido, na União Europeia, em Hong Kong, na Coreia do Sul ou no Japão.

A análise descreve capacidades e alinhamentos potenciais. Ela não afirma que o UbID ou a Paradigma SpA já tenham obtido status de Carteira Europeia de Identidade Digital, status de prestador qualificado de serviços de confiança, certificação DVS do Reino Unido, acreditação governamental canadense ou asiática, aprovação estadual nos Estados Unidos, autorização regulatória latino-americana, aprovação setorial ou qualquer certificação equivalente, salvo quando respaldado por evidência atual separada.

Referências

Fontes jurídicas, regulatórias, institucionais e técnicas de autoridade consultadas. Acessadas ou verificadas para este white paper até 30 de julho de 2026. O site corporativo da Paradigma está incluído como fonte para a descrição do desenvolvedor.

- [1] Parlamento Europeu e Conselho. Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- [2] Parlamento Europeu e Conselho. Regulamento (UE) 2024/1183 que estabelece o Marco Europeu de Identidade Digital. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
- [3] Reino Unido. Lei de Proteção de Dados de 2018. <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- [4] Information Commissioner's Office. Proteção de dados desde a concepção e por padrão. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/>
- [5] Reino Unido. Lei de Dados (Uso e Acesso) de 2025. <https://www.legislation.gov.uk/ukpga/2025/18/contents>
- [6] Departamento de Ciência, Inovação e Tecnologia do Reino Unido. Marco de Confiança dos Serviços de Verificação Digital do Reino Unido 1.0. <https://www.gov.uk/government/publications/uk-digital-verification-services-trust-framework-1-0/uk-digital-verification-services-trust-framework-1-0-pre-release>
- [7] Chile. Lei nº 19.628 sobre Proteção da Vida Privada / Dados Pessoais. <https://www.bcn.cl/levchile/navegar?idNorma=141599>
- [8] Chile. Lei nº 21.719 que regula a proteção de dados pessoais e cria a Agência de Proteção de Dados Pessoais. <https://www.bcn.cl/levchile/navegar?idNorma=1209272>
- [9] Chile. Lei nº 21.663, Lei Marco de Cibersegurança. <https://www.bcn.cl/levchile/navegar?idNorma=1202434>
- [10] Chile. Lei nº 19.799 sobre documentos eletrônicos, assinaturas eletrônicas e serviços de certificação. <https://www.bcn.cl/levchile/navegar?idNorma=196640>
- [11] Colômbia. Lei Estatutária 1581 de 2012, disposições gerais para a proteção de dados pessoais. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- [12] Colômbia. Decreto 1074 de 2015, Decreto Único Regulamentar do setor de Comércio, Indústria e Turismo. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608>
- [13] Superintendência de Indústria e Comércio. Política de tratamento de dados pessoais e declaração de princípios e direitos. <https://sedeelectronica.sic.gov.co/politica-de-tratamiento-de-datos-personales>
- [14] Colômbia. Lei 527 de 1999 sobre mensagens de dados, comércio eletrônico e assinaturas digitais. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013>
- [15] Comissão Federal de Comércio dos Estados Unidos. Orientações de Privacidade e Segurança para empresas. <https://www.ftc.gov/business-guidance/privacy-security>
- [16] Departamento de Justiça da Califórnia. Lei de Privacidade do Consumidor da Califórnia (CCPA). <https://oag.ca.gov/privacy/ccpa>
- [17] Procuradoria-Geral do Texas. Lei de Privacidade e Segurança de Dados do Texas. <https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act>
- [18] Assembleia Geral de Illinois. Lei de Privacidade de Informações Biométricas, 740 ILCS 14. <https://www.ilga.gov/legislation/ILCS/Articles?ActID=3004&ChapterID=57>
- [19] Agência de Proteção da Privacidade da Califórnia. Regulamentações da CCPA, incluindo atualizações com vigência em 2026. <https://coppa.ca.gov/regulations/>
- [20] Departamento de Saúde e Serviços Humanos dos EUA. Regra de Segurança da HIPAA. <https://www.hhs.gov/hipaa/for-professionals/security/index.html>
- [21] Comissão Federal de Comércio dos Estados Unidos. Regra de Salvaguardas da Lei Gramm-Leach-Bliley. <https://www.ftc.gov/legal-library/browse/rules/safeguards-rule>
- [22] Instituto Nacional de Padrões e Tecnologia. Marco de Privacidade do NIST. <https://www.nist.gov/privacy-framework>
- [23] World Wide Web Consortium. Identificadores Descentralizados (DIDs) v1.0. <https://www.w3.org/TR/did-core/>
- [24] World Wide Web Consortium. Modelo de Dados de Credenciais Verificáveis v2.0. <https://www.w3.org/TR/vc-data-model-2.0/>
- [25] OpenID Foundation. OpenID para Emissão de Credenciais Verificáveis 1.0, Especificação Final. <https://openid.net/specs/openid-4-verifiable-credential-issuance-1.0.html>

- [26] OpenID Foundation. OpenID para Apresentações Verificáveis 1.0, Especificação Final. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
- [27] IETF / RFC Editor. RFC 9901, Divulgação Seletiva para JSON Web Tokens (SD-JWT). <https://www.rfc-editor.org/rfc/rfc9901.html>
- [28] World Wide Web Consortium. Web Authentication: uma API para acesso a credenciais de chave pública — Nível 3. <https://www.w3.org/TR/webauthn-3/>
- [29] NIST. FIPS 203, Padrão de Mecanismo de Encapsulamento de Chaves Baseado em Reticulados de Módulos (ML-KEM). <https://csrc.nist.gov/pubs/fips/203/final>
- [30] NIST. FIPS 204, Padrão de Assinatura Digital Baseado em Reticulados de Módulos (ML-DSA). <https://csrc.nist.gov/pubs/fips/204/final>
- [31] Decentralized Identity Foundation. Especificação DIDComm Messaging v2.1. <https://identity.foundation/didcomm-messaging/spec/>
- [32] Projeto OP-TEE. Sobre o OP-TEE e o Ambiente de Execução Confiável baseado em Arm TrustZone. <https://optee.readthedocs.io/en/latest/general/about.html>
- [33] Shamir, A. “Como Compartilhar um Segredo”. Communications of the ACM, 22(11), 1979. <https://doi.org/10.1145/359168.359176>
- [34] Documento-fonte fornecido para este white paper: “Identidade na Sociedade Digital: A Abordagem UbID” (inglês, 14 páginas).
- [35] Paradigma SpA. “Construindo uma Identidade Digital Confiável” e visão geral da empresa. <https://paradigma.global> (redireciona para <https://paradigma.cl/>).
- [36] Instituto Nacional de Padrões e Tecnologia. NISTIR 8202, Visão Geral da Tecnologia Blockchain. <https://csrc.nist.gov/pubs/ir/8202/final>
- [37] AMD. Secure Encrypted Virtualization e computação confidencial SEV-SNP. <https://www.amd.com/en/developer/sev.html>
- [38] Intel. Visão geral do Trust Domain Extensions (Intel TDX). <https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html>
- [39] Amazon Web Services. O que é Nitro Enclaves? <https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html>
- [40] GlobalPlatform. Perfil de Proteção TEE v1.3. <https://globalplatform.org/specs-library/tee-protection-profile-v1-3/>