Deloitte.

Imagem perfeita

Um modelo para identificação digital

Índice

Introdução

Caros colegas,

Cada setor está enraizado em uma tecnologia inovadora. Os concentrados congelados transformaram o suco de laranja em uma commodity no mundo todo. O transistor se tornou a base da eletrônica de hoje. A anestesia (juntamente com a teoria do germe da doença), inaugurou a era da cirurgia moderna.

E agora temos a identificação digital.

Os sistemas de identificação que utilizamos hoje estão retardando a inovação na tecnologia para o setor financeiro. Estão começando também a prestar serviços financeiros online. As transações globais digitais, tão próximas de nós, só acontecerão junto com a identificação digital.

Pensando nisso, a Deloitte e o Fórum Econômico Mundial trazem este estudo sobre identificação digital, realizado ao longo de um ano. A meta? Entender o papel que as instituições financeiras devem desempenhar na construção de um padrão global de identificação digital.

Este documento é um resumo das constatações. Começa com um exame da identificação e sua importância para a tecnologia e os serviços financeiros e as sociedades em geral. Segue-se uma análise da própria identificação digital – o que é, como são os sistemas de identificação digital, alguns princípios orientadores para desenvolvê-los e os benefícios que podemos esperar. Por fim, imaginamos algumas das formas de aplicação da identificação digital no ramo de serviços financeiros.

Se você está ajudando a determinar a direção dos serviços financeiros, este artigo é para você. O documento deve lhe dar uma ideia geral da natureza da identificação e seu papel mais amplo de como vivemos. Esperamos que lhe dê também um sentido de urgência sobre desenvolvimento de sistemas de identificação digital para instituições financeiras e outras mais. Quando chegar à última página, você talvez concordará que o momento de agir é agora.

Atenciosamente,

Bob Contri

Líder global de Serviços
financeiros da Deloitte
bcontri@deloitte.com

Rob Galaski

Líder da Deloitte para o projeto Fórum do Futuro
dos Serviços Financeiros Deloitte Canadá
rgalaski@deloitte.ca

A identificação digital e o papel das instituições financeiras

A identificação do usuário é um problema complicado o setor financeiro. Hoje, uma transação que exige identificação – seja para um pagamento, um empréstimo ou outra operação – significa coletar comprovante físico por meio de um canal digital (como a fotografia de uma carteira de motorista) ou depender de processos de reconhecimento do cliente (KYC, *know your customer*, na sigla em inglês) pelas instituições financeiras. Até que esse problema esteja resolvido, uma oferta puramente digital da tecnologia em finanças é coisa do futuro.

A chave das transações online

A identificação do cliente é importante porque está no âmago de muitos processos de serviços financeiros. As instituições precisam desta identificação para cumprir regulamentos, avaliar riscos de seguro e crédito e proporcionar uma experiência personalizada do consumidor. Detalhes e precisão são fundamentais. A identificação digital promete melhorar isso ao remover as ineficiências dos processos que são, atualmente, em grande parte, manuais.

Mas a identificação digital não é importante apenas para os serviços financeiros. Pense nos serviços públicos que exigem comprovação de identidade: segurança de idosos, seguro desemprego, educação, assistência médica, eleições e muito mais. O comprovante de identidade é também necessário em muitas situações do comércio privado, como compra de bebidas, aluguel de apartamento ou aquisição de um carro. Toda essa exposição coloca pessoas e organizações em risco. Quando se trata de sistemas de identificação física, roubo e fraude são geralmente as primeiras coisas em que pensamos.

E a necessidade de uma solução digital está se tornando urgente. As transações estão crescendo em volume e complexidade. Os clientes esperam cada vez mais prestações de serviço regulares e de multicanais, e levarão seus negócios para outro lugar se não forem atendidos. Os reguladores, por sua vez, estão exigindo maior clareza nas transações. Esses órgãos responsabilizarão as empresas se as informações sobre a identidade estiverem ausentes ou imprecisas.

Finalmente, a sofisticação dos ataques digitais está aumentando. Os hackers podem explorar sistemas de identificação fracos mais facilmente do que nunca, causando estragos financeiros e de reputação em um piscar de olhos.

