CONCURSO PÚBLICO INTERNACIONAL N.º 88/2025/EACD/AQUISIÇÃO DE SOLUÇÃO DE SOFTWARE DE BIOMETRIA DE IDENTIDADE DIGITAL

Especificações Técnicas

Índice

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por "AMA"), na sequência de procedimento pré-contratual que tem por objeto o fornecimento de solução de biometria de identidade digital para a Administração Pública Portuguesa, através de (Lote 1) Plataforma de orquestração biométrica e (Lote 2) Software de validação de identidade incluindo validação de segurança de documentos de identificação, verificação facial, deteção de vida ("liveness"), e autenticação biométrica e respetivos serviços acessórios, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.
2. Os concorrentes poderão apresentar proposta para um ou para ambos os lotes.
3. Relativamente aos serviços de suporte e manutenção do software fornecido pelo cocontratante, no âmbito do lote 1, que se revelem necessários após o término do contrato a celebrar no âmbito do presente procedimento, para aquisição dos mesmos poderá ser adotado um procedimento de ajuste direto, nos termos na alínea a) do n.º 1 do artigo 27.º do CCP, caso se verifiquem todos os requisitos.

Cláusula 2.ª

Local da prestação de serviços

Os serviços serão prestados nas instalações da AMA, sitas à Rua de Santa Marta, n.º 55 – 3.º, 1150-294, em Lisboa ou remotamente em regime de teletrabalho, conforme venha a ser acordado entre as partes.

Cláusula 3.ª

Duração

Os contratos terão a duração de 36 meses, iniciando a sua execução após a decisão de procedência do Tribunal de Contas, relativamente a ambos, ao abrigo do disposto no n.º 1 do artigo 17.º-A da Lei n.º 30/2021, de 21 de maio e da recomendação do Tribunal de Contas, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preços base

1. O preço base global do procedimento é de 2.999.850,00 €, acrescido de IVA à taxa legal em vigor, distribuído do seguinte modo:

a) Lote 1: O preço base é de **1 200 000,00 €,** a que acresce o IVA à taxa legal em vigor;

b) Lote 2: O preço base é de **1 799 850,00 €,** a que acresce o IVA à taxa legal em vigor.

2. Serão excluídas as propostas cujo valor seja superior aos preços base referidos no número anterior.

3. Os preços propostos deverão observar o cumprimento das condições descritas no Anexo II do Programa de Procedimento, sob pena de exclusão da respetiva proposta.

4. O preço referido nos números anteriores inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à AMA, designadamente:

a) Despesas com deslocações, estadias e despesas de alimentação;

b) Encargos com telecomunicações;

c) Computador;

d) Seguro de acidentes de trabalho.

Cláusula 5.ª

Condições de pagamento

1. A faturação será efetuada da seguinte forma:

a) Lote 1

i. Licenciamento ilimitado da plataforma realizado após a disponibilização e aceitação da plataforma (até 90 dias após a celebração do contrato), 100 %;

ii. Trimestralmente, 25% do valor anual para suporte da plataforma;

iii. Mensalmente, o valor correspondente ao volume de horas de manutenção evolutiva executado e aceite pela AMA, até esgotar o montante global previsto para a bolsa de horas.

b) Lote 2

i. Licenciamento ilimitado da plataforma realizado após a disponibilização e aceitação da plataforma (até 30 dias após a celebração do contrato);

ii. Trimestralmente, 25% do valor anual para suporte da plataforma.

2. Considerando que as despesas inerentes ao suporte de software nos anos 2027 e 2028 será financiada de acordo com as verbas previstas e disponíveis nos Orçamentos de Estado de 2027 e 2028, a sua execução e pagamento ocorrerá nos anos de 2027 e 2028, não podendo ser antecipados, sem que se verifiquem as devidas formalidades legais.

3. O pagamento será efetuado no prazo 30 dias a contar da data da receção das faturas correspondentes, as quais só podem ser emitidas após o vencimento da obrigação a que se referem.
4. As faturas devem discriminar os serviços a que se reportam, o número do contrato bem como o número de compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.
5. Caso as faturas apresentadas não sejam validadas pela AMA esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
6. As faturas deverão revestir a forma eletrónica, caso em que devem ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o Portal FEAP (Faturação Eletrónica na Administração Pública) disponibilizado pela ESPAP.
7. Só serão devidos os valores referentes bens fornecidos e aos serviços efetivamente prestados e aceites nos termos do presente caderno de encargos.
8. O pagamento será realizado para o NIB/IBAN indicado em documento bancário apresentado pelo cocontratante o qual deverá ser atualizado sempre que necessário.
9. Em caso de atraso no cumprimento das obrigações pecuniárias por parte da AMA, o cocontratante tem o direito aos juros de mora sobre o montante em dívida, nos termos previstos no artigo 326.º do CCP e da Lei n.º 3/2010, de 27 de abril.

Cláusula 6.ª

Propriedade intelectual

1. São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
2. O cocontratante obriga-se a transferir a posse e a propriedade dos elementos a desenvolver ao abrigo do contrato para a AMA incluindo os direitos autorais sobre todas as criações intelectuais abrangidas pelos serviços a prestar, incluindo os previstos no n.º 4 do artigo 14.º do Código do Direito de Autor e dos Direitos Conexos, bem como de outros direitos de propriedade intelectual, relativos aos serviços objeto do presente caderno de encargos, produtos dele resultantes nomeadamente, código fonte, documentação e elementos afins, bem como dos produtos consequentes a todas as ulteriores adaptações que se venham a revelar necessárias.
3. O cocontratante entregará à AMA no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos desenvolvidos, incluindo as respetivas fontes que serão propriedade da AMA.
4. A AMA poderá transformar e reproduzir todos os documentos e todo o software desenvolvido, bem como proceder à sua distribuição, onerosa ou gratuita, de forma inteiramente livre.
5. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos.

6. Correm inteiramente por conta do cocontratante, os encargos e responsabilidades decorrentes da utilização, na execução do fornecimento dos equipamentos, de materiais, de elementos de construção, de hardware, de software ou de outros a que respeitem quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor ou conexos.

7. Se a AMA vier a ser demandada por ter sido infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o cocontratante responderá nos termos do disposto no artigo 447.º, n.º 2,do Código dos Contratos Públicos.

Cláusula 7.ª

Sigilo

1. O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da AMA ou qualquer outra entidade envolvida na execução do contrato.
2. A informação e documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
4. O cocontratante assume igualmente o compromisso de restituir, remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados, incluindo dados pessoais, e que a AMA lhe indique para esse efeito.
5. O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da AMA, nos termos legalmente previstos, relativamente à proteção de dados pessoais e à proteção jurídica de bases de dados.
6. Após ter conhecimento de alguma violação de dados pessoais o cocontratante notifica a AMA sem demora injustificada, em prazo inferior a 48 horas.
7. O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.

Cláusula 8.ª

Proteção de dados

1. O Cocontratante é obrigado a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto

no Regulamento Geral de Proteção de Dados Pessoais aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), devendo, nomeadamente:

a) Tratar os dados pessoais apenas mediante instruções documentadas da Entidade Adjudicante, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso a Entidade Adjudicante desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adotar todas as medidas exigidas nos termos do artigo 32.º do RGPD;

d) Garantir o cumprimento do RGPD, nas condições aqui previstas, quando pretenda contratar um subcontratante;

e) Tomar em conta a natureza do tratamento, e na medida do possível, prestar assistência à Entidade Adjudicante pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos previstos no capítulo III do RGPD;

f) Prestar assistência à Entidade Adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao seu dispor;

g) Consoante a escolha da Entidade Adjudicante, apagar ou devolver-lhe todos os dados pessoais depois de concluído o contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;

h) Disponibilizar à Entidade Adjudicante todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula, facilitando e contribuindo para as auditorias, inclusive as inspeções, conduzidas pela Entidade Adjudicante ou por outro auditor por esta mandatado.

