CONCURSO PÚBLICO INTERNACIONAL N.º 92/21/DCP/GACD/

IDENTIDADE DIGITAL 2030

Caderno de Encargos

cláusulas jurídicas ____ **3**

Cláusula 1.ª Objeto ____ *3*

Cláusula 2.ª Local da prestação de serviços ____ *3*

Cláusula 3.ª Duração ____ *3*

Cláusula 4.ª Preço base ____ *3*

Cláusula 5.ª Condições de pagamento ____ *4*

Cláusula 6.ª Propriedade intelectual ____ *4*

Cláusula 7.ª Sigilo e Impedimentos ____ *5*

Cláusula 8.ª Proteção de dados ____ *6*

Cláusula 9.ª Cessão da posição contratual e subcontratação ____ *7*

Cláusula 10.ª Comunicações e notificações ____ *7*

Cláusula 11.ª Penalidades contratuais ____ *8*

Cláusula 12.ª Caução ____ *9*

Cláusula 13.ª Foro competente ____ *9*

Cláusula 14.ª Legislação aplicável ____ *9*

Cláusulas Técnicas ____ **10**

Cláusula 15.ª Descrição técnica e âmbito dos serviços ____ **10**

Cláusula 16.ª ____ *30*

Requisitos específicos de implementação para o tratamento de dados pessoais ____ *30*

Cláusula 17.ª ____ *31*

Acessibilidade e Usabilidade ____ *31*

Cláusula 18ª Perfil técnico dos recursos a afetar aos serviços ____ *32*

Cláusula 19ª Substituição das equipas ____ *35*

Cláusula 20ª Planeamento ____ *35*

Cláusula 21ª Entregáveis e documentação ____ *35*

Cláusula 22ª Mecanismos Formais de Acompanhamento ____ *36*

Cláusula 23ª Outras condições ____ *37*

Cláusula 24ª Gestor do Contrato ____ *37*

Cláusula 25.ª Gestão de Dados ____ *37*

Cláusula 26.ª Requisitos específicos de implementação para a segurança de informação ____ *38*

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por "AMA"), na sequência de procedimento pré-contratual que tem por objeto a aquisição de serviços de gestão de projeto, gestão estratégica, arquitetura de sistemas de informação, testes, suporte e operação de iniciativas de Identidade Digital, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de serviços

Os serviços serão prestados nas instalações da AMA, sitas em Lisboa e remotamente, sempre que indicado pela AMA.

Cláusula 3.ª

Duração

O contrato terá a duração estimada de 26 meses a contar do visto prévio do Tribunal de Contas ou da data da sua celebração se o seu valor for inferior a 750.000,00 €, terminando no máximo a 31 de dezembro de 2023, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base

1. O preço base é de € 971 520,00 (novecentos e setenta e um mil, quinhentos e vinte euros), acrescido de IVA à taxa legal.
2. São excluídas as propostas cujo valor seja superior ao preço base.
3. 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) Seguro de acidentes de trabalho.

Cláusula 5.ª

Condições de pagamento

1. A faturação é efetuada trimestralmente, após aceitação pela AMA de relatório referente aos trabalhos realizados no último trimestre.
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, 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 às tarefas efetivamente prestadas 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. Só são efetuados pagamentos após o pagamento dos emolumentos devidos ao Tribunal de Contas pela concessão do visto pelo cocontratante, nos termos do artigo 7.º do Decreto-Lei n.º 66/96, de 31 de maio.

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 e 49.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 no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos desenvolvidos, incluindo as respetivas fontes que serão propriedade da AMA.
4. A AMA poderá transformar e reproduzir todos os documentos e todo o software desenvolvido, bem como proceder à sua distribuição, onerosa ou gratuita, de forma inteiramente livre.
5. Pela cessão dos direitos a que alude o número dois não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos.

Cláusula 7.ª

Sigilo e Impedimentos

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 ser 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.

8. O dever de sigilo mantém-se em vigor até ao termo do prazo de 20 (vinte) anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

9. O cocontratante fica impedido de se candidatar, concorrer ou integrar qualquer agrupamento nos procedimentos de contratação pública a lançar pela AMA IP, em que tenha prestado assessoria ou apoio técnico na preparação e elaboração das peças do procedimento nos termos previstos no ponto 3.1 das clausulas técnicas do presente caderno de encargos.

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 (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD), devendo, nomeadamente:

a) Tratar os dados pessoais apenas mediante instruções documentadas da AMA, 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 AMA 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 AMA 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 AMA 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 AMA, 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 AMA 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 AMA ou por outro auditor por esta mandatado.

2. A AMA, 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 AMA 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 AMA 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, por fim ao incumprimento e demonstrá-lo à AMA.

6. O não cumprimento do RGPD, por facto imputável ao cocontratante, é considerado, para todos os efeitos, incumprimento definitivo, podendo a AMA 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 AMA 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. O incumprimento de qualquer das obrigações decorrentes para o cocontratante da celebração do contrato, determina a aplicação pela AMA de sanções pecuniárias ao mesmo, nos termos previstos nos números seguintes.
2. No caso de incumprimento dos prazos fixados e/ou níveis de serviço estipulados, bem como dos entregáveis acordados e por causa imputável ao cocontratante, poderá ser aplicada uma penalidade, calculada de acordo com a seguinte fórmula:
    a) P=V*A/500

       em que:

       P - Corresponde ao montante da penalidade;

       V - Corresponde ao valor do contrato; e,

       A - Corresponde ao número de dias em atraso.

    b) Pela não comparência do Cocontratante em qualquer reunião, independentemente da parte que a convocou, poderá ser aplicada uma sanção de 250 €.

    c) Pelo incumprimento dos requisitos exigidos para cada recurso previstos na cláusula 18.ª e apresentados na proposta, poderão ser aplicadas penalidades até 0,3% do preço contratual por cada dia de incumprimento;

    d) Pela não comparência dos recursos previstos poderá ser aplicada uma penalidade até 0,3% do preço contratual por cada dia em falta;

    e) Pelo incumprimento das regras para substituição dos recursos previstas na cláusula 19.º poderá ser aplicada uma penalidade até 0,3% do preço contratual por cada dia de incumprimento.
3. 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.
4. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.

5. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.
6. 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 %.
7. A aplicação das sanções previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 12.ª

Caução

1. O cocontratante deverá prestar uma caução destinada a garantir a celebração do contrato, bem como o exato e pontual cumprimento de todas as obrigações legais e contratuais que assume com essa celebração, no valor de 5% do preço contratual.
2. Ao prazo e ao modo de prestação da caução, assim como à determinação da responsabilidade pelas respetivas despesas, é aplicável o previsto no artigo 90.º do CCP.
3. Os modelos referentes à caução são os previstos no Anexo III ao programa de concurso.

Cláusula 13.ª

Foro competente

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

Cláusula 14.ª

Legislação aplicável

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

CLÁUSULAS TÉCNICAS

CLÁUSULA 15.ª

DESCRIÇÃO TÉCNICA E ÂMBITO DOS SERVIÇOS

1. Enquadramento

A AMA é responsável por soluções de autenticação que visam garantir a segurança, física e eletrónica, reduzindo os riscos de fraude e preservando os direitos de confidencialidade e privacidade dos dados pessoais.

Como objetivos principais destacam-se a simplificação, a segurança, e o desenvolvimento de serviços eletrónicos eficientes, racionais, e em conformidade com os requisitos da União Europeia.

