IDENTIDADE NA SOCIEDADE DIGITAL

A abordagem UbID

Identidade digital que preserva a privacidade

LIVRO BRANCO Privacidade global, proteção de dados pessoais, blockchain/DLT, proteção criptográfica

Data de publicação: 30 de julho de 2026

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

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

? O UbID está melhor posicionado como uma infra-estrutura de identidade que aumenta a privacidade e permite a conformidade, e não como uma infra-estrutura legal automática. produto de conformidade. ? A divulgação seletiva e as provas derivadas podem reduzir materialmente a quantidade de dados pessoais coletados pelas partes confiáveis. ? O controle do titular fortalece a transparência e a autonomia, mas as instituições ainda precisam de bases legais, avisos, contratos, retenção políticas e procedimentos de resposta a direitos. ? A recuperação distribuída e os controles do ciclo de vida do dispositivo podem reduzir o risco de controle de contas sem devolver todo o poder de recuperação a um único administrador. ? O processamento biométrico deve ser opcional ou legalmente justificado, isolado, com finalidade específica e regido por jurisdição específica consentimento, retenção e regras de segurança. ? A Europa e o Reino Unido fornecem estruturas formais de identidade digital que o UbID pode atingir, mas o status regulamentado e marcas de confiança exigem certificação e registro independentes. ? A Lei n.º 21.719 do Chile cria uma prioridade de implementação imediata antes da sua data de entrada em vigor, 1 de dezembro de 2026. ? A Colômbia exige fortes evidências de autorização, limitação de finalidade, segurança e procedimentos eficazes de habeas-data sob seu quadro atual. ? Os Estados Unidos exigem uma sobreposição de conformidade configurável estado por estado e setor por setor, em vez de um único sistema nacional perfil de privacidade. ? Uma implantação global única deveria usar perfis de jurisdição versionados, em vez de tentar forçar todos os países a entrarem em um só. configuração de privacidade. ? Nova York e Califórnia exigem sobreposições distintas dos Estados Unidos: Nova York enfatiza salvaguardas e violações razoáveis governança, enquanto a Califórnia acrescenta amplos direitos do consumidor, controles de dados confidenciais, avaliações de risco, auditorias de segurança cibernética e requisitos de decisão automatizada. ? Os regimes latino-americanos convergem cada vez mais em matéria de responsabilização, direitos dos titulares de dados, salvaguardas de dados sensíveis e transferência controlos, mas as suas autoridades, bases jurídicas, procedimentos e maturidade de implementação permanecem específicos da jurisdição. ? As implantações na Ásia exigem tratamento personalizado: Hong Kong está organizada em torno de seis princípios de proteção de dados; Coreia do Sul aplica um regime PIPA abrangente com expectativas rigorosas de biometria e de operador estrangeiro; Japão exige separação entre a conformidade com APPI e o ecossistema especial My Number/JPKI. ? O UbID foi desenvolvido pela Paradigma SpA, Chile, cuja proposta institucional centra-se em soluções seguras, interoperáveis e ecossistemas de identidade digital resistentes à fraude. [35]

A análise ampliada também distingue a tecnologia blockchain da atividade regulamentada de criptoativos, avalia o funcionamento perímetro nas mesmas jurisdições e define os controles criptográficos, de execução confiável e KMS em camadas necessários para proteja os dados UbID em repouso, em trânsito e em uso. As leis de blockchain e criptoativos são tratadas como uma sobreposição funcional separada; nenhuma inferência de licenciamento, autorização ou status legal é feita a partir do uso de criptografia ou identidade descentralizada padrões.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A chave privada permanece sob controle exclusivo do usuário e é armazenada em um cofre criptográfico local criptografado. Portanto, o blockchain Stacks não criptografa ou armazena diretamente a chave privada; em vez disso, fornece o ligação criptográfica, verificabilidade e rastreabilidade necessárias para associar com segurança a identidade UbID ao titular conta blockchain. ? Os controles TEE e KMS fornecem defesa profunda para dados em uso e chaves institucionais, mas exigem atestado, privilégio mínimo, governação fundamental do ciclo de vida, garantia independente e recuperação testada. ? As funções regulamentadas dos criptoativos devem ser segregadas da plataforma de identidade e avaliadas de forma independente em cada jurisdição.

