União Africana

An Integrated, Prosperous and Peaceful Africa

QUADRO DE INTEROPERABILIDADE DA UA PARA A IDENTIFICAÇÃO DIGITAL

FEVEREIRO 2022

ÍNDICE

SUMÁRIO EXECUTIVO

Centenas de milhões de pessoas em África carecem de identificação legal (ID) e muitas mais têm identificações que não são adequadas à era digital. Consequentemente, enfrentam desafios de acesso a serviços e oportunidades que estão a ser criadas através da digitalização. Por conseguinte, sistemas de identificação digital interoperáveis, fiáveis e inclusivos, que proporcionam às pessoas a capacidade de verificarem a sua identidade legal num ambiente virtual e não virtual, podem ajudar a enfrentar esses desafios e têm um potencial significativo para acelerar a digitalização das economias e sociedades africanas, apoiando o empreendedorismo e contribuindo para a implementação bem-sucedida da Zona de Comércio Livre Continental Africana (ZCLCA). É por estas razões que a maioria dos países africanos está actualmente a modernizar os seus ecossistemas de identificação, embora em fases diferentes.

O Quadro de Interoperabilidade da UA para a Identificação Digital (o Quadro) estabelece uma visão que **permitirá que todos os cidadãos africanos tenham a possibilidade de aceder com facilidade e segurança aos serviços públicos e privados de que necessitam, quando precisam deles, independentemente da sua localização.** Para este efeito, o Quadro define requisitos comuns, normas mínimas, mecanismos de governação e um maior alinhamento entre os quadros jurídicos com os objectivos que se propõem:

1. permitir aos cidadãos africanos verificar a sua identidade jurídica offline e online para acederem aos serviços dos sectores público e privado nos Estados-membros da UA, contribuindo para alcançar um progresso acelerado no sentido da unidade e integração continental para um crescimento sustentado, comércio, trocas de bens, serviços, livre circulação de pessoas e capitais através do estabelecimento de uma África unida e de uma integração económica rápida através da ZCLCA, conforme consta da aspiração 2 da Agenda 2063;

2. capacitar os cidadãos africanos com controlo sobre os seus dados pessoais, incluindo a capacidade de revelar selectivamente apenas os atributos necessários para uma determinada transacção; a informação pessoal a revelar deve ser mínima, proporcional e conter apenas a informação relevante para essa transacção que considerou a situação particular de África e em conformidade com as melhores práticas internacionais[1]; e

3. reforçar a confiança e a interoperabilidade entre os sistemas de identificação fundacional dos Estados-membros da UA.

O Quadro prevê fornece uma norma comum a nível continental para representar digitalmente as provas de identidade emitidas por fontes fiáveis dos Estados-membros da UA e para assegurar a interoperabilidadecionalidade em todo o continente. Os indivíduos que possuem uma identificação de um sistema nacional poderão obter uma credencial de identidade digital interoperávelacional (IDC-ID) que assumirá a forma de um crédito verificável[2]. Serão estabelecidas normas para o quadro de interoperabilidadecionalidade que definirão elementos

1 Consultar o Regulamento Geral da UE sobre Protecção de Dados (RGPDGDPR), 2016: https://gdpr.eu.

2 As reivindicações são uma colecção de atributos sobre uma pessoa em causa: por exemplo, nome de família, ou dados de nascimento. Uma "alegação verificável" é uma versão inviolável desta informação que pode ser verificada criptograficamente para verificar confirmar a sua autenticidade.

fundamentais da, pela IDC-ID. Estas normas e que demonstrarão a confiança nas credenciais digitais conforme criadas sob a governação de um quadro fiável que define as condições sob as quais tais credenciais serão emitidas por fontes fidedignas dos Estados-membros da UA.

Os Estados-membros da UA são livres de escolher como querem emitir esta credencial digital. Pode ser armazenado num formato puramente digital numa aplicação baseada em telefones inteligentes, num servidor baseado em nuvem, num cartão inteligente ou numa ligação à representação digital que pode ser estabelecida usando um código de barras de uma ou duas dimensões num documento em papel (impresso em papel, cartão plástico). Os Estados-membro podem igualmente decidir reutilizar esta norma para representar os dados de identidade a nível nacional, como parte de uma solução de identificação digital a nível continental ou das CER, ou mesmo emitida separadamente em complemento dos sistemas de identificação digital preexistentes.

O Quadro será baseado no desenvolvimento de sistemas de identificação fundacionais interoperáveis, inclusivos e de confiança, uma vez que estes fornecem a espinha dorsal de fontes de dados fiáveis sobre a identidade legal das pessoas, permitindo assim ao IDC-ID alcançar níveis mais elevados de garantia. Os Estados-membros da UA são, portanto, incentivados a reforçar os seus sistemas de identificação fundacionais levando em conta mecanismos de suporte como os *Princípios de Identificação para o Desenvolvimento Sustentável.*[3] Este quadro leva igualmente em consideração e tem em conta os esforços continentais paralelos para criar um ambiente propício com vista a proteger os dados pessoais, manter a segurança cibernética e salvaguardar os direitos das pessoas, com a adopção da Convenção de Malabo sobre a *Segurança Cibernética e Protecção de Dados Pessoais na União Arficana*[4] e o trabalho em curso para desenvolver um quadro de política continental de dados.

A emissão do IDC-ID pode ser completada com uma infra-estrutura que permita casos de utilização mais avançada, tais como a autenticação à distância. Este Quadro destaca várias opções técnicas que estão à disposição dos Estados-membros da UA para implementar este nível, por exemplo, uma federação de fornecedores de identidade que proporcione mecanismos de autenticação aos detentores de IDC-ID, ou o desenvolvimento de soluções de carteira de identidade digital ou quaisquer outros modelos que permitam a interoperabilidade. Os Estados-membros da União Africana poderão também procurar um acordo sobre a forma de estabelecer esta infra-estrutura do nível de autenticação e estabelecer parcerias com as CER e outras iniciativas continentais que já estão a investigar a introdução de soluções interoperáveis de identificação digital fundacionais para aceder aos serviços à distância.

O êxito da implementação do Quadro proposto baseia-se no pressuposto de que este será adoptado e aprovado pelos Estados-membros da UA. O risco de exclusão, os fracos mecanismos de segurança, o risco de destruição da privacidade pessoal, uma falta de procura (muitas vezes devida a incertezas sobre o benefício dos sistemas de identificação digital fundacional), uma falta de competências técnicas e financeiras, a escassez de centros de dados (importantes para o armazenamento de dados sensíveis) em toda a África. A presença de sistemas de identificação não operacionais e os quadros legais e regulamentares desactualizados são alguns dos riscos identificados a serem mitigados e solucionados, e alguns dos desafios a superar. Estes desafios são tratados mais aprofundadamente na secção 5.

3 Os Dez Princípios para a Identificação do Desenvolvimento Sustentável foram aprovados por 30 organizações internacionais e regionais, incluindo instituições africanas como a UNECA, AfDB e Smart Africa, bem como foram adoptados por uma série de países africanos. Vide: https://id4d.worldbank.org/principles

4 União Africana (2014), Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

O documento é constituído pelas seguintes secções:

1. Um **historial** sobre o trabalho da União Africana que levou à criação deste documento, uma visão geral do estado dos sistemas de identificação em África e uma série de iniciativas que promovem a interoperabilidade da identificação digital no continente;
2. Uma **introdução** à visão, objectivos, âmbito e casos de utilização potencial para o Quadro proposto;
3. Uma visão geral dos **elementos fundamentais que constituem o Quadro**, nomeadamente os princípios orientadores para a sua concepção e implementação, o modelo seleccionado, os principais componentes do Quadro que terão de ser melhor definidos (por exemplo, regras de participações, interoperabilidade e requisitos técnicos), bem como três potenciais opções arquitectónicas para definir um nível de autenticação da interoperabilidade;
4. Um **roteiro de alto nível** que detalha a abordagem faseada proposta para a definição e implementação do Quadro, bem como as acções concretas que os Estados-membros e a União Africana podem levar a cabo;
5. 5.Pressupostos de alto nível, desafios, riscos a enfrentar e mecanismos de mitigação recomendados.

O Quadro não exige a criação de um sistema unificado de identificação digital a nível continental, mas estabelece um enquadramento de interoperabilidade entre os sistemas de identificação digital fundacionais existentes entre os Estados-membros da UA, e tem em consideração a soberania digital dos Estados-membros da UA, as diferenças na implantação da infra-estrutura digital, a disponibilidade de políticas e regulamentos associados, os diferentes tipos de sistemas de identificação e a vulnerabilidade das populações durante e após a implementação dos sistemas interoperáveis de identificação digital.

ACRÓNIMOS E ABREVIATURAS

ZCLCA	Zona de Comércio Livre Continental Africana
AML/CFT	Combate ao Branqueamento de Capitais/Combate ao Financiamento do Terrorismo
IPA	Interface de Programação da Aplicação
UA	União Africana
CUA	Comissão da União Africana
ERII	Equipas de Resposta a Incidentes Informáticos
RCEV	Registo Civil e Estatísticas Vitais
APD	Autoridade de Protecção de Dados
AIPD	Avaliação do impacto da protecção de dados
CAO	Comunidade da África Oriental
CEDEAO	Comunidade Económica dos Estados da África Ocidental
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	Associação GSM
MSE	Módulos de Segurança de Equipamentos
TIC	Tecnologias de Informação e Comunicação
CDI-ID	Credencial Digital Interoperável de Identidade
UIT	União Internacional das Telecomunicações
CEC	Conheça o seu cliente
NDG	Nível de Garantia
QCPA	Quadro de Confiança Pan-Africano
CER	Comunidade Económica Regional
TC	Terceiros de confiança
AFAI	Aliança Fiduciária da África Inteligente
O Quadro	Quadro de Interoperabilidade da UA para a Identificação Digital
UNECA	Comissão Económica das Nações Unidas para África
WURI	Identificação Única da África Ocidental para a Integração e Inclusão Regional

Ver Anexo I para definições de trabalho.

1. ANTECEDENTES

1.1. CONTEXTO

Ser capaz de provar a sua própria identidade é essencial para a sua capacidade de aceder aos serviços e exercer os seus direitos. Tradicionalmente, a prova de identidade podia ser feita com base na familiaridade, aparência e comprovação por outros, o que funcionava em comunidades mais pequenas e informais. À medida que as sociedades e economias se tornaram maiores, mais formalizadas e integradas, foram introduzidas credenciais físicas como documentos de identificação e passaportes para estabelecer a confiança. Contudo, à medida que os países mudam para sociedades e economias digitais, tais credenciais físicas não são muito úteis para provar a identidade através da Internet e realizar outras transacções digitais, tais como pagamentos digitais e partilha de dados pessoais. Um pré-requisito para a confiança electrónica são, portanto, as identidades digitais, representadas por identificações digitais que utilizam tecnologias e abordagens modernas para permitir às pessoas provar e verificar com segurança a sua identidade virtual.

A identificação, e em particular a identificação digital, pode proporcionar uma vasta gama de benefícios para os países, tais como a boa governação, inclusão financeira, igualdade de género e o empoderamento das mulheres, o reforço da protecção social, dos cuidados de saúde e dos resultados da educação. Para as pessoas, as identificações digitais são um instrumento para fazer valer os seus direitos e elegibilidade para os serviços e transacções. Da mesma forma, proporcionam uma plataforma para governos e empresas para racionalizar, expandir e inovar a sua prestação de serviços operacionais através da utilização da digitalização e da automatização, especialmente quando encarada como uma "pilha digital" com partilha de dados e plataformas de pagamento digital de confiança.[5] Considerando que a Internet não tem fronteiras, as identificações digitais que são emitidas num país e reconhecidas noutros podem também ser um poderoso motor de integração social e económica, seja a nível bilateral, regional ou global.

As identificações digitais alcançam a maior segurança e impacto quando se baseiam na identidade legal dos indivíduos. A identidade legal é tipicamente gerida pelo ecossistema de identificação fundacional de um país, incluindo o registo civil, a identificação nacional e outros sistemas semelhantes. No entanto, centenas de milhões de pessoas em África ainda carecem de identificação fundacional, tal como um BI nacional ou uma certidão de nascimento.[6] É neste contexto que, em Julho de 2016, a Conferência da União Africana declarou os anos entre 2017-2026 como a década para o reposicionamento da CRVS em África como agenda de desenvolvimento continental, regional e nacional e instou os governos a responderem com acções apropriadas.

Agenda 2063: "A África que queremos", que é o quadro estratégico para o desenvolvimento socioeconómico e a transformação do continente num período de 50 anos, exigiu uma identidade jurídica para todos. A Estratégia de Transformação Digital para África (ETED) aprovada na 36.ª Sessão Ordinária do Conselho Executivo da União Africana em Fevereiro

5 A COVID-19 realçou a importância das pilhas digitais, uma vez que os países com as mesmas parcial ou totalmente implementadas antes da pandemia apresentaram maior capacidade para fornecerem assistência social mais rápida e eficazmente e foram mais resilientes quando os serviços presenciais tiveram de ser movidos para uma presença virtual.

6 Banco Mundial, Global ID4D Dataset, vide: https://id4d.worldbank.org/global-dataset.

de 2020 em Adis Abeba, Etiópia (EX.CL/Dec. 1074 (XXXVI)), também sublinhou a importância da Identificação Digital como um elemento fundamental para a criação de um Mercado Único Digital (uma missão que é também partilhada pela Aliança Inteligente de África) em conformidade com a ZCLCA.