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

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por outro canal (SMS, App mobile, entre outros). Este mecanismo de identificação está disponível para cidadãos nacionais e não nacionais, permitindo a sua associação a documentos como o Passaporte, o Título de Residente e o Cartão de Residência.
A AMA desenvolve ainda diversos projetos de inovação, transferência de tecnologia e Transformação digital no contexto da identificação eletrónica, enquadrados em programas europeus e nacionais (e.g., CEF, H2020, POCI/COMPETE 2020), que importa gerir, monitorizar e otimizar.

2. Plataformas Tecnológicas Relevantes para os Serviços a Prestar

Nesta secção apresenta-se uma descrição sucinta de projetos já realizados ou em curso que se consideram relevantes no âmbito deste procedimento.

2.1. 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:

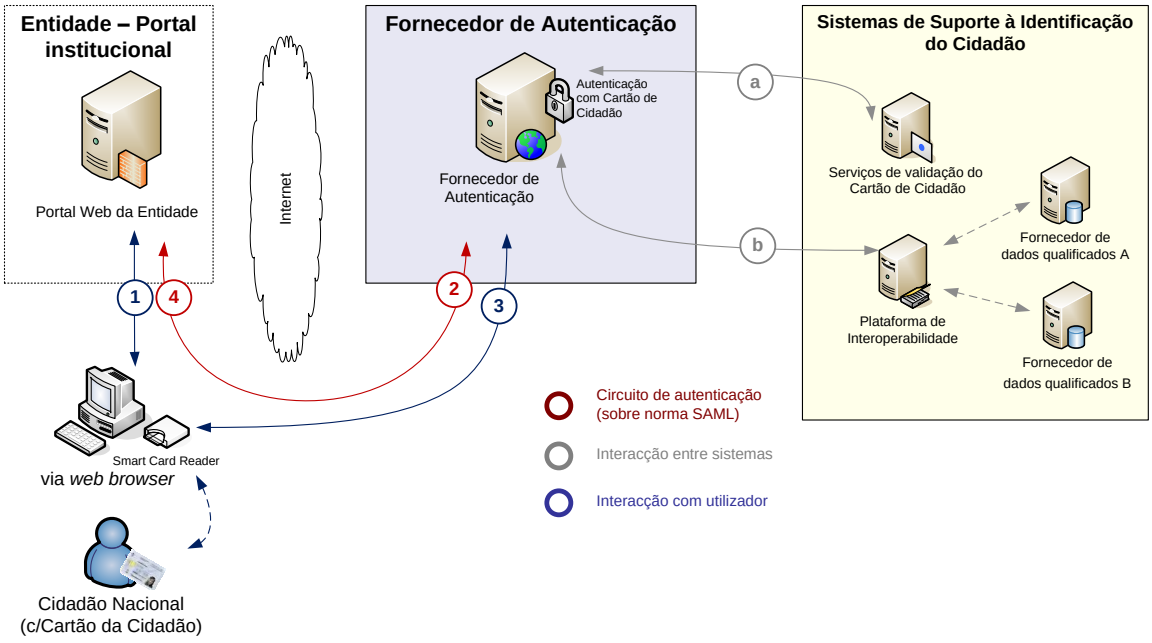
- Ser o **documento de Identificação Nacional Presencial de Elevada Segurança**, designadamente de forma a ultrapassar os reconhecidos problemas de segurança, contrafação e falsificação inerentes ao Bilhete de Identidade;
- **Substituir 5 cartões** de identificação, agregando num único documento os respetivos n.º de identificação;
- Ser o mecanismo de **Autentificação 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;
- Permitir a **autenticação** forte do cidadão por **canais alternativos**, nomeadamente o telefone (para cidadãos que não usam a Internet);

- 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").

2.2. 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.

2.3. 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.

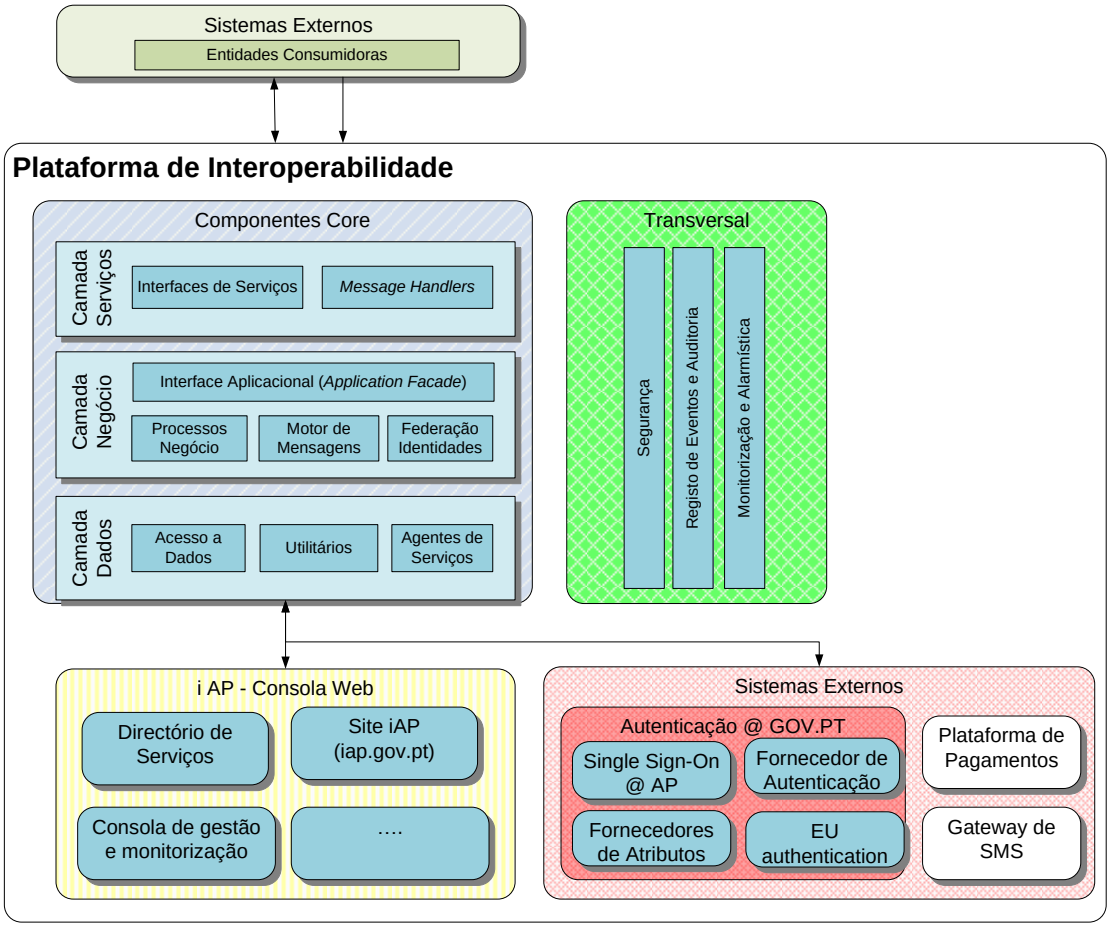


Figura 2 – Arquitetura lógica

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:
  - **Diretório de Serviços** – responsável pela listagem e gestão dos serviços eletrónicos disponibilizados pela Plataforma;
  - **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;
  - **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:
  - **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.

2.4. 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.