Escopo e Método

A análise regulatória é baseada na legislação primária, nas orientações das autoridades supervisoras e nos padrões atuais para o data limite da pesquisa. Centra-se na proteção geral de dados pessoais e nas obrigações de identidade digital. Específico do setor requisitos podem ser aplicados em finanças, saúde, seguros, emprego, educação, telecomunicações, governo e infraestrutura crítica.

A palavra ?alinhamento? neste documento significa que uma capacidade UbID pode apoiar ou fornecer evidências para uma decisão legal ou de governança. exigência. Isso não significa que toda configuração padrão satisfaça todas as jurisdições, nem que uma implementação tenha foi certificado, aprovado ou reconhecido por uma autoridade.

A conformidade deve ser expressa como perfis de jurisdição e controles de políticas: a mesma tecnologia de credenciais pode ser usada globalmente, enquanto bases legais, regras de divulgação, períodos de retenção, condições biométricas, cronogramas de incidentes, salvaguardas de transferência e dados do titular dos dados os fluxos de trabalho são configurados para a instituição e local em que ocorre o processamento.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Contexto Institucional e Desenvolvedor: Paradigma SpA Chile

UbID foi desenvolvido pela Paradigma SpA, Chile. O site oficial da Paradigma descreve a empresa como uma organização focado no gerenciamento de TI e na transformação digital estratégica, com a missão de arquitetar soluções seguras, interoperáveis e anti-fraude. estruturas de identidade resistentes para instituições. [35]

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Contribuição Estratégica da Paradigma

? Uma plataforma de identidade desenvolvida no Chile e projetada para interoperabilidade internacional, em vez de um único silo de identidade nacional. ? Uma arquitetura que aumenta a privacidade e que permite às instituições verificar reivindicações e, ao mesmo tempo, reduzir a replicação desnecessária de documentos e concentração de dados pessoais. ? Um modelo de governança que separa as responsabilidades do emissor, do detentor, do verificador, do custodiante e da infraestrutura, apoiando uma abordagem mais clara responsabilidade. ? Uma camada de controle que permita a conformidade, capaz de aplicar jurisdição, setor, finalidade, garantia, retenção, transferência e políticas de gestão de direitos. ? Uma estratégia de segurança de longo prazo que combine a criptografia interoperável atual com a migração controlada para o pós- proteções quânticas.

Identidade na Sociedade Digital: A Abordagem UbID

Os serviços de identidade são fundamentais para as sociedades modernas. Cada país fornece credenciais de identidade ? como credenciais nacionais carteiras de identidade, passaportes, autorizações de residência e carteiras de motorista ? que servem como uma raiz de confiança para os indivíduos que interagem com instituições públicas, empresas privadas e outras pessoas.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

As senhas podem ser adivinhadas, reutilizadas, roubadas ou vazadas. Telefones celulares e cartões SIM podem ser roubados ou fraudulentos duplicado. As contas de e-mail podem ser controladas. As informações biométricas podem ser capturadas, reproduzidas ou armazenadas de forma insegura. Os procedimentos de recuperação são muitas vezes ainda mais vulneráveis do que o método de autenticação original, tornando a recuperação de conta em um dos principais pontos de entrada para roubo de identidade.

Estes riscos são especialmente graves em domínios de elevado valor, como a banca, os cuidados de saúde, os seguros, os serviços governamentais, telecomunicações, infraestrutura crítica e administração de sistemas. Nestes setores, uma representação bem-sucedida não não se limita a expor uma conta: pode permitir transferências financeiras, acesso a informações médicas sensíveis, fraudes contratação, alterações não autorizadas na infraestrutura ou assunção da identidade legal de uma pessoa.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Este modelo permitiu a expansão dos serviços digitais, mas também produziu grandes concentrações de serviços pessoais. informação. Cada repositório central de identidades torna-se um alvo potencialmente valioso. Uma única violação pode expor o informações de milhares ou milhões de pessoas, enquanto os indivíduos têm visibilidade ou controle limitado sobre como sua identidade os dados são copiados, processados, compartilhados, retidos ou reutilizados.

