CONCURSO PÚBLICO INTERNACIONAL N.º 87/22/DCP/GACD/EVOLUÇÃO E MASSIFICAÇÃO DE SOLUÇÕES DE IDENTIDADE DIGITAL

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 ____ *3*

Cláusula 6.ª Propriedade intelectual ____ *4*

Cláusula 7.ª Sigilo ____ *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 ____ *7*

Cláusula 12.ª Foro competente ____ *8*

Cláusula 13.ª Legislação aplicável ____ *9*

Cláusulas Técnicas ____ **10**

Cláusula 14.ª Descrição técnica e âmbito dos serviços ____ *10*

Cláusula 15.ª Perfil técnico dos recursos a afetar aos serviços ____ *30*

Cláusula 16.ª Substituição das equipas ____ *32*

Cláusula 17.ª Planeamento ____ *32*

Cláusula 18.ª Entregáveis e documentação ____ *33*

Cláusula 19.ª Gestor do Contrato ____ *36*

Cláusula 20.ª Mecanismos Formais de Acompanhamento ____ *36*

Cláusula 21.ª Requisitos específicos de implementação para o tratamento de dados pessoais ____ *37*

Cláusula 22.ª ____ *38*

Acessibilidade e Usabilidade ____ *38*

Cláusula 23.ª Acesso a informação da AMA ____ *39*

Cláusula 24.ª Outras condições ____ *39*

Cláusula 25.ª Requisitos específicos de implementação para a segurança da informação ____ *39*

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 prestação de serviços de consultadoria funcional e tecnológica para evolução e massificação de soluções 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, na área metropolitana de Lisboa, ou remotamente nas instalações do adjudicatário, a indicar em sede de execução contratual pela AMA.

Cláusula 3.ª

Duração

O contrato terá a duração de 36 meses a contar da data de notificação ao adjudicatário da concessão de visto do Tribunal de Contas, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base

1. O preço base é de € 2 221 560,00 (dois milhões duzentos e vinte e um mil, quinhentos e sessenta euros), a que acresce o IVA à taxa legal em vigor.

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 nos seguintes termos:

a) 20% do preço contratual com a entrega do Plano detalhado de Projeto, ponto 4.1.1 da cláusula 18.ª das cláusulas técnicas do presente caderno de encargos, mediante aceitação pela AMA;

b) 20% do preço contratual com a entrega dos documentos previstos nos números 4.2.1; 4.2.2; 4.3.1; 4.3.2. 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.7.1, 4.8.1, 4.9.1 da cláusula 18.ª das cláusulas técnicas do presente caderno de encargos, mediante aceitação pela AMA;

c) 20% do preço contratual com a entrega da Documentação prevista nos números4.2.3.; 4.3.3 da cláusula 18.ª das cláusulas técnicas do presente caderno de encargos, mediante aceitação pela AMA;

d) 20% do preço contratual com a entrega Documentação prevista nos números 4.7.2; 4.8.2., 4.8.3, 4.9.2., 4.9.3 da cláusula 18.ª das cláusulas técnicas do presente caderno de encargos, mediante aceitação pela AMA;

e) 20% do preço contratual com a conclusão e aceitação pela AMA de todos os serviços e documentos.

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. Com a entrega dos elementos a desenvolver ao abrigo do contrato o cocontratante transfere para a AMA a sua posse e propriedade, 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 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 (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 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, por 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 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:

   i. 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 mínimos exigidos para cada recurso previstos na cláusula 15.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 até 0,3% do preço contratual por cada dia em falta;

e) Pelo incumprimento das regras para substituição dos recursos previstas na cláusula 16.º até 0,3% do preço contratual por cada dia de incumprimento.

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 nota de crédito.

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

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

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

Cláusula 12.ª

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 13.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 14.ª

Descrição técnica e âmbito dos serviços

1. Enquadramento

A identificação é central para o acesso e a realização da generalidade dos serviços públicos e privados.
Tem-se verificado uma transição para os canais digitais não só no crescimento da oferta de serviços, como na sua utilização.