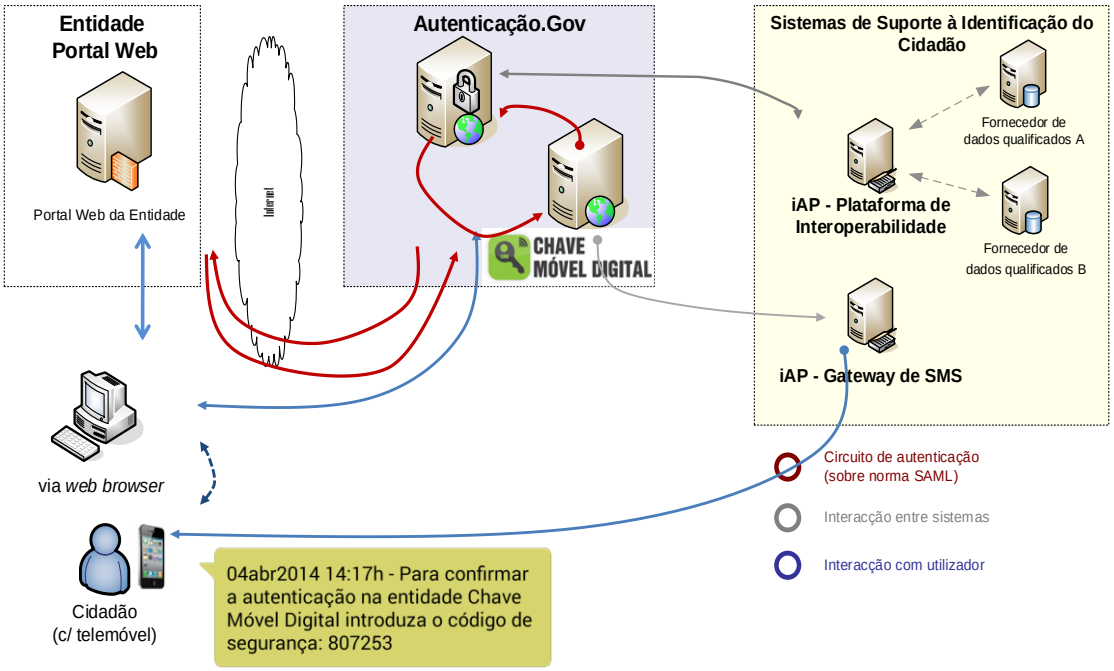
Do ponto de vista funcional a utilização da CMD passa pelos seguintes passos:
1 – O cidadão acede ao portal ou sítio da Administração Pública na Internet
2 – O cidadão insere a sua identificação (número de telemóvel) e palavra-chave
3 – O cidadão recebe por SMS o código de utilização único por cada autenticação gerado pela CMD para confirmar os dados e concluir a autenticação
4 – O cidadão insere o código no computador
5 – O cidadão faz Login

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.

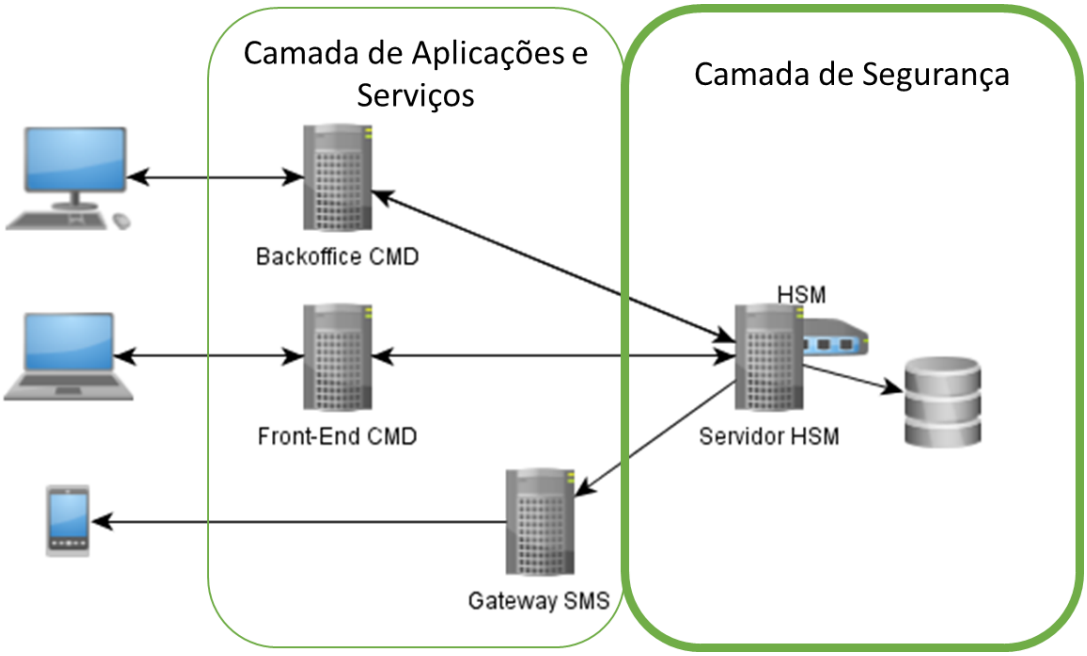
A CMD encontra-se já disponível em vários portais e sistemas (como o ePortugal (Portal do Cidadão), Portal do Utente, entre outros), assegurando:

- 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:



2.5. 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.

[1] Para mais detalhes em relação ao projeto Cartão de Cidadão ver http://www.cartaodecidadao.pt e https://pki.cartaodecidadao.pt

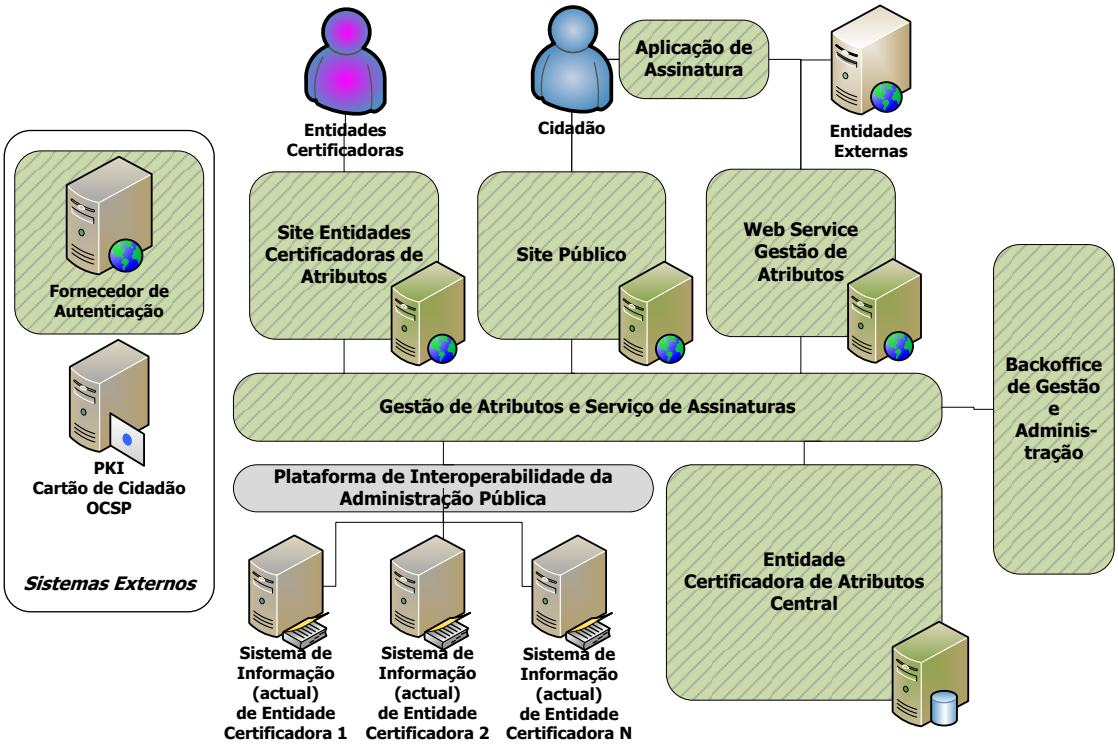


Figura 3 – Arquitetura Global da Solução

2.6. 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.

