

**CONCURSO PÚBLICO INTERNACIONAL N.º 102/2025/DCP/NGP/AQUISIÇÃO
DE SERVIÇOS DE CONSULTORIA NO ÂMBITO DA CONFIANÇA DIGITAL,
IDENTIDADE ELETRÓNICA E INFRA-ESTRUTURA PKI DE SUPORTE À
DESMATERIALIZAÇÃO DE FATURAÇÃO**

CADERNO DE ENCARGOS

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir nos contratos a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por “AMA”), na sequência de procedimento pré-contratual que se encontra dividido em 2 lotes e tem por objeto a aquisição de serviços de consultoria no âmbito da confiança digital, identidade eletrónica e infra-estrutura PKI de suporte à desmaterialização de faturação, melhor descrito nas cláusulas técnicas e anexos neste procedimento.
2. Para execução das Medidas PRR acometidas à AMA e para apoio à desmaterialização da faturação, pretende-se a contratação dos serviços de consultoria, de acordo com os lotes seguintes:
 - a) O **Lote 1** consiste na contratação de serviços de desenvolvimento e auditoria de infra-estruturas PKI e identidade digital para suporte a assinaturas qualificadas de faturas eletrónicas.
 - b) O **Lote 2** consiste na contratação de serviços para consultoria e governação de soluções eID e certificação eletrónica para massificar a faturação digital.
3. Os interessados podem concorrer para um ou ambos os lotes.

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, conforme venha a ser estabelecido entre as partes, em sede de execução contratual.

Cláusula 3.ª

Duração

1. Os contratos, correspondentes a cada um dos lotes, produzem os seus efeitos a partir do dia seguinte da data da sua celebração ou após a obtenção de visto de conformidade do Tribunal de Contas, quando aplicável, e cessam a 30 de junho de 2026, ou antes se esgotado o seu valor, sem

prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

2. Todos os contratos poderão cessar antes das datas prevista nos números anteriores se atingido o preço contratual previsto no n.º 1 da cláusula 4.ª.

Cláusula 4.ª

Preços contratuais e preços base unitários

1. O preço contratual é de 507.414,00 €, valor ao qual acresce o IVA à taxa legal em vigor, o qual se encontra dividido nos seguintes lotes:
 - a. Para o **Lote 1** o preço contratual é de 207.279,00 €, com valor estimado de 50% (103.639,00 €) em 2025 e 50% (103.639,00 €) em 2026.
 - b. Para o **Lote 2** o preço contratual é de 300.135,00 €, com valor estimado de 50% (150.067,00 €) em 2025 e 50% (150.067,00 €) em 2026.
2. Os preços contratuais de cada lote serão consumidos de acordo com os seguintes preços base por hora e por perfil e lote:

Lote 1

| Perfil | FTES | Horas Estimadas | Preço base por hora |
|------------------------------------|-------------|------------------------|----------------------------|
| Consultor tecnológico estratégico | 1 | 525 | 71,55 € |
| Consultor tecnológico Júnior | 1 | 500 | 40,07 € |
| Software developer EUDI Wallet | 1 | 500 | 40,07 € |
| Software developer Java e Python | 1 | 1000 | 40,07 € |
| Devop ou administrador de sistemas | 1 | 500 | 53,23 € |
| Consultor Tecnológico Auditorias | 1 | 500 | 62,96 € |
| Gestor de Projeto | 1 | 500 | 62,96 € |

Lote 2

| Perfil | FTEs | Horas Estimadas | Preço base por hora |
|---------------------------------------------------|-------------|------------------------|----------------------------|
| Coordenador / Arquiteto de Sistemas de Informação | 1 | 1595 | 74,41 € |
| Gestor de Projeto | 1 | 1585 | 62,96 € |
| Consultor funcional / de gestão | 1 | 1585 | 51,52 € |

3. Pela prestação dos serviços objeto dos contratos, constantes do presente caderno de encargos, a AMA deve pagar ao cocontratante o valor resultante da aplicação dos preços unitários hora, apresentados na proposta, aos serviços efetivamente prestados, acrescido de IVA à taxa legal em vigor, se este for legalmente devido, até perfazer o preço contratual, acrescido de IVA à taxa legal em vigor.
4. Os valores contratuais referidos para cada um dos lotes no ponto anterior não são submetidos à concorrência.
5. Aos valores previstos nos números anteriores, acresce o valor do IVA à taxa legal em vigor.
6. As horas indicadas por perfil em cada um dos lotes são uma estimativa, podendo as mesmas sofrer ajustes para mais ou menos horas conforme o desenvolvimento do projeto objeto do presente procedimento.
7. Em sede de execução, e caso se verifique necessidade, poderá a AMA solicitar mais FTE´s do que os previstos nas tabelas supra.
8. São excluídas as propostas cujo valor seja superior a qualquer um dos preços base unitários indicados no número 3.
9. A AMA não fica vinculada ao consumo da bolsa de horas não advindo da ausência de consumo das mesmas quaisquer responsabilidades ou direito a indemnização a qualquer título.
10. O preço referido no n.º 1 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.
- e) Todos os encargos derivados da apresentação da proposta, assinatura do contrato, prestação de garantias e seguros são da responsabilidade do cocontratante, incluindo, caso seja concedido o Visto, se aplicável, os emolumentos devidos ao Tribunal de Contas.

Cláusula 5.ª

Condições de pagamento

1. A faturação deverá ser mensal, após validação pela AMA dos relatórios mensais de consumo de horas e serviço efetivamente prestado e aceite.
2. 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.
3. As faturas devem discriminar os serviços a que se reportam (incluindo o número de horas por perfil), o número do contrato bem como o número de compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.
4. Caso as faturas apresentadas não sejam validadas pela AMA, esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
5. 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.
6. Só serão devidos os valores referentes aos serviços efetivamente prestados e aceites nos termos do presente caderno de encargos.
7. O pagamento será realizado para o NIB/IBAN indicado em documento bancário apresentado pelo cocontratante o qual deverá ser atualizado sempre que necessário.
8. 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.
9. Todos os encargos derivados da apresentação da proposta, assinatura do contrato, prestação de

garantias e seguros correm por conta do cocontratante, incluindo, caso seja concedido o Visto, os emolumentos devidos ao Tribunal de Contas, quando aplicável.

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, ambos 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 sempre que solicitados, no prazo máximo de 5 dias úteis, 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.

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), e da Lei n.º 58/2019, de 08 de agosto 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 não pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da 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 de qualquer dos objetivos e atividades previstas na alínea c) do n.º 7 da cláusula 16.ª, poderá ser aplicada uma sanção pecuniária no montante de 10% do preço a pagar na fatura seguinte;
 - b) Pelo incumprimento do prazo previsto no n.º 6 da cláusula 19.ª, poderá ser aplicada uma

- sanção pecuniária no montante de 1.520,00 €, por cada dia de atraso;
- c) Pelo incumprimento do prazo previsto no n.º 1 da cláusula 20.ª, poderá ser aplicada uma sanção pecuniária no montante de 1.520,00 €, por cada dia de atraso;
 - d) Pelo incumprimento do prazo previsto no n.º 2 da cláusula 20.ª, poderá ser aplicada uma sanção pecuniária no montante de 720,00€, por cada dia de atraso;
 - e) Pelo incumprimento das regras para substituição dos recursos previstas no n.º 6 da cláusula 20.ª, poderá ser aplicada uma sanção pecuniária no montante de 1% do preço contratual, por cada dia de incumprimento;
 - f) Pelo incumprimento do prazo previsto na cláusula 21.ª, poderá ser aplicada uma sanção pecuniária no montante de 1.520,00 € por cada dia de atraso;
 - g) Pelo incumprimento de qualquer dos mecanismos de acompanhamento previstos no n.º 5 e 6 da cláusula 23.ª, poderá ser aplicada uma sanção pecuniária no montante de 10% do preço a pagar no mês em que ocorre o incumprimento;
 - h) Pelo incumprimento de qualquer dos prazos previstos nos n.ºs 7 e 8 da cláusula 25.ª, poderá ser aplicada uma penalidade no montante de 720,00€, por cada dia de atraso;
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 correspondente.
 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, salvo nos casos previstos no n.º 3 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 12.ª

Direito de Retenção

Quando não tenha sido exigida a prestação de caução, caso se revele pertinente, a AMA poderá proceder à retenção de 10% do valor dos pagamentos a efetuar, tendo em vista a garantia da perfeita e tempestiva execução do contrato, nos termos do disposto no n.º 3 do artigo 88.º do Código dos Contratos Públicos.

Cláusula 13.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 14.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 15.ª

Legislação aplicável

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

CLÁUSULAS TÉCNICAS

Cláusula 16.^a

Descrição técnica do contrato

1. Os serviços a prestar em cada lote encontram-se descritos no Anexo II deste documento.
2. Os serviços a prestar em cada lote serão desenvolvidos por uma equipa técnica do fornecedor, coordenada por um Diretor de Projeto, a qual terá uma dimensão variável, em função das necessidades e prioridades estabelecidas pela AMA, no âmbito do exercício dos seus poderes de direção e fiscalização, nos termos dos artigos 303.º e seguintes do CCP.
3. O fornecedor deverá seguir as regras e normas vigentes na AMA no âmbito da qualidade, planeamento e gestão de projetos, devendo-lhe ser facultadas no início dos trabalhos.
4. O fornecedor garantirá a qualidade dos serviços de acordo com os padrões exigíveis e em conformidade com o Sistema de Gestão da Qualidade em vigor na AMA.
5. O fornecedor obriga-se a prestar à AMA todos os esclarecimentos e informações necessárias ao conveniente acompanhamento da execução do contrato.
6. Para o acompanhamento da execução do contrato, o fornecedor fica obrigado a manter, com uma periodicidade a acordar com a AMA em sede de execução do contrato, reuniões de coordenação com os representantes por ela designados para o efeito.
7. A governação e gestão de horas deverá ser feita de acordo com os seguintes momentos:
 - a) Apresentação do planeamento do trabalho a realizar pela equipa do fornecedor de acordo com os marcos e metas definidos pela AMA.
 - b) O plano referido no ponto anterior deve estar organizado por blocos de intervalo temporal entre 2 e 4 semanas (interações), detalhando as atividades a realizar por cada um dos elementos da equipa, a estimativa de horas dessas atividades e os respetivos entregáveis, em modelo fornecido pela AMA.
 - c) O plano de trabalho de cada interação deve ser entregue até 5 dias úteis antes do seu respetivo início e obter a aprovação por parte do responsável do projeto por parte da AMA.
 - d) No final de cada interação, haverá lugar à revisão do trabalho realizado face ao seu planeamento inicial, na qual serão avaliados os resultados esperados e o desempenho dos serviços.

- e) Caso o fornecedor exceda o total de horas aprovado pela AMA em cada iteração, esse desvio deverá ser justificado pelo fornecedor e este poderá não ser aceite se exceder em 20% o total de horas previsto por razões exclusivamente imputáveis a este último não sendo devido o pagamento dessas horas.
 - f) Caso não atinjam os dos resultados esperados a AMA poderá solicitar a substituição de recursos, conforme descrito na Cláusula 20.^a.
8. O esforço, o número de recursos e as horas estimadas, corresponde ao identificado em cada um dos perfis por lote, sem prejuízo de adaptação em sede de execução, de acordo com as necessidades da AMA. A AMA, pode determinar, a alteração dos recursos afetos ao contrato, em caso de insuficiência dos resultados, da incapacidade revelada ou da necessidade na execução do objeto do presente procedimento.
9. Todos os relatórios, registos, comunicações, e demais documentos elaborados pelo fornecedor devem ser integralmente redigidos em português. Adicionalmente, a AMA poderá solicitar a sua tradução para língua inglesa, sendo o cocontratante responsável pelos custos inerentes.

Cláusula 17.^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:
 - i) Mascaram dados sensíveis de acordo com o nível de permissões do utilizador;
 - ii) Apagamento, consulta, alteração/atualização, exportação/portabilidade dos dados;
 - iii) 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;
 - h) Uma estrutura multicamada, composta pelas camadas de Apresentação ou *Front-end* (FE), Aplicacional (APP) e Base de dados (BD).
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 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) Detecção 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 18.^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, ambos do Decreto-Lei n.º 83/2018, de 19 de outubro, 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, de 19 de outubro, 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;
 - 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/>, em articulação com a Equipa de Experiência Digital, da Direção de Transformação Digital da AMA.