Um problema de várias camadas

Então, em que pé estamos com os sistemas de identificação digital? Uma maneira de entender isso é enxergá-lo como um problema de várias camadas. No fundo estão as normas que regem o funcionamento do sistema – e que precisam ser desenvolvidas. No topo está a prestação de serviços, que deve ser eficiente, eficaz e regular para os usuários. No meio estão a autorização, a troca de atributos, a autenticação e a coleta de atributos. Cada um deles tem seus próprios desafios.

Muitos esforços hoje cuidam de uma camada, mas não das outras. Por exemplo, as soluções de tecnologia de autenticação tendem a confiar em atributos que já foram coletados. Essas soluções fornecem uma melhor experiência para os usuários e garantem que cada operação seja feita pela mesma pessoa, mas não ajudam a identificar quem ela realmente é.

Camada de identidade	Finalidade	Problemas
Prestação de serviços	Oferecer serviços regulares para os usuários	Prestação ineficiente ou inadequada
Autorização	Prestar os serviços aos quais os usuários têm direito com base em seus atributos	Regras e relacionamentos de autorização complexos
Troca de atributos	Proporcionar meios de troca de atributos entre as partes	Falta de segurança e compromisso com a privacidade
Autenticação	Proporcionar meios de vincular usuários aos atributos	Autenticação fraca ou inconveniente
Coleta de atributos	Capturar e armazenar os atributos do usuário	Coleta de atributos insuficiente ou imprecisa
Normas	Desenvolver normas para reger a operação do sistema	Falta de coordenação e coerência

Outras soluções atendem a apenas um determinado tipo de transação. Essas soluções podem facilitar a prestação de um serviço público, por exemplo, mas é só. Essa abordagem também termina por coletar dados "lapidares" – coisas como nome e data de nascimento – em vez de dados que tragam outras variantes do usuário.

Finalmente, vemos muitas normas e procedimentos desenvolvidos com base em consenso, em detrimento do desenvolvimento de uma solução de identificação completa que poderia ser colocada amplamente em uso comercial.

A busca por um denominador comum

Essas lacunas são o resultado de um panorama de identificação digital congestionado. As empresas de tecnologia, as organizações profissionais e os governos estão todos esculpindo seu nicho. Tudo bem. Uma solução pode ser válida sem abordar todos esses aspectos.

É preciso, porém, haver alguma maneira de unir soluções para que formem um sistema de identificação forte. Algo que seja conveniente, eficaz, que permita aos usuários controlar suas informações e as proteja onde estiverem em uso. Algo que possa manusear grandes volumes de transações e faça sentido para todos os envolvidos. Tudo isso é óbvio, mas não torna as coisas mais fáceis de serem realizadas.

É por isso que as instituições financeiras devem assumir a liderança. Essas organizações estão excepcionalmente bem posicionadas para preencher as lacunas na identificação digital.

Para começar, as instituições executam muitas funções de identificação digital durante suas atividades normais. Já armazenam e verificam as informações do usuário. Suas operações abrangem várias jurisdições. As instituições financeiras têm capacidade comprovada para criar novos sistemas e normas. Em economias desenvolvidas, englobam pessoas, entidades jurídicas e ativos de forma quase completa.

Além do mais, estão estabelecidas. As operações das instituições financeiras e o uso de dados de clientes são estritamente regulados. Essas organizações funcionam como sancionadoras em muitas operações. Os consumidores confiam mais nas instituições financeiras para suas informações e ativos do que em outros tipos de entidades.

As vantagens de estar na frente

Quais as vantagens para as instituições financeiras? São três: eficiência (com toda sua contenção de custo), receita e transformação. Vamos dar uma olhada em cada uma.

Eficiência. Um banco de atributos de usuário confiável e consolidado pode eliminar o tempo e o potencial de erro humano do processo do negócio. Também pode criar novas maneiras de atender os clientes e construir melhores perfis de risco.

Receita. Maior conhecimento do cliente pode revelar as necessidades de novos produtos e serviços para esses clientes. Pode também abrir oportunidades de gerar receita de outras empresas que não têm acesso a esse tipo de informação do cliente ou não desejam retê-las, ou de pessoas que não são clientes, mas precisam comprovar suas identidades para alguma outra finalidade.