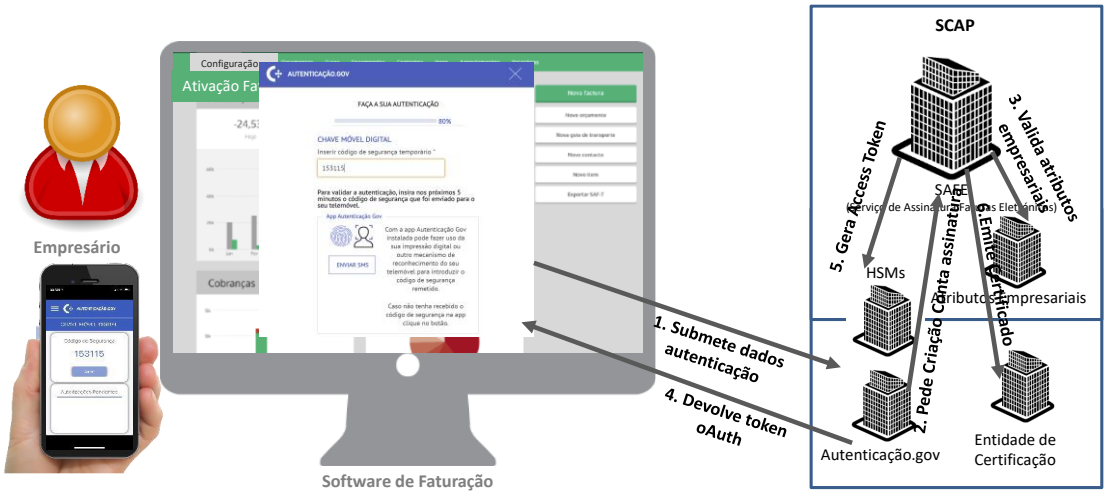


Figura 4 – Emissão periódica de certificado para emissão de fatura

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.

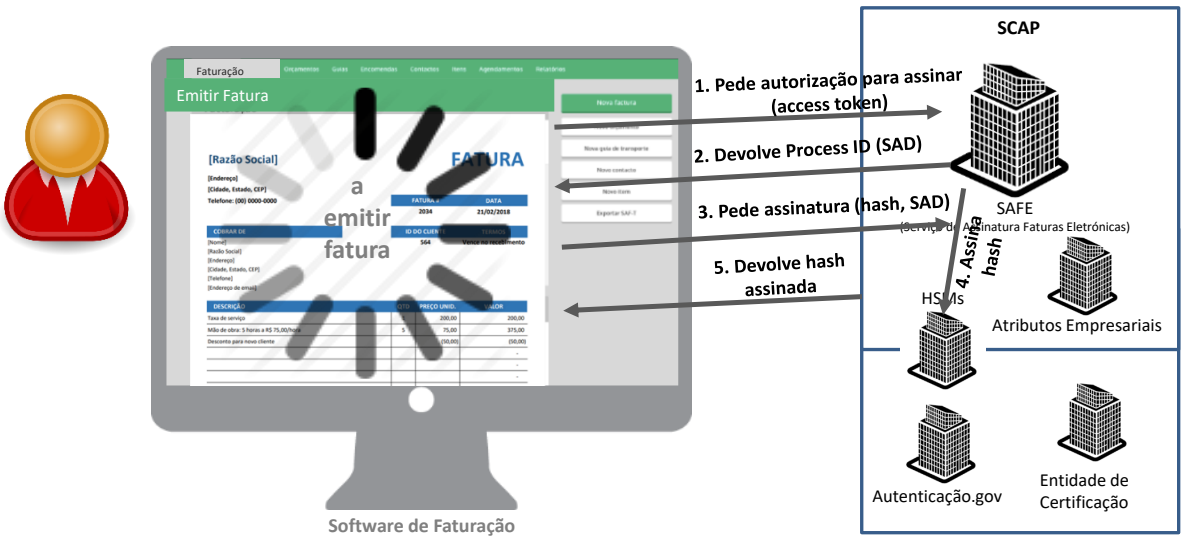


Figura 5 – Assinatura de fatura com SAFE

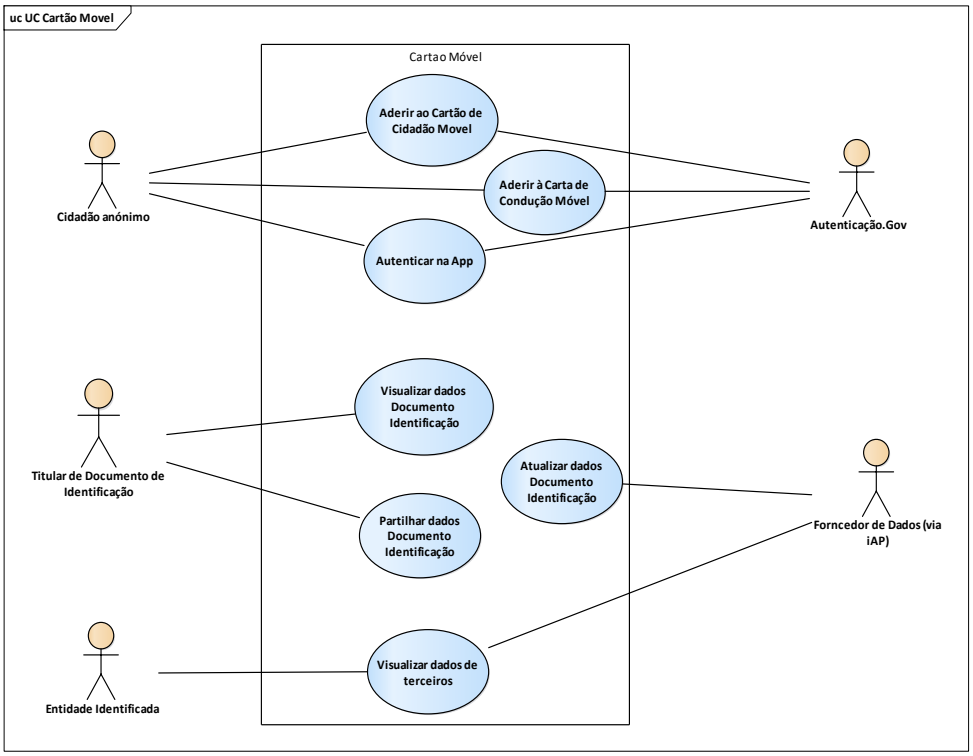
Assim, aquando da emissão da fatura, o software de faturação (devidamente autenticado) envia para o SAFE o "Acess token" (obtido aquando da ativação periódica do certificado, previamente descrito) e, seguindo uma sequência standard para a geração de assinaturas, é gerado um identificador do processo 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.