Cláusula 19.^a

Perfis técnicos dos recursos a afetar aos serviços

1. Os perfis, número mínimo estimado de FTE's por perfil e horas estimadas por perfil de cada um dos lotes, estão descritos no Anexo II, em cada um dos lotes respetivamente.
2. O cocontratante pode propor a afetação do mesmo recurso em diversas prestações de serviços, nomeadamente para diferentes perfis e diferentes lotes, desde que cumpra os requisitos mínimos dos perfis para o qual o recurso foi proposto.
3. Em sede de análise de propostas, caso a aplicação do modelo de avaliação determine a adjudicação ao mesmo concorrente de ambos os lotes, para os quais tenha indicado o mesmo recurso, caso o somatório do número mínimo de FTE's por perfil proposto seja superior ao número de FTE's previsto no Anexo II, será adjudicada a proposta que se encontre ordenada em primeiro lugar na declaração de ordem de preferência dos lotes apresentada pelo Concorrente, sendo as restantes propostas excluídas, na medida em que o recurso proposto e que será afeto à execução do contrato se encontre impossibilitado de assegurar a execução dos restantes contratos, por exceder os FTE's previstos.
 - a) O somatório do número mínimo de FTE's dos diferentes lotes e perfis aos quais o recurso foi afeto não pode ser superior a 1 (um), de acordo com o número mínimo de FTE's por perfil e por lote, indicado no Anexo II.
4. Os recursos do adjudicatário serão integrados em equipa de projeto da AMA e desenvolverão as suas atividades na sede da AMA ou remotamente, conforme definido pela AMA.
5. A AMA não fica vinculada ao consumo da bolsa de horas não advindo da ausência de consumo das mesmas quaisquer responsabilidades ou direito a indemnização a qualquer título.
6. Por cada recurso apresentado deve ser preenchida a ficha resumo conforme o modelo solicitado no programa de concurso para aferição do cumprimento de cada requisito (mínimo obrigatório e preferencial). Os recursos que não cumpram os requisitos mínimos obrigatórios levam à exclusão da proposta.
7. Após a celebração do contrato, o adjudicatário deverá entregar à AMA, no prazo máximo de 2 dias úteis, toda a documentação respeitante a cada um dos recursos que integram a equipa a afetar à

prestação de serviços, designadamente:

- a) Curriculum Vitae dos recursos propostos, evidenciando a experiência declarada na proposta do concorrente;
- b) Outros documentos que comprovem o cumprimento dos requisitos, que foram submetidos com a proposta nos termos do artigo 8.º, n.º 2, alínea c) do Programa de Concurso. Para este efeito, a AMA poderá solicitar a entrega de documentos que comprovem a experiência declarada em fase de proposta.

Cláusula 20.ª

Alocação e substituição de recursos

1. A prestação dos serviços objeto do presente procedimento, deve ser iniciada no máximo até 10 dias úteis, a contar do início da execução do contrato.
2. Dentro do prazo referido no número anterior, devem ser alocados, no mínimo 50% dos FTE's de acordo com a proposta do adjudicatário, devendo os restantes recursos ser alocados no máximo até 1 mês a contar da data de doo início da execução do contrato.
3. Qualquer alteração à composição da equipa deve ser previamente comunicada à AMA e dependente da sua aceitação formal.
4. Logo após a celebração do contrato, a substituição de alocação de recursos apresentados em sede de proposta, ou a alocação de novos recursos só será aceite caso reúna os requisitos mínimos exigidos em sede de cadernos de encargos para os perfis, devendo ser apresentados nomeadamente:
 - a. CV evidenciando de que forma o concorrente se propõe a cumprir com os requisitos mínimos e preferenciais definidos nas peças do procedimento. Para efeitos de avaliação dos requisitos associados a cada perfil não serão considerados aqueles que se limitem a transcrever a descrição que consta das peças do procedimento.
 - b. Cópia de todos os documentos comprovativos dos requisitos obrigatórios exigidos;
5. Durante a execução do contrato, perante a necessidade de substituição de recursos, apresentados nos termos do número anterior, deverão ser indicados recursos com os mesmos atributos avaliados e valorados em sede de proposta, devendo observar-se os prazos que se indicam no número seguinte.
6. No caso de alocação (sempre que a AMA verifique a necessidade de aumentar o n.º de FTE's previsto inicialmente) e substituição de novos recursos, que não os apresentados em fase de

formação do contrato, deverão ocorrer da seguinte forma:

- a) O cocontratante deverá, em 5 dias úteis, identificar o seu melhor recurso considerando os requisitos mínimos e preferenciais do perfil previstos no caderno de encargos e obter a aceitação pela AMA;
 - b) O cocontratante deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço;
 - c) O cocontratante deverá assegurar a passagem de conhecimento para o novo recurso, durante um período mínimo de 10 dias úteis, de modo que este possa retomar de imediato as tarefas destinadas ao seu perfil.
7. Sempre que se constate a inadequação de algum elemento da equipa encarregue da execução dos serviços contratados, tendo em conta os requisitos exigidos e o comportamento comumente expectável, poderá a AMA exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

Cláusula 21.^a

Entregáveis e documentação

1. Todo o software e documentação deverão ser desenvolvidos de acordo com os padrões de qualidade definidos pela AMA e são entregues à AMA, sempre que solicitado no prazo máximo de 3 dias úteis.
2. Os entregáveis devem ser apresentados em formato digital editável (e, quando aplicável, nos formatos técnicos exigidos pela AMA) e acompanhados de manual técnico, registo de testes e evidências de conformidade com os requisitos de segurança, RGPD e acessibilidade previstos neste Caderno de Encargos.
3. A aceitação dos entregáveis está sujeita a validação pela AMA. Caso apresentem desconformidades, o adjudicatário dispõe de 5 dias úteis para proceder à respetiva correção, sob pena de se considerar verificado o incumprimento para todos os efeitos contratuais.
4. Incumprimento das obrigações de entrega:
 - a) A AMA pode recusar os entregáveis até à sua correção, não produzindo estes quaisquer efeitos enquanto não forem validados.
 - b) São suspensos os pagamentos relativos à fase ou atividade associada aos entregáveis em falta, até regularização satisfatória, nos termos da cláusula 5.^a.

c) Podem ser aplicadas penalidades contratuais previstas na cláusula 11.^a, graduadas em função da gravidade, número e impacto do atraso ou da não conformidade.

d) Se o incumprimento for reiterado ou causar sério prejuízo aos objetivos do contrato, a AMA poderá propor a sua resolução.

Cláusula 22.^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. O responsável pela execução do contrato, por parte da entidade cocontratante, deverá reunir semanalmente com o gestor de contrato da AMA, ou outra pessoa designada por este último, para acompanhamento dos serviços prestados.
4. O responsável pela execução do contrato, por parte da entidade cocontratante, deverá garantir a aplicação de mecanismos de monitorização da qualidade dos serviços prestados.
5. 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 23.^a

Mecanismos formais de acompanhamento

1. Deve ser produzido, pelo responsável pela execução do contrato do cocontratante, um relatório de progresso semanal das tarefas realizadas e respetivo consumo de horas, por recurso, de acordo com modelo proposto pela AMA.
2. Este relatório de progresso deve ser enviado ao gestor de contrato designado pela AMA, um dia antes da reunião de progresso semanal a realizar entre as partes para acompanhamento dos serviços.
3. Os recursos alocados à prestação do serviço devem participar nas reuniões diárias de

acompanhamento do projeto (daily meetings).

4. Todos os resultados produzidos pelo cocontratante deverão ser alvo de aceitação por parte da AMA;
5. A AMA terá um prazo de 5 dias úteis para se pronunciar em relação aos resultados dos serviços realizados;
6. No caso da não-aceitação, por parte da AMA, dos resultados dos serviços executados, deverá o cocontratante, num prazo inferior a 5 dias úteis, proceder às alterações necessárias para nova análise da AMA (nos termos supra).

Cláusula 24.ª

Gestão de Dados

1. O cocontratante deverá garantir que os entregáveis, objeto deste procedimento contemplem os mecanismos necessários para a gestão de dados de modo que os mesmos sejam guardados e disponibilizados à AMA em todo o ciclo de vida do produto.
2. Para os efeitos previstos no número anterior considera-se que “Dados” são:
 - a) eventos correspondentes a uma sequência de símbolos qualificáveis ou quantificáveis, não assumindo significado por si só, tendo por base, observações, medições, acontecimentos;
 - b) considerados o idioma de entrada para um computador, sendo a informação o resultado de saída;
 - c) estruturados, quando formatados, organizados numa estrutura predefinida, como por exemplo tabelas constituídas por linhas e colunas;
 - d) não estruturados, quando não possuem uma formatação predefinida;
 - e) qualquer texto ou algarismo, mesmo que possa não ser percecionado para o leitor, como são por exemplo dados para georreferenciação;
 - f) Independentemente do formato de entrega, todos os elementos registados e armazenados por um suporte digital devem ser complementados por um conjunto de informações que os ajudem a compreender, designados por Metadados, os quais podem ser estruturais, técnicos, descritivos, administrativos e de direitos;
 - g) Constituem exemplos de dados, algarismos, símbolos, texto, coordenadas, mensagens,

imagens, sons e vídeo.

3. O(s) formato(s) dos dados deve(m) ficar definidos no âmbito da execução do contrato tendo em consideração as características dos dados e as necessidades específicas a que se destinam, como por exemplo a georreferenciação.
4. Fica prevista a disponibilização de dados abertos no portal dados.gov.pt, excluindo-se todos os dados sujeitos ao regime legal de proteção de dados pessoais, bem como informação considerada sensível por parte da Entidade Adjudicante.

Cláusula 25.^a

Requisitos específicos de implementação para a segurança da informação

1. No decorrer da execução do contrato o fornecedor obriga-se a cumprir as políticas e procedimentos do SGSI sempre que estes se apliquem.
2. Cumprir o Procedimentos de desenvolvimento seguro englobado no SGSI, incluindo:
 - a) Na definição de requisitos incluir os requisitos de segurança e privacidade;
 - b) Não utilização de bibliotecas de terceiros sem prévia validação da AMA;
 - c) Revisão de código por outro membro da equipa de desenvolvimento outra equipa do fornecedor, antes da passagem da aplicação para testes;
 - d) Executar análise dinâmica à aplicação para verificação de problemas relativos a segurança;
 - e) Relatório de PDS com informação sobre componentes de segurança e cumprimento do procedimento de desenvolvimento seguro;
 - f) Relatório de testes à aplicação com inclusão dos testes relativos à componente de segurança antes da passagem a qualidade/produção.
3. O equipamento usado pelos consultores externos tem o Sistema Operativo atualizado, estão protegidos com sistemas antivírus e são regularmente verificados pelo fornecedor quanto à presença de *malware*.
4. Os equipamentos dos fornecedores que contenham informação da AMA de nível superior a público devem estar encriptados para proteção da informação em caso de perda ou roubo do equipamento.
5. O fornecedor fica sujeito a política de Gestão de fornecedores.

6. Os fornecedores só terão acesso à informação necessária para execução do projeto após esta ser disponibilizada pela AMA. O acesso à informação, nomeadamente ao código fonte, será dado mediante abertura de acessos individuais ao consultor, após efetuado o respetivo pedido pelo GP junto da DIT.
7. Durante a execução do contrato o fornecedor tem os seguintes prazos para resolução de vulnerabilidades encontradas nos sistemas de produção:
 - a) *Critical*: 5 dias seguidos;
 - b) *High*: 7 dias úteis;
 - c) *Medium*: 15 dias úteis;
 - d) *Low*: 40 dias úteis.
8. No período de garantia do contrato o fornecedor tem os seguintes prazos para resolução de vulnerabilidades encontradas nos sistemas de produção:
 - a) *Critical*: 10 dias seguidos;
 - b) *High*: 17 dias úteis;
 - c) *Medium*: 25 dias úteis;
 - d) *Low*: 50 dias úteis.
9. O fornecedor não pode negar uma auditoria relativamente às condições de desenvolvimento do projeto por parte dos seus consultores, caso esta seja requerida pela AMA.
10. Todos os consultores são obrigados a reportar qualquer incidente de segurança de informação que esteja relacionada com informação da AMA, de acordo com o Procedimento PR-005 Procedimento de Gestão de Incidentes.
11. No caso de ser um produto alojado em Cloud é obrigatório que conste da proposta apresentada, o local ou locais onde a informação possa ficar alojada e quais as certificações de segurança nacionais e internacionais que o local (físico e lógico) possui.