Transformação. Com a identificação digital, as empresas podem vislumbrar mais do que seu negócio atual. Podem funcionar como um corretor certificado para partes contratantes em outros setores e prestar serviços de identificação ao setor público (pense em serviços sociais e declaração de imposto). Podem também transferir a responsabilidade por informação errada para os usuários e eliminar a mineração de dados por terceiros na avaliação do histórico de crédito do cliente. O serviço ao cliente pode ser estendido a trabalho consultivo não financeiro.

Há diversas formas de configurar um sistema de identificação, que vão depender da situação. Falaremos disso em breve, mas, primeiramente, vamos examinar os tipos de problemas que a identificação pode criar para instituições financeiras.

O desafio da identificação global

As instituições financeiras estão familiarizadas com as dificuldades de coletar as informações necessárias para confirmar a identidade. Conformidade, devida diligência, conheça seu cliente (KYC) – nenhum desses processos é conhecido por sua eficiência, especialmente tendo em conta a obrigação de proteger as informações pessoais.

E esses são desafios gerais. Pense naqueles que os bancos de varejo, para não mencionar os bancos que atendem empresas de pequeno e médio porte, devem enfrentar. A falta de visibilidade do histórico financeiro de clientes novos torna muito mais difícil às empresas evitar fraudes, prestar serviços e fornecer produtos adequados.

E depois há os bancos de investimentos e corporativos, que têm seus próprios problemas de identificação. Rastrear a origem e a propriedade do ativo é um deles. Outro, é monitorar e rastrear os ativos re-hipotecados.

Grande parte desses problemas tem uma origem comum: são derivados de um sistema projetado para atender transações cara a cara. Dito de outra forma: temos uma economia digital moderna que ainda depende de registros físicos para estabelecer a identificação.

Então, qual é a alternativa? Como seria um sistema de identificação digital?

Em um sistema de identificação digital, a "identidade" é um conjunto de registros digitais que representa um usuário. Esses registros são mantidos em formato padrão por entidades que fornecem informações de identificação ou garantia necessária para conclusão de transações. Uma identidade digital também aceita e integra novos registros para criar uma visão valiosa do usuário.

Um sistema desses facilita a coleta e o compartilhamento da documentação de apoio Graças aos mais recentes protocolos de segurança e autenticação, um sistema de identificação digital também torna mais difícil danificar, perder, roubar ou adulterar registros de identidade. Finalmente, as identificações digitais oferecem às instituições voltadas para o cliente, tais como instituições de serviços financeiros e muitas outras, uma maneira melhor de prestar assistência a seus clientes.

Algumas tecnologias promissoras estão nos aproximando de um sistema de identificação digital. Avanços no armazenamento de dados oferecem melhorias para guardar informações do usuário, com mais privacidade, segurança e controle do usuário. Novos protocolos de transferência de dados aumentam a proteção contra interceptação e decodificação, deixando também mais controle nas mãos dos usuários. Também estão em desenvolvimento novas técnicas de autenticação, que vinculam os usuários a suas atividades digitais de forma mais robusta e persistente.

Porém, o caminho tem sido acidentado. Entre todas as novas tecnologias em desenvolvimento em todo o mundo, algumas já falharam. Obviamente, se o sistema não foi bem projetado, se não funciona direito ou não parece digno de confiança, as pessoas simplesmente não o usam. E qualquer esforço de desenvolvimento pode minar o capital. No entanto, há também armadilhas mais sutis, como atender um conjunto muito estreito de interesses ou terminar do lado errado da política pública. Isso reforça a ideia de que a identificação digital deve proporcionar igualmente uma variedade de benefícios para pessoas, empresas e a sociedade.

Uma cartilha de identificação digital

Uma identidade é composta de muitas partes diferentes de informações, também chamadas de atributos. Quanto mais atributos existirem, mais forte será a identidade. Isso é verdadeiro mesmo se um atributo for exclusivo.

Por exemplo, o governo pode emitir para alguém um número exclusivo. Contudo, o número, por si só, não diz quase nada. Se você também tiver o nome e a data de nascimento da pessoa, você conhece um pouco mais. Adicione uma foto, um número de celular, um endereço residencial, registros escolares e o histórico de emprego, e, de repente, você conhece mais ainda.