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

As instituições, portanto, gastam recursos consideráveis verificando repetidamente informações que já podem ter sido validadas por outra organização confiável. Os indivíduos são obrigados a enviar os mesmos documentos várias vezes, divulgar mais informações do que o necessário e dependem 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 os ativos digitais e os identificadores descentralizados podem ser controlado 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.

No entanto, a adopção generalizada destas tecnologias tem sido restringida pela dificuldade de gerir com segurança chaves. Uma chave privada pode fornecer uma forte proteção matemática, mas perdê-la pode resultar na perda permanente de acesso. Copiando colocá-lo em um local inseguro, armazená-lo em texto simples ou expô-lo por meio de um dispositivo comprometido pode permitir que um invasor assumir o controle da identidade.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

O desafio não é, portanto, apenas criar identificadores descentralizados. Uma arquitetura de identidade digital completa deve proteger as chaves, apoiar a recuperação segura, operar em vários dispositivos, permitir a divulgação controlada de dados pessoais atributos, permanecem interoperáveis com sistemas institucionais e fornecem um caminho de migração confiável para o pós-quântico segurança.

Um novo paradigma: identidade digital autogerenciada

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Isso muda fundamentalmente o modelo de identidade digital. A pessoa não é mais representada exclusivamente por contas mantidos por organizações externas. O indivíduo possui uma coleção reutilizável e portátil de dados criptograficamente credenciais verificáveis que podem ser apresentadas em diferentes serviços e contextos.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

UbID: uma infraestrutura de identidade segura centrada na pessoa

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

O seu objectivo não é eliminar instituições confiáveis. Governos, universidades, bancos, prestadores de cuidados de saúde, empregadores e os organismos de certificação continuam sendo fontes essenciais de informações confiáveis. UbID muda a forma como a confiança é criada, transportado, verificado e controlado.

As instituições continuam a emitir declarações oficiais, mas os indivíduos podem manter e reutilizar essas declarações sem exigir todos os esforços. verificador para manter outra cópia isolada dos mesmos dados. A confiança se torna portátil, verificável criptograficamente e sujeito ao controle explícito do titular.

Para indivíduos, o UbID fornece uma identidade digital portátil e não permanentemente confinada a um único provedor, aplicativo ou dispositivo. A pessoa pode manter o controle sobre as credenciais de identidade e decidir quando, onde e para quê finalidade em que são apresentados.

Isso reduz a dependência de senhas e procedimentos centralizados de recuperação de contas. A autenticação pode ser reforçada por meio de chaves de acesso, verificação biométrica, dispositivos confiáveis, provas criptográficas e combinações baseadas em políticas destes mecanismos.

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

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

? Menos dependência de senhas e questões de segurança vulneráveis. ? Maior controle sobre informações pessoais e divulgação de credenciais. ? Necessidade reduzida de carregar repetidamente cópias de documentos de identidade. ? Portabilidade de credenciais entre serviços compatíveis. ? Registro mais seguro de dispositivos adicionais. ? Revogação controlada de dispositivos perdidos ou comprometidos. ? Proteção mais forte contra apropriação de contas e recuperação fraudulenta. ? Apresentação seletiva apenas dos atributos necessários para uma transação. ? Prova criptográfica de integridade e procedência de credenciais.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Para as instituições, o UbID fornece um mecanismo para receber identidades mais fortes, mais estruturadas e verificáveis criptograficamente evidência.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Isto pode reduzir a fraude documental, a revisão manual, a repetida prova de identidade e o custo operacional de manutenção de grandes quantidades de dados pessoais duplicados.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

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

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Este equilíbrio permite que as instituições beneficiem da automatização, mantendo ao mesmo tempo a responsabilização, a segregação de funções e a gestão humana. supervisão.

O UbID não assume que todas as reivindicações de identidade sejam igualmente confiáveis. A confiança depende do emissor, do tipo de credencial, do método de verificação, o status atual da credencial, a política aplicável e o contexto no qual a credencial é apresentado.