ANEXO I

Enquadramento e Contexto

1. Enquadramento

- a. A Agência para a Modernização Administrativa, I. P., abreviadamente designada por AMA, I. P., é um instituto público de regime especial, dotado de autonomia administrativa e financeira e património próprio. A AMA é o instituto público responsável pela promoção e desenvolvimento da modernização administrativa em Portugal, estando a sua atuação repartida por três eixos fundamentais: transformação digital, serviço público omnicanal e simplificação administrativa.
- b. Perspetiva-se que, em 2025, se persiga um conjunto de atividades alinhadas com o progresso e consolidação da melhoria dos serviços públicos, consonantes com as iniciativas de transformação digital presentes nos investimentos AMA que constam do Plano de Recuperação e Resiliência (PRR) robustecido pela reorganização efetuada e pelas novas competências adquiridas, sejam as referentes aos Territórios Inteligentes sejam as oriundas da extinta Estrutura de Missão Portugal Digital e cuja efetiva implementação importa assegurar. Por outro lado, em cumprimento do Decreto-Lei n.º 94/2024, de 28 de novembro - que procedeu à extinção, por fusão, do Centro de Gestão da Rede Informática do Governo (CEGER) - recairão sobre esta agência as competências do CEGER relativas à atividade de certificação eletrónica e de certificados digitais identificadores da qualidade de titular de alto cargo. Assim, passam a estar integradas na missão e atribuições da AMA as seguintes competências:
 - a. Emitir, no âmbito da atividade de certificação eletrónica, certificados digitais identificadores da qualidade de titular de alto cargo, ou outros de especial relevo, da Administração Pública, nos termos definidos pelo conselho gestor do Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas (SCEE);
 - b. Assegurar serviços de certificação temporal que permitam a validação cronológica de transações e documentos eletrónicos.
- c. Complementarmente, às recém-adquiridas responsabilidades absorvidas por via da extinção do CEGER, a AMA continuará a desenvolver o seu portefólio de projetos e iniciativas de identidade digital e de certificação eletrónica (eID) que inclui projetos^[1] e iniciativas de entre as quais se salienta:
 - a. Chave Móvel Digital – Evolução para curvas elípticas NIST-P
 - b. Arquitetura da App Cidadão e alinhamento à arquitetura EUDIW

- c. Quiosques Biométricos/Quiosque Digital
 - d. Plataforma de Interoperabilidade de dados biométricos
 - e. Processos desmaterializados de recuperação de pins e puk
 - f. Passaporte digital (integração na App Cidadão, especificação de piloto, casos de uso)
 - g. Vistos desmaterializados
 - h. Aumentar a dispersão de serviços com integração na App Cidadão e Autenticação.Gov
 - i. Middleware Cartão de Cidadão em plataformas Mobile
 - j. EUDI wallet e Projeto POTENTIAL no seu âmbito
 - k. Plataforma de Gestão de Consentimentos
 - l. Serviço de Selos Temporais Qualificados
 - m. Public API Marketplace
 - n. Representação do Grupo “Digital Nations”
- d. Os produtos e soluções eID disponibilizados pela AMA suportam centenas de parceiros e clientes públicos e empresariais que há que gerir, monitorizar e otimizar tendo em vista serviços de identidade digital de excelência, contextualizados e que deem resposta às necessidades da sociedade portuguesa.
- e. Pelo atrás exposto, fica saliente que a vertente dos certificados digitais e da certificação eletrónica, a gestão da relação da AMA com clientes e parceiros de produtos e soluções eID, bem como o suporte a utilizadores no uso e adesão a estas funcionalidades assumem particular relevância no sentido de promover e alargar o efetivo uso destas soluções pelos cidadãos e empresas, concretizando verdadeiramente as competências que lhe estão consagradas na lei.

2. Objetivos e Desafios

- a. A lista diversa de responsabilidades, projetos e iniciativas elencados atrás comporta um conjunto de objetivos e desafios particulares que importa identificar, desde logo porque a sua execução ocorre em paralelo, o que confere uma complexidade adicional à responsabilidade de garantir a concretização das metas preconizadas.

| Projeto / Responsabilidade eID | Objetivos / Desafios |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chave Móvel Digital – Evolução para curvas elípticas NIST-P | <ul style="list-style-type: none"> • Alinhamento ao esquema criptográfico do novo Cartão de Cidadão • Revisão de infraestrutura de suporte ao serviço • Melhoria do serviço ao nível de recolha de métricas e regras de negócio |
| Arquitetura da App Cidadão e alinhamento à arquitetura EUDIW | <ul style="list-style-type: none"> • Agregação das aplicações Autenticação.gov e ID.Gov • Adoção das diretivas europeias neste âmbito na evolução e desenvolvimento da aplicação gov.pt |
| Quiosques Biométricos/Quiosque Digital | <ul style="list-style-type: none"> • Enrollment de dados biométricos em quiosques físicos e digitais • Processos de autenticação biométrica (face match e liveness detection) • Background removal and validação de requisitos ICAO for Digital Onboarding • Correção do posicionamento do corpo no enquadramento da fotografia recolhida • Orquestração dos pedidos entre entidades do ciclo de vida do CC • Passaporte e outras entidades da Administração Pública (AP) |
| Plataforma de Interoperabilidade de dados biométricos | <ul style="list-style-type: none"> • Criar um broker à semelhança da IAP que permita gerir os fluxos de dados biométricos entre entidades emissoras e subscritoras da AP • Disponibilizar serviço ao Cidadão integrado com o Fornecedor de Autenticação da AMA • Disponibilizar serviço às entidades públicas e privadas, garantindo que o Cidadão recebe um pedido de consentimento e pode gerir esse consentimento de acordo com o ciclo de vida do mesmo previsto no RGPD • Facilitar a reutilização dos dados biométricos para emissão de documentos emitidos pela administração pública (CC, Passaporte, Carta de Condução, Cartão ADSE, Cartão Jovem, |

| | |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>passes sociais, etc), no cumprimento dos respetivos prazos legais de validade dos dados biométricos, evitando a dispersão destes dados e a recolha repetida de dados biométricos pelo Cidadão.</p> |
| <p>Processos desmaterializados de recuperação de pins e puk</p> | <ul style="list-style-type: none"> • Junção da Autenticação.gov e ID.Gov • Autenticação dupla • Autenticacao.gov • Biometria facial + Liveness Detection • Integração com IRN em que se substitui o passo de Match-on-Card pelo passo de autenticação prévia feita no ponto anterior • Envio da carta de pin (opcional para motivar a redução de custos de envio de produção e envio de cartas) • Obtenção de códigos através da App Cidadão com uma opção de visualização dos códigos por baixo do Cartão de Cidadão (como acontece com os cartões bancários do Revolut, Pleo, entre outros) em que os códigos só são disponibilizados após nova autenticação biométrica |
| <p>Passaporte digital (integração na App Cidadão, especificação de piloto, casos de uso)</p> | <ul style="list-style-type: none"> • Disponibilização do passaporte eletrónico português na App Cidadão, com possibilidade de verificação junto das relying parties • Alinhado com a EUDIW • Alinhado com os requisitos do Doc 9303 da <i>International Civil Aviation Organization</i> (ICAO) |
| <p>Vistos desmaterializados</p> | <ul style="list-style-type: none"> • Conceito de emissão e controlo dos vistos • Vistos totalmente desmaterializada e vistos papel e/ou selo autocolante com a aposição de selo digital visual (formato visto Schengen) • Integração com a SPMS para validação de certificados de vacinação e outros requisitos profiláticos necessários |
| <p>Aumentar a dispersão de serviços com integração na App Cidadão e Autenticação.Gov</p> | <ul style="list-style-type: none"> • Integração das contraordenações (ANSR) na App Cidadão • Integração do SIAC |

| | |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Middleware Cartão de Cidadão em plataformas Mobile</p> | <ul style="list-style-type: none"> • Com a adoção da tecnologia contactless para documentos (Cartão de Cidadão, Título de Residência e Passaporte Eletrónico), a utilização de uma solução desktop terá gradualmente uma menor procura em favorecimento da utilização de tecnologias móveis que permitem a leitura contactless destes documentos por NFC. • A criação de uma solução de aplicação móvel para smartphones e tablets, que permita gradualmente adotar todas as funcionalidades existentes da aplicação desktop do middleware do CC irá permitir iniciar a transição gradual da tecnologia. |
| <p>Projeto POTENTIAL</p> | <ul style="list-style-type: none"> • Coordenação nacional da implementação dos pilotos com as diversas entidades nacionais envolvidas, tais como IRN (UC1), SIBS (UC2), IMT e INCM (UC4), SPMS (UC6) • Reporte executivo semanal • Definição de arquitetura tecnológica para evolução da aplicação id.gov, de forma a estar em conformidade com ARF e EUDIW • Coordenação da implementação dos pilotos com os diversos parceiros dos Estados-Membros envolvidos • Apoio no reporte financeiro dos custos diretos e indiretos • Preparação e realização de Ponto de Situação Semanal com entidades nacionais • Apoio na definição e implementação de ações de disseminação e comunicação • Preparação, realização e apoio de apresentações ao Consórcio acerca dos produtos de identidade digital e certificação eletrónica • Apoio na representação de Portugal junto da Coordenação do Consórcio com AMA como <i>single point of contact</i> (SPOC) • Gestão de Consórcio, incluindo gestão de planeamento, custos, capacidade, âmbito, alterações, stakeholders, qualidade |

| | |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plataforma de Gestão de Consentimentos | <ul style="list-style-type: none"> • Plataforma que permita servir de 3ª parte de confiança entre entidades que requerem os dados biográficos e biométricos de Cidadãos, na qual são guardados os consentimentos atribuídos pelo Cidadão e onde ele pode gerir centralmente todos os consentimentos que atribuiu, desde que a plataforma requerente seja aderente à integração com a plataforma de consentimentos disponibilizada pelo Estado Português • A Plataforma deverá ser implementada de forma que permita que a integração seja feita com produtos da AMA (Autenticacao.Gov, Gov, App Cidadão) ou com outras soluções disponíveis no mercado; • Este serviço transmitirá maior confiança ao Cidadão no armazenamento dos consentimentos atribuídos, às plataformas requerentes confere-lhe maior transparência e redução de custos de gestão de informação e ao Estado Português permite-lhe ter informação gerida de forma segura e auditável que seja passível de utilização pelas entidades judiciais ou outras entidades em caso de disputas/diferendos |
| Serviço de Selos Temporais Qualificados | <ul style="list-style-type: none"> • Implementação de serviço de selos temporais qualificados que possa ser utilizado pelo Cidadão em processos de assinatura digital qualificada através do Middleware CC, Autenticacao.Gov ou App Cidadão, assim como disponibilizar um serviço a entidades públicas, entidades privadas para que possam utilizar o serviço ao abrigo de um protocolo que respeite as regras de negócio a definir pela AMA • Este serviço permitirá reduzir a dependência do serviço de selos temporais qualificados do Cartão de Cidadão e também aumenta a redundância neste âmbito para o uso geral do Cidadão nos seus processos de assinatura digital, assim como para vários serviços públicos que precisam de frequentemente utilizam estes serviços para documentação digital (Segurança Social, ANSR, EMEL, entre outros) |
| Public API Marketplace | <ul style="list-style-type: none"> • Potenciar a utilização de serviços públicos disponibilizados à sociedade no geral |

| | |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Aumentar a visibilidade e “comercialização” dos serviços públicos digitais disponibilizados à sociedade • Aumentar a maturidade digital da sociedade na utilização de serviços digitais disponibilizados pelo Estado Português • Documentação apropriada das APIs e da forma de utilização (após registo e aprovação de conta para acesso à área privada) • Disponibilizar ambientes de testes para que possam testar as referidas APIs (após registo e aprovação de conta para acesso à área privada) |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- b) Os projetos eID caracterizam-se pela utilização de tecnologia para identificar e autenticar os utilizadores de forma digital, recorrendo a sistemas de autenticação segura, biometria, chips RFID e outros meios eletrónicos, num ambiente cada vez mais baseado em MOBILE.
- c) As preocupações de segurança estendem-se igualmente às políticas de gestão de dados para garantir o armazenamento dos dados dos utilizadores em bases de dados acessíveis apenas por sistemas autorizados. Subjacentes a estas iniciativas estão também os conceitos de acessibilidade, usabilidade e interoperabilidade de modo a permitir que as soluções sejam utilizadas em inúmeros contextos e serviços, com a finalidade primordial de simplificar processos, aumentar a segurança e facilitar o acesso aos serviços públicos pelos cidadãos.
- d) Importa ainda ressaltar os objetivos e desafios transversais a todas as iniciativas e responsabilidades atribuídas à AMA, caracterizados pelas várias categorias de responsabilidades subjacentes:

| Vertente | Objetivos / Desafios Transversais às iniciativas de eID |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Coordenação/Gestão de Projeto | <ul style="list-style-type: none"> • Planeamento e implementação eficaz de projetos de eID; • Elaborar planos detalhados que assegurem a implementação bem-sucedida de soluções de eID, alinhados com as metas de modernização administrativa e transformação digital; • Assegurar a alocação eficiente de recursos humanos, financeiros e tecnológicos para a execução dos projetos |

| | |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Estabelecer cronogramas realistas e monitorizar a evolução dos projetos para garantir a atempada concretização das iniciativas; • Promover a Interoperabilidade das soluções eID e a sua integração com os sistemas atuais da Administração Pública e com plataformas de parceiros externos; • Garantir que os processos de identidade digital e de certificação eletrónica estejam em conformidade com regulamentos nacionais e internacionais; • Assegurar a Segurança e a Privacidade dos Dados. |
| Coordenação operacional de práticas de certificação eletrónica | <ul style="list-style-type: none"> • Garantir que as práticas de certificação eletrónica estão em conformidade com os regulamentos aplicáveis, como o eIDAS (Regulamento sobre Identificação Eletrónica e Serviços de Confiança para Transações Eletrónicas no Mercado Interno) e outras normas relevantes; • Facilitar a integração e compatibilidade dos serviços de certificação eletrónica com os sistemas e requisitos de outros prestadores de serviços, clientes e parceiros; • Desenhar, apoiar a implementação e monitorizar práticas operacionais eficazes e eficientes para suportar as atividades de certificação eletrónica – emissão, renovação e revogação de certificados digitais; • Salvaguardar a segurança das operações, a proteção de dados e a integridade dos certificados emitidos; • Desenho de arquiteturas de Infraestruturas de Chaves Públicas (PKI) robustas que deem resposta aos requisitos funcionais e operacionais dos projetos; • Garantir que a PKI esteja em conformidade com normas internacionais; • Desenhar e apoiar a implementação e operação eficiente e segura de PKI. |
| Gestão de Relação com clientes e Parceiros | <ul style="list-style-type: none"> • Fortalecer a Confiança e a Adesão às Soluções de eID - Prover segurança, privacidade e transparência nos processos relacionados ao uso de soluções de eID; |

| | |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Promover a adoção do eID - Implementar campanhas de sensibilização e capacitação para incentivar cidadãos e empresas a utilizarem as soluções disponíveis; • Criar diretrizes claras sobre a identidade digital e seu papel nas relações entre o governo, parceiros e cidadãos; • Garantir que os cidadãos e parceiros usufruam de uma experiência simples e intuitiva ao utilizar serviços que envolvam eID; • Promover a Inclusão Digital; • Monitorizar e Avaliar o Desempenho dos Projetos. |
| Gestão de representação externa e promoção de relações de cooperação no âmbito eID | <ul style="list-style-type: none"> • Representar os interesses de Portugal em fóruns e organizações internacionais, garantindo que as necessidades e prioridades nacionais sejam consideradas no âmbito da evolução global das soluções eID; • Superar diferenças entre os sistemas de identidade digital de diferentes países e promover a adopção de padrões comuns; • Promover cooperação internacional no desafio de enfrentar ameaças crescentes de cibersegurança, como roubo de identidade e ataques a infraestruturas de eID; • Coordenar diferentes interesses entre países para alcançar objetivos comuns no âmbito do eID, evitando conflitos de jurisdição ou soberania tecnológica. |

ANEXO II

Descrição dos Lotes 1 e 2

LOTE 1

Desenvolvimento e auditoria de infra-estruturas PKI e identidade digital para assinatura qualificada de faturas eletrónicas.

Prestação de serviços especializados em CMD, SCAP, SAFE e backend da EUDI Wallet, incluindo revisão documental, hardening de segurança e suporte a auditorias eIDAS, para garantir autenticidade, integridade e interoperabilidade do sistema de desmaterialização de faturas nas suas diversas vertentes.

Âmbito dos Trabalhos

Nesta secção procede-se á descrição das áreas de trabalho e atividades que se pretende que a equipa do cocontratante venha a desenvolver no âmbito deste projeto.

1. Políticas, Procedimentos e instalações CMD

Revisão, atualização e melhoria de documentação referente a políticas e procedimentos CMD e seu alinhamento com PKI do CC e tendo em vista auditorias anuais periódicas (externa), incluindo:

- Regras de Documentação – descrição de todos os tipos de documentos e o seu objetivo;
- Regras de Recursos Humanos - descrição dos Grupos de Trabalho previstos e a sua função;
- Regras de Ambientes - descrição do tipo e categoria de ambientes;
- Política de Identificadores a usar no CMD;
- Política de gestão de Certificados – descrição de perfil e política de gestão de ciclo de vida dos certificados
- Declaração de Práticas - práticas que segue para garantir a confiança no processo de certificação de atributos;
- Política de Cerimónias - todas as cerimónias referentes à gestão do ciclo de vida dos certificados emitidos, incluindo procedimentos e formulários associados a cada cerimónia;
- Política de Ambientes - concretização dos Ambientes e artefactos;

- Política de Recursos Humanos - concretização dos RH baseado nas Regras de Recursos Humanos;
- Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento do CMD;
- Políticas e procedimentos para sub-CA CMD da PKI do CC – incluindo revisão das políticas, procedimentos e documentação da PKI do CC;
- Elaboração de documentação para credenciação nos termos da especificação técnica CEN EN 419241-2:2019;
- Outros documentos, ou diagramas referentes a políticas e procedimentos que se revelem necessários para a concretização da eventual certificação;
- Verificação das políticas, infraestruturas e procedimentos implementados na CMD;
- Recomendação de melhorias a implementar;
- Segunda verificação das políticas, infraestruturas e procedimentos CMD após implementação de melhorias;
- Acompanhamento de auditorias externas a solução CMD assinatura.
- Participação e suporte às auditorias internas a solução CMD assinatura.

2. Políticas, Procedimentos e instalações SCAP

Revisão, atualização e melhoria de documentação referente a políticas e procedimentos SCAP, incluindo:

- Regras de Documentação;
- Regras de Recursos;
- Regras de Ambientes;
- Política de Identificadores a usar no SCAP;
- Política de gestão de Certificados
- Declaração de Práticas;
- Política de Cerimónias;
- Política de Ambientes;
- Política de Recursos Humanos;
- Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento do SCAP;

- Outros documentos, ou diagramas referentes a políticas e procedimentos que se revelem necessários para a concretização da eventual certificação.
- Verificação das políticas, infraestruturas e procedimentos implementados no SCAP;
- Recomendação de melhorias a implementar;
- Segunda verificação das políticas, infraestruturas e procedimentos SCAP após implementação de melhorias.
- Definição de Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento dos fornecedores de atributos;
- Definição de orientações, políticas e procedimentos transversais que deverão ser asseguradas por Fornecedores de Atributos;
- Verificação do cumprimento de políticas e procedimentos em Fornecedores de Atributos (10);
- Acompanhamento de auditorias externas a solução SCAP.
- Participação e suporte às auditorias internas a solução SCAP.

3. SAFE. Revisão, atualização e melhoria de documentação referente a políticas e procedimentos SAFE, incluindo:

- Regras de Documentação;
- Regras de Recursos;
- Regras de Ambientes;
- Política de Identificadores a usar no SAFE;
- Política de gestão de Certificados
- Declaração de Práticas;
- Política de Cerimónias;
- Política de Ambientes;
- Política de Recursos Humanos;
- Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento do SAFE;
- Outros documentos, ou diagramas referentes a políticas e procedimentos que se revelem necessários para a concretização da eventual certificação.
- Verificação das políticas, infraestruturas e procedimentos implementados no SAFE;
- Recomendação de melhorias a implementar;

- Verificação periódica das políticas, infraestruturas e procedimentos SAFE após implementação de melhorias.
- Acompanhamento de auditorias externas a solução SAFE.
- Participação e suporte às auditorias internas a solução SAFE.

4. eIDAS

- Atualização informação em relação a infraestrutura eIDAS e sistemas de Identificação Digital nacionais
- Suporte à participação e participação nas reuniões do EUDI Cooperation Group e suas Comissões Técnicas e Grupos de Trabalho.
- Pareceres técnicos, assessments e esclarecimento de dúvidas decorrentes do ponto anterior.

5. Pareceres técnicos, assessments, e esclarecimento de dúvidas decorrentes dos trabalhos de auditoria ou credenciação por entidades externas

6. Cartão de Cidadão

- Acompanhamento de auditorias externas a solução Cartão de Cidadão
- Participação e suporte às auditorias internas a solução Cartão de Cidadão

7. EUDI Wallet. De acordo com o Regulamento eIDAS 2 (Regulamento (EU) 2024/1183) e com o ARF (European Digital Identity Wallet Architecture and Reference Framework), e utilizando a implementação de referência da EUDI Wallet, possibilitar a realização de testes de interoperabilidade, incluindo:

- Disponibilização e operação em ambiente de testes (ou pré-produção) das várias componentes de backend necessárias ao ecossistema EUDI Wallet, nomeadamente Provider (para PID, EAA e PUB-EAA), Registrar de Relying Party, Verifier e assinatura digital (signer e SCA).
- Disponibilização e operação em ambiente de testes (ou pré-produção) das PKIs necessárias para o funcionamento das componentes do ponto anterior.

- Integrações e alterações necessárias às plataformas indicadas em 3.1.7.1 para suporte a testes nacionais e internacionais.

De acordo com o Regulamento eIDAS 2 (Regulamento (EU) 2024/1183) e com o ARF (European Digital Identity Wallet Architecture and Reference Framework), e utilizando a implementação de referência, estudar a evolução necessária para que as plataformas indicadas em 3.1.7.1 e 3.1.7.2 possam suportar serviços em produção, incluindo:

- Análises, pareceres técnicos e esclarecimento de dúvidas sobre a integração das plataformas com os serviços geridos pela AMA (SCAP, SAFE, CMD).
- Análises, pareceres técnicos e esclarecimento de dúvidas sobre a integração da plataforma de assinatura remota gerida pela AMA, com a EUDI Wallet;
- Análises, pareceres técnicos e esclarecimento de dúvidas sobre as certificações, credenciações e auditorias necessárias.

8. Serviços qualificados do QTSP AMA

De acordo com o Regulamento eIDAS 2 (Regulamento (EU) 2024/1183) estudar a evolução dos requisitos que os serviços qualificados do QTSP AMA têm de cumprir, em relação ao Regulamento eIDAS (Regulamento (EU) 910/2014), incluindo:

- Análises, pareceres técnicos e esclarecimento de dúvidas sobre certificações, credenciações e auditorias necessárias.
- Análises, pareceres técnicos e esclarecimento de dúvidas sobre alterações e evoluções necessárias.
- Prazos para as re-certificações dos serviços qualificados de acordo com o eIDAS 2.

9. Serviços qualificados do QTSP ECCE

Garantir a conformidade dos serviços de confiança prestados pela da Entidade Certificadora Comum do Estado (ECCE) com o Regulamento eIDAS 2.0, em concreto no que se refere aos seguintes serviços qualificados:

- a) Assinaturas eletrónicas;
- b) Selos eletrónicos;
- c) Selos temporais;

Concomitantemente verificar o compliance com as ESTI aplicadas aos serviços anteriormente descritos, nas suas versões mais atuais, caso as a seguir indicadas já tenham sofrido algum tipo de atualização, a saber:

- I. ETSI EN 319 401 V3.1.1 (2024-06)
- II. ETSI TS 119 312 V1.3.1 (2019-02)
- III. ETSI EN 319 411-1 V1.3.1 (2021-05)
- IV. ETSI EN 319 411-2 V2.5.1 (2023-10)
- V. ETSI EN 319 412-2 V2.3.1 (2023-09)
- VI. ETSI EN 319 412-5 V2.4.1 (2023-09)

Selos Temporais

- I. ETSI EN 319 421 V1.2.1 (2023-05)
- II. ETSI EN 319 422 V1.1.1 (2016-03)
- III. ETSI TS 102 023 V1.2.2 (2008-10)

Recursos Humanos

ETSI EN 319 412-3 V1.3.1 (2023-09)

Por fim:

- 1) monitorização dos prazos para as recertificações dos serviços qualificados de acordo com o eIDAS 2, e políticas, objetivos e procedimentos da organização;
- 2) Acompanhamento de auditorias externas relativas aos serviços de confiança prestados pela ECCE.

10. É requisito obrigatório que a entidade concorrente tenha credenciação de segurança no grau confidencial concedida pela autoridade nacional de segurança ou entidade congénere equivalente.