As pessoas físicas não são as únicas que têm identidades. As pessoas jurídicas (tais como empresas e fundações) e os ativos (patrimônio) também têm. Os atributos que acompanham a sua identidade ajudam outros a decidir a fechar um negócio com você – aceitar seu voto, abrir uma conta poupança, vender-lhe uma garrafa de vinho, e assim por diante. O mesmo vale para pessoas jurídicas e ativos. Suas identidades, ou melhor, alguns de seus atributos, ajudam os outros a decidir fazer negócios com o proprietário, representante ou custodiante em questão.

A garantia é um fator-chave em transações de identificação, e refere-se ao grau de certeza de que a identidade é real e pertence à pessoa que a usa. Algumas transações, como registrar-se em um site de notícias ou pagar uma multa de estacionamento, podem não valer todo o trabalho necessário para autenticar uma identidade em elevado grau de certeza. O oposto é verdadeiro para transações tais como usar uma conta de corretagem online ou receber determinados serviços do governo. Essas devem ser operações altamente seguras.

Outra faceta das transações de identificação é a de que tendem a formar redes dependendo do tipo de identidade. Por exemplo, sistemas de identificação do governo e sistemas de gestão de funcionários estão centrados em pessoas. Registros de negócios e sistemas de identificação do setor estão centrados em entidades jurídicas. Registros de ativos têm como base... bem, você entendeu.

Mas todos os sistemas de identificação têm algo em comum. Todos têm **usuários** – aqueles que têm uma identidade no sistema para poder realizar operações. Todos têm **provedores de identificação** – aqueles que armazenam os atributos de usuário, certificam que são reais e concluem as transações em nome dos usuários. Há também **terceiros confiáveis**, aqueles que atendem os usuários após os provedores de identificação os certificarem.

Além disso, todos os sistemas têm um órgão de governança que o supervisiona e determina as regras. E, como apoio, há uma espécie de plataforma que conclui as operações, fornecendo às partes o qu precisam.

Até agora, nada disso é novidade. É o mesmo sistema que as pessoas vêm usando ao longo da história. Alguém chega em uma agência de emprego com uma carta de apresentação; é um usuário. A carta é de alguém que certifica o usuário; este é um provedor de identificação. Aquele a quem a carta é dirigida é o terceiro credenciador. O terceiro credenciador decide se vai aceitar as pretensões da carta com base em seu próprio julgamento e no que sabe do provedor da identificação.

Um sistema de identidade digital segue esse mesmo processo, mas por via eletrônica. Tudo acontece online. Entretanto, a identificação digital tem várias vantagens. É mais fácil compartilhar entre as partes de uma transação. Pode incluir muito mais informações do que uma coleção de documentos físicos. E com a tecnologia adequada, pode dar aos usuários muito mais controle sobre como suas informações são armazenadas e usadas.

O panorama dos sistemas de identificação digital

Os sistemas de identificação digital dividem-se em cinco categorias básicas.

A primeira é o **gerenciamento interno de identidades**. Nesse tipo de sistema, a mesma parte funciona como provedor de identificação e terceiro credenciador. Por exemplo, uma empresa pode deixar os funcionários acessar diferentes serviços com base em seus atributos.

O segundo tipo de sistema é a **autenticação externa**. É semelhante ao primeiro tipo de sistema, mas com um conjunto adicional de provedores de identificação para autenticar usuários. A vantagem neste caso é que os usuários podem usar um conjunto de credenciais, ao invés de manter diferentes nomes de usuário e senhas para cada serviço.

A **identificação centralizada** é outra categoria. Nesse tipo de sistema, uma das partes (por exemplo, um governo) é um provedor de identificação que transfere os atributos de usuário para os terceiros credenciadores. Por exemplo, um registro de cidadão que permite que usuários votem, declarem imposto e assim por diante. Um terceiro credenciador pode ser uma entidade pública ou privada. Uma entidade privada pode acessar dados depois de pagar uma taxa e obter o consentimento do usuário.