A Estratégia de Transformação Digital para África reconheceu igualmente que o desenvolvimento da economia e da sociedade digitais depende de importantes facilitadores, nomeadamente um forte ambiente favorável no que diz respeito à segurança cibernética e à protecção de dados. A Convenção Malabo de 2014 sobre Segurança Cibernética e Protecção de Dados Pessoais[7] estabelece um quadro jurídico, político e regulamentar que apoia a criação de um ambiente digital seguro para a transacção digital, o comércio electrónico e a transferência de dados. Infelizmente, este quadro jurídico ainda não foi assinado e ratificado pelo número necessário de Estados-membros da UA para a sua entrada em vigor, o que limita efectivamente a sua eficácia.[8] Tal quadro jurídico não só contribuirá para a promoção da confiança no Quadro e inclusão, mas também mitigará os riscos ligados à vigilância e discriminação não autorizadas, particularmente para grupos vulneráveis ou marginalizados, bem como assegurará a responsabilização das autoridades de implementação.

1.2 SITUACIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN EN ÁFRICA

Os sistemas de identificação (ID) fiáveis e inclusivos são um factor impulsionador de muitos resultados de desenvolvimento, tais como a erradicação da pobreza, boa governação, migração segura e ordenada, protecção social, igualdade de género, e são um importante motor da transformação digital. Dada a necessidade fundamental de uma identificação e autenticação electrónica segura e precisa, a identificação digital e outros serviços de confiança – como as assinaturas digitais – representam a próxima fronteira para os países do continente. Quando activados por infra-estruturas digitais que colocam pessoas e organizações online, os serviços de identificação digital e de confiança podem ser alavancados por plataformas governamentais e comerciais para facilitar uma variedade de transacções digitais, incluindo pagamentos digitais. A nível de país, a identificação digital poderia funcionar como um identificador único para os sistemas centrados no cidadão, tornando viável a integração de sistemas. Em conjunto, as plataformas de identificação digital e de pagamentos fornecem os meios para avançar para uma sociedade sem dinheiro, criando ganhos de produtividade, reduzindo a corrupção e a fraude, e melhorando ainda mais a conveniência do utilizador.

Em todo o continente, existe uma vasta gama de tipos de sistemas de identificação e níveis de ligações de desenvolvimento à prestação de serviços. Muitos outros encontram-se em níveis intermédios de desenvolvimento com lacunas de cobertura entre populações vulneráveis e capacidades digitais emergentes, enquanto outros ainda têm sistemas de identificação fundacionais inexistentes ou emergentes. Globalmente, o número de países que implementam sistemas nacionais de identificação aumentou exponencialmente durante as últimas duas décadas, impulsionado pelo desejo de melhorar a eficiência e a orientação dos pagamentos e transferências governamentais, de reforçar a integridade do sector financeiro (incluindo através do registo KYC e SIM) e o das eleições, de reforçar a segurança pública e de promover

7 União Africana (2014), Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

8 Desde Julho de 2021, 14 dos 55 EM assinaram a Convenção Malabo, entre os quais 10 EM a ratificaram. Para entrar em vigor, é necessária uma ratificação por pelo menos 15 Estados-membros

uma migração segura e ordenada. Há um impulso contínuo para reformar e modernizar a concepção do sistema e as abordagens de implementação online com a expansão das provas sobre boas práticas e lições aprendidas com programas de identificação bem-sucedidos.[9]

Um bom exemplo é dado pelo Ruanda que conduziu uma campanha para digitalizar a sua economia e dar poder à sua classe média, conduzindo acções como a mudança para uma economia sem dinheiro, que o governo pretende alcançar através da penetração omnipresente dos telemóveis e do acesso de alta velocidade à Internet. O Ruanda aderiu à Aliança Melhor do que Dinheiro, uma parceria global empenhada em passar de pagamentos em numerário para pagamentos digitais. O Ruanda já está a sentir uma maior eficiência e maiores receitas geradas pela eliminação de custos de cobrança e outras despesas. Tornou-se igualmente um líder do conhecimento na região, e está a partilhar as melhores práticas com outros interessados em seguir um caminho semelhante.[10]

As capacidades digitais dos sistemas de identificação aumentaram muito, embora a identificação digital no contexto de transacções online ainda esteja na sua fase embrionária. Durante a última década, muitos países envidaram esforços para modernizar os seus sistemas de identificação, com o objectivo de criar uma plataforma digital e emitir credenciais que sustentem uma variedade de usos e serviços. Estas reformas envolvem frequentemente uma transição de sistemas baseados em papel para sistemas digitais utilizando a captação e gestão electrónica de dados, e introduzindo mecanismos de verificação e autenticação da identidade digital - por enquanto, principalmente no contexto de transacções presenciais. A maioria (85%) dos países africanos tem sistemas nacionais de identificação baseados numa base de dados electrónica, embora muitos ainda dependam de registos e processos civis em papel, e muitos sistemas oferecem uma utilidade limitada para a prestação de serviços. Os dados biométricos são recolhidos por mais de 70% dos países africanos no momento do registo para garantir a exclusividade das identidades. Embora alguns países - tais como o Quénia, Lesoto, Nigéria, Ruanda, África do Sul - ofereçam serviços de verificação de identidade digital (a ministérios governamentais, bancos, etc.) para validar informações de identidade ou credenciais contra uma base de dados central, a autenticação para a maioria das transacções continua a depender da inspecção manual dos cartões de identificação física. As soluções de identidade digital que permitem autenticação segura para serviços e transacções online estão ainda na sua infância no continente, com tais serviços disponíveis apenas em alguns países (por exemplo, na África do Sul por bancos, em Cabo Verde, Seychelles para serviços de governo electrónico).

Apesar de muitas melhorias e do lançamento de novos sistemas nos últimos anos, os países africanos e os seus residentes enfrentam vários desafios no que diz respeito à identificação. Algumas das áreas fundamentais que necessitavam de reforço incluem a acessibilidade dos sistemas de identificação, a sua capacidade de apoiar eficazmente a prestação de serviços, e a implementação de salvaguardas que promovam a confiança e a privacidade dos dados.

Garantir o acesso universal dos sistemas de identificação é um desafio permanente. Estima-se que mil milhões de pessoas em todo o mundo carecem de documentos de identidade básicos - e aproximadamente metade da população reside em África.[11] África é igualmente o berço de 8 dos 10 países com as maiores disparidades de género na identificação a nível mundial e a cobertura de identificação entre adultos na África Subsariana é cerca de 10 pontos percentuais

9 Um inquérito de 2018 a funcionários governamentais africanos revelou que 60 por cento dos países africanos tencionavam lançar um sistema de identificação ou modernizar o sistema existente até ao final de 2020.
10 ITU/DIAL (2019) Quadro de Investimento Digital dos OSD, vide: https://www.itu.int/pub/D-STR-DIGITAL.02-2019
11 ID4D Global Dataset 2018: https://id4d.worldbank.org/global-dataset

mais baixa entre as mulheres do que entre os homens.[12] Os desafios na identificação começam desde o nascimento: 100 milhões de crianças com menos de cinco anos em África não tiveram seu nascimento registado.[13] As razões para estas lacunas de cobertura são múltiplas e incluem: elevados custos directos e (particularmente) indirectos de inscrição, incluindo o custo da viagem para locais de registo frequentemente distantes; requisitos documentais e administrativos complexos para o registo; e procura limitada nos casos em que os sistemas de identificação oferecem um valor limitado em termos de facilitação do acesso aos serviços.[14]

A utilização de tecnologias modernas também aumentou a complexidade e apresenta novos riscos. Por exemplo, nem todas as soluções estão bem adaptadas às necessidades e contextos locais onde a conectividade à Internet, o acesso à electricidade, ou a literacia digital entre funcionários públicos ou a população em geral podem ser limitados. O bloqueio de fornecedores é uma preocupação comum e está muitas vezes associado a custos operacionais insustentavelmente elevados, à interoperabilidade limitada do sistema de identificação e a baixos níveis de supervisão e controlo governamental e individual sobre dados de identidade. Além disso, com a crescente adopção das tecnologias digitais na identificação e autenticação, bem como com a mudança para as credenciais digitais, as pessoas com literacia digital limitada e acesso a dispositivos conectados correm o risco de ficar para trás.

À medida que os sistemas e o processamento de dados se tornam digitalizados, a necessidade de implementar salvaguardas eficazes para proteger os dados e a privacidade do indivíduo também aumentou. As salvaguardas inadequadas para a protecção de dados, privacidade, e direitos dos utilizadores - quer sejam jurídicos, institucionais, ou tecnológicos - podem deixar os sistemas de identificação vulneráveis a violações e os dados das pessoas desprotegidas. Muitos países têm ainda um longo caminho a percorrer na construção de sistemas de identificação seguros e fiáveis: de acordo com a CNUCED, apenas 28 países (50%) em África adoptaram legislação sobre protecção de dados e privacidade e 39 (70%) têm legislação sobre cibercriminalidade em vigor[15]. Mesmo onde tais quadros existem, traduzir disposições legais em controlos institucionais, operacionais e técnicos eficazes pode ser um desafio. A partir de hoje, apenas alguns países armazenam e gerem os seus dados de acordo com as melhores práticas internacionais de protecção contra roubo ou perda não intencional de dados.[16]

Os sistemas de identificação digital enfrentam os mesmos desafios que o desenvolvimento de ecossistemas digitais; estes desafios abrangem, entre outros aspectos, questões de financiamento, uma vez que os ciclos de financiamento, principalmente os baseados em dadores que são baseados em projectos e limitados no tempo, estão desligados dos ciclos de desenvolvimento tecnológico. Além disso, o planeamento em silos e a tomada de decisões entre grupos de interessados levam a oportunidades limitadas de coordenação entre os grupos de interessados; isso limita a reutilização de soluções digitais e prejudica a sua potencial aplicabilidade entre programas e sectores. As deficiências na literacia digital, nomeadamente a falta de capacidade na liderança das TIC, e na selecção, concepção, implementação, expansão e manutenção de soluções TIC, são frequentemente um problema entre governos e profissionais de desenvolvimento. Finalmente, a ausência de financiamento para a expansão de soluções de TIC é outra grande preocupação, uma vez que normalmente podem estar

12 https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf
13 https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf
14 https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf
15 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
16 https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

disponíveis fundos para financiar as fases iniciais do ciclo de vida do desenvolvimento tecnológico, mas com financiamento limitado disponível para a expansão a nível nacional (Quadro de Investimento Digital do ODS, ITU/DIAL, 2019).

1.3 OUTRAS INICIATIVAS QUE PROMOVEM O RECONHECIMENTO MÚTUO E A INTEROPERABILIDADE DAS IDENTIFICAÇÕES DIGITAIS EM ÁFRICA

Uma série de iniciativas existentes complementares ao Quadro já promovem o reconhecimento mútuo e a interoperabilidade de identificação digitais em África. Estes incluem, mas não estão limitados a:

1.3.1. ESTRATÉGIA DE TRANSFORMAÇÃO DIGITAL PARA ÁFRICA (2020-2030)

A identificação digital é reconhecida como um dos cinco temas transversais da Estratégia, que também faz dez recomendações políticas e propõe acções em dois temas para garantir a inclusão, segurança, privacidade e apropriação de dados, e apoiar a interoperabilidade e a neutralidade. Embora estas recomendações abranjam principalmente o desenvolvimento de sistemas nacionais de identificação digital, uma recomendação apela ao estabelecimento de uma "identidade digital continental interoperável e aberta, permitindo a validação e autenticação de indivíduos", enquanto outra recomendação solicita à CUA, à UNECA e a outros parceiros que "trabalhem em conjunto sobre normas continentais e regionais, incluindo sobre protocolos de autenticação, campos de dados mínimos, protocolos de duplicação, formatos biométricos, bem como outros formatos, regulamentos-modelo, e outras normas".

1.3.2. INICIATIVA DA UNECA SOBRE IDENTIDADE DIGITAL

A Comissão Económica das Nações Unidas para África (UNECA) lançou uma iniciativa sobre Identidade Digital, Comércio e Economia Digital (DITE), actuando como Centro de Excelência, que visa a harmonização de normas relacionadas, a adopção de regulamentos para salvaguardar a segurança, o aumento dos investimentos, e o desenvolvimento da capacidade e competências dos actores principais.[17] O Centro de Excelência Digital da CEA apoia o trabalho que visa estabelecer um quadro continental africano harmonizado sobre a Identificação Digital, definindo e moldando políticas e normas para a Identificação Digital, proporcionando o desenvolvimento de capacidades para os Estados-membros, Comunidades Económicas Regionais e a União Africana. A CEA produziu um livro branco sobre um quadro para a interoperabilidade digital através do estabelecimento de um Quadro Pan-Africano de Confiança (PATF).

17 UNECA, DITE for Africa, vide : https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa

1.3.3. ALIANÇA FIDUCIÁRIA DA ÁFRICA INTELIGENTE (SATA)

A África inteligente é uma iniciativa dos Chefes de Estado africanos para acelerar o desenvolvimento socioeconómico em África, alavancando as TIC. Em 2020, o Benim defendeu um projecto emblemático da África Inteligente para desenvolver o Plano de Identificação Digital, apoiado por um grupo de trabalho que incluiu o Ruanda, a Tunísia, a União Africana (UA), a União Internacional de Telecomunicações (UIT), o Banco Mundial, a Rede Omidyar, a Comissão Económica das Nações Unidas para África (UNECA), a Associação GSM, o Fórum Económico Mundial, a Gesellschaft für Internationale Zusammenarbeit (GIZ) e várias empresas privadas. Foi adoptado pelo Conselho da África Inteligente, incluindo os seus 32 Estados-membros, a UA e a UIT. O Projecto em Acção[18] propõe a SATA como uma plataforma para facilitar o reconhecimento fiável da Identificação Digital entre uma série de actores através de mecanismos federados de certificação. Prevê-se a realização de projectos-piloto da SATA entre o Benim, o Ruanda, a Tunísia e outros Estados-membros da África Inteligente. A SATA servirá como uma solução ágil e adaptável para permitir a interoperabilidade entre vários esquemas de identidade pública e privada no continente. Mais detalhes estarão disponíveis na página sata.smartafrica.org.