2.7. Id.Gov.PT

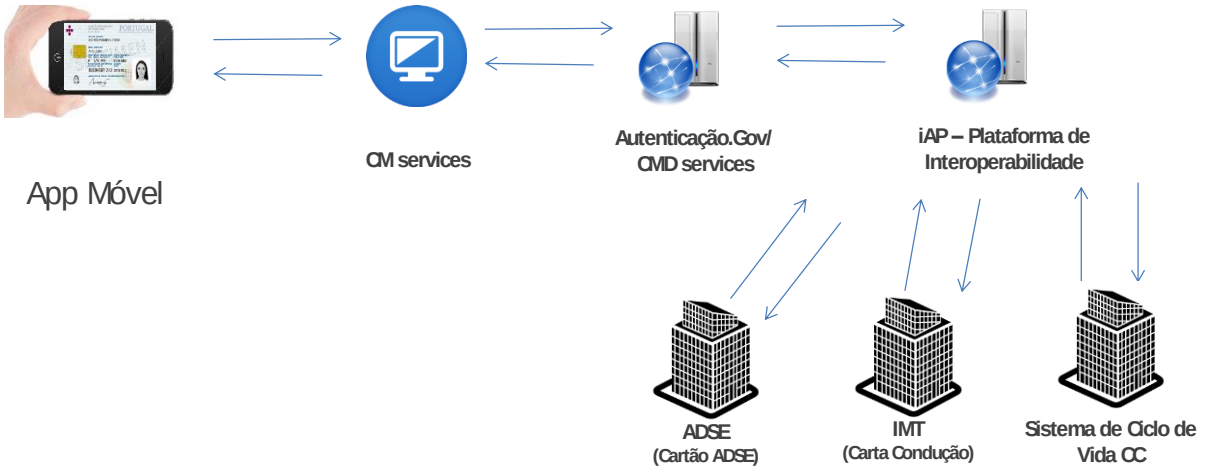
Aplicação Móvel que possibilita ao cidadão "transportar" os seus documentos de identificação no seu telemóvel, assegurando-se que os dados apresentados e validade dos mesmos é coincidente e dependente da informação residente nos sistemas de informação públicos, nomeadamente Cartão de Cidadão, Carta de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



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

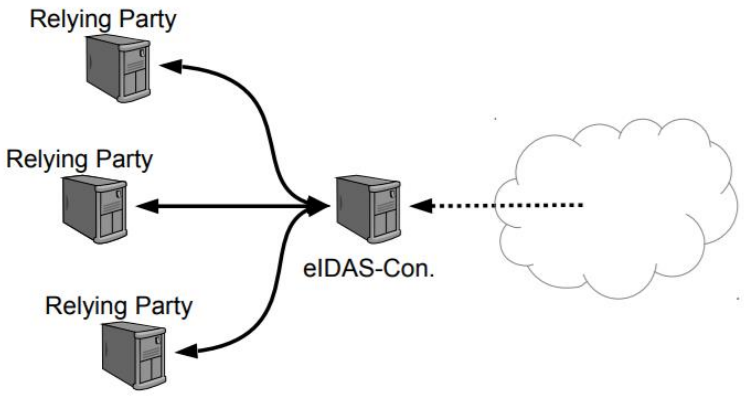


Principais componentes aplicacionais:

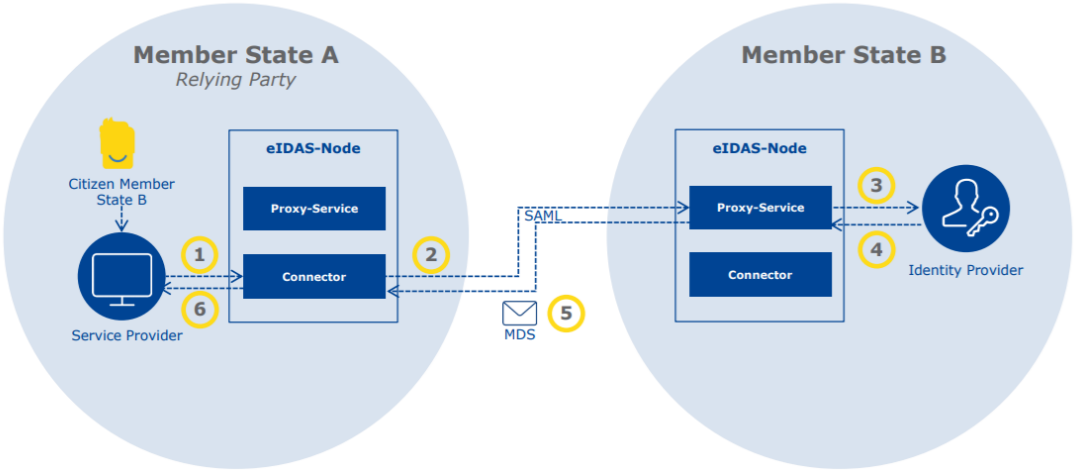


2.8. Nó eIDAS Nacional

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).

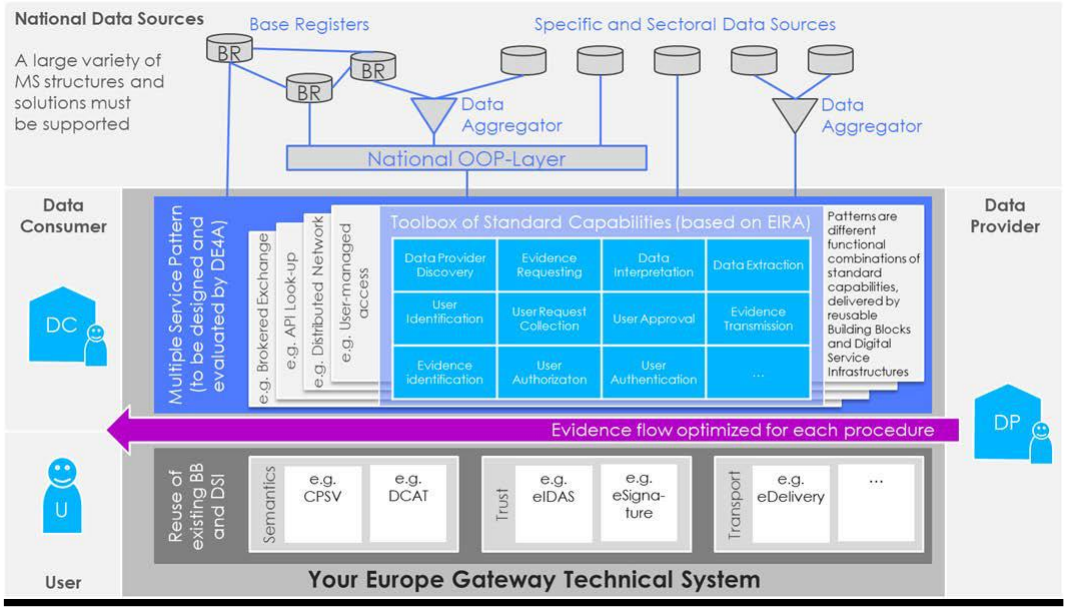
2.9. Digital Europe for All (DE4A)

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 Eletrônico 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 27 parceiros e tem uma duração de três anos (com início em janeiro de 2020).