Em seguida, vêm os sistemas de **autenticação federada**, em que um provedor de identificação usa um conjunto de terceiros para autenticar usuários para terceiros credenciadores. Esses sistemas são semelhantes aos sistemas de identificação centralizada, exceto que uma variedade de corretores privados emite as identificações digitais como um serviço para quem se inscreve.

Por último, os sistemas de **identificação distribuída** conectam muitos provedores de identificação a muitos terceiros credenciadores. Este tipo de sistema configura os usuários com uma "carteira" digital que funciona como um login universal para vários sites e aplicativos. Geralmente esses sistemas são de propriedade privada e dependem de normas operacionais comuns ao invés de um órgão administrativo.

1 Gestão de identificação interna	A mesma entidade é o provedor de identificação e terceiro credenciador	Melhor para gerenciar permissões de usuário dentro de uma única entidade com base em informações internas, para garantir que os indivíduos tenham acesso aos recursos corretos
2 Autenticação externa	Diversos provedores de identificação autenticam os usuários para um único terceiro credenciador	Melhor para simplificar o acesso do usuário a um conjunto de serviços oferecidos por uma única entidade, eliminando logins proprietários
3 Identificação centralizada	Um provedor de identificação atende diversos terceiros credenciadores	Melhor para proporcionar uma visão completa, precisa e padronizada de dados não-confidenciais para diferentes usuários
4 Autenticação federada	Um conjunto de provedores de identificação autentica os usuários para diversos terceiros credenciadores	Melhor para proporcionar uma visão completa, precisa e padronizada de dados, permitindo que os usuários se autentiquem em várias entidades, eliminando logins proprietários
5 Identificação distribuída	Diversos provedores de identificação atendem diversos terceiros credenciadores diferentes	Melhor para a conveniência, controle e privacidade do usuário em um ambiente online

Princípios orientadores

Uma rede de identificação natural bem-sucedida deve se basear em cinco princípios.

O primeiro deles é o Social Good. Ou seja, um sistema de identificação deve fornecer identificação a todos os usuários, atender a seus interesses e estar aberto a todos que queiram participar. Instituições financeiras, com suas diversas relações com usuários, podem influenciar essa inclusão e ajudar na adoção do sistema.

Em segundo lugar, os sistemas de identificação devem proteger as informações do usuário. Os sistemas de identificação atuais colocam os usuários em risco – deixam as informações do usuário vulneráveis à violação de privacidade, vazamento de dados e superexposição. Um sistema de identificação digital deve garantir que os terceiros credenciadores vejam apenas os dados de que necessitam e os usem apenas para os propósitos que divulgam. Para as instituições financeiras, isso significa que os sistemas de identificação devem ser ciberflexíveis e atender às normas de proteção de dados e armazenamento.

Isso leva ao próximo princípio, que é o de dar controle aos usuários sobre o armazenamento e a transferência de suas informações pessoais no sistema de identificação. Mais de um sistema de identificação falhou porque os usuários não confiavam nele. Sob essa orientação, as instituições financeiras precisarão do consentimento do usuário antes de acessar ou compartilhar informações de identificação.

Em seguida vem o tratamento de um sistema de identificação como um negócio sustentável de longo prazo. As partes interessadas devem saber que seu investimento compensará. Como entidades privadas importantes e confiáveis, as instituições financeiras têm papel fundamental na definição de normas e requisitos operacionais do sistema. Pode também ser uma oportunidade de oferecer a identificação como serviço.

O último princípio é a construção de sistemas de identificação em padrões de tecnologia e dados abertos. Projete-os para integrar as novas partes e atender às necessidades mutantes do usuário. A implicação para as empresas é que isso facilitará a troca de instituições financeiras para os usuários.

Construir uma rede de identificação bem-sucedida não é fácil. Quem serão os usuários? Qual problema o sistema de identificação irá solucionar? A resposta a estas perguntas ajudará você a determinar que tipo de sistema desenvolver. Então, os princípios orientadores de identificação, juntamente com suas implicações para as instituições financeiras, irão ajudar você a fazer as escolhas adequadas para todo o resto.