1.3.4. PROGRAMA DE IDENTIFICAÇÃO ÚNICA PARA A INTEGRAÇÃO E INCLUSÃO REGIONAL DA ÁFRICA OCIDENTAL (WURI)

O WURI[19] é um programa regional que utiliza o financiamento do Banco Mundial para aumentar o acesso a serviços nos Estados-membros participantes da CEDEAO através da construção de sistemas de identificação fundacionais acessíveis a todas as pessoas no território do país - sem consideração de nacionalidade ou estatuto legal - e que foram concebidos tendo em vista a interoperabilidade transfronteiriça para desbloquear o acesso a serviços sociais, de saúde, financeiros e outros serviços além-fronteiras. A Costa do Marfim, a Guiné e a Comissão da CEDEAO juntaram-se na primeira fase durante o ano de 2018, e o Benim, Burkina Faso, Níger e Togo juntaram-se na segunda fase durante o ano de 2020. Os princípios fundamentais do WURI incluem registo universalmente acessível e inclusivo, minimização de dados, e credenciais básicas que são fornecidas à população a custo zero.

1.3.5. PROTOCOLO DO MERCADO COMUM DA CEA

Através do artigo 8º do Protocolo, os seis Estados Parceiros da EAC comprometeram-se a trabalhar progressivamente no sentido de "...um sistema normalizado comum de emissão de documentos de identificação nacionais para os seus cidadãos".[20] Isto está fortemente ligado à realização de outros objectivos do Protocolo, incluindo a livre circulação de mercadorias (artigo 6º), pessoas (artigo 7º), mão-de-obra/trabalhadores (artigo 10º), serviços (artigo 16º), e capital (artigo 24º), bem como os direitos de estabelecimento e residência (artigos 13º e 14º, respectivamente). No entanto, os sistemas nacionais de identificação encontram-se em diferentes fases de desenvolvimento. Todavia, no espírito da geometria variável e como iniciativa dos Projectos de Integração de Corredores Nacionais (NCIP), Quénia, Ruanda e Uganda começaram em 2014 a reconhecer os cartões de identidade nacionais respectivos

18 Smart Africa, Blueprint | Smart Africa Alliance – Digital Identity, Outubro de 2020, ver: https://smartafrica.org/knowledge/digital-id/

19 Banco Mundial. Programa de Identificação Única para a Integração e Inclusão Regional da África Ocidental (WURI). https://projects.worldbank.org/en/projects-operations/project-detail/P161329 ; https://projects.worldbank.org/en/projects-operations/project-detail/P169594

20 https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png

como documentos de viagem válidos. No âmbito da NCIP, tem havido discussões no sentido de se desenvolverem casos de utilização adicional, tais como serviços electrónicos, embora estes ainda não se tenham materializado. Em 2018, o Banco Mundial e o secretariado da EAC realizaram um estudo sobre as opções para o reconhecimento mútuo de identificação nacionais (DNIs) na CEA que propôs quatro marcos.

1.4. SOBERANIA DIGITAL

Com 55 nações soberanas, África tem, portanto, 55 jurisdições legais a serem consideradas. A soberania digital descreve um espectro de diferentes conceitos técnicos e regulamentares, desde a localização física dos servidores, a construção de cabos submarinos, até às leis e práticas relativas à protecção de dados e à tributação dos mercados de dados, que permitem aos Estados tomar as suas próprias decisões sobre as escolhas tecnológicas e a sua regulamentação.

A fim de garantir a soberania dos dados, os Estados-membros da UA são encorajados a:

criar sistemas seguros de armazenamento de dados pessoais (incluindo dados sensíveis) através da concepção e criação de centros de dados nacionais que devem prever o controlo de dados pelo Estado e incluir pelo menos espaço de armazenamento e processamento dedicado exclusivamente a dados pessoais e sensíveis. Será necessário estabelecer as salvaguardas necessárias (técnicas, em particular) para assegurar que os dados utilizados no intercâmbio transfronteiriço de informações não incluam de forma alguma dados pessoais ou sensíveis cujo tratamento ou armazenamento possa colocar em risco os direitos dos indivíduos ou a soberania dos Estados membros da UA.

criar capacidade e infra-estruturas para o desenvolvimento de talentos e conjuntos de competências africanas para enfrentar os novos desafios e reforçar a soberania digital. Espera-se que os Estados-membros assumam a liderança no avanço das competências (incluindo competências de ciber-resiliência) de todos os cidadãos e residentes, e devem capacitar as pessoas a terem controlo sobre os seus dados pessoais.

estabelecer parcerias baseadas no respeito mútuo, em situações vantajosas para ambas as partes sem comprometer a soberania e a propriedade nacional e evitar interferências estrangeiras que possam afectar negativamente a segurança nacional, os interesses económicos e a evolução digital dos Estados-membros da UA.

O Quadro será orientado pelas regras soberanas representadas pela autoridade ou autoridades de registo e emissão de identidade de cada Estado-membro da UA, e a estrutura de governação, incluindo a criação de uma instituição de coordenação continental de supervisão, será aprovada pelos Estados-membros da UA. Além disso, os mecanismos de responsabilização, incluindo o tratamento de responsabilidades em caso de má conduta, serão definidos e aprovados pelos Estados-membros da UA. O desenvolvimento da confiança continental entre

Estados soberanos com esquemas de identificação digital divergentes é uma tarefa complexa mas exequível que requer a colaboração de múltiplas partes interessadas. Para alcançar a interoperabilidade para o intercâmbio de informações de identidade jurídica nos respectivos países africanos, as semelhanças entre as regras e normas nacionais existentes devem ser reconhecidas, com base num conjunto mínimo de critérios que permitam tanto a soberania local como a confiança suficiente na abordagem um do outro.

Para este efeito, os Estados-membros da UA necessitam de reforçar e melhorar os seus quadros jurídicos as suas capacidades de execução, em particular as capacidades das autoridades de protecção de dados no controlo das transferências transfronteiriças de dados e na aplicação das leis e regulamentos relevantes em casos de violação ou utilização indevida.

O quadro proposto abraçará as tecnologias mais avançadas e respeitará as legislações e regulamentos dos países. Os governos não devem ser obrigados a utilizar tecnologias específicas. A utilização de normas e padrões abertos deve garantir uma grande diversidade de escolhas tecnológicas por parte dos Estados, facilitando ao mesmo tempo a apropriação e a interoperabilidade pelos países.

2. INTRODUÇÃO

Em 2020, os Estados membros da União Africana adoptaram a Estratégia de Transformação Digital (ETED) para África (2020-2030) com a visão de:

Uma sociedade e economia digital integrada e inclusiva em África que melhore a qualidade de vida dos cidadãos africanos, reforce o sector económico existente, permita a sua diversificação e desenvolvimento, e assegure a apropriação continental com África como produtor e não apenas como consumidor na economia global.

A concretização desta ambição - bem como da ZCLCA - depende do desenvolvimento de sistemas de identificação digital inclusivos e fiáveis que permitam que todos os cidadãos africanos provem e verifiquem a sua identidade legal de forma fiável e segura ao efectuarem transacções presenciais e virtuais, e permitir aos prestadores de serviços dos sectores público e privado reconhecerem as credenciais de identidade, independentemente do local de origem em África onde tenham sido emitidas. É importante que os sistemas de identificação digital fundacionais sejam concebidos para empoderar as pessoas, especialmente as populações desfavorecidas e marginalizadas. Isto permitirá a todos participar de forma significativa na economia e sociedade digital, desbloquear o acesso aos serviços dentro dos países e além-fronteiras, promover o comércio como parte da ZCLCA, aumentar a confiança na sociedade e economia digitais, e reduzir a fraude e os custos de fazer negócios.

É importante notar que os sistemas de identificação digital fundacionais podem também sustentar o desenvolvimento de "pacotes digitais" mais amplos[21] com plataformas de pagamento digital e de partilha de dados fiáveis para criar oportunidades de inovação e uma vasta gama de transacções sem presença, sem papel e sem numerário em todo o continente. Contudo, isto também exige que os riscos relacionados com a exclusão, protecção de dados, segurança cibernética e tecnologia e o "bloqueio" de fornecedores sejam atenuados de forma abrangente. É por estas razões que a identificação digital é um dos cinco temas transversais da ETED, conferindo o mandato e o âmbito deste Quadro.

2.1. VISÃO, OBJECTIVOS E CASOS DE USO INDICATIVO

A visão do Quadro de interoperabilidade da UA para a Identificação Jurídica Digital é que todos os cidadãos africanos possam aceder com facilidade e segurança aos serviços de que necessitam, quando deles necessitam, tanto dos fornecedores do sector público como do privado, o que incentivará uma participação inclusiva e significativa na economia e sociedade digital em geral e permitirá que os serviços funcionem com maior confiança e certeza.

Para este efeito, o Quadro define requisitos comuns, normas mínimas, regras, mecanismo de governação e um alinhamento entre os quadros jurídicos e os objectivos a atingir:

21 No contexto das tecnologias digitais, um "pacote" é uma colecção de componentes ou infra-estruturas de software independentes que trabalham em conjunto para apoiar a execução de um caso de utilização

1. permitir a todos os cidadãos africanos verificar a sua identidade jurídica offline e online para acederem aos serviços dos sectores público e privado em todos os Estados-membros participantes da UA, contribuindo para alcançar um progresso acelerado no sentido da unidade e integração continental para um crescimento sustentado, comércio, trocas de bens, serviços, livre circulação de pessoas e capitais através do estabelecimento de uma África unida e de uma integração económica rápida através da ZCLCA, conforme consta da aspiração 2 da Agenda 2063;
2. empoderar a todos os cidadãos africanos com controlo sobre os seus dados pessoais, incluindo a capacidade de revelar selectivamente apenas os atributos que são necessários para uma determinada transacção;
3. reforçar a confiança e a interoperabilidade entre os sistemas de identificação fundacional dos Estados-membros da UA.

O Quadro não exige a criação de um sistema de identificação digital continental unificado, mas fornece uma base para a interoperabilidade entre os sistemas de identificação digital existentes nos Estados-membros da UA, que tem em consideração a soberania digital dos Estados-membros da UA, as diferenças na implantação da infra-estrutura digital, a disponibilidade de políticas e regulamentos associados, os diferentes níveis de sistemas de identificação e a vulnerabilidade das populações durante e após a implementação dos sistemas de identificação digital.

É primordial que este Quadro seja desenvolvido de acordo com as melhores práticas e normas internacionais[22] que visam proteger os dados pessoais, manter a segurança cibernética e salvaguardar os direitos das pessoas. Com a adopção da Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais e o trabalho em curso para desenvolver um quadro de política de dados continental[23], a União Africana deu um passo importante para estabelecer um ambiente digital credível para as transacções electrónicas através da adopção de um conjunto comum de regras que regem a transferência transfronteiriça de dados pessoais em todo o continente e o alinhamento dos quadros nacionais de protecção de dados e de segurança cibernética.

Um quadro continental pode facilitar o **acesso a serviços em todos os países participantes, permitindo às pessoas e empresas** verificar as credenciais e outros factos sem revelar dados pessoais. Isto inclui a possibilidade de autenticar a sua identidade ao aceder a serviços electrónicos (por exemplo, serviços governamentais) noutro país com a sua identificação digital sem a necessidade de se inscreverem nas soluções de identidade fundacional local reconhecidas pelos prestadores de serviços estrangeiros. O reconhecimento mútuo e a interoperabilidade da identificação digital também facilitam a partilha e o consentimento de credenciais verificáveis e de dados de confiança quando se solicita serviços onde a lei exige tal verificação (por exemplo, prova de seguro, estatuto de vacinação para qualificação), permitindo às pessoas poupar tempo e reduzir a burocracia.

Pode igualmente **reforçar a integridade e acessibilidade dos pagamentos e serviços financeiros transfronteiriços em África, e criar oportunidades de inovação.** Sistemas de identificação

22 Isto inclui, entre outros aspectos, a UIT-T X.1058 | ISO/IEC 29151, os Princípios e recomendações da ONU para sistemas de estatísticas vitais, os Dez Princípios sobre Identificação para o Desenvolvimento Sustentável, normas internacionais sobre protecção de dados, o Regulamento Geral Europeu sobre Protecção de Dados e outros

23 União Africana, Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

fracos e não fiáveis, a ausência de harmonização das regras criam riscos de branqueamento de capitais/ financiamento do terrorismo (AML/CFT)[24] que introduzem barreiras às trocas transfronteiriças, aumentam os custos dos serviços (por exemplo, remessas) e dificultam a inovação. A identificação digital pode facilitar a identificação e verificação do cliente a bordo, apoiar os processos "Conheça o seu Cliente (KYC)" e ajudar na monitorização das transacções com o objectivo de detectar e comunicar transacções suspeitas. O reconhecimento mútuo não só facilitará aos migrantes o envio de dinheiro para casa, facilitando a verificação de KYC e o encargo da autenticação, como também ajudará a baixar os custos, ajudando África a aproximar-se da meta do ODS (10.c) de três por cento até 2030.

Um quadro continental pode igualmente **reforçar o comércio e o comércio electrónico, aumentando a confiança nas transacções comerciais electrónicas e facilitando a realização de negócios e o comércio em todo o continente africano.** Em 2020, o comércio intra-africano representava aproximadamente 16.6% do PIB de África.[25] A ZCLCA foi lançada em 2019 para desbloquear novas oportunidades de comércio e comércio electrónico até 2030. O reconhecimento transfronteiriço da identificação digital pode ajudar a reforçar os controlos de identidade de compradores e vendedores, especialmente no caso de bens restritos vendidos electronicamente. Pode igualmente permitir assinaturas digitais para transacções 100% electrónicas, sem papel, que permitem às empresas e clientes poupar tempo e aumentar a segurança, reduzindo os riscos de fraude de identidade. Também simplifica a realização de negócios além-fronteiras, permitindo às empresas gerir digitalmente a sua interacção com o governo, por exemplo declarando impostos, participando em procedimentos de aquisição, solicitando número de IVA e aplicando autorizações.