2. A Entidade Adjudicante, no caso de suspeitar de incumprimento do RGPD, pode notificar o Cocontratante para este, no prazo de 5 dias, demonstrar o total cumprimento do referido regulamento.

3. Caso o Cocontratante não demonstre o total cumprimento do RGPD, seja porque não o demonstrou, seja porque não o cumpre, a Entidade Adjudicante fica autorizada a proceder à auditoria aos sistemas de informação do Cocontratante, ficando este responsável por todos os custos dessa auditoria.

4. No caso previsto no número anterior, a Entidade Adjudicante poderá compensar os custos que tenha suportado com eventuais quantias que sejam devidas ao Cocontratante, ou através do acionamento da caução, caso esta tenha sido prestada, ou através do recurso às retenções que eventualmente tenham sido

efetuadas.

5. No caso de se verificar algum incumprimento do RGPD por parte do Cocontratante, este deverá, no prazo de 10 dias, pôr fim ao incumprimento e demonstrá-lo à Entidade Adjudicante.
6. O não cumprimento do RGPD, por facto imputável ao cocontratante, é considerado, para todos os efeitos, incumprimento definitivo, podendo a Entidade Adjudicante resolver o contrato, ao abrigo da alínea a) do n.º 1 do artigo 333.º do CCP.
7. Caso o Cocontratante impeça ou não colabore na realização da auditoria referida no n.º 3 da presente cláusula, a Entidade Adjudicante poderá resolver o contrato, por oposição reiterada ao exercício dos poderes de fiscalização, ao abrigo da alínea c) do n.º 1 do artigo 333.º do CCP.

Cláusula 9.ª

Cessão da posição contratual e subcontratação

1. O cocontratante pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo, desde que previamente autorizado pela AMA**.**
2. Nos casos de subcontratação, o cocontratante permanece integralmente responsável perante o contraente público pelo exato e pontual cumprimento de todas as obrigações contratuais.
3. A subcontratação de prestações contratuais que envolvam o tratamento de dados pessoais carece de autorização prévia da AMA que deverá ser realizada nos termos legalmente previstos para o efeito.
4. O cocontratante é responsável pelo tratamento de dados pessoais no âmbito da execução do contrato, mesmo que seja realizado por subcontratado.

Cláusula 10.ª

Comunicações e notificações

1. Sem prejuízo de se acordarem outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas para o domicílio ou sede contratual de cada uma nos termos previstos no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 11.ª

Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a AMA pode exigir ao cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
    a) Pelo incumprimento nos níveis de serviço de Alojamento da CMD e Entidade Certificadora poderão ser aplicadas penalidades de 1% do preço contratual por cada 0,1% abaixo do nível de serviço

aferido mensalmente;

b) Pelo incumprimento da cláusula 18.ª, poderá ser aplicada uma penalidade de 500€ por cada dia de atraso;

c) Pelo incumprimento da cláusula 19.ª, poderá ser aplicada uma penalidade de 500€ por cada dia de atraso;

d) Pelo incumprimento da cláusula 21.ª, poderá ser aplicada uma penalidade de 500€ por cada dia de atraso.

e) Pelo incumprimento do prazo de disponibilização da solução proposta, de acordo com o indicado no ponto 3 da cláusula 3ª, poderá ser aplicada uma penalização igual a 20% do valor total do contrato, levando ainda á rescisão contratual.

2. Na determinação da gravidade do incumprimento, a AMA tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante e as consequências do incumprimento.

3. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida a fatura respetiva.

4. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.

5. Nos casos em que seja atingido o limite previsto no número anterior e a AMA decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 %.

6. A aplicação das sanções previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 12.ª

Trabalhadores afetos à prestação de serviços

O cocontratante deve garantir, relativamente aos trabalhadores afetos à execução do contrato a celebrar, o cumprimento integral das disposições previstas no artigo 419.º-A do CCP.

Cláusula 13.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Círculo de Lisboa.

Cláusula 14.ª

Legislação aplicável

Em tudo o omisso neste Caderno de Encargos, observar-se-á o previsto no Código dos Contratos Públicos e demais legislação aplicável.

CLÁUSULAS TÉCNICAS

Cláusula 15.ª

Descrição técnica do contrato

1. Enquadramento

A AMA – Agência para a Modernização Administrativa, IP é a entidade responsável pela operacionalização de vários processos transversais que têm por objetivo melhorar a Administração Pública Portuguesa e disponibilizar serviços públicos pelo canal que o cidadão considere mais adequado.

A identificação inequívoca do cidadão perante os serviços públicos é uma necessidade premente à massificação na utilização dos serviços públicos na sua vertente eletrónica, tendo a AMA vindo a desenvolver um conjunto de soluções de autenticação e de assinatura eletrónica qualificada com o Cartão de Cidadão (CC) de forma a garantir a toda a Administração Pública a possibilidade de integrar estas funcionalidades nos seus portais de forma simples e eficiente.

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS.

No contexto da medida SIMPLEX "**CMD SIMPLEX**" e de autorização legislativa ficou definida a simplificação do processo de adesão à CMD, nomeadamente:

- Adesão em aplicação móvel (de forma autónoma), recorrendo à validação de documento de identificação, deteção de vida (liveness) e reconhecimento facial.
- Adesão através de Videoconferência, assistido por Operador, procedendo-se à validação de documento de identificação, e a reconhecimento facial.

Desde o início de 2023 que está em funcionamento o processo de adesão totalmente automatizado e remoto através da App autenticação.gov, sendo neste momento a forma mais utilizada de adesão à chave móvel digital.

A utilização de biometria no contexto da identidade digital (verificação facial, presença de vida, validação de documentos de identidade, e outros fatores) de forma transversal à Administração Pública, abre caminho a diferentes casos de utilização, não só no âmbito da Chave Móvel Digital, mas também do Cartão de Cidadão, Passaporte e outros casos de uso. Assim, considerando estas potencialidades e benefícios, com este procedimento pretende-se disponibilizar "*building block*" para utilização transversal e sem limitações pela

Administração Pública. Para além dos casos de uso em seguida descritos (e dos já existentes de adesão à CMD e ativação do Cartão de Cidadão com base em biometria), a título exemplificativo, identificam-se outros que poderão fazer uso dos componentes de software a fornecer no âmbito deste procedimento:

- Verificação de identidade regular do Titular de CMD (ou sempre que se identifiquem motivos de segurança)
- Autenticação com Chave Móvel Digital sem recurso a códigos permanentes ou temporários ("PINless")
- Pedido, renovação ou entrega de Cartão de Cidadão ou passaporte (designadamente em canais presenciais e remotos)
- Prova de Vida para fins de benefícios e pensões.

Assim, este procedimento está estruturado em 2 lotes, com os seguintes enfoques:

- Lote 1: Plataforma de orquestração biométrica, que disponibilizará uma interface (API e SDK) normalizada na integração com as aplicações clientes, videoconferência, bem como um motor visual de modelação de fluxos biométricos e integração com os softwares de providers biométricos (designadamente os previstos no lote 2).

- Lote 2: software de validação de identidade (API e SDK) incluindo validação de segurança de documentos de identificação, verificação facial, deteção de vida ("liveness"), e autenticação biométrica e respetivos serviços acessórios

Pretende-se assim disponibilizar uma plataforma de orquestração que permite desenhar diferentes fluxos de operação, seja para o onboarding seja para autenticação, com a possibilidade de introduzir, retirar ou combinar diferentes motores biométricos e de análise, garantindo que a solução poderá evoluir á medida que as tipologias destes motores evoluam ao longo dos próximos anos, acompanhando também as alterações regulamentares que possam existir.

2. Descrição técnica

Apresenta-se na Figura 1 a arquitetura conceptual das várias componentes da solução, com a identificação dos Lotes onde as mesmas deverão ser fornecidas neste processo aquisitivo.