Princípios orientadores para a identificação digital

- **Social Good.** O sistema está disponível para todos os usuários e proporciona o máximo benefício para uma variedade de partes interessadas.
- **Melhoria da privacidade.** Informações do usuário são expostas apenas para as entidades certas sob as circunstâncias certas.
- **Centrado no usuário.** Os usuários têm controle sobre suas informações e podem determinar quem as detém e as acessa.
- **Viável e sustentável.** O sistema é sustentável como negócio e suporta a mudança de prioridades políticas.
- **Aberto e flexível.** O sistema é construído em padrões abertos para permitir escalonamento e desenvolvimento; normas e diretrizes são transparentes para as partes interessadas.

Benefícios

Bem planejada, uma rede de identificação digital deve beneficiar não só as instituições financeiras, mas também aqueles que trabalham com elas, como: usuários, provedores de identificação, terceiros credenciadores, governos e reguladores.

Partes interessadas da rede

Privacidade

Os usuários podem controlar quem tem acesso aos seus atributos.

Segurança

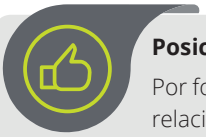
Os atributos do usuário são mantidos em locais seguros, enquanto os terceiros credenciadores sabem quem é genuíno.

Transparência

Os usuários sabem como e quando seus atributos são expostos.

Conveniência

A transferência de atributos digitais torna as transações de usuário mais eficientes.

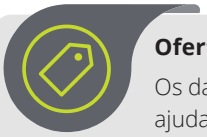


Posicionamento

Por forjar um relacionamento forte com os usuários, os provedores de identificação se tornam uma parte essencial da economia digital.

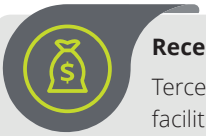
Fechamento

Uma experiência de usuário simplificada remove as barreiras para concluir transações.



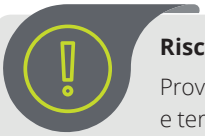
Ofertas

Os dados do cliente ajudam os provedores de identificação e terceiros credenciadores a oferecer produtos e serviços personalizados.



Receita

Terceiros credenciadores facilitam a conclusão de transações, enquanto os provedores de identificação podem cobrar para processá-las.



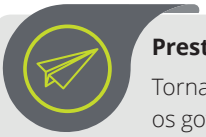
Risco

Provedores de identificação e terceiros credenciadores compreendem sua responsabilidade em caso de perda ou violação de dados.

Governos e reguladores

Processo

Governos podem interagir com os cidadãos de forma mais eficiente, poupando tempo e dinheiro.



Prestação de serviços

Torna-se mais fácil para os governos identificar e prestar serviços para vários grupos de cidadãos.

Ativos

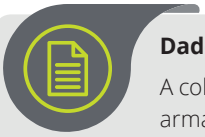
Os reguladores dispõem de uma melhor maneira de rastrear a origem e propriedade dos ativos.

Entidades

Os reguladores têm uma visão agregada das entidades em todas as suas hierarquias.

Conformidade

Os reguladores acessam atributos de usuário confiáveis e atualizados, fortalecendo o processo de conformidade global.



Dados

A coleta e o armazenamento de dados são padronizados em todas as instituições financeiras, removendo atritos da agregação de dados.

Instituições financeiras

Ofertas

Empresas podem usar informações detalhadas e confiáveis do cliente para fornecer serviços personalizados.

Operações

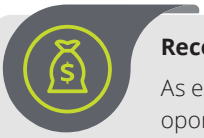
A transferência e a manipulação de atributos digitais permitem às instituições financeiras simplificar e automatizar muitos processos, eliminando o erro humano.

Segurança

O armazenamento seguro e digital das informações do usuário reduz a fraude resultante de informações roubadas ou de autenticação comprometida.

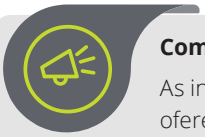
Conformidade

Graças à manipulação de atributos digitais e ao maior acesso à identidade do usuário, a conformidade se torna mais fácil e precisa.



Receita

As empresas têm a oportunidade de aumentar a receita com melhores produtos e serviços, bem como oferecer a identificação como serviço.



Competitividade

As instituições financeiras oferecem uma experiência de usuário simplificada e se posicionam como parte essencial da economia digital.

Aplicações futuras

Além de seus benefícios inerentes, como ficaria a identificação digital no ramo dos serviços financeiros? Como de costume com uma nova tecnologia, isso depende de como é usada. Aqui, exploramos oito aplicações potenciais.