2.2 ÂMBITO

Para atingir estes objectivos, o Quadro definirá:

- o **tipo de informação/dados** que podem ser partilhados sob a forma de um conjunto mínimo de dados para informação de identidade fundacional;[26]
- a **forma de provar quem emitiu os dados** e que se pode confiar nos mesmos;
    - criar um processo de comunicação de fontes fiáveis e autorizadas de dados de identidade em cada Estado-membro da UA;
    - determinar como verificar a autenticidade da reivindicação digital;
- normas e processos que descrevem a **forma como os dados são partilhados** pelos utilizadores e verificados por outros em ambiente fora do sistema e de forma electrónica.

O presente documento define as bases de um quadro de confiança e interoperabilidade para a identificação jurídica digital em todo o continente africano. Definirá os requisitos mínimos necessários para assegurar a interoperabilidade entre os actuais e futuros sistemas de

24 Os riscos de AML/CFT referem-se aos riscos de branqueamento de capitais e de combate ao financiamento do terrorismo. O GAFI recomenda aos governos que desenvolvam uma abordagem integrada de múltiplas partes interessadas para compreender as oportunidades e riscos relevantes para a identificação digital e desenvolver regulamentos e orientações para mitigar esses riscos.

25 CNUCED , Relatório sobre o Desenvolvimento Económico em África de 2019: Made in Africa: Regras de origem para um maior comércio intra-africano, vide: https://unctad.org/press-material/facts-figures-0

26 Embora o âmbito deste documento incida nos dados de identidade, o quadro de confiança proposto pode ser alargado pelos Estados-membros da UA para representar outras provas e realizações, tais como diplomas, qualificações profissionais, etc.

identificação digital. O Quadro não define um sistema unificado de Identificação Digital para África e não aborda os acordos comerciais e de responsabilidade entre os Estados-membros participantes.

Muitos países africanos já possuem sistemas de identificação digital bem encaminhados e alguns introduziram capacidades de autenticação digital. **O Quadro fornece requisitos comuns para a comunicação de dados e processos de identidade fundacional que seriam interoperáveis e aceites noutros Estados-membros africanos, enquanto os Estados-membros mantêm o pleno controlo e escolha para a concepção dos seus sistemas nacionais.**

O Quadro complementará e desenvolverá, em vez de duplicar, as actividades associadas ao Protocolo ao Tratado que estabelece a Comunidade Económica Africana Relativa à Livre Circulação de Pessoas, Direito de Residência e Direito de Estabelecimento, e à Conferência dos Ministros Africanos Responsáveis pelo Registo Civil e o Programa Africano para a Melhoria Acelerada da CRVS (APAI-CRVS). A implementação do Quadro deve ser estreitamente coordenada com esta e outras iniciativas relevantes, tais como explorar a migração como um caso de utilização adicional para a identificação digital no momento apropriado e assegurar que a cobertura e a qualidade dos sistemas de CRVS sejam melhoradas como um contributo importante para os sistemas de identificação digital fundacional.

2.3. QUADRO DE CONFIANÇA, PRIVACIDADE DE DADOS, INTEROPERABILIDADE E NORMAS

Os sistemas de identidade devem fomentar a confiança entre as várias partes participantes, assegurando que os direitos legais tanto dos utilizadores individuais como das agências operacionais sejam respeitados, e que a utilização ética dos sistemas de identidade seja promovida. **Para assegurar esta confiança é necessário definir um conjunto de regras que todas as partes subscrevem e observam,** um Quadro de Confiança.

Enquanto a tecnologia actua como um facilitador fundamental, o Quadro de Confiança também incide no processo e procedimento. Um quadro de confiança robusto deve definir claramente o:

O Quadro baseia-se **na interoperabilidade.** Para facilitar a interoperabilidade, uma entidade deve poder confiar noutra entidade com base não só na integridade dos processos técnicos (por exemplo, prova criptográfica, etc.), mas também na proveniência dos dados a partilhar (por exemplo, os processos para a sua recolha e para a atribuição de um determinado registo a um indivíduo).

A interoperabilidade não exige que os sistemas de identificação fundacionais sejam uniformes, apenas que certas normas comuns e abertas sejam seguidas. Ao abrigo do Quadro, cada país participante pode criar sistemas de identificação fundacionais adaptados às necessidades, tradições e legislação locais, desde que sejam seguidas certas normas que permitam a interoperabilidade. Normas Abertas estabelecem protocolos de intercâmbio universalmente compreendidos e consistentes, regimes de teste, medidas de qualidade e boas práticas relativamente à captura, armazenamento, transmissão e utilização de dados de identidade legal, bem como o formato e características das credenciais de identidade legal e protocolos de autenticação.

Ao considerar a interoperabilidade das credenciais de identidade jurídica e autenticação em todo o continente, será importante considerar normas abertas para as reivindicações de identidade, a forma como são emitidas e a forma como a confiança é comunicada entre as entidades envolvidas no Quadro de Confiança. Estas reivindicações, que constituirão a base da identificação digital legal, terão frequentemente origem em fontes autorizadas, tais como agências governamentais. Deve ser igualmente definido um mecanismo de autenticação que permita aos detentores de identificação digital legal partilhar adequadamente estas reivindicações com os prestadores de serviços, assegurando que a divulgação de dados seja - binária e que quaisquer metadados sejam ocultados, e que a privacidade e os direitos dos indivíduos sejam protegidos a todo o momento.

Este quadro definirá a **forma como a confiança pode ser estabelecida nestas reivindicações verificáveis, e como funcionam os elementos e normas de governação dos dados.** A implementação técnica da solução pode ser impulsionada pelo mercado que será capaz de alavancar o quadro de confiança para desenvolver soluções inovadoras de identificação digital fundacional. O Quadro coloca a privacidade, auditoria e protecção de dados no centro e estabelece um procedimento transparente a ser aplicável a todos os envolvidos. As Partes confiantes sobre a forma como os dados são solicitados, recolhidos, transmitidos e armazenados e segue normas bem aceites sobre o procedimento de partilha de informações/dados. A importância da atribuição de símbolos na redução das oportunidades de recolha de dados, clonagem e fraude, através da apresentação ao titular da identificação, da funcionalidade de emissão de identificações virtuais, a fim de proteger as próprias identificações reais, é um aspecto adicional que será aprofundado para reforçar a privacidade dos dados a nível nacional/continental.

3. O QUADRO

O Quadro de Interoperabilidade da UA para a Identificação Digital propõe definir a nível continental uma abordagem harmonizada para a partilha de reivindicações de identificação digital[27] emitidas por autoridades de confiança com fornecedores de serviços, a fim de provar a sua identidade legal num ambiente virtual e não virtual. Consistirá em acordar numa **norma comum para representar as provas existentes de identidade jurídica emitidas pelos Estados-membros da UA num formato digital.**[28] A autenticidade de tais credenciais[29] seria capaz de ser verificada a fim de garantir um alto nível de confiança e segurança.

Não há restrições impostas aos sistemas nacionais de identificação fundacional como funcionam ou que tipos de credenciais utilizam para autenticar indivíduos; cada país é soberano a este respeito. A intenção do quadro é criar condições para a interoperabilidade à escala continental com base nos sistemas existentes onde eles existem e em vez de restringir a sua utilização alargando o seu alcance.

As credenciais de identidade jurídica digital interoperáveis (IDC-ID) emitidas em conformidade com o Quadro da UA assumirão a forma de uma reivindicação verificável que será complementar aos sistemas nacionais de identificação fundacional existentes e aos projectos de cooperação regional, sem substituir os sistemas nacionais de identificação digital dos Estados-membros da UA. Os Estados-membros da UA permanecem livres para seleccionar a forma como querem emitir esta credencial digital. Pode ser armazenado num formato puramente digital numa aplicação baseada em telefones inteligentes, um servidor baseado em nuvem, um cartão inteligente ou uma ligação à representação digital pode ser estabelecida usando um código de barras de uma ou duas dimensões num documento em papel (impresso em papel, cartão plástico).

O Quadro será baseado no desenvolvimento de sistemas de identificação interoperáveis, inclusivos e de confiança, uma vez que estes constituem a espinha dorsal de fontes de dados fiáveis sobre a identidade legal das pessoas, permitindo assim ao IDC-ID alcançar níveis mais elevados de garantia. Os Estados-membros da UA são, portanto, incentivados a reforçar os seus sistemas de identificação, bem como os *Princípios de Identificação para o Desenvolvimento Sustentável.* Podem ser consideradas soluções alternativas para obter uma IDC-ID para pessoas que estão actualmente excluídas de um sistema de identificação.

As normas para uma identificação digital legal interoperável poderiam ser utilizadas a nível nacional ou apoiar casos de utilização transfronteiriça. Por exemplo, a norma poderia ser adoptada para:

- representam dados de identificação digital fundacionais a nível nacional sobre credenciais de identidade digital recentemente emitidas ou actualizadas; ou,
- representam dados de identificação digital fundacionais a nível continental ou das CER;
- emitidos separadamente em complemento dos sistemas de identificação digital preexistentes.

27 As reivindicações são uma colecção de atributos sobre uma pessoa em causa: por exemplo, nome de família, dados de nascimento

28 O quadro actual centra-se na definição de reivindicações verificáveis para provar dados de identificação, mas poderia ser utilizado para partilhar reivindicações verificáveis sobre realizações académicas, qualificações profissionais, etc...

29 Uma credencial é composta por uma reivindicação de identidade, metadados sobre o emissor e uma prova de autenticidade que é normalmente uma assinatura digital.

O elemento interoperável, confiança e inclusão definido como parte deste quadro constitui uma plataforma de lançamento para um quadro continental mais abrangente e uma infra-estrutura para a identificação e autenticação digital no continente.

3.1. PRINCÍPIOS ORIENTADORES

Os seguintes princípios orientarão a implementação da interoperabilidade transfronteiriça do quadro:

1. Transparência na governação e no funcionamento
2. Facilmente acessível, financeiramente e operacionalmente sustentável e amplamente utilizável,
3. Promover o respeito e defender os direitos humanos e a liberdade[30]
4. Garanta a integridade técnica, incluindo identidade exclusiva, segura, escalável e precisa
5. Garantir a soberania dos Estados-membros. garantir a soberania dos dados, nomeadamente os dados de identificação digital, pertence e permanece sob o controlo de África:
6. Ser interoperável entre os Estados-membros da UA
7. Utilizar normas abertas[31] e evitar o bloqueio de fornecedores e tecnologias
8. Protegem a privacidade e permitem que as pessoas controlem os seus dados pessoais, incluindo a proporcionalidade dos dados através da concepção do sistema
9. Salvaguardar a privacidade, segurança e direitos dos dados através de um quadro jurídico e regulamentar abrangente.
10. Estabelecer mandatos institucionais claros e responsabilização

Considerando que o Quadro depende de fontes autorizadas, tais como sistemas de identificação legal, a qualidade e cobertura destes sistemas, tem portanto um impacto na sua implementação. A exclusão destes sistemas e outros desafios como a fraca segurança, por exemplo, conduzirá ao mesmo em termos da capacidade de emitir e utilizar correctamente as credenciais.

Por conseguinte, os Estados-membros da UA devem cumprir as suas obrigações de garantir que todas as pessoas presentes no seu território tenham acesso à identificação legal, em conformidade com a Convenção sobre os Direitos da Criança e outros instrumentos jurídicos internacionais e regionais. Além disso, são também fortemente incentivados a aderir às normas

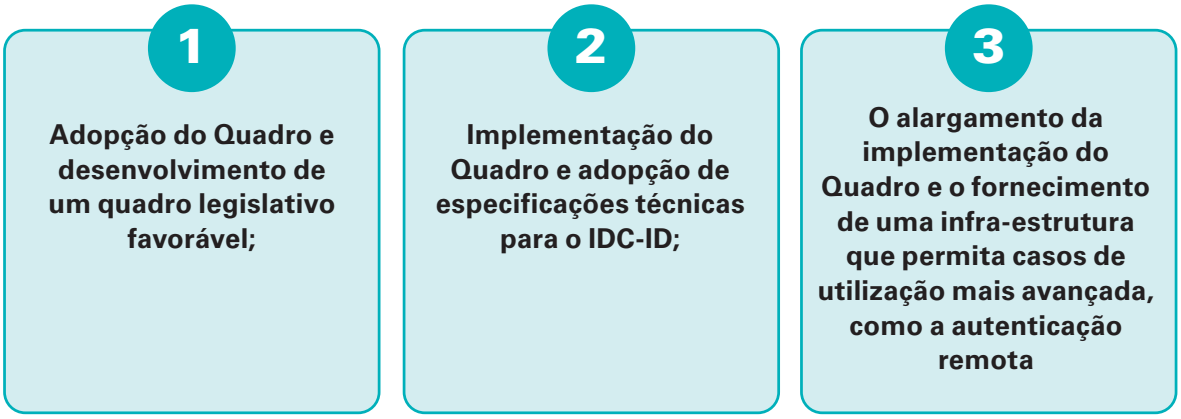
30 Segundo a Carta Africana (Banjul) sobre os Direitos Humanos e dos Povos (Adoptada a 27 de Junho de 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrou em vigor a 21 de Outubro de 1986)

31 Normas Abertas são normas disponibilizadas ao público em geral e são desenvolvidas (ou aprovadas) e mantidas através de um processo de colaboração e de consenso. As "Normas Abertas" facilitam a interoperabilidade e o intercâmbio de dados entre diferentes produtos ou serviços e destinam-se a uma adopção generalizada (adoptadas a partir da UIT-T).

e princípios internacionais relevantes existentes[32,33] e a assegurar que as fontes autorizadas, e especialmente os seus sistemas de identificação legal, sejam inclusivas, protectoras dos dados e direitos das pessoas, e concebidas para apoiar a integração económica e social continental.