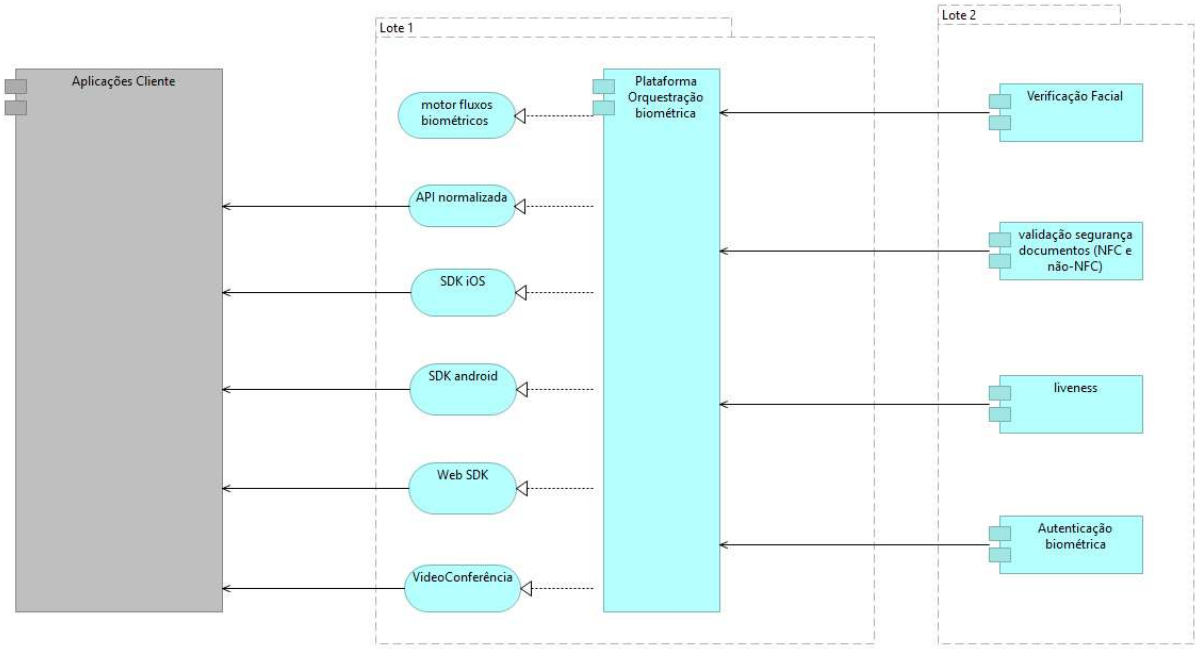

Figura 1 – Arquitetura global building block biométrico Nacional (a cinzento componentes fora de âmbito)

Com esta arquitetura pretende-se assegurar uma normalização da interface para as aplicações clientes, desacoplando-se as API e SDKs usadas pelas aplicações Clientes dos diferentes motores e fornecedores de software biométrico que poderá ser usado, num dado momento, de acordo com as condições de mercado, técnicas e contratuais.

Lote 1. Plataforma de orquestração biométrica

2.1. Disponibilização de **plataforma orquestração biométrica**, incluindo:

a) **Motor visual de modelação de fluxos biométricos e back-office de gestão**, assegurando:

i. Experiência do utilizador sem atrito:

a. a construção dos diversos processos deve ser simples e "low code",

b. permitindo o desenho de fluxos com múltiplos motores de análise,

c. através de interface gráfico com mecânicas de construção "arrastar e largar" ou similares, sem depender de programação adicional,

d. nomeadamente motores de comparação de fotografias ou de Liveness,

e. permitindo efetuar o processo referido como "homogeneização" para que os resultados de análise sejam a combinação de mais do que um motor de análise. Neste sentido é requerido que sejam apresentadas evidências gráficas (screenshots e/ou vídeos), da construção dos

fluxos onde seja visível não só a mecanica drag & drop da construção dos fluxos, como a utilização de motores distintos para ilustrar o processo de homogeneização.

ii. Nos processos desenhados deverá ser possível
   a. condicionar o passo seguinte do fluxo tendo em conta as informações recolhidas em passos anteriores.
   b. Por exemplo se a pessoa que está a efetuar o onboarding tiver nascido há menos de x anos, o passo seguinte após a prova de vida, será o passo A, e se tiver nascido há mais de X anos, será o passo B. Neste sentido é requerido que sejam mostradas evidências gráficas (screenshots e/ou vídeos), da construção dos fluxos onde seja visível a utilização de dados condicionais.

iii. Interface Personalizável:
   a. Facilidade na personalização também lowcode, da interface de utilizador para refletir a marca e as preferências dos processos específicos, melhorando assim a integração visual e funcional com os sistemas existentes.

iv. Suporte a **Criação de Fluxo** onde se define toda a jornada que o utilizador final irá seguir.
   a. Um fluxo representa a sequência completa de passos que o utilizador deve realizar,
      i. desde ações simples, como o envio de informações,
      ii. até processos mais complexos, como validação biométrica ou assinatura de documentos.
   b. Independentemente da complexidade, o objetivo do fluxo é sempre o mesmo: garantir que o utilizador forneça as informações necessárias de forma segura, estruturada e orientada.
   c. Deve permitir criar novos fluxos do zero ou
   d. importar modelos existentes,
   e. adicionar ações (onde se constrói o fluxo, selecionando e ordenando os módulos necessários - Validação de Documentos, Verificação Facial, etc.)),
   f. Triggers (que define ações automáticas que ocorrem em momentos específicos do fluxo) e
   g. ainda notificação (configuração de notificações para manter o utilizador informado em pontos-chave do processo).

v. Disponibilização de diferentes **módulos** para construir processos de verificação de identidade digital e *onboarding*, incluindo:
   a. Formulário – Recolha de dados estruturados.
   b. Validação e Assinatura de Documentos – Verificação de autenticidade e assinatura digital.
   c. Comparação e Verificação Facial – Confirmação de identidade através de imagens faciais.
   d. Deteção de Presença (Liveness) – Garante que o utilizador está fisicamente presente.
   e. Autenticação OTP – Código temporário seguro para validação do utilizador.

f. Videoconferência e Presença em Vídeo – Interação ao vivo para revisão manual.
g. Leitura NFC – Extração e validação de dados de documentos NFC.
h. Análise de Risco – Avaliação do nível de risco do utilizador ou transação.

vi. **Personalização**. Controlo total sobre a experiência visual e interativa dos utilizadores permitindo ajustar
a. cores,
b. ícones,
c. fontes,
d. logótipos
e. e imagens de fundo para alinhar o design à identidade da marca.
f. Suporte a traduções e definir configurações específicas para adaptar a interação ao público.

Esta personalização deve assegurar uma experiência fluida e integrada, mantendo a segurança e a fiabilidade do processo de verificação.

vii. **Integração** com sistemas externos, garantindo controlo total sobre a interação com aplicações externas com os fluxos de verificação, dados e segurança, designadamente considerando:
a. **Aplicações** – Identificadores que ligam aplicações a fluxos de verificação específicos, assegurando governação e rastreabilidade.
b. **Credenciais** – Definem permissões seguras para envio, recuperação e gestão de dados, seguindo o princípio do menor privilégio.
c. **Gestão de Certificados** – Suporte a certificados digitais para assinaturas legais, validação de transações e encriptação de dados.

b) API normalizada na integração com as aplicações clientes

c) SDK iOS e Android para integração em aplicações cliente (que deverá consolidar com os softwares dos providers de software adquiridos no Lote 2) e manter a retrocompatibilidade com o API do SDK atualmente usado pela a AMA – vide https://biometrid.gitbook.io/biometrid-android-sdk e https://biometrid.gitbook.io/biometrid-ios-sdk

- Deve ser disponibilizado um SDK para iOS e para Android
- O SDK para iOS deve ser desenvolvido Objective-C ou Swift
- O SDK para Android deve ser desenvolvido em Java ou Kotlin
- Os SDK's devem funcionar em redes Wi-Fi que não permitam a utilização do utilitário de rede para endereços externos à rede.
- Os SDK's disponibilizam todos os endpoints necessários para a Integração "clássica" num frontend, existindo nesse caso a necessidade de desenhar por completo a respetiva jornada no frontend.