Uma afirmação autoemitida pode ser apropriada para uma preferência pessoal ou um atributo de perfil de baixo risco. Um documento emitido pelo governo credencial pode ser necessária para identidade legal. Uma credencial emitida por uma universidade pode estabelecer um diploma acadêmico. Um regulamentado organismo profissional pode atestar uma licença. Um processo de verificação biométrica pode demonstrar que a pessoa que apresenta um credencial corresponde ao titular inscrito.

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

Isto cria um modelo descentralizado sem eliminar a governação. A confiança permanece mensurável, contextual e política conduzido.

Divulgação seletiva e verificação de preservação de privacidade

? Comprovar a maioridade legal sem revelar a data completa de nascimento. ? Demonstrar residência sem revelar atributos de identidade desnecessários. ? Confirmar o 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.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Custódia segura de documentos e credenciais

UbID incorpora o conceito de um cofre de documentos criptografados no qual esses materiais podem ser protegidos enquanto permanecem associada à identidade do titular.

Isto proporciona aos indivíduos um repositório mais útil e seguro, enquanto as instituições recebem informações mais claras sobre a confiabilidade das provas apresentadas.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A combinação apropriada pode variar. Uma apresentação de credencial de baixo risco pode exigir apenas uma prova válida do titular. Um sensível evento de recuperação pode exigir vários dispositivos registrados, verificação biométrica, aprovação de limite e criptografia validação desafio-resposta.

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

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

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

O objetivo não é apenas recuperar o acesso. É recuperar o acesso de forma a preservar a credibilidade da identidade após a recuperação ter ocorrido.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

UbID suporta identidade controlada de vários dispositivos em vez de sincronização irrestrita. Um novo dispositivo deve estar associado com o titular legítimo e pode exigir a aprovação de um dispositivo já confiável ou outra recuperação autorizada mecanismo.

A maioria dos sistemas de identidade digital atuais baseia-se na criptografia clássica de chave pública. Esses algoritmos permanecem essenciais para interoperabilidade, mas a longa vida útil operacional das informações de identidade requer preparação para futuras operações criptográficas. transições.

Credenciais de identidade, registros de recuperação, documentos legais e atestados institucionais podem permanecer confidenciais ou valiosos para muitos anos. As informações capturadas hoje podem ser armazenadas por um invasor e atacadas posteriormente, quando um computador mais forte capacidades ficam disponíveis.

O UbID, portanto, incorpora uma abordagem progressiva à segurança pós-quântica. Algoritmos clássicos podem continuar a suportar compatibilidade com carteiras, verificadores e padrões atuais, enquanto assinaturas pós-quânticas adicionais, estabelecimento de chaves mecanismos ou evidências criptográficas podem ser introduzidas junto com eles.

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

Interoperabilidade em vez de outro silo de identidade

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

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A interoperabilidade protege as instituições da dependência excessiva de fornecedores e dá aos indivíduos maior confiança de que seus as credenciais permanecerão portáteis.

Auditabilidade, observabilidade e responsabilidade institucional

UbID incorpora observabilidade operacional, monitoramento de saúde, 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 para investigação e governança.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Isto dá às instituições maior capacidade para detectar anomalias, investigar incidentes, satisfazer os controles internos e demonstrar conformidade.

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

Esse modelo pode apoiar ecossistemas intersetoriais envolvendo governo, educação, finanças, saúde, emprego, seguros, telecomunicações e credenciamento profissional.

Uma pessoa poderia manter uma identidade digital coerente enquanto recebia credenciais diferentes de autoridades diferentes. Cada A instituição permanece responsável pelos créditos que emite, enquanto o titular continua responsável por decidir como esses créditos serão emitidos. são usados.

Habilitando agentes digitais confiáveis

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Isto cria um caminho para operações de identidade assistidas por máquinas, sem sacrificar a responsabilidade institucional ou controle individual.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

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

O valor mais amplo do UbID

Para a sociedade, oferece uma alternativa à acumulação crescente de bases de dados de identidade fragmentadas e de dados inseguros. mecanismos de autenticação. Permite um modelo no qual a confiança pode ser estabelecida criptograficamente, divulgada proporcionalmente, verificada de forma independente e governada de forma transparente.