3.2. O MODELO

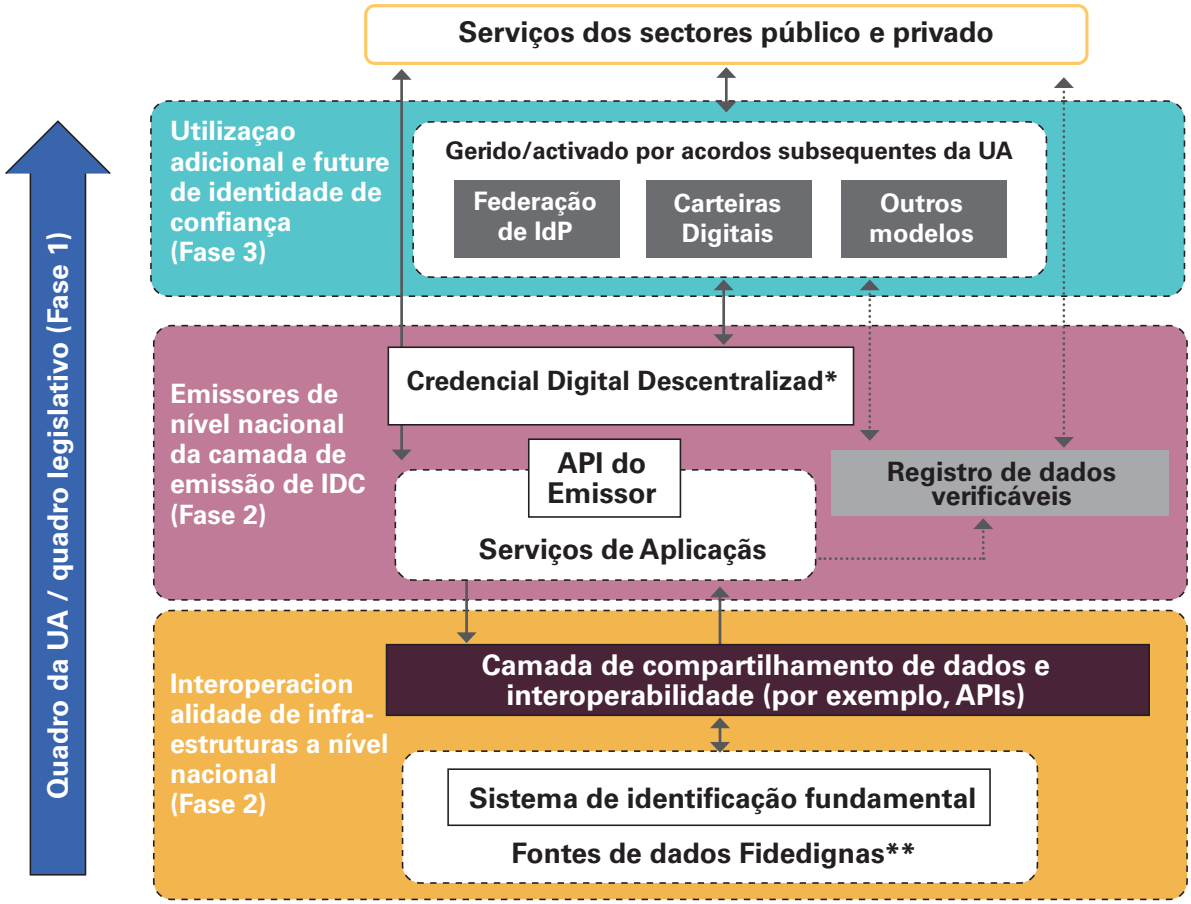
O Quadro irá propor uma implementação em três fases:



32 Isto inclui, entre outros aspectos, a convenção de Budapeste sobre a criminalidade cibernética, IEC, ISO, Princípios e recomendações da UIT-T da ONU para sistemas de estatísticas vitais, normas internacionais sobre protecção de dados (tais como o Regulamento Geral Europeu para a Protecção de Dados e a Convenção 108+ do Conselho da Europa), normas globais e regionais e quadros de confiança para a identificação.

33 Tais como os Dez Princípios de Identificação para o Desenvolvimento Sustentável, que foram endossados por 30 organizações internacionais e regionais, incluindo instituições africanas como a UNECA, o BAD e a África Inteligente, bem como adotados por vários países africanos, ver: https://id4d.worldbank.org/principles, e os Princípios sobre Desenvolvimento Digital, que foram endossados por mais de 200 organizações, ver: https://digitalprinciples.org/.

FIGURA 1 – ABORDAGEM DE IMPLEMENTAÇÃO FASEADA DO QUADRO



** Os pormenores de implementação da fase 2 serão discutidos mais aprofundadamente com os Estados-membros da UA*

*** Os Estados-membros decidirão que fontes de dados fiáveis implicam os seus sistemas de Identificação Fundacional*

O IDC-ID deve assegurar que a **autoridade emissora não tenha conhecimento dos serviços a que os indivíduos têm acesso com a sua identificação digital,** mas que a autenticidade das credenciais de identidade possa ser verificada. Isto proporciona salvaguardas em termos de protecção de dados e privacidade e mais controlo para o indivíduo sobre a forma como os seus dados são utilizados.

A camada de infra-estrutura permitirá casos de utilização mais avançada e consistirá em credenciais de identidade vinculativas emitidas no formato IDC-ID para os indivíduos reais. Existem várias opções técnicas à disposição dos Estados-membros da UA para implementar esta plataforma, que poderia ser composta por uma federação de fornecedores de identidade que forneçam mecanismos de autenticação aos detentores do IDC-ID ou o desenvolvimento de soluções de carteiras de identificação digital ou quaisquer outros modelos que permitam a interoperabilidade. Cada uma destas implementações pode oferecer **uma abordagem de minimização de dados e serviços de divulgação selectiva** para casos de uso específico, por exemplo, partilhar apenas os pontos de dados relevantes de um cartão de identificação e relatório de crédito para obter um empréstimo, procurar benefícios sociais ou de saúde, obter pensão, candidatar-se a bolsas de estudo ou tornar anónimo o conjunto mínimo de dados do IDC-ID (nome, data de nascimento) numa prova de maioridade (+18 anos ou +21 anos ou uma resposta de sim/não).

3.2.1. COMPONENTES DA ARQUITECTURA

As fontes de dados fiáveis devem cumprir as normas estabelecidas pelo Quadro no que se refere à qualidade e integridade dos dados. Em muitos casos, isto seria cumprido por um sistema de identificação fundacional (cujas fontes de dados fiáveis serão decididas pelos Estados-membros) que pode fornecer uma prova de identidade jurídica.

A Figura 1 mostra a extensão do acesso aos sistemas nacionais existentes e fontes de dados de confiança através de uma camada de Partilha de Dados e Interoperabilidade baseada em normas e protocolos que permitem a emissão de IDC de confiança. Fornecedores de serviços para verificar e recuperar dados de identidade legal ao criar credenciais de identificação digital fundacionais.

A camada de emissão da IDC representa a emissão padronizada de Credenciais de IDC com base num sistema de identificação de nível fundacional/nacional fonte de dados de confiança. Cada Emissor de Credenciais (pelo menos um por cada Estado-membro participante) terá uma série de funções essenciais (não limitadas às seguintes):

- Uma API de Emissor que permite às carteiras e outros sistemas solicitar e recuperar credenciais
- Um Registo de Dados Verificável que permite a verificação dos identificadores e a verificação da revogação das credenciais.
- Gestão de Criptografia Importante
- Visibilidade e Auditoria da utilização de credenciais para o Titular de uma credencial da IDC
- Fornecer Metadados de Credenciais juntamente com cada credencial emitida para descrever a qualidade, proveniência e nível de confiança associado à credencial emitida

3.2.2. NÍVEL NACIONAL E REQUISITOS DE INTEROPERABILIDADE

Não há nenhum requisito para que os sistemas de identificação existentes a nível nacional sejam reequipados para alcançar a interoperabilidade a nível continental. Em vez disso, serão adoptadas normas para a interoperabilidade dos dados, interoperabilidade técnica através de APIs e protocolos, e representação técnica das credenciais. A emissão de credenciais, e a sua criação, é logicamente separada dos sistemas nacionais existentes, mas estaria sob o controlo de agências nacionalmente responsáveis.

A confiança técnica, sustentada por criptografia avançada, pode não exigir uma PKI continental ou outra infra-estrutura super-nacional, mas, em vez disso, resultaria da preferência e/ou capacidade dos Estados-membros da UA utilizando quer a PKI nacional (quando utilizada) quer alternativas. Cada Estado-membro da UA continuará a exercer a soberania nacional na concepção dos sistemas de identificação nacionais, incluindo a forma como esses sistemas funcionam em conjunto com o quadro da UA.

3.2.3. NORMAS PARA A PARTICIPAÇÃO DE FONTES DE DADOS FIÁVEIS

Serão estabelecidas normas no âmbito do Quadro no que se refere à qualidade, segurança, fiabilidade, e nível mínimo de garantia associado a cada fonte de dados de confiança. Os sistemas dos Estados-membros devem fornecer provas de que alcançaram os requisitos mínimos de participação antes de poderem participar no Quadro e emitir credenciais conformes à IDC. A natureza destas normas será determinada por acordo dos Estados-membros da UA.

3.3. PROCESSO DE CONFIANÇA – O QUADRO FIDUCIÁRIO

O quadro de confiança deve descrever regras claras para a participação de entidades (por exemplo, emitentes, titulares e verificadores de identidade), o funcionamento do quadro, e os requisitos técnicos para a interoperabilidade das credenciais de confiança.

Isto permitirá a todas as entidades confiar nas credenciais partilhadas pelos titulares de identidade com base no acordo fiduciário estabelecido pela autoridade emissora (para a credencial) e nos processos que cada entidade concordou em aderir ao abrigo do quadro fiduciário.

Prevê-se que as seguintes secções fundamentais sejam redigidas pelos Estados-membros como parte do quadro de confiança

3.3.1. PAPÉIS E RESPONSABILIDADES

Uma definição clara de cada entidade (por exemplo, um emissor de credenciais), e as responsabilidades que tem para manter a confiança, tais como a gestão segura e protegida de dados e serviços, e a comunicação de incidentes.

Os papéis fundamentais que se espera venham a ser incluídos no quadro de confiança seriam:

- As **autoridades de confiança** são fontes fidedignas de dados para a prova legal da identidade, tal como endossada pelos Estados-membros da UA.
- Os **emissores** são entidades responsáveis pela emissão da prova de identidade legal no formato digital normalizado ao abrigo do Quadro de Referência para o titular. As autoridades fidedignas podem emitir elas próprias as credenciais ou mandatar outra entidade com um conjunto de competências mais adequado (por exemplo, agência TIC, sector privado).
- O **titular** do IDC-ID é o indivíduo que possui uma ou mais credenciais digitais. O titular pode ser mas nem sempre o sujeito dos atributos de identificação partilhados através de IDC.
- O **verificador** é uma parte de confiança (por exemplo, fornecedor de serviços públicos ou privados) que pretende verificar a reivindicação de identidade de um determinado sujeito.
- Os **fornecedores de identidade, fornecedores de credenciais e fornecedores de carteira digital** podem contribuir ainda mais para o ecossistema, fornecendo um autenticador para vincular a identidade do titular às credenciais e, portanto, permitir casos de utilização mais avançada que exijam autenticação remota.

- Poderá ser necessário um **organismo de controlo independente** a ser criado pelos Estados-membros para assegurar que as entidades participantes continuem a cumprir as regras estabelecidas pelo quadro fiduciário e definir as ferramentas e tecnologias mínimas necessárias para o cumprimento. O Organismo de Supervisão deve também ser incumbido da tarefa de aumentar a sensibilização para as competências de resiliência cibernética em todo o continente, a fim de assegurar a sustentabilidade do quadro.

3.3.2. REGRAS DE PARTICIPAÇÃO

As regras de participação podem incluir requisitos mínimos legais, operacionais, ou organizacionais exigidos a uma entidade de confiança autorizada que preste um serviço no âmbito do quadro fiduciário. Por exemplo, um Emissor pode ser obrigado a ter um acordo oficial para operar (de uma fonte autorizada / agência governamental).

Os serviços que aceitam o IDC-ID podem ser solicitados a confirmar a sua conformidade com os requisitos básicos de protecção de dados, privacidade e reparação (para titulares de identidade).

Pode também ser necessário um memorando de entendimento para assegurar que todas as entidades operacionais concordam com os termos do quadro de confiança.

3.3.3. GOVERNAÇÃO

Os mecanismos de governação a serem aprovados pelos Estados-membros da UA deverão estabelecer e manter as regras do quadro de confiança, aprovar alterações aos requisitos de interoperabilidade, e delegar a responsabilidade pela elaboração/desenvolvimento de alterações ao quadro nos subgrupos de governação, conforme necessário.

Poderá ser necessário um organismo de controlo independente a ser criado pelos Estados-membros da UA para assegurar que as entidades participantes continuem a cumprir as regras estabelecidas pelo quadro fiduciário. Este organismo deverá igualmente ser responsável por assegurar que todas as partes satisfaçam o cumprimento formal das normas e, caso se desviem, sejam auditadas ou levadas a prestar contas, conforme considerado necessário, por exemplo, em caso de violação de dados.