- O SDK disponibiliza todos os componentes necessários para uma Integração total do SDK que inclui todos os ecrãs necessários para o frontend para a jornada de onboarding, que será servida em todos os frontends de forma responsiva. Neste caso, após a integração deste SDK completo, deverá ser possível efetuar alterações funcionais e de design usando a plataforma integrada sem que seja necessário voltar a integrar o SDK nos frontends, nem a nova publicação das apps nas respetivas stores.

d) web-SDK

- Para estender a utilização da solução aos sítios Web e não apenas em apps nativas iOS e Android, pretende-se que o adjudicatário disponibilize um WEB SDK, tendo em consideração as tecnologias especificas descritas anteriormente e usadas nos SDK android e iOS - mantendo-se os requisitos apresentados para a versão ios e android (exceto leitura por NFC), sempre que aplicável.

e) Integração com os softwares biométricos (designadamente os que venham a ser selecionados no lote 2), assegurando independência face a motores de análise: deve ser possível integrar diversos motores de análise (existentes ou a desenvolver, desde que cumpram com requisitos técnicos standard de REST), em módulos independentes, por forma a antecipar possível obsolescência de alguns dos motores atuais, sem obrigar a novo desenvolvimento profundo da solução.

No âmbito do atual fornecimento, é da responsabilidade do adjudicatário (lote 1) assegurar a integração na plataforma de orquestração biométrica até 2 softwares de validação de identidade para cada tipologia de validação de identidade (lote 2), nomeadamente: 1) validação de segurança de documentos de identificação Portugueses; 2) validação de segurança de documentos de identificação não Portugueses; 3) validação de segurança de documentos de identificação por NFC; 4) verificação facial; 5) deteção de vida (“liveness”); e 6) autenticação biométrica.

f) Videoconferência

Disponibilização de serviço de videoconferência através de SDK e também de solução de software fornecida pelo adjudicatário que use providers (lote 2) para

i. Processo de identificação do cidadão, incluindo a verificação de documento de identificação,
ii. Reconhecimento facial
iii. Prova de Vida (Liveness)
iv. Outros aplicáveis

Software proposto deve cumprir os requisitos preconizados no Despacho n.º 154/2017 de 5 de dezembro do Gabinete Nacional de Segurança.

Os vídeos resultantes da VC deverão ser preservados ao longo do período do contrato e disponibilizados à entidade adjudicante sempre que solicitado (de forma automatizada).

g) Video auto-gravada

1. Utilizador grava um vídeo (sem a presença do agente), onde
    a. cumpre com um script aleatório gerado pelo sistema que
    b. podem incluir *prompts* verbais (informações que o utilizador deve indicar), e
    c. movimentos automaticamente verificáveis pelo sistema e,
    d. assim que termine, submete na plataforma.
    e. Posteriormente um agente valida a autenticidade desta ação.
2. Estes vídeos deverão ser preservados ao longo do período do contrato e disponibilizados à entidade adjudicante sempre que solicitado (de forma automatizada).

h) Requisitos Comuns:

i. Modularidade e Escalabilidade: A plataforma deve ser projetada para permitir a adição de novos módulos ou funcionalidades conforme necessário, mantendo-se escalável para suportar processos com pucos utilizadores como processos com utilização em massa.

ii. Interoperabilidade: Capacidade de interagir e funcionar de maneira integrada com outras plataformas, sistemas de segurança ou fontes de dados, permitindo uma abordagem holística à segurança da identidade. Nomeadamente capacidade de atuar dentro de um determinado modulo com informações externas integráveis através de webservice.

iii. Conformidade Dinâmica: A plataforma deve ser capaz de se adaptar rapidamente a mudanças nas regulamentações de privacidade e segurança de dados.

iv. A solução apresentada deve disponibilizar SDK's que integrem o fluxo desenhado completo, que possa ser integrado de forma completa nas soluções existentes de duas formas distintas:
    i) O SDK disponibiliza todos os endpoints necessários para a Integração "clássica" num frontend, existindo nesse caso a necessidade de desenhar por completo a respetiva jornada no frontend.
    ii) O SDK disponibiliza todos os componentes necessários para uma Integração total do SDK que inclui todos os ecrãs necessários para a jornada de onboarding, que será servida em todos os frontends de forma responsiva. Neste caso, após a integração deste SDK completo, deverá ser possível efetuar alterações funcionais e de design usando a

plataforma integrada sem que seja necessário voltar a integrar o SDK nos frontends, nem deve ser necessário nova publicação das apps nas respetivas stores.

i) **Casos de Uso a configurar**. Deverão ser configurados os seguintes casos de uso na Plataforma (incluindo desenho, configuração, testes):

i) Adesão à CMD via aplicação móvel gov.pt: processo atualmente em funcionamento via app gov.pt. Este processo de adesão, e o software proposto, tem de cumprir os requisitos preconizados no Despacho n.º 2705/2021, de 11 de março do Gabinete Nacional de Segurança. A solução apresentada tem de evidenciar de forma inequívoca e detalhada que cumpre com o disposto neste despacho, com indicação clara do fluxo global da solução proposta.

ii) Processo de adesão à CMD em Videoconferência: A adesão à CMD em videoconferência é realizada com agentes de Centros de Contacto da AMA, usando solução de software fornecida pelo adjudicatário de acordo com os seguintes passos:

1. Processo de identificação do cidadão, incluindo a verificação de documento de identificação,
2. o reconhecimento facial (frame da videoconferência do cidadão – selfie vs. foto no documento),
3. um segundo reconhecimento facial (frame da videoconferência do cidadão - selfie vs. foto central), seguido da criação da conta CMD e envio do PIN Provisório por SMS.
4. Prova de Vida

Este processo de adesão, e o software proposto, cumpre os requisitos preconizados no Despacho n.º 154/2017 de 5 de dezembro do Gabinete Nacional de Segurança. A solução apresentada tem de evidenciar de forma inequívoca e detalhada que cumpre com o disposto neste despacho, com indicação clara do fluxo global da solução proposta.

iii) Verificação de identidade regular do Titular de CMD (ou sempre que se identifiquem motivos de segurança)

Com autenticação de transações de acordo com análise de criticidade, e fidelização regular da Appgov.pt. O objetivo será garantir que o utilizador a operar a CMD é sempre o cidadão original e não alguém que não seja ele próprio.

iv) Ativação certificados do Cartão de Cidadão, similar e integrado no processo i)

v) Autenticação Chave Móvel Digital sem recurso a PIN, tendo por base biometria (verificação de presença de vida e verificação facial, tendo por base vetor biométrico). No processo de adesão deve ser

criado vetor biométrico que deverá ser usado em processo de autenticação, onde deve ser feita a verificação facial e o liveness 3D, sem necessidade de leitura da fotografia de alta resolução constante da base de dados ou do documento de identificação.

vi) Pedido, renovação ou entrega de Cartão de Cidadão ou passaporte (designadamente em canais presenciais e remotos), incluído: pedido de cartão de cidadão em quiosque biométrico, a renovação do cartão de cidadão através de app (com validação biométrica e de presença de vida, mas também validação ICAO da fotografia recolhida que será usada na personalização do novo documento de identificação).

vii) Prova de Vida para fins de benefícios e pensões, designadamente validando a identidade do cidadão e o liveness, quer em app, quer em web/desktop.

j) Alojamento

Devem ser disponibilizado os serviços tecnológicos para a Plataforma de orquestração biométrica (objeto do lote 1), e para os software de validação de identidade (lote 2) em infraestrutura de servidores, redes, segurança, e administração necessários para a disponibilização do âmbito descrito no presente CE (softwares previstos no Lote 1 e Lote 2) – ou seja, no âmbito do fornecimento do lote 1 inclui-se a responsabilidade da infra-estrutura, operação e disponibilização das plataformas e softwares fornecidos nos lotes 1 e 2 (bem como todo o software base necessário – sistemas operativos, SGBD, servidores aplicacionais, segurança, etc).