11. Para a execução dos serviços de consultadoria suprarreferidos deverá ser prevista uma equipa com os perfis que em seguida se indicam:

- Consultor tecnológico estratégico com:
 - o Experiência superior a 15 anos enquanto consultor tecnológico nas áreas atrás melhor descritas;

- o Experiência anterior em projetos relacionados com o Cartão de Cidadão ou outros documentos de identificação equivalentes de um país da UE, com sistema de certificação de atributos profissionais e de sistema de identidade digital como a CMD ou equivalente;
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos) com formação complementar em gestão;
 - o Credenciação pelo Gabinete Nacional de Segurança;
 - o Experiência em execução de pelo menos 5 projetos de credenciação de ICP;
 - o Participação (ou suporte à participação) no eIDAS Cooperation Group, assim como a participação na equipa que suporta o desenvolvimento do ARF.
- Software developer EUDI Wallet, com:
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos);
 - o Experiência no desenvolvimento de projetos relacionados com a EUDI Wallet;
 - o Participação na equipa de desenvolvimento de componente de backend da implementação de referência da EUDI Wallet em Portugal ou noutro país da EU, assim como experiência na utilização e operação da EJBCA (servidor utilizado nas PKIs necessárias para o funcionamento das componentes de backend da implementação de referência da EUDI Wallet);
- Software developer Java e Python com:
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos);
 - o Experiência de desenvolvimento em Java e Python (linguagem de programação utilizada nas componentes de backend da implementação de referência da EUDI Wallet)
 - o Participação na equipa de desenvolvimento de componente de backend da implementação de referência da EUDI Wallet em Portugal ou em qualquer país da EU.
- Devop ou administrador de sistemas com:
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos);
 - o Experiência de pelo menos 5 anos nesta função.
- Consultor tecnológico Júnior com:
 - o Experiência em projetos relacionados com a EUDI Wallet;

- o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos);
- o É valorizada a participação na equipa de análise e planeamento de componente de backend da implementação de referência da EUDI Wallet.
- Consultor tecnológico Auditorias com experiência superior a 10 anos, e:
 - o Experiência na realização ou participação em equipas de auditoria;
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos);
- Gestor de projeto:
 - o Experiência superior a 10 anos;
 - o Experiência na gestão de projetos;
 - o Formação superior em Informática ou Engenharia Informática (ou na mesma área de estudos).

Lote 1

| Perfil | FTES | Horas Estimadas |
|------------------------------------|-------------|------------------------|
| Consultor tecnológico estratégico | 1 | 525 |
| Consultor tecnológico Júnior | 1 | 500 |
| Software developer EUDI Wallet | 1 | 500 |
| Software developer Java e Python | 1 | 1000 |
| Devop ou administrador de sistemas | 1 | 500 |
| Consultor Tecnológico Auditorias | 1 | 500 |
| Gestor de Projeto | 1 | 500 |

As horas indicadas por perfil em cada um dos lotes são uma estimativa, podendo as mesmas sofrer ajustes para mais ou menos horas conforme o desenvolvimento do projeto objeto do presente procedimento.

Em sede de execução, e caso se verifique necessidade, poderá a AMA solicitar mais FTE´s do que os previstos nas tabelas supra.

LOTE 2

Consultoria e governação de soluções eID e certificação eletrónica para massificar a faturação digital

Serviços de arquitetura de sistemas, gestão de projectos, análise funcional e coordenação operacional que alinham iniciativas mobile e integração com parceiros, assegurando a expansão segura e escalável da faturação totalmente desmaterializada.

Âmbito

De seguida descrevem-se os serviços a adquirir de consultoria especializada de uma equipa multidisciplinar de gestão de projeto, arquitetura de sistemas de informação, análise funcional, coordenação operacional de práticas de certificação eletrónica e de gestão da relação com parceiros e clientes com especial foco nas suas soluções de vertente Mobile.

ESPECIFICAÇÃO DOS SERVIÇOS

a) No âmbito da coordenação e Arquitetura de Sistemas de Informação:

- i. Avaliação de necessidades e objetivos do negócio e participação no desenho das soluções de eID, e certificação eletrónica;
- j. Suporte na definição de requisitos técnicos no âmbito dos projetos, serviços e iniciativas de eID e de certificação eletrónica;
- k. Assessoria técnica no acompanhamento e gestão das fases de definição, desenvolvimento e implementação dos projetos, serviços e iniciativas de eID e certificação eletrónica;
- l. Desenho e especificação das arquiteturas tecnológicas, designadamente de componentes como sistemas de gestão de identidades, módulos de autenticação, bases de dados, interfaces e API para as iniciativas de eID e certificação eletrónica;
- m. Desenho e especificação de requisitos de segurança tecnológica das soluções de eID, certificação eletrónica e temporal e de certificados digitais a implementar à luz das melhores práticas internacionais de certificação eletrónica, cibersegurança e das normas técnicas do Gabinete Nacional de Segurança e demais normas vigentes para a Administração Pública;
- n. Apoio na elaboração das cláusulas técnicas dos Cadernos de Encargos para a implementação dos projetos, serviços e iniciativas de eID e certificação eletrónica (selos eletrónicos selos temporais, certificados digitais, assinaturas avançadas e qualificadas, certificados SSL/TLS, entre outros);

- o. Acompanhamento da implementação das soluções eID, certificação eletrónica garantindo a conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e sinalizando riscos de incumprimento;
- p. Assegurar orientação estratégica contínua sobre questões de proteção de dados no âmbito das áreas de intervenção dos projetos e iniciativas de eID e certificação eletrónica;
- q. Acompanhamento a auditorias, testes e controlo de qualidade para verificação de compliance dos desenvolvimentos face aos requisitos tecnológicos e de segurança.

b) No âmbito da Gestão de Projeto:

- i. Apoio na implementação dos projetos, serviços e pilotos de eID, certificação eletrónica e temporal e certificados digitais, bem como na articulação interna e com as diversas entidades externas à AMA, quer ao nível nacional, quer ao nível internacional;
- j. Apoio na coordenação nacional dos projetos, serviços e pilotos de eID, certificação eletrónica e temporal e certificados digitais, bem como na articulação com as diversas entidades nacionais e internacionais envolvidas;
- k. Apoio na representação de Portugal em projetos de eID, nomeadamente no grupo “Digital Nations”, no âmbito das responsabilidades da AMA como single point of contact (SPOC);
- l. Execução dos relatórios executivos para reporte a entidades nacionais ou estrangeiras, internas ou externas, com periodicidade a definir pela AMA, no âmbito dos projetos de eID, certificação eletrónica e temporal e certificados digitais;
- m. Execução de apresentações de suporte a reuniões de ponto de situação no âmbito dos projetos de eID com entidades nacionais ou estrangeiras, internas ou externas, com periodicidade a definir pela AMA;
- n. Apoio no reporte financeiro dos custos diretos e indiretos contemplados nas soluções, serviços e iniciativas em curso ou por implementar;
- o. Apoio na articulação com os fornecedores de serviços de implementação ou licenciamento no âmbito dos projetos, serviços e pilotos de eID, certificação eletrónica e temporal e certificados digitais;
- p. Apoio na definição e implementação de ações de disseminação, comunicação e gestão da mudança no âmbito de projetos, serviços e pilotos de eID;

- q. Apoio na coordenação de ações de gestão da relação com parceiros e clientes de eID, incluindo ações de promoção e pré-venda, gestão de atividades de adesão, identificação de necessidades e oportunidades de parceiros, aferição do grau de satisfação dos parceiros, definição de estratégias de monitorização e de aferição do grau de satisfação dos utilizadores finais, definição de estratégia de acompanhamento e resposta a comentários públicos a produtos de eID;
- r. Coordenação transversal da equipa de consultores no âmbito das iniciativas de eID, certificação eletrónica e temporal e certificados digitais;
- s. Gestão transversal de projetos incluindo o planeamento, monitorização, gestão de âmbito, gestão cronograma, gestão de custo, gestão da qualidade, gestão de recursos, e gestão de *stakeholders* no âmbito dos projetos, serviços e iniciativas de eID, certificação eletrónica e certificados digitais.

b) No âmbito da definição funcional e gestão:

- e) Levantamento detalhado de requisitos funcionais e técnicos, designadamente das situações atual e futura ao nível dos processos e segurança dos dados no âmbito das soluções, serviços e projetos de eID e certificação eletrónica;
- e) Desenho e especificação funcional e processual das soluções a implementar à luz das melhores práticas mundiais no âmbito das áreas de intervenção dos projetos e iniciativas de eID e certificação eletrónica;
- e) Acompanhamento aos testes e controlo de qualidade para verificação de compliance dos desenvolvimentos face aos requisitos funcionais;
- e) Suporte à formação e sensibilização para funcionários e outras partes interessadas sobre práticas de proteção de dados e privacidade;
- e) No âmbito da gestão da relação com clientes e parceiros de soluções eID:
 - i. Desenvolvimento de ações de promoção e pré-venda - Proposta de plano de promoção e pré-venda, organizado por setor de atividade, tipologia de entidade e por produto de ID, execução de ações de promoção e pré-venda junto de Parceiros; angariação de clientes para produtos de identidade digital;
 - ii. Gestão de atividades de adesão;
 - iii. Identificação de necessidades e oportunidades de Parceiros
 - iv. Execução de processos de adesão de serviços de ID com interlocução de diferentes equipas internas;
 - v. Reunião periódica com Parceiros;

- vi. Desenvolvimento de ações de aferição do grau de satisfação dos Parceiros;
- vii. Monitorização, Acompanhamento e Resposta a comentários públicos a produtos de Identidade Digital;
- viii. Gestão de comentários e reportes nas redes sociais (Facebook, Instagram, Twitter, entre outros a identificar em sede de projeto);
- ix. Monitorização, resposta e otimização rankings aplicações móveis nas lojas móveis (Google, Apple, entre outras);
- x. Monitorização da qualidade do serviço;
- xi. Execução de ações de aferição do grau de satisfação dos utilizadores finais;
- xii. Elaboração de inquéritos de satisfação dos processos de adesão das entidades de forma a obter informação de qualidade sobre a eficácia do membro da equipa interna ou outros elementos considerados relevantes para a concretização da adesão.

PERFIS TÉCNICOS A AFETAR AOS SERVIÇOS

1. O cocontratante deverá disponibilizar recursos com perfis que cumpram os seguintes requisitos:

Requisito obrigatório transversal a toda a equipa a apresentar: Credenciação na marca Nacional (grau mínimo Secreto) e na marca NATO (grau mínimo Secret) pelo Gabinete Nacional de Segurança ou congénere equivalente.

a) Coordenador / Arquiteto de Sistemas de Informação:

Requisitos Mínimos Obrigatórios – Habilitações académicas específicas, credenciações e formação profissional:

- Licenciatura nas áreas de Engenharia Informática, Eletrotécnica ou de Telecomunicações e Informática (ou na mesma área de estudos);
- Fluente em Português;

Requisitos Mínimos Obrigatórios – Experiência profissional:

- Experiência profissional de 15 ou mais anos em projetos de consultoria de Sistemas de Informação;
- Experiência comprovada na coordenação de projetos nacionais e internacionais nos domínios da certificação eletrónica, documentos de identificação e de viagem, físicos e digitais e na implementação de Infraestruturas de Chaves Públicas (PKI);

- Experiência comprovada em desenho, implementação e operação de Infraestruturas de Chaves Públicas (PKI);
- Experiência comprovada em processos de capacitação e conformidade nos referenciais eIDAS e ISO/IEC 27001.
- Experiência profissional de 15 ou mais anos em projetos eID envolvendo entidades do setor público portuguesas ou de países Europeus e/ou dos PALOP's;
- Participação em projetos nacionais relacionados com o Cartão de Cidadão, Chave Móvel Digital, Passaporte Eletrónico e Título de Residência ou em projetos de países europeus e/ou PALOP com documentos e soluções digitais equivalentes.
- Experiência em implementação e gestão de projetos de gestão de mudança na Administração Pública e no tecido privado no âmbito das TIC;
- Experiência em funções de responsável de segurança da informação em instituições públicas e privadas;
- Experiência em funções de responsável de tecnologias de informação em instituições públicas e privadas;
- Participação em pelo menos 10 projetos de gestão da mudança nas TIC em instituições públicas e privadas;
- Fluente em Inglês falado e escrito por experiência em projetos internacionais ou por formação específica em língua inglesa.

b) Gestor de Projeto Sénior:

Requisitos Mínimos Obrigatórios – Habilitações académicas específicas, credenciações e formação profissional:

- Licenciatura nas áreas de Engenharia, Gestão, Tecnologias ou Ciências de Informação, ou na mesma área de estudos;
- Fluente em Português;

Requisitos Mínimos Obrigatórios – Experiência profissional:

- Experiência de 5 anos em gestão de projetos de sistemas de informação na Administração Pública e no âmbito privado na vertente TIC;
- Experiência prévia em coordenação de projetos nacionais ou internacionais de identidade digital;
- Formação complementar em gestão de projetos;
- Formação complementar em Regulamento Geral de Proteção de Dados (RGPD).
- Certificação PMP de PMI ou equivalente na área de gestão de projetos;

- Formação complementar em metodologias ágeis;
- Experiência em gestão de projetos na vertente eID envolvendo entidades do setor público em Portugal ou noutro país;
- Participação prévia em projetos do âmbito do POTENTIAL levado a cabo pelos Estados-Membros da UE;
- Experiência profissional de 5 ou mais anos em coordenação de equipas em projetos de consultadoria e de tecnologias de informação e comunicações;
- Experiência prévia em projetos relacionados com o Cartão de Cidadão ou Chave Móvel Digital ou em soluções equivalentes noutros países da UE ou PALOP.
- Fluente em Inglês falado e escrito por experiência em projetos internacionais ou por formação específica em língua inglesa.

c) Consultor funcional / de gestão:

Requisitos Mínimos Obrigatórios – Habilitações académicas específicas, credenciações e formação profissional:

- Licenciatura nas áreas de Gestão, Gestão de Recursos Humanos, Tecnologias ou Ciências de Informação ou na mesma área de estudos;
- Certificado de Competências Pedagógicas;
- Fluente em Português;

Requisitos Mínimos Obrigatórios – Experiência profissional:

- Experiência profissional de 3 anos ou superior em projetos de TI envolvendo entidades do setor público e privado;
- Experiência profissional de 3 anos ou superior em projetos de TI envolvendo entidades do setor público e privado na vertente de levantamento e especificação de requisitos técnicos e funcionais e tradução de necessidades de negócio em requisitos técnicos em projetos de transformação digital;
- Experiência profissional de 3 anos ou superior em funções de construção de relatórios, reporte periódico e discussão do estado das iniciativas junto da estrutura diretiva das organizações em entidades públicas e privadas;
- Experiência de 2 anos ou superior em funções de gestão da relação com clientes e parceiros de soluções digitais em entidades públicas ou privadas;
- Certificação PMP de PMI ou equivalente na área de gestão de projetos;
- Formação complementar em metodologias ágeis;

- Experiência profissional de 5 anos ou superior projetos de TI envolvendo entidades do setor público e/ou privado;
- Experiência profissional de 5 anos ou superior em funções de gestão da comunicação e articulação de stakeholders internos e externos em entidades públicas e/ou privadas;
- Fluente em Inglês falado e escrito por experiência em projetos internacionais ou por formação específica em língua inglesa.

Lote 2

| Perfil | FTEs | Horas Estimadas |
|---------------------------------------------------|-------------|------------------------|
| Coordenador / Arquiteto de Sistemas de Informação | 1 | 1595 |
| Gestor de Projeto | 1 | 1585 |
| Consultor funcional / de gestão | 1 | 1585 |

As horas indicadas por perfil em cada um dos lotes são uma estimativa, podendo as mesmas sofrer ajustes para mais ou menos horas conforme o desenvolvimento do projeto objeto do presente procedimento.

Em sede de execução, e caso se verifique necessidade, poderá a AMA solicitar mais FTE´s do que os previstos nas tabelas supra.

ANEXO III

Plataformas e Projetos Relevantes para os Serviços a prestar

Cartão de Cidadão

Implementado em 2007, o projeto do Cartão de Cidadão (CC) veio disponibilizar um cartão de identificação dos cidadãos nacionais que agrega e substitui os diversos cartões na altura existentes, necessários à interação do cidadão com os respetivos serviços da Administração Pública.

Este cartão posicionou-se como um verdadeiro certificado de cidadania e assume a forma dupla de um documento físico que identifica visual e presencialmente o cidadão e de um documento digital que permite ao cidadão identificar-se e autenticar-se eletronicamente nos atos em que intervenha perante entidades públicas e privadas.



Figura 1: Cartão de Cidadão

Este projeto, desde o momento da sua conceção, apresentou um conjunto de objetivos e desafios únicos e ambiciosos, nomeadamente:

- Ser o documento de Identificação Nacional Presencial de Elevada Segurança, designadamente de forma a ultrapassar os reconhecidos problemas de segurança, contrafação e falsificação inerentes ao
- Bilhete de Identidade;
- Substituir 5 cartões de identificação, agregando num único documento os respetivos n.º de identificação;
- Ser o mecanismo de Autenticação Eletrónica de elevada segurança do cidadão perante todos serviços públicos (e não-públicos), designadamente na Internet;

- Permitir a Assinatura Eletrónica de documentos (com toda a força probatória inerente a este tipo assinatura, nomeadamente assegurando o total valor legal e não repúdio de documentos assinados desta forma);
- Permitir a transferência eletrónica de dados residentes no cartão (em “off-line”);
- Ser válido como um documento de viagem no espaço Schengen;
- Assegurar a proteção e defesa dos dados do cidadão e a otimização dos processos associados, implementando mecanismos de auditoria contínua e desmaterializando as atividades e recursos (nomeadamente todo o processo de pedido de CC deve ser efetuado minimizando o recurso ao suporte físico “papel”.

Autenticação.Gov

O Autenticação.Gov (ou Fornecedor de Autenticação) surge na necessidade de identificação unívoca de um utilizador portador de um Cartão de Cidadão junto dos sítios Web de cada Organismo, com a obtenção da respetiva identificação setorial. Esta solução tem por objetivo tornar-se o ponto de autenticação eletrónica dos cidadãos perante a administração pública e mesmo organismos privados. O fornecedor de autenticação pretende assim facilitar e a acelerar o processo de adesão e utilização do cartão de cidadão na autenticação eletrónica do cidadão perante os serviços públicos.

A figura seguinte exemplifica a utilização do Autenticação.Gov com base num caso de uso de autenticação de um Cidadão junto de um Organismo.



No diagrama acima identificam-se as seguintes interações:

1. Cidadão pretende aceder à área privada do portal de um Organismo, ao qual é necessário que apresente a sua identidade

2. Portal do Organismo delega a autenticação e redireciona o Cidadão para o Fornecedor de Autenticação, juntamente com um pedido de autenticação assinado digitalmente;
3. Cabe ao FA validar o pedido de autenticação recebido e solicitar a autenticação do Cidadão com Cartão de Cidadão, através da inserção do PIN. Durante este processo, o FA irá efetuar as seguintes operações internas:
 - a. Validação das credenciais do Cidadão com recurso à PKI do Cartão de Cidadão, via OCSP;
 - b. Obtenção de atributos que sejam solicitados através dos vários fornecedores de atributos qualificados, via Plataforma de Interoperabilidade. Este processo pode incluir a obtenção de dados da Federação de Identidades ou de outros Organismos;
4. A identidade e atributos do Cidadão são validados e assinados digitalmente pelo FA, que redirecionará o Cidadão de volta ao portal do Organismo original. Cabe ao Organismo a validação e utilização dos mesmos.

Dado que no processo de autenticação poderão ser solicitados mais dados que os presentes no certificado digital do Cartão de Cidadão (Nome e Número de Identificação Civil), mostra-se necessário a obtenção destes dados junto de fornecedores de atributos qualificados para o efeito.

Plataforma de Interoperabilidade da Administração Pública

A Plataforma de Interoperabilidade da Administração Pública fornece, entre outros aspetos, mecanismos robustos de autenticação e gestão de identidades, que facilitam a autenticação segura perante os organismos públicos, e mecanismos de controlo transacional, que garantem a qualidade dos dados durante o processo de utilização dos serviços eletrónicos, para além de um gateway central para os processos de pagamento eletrónico.

Na conceção do modelo da plataforma, os standards abertos impuseram-se sempre como opção estratégica, no sentido de assegurar um maior nível de interoperabilidade.

A adoção de uma Arquitetura Orientada a Serviços para a implementação de sistemas complexos e de grande dimensão, como é o caso de soluções de integração para a Administração Pública, assegura os níveis de adaptabilidade e rigor perante a mudança que é possível antecipar, deixando aberta a porta a evoluções e melhorias que se mostrem necessárias.

Esta tipificação arquitetural fornece um enquadramento sustentado, com um conjunto de regras e práticas que permitem a exposição de funções relevantes, enquanto serviços no nível de granularidade certo para quem deles usufrui. Os serviços são expostos escondendo a mecânica de implementação e utilizando um formato de interface único e baseado em standards.

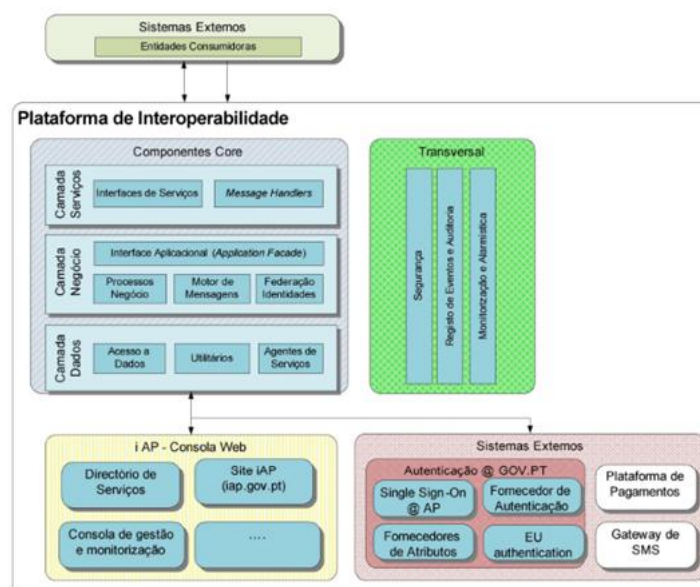


Figura 2 - Arquitetura lógica

A Plataforma de Interoperabilidade encontra-se suportada por um conjunto de componentes que visam atingir o objetivo para que a mesma foi criada. A sua arquitetura pode ser decomposta em várias áreas de atuação:

- Componentes core – agrega os componentes nucleares à utilização da plataforma como ferramenta de apoio à integração e serviço de dados. Encontram-se incluídas nesta área os componentes adaptadores aos diversos sistemas das Entidades, pipelines internos de processamento de mensagens, gestor de orquestrações e Federação de Identidades;
- Componentes transversais – abrangem todas as áreas da Plataforma de Interoperabilidade e são responsáveis pelas funcionalidades de segurança, privacidade de dados, registo e tratamento de exceções, bem como de monitorização global.
- iAP – Consola Web – apresentam-se como a camada visível da Interoperabilidade e partilha de serviços na Administração Pública. Providenciam uma imagem integrada da informação e funcionalidades disponíveis para as entidades públicas. Incluem-se neste domínio os componentes de:
 - o **Directório de Serviços** – responsável pela listagem e gestão dos serviços eletrónicos disponibilizados pela Plataforma;
 - o **Consola de Gestão** – disponibiliza aos seus utilizadores (a Administração Pública), funcionalidades de gestão e monitorização da plataforma, específicas para as Entidades que representam. Permite acesso à gestão de serviços, bem como a monitorização e gestão operacional de serviços que se encontrem em utilização;

- o **Site i-AP** – ponto visível do exterior da plataforma, com informação referente aos serviços, funcionalidades, informação para utilização da plataforma, materializado através de sítio Internet www.iap.gov.pt.
- Sistemas externos – funcionam de forma independente, mas intimamente acoplados no domínio da Plataforma de Interoperabilidade. São subsistemas que possuem funcionalidades específicas, mas basilares ao funcionamento de toda a arquitetura, servindo como elementos de suporte e de valor acrescentado. Incluem-se neste domínio os componentes de:
 - o Autenticação @gov.pt – conjunto de componentes que disponibilizam mecanismos de autenticação eletrónica perante a Administração Pública (e entidades privadas que o pretendam), assegurando funcionalidades de:
 - ♣ Fornecedor de Autenticação – descrito na secção seguinte;
 - ♣ Autenticação de Cidadãos da EU – possibilitando o acesso a serviços da Administração Pública Portuguesa por parte de cidadãos de outros Estados Membros e o acesso de cidadãos Portugueses a serviços eletrónicos de outros Estados Membros;
 - ♣ Fornecedor de Atributos – permite a obtenção de Atributos, tendo por base a autorização explícita do cidadão, para a execução de serviços eletrónicos, pelo canal Internet.
 - ♣ Single-sign-on – descrito na secção seguinte e nos serviços solicitados no âmbito deste procedimento.
- Plataforma de Pagamento e Gateway de SMS – sistemas externos, já existentes e em utilização produtiva, que se pretende que sejam disponibilizados de forma integrada e sejam potenciados pela Plataforma de Interoperabilidade, especialmente com a utilização de serviços compostos ou em processos orquestrados inteiramente.
-

Chave Móvel Digital

A Chave Móvel Digital (CMD) é 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. Com a CMD pode autenticar-se eletronicamente utilizando um computador ou dispositivos móveis com ligação à internet

As principais vantagens da CMD para o cidadão são:

- Mais simples: uma senha de acesso para todos os portais do Estado que disponibilizam este meio de autenticação.
- Mais seguro: inclui dois mecanismos de segurança: uma palavra-chave e um código temporário recebido por SMS no telemóvel registado.
- Mais cómodo: evita deslocações aos serviços públicos e tempos de espera.