A protecção dos indivíduos deve ser primordial. O Organismo de Controlo deve ter poderes para receber e agir em caso de queixas dos Titulares da IDC-ID afectados por más práticas, violação de dados, fraude de identidade, ou outros incidentes relacionados com a identidade digital. Deve igualmente ser o ponto focal dos mecanismos de reparação, mesmo que se trate apenas de um papel de coordenação e deve actuar como um defensor dos indivíduos e dos seus direitos.

3.3.4. REQUISITOS DE INTEROPERABILIDADE

3.3.4.1. NÍVEIS DE GARANTIA

Um meio de comunicar o nível de confiança de uma credencial apresentada por um Titular a um Verificador. O Quadro deve definir as condições pelas quais cada nível pode ser alcançado com base na verificação da identidade por uma fonte autorizada, o processo de emissão, e os meios de detenção e apresentação de uma credencial.

3.3.4.2. CONJUNTO DE DADOS MÍNIMOS

A quantidade mínima de dados relativos à identidade de um Titular, tal como consta de uma credencial de identidade, deve ser adequada para a identificação do indivíduo na maioria das transacções comuns, respeitando simultaneamente a necessidade de minimização de dados. Os atributos contidos no conjunto mínimo de dados podem ser fornecidos por diferentes entidades de confiança.

O órgão dirigente tem a liberdade de definir como os créditos adicionais (conjuntos de dados) podem ser incluídos opcionalmente no quadro fiduciário. Qualquer emissão de credenciais correspondentes deve estar sujeita às mesmas condições e regras que os emissores de credenciais de identidade fundacional. Requisitos Técnicos.

3.3.4.3. SEGURANÇA

Devem ser definidos requisitos de segurança de base para cada entidade que presta um serviço como parte da infra-estrutura de identidade.

3.3.4.4. PROVA CRIPTOGRÁFICA

As credenciais serão verificadas através da inclusão de uma assinatura digital criada pela autoridade emissora. A verificação da validade da assinatura actua como prova criptográfica de que o crédito feito pelo Titular que apresenta a credencial pode ser confiável. A fim de verificar uma chave pública de assinatura digital será necessária. A chave pública pode ser fornecida através de um método descentralizado ou centralizado a ser determinado como parte do quadro de confiança e dos seus requisitos técnicos.

3.3.4.5. FORMATO DE CREDENCIAL

As especificações técnicas para a criação e transmissão de credenciais devem ser definidas com base nas normas existentes, tais como as Credenciais Verificáveis W3C, quando aplicável.

- A Credencial Digital Interoperável para Identificação (IDC-ID) é um conjunto de reivindicações de identidade legal (por exemplo, atributos) e relação feita por um emissor que pode ser verificada criptograficamente. Mais especificamente, inclui:
    - Metadados de credenciais sobre o tipo de credencial emitida, data de emissão, nome do emitente;
    - Informação sobre o objecto da reivindicação e a verdadeira reivindicação de identidade jurídica (por exemplo, data de nascimento).
    - Prova de autenticidade que é normalmente uma assinatura digital.

O titular de IDC-ID é capaz de gerar apresentações verificáveis de um ou mais IDC-ID da forma que a autenticidade da reclamação ainda pode ser verificada (por exemplo, divulgação selectiva).

3.4. OPÇÕES DE AUTENTICAÇÃO EM POTENCIAL

Várias abordagens arquitectónicas podem ser adoptadas para permitir que o titular de IDC-ID seja autenticado a um determinado nível de garantia. Todas as opções seguintes podem coexistir e ser implementadas a diferentes níveis de cooperação (por exemplo, entre actores sectoriais específicos ou a nível das CER).

Dependendo da disponibilidade de outras tecnologias com práticas de implementação comprovadas, poderão ser exploradas opções adicionais.

3.4.1. OPÇÃO 1 - CARTEIRAS DIGITAIS PESSOAIS

Esta opção consiste em fornecer a indivíduos e empresas uma carteira digital pessoal contendo uma prova verificável de atributos de identidade legal que pode ser utilizada para provar a sua identidade legal ou partilhar factos específicos com um prestador de serviços. Esta opção de arquitectura refere-se aos casos de utilização de Credenciais Verificáveis do W3C.[34]

FIGURA 2 – VISÃO GERAL DA OPÇÃO 1 - CARTEIRAS DIGITAIS PESSOAIS

PROCESSO DE AUTENTICAÇÃO

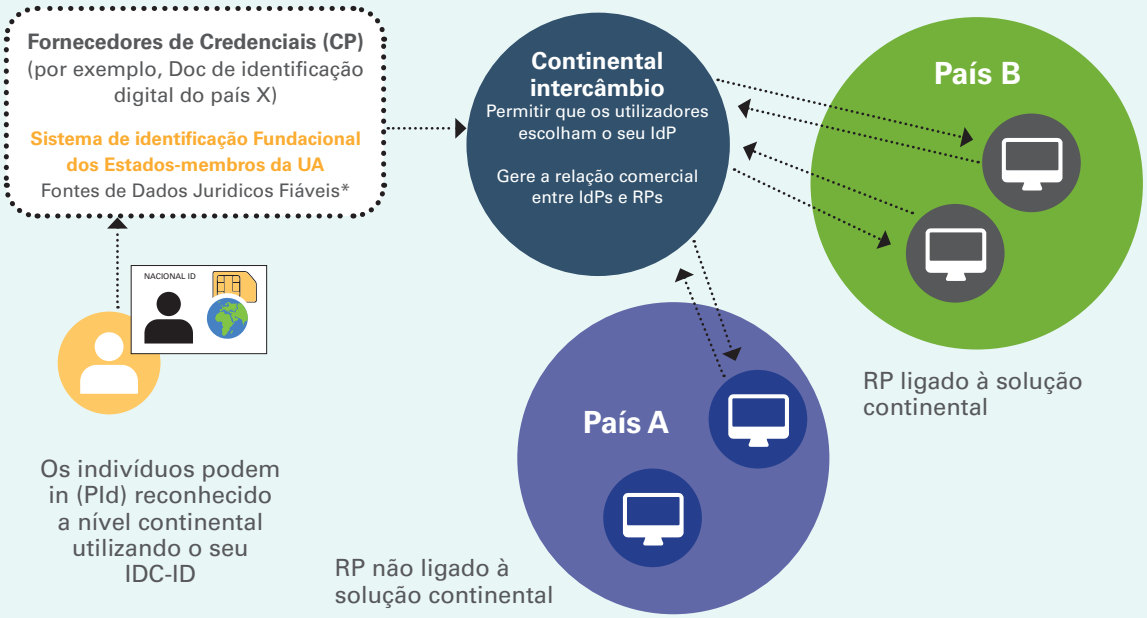
1. O indivíduo selecciona um fornecedor de carteira de identidade para guardar o seu IDC e é necessário um processo de bordo.
2. O indivíduo recebe um IDC verificável (por exemplo, identificação, prova de morada) dos emissores autorizados e guarda-o numa **carteira digital**
3. Ao mesmo tempo da emissão, a autoridade regista uma impressão digital do **crédito numa infra-estrutura de chave pública descentralizada tendo em conta a privacidade dos cidadãos.**
4. Os indivíduos podem apresentar a um prestador de serviços (por exemplo, um seguro) uma reclamação, tal como uma **prova de morada** utilizando a sua carteira (por código QR, Bluetooth, NFC)
5. O prestador de serviços pode verificar na infra-estrutura de chave pública descentralizada que o crédito é autêntico e foi emitido por uma autoridade reconhecida.

34 W3C, Casos de Utilização de Credenciais verificáveis, vide: https://www.w3.org/TR/vc-use-cases/

3.4.2. OPÇÃO 2 - FEDERAÇÃO CONTINENTAL DE IDENTIFICAÇÃO DIGITAL DE FUNDAÇÕES

Segundo este modelo, cada residente africano poderia embarcar com um fornecedor de credenciais fundacionais a nível continental à sua escolha.

FIGURA 3 – VISÃO GERAL DA OPÇÃO 2 – FEDERAÇÃO CONTINENTAL DE IDENTIFICAÇÃO DIGITAL



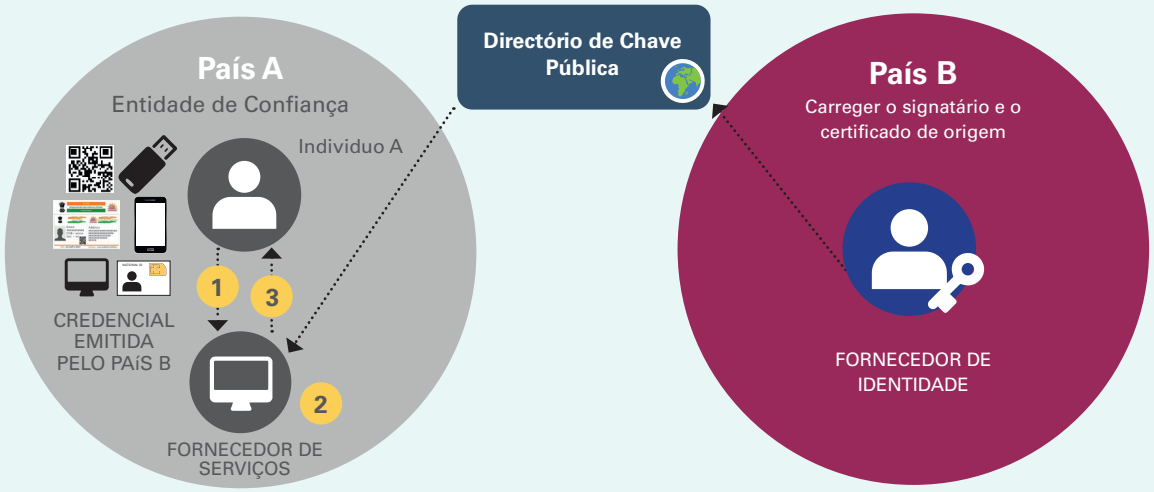
PROCESSO DE AUTENTICAÇÃO

1. **É estabelecida uma federação continental de fornecedores de credenciais de identificação fundacional:** operadores de telecomunicações, bancos, governos, etc... podem fornecer serviços de autenticação.
2. É criada uma **troca continental**, fornecendo um ponto de contacto único para todos os fornecedores de credenciais participantes e partes confiantes que queiram autenticar indivíduos.
3. Os indivíduos podem usar o seu IDC para a **bordo** do fornecedor de credenciais da sua escolha. O CP da identificação fundacional pode verificar a autenticidade do IDC.
4. Após verificação bem-sucedida, o CP emite um meio de **autenticação** para o indivíduo.
5. O indivíduo pode usar o seu meio de autenticação para aceder electronicamente **e pessoalmente aos serviços** que estão ligados ao intercâmbio continental.

3.4.3. OPÇÃO 3 - CREDENCIAIS ASSINADAS DIGITALMENTE

Este modelo permite a autenticação através da verificação dos dados de identidade legal assinados digitalmente numa credencial com uma chave pública, bem como um meio adicional para partilhar a fotografia do titular.

FIGURA 4 – VISÃO GERAL DA OPÇÃO 3 - CREDENCIAIS ASSINADAS DIGITALMENTE



PROCESSO DE AUTENTICAÇÃO

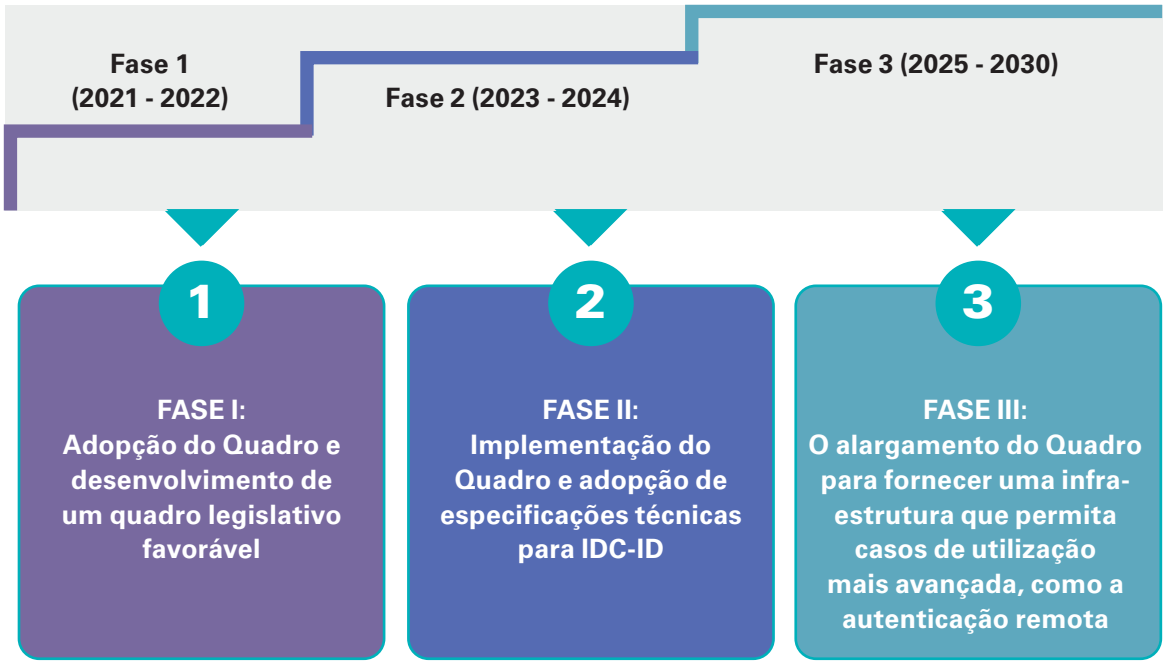
1. Os países acordam numa **norma (por exemplo, código QR)** e fontes autorizadas assinam criptograficamente as **credenciais** (através de uma senha privada)
2. Fontes autorizadas partilham a sua chave pública num **Directório de Chaves Públicas** (PKD) cuja governação será aprovada pelos Estados-membros da UA e gerida a nível continental.
3. Os países criam um serviço separado que permite partilhar uma cópia da imagem do detentor de IDC-ID acessível através de API seguro, a fim de autenticar o detentor. Para trabalhar desconectado, é também possível que um grupo de países (por exemplo, CER) chegue a acordo sobre a emissão de uma credencial física contendo uma fotografia do titular.[35]
4. As fontes autorizadas dos países emitem **formulários padronizados de IDC** a indivíduos
5. É criado um **software de verificação** (app ou website) para permitir aos prestadores de serviços verificar a autenticidade e integridade da assinatura no IDC.
6. Os indivíduos podem utilizar o seu IDC para obter a sua identidade jurídica digitalmente verificada por entidades públicas ou privadas de confiança no seu país ou no estrangeiro e **aceder aos serviços**.
7. Cada Estado-membro deverá manter em armazenamento seguro tais como Módulos de Segurança de Hardware (HSMs), as chaves privadas, certificados de raiz e algoritmos de *hashing* a serem utilizados para encriptação e verificação de integridade

35 A emissão de credenciais físicas tem um custo adicional. Os Estados-membros participantes teriam de continuar a discutir o financiamento de tal solução para não criar barreiras ao acesso.