A infraestrutura apresentada deverá assegurar as operações e a sua respetiva escalabilidade em casos pontuais de picos de carga.

No mínimo, devem ser disponibilizados os seguintes **servidores dedicados** num datacenter localizado em território europeu, preferencialmente em Portugal, assegurando redundância mínima da seguinte infraestrutura:

a. Servidor Base de Dados (CPU 4 cores, 6GB RAM, 40 GB Disco)
b. Servidor Front-end Backoffice (CPU 4 cores, 6GB RAM, 20 GB Disco)
c. Servidor Aplicacional Verificação Documentos (CPU 4 cores, 8GB RAM, 20 GB Disco)
d. Servidor Aplicacional Face Match (CPU 4 cores, 6GB RAM, 20 GB Disco)
e. Servidor Aplicacional Liveness (CPU 4 cores, 8GB RAM, 20 GB Disco)
f. Servidor Aplicacional Video-Conferencia (CPU 4 cores, 6GB RAM, 20 GB Disco)
g. Servidor web Video-Conferencia (CPU 4 cores, 6GB RAM, 20 GB Disco)
h. Firewall e IDS

O número de servidores e equipamentos poderá aumentar de forma a responder aos requisitos constantes do CE.

Deve ainda ser disponibilizado ambiente de testes e/ou qualidade (responsabilidade do adjudicatário).

Backups

A solução proposta deverá contemplar backups a toda a infraestrutura, com a seguinte política de backups:

- 1x diário incremental
- 1x full semanal
- Retenção: 30 dias

A gestão dos Backups, isto é, a configuração e monitorização dos trabalhos de Backup fica a cargo do concorrente.

Todos os *jobs* de backups deverão ter uma taxa de sucesso de 100%. *Jobs* de backups que tenham algum tipo de erro, deverão ser relançados assim que possível.

Os dados de *backups* deverão estar encriptados, com um standard de AES-256 ou semelhante. A gestão da encriptação e rotatividade da chave de encriptação deverá estar a cargo do concorrente.

Deverá ser possível ajustar a política de backups ao longo do contrato celebrado.

Para todos os dados de backup, a 1ª cópia deverá ser feita e armazenada no mesmo Data Center onde está alojada a infraestrutura e uma 2ª cópia para um Data Center secundário.

Monitorização

Monitorização para todos os clusters, com métricas e alarmística disponível 24x7. Tipo de métricas:

- Utilização de CPU;
- Utilização de memória;
- Utilização do disco;
- Disponibilidade de serviços;
- Possibilidade de configurar alarmística;

Segurança

Controlo de Acesso à Rede:

- Firewall de perímetro rede para restringir o tráfego de entrada e saída para os nós e outros componentes. A Firewall deverá ter funcionalidades de deteção e prevenção de intrusão (IDS/IPS).

- Utilizar Network Policies para segmentar o tráfego de rede entre pods e namespaces, aplicando o princípio do menor privilégio;
- Isolar a rede da plataforma de outras redes internas e externas;
- Restringir o acesso SSH aos nós e utilização de chaves SSH;
- Registar em *Logs* os acessos aos nós;

Segurança da Aplicação:

- Aplicar as boas práticas recomendadas pelo OWASP Top 10.
- Garantir encriptação AES-256 para dados em repouso e em trânsito.
- Mascarar e tratar dados sensíveis nos ambientes não produtivos (DEV), de acordo com a normativa RGPD.
- Registar logs detalhados para acessos críticos e atividades administrativas.
- Todas as aplicações devem ser testadas e analisadas para vulnerabilidades periodicamente e antes de serem utilizadas em produção
- O repositório de imagens deverá suportar políticas de segurança com logs de acesso.

Encriptação

Todos os dados da solução, incluindo dados de Backup, devem estar encriptados. A gestão da encriptação e da desencriptação, no decorrer da operação diária, é da responsabilidade do cocontratante.

Gestão, manutenção e *Hardening* de sistemas

- A solução proposta deverá ser gerida, num período de 24x7, pelo cocontratante. Todos os sistemas que suportem a solução, assim como serviços complementares (Backups, Firewall, Load Balancers, etc) devem estar incluídos na gestão de sistemas.
- Todos o sistema operativo, software de orquestração e distribuições de Linux propostas devem estar assentes em distribuições suportadas por fabricante;
- Todo o software deverá estar com suporte ativo de fabricante durante o período contratual. Não são permitidas soluções que não tenham contemplado o suporte de fabricante;
- O cocontratante tem a responsabilidade da aplicação de atualizações e patches de segurança do sistema operativo e de todas as dependências de software;
- O cocontratante tem a responsabilidade de reduzir a superfície de ataque, através da desativação de serviços, funcionalidades e portos de rede desnecessários.

Disponibilidade de serviço

Toda a infraestrutura que suporta o serviço proposto deverá ter redundância ao nível do Data Center proposto, nomeadamente:

- Redundância no fornecimento de energia (UPS, geradores e baterias);
- Redundância de networking (Cores de rede redundantes, switching de distribuição redundante);
- Redundância de storage (controladoras, RAID);
- Redundância dos *hosts* físicos que suportam os clusters e as BDs;
- Capacidade de levantar infraestrutura (parcial ou total) num outro Data Center do concorrente, mediante solicitação da AMA;

Elasticidade

O serviço proposto deverá ter a capacidade de escalar a quantidade de recursos para suportar a carga necessária. O serviço deverá ter a capacidade de adicionar mais vCPU, RAM, Disco e nós nos clusters, num horizonte temporal compreendido entre minutos a 1 hora no máximo.

Disaster Recovery

O serviço proposto deverá incluir um plano de Disaster Recovery (DR) entre dois Data Centers do concorrente. Os Data Centers deverão estar geograficamente separados por uma distância mínima de 200 km, de forma a garantir uma redundância eficaz em caso de catástrofe natural, falha de infraestrutura crítica ou outro incidente de grande escala, assegurando a continuidade e resiliência dos serviços prestados.

A solução proposta deverá replicar os dados para outro Data Center e ter a capacidade de levantar a totalidade da infraestrutura.

Pretende-se um SLA de RTO (Recovery Time Objective) de 4 horas e RPO (Recovery Point Objective) de 2 horas.

O cocontratante deverá também assegurar um plano de "failback", isto é, após levantamento da infraestrutura em DR, restaurar o serviço no Data Center de origem.

Disponibilidade de serviços com nível de disponibilidade superior ou igual a 99.9950%, em período 24hx7d, devendo assegurar-se os seguintes requisitos:

i. Número máximo de pedidos de OCR Cartão de Cidadão e verificação de segurança CC: 1000 pedidos/hora;

j. Número máximo de pedidos de liveness: 300 pedidos/hora;

k. Número máximo de pedidos de Comparação da Foto: 500 pedidos/hora;