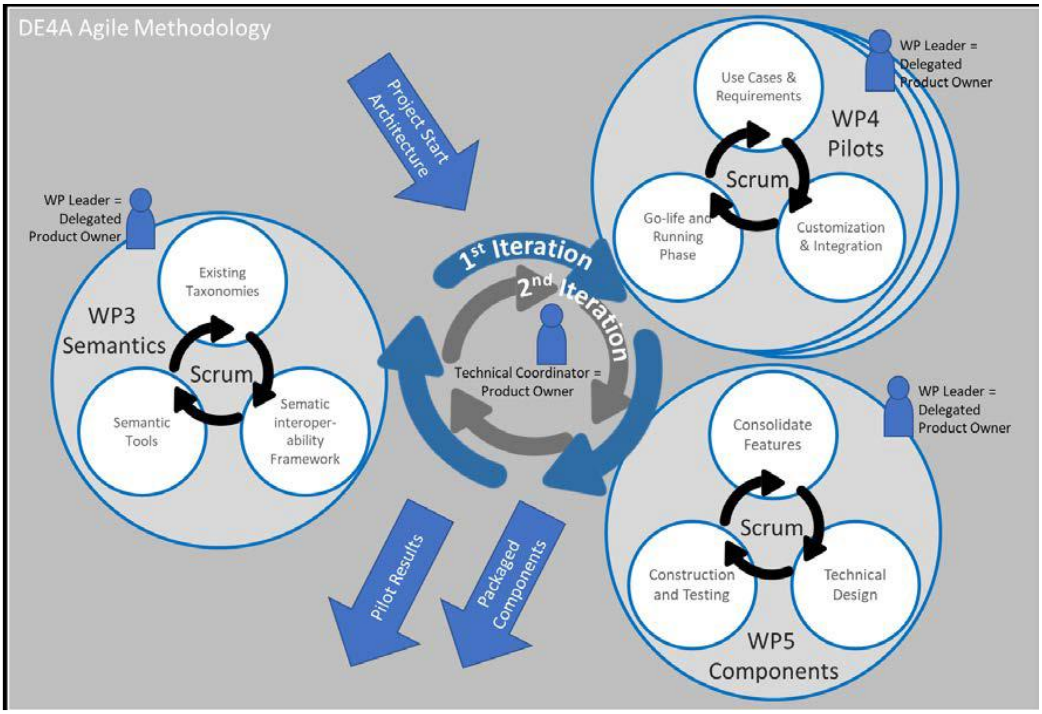
Partindo das necessidades e capacidades dos Estados-Membros, a abordagem escalável, holística e flexível do DE4A concentra-se em procedimentos totalmente on-line de alta qualidade acessíveis através do Ponto único de contacto (ePortugal.gov.pt , no caso Português), com base em uma caixa de ferramentas 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.



3. Âmbito dos Serviços

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

3.1 Objetivos e atividades no âmbito deste procedimento

De uma forma geral, as atividades descritas neste capítulo serão executadas pela equipa proposta pelo cocontratante, com colaboração da AMA, e têm por objetivo a gestão de projeto, a definição das soluções tecnológicas e funcionais, e os testes e controlo de qualidade, o suporte a utilizadores e parceiros no uso e adesão às funcionalidades e soluções descritas no ponto 2, nas seguintes áreas:

- Ao nível estratégico e de gestão de projeto:
    - O levantamento detalhado de requisitos designadamente da situação atual a nível dos processos e organização;
    - O levantamento e sistematização das melhores práticas mundiais no âmbito das áreas de intervenção do projeto, do ponto de vista processual e funcional;
    - O suporte na definição de protótipos, o acompanhamento e gestão da implementação de protótipos (a realizar por várias outras entidades), a sistematização de resultados do

protótipo, a identificação de conclusões;

- O desenho e especificação organizacional e processual da solução a implementar;
- A elaboração das cláusulas técnicas dos Cadernos de Encargos para a implementação processual e funcional;
- A definição de estratégia de comunicação da mudança;
- Realização de gestão de projeto incluindo o planeamento, monitorização, gestão de âmbito, gestão cronograma, gestão de custo, gestão da qualidade, gestão de recursos, e gestão de stakeholders.

- Ao nível tecnológico:
  - O levantamento detalhado de requisitos designadamente da situação atual a nível dos sistemas e tecnologias de informação das entidades envolvidas;
  - O levantamento e sistematização das melhores práticas mundiais no âmbito das áreas de intervenção do projeto.
  - O desenho e especificação tecnológica da solução a implementar;
  - A elaboração das cláusulas técnicas dos Cadernos de Encargos para a implementação dos vários sistemas de informação no âmbito deste projeto;
  - A execução de testes e controlo de qualidade
  - O suporte, despiste tecnológico e intermediação entre as equipas de 1ª linha e as equipas de desenvolvimento e infra-estrutura.

Mais concretamente, pretende-se que o cocontratante forneça consultoria tendo em vista os seguintes objetivos:

1. Estratégia e Gestão de Projetos

1.1. Detalhe da Visão e Objetivos da Identidade Digital 2030, nomeadamente:

1.1.1. O que deve ser a Identidade Digital

1.1.2. Para que deve servir

1.1.3. Que dados deve disponibilizar

1.1.4. Benefícios esperados

1.1.5. Condicionantes (prazos, standards, entidades a envolver)

1.1.6. Identificação de riscos

1.2. Levantamento da realidade Europeia ao nível das valências eletrónicas (autenticação e assinatura) de identidade digital e documentos de identificação (ou mecanismos paralelos)

1.2.1. Definição de metodologia e parâmetros comparativos para levantamento de benchmarking europeu

1.2.2. Levantamento e sistematização das melhores práticas europeias no âmbito das áreas de intervenção do projeto (e.g., identidade, cartões de e-ID/ saúde/ bancários (e acessórios), autenticação, PKI, entre outros)

1.2.3. Produção de relatório analítico das diferentes realidades, para cada um dos parâmetros analisados, com indicação de tendências de evolução tecnológica e estratégica

1.3. Proposta e apoio à implementação de modelo de governação para a identidade digital em Portugal.

1.4. Gestão de projeto e suporte na implementação do novo Cartão de Cidadão, no contexto do RE 2019/1157, designadamente o levantamento da situação atual, proposta e gestão da implementação de alterações ao nível visual, eletrónico e de segurança no Cartão de Cidadão.

1.5. Análise de Valor

- Identificação de Modelos de Negócio aplicáveis e seus impactos na exploração da identidade digital
- Identificação do Valor a obter com a concretização da identidade digital (benefícios, quantificáveis e não quantificáveis)
- Definição de indicadores para aferição da obtenção dos benefícios

1.6. Análise Financeira e Modelo de Financiamento

- Identificação de custos de investimento
- Identificação de custos de funcionamento
- Identificação de potenciais receitas
- Análise financeira do retorno de investimento associado
- Identificação de Modelos de Negócio aplicáveis e seus impactos

1.7. Gestão de Projetos identidade digital, incluindo reporting aos vários órgãos de governação internos e externos à AMA.

1.8. Gestão e execução de projetos e iniciativas nacionais e europeias em que a AMA participa.

1.9. Levantamento e manutenção de arquitetura empresarial do ecossistema de identidade digital (incluindo contexto interno e externo à AMA)

2. Adesão e Gestão de Parceiros de Identidade Digital

2.1. Levantamento da situação atual (em termos processuais e tecnológica).

2.2. Proposta de revisão de processos e procedimento adesão.

2.3. Execução de processos de adesão de parceiros a plataformas de identidade digital (e.g., fornecedor de autenticação, CMD assinatura, SCAP, SAFE, id.gov, nó eIDAS, entre outros), incluindo disponibilização

de documentação, esclarecimento de dúvidas de adesão, despiste de problemas, execução de testes, certificação de qualidade, execução de configurações, reunião com parceiros, articulação de equipas internas e externas, entre outros.

3. Suporte e Controlo de Qualidade

3.1. Suporte a centro de contactos e intermediação com equipas de desenvolvimento e infra-estrutura (Help-desk especializado).

3.2. Resposta a utilizadores das soluções de identidade digital.

3.3. Monitorização e Estatísticas das Plataformas eID, incluindo a configuração de ferramentas e recolha e disponibilização de indicadores periódicos das soluções de eID.

3.4. Testes Novas Funcionalidades, incluindo definição de plano de testes, execução de testes (funcionais, segurança, carga, integração, usabilidade, ou outros), disponibilização de relatórios de testes.