O objetivo final é permitir que os indivíduos se representem de forma segura no mundo digital, ao mesmo tempo que permite às instituições confiar nas evidências que recebem ? sem exigir dados desnecessários, sem depender exclusivamente de pessoas vulneráveis intermediários, e sem renunciar à segurança ou à interoperabilidade a longo prazo.

Neste modelo, a identidade digital torna-se mais do que um mecanismo de acesso. Torna-se uma infraestrutura confiável reutilizável para os modernos sociedade.

Contribuição regulatória e de proteção de dados do UbID

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Arquitetura de conformidade entre jurisdições

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.	
Limitação de finalidade As solicitações de credenciais podem estar vinculadas a uma finalidade declarada, parte confiável, público, nonce, transação e decisão política.	
Agência titular A pessoa pode autorizar explicitamente a emissão e apresentação, fiscalizar o que for solicitado e controlar dispositivos registrados.	
Responsabilidade Eventos de emissão, apresentação, verificação, status, dispositivo e recuperação podem criar evidências auditáveis sem registrar material secreto.	
Habilitação de direitos Os índices de credenciais e de cofre podem suportar acesso, retificação, supressão, revogação, restrição e fluxos de trabalho de portabilidade.	
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.	

Limite de governança: o que o UbID não substitui

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A regulamentação do Blockchain não é uma categoria legal única. Um livro-razão distribuído pode ser usado como um mecanismo de integridade interna, um registro público, uma via de pagamento, uma infraestrutura de mercado, uma plataforma de emissão de tokens ou um sistema de custódia. A lei aplicável segue a função, os direitos representados, as partes atendidas e os riscos criados ? não o uso da palavra ?blockchain?. Da mesma forma, o NIST trata o blockchain como uma família técnica de livros-razão distribuídos e criptograficamente vinculados, e não como um sinônimo de criptomoeda. [36]

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A análise de privacidade aplica-se mesmo quando um livro-razão armazena apenas identificadores, endereços, hashes ou valores criptografados, se esses elementos podem razoavelmente ser vinculados a uma pessoa. As diretrizes finais de blockchain do Conselho Europeu de Proteção de Dados de julho 2026 enfatizam a seleção de arquitetura, atribuição de funções, proteção de dados desde a concepção, minimização e direitos efetivos, e cautela contra a colocação de dados pessoais em cadeia quando isso entre em conflito com os princípios de proteção de dados. A mesma engenharia princípio é prudente em todas as jurisdições neste documento.

? Mantenha credenciais, reivindicações, biometria, imagens de documentos, identificadores de dispositivos, dados de recuperação e históricos de apresentação fora do seu alcance. cadeia. ? Se a ancoragem for justificada, publicar apenas um compromisso irreversível gerado com separação de domínio, um sal secreto ou construção chaveada; um simples hash de dados pessoais previsíveis não é anonimização. ? Não presuma que a criptografia de dados pessoais na rede resolve o apagamento. Texto cifrado, chaves, metadados e futuro o risco criptoanalítico deve ser avaliado durante todo o período de retenção. ? Prefira governança autorizada quando houver responsabilidade institucional, localização de nós, controle de acesso, correção os procedimentos e a resposta a incidentes devem ser aplicáveis. ? Documentar operadores de nós, funções de controlador e processador, governança de consenso, autoridade de mudança de software, jurisdição, retenção e procedimento para registros contestados ou ilegais.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

? Nenhum dado pessoal, carga útil de credencial, modelo biométrico ou fragmento de recuperação em um blockchain público. ? Nenhum valor transferível ou direito de investimento em uma credencial de identidade. ? Nenhuma capacidade institucional para movimentar os activos do titular apenas porque pode ajudar a recuperar o acesso à identidade. ? Entidades legais separadas, descrições de serviços e hierarquias de chaves onde são adicionados serviços regulamentados de criptoativos. ? Um perfil de jurisdição versionado deve registrar o perímetro legal, regulador, licença, data de vigência, atividades permitidas e funções proibidas.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