l. Tempo médio de resposta a pedidos de liveness, comparação de foto, OCR Cartão de Cidadão e verificação básica de segurança: 3 segundos em 90% dos pedidos;
m. Tempo máximo de resposta a pedidos de liveness, comparação de foto, OCR Cartão de Cidadão e verificação básica de segurança: 10 segundos em 100% dos pedidos;
n. Tempo médio de resposta a pedidos de verificação de segurança avançada Cartão de Cidadão: 5 segundos em 90% dos pedidos;
o. Tempo máximo de resposta a pedidos de verificação de segurança avançada Cartão de Cidadão: 20 segundos em 100% dos pedidos;
p. Tempo máximo de resposta de Interface web de videoconferência (utilizada pelo Operador e/ou cidadão): 2 segundos em 90% dos pedidos;
q. Tempo máximo de resposta de Interface web de videoconferência (utilizada pelo Operador e/ou cidadão): 4 segundos em 99% dos pedidos;
r. Tempo máximo de resposta de Interface web de videoconferência (utilizada pelo Operador e/ou cidadão): 5 segundos em 100% dos pedidos;
s. Número máximo de pedidos de autenticação (vetor biométrico): 100 000 pedidos/hora;
t. Tempo médio de resposta a pedidos de autenticação: 1 segundo em 90% dos pedidos;
u. Tempo médio de resposta a pedidos de autenticação: 2 segundos em 99,90% dos pedidos;
v. Todos os dados pessoais (incluindo dados biométricos e de identificação) devem ser eliminados dos equipamentos (servidores e equipamentos de rede) após a resposta e, obrigatoriamente, no final de cada dia (em caso de incidentes ou erros).
w. O centro de dados deve assegurar entre outros:
    i) O acesso físico aos vários níveis de segurança, aos elementos previamente identificados pela AMA;
    ii) Que todos os alarmes oriundos do Sistema de Segurança, devem ser comunicados à AMA no prazo máximo de 2 horas, devendo ser integrado com o sistema de monitorização da AMA se a tecnologia o permitir;
    iii) Energia elétrica AC/DC socorrida com UPS, bem como gerador diesel e redundância de UPS;
    iv) Climatização e refrigeração – AVAC, incluindo ar condicionado industrial com condutas corta-fogo, detetor e regulador de humidade do ar e redundância de ar condicionado;
    v) Chãos falsos com esteiras para cablagem;
x. Informar a AMA das regras de uso do Centro de Dados;
y. Manter o sigilo e a confidencialidade da informação respeitante aos equipamentos e aplicações informáticas, bem como a quaisquer dados e conhecimentos específicos, de qualquer natureza, da plataforma tecnológica a alojar;

z. Assumir a responsabilidade por quaisquer danos que a AMA venha a sofrer por causa imputável às condições de alojamento no Centro de Dados;

aa. Conceder apoio na remoção da plataforma tecnológica alojada após a cessação da vigência do presente Protocolo, e apresentar plano de remoção com detalhe e cronograma.

3. O Centro de dados deve cumprir com o regulamento RGPD e legislação Portuguesa e Europeia, em todas as suas vertentes nomeadamente tendo em consideração a natureza especialmente relevante do tratamento de dados biométricos de cidadão portugueses.

4. A entidade deverá ser capaz de disponibilizar e implementar, em caso de necessidade manifestada pelo adjudicante, a infraestrutura física em instalações **que obedeçam às regras e boas práticas definidas por Certificação** Tier III (nível 3), devendo apresentar as evidências para o efeito, no âmbito da proposta.

k) Manutenção Evolutiva - Bolsa de horas

a. Para a manutenção evolutiva deve ser incluído um pacote de 500 horas. Estes serviços de manutenção evolutiva poderão incluir a implementação de novas funcionalidades, a alteração das existentes ou a implementação de novos processos (além dos previstos neste Caderno de Encargos).

b. A manutenção evolutiva apenas é executada após aceitação expressa da entidade adjudicante.

2.2. Lote 2

No âmbito do presente fornecimento pretende-se o fornecimento de software de adesão biométrica a identidade digital (API e SDK), incluindo validação de segurança de documentos de identificação, reconhecimento facial, deteção de vida (“liveness”) que assegure os seguintes requisitos:

i) Requisito global a todos os motores descritos nos pontos a seguir

Todos os motores propostos deverão ser integráveis e utilizáveis “on Prem”, isto é, deverão ser capazes de ser instalados e integrados no datacenter definido e indicado pela AMA (que estará indicado na proposta adjudicadado Lote 1). Soluções que estejam, portanto, alojadas remotamente em serviços cloud ou outros, acessíveis por via de API’s e que não possam ser integrados “on prem”, não serão considerados. Estes softwares também deverão ser disponibilizados ou passiveis de ser integrados em SDK para serem disponibilizados em android, iOS e Web.

ii) Verificação de presença de vida (liveness)

1. Requisitos Gerais

a. Capacidade de Deteção de Liveness em 3D: A solução deve utilizar técnicas avançadas de deteção de profundidade e análise de textura para diferenciar entre um ser humano real e uma representação falsa.
b. Neste processo deve ser assegurado a medida da profundidade 3D não dependendo de movimentos laterais efetuados pelo utilizador com a sua cabeça ou com os seus olhos, geralmente designada por Liveness "ativo", devendo por isso recorrer a técnicas alternativas que permitam construir um mapa 3D da face da pessoa.
c. Resistência a Ataques via Deepfake e Injeção de Vídeo: A tecnologia deve ser capaz de detetar e rejeitar deepfakes e tentativas de spoofing que utilizem vídeos ou imagens manipuladas. Neste campo valoriza-se a realização de testes de penetração recorrentes e mecanismos de incentivo para entidades especialistas terceiras tentarem "quebrar" a segurança.
d. Compatibilidade com Diversos Dispositivos: Deve funcionar em uma ampla gama de dispositivos, incluindo smartphones, tablets e computadores, sem depender de hardware específico.

2. Requisitos Técnicos

a. SDK Integrável no Dispositivo: A solução deve incluir um kit que possa ser integrável num SDK para que que possa ser integrado em aplicativos dos clientes para acesso e verificação biométrica.
b. Alta Precisão em Condições Variadas: Eficiência comprovada sob diferentes condições de iluminação e contra várias técnicas de spoofing, como fotos, vídeos e máscaras.
c. Certificações de Segurança: Deve atender ou exceder os padrões de segurança biométrica estabelecidos por organismos como ISO e IEC, especialmente ISO/IEC 30107-3 para deteção de apresentação de ataques, nível 1 e nível 2, ou equivalente (com certificação válida e obtida há menos de 18 meses).

3. Requisitos de Conformidade e Privacidade

a. Conformidade com GDPR e Outras Regulamentações de Privacidade: A solução deve garantir que os dados biométricos sejam processados e armazenados conforme as leis de proteção de dados aplicáveis.
b. Transparência no Processamento de Dados: Deve fornecer logs detalhados e auditáveis de todas as verificações de liveness para monitorização e análise de conformidade.

4. Requisitos de Desempenho

a. Baixa Taxa de Falsa Rejeição (FRR): Minimizar os casos em que usuários legítimos são incorretamente rejeitados.

b. Baixa Taxa de Aceitação Falsa (FAR): Maximizar a capacidade do sistema de rejeitar impostores e não aceitar identidades falsas como legítimas.

5. Requisitos de Evolução

a. Atualizações Regulares para Combater Novas Técnicas de Spoofing: A solução deve ser atualizada regularmente para proteger contra novas vulnerabilidades e técnicas de spoofing.

6. Requisitos de Usabilidade

a. Interface de utilizador Amigável: A solução deve ser fácil de usar para os utilizadores finais, com instruções claras e feedback imediato durante o processo de verificação de liveness. Não devem ser feitos pedidos movimentos específicos dos olhos ou da face do utilizador, nomeadamente pedidos para piscar olhos ou rodar a cabeça lateralmente.

Tempo de Resposta Rápido: A deteção de liveness deve ser concluída em poucos segundos para garantir uma boa experiência do usuário sem sacrificar a segurança

iii) Comparações de Fotografia

1. Foto visível no Cartão com a selfie
   a. O software fornecido deve assegurar a comparação da imagem de baixa resolução da fotografia constante no cartão de cidadão disponibilizada pelo IRN, com a imagem extraída do processo de prova de vida (liveness).
   b. Deve ser possível guardar foto resultante do processo de prova de vida, com a opção de remover o fundo da foto, substituindo por uma cor neutra a definir, cumprindo com os requisitos ICAO no que concerne a fotos em documentos de identificação.
   c. Taxa de falsos positivos (False accept rate - FAR) inferior ou igual a 1/1 000 000, com taxa de falsos negativos (False reject rate - FRR) inferior a 1%. (True acceptance rate - TAR superior ou igual a 99%).
2. Comparação da Foto na Base de dados com selfie
   a. O software fornecido deve assegurar a comparação da fotografia de alta resolução recolhida aquando do pedido de Cartão de Cidadão com a imagem extraída do processo de prova de vida(incluindo a deteção de gémeos)
   b. Taxa de falsos positivos (False accept rate - FAR) inferior ou igual a 1/10 000 000, com taxa de falsos negativos (False reject rate - FRR) inferior a 2%. (True acceptance rate - TAR superior ou igual a 98%).