3.5. Implementação de devOps no âmbito dos projetos descritos na secção 2, incluindo:

- Proposta de metodologia para implementação de devops
- Análise e proposta de ferramentas para suportar devops, tendo por base as ferramentas existentes na organização e as melhores práticas Internacionais (incluindo contolo de logs, controlo de versões, depuração e controlo de qualidade de código fonte, gestão de configurações, integração contínua, monitorização, testes, orquestração processo devops, entre outras)
- Implementação de fluxo devops, incluindo:
  - Integração contínua (Continuous integration), assegurando que o código está continuamente atualizado, disponível e automaticamente testado num repositório comum
  - Entrega contínua (Continuous delivery), assegurando que as alterações ao código são automaticamente construídas, testadas e empacotadas para disponibilização em produção
  - Instalação contínua (Continuous deployment), assegurando a total automatização da disponibilização em produção de correções, e novas funcionalidades
  - Monitorização e feedback contínuo, assegurando a medição em tempo real e feedback dos produtos, permitindo feedback imediato do IT às equipas de desenvolvimento

Cláusula 16.ª

Requisitos específicos de implementação para o tratamento de dados pessoais

1. A arquitetura das soluções a propor deverá contemplar:
   a) Gestão de permissões para os vários utilizadores que permita uma gestão ao nível de cada dado pessoal;
   b) Funcionalidades que permitam:
      i) Mascarar 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 das soluções 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.

Cláusula 17.ª

Acessibilidade e Usabilidade

1. No âmbito dos trabalhos a desenvolver, o cocontratante obriga-se a garantir que os entregáveis objeto deste procedimento cumprem as obrigações legais, os requisitos e as melhores práticas no que se refere às áreas da Acessibilidade, Usabilidade e Experiência de Utilização dos sítios *Web* e das aplicações móveis, nomeadamente os seguintes fatores essenciais:
   a) Cumprimento do Decreto-Lei n.º 83/2018, de 19 de outubro, que transpõe para a ordem jurídica interna a Diretiva (UE) 2016/2102, do Parlamento Europeu e do Conselho, de 02 de dezembro de 2016, relativa à Acessibilidade dos sítios Web e das aplicações móveis dos organismos do setor público, nomeadamente o nível de conformidade "AA" das WCAG 2.1 do W3C, que equivale à norma europeia EN 301 549 harmonizada;
   b) Elaboração da Declaração de Acessibilidade e Usabilidade prevista nos Artigos 8.º e n.º 5 do artigo 9.º do Decreto-Lei n.º 83/2018, bem como as respetivas evidências, nos termos estipulados no referido diploma legal e nos sítios Web https://selo.usabilidade.gov.pt/index.html e http://www.acessibilidade.gov.pt;
   c) Cumprimento do Regulamento Nacional de Interoperabilidade Digital (RNID), estabelecido nos termos do artigo 5.º da Lei n.º 36/2011, de 21 de junho, e aprovado através da Resolução do Conselho de Ministros n.º 91/2012, de 08 de novembro, alterado pela Resolução do Conselho de Ministros n.º 2/2018, de 5 de janeiro, na redação conferida pelo Decreto-Lei n.º 83/2018, nomeadamente quanto à alteração da Tabela III "Tecnologias de interface Web, incluindo acessibilidade, ergonomia, compatibilidade e integração de serviços";
   d) Cumprimento dos requisitos do Selo de Usabilidade e Acessibilidade e respetiva aposição, de acordo os parâmetros definidos no sítio Web https://selo.usabilidade.gov.pt/, devendo garantir, em conjunto com a Declaração de Acessibilidade e Usabilidade, o nível mínimo de _____ [selecionar: Selo Prata (https://selo.usabilidade.gov.pt/prata.html) [caso se trate de sítio Web novo, de sítio Web pré-existente e alvo de renovação substancial ou de aplicação móvel novo] ou Selo Bronze (https://selo.usabilidade.gov.pt/bronze.html) [caso se trate de sítio Web pré-existente e alvo de melhorias ou aplicação móvel pré-existente e alvo de renovação substancial]];
   e) Cumprimento das melhores práticas de Acessibilidade, Usabilidade e Experiência de Utilização coligidas nos sítios Web http://www.acessibilidade.gov.pt/, https://usabilidade.gov.pt/menu-interior e https://selo.usabilidade.gov.pt/bronze.html, em articulação com a Equipa de Experiência Digital, da

Direção de Transformação Digital da AMA.

Cláusula 18ª

Perfil técnico dos recursos a afetar aos serviços

1. Os recursos humanos do cocontratante serão integrados em equipa de projeto da AMA e desenvolverão as suas atividades na sede da AMA ou remotamente, sempre que indicado pela AMA.
2. Para a execução dos serviços de consultadoria suprarreferidos deverá ser prevista uma equipa com os seguintes perfis e, no mínimo, a seguinte afetação:
   - Um Gestor de Projeto sénior que desenvolverá as atividades descritas no CE, que assessorá a estrutura da AMA e coordenará os trabalhos a desenvolver pela equipa, sendo o principal interlocutor com a estrutura de coordenação a designar pela AMA, com experiência superior a 5 anos, dedicação ao projeto de 100 %, e:
     - Experiência anterior em projetos relacionados com o Cartão de Cidadão ou Chave Móvel Digital;
     - Formação superior em Informática ou Engenharia Informática sendo valorizada formação complementar em gestão;
     - Licenciatura em engenharia, gestão ou economia;
     - Credenciação do Gabinete Nacional de Segurança ou demonstrar que iniciaram o processo de credenciação junto da referida entidade;
     - Experiência em gestão de projetos de gestão de mudança na Administração Pública e no tecido privado no âmbito das TIC:
     - Participação em 10 projetos de gestão da mudança nas TIC;
     - Experiência como gestor de projeto em 5 projetos de gestão da mudança;
     - Experiência em gestão e coordenação de equipas internas, externas à Administração Pública:
       - Experiência na gestão e coordenação de equipas pluridisciplinares, de pelo menos 5 anos;
       - Experiência na gestão e coordenação de equipas intra e interministeriais, de pelo menos 2 anos;
     - 5 ou mais anos de experiência de coordenação de equipas envolvidas em projetos de consultadoria e de tecnologias de informação e comunicações.
   - Um Consultor Funcional sénior que desenvolverá as atividades descritas no CE, com experiência superior a 5 anos, dedicação ao projeto de 100 %, e:
     - Experiência anterior em projetos relacionados com o Cartão de Cidadão, e Chave Móvel Digital.

- Licenciatura em gestão, economia ou engenharia (ou equivalente);
- Experiência em implementação e gestão de projetos de gestão de mudança na Administração Pública e no tecido privado no âmbito das TIC:
- Participação em 10 projetos de otimização de processos e gestão da mudança nas TIC;
- Experiência como gestor de projeto em 5 projetos de gestão da mudança;