A arquitetura deve preservar uma hierarquia na qual os detentores controlam as credenciais, as aplicações recebem apenas informações de escopo restrito. serviços criptográficos, o KMS rege as chaves institucionais e os TEEs protegem a computação de alto risco em uso. Nenhuma camada é uma substituir os demais: um TEE sem um gerenciamento de chaves adequado pode receber o segredo errado; um KMS sem atestado a execução pode liberar um segredo correto para o código comprometido; e algoritmos fortes não corrigem privilégios excessivos, fraca recuperação ou má governança de auditoria.

Ambientes de execução confiáveis ??e dados em uso

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

O UbID Custodian TEE Profile é um trabalhador de infraestrutura executado em um ambiente de computação confidencial de classe de servidor como SEV-SNP, TDX ou Nitro Enclaves. Ele valida a solicitação DIDComm autenticada, desafio, nonce, transação contexto, janela de reprodução, decisão política e estado de atestado e, em seguida, libera apenas um fragmento de recuperação autorizado. Nunca reconstrói o segredo completo do titular e produz provas assinadas e minimizadas da decisão.

O perfil UbID Edge TEE usa OP-TEE ou um ambiente confiável comparável em um dispositivo Arm, gateway ou IoT adequado plataforma. Ele pode receber três fragmentos autorizados, reconstruir localmente, usar o segredo recuperado para o aprovado com restrição operação e zerar material transitório sem exportar o segredo completo para o sistema operacional normal. OP-TEE é complementar aos TEEs do servidor: protege a computação da borda final, enquanto os TEEs custodiantes protegem os fragmentos independentes lançamento.

? O titular inicia a recuperação e recebe um identificador de transação, desafio criptograficamente aleatório, nonce e short janela de validade. ? O TEE de borda ou destino produz atestado vinculado a uma chave pública efêmera, medição de carga de trabalho aprovada, versão de segurança e a transação de recuperação. ? Cada custodiante valida de forma independente a autenticação do titular, política de dispositivo e recuperação, atualização de nonce, reprodução estado, controles de jurisdição e atestado TEE.

? O KMS autoriza apenas a operação criptográfica necessária ou agrupa um fragmento na chave efêmera atestada; o fragmento nunca é retornado em texto simples para o serviço comum. ? Três fragmentos são reconstruídos apenas dentro do TEE de borda aprovado ou do ambiente de suporte designado. O completo o segredo não é registrado, persistido ou exposto por meio de diagnóstico. ? O ambiente executa a ação aprovada de rechaveamento, abertura de cofre ou recuperação, zera valores transitórios e emite evidências assinadas contendo identificadores e resultados, mas nenhum material secreto.

Criptografia Pós-Quantum e Cripto-Agilidade

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

O SD-JWT compacto e interoperável não deve receber uma segunda assinatura ad hoc que quebre a carteira externa e o verificador compatibilidade. Até que os formatos de consumo padrão suportem assinaturas pós-quânticas, o UbID pode manter a credencial interoperável e expor uma prova PQC vinculada separadamente ou usar um contêiner com múltiplas assinaturas apenas em ecossistemas controlados. Cada artefato deve indicar se o PQC é experimental, evidência paralela ou verificação necessária; fallback silencioso do híbrido a validação apenas clássica deve ser proibida para fluxos que reivindicam garantia pós-quântica.

Ancoragem Blockchain e Segurança Criptográfica

Um hash de blockchain prova, no máximo, que uma determinada sequência de bytes ou compromisso existia em relação a um evento contábil; isso acontece não provar que o documento de origem era autêntico, obtido legalmente, exato, atual ou vinculado à pessoa correta. Essas propriedades vêm da governança do emissor, prova de identidade, assinaturas, status, vinculação do titular e política do verificador. UbID deve, portanto, tratar a ancoragem da blockchain como carimbo de data/hora opcional ou evidência de integridade, nunca como um substituto para validação de credenciais.