   A Solução de comparação de fotos deve ser avaliada por entidade de referência independente ou de laboratório devidamente creditado (e.g., NIST, IARPA, WIDER, ENISA), mostrando evidência dessa análise através de Relatório emitido pela entidade ou laboratório respetivos.

iv) OCR Cartão de Cidadão e verificação de segurança Cartão de Cidadão (CC)

O software fornecido deve assegurar a recolha de todos os dados constantes do Cartão de Cidadão (CC) e uma verificação de segurança, nomeadamente assegurando:

1. Identificação de fotocópias a cores de elevada resolução (de cartão original).
2. OCR de todos os dados constantes do Cartão (letras, algarismos e símbolos)
3. Comparação dados contantes na MRZ com restantes dados do CC
4. Recolha de fotografia constante do Cartão (em formato compatível com mecanismo de comparação de fotos, mais à frente descrito).
5. Verificação de mecanismos base de segurança, incluindo
   c. sobreposição de microtexto,
   d. presença de símbolos base de Cartão de Cidadão,
   e. verificação da presença de presença e autenticidade dos mecanismos de segurança ótica (incluindo DOVID e filete holográfico)
   f. verificação de presença de todos os campos
   g. Deteção de adulteração do Cartão (e.g., alteração de dados impressos, alteração de fotografia)
6. Para utilização durante o fluxo onde é efetuada o onboarding via Entrevista de Vídeo é necessário que sejam efetuadas as validações de segurança a outros documentos distintos do Cartão de Cidadão, nomeadamente Passaportes, Título e Cartão de Residência e cartões de identificação dos outros Estados Membros da EU e da Ucrânia.

   Assim, o software deve receber 2 fotografias da frente e verso (onde se aplica) do documento e devolver todos os dados constantes do documento, bem como uma indicação do nível de fidedignidade do documento.

v) NFC (Near-Field Communication)

O software deverá incluir o uso de tecnologias NFC para identificar o utilizador final, utilizando os dados extraídos do seu documento de identificação. Este método fornece uma camada adicional de segurança ao eliminar a possibilidade de ataques sintéticos, garantindo que apenas documentos autênticos sejam validados, facilitando uma verificação rápida e precisa da identidade do utilizador através da leitura direta de cartões ou documentos equipados com chips NFC.

vi) Autenticação biométrica

Autenticação recorrendo a biometria (verificação de presença de vida e verificação facial), tendo por base vetor biométrico. Deve ser criado vetor biométrico (aquando da 1ª utilização do sistema, com execução de liveness e verificação facial com comparação de fotografia constante de sistema central ou obtida por NFC do documento de identificação) que deverá ser usado em processos de autenticação posterior – onde deve ser feita a verificação facial e o liveness 3D (sem necessidade de leitura da fotografia de alta resolução constante da base de dados ou do documento de identificação, nessas autenticações posteriores).

vii) Outros (Valorativo)

São ainda valorizadas propostas que, opcionalmente, incluam (para uso ilimitado, em casos de uso inovadores) os seguintes requisitos:

- Inclusão de software de autenticação passiva por voz, independente do idioma (uso ilimitado durante o contrato) com certificação iBeta Level 1 Presentation Attack Detection (PAD) de acordo com ISO/IEC 30107-3
- Funcionalidade de verificação de idade (com base em captura de selfie-video)
- Funcionalidade de liveness pode ser configurado para funcionamento em modo passivo ou ativo
- Software com possibilidade de geração de QRCode, com base em vetor biométrico, irreversível, e comparação com imagem capturada posteriormente.
- Software integrado com liveness que possibilite a remoção de fundo de fotografias
- Software integrado com liveness que possibilite a validação de requisitos ICAO para fotografias a colocar em documentos de viagem (e.g., Cartão de Cidadão, passaporte) e correção de fotografia automatizado, sempre que aplicável (e.g., alteração de zoom para assegurar distância entre olhos, endireitar rosto, etc.)

Dimensionamento Solução (Lote 1 e Lote 2)

Para fins de dimensionamento das soluções a fornecer nos lotes 1 e 2, devem ser consideradas as seguintes métricas para os diferentes casos de uso identificados (métricas referentes a adesões, ativações ou utilizações com sucesso).

Caso de Uso/Métrica	ano 1	ano 2	ano 3	Total
Nº adesões CMD ou ativações certificados CC app	800 000	960 000	1 152 000	**2 912 000**
Nº adesões CMD por Video-Chamada	1 000	1 200	1 440	**3 640**
Verificação de identidade regular do Titular de CMD	80 000	100 000	120 000	**300 000**
Nº autenticações CMD biometria	1 500 000	4 950 000	9 075 000	**15 525 000**
Nº utilizadores unicos com vetor biométrico (em cada ano)	960 000	1 152 000	1 382 400	**3 494 400**
Pedido, renovação ou entrega de Cartão de Cidadão ou passaporte	12 000	240 000	480 000	**732 000**
Prova de Vida para fins de benefícios e pensões	-	25 000	50 000	**75 000**
Outros		50 000	100 000	**150 000**

Note-se que estes valores são meramente indicativos não devendo ser usados para colocar limitações ao âmbito e termos do fornecimento e licenciamento solicitado neste CE

3. Licenciamento e Suporte (Lote 1 e Lote 2)

Pretende-se um licenciamento para utilização ilimitada por parte da Administração Pública Portuguesa, para todos os componentes de software para a total duração do contrato (lote 2) ou perpétuo (lote 1), incluindo:

1. Licença de utilização ilimitada da plataforma de orquestração (lote 1) nas várias componentes ((API e SDK), videoconferência, motor de modelação de fluxos biométricos e integração com os softwares de providers biométricos) e para os componentes de software de validação de identidade (lote 2) (incluindo validação de segurança de documentos de identificação, verificação facial, deteção de vida, e autenticação biométrica)
2. Permanente atualização das versões de software, incluindo sistema operativo, software base (com sistemas de gestão de BD, servidores aplicacionais ou outros) e software específico fornecido.
3. Guarda e armazenamento das entrevistas de vídeo (lote 1)
4. Manutenção preventiva e corretiva.
   a. Entende-se por manutenção preventiva e corretiva o conjunto das ações efetuadas pelo adjudicatário de forma a corrigir quaisquer erros, anomalias ou incorreções, incluindo revisões preventivas, manutenção remota e reparação de avarias, assegurando um tempo de reposição do serviço de acordo com o especificado mais à frente, nesta secção.
   b. Entende-se por tempo de reposição do serviço a soma do "tempo de resposta" e do "tempo de reparação".
   c. Entende-se por tempo de resposta o prazo compreendido entre a comunicação da anomalia ao Adjudicatário (por telefone, ou email) e o início da sua reparação.
   d. Entende-se por tempo de reparação o prazo compreendido entre o início da intervenção e a reposição completa do serviço em funcionamento.
   e. Tendo em conta os pontos anteriores, os concorrentes deverão considerar na proposta apresentada os serviços suporte e de manutenção preventiva, e corretiva, incluído no preço da proposta assegurando os SLA definidos na tabela seguinte (Em período 24x7), de acordo com nível de prioridade definido pela AMA:

Nível de Prioridade	Exemplo	Tempo resposta	Tempo reposição
Baixo	Problema que afeta menos de 1% dos pedidos	24 horas	5 dias uteis
Médio	Problema que afeta até de 10% dos pedidos	2 horas	4 horas
Elevado	Serviço indisponível, Problema que afeta mais de 10% dos pedidos	30 minutos	1 hora

Cláusula 16.ª

Requisitos específicos de implementação para o tratamento de dados pessoais

1. No âmbito dos trabalhos a desenvolver e sempre que aplicável, o cocontratante obriga-se a garantir:

a) Gestão de permissões para os vários utilizadores que permita uma gestão ao nível de cada dado pessoal;

b) Funcionalidades que permitam:

1. Mascarar dados sensíveis de acordo com o nível de permissões do utilizador;
2. Apagamento, consulta, alteração/atualização, exportação/portabilidade dos dados;
3. Encriptação de dados sensíveis.