Perfis de risco personalizados. As instituições financeiras criam um perfil de risco a partir de uma combinação de algoritmos preditivos e qualquer informação que tenham coletado sobre o cliente. No futuro, as instituições poderão fazer uso dos atributos já existentes no perfil digital do usuário, juntamente com uma gama de outros atributos que o usuário aceite fornecer. Com a disponibilidade de informações em maior quantidade e qualidade, as empresas podem criar produtos de risco e crédito personalizados para seus clientes incentivando-os, por sua vez, a não se afastar.

Restabelecimento internacional. Sem comprovação de identidade, qualquer um que tentar abrir uma conta está fadado a fracassar. Se puder estabelecer a identidade, mas não o histórico financeiro, a instituição financeira pode optar por correr o risco, de qualquer forma, se não quiser perder o negócio. Essa situação desagradável de "tabula rasa" pode ser evitada se os usuários incorporarem uma identificação digital. Em qualquer lugar no mundo, os usuários podem acessar serviços financeiros, e outros, com base nas certificações e atributos coletados por instituições anteriores. E cada nova instituição se torna outro provedor de identificação, reforçando ainda mais as credenciais digitais do usuário.

Atributos vinculados a tokens de pagamento. Suponha que você nunca mais tenha que confirmar manualmente sua idade, endereço de entrega ou qualquer outra coisa no ponto de venda. A identificação digital pode tornar isso realidade, permitindo que comerciantes obtenham as informações que precisam das instituições financeiras, com o consentimento do usuário. A transferência digital de atributos estaria livre de potenciais erros humanos e ajudaria a fechar mais transações. Acrescente a isso a autenticação, e as fraudes potenciais também estarão eliminadas.

Declaração de impostos digital. Nesse momento, pessoas e empresas devem recolher informações de várias fontes – instituições financeiras, empregadores, escolas e assim por diante – antes que possam fazer suas declarações. Em vez disso a identificação digital pode persuadir governos a aceitar declarações de instituições financeiras designadas pelos contribuintes. As empresas usariam seu total conhecimento das participações financeiras, ativos, receita e circunstâncias pessoais dos clientes para preencher automaticamente os formulários de declaração de rendimentos.

Determinação da exposição total de risco. Entidades jurídicas muitas vezes têm dificuldade em determinar sua exposição total de risco em uma transação, devido a estruturas complicadas de patrimônio e a quantidade de trabalho que requer a devida diligência. A identificação digital pode proporcionar uma visão consolidada de cada parte em uma transação, permitindo às empresas responder suas próprias perguntas sobre o risco de forma muito mais conveniente.

Identificação das contrapartes de uma transação. Identificar todos os participantes de uma transação intermediada pode ser quase impossível hoje. Todavia, com a identificação digital, as entidades jurídicas podem pedir para examinar a identidade consolidada de um terceiro e o histórico de posse de qualquer ativo envolvido. Saber mais sobre o cliente direto e o cliente final pode levar a uma decisão mais informada sobre como concluir a transação.

Vinculação da identidade individual à identidade corporativa. As empresas não estão necessariamente vinculadas a todas as pessoas que trabalham com elas. Se os atributos de identidade para pessoas físicas e jurídicas forem coletados, armazenados e transferidos digitalmente de forma padrão, as instituições financeiras teriam conhecimento ou percepções confiáveis sobre seus relacionamentos. As informações precisas e atualizadas atenderiam o KYC e muitas outras finalidades.

Rastreamento total de ativos re-hipotecados. Quando ativos são re-hipotecados, suas transações e histórico de posse podem se tornar ambíguos. Isso cria risco para a contraparte e torna difícil determinar o justo valor do ativo. Além disso, a falta de um mecanismo de rastreamento histórico impede a imposição de limites sobre a extensão dos ativos re-hipotecados. Informações consolidadas, padronizadas e digitais sobre os ativos tornaria possível verificar coisas como emitente e histórico de transações. Isso ajudaria a evitar re-hipotecas excessivas e tornar as transações menos arriscadas

Conclusão

Haverá uma única solução global para a identificação? Não conte com isso. Pode não fazer sentido, afinal, enquanto tivermos uma base de princípios para desenvolver e conectar redes de identificação.