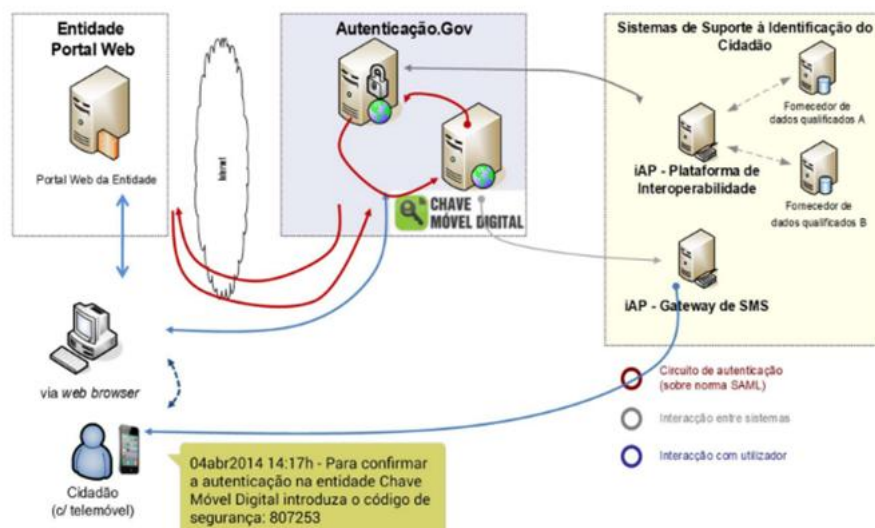
Para ativar, o cidadão deve dirigir-se a uma Loja de Cidadão, Balcão Multisserviços ou Espaço Cidadão para obter a CMD e apresentar o seu Cartão de Cidadão ou Bilhete de Identidade. A ativação do serviço é gratuita.

É ainda possível fazer o registo online na CMD (sem deslocação presencial), fazendo uso do Cartão de Cidadão.

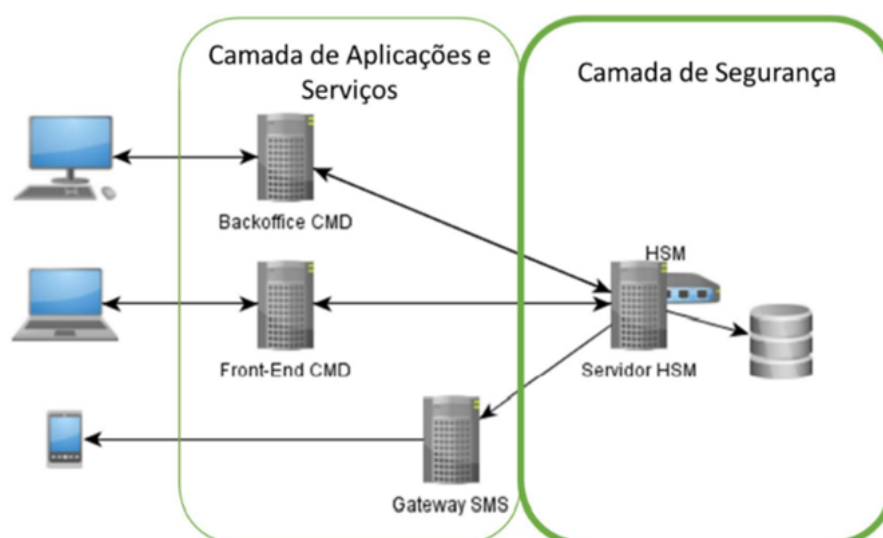
A CMD encontra-se já disponível em vários portais e sistemas (como o ePortugal (Portal do Cidadão), Portal do Utente, entre outros), assegurando:

- Maior eficácia e elevada segurança: o registo é imediato, não obriga a processos de confirmação da identidade do cidadão como o envio de cartas para o domicílio de cidadão, nem a processos de reenvio de senhas, no caso de esquecimento da mesma.
- Fácil migração: caso o portal público já disponibilize autenticação com o Cartão de Cidadão utilizando o serviço Autenticação.Gov (vulgo Fornecedor de Autenticação) – como já acontece com os principais
- Portais que disponibilizam serviços públicos, como o ePortugal (Portal do Cidadão, o Portal da Empresa), o Portal das Finanças, o Portal da Saúde, o Portal da Segurança Social, entre outros - para disponibilizar a autenticação com CMD num portal, basta incluir no atual pedido ao serviço “Autenticação.Gov” um parâmetro que indica que o portal também aceita Chave Móvel Digital.

A figura seguinte apresenta o fluxo global da solução implementada.



Encontra-se implementado mecanismo de assinatura associado à CMD, conforme arquitetura patente na figura seguinte:



Sistema de Certificação de Atributos Profissionais com Cartão de Cidadão

O Cartão de Cidadão possui dois certificados digitais (X509 v3)¹ que permitem aos seus possuidores a criação de Assinaturas Digitais Qualificadas, na qualidade de cidadão português, e a autenticação perante sistemas informáticos na mesma qualidade.

O principal enfoque deste procedimento é a gestão global das várias iniciativas tecnológicas e de negócio para implementação deste sistema que possibilite a utilização do Cartão de Cidadão para a criação de assinaturas digitais e a autenticação em diferentes qualidades, nomeadamente as qualidades profissionais – este sistema é designado por SCAP (“sistema de Certificação eletrónica de atributos do Cartão de Cidadão”).

Pretende-se que o sistema permita aos cidadãos escolher a qualidade através da qual pretendem assinar um documento, ou através da qual pretendem autenticar-se para aceder a serviços reservados ou associados às respetivas qualidades.

A arquitetura lógica da solução e os seus respetivos módulos é apresentada na figura seguinte.

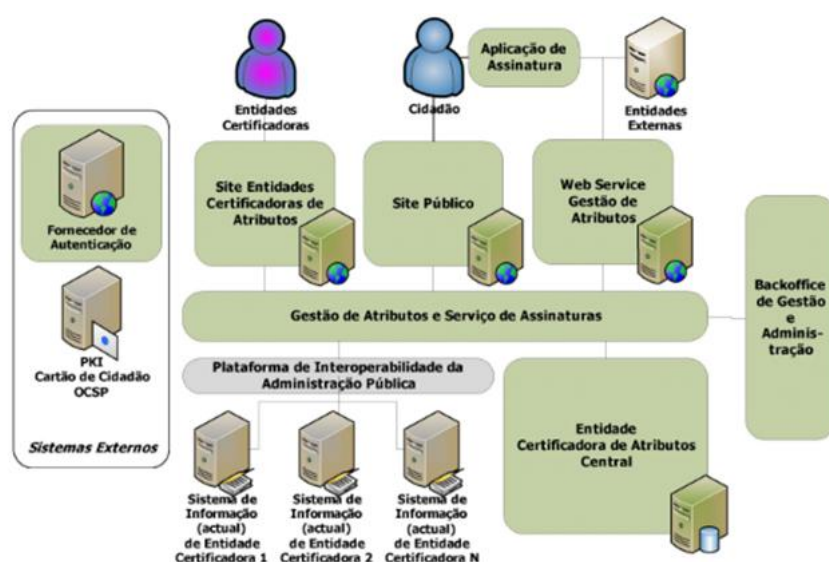


Figura 3 - Arquitetura Global da Solução

Serviço de Assinatura de Faturas Eletrónicas

O Decreto-Lei n.º 28/2019, de 15 de fevereiro torna obrigatória a emissão de faturas eletrónicas por intermédio do uso de uma assinatura digital qualificada ou de um selo eletrónico qualificado, a partir de janeiro 2021.

Neste contexto, e também da medida do programa Simplex “Fatura eletrónica mais acessível”, a AMA implementou o Serviço de Assinatura de Faturas Eletrónicas (SAFE), enquadrado no Sistema de Certificação de Atributos Profissionais (SCAP), com o objetivo de oferecer uma solução segura e simples de assinatura eletrónica qualificada de faturas à Economia.

O Serviço de Assinatura de Faturas Eletrónicas (SAFE) oferece uma solução para a assinatura eletrónica qualificada em conformidade com o referido enquadramento legal. Este serviço público permite a administradores, gerentes, diretores ou outros por estes designados, sem custos adicionais, assinar faturas de forma simples e segura através de integração com os respetivos softwares de faturação.

O SAFE vem adicionar a funcionalidade de assinatura de faturas ao já existente SCAP - Sistema de Certificação de Atributos Profissionais (www.autenticacao.gov.pt).

Este serviço permite ao cidadão, enquanto profissional de uma empresa, assinar digitalmente faturas eletrónicas, através de mecanismo automatizado pelo software de faturação.

Assim, o empresário aderente ao SCAP, tem acesso a novo certificado qualificado específico para a assinatura de faturas. Este processo é sumariado na figura seguinte.



Figura 4 - Emissão periódica de certificado para emissão de fatura

Assim, de forma a obter um certificado de assinatura de faturas SAFE, o empresário/comerciante autentica-se com o Cartão de Cidadão ou a Chave Móvel Digital e, após verificação da existência de poder associado (no SCAP) para assinatura de faturas, é gerado um código ("Access Token") que é guardado de forma segura no software de faturação. Este "Access Token" permitirá a assinatura de faturas pelo empresário, sem necessitar de voltar a colocar qualquer PIN, durante um período até 45 dias (ou com o atingimento de um limite máximo de faturas).

No processo corrente, de emissão de faturas, a sua assinatura eletrónica é "transparente" para o empresário, conforme figura seguinte.



Figura 5 - Assinatura de fatura com SAFE

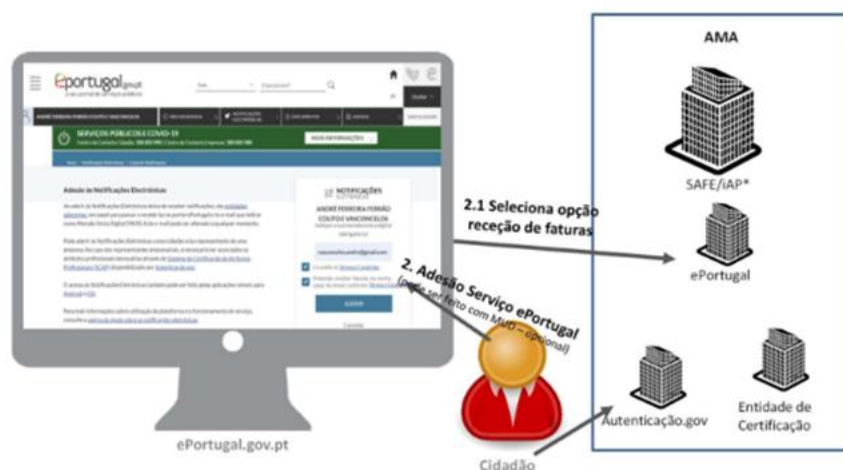
Assim, aquando da emissão da fatura, o software de faturação (devidamente autenticado) envia para o SAFE o

“Access token” (obtido aquando da ativação periódica do certificado, previamente descrito) e, seguindo uma sequência standard para a geração de assinaturas, é gerado um identificador do processo de assinatura que, quando enviado em conjunto com a hash da fatura, permite a sua assinatura pelo SAFE. Finalmente o software de faturação agrega a hash assinada da fatura, com o documento da fatura (que nunca é enviado para o SAFE), e disponibiliza a fatura assinada ao empresário.

Fatura Sem Papel

A solução da “Fatura sem Papel” tem por objetivo o envio aos cidadãos ou empresas, de fatura digital decorrente da aquisição de bens ou serviços, substituindo, por sua opção, a versão física. Com esta solução pretende-se permitir a todo e qualquer empresário/comerciante, enviar para o email do seu cliente faturas emitidas, sem necessitar de obter o respetivo endereço de email.