c) Estruturas de dados que permitam:

i) Implementação de um modelo de dados que contemple categoria, finalidade, consentimento, fundamento, bem como outros atributos relacionados, e permita estabelecer as relações necessárias;

ii) Registo dos tempos de retenção por finalidade.

d) Desenho de interface que permita:

i) Pesquisas por dados isolados assegurando a segregação por titular dos dados e/ou atributos;

ii) Informação e recolha de consentimento de forma contextualizada com a funcionalidade/página que procede à utilização dos dados pessoais.

e) Mecanismos de registo de utilizador/data/hora de atividades CRUD (*Create*, *Read*, *Update*, *Delete*) sobre dados pessoais;

f) Procedimentos automáticos para garantir que findo o período de retenção, os dados serão anonimizados, eliminados, encriptados ou renovado o período de retenção, e recolhido o consentimento caso seja aplicável, dependendo da finalidade ou fundamentação existente para a sua retenção;

g) Segurança de redes e sistemas de informação em conformidade com os requisitos obrigatórios previstos no anexo da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, sempre que aplicáveis;

2. A arquitetura da solução de acordo com estes e restantes requisitos deverá ser apresentada e detalhada nos entregáveis das várias fases que compõem o projeto, sujeitos à aprovação da AMA.

3. Nos entregáveis deverá estar incluído um documento de "Conformidade com o RGPD", no qual o cocontratante deve incluir o inventário de dados pessoais sujeitos a tratamento pela solução e sua categorização, funcionalidades, estruturas de dados e mecanismos de segurança implementados, bem

como, a forma de cumprimento dos requisitos estabelecidos como obrigatórios previstos na alínea g), justificando os casos de não aplicabilidade.

4. Os seguintes requisitos serão assegurados pelo adjudicatário:

a) Pela natureza especialmente sensível da informação tratada no caso específico da CMD, a entidade e os elementos envolvidos na implementação, acompanhamento e desenvolvimento de todos os componentes de software associados, devem ter acreditação de segurança do GNS ou em processo de acreditação em curso. Neste sentido, é requerido que sejam fornecidas evidências que comprovem o solicitado.

5. Os seguintes requisitos serão assegurados pela AMA:

a) Análise de vulnerabilidades no contexto da cibersegurança, sendo a sua correção da responsabilidade do cocontratante;

b) Implementação de protocolos de segurança TLS (*Transport Layer Security*) fornecendo os certificados digitais, desde que o alojamento do sistema/aplicação/portal seja em infraestrutura gerida pela entidade contratante;

c) Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas *firewalls*, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Web Application Firewall* (WAF), etc.);

d) Fornecimento de VPN para acesso remoto aos sistemas;

e) Segurança de DNS e correio eletrónico;

f) Backups com redundância geográfica.

Cláusula 17.ª

Acessibilidade e usabilidade

1. No âmbito dos trabalhos a desenvolver, o cocontratante obriga-se a garantir que os entregáveis que são objeto deste procedimento cumprem as obrigações legais, os requisitos e as melhores práticas no que se refere às áreas da Acessibilidade, Usabilidade e Experiência de Utilização dos sítios Web e das aplicações móveis, nomeadamente os seguintes fatores essenciais:

a) Cumprimento do Decreto-Lei n.º 83/2018, de 19 de outubro, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/2102, do Parlamento Europeu e do Conselho, de 02 de dezembro de 2016, relativa à Acessibilidade dos sítios Web e das aplicações móveis dos organismos do setor público, nomeadamente o nível de conformidade "AA" das WCAG 2.1 do W3C, que equivale à norma europeia EN 301 549 harmonizada;

b) Elaboração da Declaração de Acessibilidade e Usabilidade prevista nos Artigos 8.º e n.º 5 do artigo 9.º do Decreto-Lei n.º 83/2018, bem como as respetivas evidências, nos termos estipulados no

referido diploma legal e nos sítios Web https://selo.usabilidade.gov.pt/index.html e http://www.acessibilidade.gov.pt;

c) Cumprimento do Regulamento Nacional de Interoperabilidade Digital (RNID), estabelecido nos termos do artigo 5.º da Lei n.º 36/2011, de 21 de junho, e aprovado através da Resolução do Conselho de Ministros n.º 91/2012, de 08 de novembro, alterado pela Resolução do Conselho de Ministros n.º 2/2018, de 5 de janeiro, na redação conferida pelo Decreto-Lei n.º 83/2018, nomeadamente quanto à alteração da Tabela III "Tecnologias de interface Web, incluindo acessibilidade, ergonomia, compatibilidade e integração de serviços";

d) Cumprimento dos requisitos do Selo de Usabilidade e Acessibilidade e respetiva aposição, de acordo os parâmetros definidos no sítio Web https://selo.usabilidade.gov.pt/, devendo garantir, em conjunto com a Declaração de Acessibilidade e Usabilidade, o nível mínimo de Selo Bronze https://selo.usabilidade.gov.pt/bronze.html;

e) Cumprimento das melhores práticas de Acessibilidade, Usabilidade e Experiência de Utilização coligidas nos sítios Web http://www.acessibilidade.gov.pt/, https://usabilidade.gov.pt/menu-interior e https://selo.usabilidade.gov.pt/bronze.html, em articulação com a Equipa de Experiência Digital, da Direção de Transformação Digital da AMA.

Cláusula 18.ª

Planeamento

1. Deve ser entregue um plano detalhado de implementação de todos os serviços propostos.
   i. A Plataforma de orquestração biométrica (Lote 1), devidamente configurada (incluindo motor de fluxos, SDK iOS e Android, WebSDK, integração com softwares biométricos do lote 2, Videoconferência e vídeo auto-gravado e casos de uso) deve ser disponibilizada no prazo máximo de 90 dias após celebração de contrato.
   ii. Os Softwares de validação de identidade (lote 2) devem ser deve ser disponibilizada no prazo máximo de 30 dias após celebração de contrato.
2. Este plano deve ter suporte gráfico ("gráfico de Gantt") e descrição em texto de cada etapa e respetivas sub-etapas que compõem o plano.

Cláusula 19.ª

Entregáveis e documentação

O adjudicatário entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital:

a. Documentação de APIs das várias componentes do software disponibilizado;
b. Relatório mensal referente aos serviços prestados, incluindo níveis de serviço assegurados;
c. A AMA poderá proceder à reprodução de todos os documentos referidos no número anterior (para os fins que assim o entender).

Cláusula 20.ª

Gestor do contrato

1. O gestor do contrato, com a função de acompanhar permanentemente a execução contratual, nos termos e para os efeitos previstos no artigo 290.º-A do CCP, será designado pela AMA no contrato.

2. O cocontratante deverá indicar a pessoa na sua organização que será responsável pela execução do contrato, e que será o interlocutor com o gestor do contrato designado pela AMA, bem como a pessoa responsável pelo tratamento de dados pessoais.

3. No âmbito do presente contrato, a AMA, através do gestor do contrato designado nos termos do número 1., procederá à avaliação do cocontratante, de acordo com a matriz de avaliação de que se encontra disponibilizada no site institucional da AMA, em: https://www.ama.gov.pt/

Cláusula 21.ª

Mecanismos formais de acompanhamento

No âmbito do presente procedimento o adjudicatário deverá respeitar a orgânica indicada na sua proposta para a realização dos trabalhos e a coordenação conjunta do projeto com a AMA, incluindo os diversos níveis, tendo em consideração os seguintes requisitos:

a. Todos resultados produzidos pelo adjudicatário no âmbito do presente fornecimento deverão ser alvo de aceitação por parte da AMA;
b. A AMA terá um prazo de 2 semanas para se pronunciar em relação aos resultados apresentados pelo adjudicatário.
c. No caso da não-aceitação, por parte da AMA, dos resultados, deverá o adjudicatário (num prazo inferior a 5 dias) proceder às alterações necessárias para nova análise da AMA (nos termos supra).