Por um lado, a identificação precisa variar por usuário. As pessoas precisam concluir transações com segurança e de forma conveniente. Entidades jurídicas precisam de uma forma abrangente de agregar dados para o gerenciamento de risco. Ativos precisam de um sistema de rastreamento que seja transparente sobre patrimônio e valor.

Outro aspecto é a privacidade – algo que as pessoas precisam. Entidades jurídicas e ativos podem dispensá-la; na verdade, a privacidade pode até interferir com suas finalidades principais. Em qualquer caso, as pessoas têm autodeterminação, enquanto entidades jurídicas e ativos têm custodiantes que agem em seu nome.

Além disso, a identidade é cultural. Cidadãos de algumas nações aceitam uma carteira nacional de identidade. Outros não. Alguns governos podem não ser suficientemente estáveis para realizar a identificação digital.

Portanto, não existe uma solução única. Diferentes grupos construirão suas próprias redes de identificação. Provavelmente é assim que deve ser. Mesmo assim, no nível mais alto, todas as redes compartilham o mesmo caminho básico para o desenvolvimento:

1. Saiba quem você está tentando atender.
2. Compreenda as necessidades que você está tentando preencher.
3. Decida quem deve ser envolvido para que o sistema funcione.
4. Descubra uma maneira de unir forças – seja como parceria privada, consórcio, utilitário ou algum outro modelo.
5. Descreva o que a solução deve conseguir fazer e traduza isso em requisitos técnicos que um desenvolvedor de sistema possa seguir.
6. Monte a solução, teste-a e lance-a.

Incentivamos as empresas a considerar uma abordagem de baixo para cima para a identificação digital. Em primeiro lugar, teste e refine o sistema com uma massa crítica das partes. Então, vá escalonando-o gradualmente para incluir mais usuários, terceiros credenciadores e provedores de identificação.

Aqui está outra coisa que as instituições financeiras podem fazer como grupo: construir os conectores entre as redes. Isso é o que permite às redes de identificação digital serem formadas dentro de seus limites naturais, atendendo seus componentes da forma que melhor lhes convêm, indefinidamente. Essas conexões são os trilhos de interoperabilidade – e permitem o surgimento de um plano global de identificação digital.

Contatos

Contatos globais

Anna Celner

Líder global, Banking & Securities
Zurich
acelner@deloitte.ch

Neal Baumann

Líder global, Seguros
New York
nealbaumann@deloitte.com

Cary Stier

Líder global, Gestão de investimentos
New York
cstier@deloitte.com

Rob Galaski

Deloitte Canada
Líder da Deloitte para o projeto Fórum do Futuro dos Serviços Financeiros
Toronto
rgalaski@deloitte.ca

Ted DeZabala

Líder global, Cyber Risk Services
New York
tdezabala@deloitte.com

Joe Guastella

Líder global, Consultoria para Serviços Financeiros
New York
jguastella@deloitte.com

Vikram Bhat

Líder global Cyber Risk Services para Serviços Financeiros
New York
vbhat@deloitte.com

Contatos regionais

Brasil

Clodomir Félix

São Paulo
clodomirfelix@deloitte.com

Paschoal Baptista

São Paulo
pabaptista@deloitte.com

Américas

Rohit Malhotra

Estados Unidos
rmalhotra@deloitte.com

Andre Romanovskiy

Canadá
aromanovskiy@deloitte.ca

Linda Pawczuk

Estados Unidos
pawczuk@deloitte.com

Europa, Oriente Médio e África

Michel De La Belliere

França
mdelabelliere@deloitte.fr

Nick Seaver

Reino Unido
nseaver@deloitte.co.uk

Chris Verdonck

Bélgica
cverdonck@deloitte.com

Ásia-Pacífico

Trey Gannon

Austrália
tregannon@deloitte.com.au

Mitsuhiko Maruyama

Japão
mitsuhiko.maruyama@tohmatsu.co.jp

Tse Gan Thio

Sudeste asiático
tgthio@deloitte.com

Um agradecimento especial a Christine Robson da Deloitte Canadá por seu auxílio neste relatório.

Deloitte.