- Um consultor Tecnológico, com experiência nas tecnologias e soluções descritas na secção 2, em particular no desenho de arquiteturas de projetos em tecnologia .NET, nomeadamente na linguagem C#, ASP, ASPX, que será responsável pela configuração de parceiros nas plataformas de eID, pelos testes e pela certificação de qualidade das Soluções, e pelo suporte e despiste de incidentes, com experiência tecnológica superior a 5 anos, com uma dedicação ao projeto igual a 100%, preferencialmente com:
  - Experiência anterior em projetos relacionados com o Cartão de Cidadão, Chave Móvel Digital e plataformas descritas no presente caderno de encargos;
  - Formação superior tecnológica;
  - Licenciatura nas áreas de Engenharia Informática, Sistemas de Informação, Engenharia Eletrotécnica;
  - Experiência comprovada (superior a 3 anos) em:
    - Implementação de projetos na tecnologia.NET, nomeadamente na linguagem C#, ASP, ASPX;
    - Implementação de projetos Mobile recorrendo a plataforma Xamarin;
    - Implementação com utilização de SGBD relacional;
    - Notação UML;
    - Implementação de projetos com Service Oriented Architectures (SOA), fazendo uso de SOAP, XML, e normas WS*.
- Dois consultores Tecnológicos, com experiência nas tecnologias e soluções descritas na secção 2, em particular no desenho de arquiteturas de projetos em tecnologia Java e Liferay, que serão responsáveis pela configuração de parceiros nas plataformas de eID, pelos testes e pela certificação de qualidade das Soluções e pelo suporte e despiste de incidentes, com experiência tecnológica superior a 5 anos, com uma dedicação ao projeto igual a 100% (cada recurso), preferencialmente com:
  - Experiência anterior em projetos relacionados com o Cartão de Cidadão, Chave Móvel Digital e plataformas descritas no presente caderno de encargos;
  - Formação superior tecnológica;
  - Licenciatura nas áreas de Engenharia Informática, Sistemas de Informação, Engenharia

Eletrotécnica;

- Experiência comprovada (superior a 3 anos) em:
  - Implementação de projetos na tecnologia Java e preferencialmente em LifeRay;
  - Implementação com utilização de SGBD relacional;
  - Notação UML;
  - Implementação de projetos com Service Oriented Architectures (SOA), fazendo uso de SOAP, XML, e normas WS*.

- Um Consultor Estratégico sénior que desenvolverá as atividades descritas no CE, com experiência superior a 5 anos, dedicação ao projeto de 50%, e:
  - Experiência anterior em projetos relacionados com o Cartão de Cidadão, e Chave Móvel Digital.
  - Licenciatura em Engenharia Informática, eletrotécnica (ou equivalente);
  - Experiência em implementação e gestão de projetos de gestão de mudança na Administração Pública e no tecido privado no âmbito das TIC.
- Um Arquiteto de Sistemas de Informação desenvolverá as atividades descritas no CE, com experiência profissional superior a 5 anos, dedicação ao projeto superior ou igual a 50 % e:
  - Experiência anterior em projetos relacionados com o Cartão de Cidadão, e Chave Móvel Digital.
  - Licenciatura em Engenharia Informática, eletrotécnica (ou equivalente);
  - Experiência em implementação e gestão de projetos de gestão de mudança na Administração Pública e no tecido privado no âmbito das TIC.

3. O cocontratante deverá fornecer a seguinte informação sobre os recursos: Curricula Vitae expurgados de dados pessoais, mas em que seja inequívoco relacionar o mesmo ao recurso que vai prestar o serviço e que deverão conter, no mínimo, os seguintes dados:

- Data da Contratação, Função na organização e tipo de vínculo;
- Habilitações literárias;
- Formação profissional;
- Experiência profissional;
- Descrição de tarefas e projetos anteriormente desenvolvidos de acordo com as funções e requisitos pretendidos;
- Outros conhecimentos e experiências úteis para as funções.

Cláusula 19ª

Substituição das equipas

1. Qualquer alteração à composição da equipa indicada em sede de formação do contrato deve ser previamente comunicada à AMA e só será aceite caso reúna os requisitos mínimos exigidos na cláusula anterior bem como os propostos em sede de proposta, podendo, para o efeito, ser solicitada informação e documentação adicional para confirmação dos elementos curriculares apresentados.
2. A substituição referida no número anterior deverá ocorrer da seguinte forma:
    a) O cocontratante deverá, em 5 dias úteis, identificar o seu melhor recurso considerando os requisitos mínimos exigidos 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.
3. 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 comummente expectável, poderá a AMA exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

Cláusula 20ª

Planeamento

1. Os serviços suprarreferidos deverão ser iniciados após a celebração do contrato e integralmente concluídos num prazo de **26 meses (até 31-12-2023)**, 24 meses de trabalho efetivo (com a interrupção dos trabalhos durante 2 meses, em datas a definir pela AMA).
2. Espera-se que o cocontratante apresente em fase de propostas um calendário para o desenvolvimento dos serviços apresentados no ponto 3.1 da cláusula 15.ª, com indicação clara da alocação dos recursos e sua alocação às diferentes fases e entregáveis do projeto.
3. O planeamento apresentado pode vir a sofrer alterações em função de prioridades no decurso do projeto, ou em reunião de Kick-Off do projeto.

Cláusula 21ª

Entregáveis e documentação

1. O cocontratante entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital (.pdf e .odf):

1. Gestão projeto
    1.1. Plano detalhado do Projeto;
    1.2. Atas e apresentações de suporte a reuniões;

1.3. Relatórios mensais e trimestrais de gestão de projeto, planeamento e reporting.

2. DevOps
   2.1. Relatório com proposta de abordagem para DevOps (incluindo ferramentas, metodologia, faseamento)
   2.2. Relatório com resultado implementação e ações de melhoria
3. Relatório de Gestão de cada projeto alvo (vide secção 2)
   Relatórios de planeamento, monitorização, gestão de âmbito, gestão cronograma, gestão de custo, gestão da qualidade, gestão de recursos, e gestão de stakeholders.
4. O levantamento e sistematização das melhores práticas nacionais e internacionais no âmbito das áreas de intervenção dos projetos
5. Relatório sobre Help-desk
6. Relatório referente a requisitos
7. Relatório com Arquitetura dos Sistemas de Informação e especificações técnicas dos vários Sistemas de Informação
8. Cláusulas Técnicas dos Cadernos de Encargos.
9. Relatório executivo que sintetize as principais conclusões e recomendações dos restantes relatórios
10. Apresentação multimédia que suporte a comunicação do relatório executivo.

2. A AMA poderá proceder à reprodução de todos os documentos referidos no número anterior (para os fins que assim o entender).

Cláusula 22ª

Mecanismos Formais de Acompanhamento

1. No âmbito da prestação de serviços objeto do presente procedimento o cocontratante deverá respeitar a orgânica indicada na sua proposta para a realização dos trabalhos e a coordenação conjunta do projeto com a AMA, incluindo os diversos níveis.

2. Deverá também assegurar os mecanismos propostos para efeitos de gestão e acompanhamento dos trabalhos do projeto, que inclui os instrumentos de controlo, periodicidade e forma como serão envolvidos no projeto, do ponto de vista do seu acompanhamento, bem como os vários níveis constituintes da orgânica definida, tendo em consideração os seguintes requisitos:

- Devem ser produzidos, pelo cocontratante, relatórios quinzenais de execução dos trabalhos;
- Deve o cocontratante estar disponível para uma reunião semanal de projeto;

- Todos os resultados produzidos pelo cocontratante no âmbito do presente fornecimento deverão ser alvo de aceitação por parte da AMA;
- A AMA terá um prazo de 1 mês para se pronunciar em relação aos resultados apresentados pelo cocontratante;
- No caso da não aceitação, por parte da AMA, dos resultados, deverá o cocontratante (num prazo inferior a 15 dias) proceder às alterações necessárias para nova análise da AMA (nos termos supra).

Cláusula 23ª

Outras condições

1. O cocontratante deverá garantir o sigilo quanto à informação que venha a ter acesso durante a execução do projeto, assim como relativamente aos seus produtos resultantes que serão propriedade exclusiva da AMA.

2. Quaisquer produtos, documentação, software, ou entregáveis desenvolvidos no âmbito do presente procedimento são propriedade exclusiva do Estado Português – podendo ser livremente usados pela AMA e qualquer entidade que a AMA autorize, sem outros ónus ou encargos.

Cláusula 24ª

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.

Cláusula 25.º

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 a 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 especificas 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 26.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 DSI.
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.