A solução tem por missão o envio das faturas eletrônicas em formato digital emitidas pelos empresários que disponham de softwares de faturação eletrónica para os respetivos consumidores finais (pessoas singulares ou coletivas). Para tal, a solução recebe a respetiva fatura emitida pelo empresário, e o NIF/NIPC do titular, ao qual se encontra associado um endereço de correio eletrónico, para o qual é enviada a respetiva fatura.



Assim, a adesão ao serviço pelo cidadão é efetuada através do portal ePortugal. O processo de autenticação será através do serviço autenticação.gov, sendo necessário a obtenção do NIF associado. Neste portal, é disponibilizado o serviço de envio da fatura digital.

Aquando da emissão de uma fatura, caso o software do empresário/comerciante esteja integrado com a solução disponibilizada, e o cidadão tenha aderido à solução no ePortugal, a fatura eletrónica pode ser enviada de forma desmaterializada para o cidadão, conforme imagem seguinte.

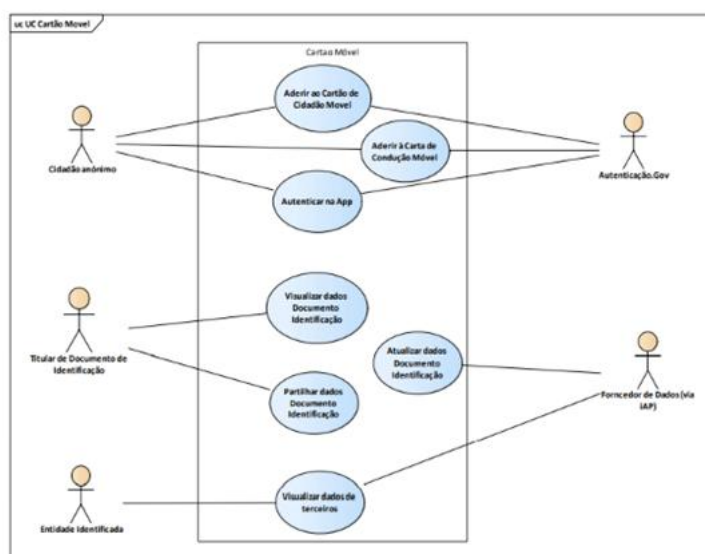


Figura 6 - Fluxo de envio de fatura

Gov.PT

Aplicação Móvel que possibilita ao cidadão “transportar” os seus documentos de identificação no seu telemóvel, assegurando-se que os dados apresentados e validade dos mesmos é coincidente e dependente da informação residente nos sistemas de informação públicos, nomeadamente Cartão de Cidadão, Carta de Condução e Cartão ADSE.

Os principais casos de uso encontram-se identificados no diagrama seguinte:

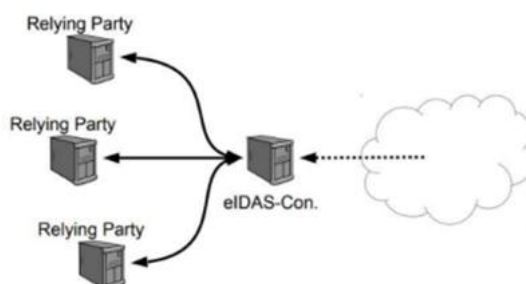


Principais componentes aplicacionais:

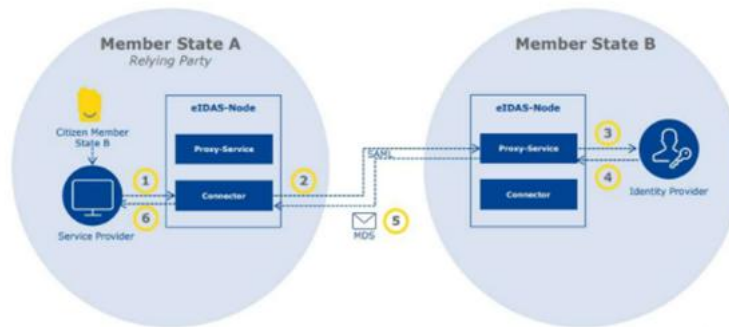


Nó eIDAS Nacional

De forma a assegurar a interoperabilidade de eID entre Estados Membros Portugal segue uma abordagem centralizada de um nó eIDAS Nacionais, com diferentes fornecedores de autenticação e atributos – conforme figura seguinte.



O funcionamento do nó eIDAS nacional encontra-se sistematizado na figura seguinte.



O nó eIDAS nacional suporta-se no serviço Autenticação.gov, disponibilizando os mecanismos de autenticação aí existentes (e.g., Cartão de Cidadão, Chave Móvel Digital e Sistema de Certificação de Atributos Profissionais).

Public API Marketplace

Trata-se de uma Plataforma pública para divulgação de APIs de serviços públicos disponibilizados a entidades públicas e privadas, sendo do especial interesse de entidades integradoras.

Numa primeira fase a AMA daria o exemplo disponibilizando as APIs para interação com a CMD, FA, Gov, SAFE, entre outros, e em fases seguintes disponibilizaria a plataforma para entidades como IRN/IGFEJ, AT, SS, IEFP, possam publicar as suas APIs numa plataforma pública oficial, assim como a integração com os seus ambientes de testes (poderá daqui surgir novas oportunidades para evolução da IAP para integração com mais entidades públicas e serviços das mesmas).

Os principais objetivos da solução são:

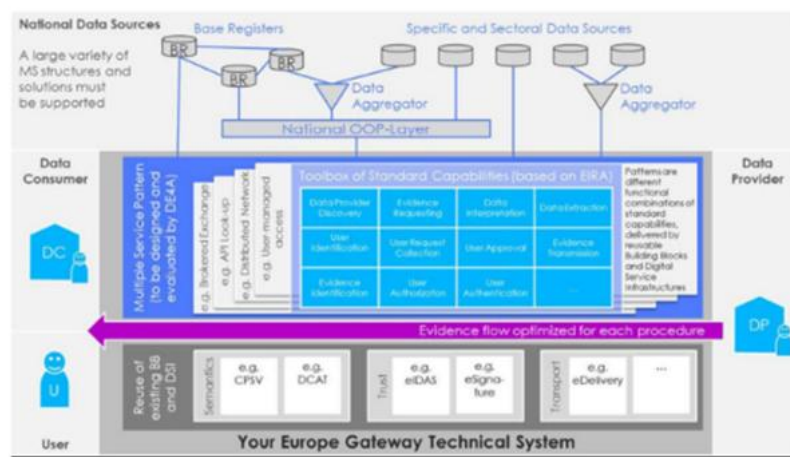
- Potenciar a utilização de serviços públicos disponibilizados à sociedade no geral
- Aumentar a visibilidade e “comercialização” dos serviços públicos digitais disponibilizados à sociedade
- Aumentar a maturidade digital da sociedade na utilização de serviços digitais disponibilizados pelo Estado Português
- Documentação apropriada das APIs e da forma de utilização (após registo e aprovação de conta para acesso à área privada)
- Disponibilizar ambientes de testes para as referidas APIs (após registo e aprovação de conta para acesso à área privada)

Digital Europe for All (DE4A)

Para um mercado único digital totalmente funcional, que permita efetivamente o exercício transfronteiriço dos cidadãos e das empresas dos seus direitos no mercado único, os Estados-Membros devem enfrentar vários desafios na prestação de melhores serviços.

O projeto Digital Europe for All (DE4A) é um piloto orientado pelos Estados-Membros, alinhado ao Plano de Ação Estratégico para o Governo Eletrónico 2016-2020 e com o EIF e com total conformidade regulamentar (SDGR, GDPR, eIDAS, Diretiva Serviços ...), estabelecendo uma cultura de cocriação, transparência, responsabilidade e confiabilidade. Tem por objetivo facilitar a migração para os Serviços Públicos Digitais Europeus em parceria entre países, entre setores e com diferentes participantes, reforçando a confiança nas instituições públicas e desencadeando múltiplos impactos positivos mensuráveis nos ganhos de eficiência e redução de encargos e custos administrativos.

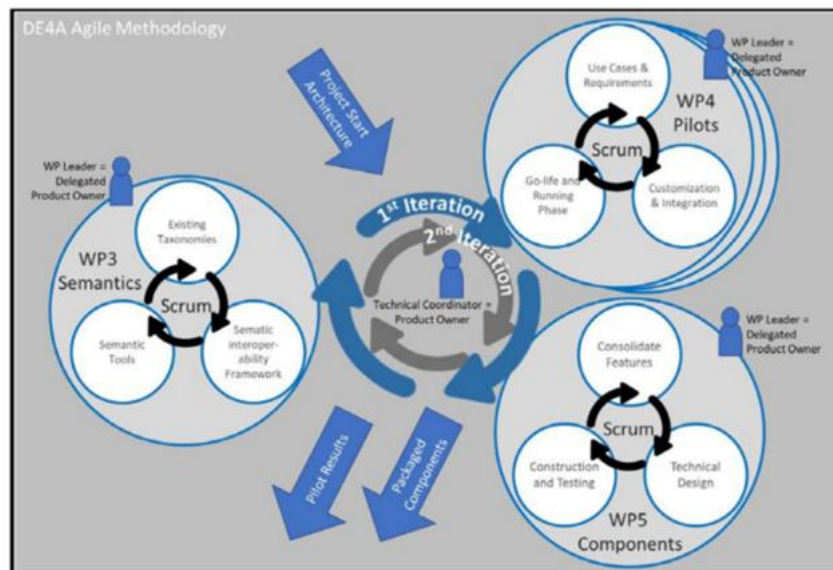
O DE4A inclui 25 parceiros e tem uma duração de três anos (com início em janeiro de 2020). Partindo das necessidades e capacidades dos Estados-Membros, a abordagem escalável, holística e flexível do DE4A concentra-se em procedimentos totalmente on-line de alta qualidade acessíveis através do Ponto único de contacto (ePortugal.gov.pt , no caso Português), com base em uma caixa de ferramentas de interoperabilidade estendida.



Tecnologias inovadoras como blockchain, machine learning, ontologias auto-emergentes e provas de zero knowledge proofs são abordadas.

Os pilotos que envolvem acesso seguro aos principais procedimentos administrativos da vida real e eventos de negócios devem destacar aspetos do ecossistema técnico disponível para a implementação dos Pontos únicos de contacto, provar sua viabilidade técnica e avaliar o desempenho e o grau em que os requisitos não funcionais podem ser atendidos. Entre os pilotos destacam-se os casos de uso: i) da mudança de morada e ii) de estudar noutro Estado Membro.

O projeto prevê-se que seja desenvolvido tendo por base uma metodologia ágil, conforme figura seguinte.



Building Blocks Identidade Digital – Arquitetura Empresarial na Administração Pública

Esta iniciativa visa promover princípios comuns de arquitetura empresarial na AMA, com representação de todos

os componentes de arquiteturas transversais numa arquitetura empresarial comum.

Tem por objetivos:

- Evoluir a capacidade de Arquitetura Empresarial nas equipas da AMA;
- Criação de elementos base da Arquitetura Empresarial na Administração Pública;
- Estabelecer modelo de governação da arquitetura empresarial, no âmbito do CDAP.

A AMA deverá dar resposta ao definido nas Metas PPR-C19 e Estratégia para a Transformação Digital 2021-2026.

Plano Identidade Digital 2025

Tendo em vista a orientação estratégica de desenvolver a Administração Pública Digital, esta iniciativa visa promover uma visão que permita dotar o país de uma identidade digital universal, segura e confiável, que suporte serviços públicos e privados em todos os canais garantindo uma experiência de utilização simples.

Objetivos:

- Coordenar o conjunto de iniciativas e metas organizadas em eixos de atuação;
- Promoção de casos de uso que permitam alavancar as iniciativas desenvolvidas.

A AMA deverá coordenar, em conjunto com o CDAP, as iniciativas a desenvolver que permitam implementar o Plano Identidade Digital 2025.

ECCE – Entidade Certificadora Comum do Estado

Coordenação e operacionalização de operações de gestão de infraestruturas de chaves públicas da ECCE, com especial enfoque na gestão e operacionalização destas infraestruturas, bem como a operacionalização e coordenação do fornecimento de certificados digitais, de várias tipologias, a todas as entidades que o solicitem no âmbito dos serviços prestados pela ECCE.

Objetivos:

- Garantir o fornecimento de certificados digitais a todas as entidades que os requisitem à AMA no âmbito da oferta existente na ECCE;
- Garantir as boas práticas de segurança das infraestruturas de chaves públicas da ECCE;
- Garantir o compliance da ECCE com os standards internacionais aplicáveis à tipologia de certificados digitais a fornecer (e.g. eIDAS);