Se a ancoragem for adotada, cada credencial deverá usar um compromisso aleatório ou construção Merkle que evite recuperação de dicionário e correlação entre contextos. A cadeia não deve conter nenhum DID que resolva diretamente dados pessoais, nenhum hash de documento derivado de campos previsíveis, nenhum material biométrico, nenhum motivo de revogação e nenhum histórico de apresentação. Os sistemas fora da cadeia devem manter a base legal, a finalidade, a retenção e o fluxo de trabalho de direitos, enquanto a governança do razão deve suportar defeitos de software, chaves de assinatura comprometidas e entradas contestadas.

? Mantenha uma lista de materiais criptográficos assinada cobrindo algoritmos, bibliotecas, tamanhos de chaves, protocolos, perfis de certificados, raízes de hardware de confiança e datas de descontinuação. ? Classifique cada chave por proprietário, finalidade, ambiente, sensibilidade, exportabilidade, rotação, backup, revogação e procedimento de destruição. ? Use montagens, chaves e políticas KMS separadas para assinatura JWT, emissão de credenciais, criptografia de documentos e recuperação empacotamento, integridade de auditoria e ambientes de teste. ? Exigir controle duplo para geração de token raiz, escalonamento de políticas, operações de abertura de lacre e compartilhamento de recuperação; preservar provas sem registrar as ações. ? Verifique o atestado TEE, o status do firmware, a medição da carga de trabalho, a versão de segurança e as informações de revogação antes cada lançamento sensível. ? Exercitar restauração KMS, selar/desselar, revogação de token, rotação de chave, resposta de chave de emissor comprometida, TEE rolagem de medição e recuperação total, pelo menos em um cronograma definido com base em risco. ? Modelagem de ameaças da Comissão e testes de penetração para canais secundários, repetição, reversão, caminhos de deputados confusos, custodiantes maliciosos, comprometimento da cadeia de suprimentos e vazamento de observabilidade. ? Representar o status da implementação com precisão: objetivo da arquitetura, prova de conceito, controle de preparação testado e o controle garantido pela produção são reivindicações distintas.

Estes controlos reforçam a confidencialidade, a integridade, a disponibilidade e a responsabilização, mas por si só não criam conformidade legal ou certificação formal. As instituições continuam responsáveis pela atribuição de funções, pelo processamento legal, pelas regras do sector, aceitação de risco, garantia independente, notificação de incidentes e adequação do TEE selecionado e criptográfico módulo para cada jurisdição e caso de uso.

Perfil de controle regulatório UbID

Uma implantação de produção deve traduzir as obrigações regulatórias em um perfil de controle versionado e legível por máquina. O O perfil deve ser avaliado na emissão, apresentação, verificação, recuperação, registro do dispositivo, ingestão de documentos e pontos de exceção administrativa. Deve apoiar sobreposições de papéis institucionais, de países, estados ou províncias, sectoriais e, ao mesmo tempo, mantendo a versão exata da política usada para cada transação histórica.

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.
Papel institucional Controlador, processador, emissor, verificador, provedor de serviços de detentor, custodiante, provedor de orquestração ou trust- provedor de serviços.
Base legal Consentimento, contrato, obrigação legal, tarefa pública, interesses legítimos ou outro fundamento autorizado, com condições de categoria especial.
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.
Tratamento de direitos Acesso, correção, supressão, supressão, oposição, restrição, portabilidade, reclamação e recurso fluxos de trabalho.
Retenção e status Validade de credenciais, revogação, retenção de evidências, retenção legal, exclusão de cofre e destruição biométrica períodos.
Obrigações de incidente Detecção, escalonamento, cronogramas de notificação individual e reguladora, preservação de evidências e recuperação.
Decisões automatizadas Limites de aprovação humana, explicação, contestabilidade, monitoramento de preconceitos e automação proibida ações.
Versão legal e data de vigência Lei promulgada, data de vigência, disposição transitória, regulamento, orientação da autoridade e aprovação interna data.
Modelo de consentimento e notificação Idioma de notificação exigido, granularidade de consentimento, tratamento de retirada, fundamentos legais alternativos e formato de evidência.
Dados sensíveis e biométricos Classificação, teste de necessidade, alternativas, localização de templates, acesso, retenção, destruição e anti- requisitos de repetição.
Transferências internacionais Origem, destino, destinatário, mecanismo legal, regra de localização, condições de transferência subsequente e controles de acesso remoto.
Fluxo de trabalho de incidentes e reguladores Limites de detecção, padrão de avaliação, prazos de notificação, autoridade competente, comunicação pessoal e retenção de evidências.
Controles de decisão automatizados Perfil aplicável ou regras ADMT, explicação, revisão humana, objeção, cancelamento e avaliação de risco requisitos.
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.