4. ROTEIRO DE ALTO NÍVEL PARA IMPLE MENTAÇÃO

Para acelerar o caminho para alcançar os ambiciosos objectivos deste Quadro, os Estados-membros da UA devem aumentar a sua colaboração para aperfeiçoar os pormenores do quadro técnico e de referência, normas e processos comuns.

A proposta é de dividir a implementação do Quadro em três fases, como mostra o diagrama abaixo:



Para cada fase, serão planeadas oportunidades de consulta com os Estados-membros da UA, a sociedade civil e as partes interessadas do ecossistema de identidade, a fim de assegurar que o Quadro e a sua implementação se mantenham alinhados com as necessidades dos indivíduos e dos contextos locais. A documentação principal será publicada e proporcionará um período de tempo adequado para contribuições.

4.1. FASE 1: ADOPÇÃO DO QUADRO E AMBIENTE FAVORÁVEL

Submissão do projecto de Quadro à 4ª sessão ordinária do CTE de Comunicação e TIC para adopção e a aprovação pelos órgãos deliberativos.

Na sequência da aprovação do presente documento, os pormenores do Quadro de Confiança serão especificados com mais detalhe e as seguintes actividades serão realizadas, nomeadamente:

- sensibilização;
- estudo de viabilidade sobre o panorama actual do sistema de identificação digital em África;
- estabelecimento de um quadro de consulta para os intervenientes no ecossistema digital destinado a salvaguardar os interesses de cada interveniente;
- desenvolvimento de instrumentos jurídicos e regulamentares harmonizados;
- definição das regras de participação;
- criação dos mecanismos de governação e fórum para partilhar as melhores práticas ao longo de todo o processo de implementação;
- definição de disposições jurídicas que terão de ser integradas nos quadros jurídicos nacionais dos Estados-membros da UA, a fim de implementar o Quadro, incluindo salvaguardas adequadas em matéria de segurança cibernética e protecção de dados;
- ratificação da Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais;
- a adopção do quadro político continental em matéria de dados;
- nomeação de grupos de peritos pelos Estados-membros da UA para definir a interoperabilidade e os requisitos técnicos;
- criação de estruturas institucionais independentes a nível nacional (autoridades de protecção de dados; responsável pelo controlo das autoridades de certificação; e equipas de resposta a incidentes informáticos (CIRTs) e reforço da cooperação entre instituições nacionais;
- desenvolvimento de iniciativas de desenvolvimento de capacidades;
- apoio à implantação de infra-estruturas digitais, incluindo centros de dados a nível nacional, regional/continental, que sejam necessários para apoiar e sustentar a operacionalização dos sistemas de identificação digital;
- mobilização de recursos.

Para garantir o sucesso do Quadro, será definida uma série de **casos de utilização** que representam as maiores oportunidades para o continente. Um grupo de Estados-membros da UA pode ainda colaborar para testar e pilotar casos de utilização específica, juntamente com outras partes interessadas, conforme necessário.

Deve ser realizada uma avaliação dos **principais custos e benefícios** do quadro proposto e das opções de autenticação subsequente, a fim de dar maior visibilidade às necessidades de financiamento para informar os Estados-membros da UA sobre a tomada de decisões. Neste momento, espera-se que o cumprimento de uma norma harmonizada para representar informação de identidade gere custos limitados para os Estados-membros da UA, uma vez que poderia ser integrada como requisito técnico nos projectos de digitalização existentes dos seus sistemas de identificação fundacionais. Contudo, espera-se que o estabelecimento da infra-estrutura de autenticação gere custos adicionais e, dependendo dos tipos de intervenientes envolvidos, exige a definição de modelos de negócio. Para esta fase, terá de ser realizada uma avaliação de impacto detalhada a fim de assegurar que as opções de autenticação propostas se mantenham inclusivas.

Paralelamente, os Estados-membros da UA comprometem-se a:

- elaborar e implementar quadros legais e regulamentares harmonizados que permitam criar confiança nos sistemas de identificação digital fundacional;
- Elaborar legislação harmonizada sobre dados pessoais e regulamentação de melhores práticas de protecção de dados para facilitar a harmonização entre países e para que os cidadãos possam ter mais poder, mantendo ao mesmo tempo a soberania dos dados;
- desenvolver infra-estruturas digitais, incluindo infra-estruturas de dados (centros de dados nacionais), que constituem a base para a implementação do sistema de identificação digital;
- ratificar a Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais (se ainda não tiver sido feita) e acelerar a sua entrada em vigor e o trabalho para acelerar a criação de autoridades de protecção de dados para a supervisão nos países participantes;
- elaborar a estratégia nacional de segurança cibernética e constituir equipas de resposta a incidentes informáticos (CIRT) para mitigar os riscos e ameaças relacionados com ataques cibernéticos, roubo de dados e tratamento incorrecto de informações sensíveis;
- adoptar o quadro da Política Continental de Dados da UA. Estes devem capacitar os indivíduos e proteger a privacidade electrónica como um direito fundamental (incluir a escolha e controlo do utilizador, consentimento informado/mensurável, soberania/propriedade de dados, etc.);
- proceder ao lançamento e/ou aumento de esforços para reforçar os sistemas de identificação fundacional, para assegurar que estes sejam inclusivos e de confiança, em conformidade com normas e iniciativas relevantes, tais como o Programa Africano de Melhoria Acelerada dos Sistemas de Registo Civil e Estatísticas Vitais (APAI-CRVS) e os *Princípios de Identificação para o Desenvolvimento Sustentável.*

Estas fases serão finalizadas com a adopção da versão completa do Quadro pelos Estados-membros da UA.

4.2. FASE 2: IMPLEMENTAÇÃO DO QUADRO E ADOPÇÃO DE ESPECIFICAÇÕES TÉCNICAS PARA IDC-ID

A segunda fase consistirá em estabelecer o quadro de confiança e os mecanismos de governação e cooperação e fornecer a **especificação técnica** para a introdução do IDC-ID que incluirá, entre outras:

- desenvolvimento de padrões mínimos e normas para a interoperabilidade;
- atribuição de perfis para o conjunto mínimo de dados (formatos de dados) e metadados associados;
- Formato de apresentação (por exemplo, códigos de barras 2d, credenciais verificáveis W3C);
- nível de garantia (como ponto de referência para a interoperabilidade);
- elementos criptográficos para assinatura e encriptação de dados;
- protocolos de verificação para casos de utilização online e offline.

Um grupo de EM da UA pode desenvolver uma **amostra de implementação** (aplicação ou website) para verificação básica do IDC-ID para testar a interoperabilidade da credencial e já apoiar provas verificáveis da identidade legal. A implementação implementará a privacidade e a segurança por concepção.

Pode ser considerada a definição de **soluções alternativas para obter um IDC-ID** para pessoas que estão actualmente excluídas de qualquer sistema de ID fundacional.

Será realizado um **mapeamento de outras iniciativas em curso da União Africana** que poderão basear-se no quadro (por exemplo, Quadro de Qualificações Africano Continental).

A Fase 2 será concluída com a definição de um plano de acção claro para a definição da infra-estrutura de autenticação como parte da Fase 3.

4.3. FASE 3: DESENVOLVIMENTO DA INFRA-ESTRUTURA PARA PERMITIR A AUTENTICAÇÃO À DISTÂNCIA

A Fase 3 começará a **implementar o quadro fiduciário** definido como parte da Fase 2:

Nesta fase, a camada que representa a emissão do IDC-ID será aumentada e expandida para implementar uma infra-estrutura que permita casos de utilização mais avançada, como a autenticação remota. Esta camada de autenticação permitirá aos indivíduos provar a sua identidade digitalmente, exercendo o controlo de um ou mais factores de autenticação (por exemplo, um código biométrico ou PIN) ligados à sua identidade legal previamente verificada, o IDC-ID. Diversas opções técnicas estão disponíveis aos Estados-membros da UA para implementar esta camada, por exemplo, uma federação de fornecedores de identidade que forneça mecanismos de autenticação aos titulares do IDC-ID, ou o desenvolvimento de soluções de carteira de identidade digital ou quaisquer outros modelos que permitam a interoperabilidade. Cada uma destas implementações pode oferecer uma abordagem de minimização de dados e serviços de divulgação selectiva para casos de uso específico, por exemplo, partilhando apenas os pontos de dados relevantes de um cartão de identificação e relatório de crédito para obter um empréstimo, procurar benefícios sociais ou de saúde, obter pensão, quando a autenticação é legalmente exigida ou anonimizar o conjunto mínimo de dados da IDC-ID (por exemplo, nome, data de nascimento) numa prova de maioridade (+18y ou +21y ou uma resposta de sim/não).

Os Estados-membros da União Africana poderão também procurar mais discussão e acordo sobre a forma de estabelecer esta infra-estrutura da camada de autenticação e estabelecer parcerias com as CER e outras iniciativas continentais que já estão a investigar a introdução de soluções interoperáveis de ID digital para aceder aos serviços à distância. De facto, os Estados Membros e as organizações poderão tirar partido da representação comum baseada em padrões de informação de identidade num formato digital seguro e de confiança e construir serviços adicionais sobre a mesma.

Os Estados-membros da UA continuarão a colaborar para reforçar o quadro de confiança e os mecanismos de governação e cooperação, na sequência do acordo sobre as infra-estruturas adicionais que se seguirão:

- **Coordenação com outras iniciativas** destinadas a estabelecer a interoperabilidade a nível continental (por exemplo, SATA e RECs);

- **Acordo sobre a melhor opção arquitectónica** (por exemplo, federação, carteiras digitais, etc.) para desenvolver a função de autenticação remota que se basearia nas Credenciais Digitais Interoperáveis (IDC-ID).

A Fase 3 será concluída com um plano de acção claro sobre a implementação da camada de autenticação de acordo com a opção arquitectónica a ser acordada entre os Estados-membros e organizações da UA.

5. SUPOSIÇÕES DE ALTO NÍVEL, DESAFIOS E RISCOS

5.1. PRESSUPOSTOS

Os Estados-membros adoptarão o quadro, colaborarão, comprometer-se-ão a implementar e a levar a cabo as reformas legais e regulamentares necessárias e exigidas.

5.2. DESAFIOS GERAIS E PROPOSTAS DE MITIGAÇÃO DE ALTO NÍVEL

O quadro abaixo resume os desafios gerais e os mecanismos de mitigação propostos.

#	Desafios	Propostas de Mitigações
1	Exclusão, segurança fraca e erosão da protecção de dados pessoais	Aplicação dos Princípios definidos no quadro (3.1) e reforço dos quadros jurídicos e infra-estruturas de segurança e protecção de dados nos Estados-membros da UA.
2	Relutância dos Estados-membros da UA em adoptar e implementar o quadro	Sensibilizar para os benefícios do Quadro de interoperabilidade a nível nacional e continental e reforçar o sistema de identificação fundacional.
3	Falta de capacidade técnica e financeira nos Estados-membros da UA	Aumentar a capacidade e promover o intercâmbio de conhecimentos entre pares entre os Estados-membros da UA, bem como considerar a relação custo-eficácia das soluções tecnológicas a serem acordadas nas Fases 2 e 3
4	Centros de dados inadequados a nível nacional/regional/continente	Construir centros de dados nacionais/ regionais/nacionais e promover a sua utilização por África.

5.3. RISCOS E PROPOSTAS DE MITIGAÇÃO

O quadro abaixo resume os riscos e os mecanismos de mitigação propostos.

#	Riscos	Propostas de Mitigação
1	Ausência de uma definição adequada de norma comum e falta de compreensão por parte dos Estados-membros da UA e incapacidade de seguir e adoptar normas comuns.	Definição de normas e comunicação das mesmas aos Estados-membros da UA durante a implementação e acompanhamento regular por um organismo pan-africano de confiança e capacitado que é apoiado e aprovado por todos os Estados-membros da mesma para garantir a adesão às normas. Discussões e workshops focalizados com as partes interessadas para assegurar uma definição clara das normas para a estratégia de implementação escolhida. Avaliação de referência da estratégia de implementação baseada em padrões do Estado-membro da UA em relação a programas de identificação nacionais fundacionais similares baseados em padrões estabelecidos em todos os Estados-membros da UA.
2	Baixos níveis de confiança entre as autoridades nacionais com capacidades de execução heterogéneas conduzem a uma lenta aceitação do quadro a uma grande escala continental. Além disso, os Estados-membros não estão dispostos a aceitar um organismo de supervisão supranacional, retardam a implementação do quadro de confiança.	O quadro deveria visar a harmonização e o reconhecimento mútuo como um objectivo a longo prazo, mas permanecer aberto ao desenvolvimento de soluções flexíveis e ágeis, que poderiam criar mecanismos de auditoria partilhados entre países dispostos a estabelecer confiança entre si, mantendo-se simultaneamente soberanos - através do reconhecimento unilateral dos certificados de confiança emitidos.
3	A solução, benefícios e opções não estão bem adaptadas ao ambiente local ou a informação é mal divulgada e as pessoas não estão a utilizar a solução levando a uma má aceitação e, em última análise, a custos elevados com poucos benefícios.	Desenvolver fortes estruturas de desenho centradas no utilizador para identificar soluções que sejam fáceis de utilizar e acessíveis a todos; Desenvolver fortes mecanismos de disseminação através dos Estados-membros da UA que incorporem todos os actores locais com os mesmos objectivos.