Jurisdição Estrutura primária Ênfase regulatória Contribuição UbID Residual institucional obrigações		
União Europeia GDPR; EUDI/eIDAS 2.0 Base legal, minimização, direitos, DPIA, transferências, funções regulamentadas de carteira/confiança		
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.		
Estados Unidos - federal FTC; HIPAA; GLBA; COPPA; leis do setor Práticas injustas/enganosas, segurança e deveres do setor Sobreposições configuráveis, autenticação forte, auditoria evidência		
Estado de Nova York Lei ESCUDO; NYDFS Parte 500 Salvaguardas razoáveis, relatórios de violação, segurança cibernética		
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.		
México Leis de dados públicos/privados de 2025 Legalidade, finalidade, consentimento, proporcionalidade, ARCO, segurança, transferências		
Salvador Decreto 144/2024; lei de segurança cibernética Privacidade e segurança abrangentes emergentes governança		
Colômbia Lei 1581; Decreto 1.074; Lei 527 Autorização, finalidade, circulação restrita, habeas dados		
Perú Lei 29.733; DS 016-2024-JUS Consentimento, ARCO, bancos de dados, segurança, dados sensíveis, transferências		
Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.		
Chile Lei 19.628; Lei 21.719; lei cibernética Direitos modernizados, supervisão, segurança, transferências Pré-conformidade arquitetura, direitos fluxos de trabalho, observabilidade		
Paraguai Lei 7.593/2025 Novo quadro abrangente; implementação transição		
Argentina Lei 25.326; Decreto 1558/2001 Consentimento, habeas data, segurança, bancos de dados, transferências Suporte aprovação, direitos índice, criptografia e proveniência		
Hong Kong PDPO e seis DPPs Coleção, retenção, usar, segurança, abertura, acesso/correção		
Coreia do Sul PIPA; Orientação PIPC Consentimento granular, IDs confidenciais, biometria, transferências, segurança		
Japão APPI; Lei do Meu Número/JPKI Finalidade, segurança, transferências, direitos; especial meu Controles numéricos		

Proposta de Valor Regulatório

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

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

Limitações e Aviso Legal

Este white paper é uma análise estratégica e técnica, não um aconselhamento jurídico. Leis, regulamentos, orientação de supervisão, certificação os esquemas e as práticas de aplicação mudam ao longo do tempo. Cada instituição deve completar o seu próprio mapeamento de funções, base jurídica análise, avaliação de impacto na proteção de dados, revisão contratual, análise setorial e envolvimento regulatório antes implantação no Canadá, Estados Unidos, Estado de Nova York, Califórnia, México, El Salvador, Colômbia, Peru, Brasil, Chile, Paraguai, Argentina, Reino Unido, União Europeia, Hong Kong, Coreia do Sul ou Japão.

A análise descreve capacidades e alinhamento potencial. Isso não significa que a UbID ou a Paradigma SpA já tenham obteve status de Carteira de Identidade Digital Europeia, status de serviço confiável qualificado, certificação DVS do Reino Unido, Canadá ou Ásia acreditação governamental, aprovação do estado dos Estados Unidos, autorização regulatória da América Latina, aprovação do setor ou qualquer certificação equivalente, a menos que seja apoiada por evidências atuais separadas.

Referências

https://www.gov.uk/government/publications/uk-digital-verification-services-trust-framework-1-0/uk-digital-verification-services-trust- framework-1-0-pré-lançamento

Error 500 (Server Error)!!1500.That?s an error.There was an error. Please try again later.That?s all we know.