#	Riesgos	Medidas de mitigación propuestas
4	Ausência de Instituição Certificadora a nível continental e falta de governação inadequada os requisitos criptográficos para a assinatura digital podem revelar-se um obstáculo na criação do sistema de Interoperabilidade.	Criação de um quadro legal que permita o estabelecimento de uma instituição coordenadora a nível continental que seja apoiada por uma estrutura de governação equitativa que contabilize a soberania de cada Estado-membro para a implementação e gestão das assinaturas digitais, a sua emissão, revogação e substituição e actualização atempadas. Criação de uma estrutura de organização detalhada e dinâmica para permitir a governação da infra-estrutura de assinatura digital / PKI durante toda a fase de implementação e de operações.
5	Devido a dados incorrectos e incompletos, a concepção e estratégia de implementação de alguns dos componentes de interoperabilidade, como as assinaturas digitais, pode ser afectada. O atraso na partilha de dados e informações relevantes do cidadão ou residente pode também ter impacto nos prazos do projecto.	Reuniões com agências governamentais para a recolha de dados relativos à implementação nas lacunas de informação, aproveitando a experiência dos peritos através da aprendizagem entre pares para encorajar a colaboração e a apropriação regional e continental. Monitorização dos prazos e marcos do projecto para evitar atrasos. É também imperativo ter um calendário de implementação detalhado e abrangente que tenha sido acordado pelos Estados-membros da UA e pelas principais partes interessadas.
6	Ausência de directrizes de gestão da mudança claramente definidas para assegurar que o Quadro se mantém alinhado com as práticas, necessidades e desenvolvimento tecnológico actuais:	Implementação de um processo sólido e bem definido de gestão da mudança como parte do quadro de governação

#	Riesgos	Medidas de mitigación propuestas
7	Os Estados-membros decidirão sobre a tecnologia apropriada durante a fase de implementação, no entanto, se optarem pela tecnologia PKI, As agências certificadoras em África podem não chegar a um consenso em relação à gestão de PKI a nível de todo o continente. Em segundo lugar, pode não haver consensos sobre a criação de intercâmbio de assinaturas digitais.	Os Estados-membros da UA criaram uma nova instituição de certificação para a gestão de PKI a nível do continente ou aprovam um mecanismo para trazer as agências existentes para uma plataforma comum.
8	Não ter o ambiente legal mínimo necessário a nível nacional e regional.	Os Estados-membros da UA a acelerarem a implementação dos quadros jurídicos e regulamentares harmonizados necessários.

6. ANEXO

6.1. DEFINIÇÕES DE TRABALHO

Atributo é uma qualidade nomeada ou característica inerente ou atribuída a alguém ou algo (adaptado de NIST 800-63:2017). Nos sistemas de identificação, os atributos comuns de identidade incluem nome, idade, sexo, local de nascimento, endereço, impressões digitais, fotografia, assinatura, número de identidade, etc.

A autenticação é o processo de estabelecer a confiança de que uma pessoa é quem afirma ser. A autenticação digital envolve geralmente uma pessoa que apresenta electronicamente um ou mais "factores" para "afirmar" a sua identidade - isto é, para provar que é a mesma pessoa a quem a identidade ou credencial foi originalmente emitida. Estes factores podem incluir algo que uma pessoa sabe (por exemplo, uma senha ou PIN), tem (por exemplo, um cartão de identificação, ficha, ou cartão SIM móvel), ou é (por exemplo, as suas impressões digitais) (adaptado de NIST 800-63:2017 e OWI 2017).

A autorização é o processo de determinação das acções que podem ser realizadas ou dos serviços acedidos com base na identidade afirmada e autenticada (Nyst et al. 2016).

Fonte autorizada é uma fonte autorizada de informação de identidade é um repositório ou sistema que contém atributos sobre um indivíduo e é considerado como sendo a fonte primária ou mais fiável para esta informação. No caso de dois ou mais sistemas não corresponderem ou terem dados contraditórios, os dados dentro da fonte de dados autorizada são considerados os mais exactos (FICAM, sem data).

Reivindicação é uma qualificação, realização, qualidade, ou informação sobre o passado de um sujeito, tal como um nome, identificação governamental, endereço de casa, ou grau universitário. (Adaptado de W3C)

O **consentimento** da pessoa em causa significa qualquer indicação livre, específica, informada e inequívoca da vontade da pessoa em causa, pela qual esta, através de uma declaração ou de uma acção afirmativa clara, manifesta a sua concordância com o tratamento dos dados pessoais que lhe dizem respeito.

Credencial é um documento, objecto ou estrutura de dados que garante a identidade de uma pessoa através de algum método de confiança e autenticação. Os tipos comuns de credenciais de identidade incluem - mas não estão limitados a - cartões de identificação, certificados, números, senhas, ou cartões SIM. No caso deste Quadro, a credencial é um crédito verificável designado por IDC-ID.

Por **responsável pelo tratamento de dados** entende-se qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que, sozinha ou em conjunto com outras, decida recolher e tratar dados pessoais e determine as finalidades.

A **protecção de dados** regula a forma como os dados são utilizados ou processados e por quem, e assegura que os cidadãos têm direitos sobre os seus dados. É particularmente importante para assegurar a dignidade digital, pois pode abordar directamente o desequilíbrio de poder inerente entre "pessoas em causa" e as instituições ou pessoas que recolheram os dados.

As Autoridades de Protecção de Dados (APD) são autoridades públicas independentes que controlam e supervisionam, através de poderes de investigação e correctivos, a aplicação da lei de protecção de dados. Prestam aconselhamento especializado sobre questões de protecção de dados e tratam queixas que possam ter infringido a lei.

Por **pessoas em causa** entende-se qualquer pessoa singular que seja objecto de tratamento de dados pessoais.

A **dignidade digital** (no contexto da identificação digital) significa que a identidade humana por detrás da identificação digital tem privacidade e os seus dados são protegidos.

O **sistema de identificação digital (ID)** é um sistema de identificação que utiliza tecnologia digital durante todo o ciclo de vida da identidade, incluindo para a captura, validação, armazenamento e transferência de dados; gestão de credenciais; e verificação e autenticação de identidade (adaptado do relatório de Cooperação Público-Privada ID4D).

A **identidade digital** é um conjunto de atributos e/ou credenciais electronicamente capturados e armazenados que identificam de forma única uma pessoa (adaptado de Harbitz & Kentala 2013 e do relatório intitulado ID4D Technology Landscape).

A **assinatura digital** é uma operação de chave assimétrica em que a chave privada é utilizada para assinar digitalmente dados e a chave pública é utilizada para verificar a assinatura. As assinaturas digitais fornecem protecção de autenticidade, protecção de integridade e não repúdio, mas não protecção de confidencialidade (NIST 800-63:2017).

O **sistema de identificação fundamental** é um sistema de identificação criado principalmente para gerir informações de identidade para a população em geral e fornecer credenciais que servem como prova de identidade para aceder a serviços públicos e privados tais como educação, cuidados de saúde, protecção social e serviços financeiros, etc. (adaptado de Gelb & Clark 2013a e várias publicações ID4D). Para os fins deste Quadro, os Estados-membros da UA decidirão quais as fontes de dados fiáveis que implicam os seus Sistemas de Identificação Fundacionais.

Sistemas funcionais de identificação é um sistema de identificação criado para gerir a identificação, autenticação e autorização para um determinado serviço ou transacção, tais como votação, administração fiscal, programas e transferências sociais, serviços financeiros, e muito mais. Credenciais de identidade funcionais - tais como identificação do eleitor, registos de saúde e de seguros, números de identificação fiscal, cartões de racionamento, cartas de condução, etc. - podem ser geralmente aceites como prova de identidade para fins mais amplos fora da sua intenção original, particularmente quando não existe um sistema de identificação fundacional (adaptado de Gelb & Clark 2013a e várias publicações ID4D).

A **harmonização** está a assegurar uniformidade nos sistemas através da utilização de normas mínimas para facilitar a interoperabilidade e quadros legais e de confiança (por exemplo, para níveis de garantia) para estabelecer regras e criar confiança nos respectivos sistemas.

Identificação é um acrónimo para credencial de identidade ou documento de identidade em algumas áreas.

Sistema de identificação (ID) são as bases de dados, processos, tecnologia, infra-estrutura, credenciais e quadros legais associados à captura, gestão e utilização de dados de identidade pessoal para um fim geral ou específico (adaptado dos Princípios sobre Identificação).

A **identificação** é o processo de estabelecer, determinar ou reconhecer a identidade de uma pessoa. (adaptado de ISO/IEC 24760-1:2011 e ITU-T X.1252)

A **identidade** são as coordenadas sociais relativas que distinguem um indivíduo de outro. A identidade pode mudar dependendo dos actores ou do cenário em que os indivíduos se encontram e, portanto, não é fixa nem absoluta.

O **fornecedor de identidade** é uma entidade autorizada - por exemplo, uma agência governamental ou empresa privada - que emite e gere identidades legais, credenciais e processos de autenticação ao longo do ciclo de vida da identidade (documento de Cooperação Público-Privada ID4D).

Interoperabilidade é a capacidade das diferentes unidades funcionais - por exemplo, sistemas, bases de dados, dispositivos ou aplicações - de comunicar, executar programas, ou transferir dados de uma forma que requer que o utilizador tenha pouco ou nenhum conhecimento dessas unidades funcionais (adaptado de ISO/IEC 2382:2015).

O **nível de garantia (LOA)** é a capacidade de determinar, com algum nível de certeza ou garantia, que uma reivindicação de uma determinada identidade feita por alguma pessoa ou entidade pode ser considerada como sendo de facto a identidade "verdadeira" do requerente (ID4D Cooperação Público-Privada). O nível global de garantia é função do grau de confiança de que a identidade reivindicada pelo requerente é a sua identidade real (o nível de garantia de identidade ou IAL), a força do processo de autenticação (nível de garantia de autenticação ou AAL), e - se utilizar uma identidade federada - o protocolo de afirmação utilizado pela federação para comunicar a autenticação e atribuir informação (nível de garantia de identidade ou FAL) (adaptado de NIST 800-63:2017).

Normas Abertas são normas disponibilizadas ao público em geral e são desenvolvidas (ou aprovadas) e mantidas através de um processo de colaboração e de consenso. As "Normas Abertas" facilitam a interoperabilidade e o intercâmbio de dados entre diferentes produtos ou serviços e destinam-se a uma adopção generalizada (adoptadas a partir da UIT-T).

Por **dados pessoais** entende-se qualquer informação relativa a uma pessoa singular identificada ou identificável através da qual essa pessoa possa ser identificada, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a factores mais específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.

A **privacidade e a segurança** através da concepção significa incorporar proactivamente mecanismos de privacidade e segurança na concepção e operação de produtos e serviços tanto de sistemas não informáticos como de TI, infra-estruturas em rede, e práticas comerciais. Isto requer que a governação da privacidade e segurança seja considerada ao longo de todo o processo de engenharia e do ciclo de vida do produto.

A **Avaliação de Impacto da Protecção de Dados (DPIA)** é um processo concebido para identificar os riscos decorrentes do processamento de dados pessoais e para minimizar esses riscos o mais longe e o mais cedo possível. Os DPIAs são ferramentas importantes para negar o risco, e para demonstrar o cumprimento das leis e regulamentos de protecção de dados.

Por **tratamento de dados pessoais** entende-se qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, seja ou não por meios automáticos como a recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, cópia de segurança, cópia de segurança, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação e bloqueio, encriptação, apagamento ou destruição de dados pessoais.

A **prova de identidade legal** é uma credencial, tal como uma certidão de nascimento, bilhete de identidade ou credencial de identidade digital, que é reconhecida como prova de identidade legal ao abrigo do direito nacional e de acordo com as normas e princípios internacionais emergentes (Grupo de Peritos em Identidade Legal das Nações Unidas Definição Operacional de Identidade Legal).

A **parte confiante (RP)** é uma entidade que depende das credenciais e mecanismos de autenticação fornecidos por um sistema de identificação, normalmente para processar uma transacção ou conceder acesso à informação ou a um sistema (adaptado de NIST 800-63:2017).

O **quadro de confiança** refere-se aos requisitos empresariais, técnicos, operacionais e legais do sistema de identidade para promover a interoperabilidade entre as várias partes participantes.

Apresentação verificável é uma apresentação inviolável (Dados derivados de uma ou mais credenciais verificáveis) codificada de tal forma que a autoria dos dados pode ser confiada após um processo de verificação criptográfica. Por exemplo, abordagens de divulgação selectiva que sintetizam os dados e não transmitem as credenciais originais verificáveis (Adaptado do W3C)

A **verificação** é definida como o processo de verificação de atributos de identidade específicos ou de determinação da autenticidade das credenciais, a fim de facilitar a autorização para um determinado serviço.

Bureau of the Chairperson
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int