Assim, a Identidade Digital (ID) de cidadãos, nos vários papeis desempenhados (pessoais, profissionais, empresariais), é cada vez mais um fator crítico para o Estado desempenhar a sua missão de serviço às populações, e também para competitividade da Economia e da própria existência do indivíduo numa Sociedade cada vez mais digital

Com a emergência do digital, a necessidade de uma identidade digital, que assegure o acesso a serviços (públicos e privados) em múltiplos canais é igualmente importante, levantando desafios adicionais de segurança e de experiência do utilizador.

Tendo em vista a orientação estratégica de desenvolver a Administração Pública Digital, este procedimento vem contribuir para 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.



Designadamente pretende-se massificar a identidade digital a toda a sociedade, promover e alargar os serviços suportados em funcionalidades de identidade digital, criar um catálogo de atributos certificados que possam ser disponibilizados ao seu titular que pode autorizar e controlar o seu uso, assegurando uma integração físico-digital, possibilitando o uso de meios digitais no dia-a-dia.

Com o presente procedimento pretende-se implementar, desenvolver e evoluir tecnologicamente soluções de identidade digital nomeadamente a evolução tecnológica e funcional das soluções de autenticação e autorização,

chave móvel digital, atributos profissionais, serviço de assinatura de faturas, Serviços Cartão de Cidadão, Alteração de Morada, serviços biométricos, arquivo e preservação temporal de assinaturas, entre outros.

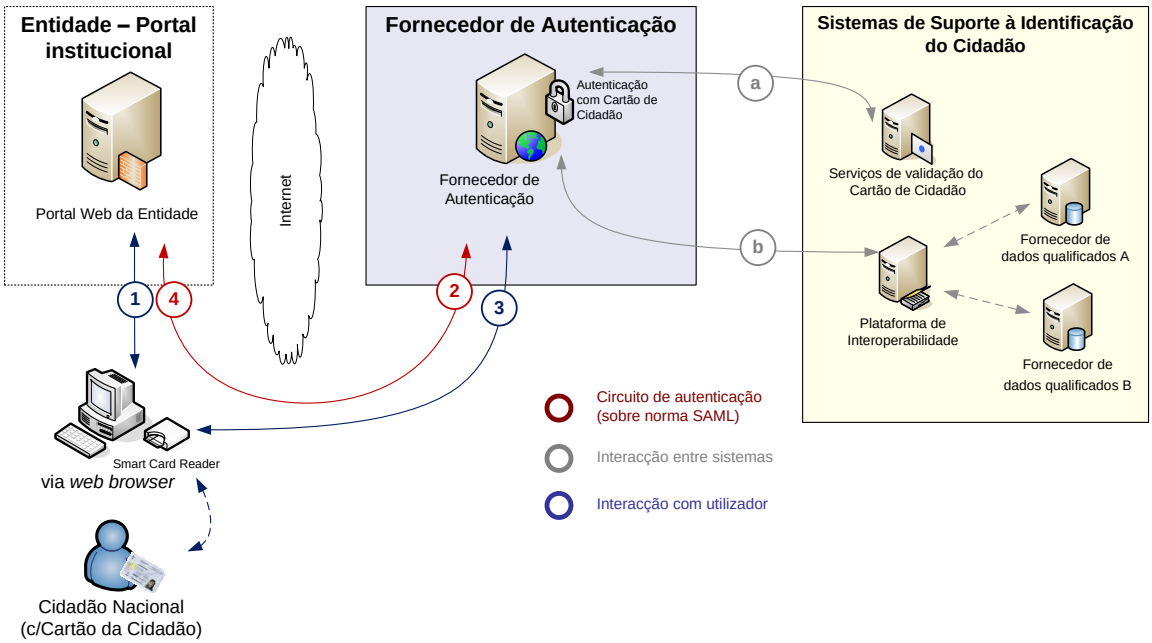
2. Plataformas Tecnológicas Relevantes para os Serviços a Prestar

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

2.1. 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.

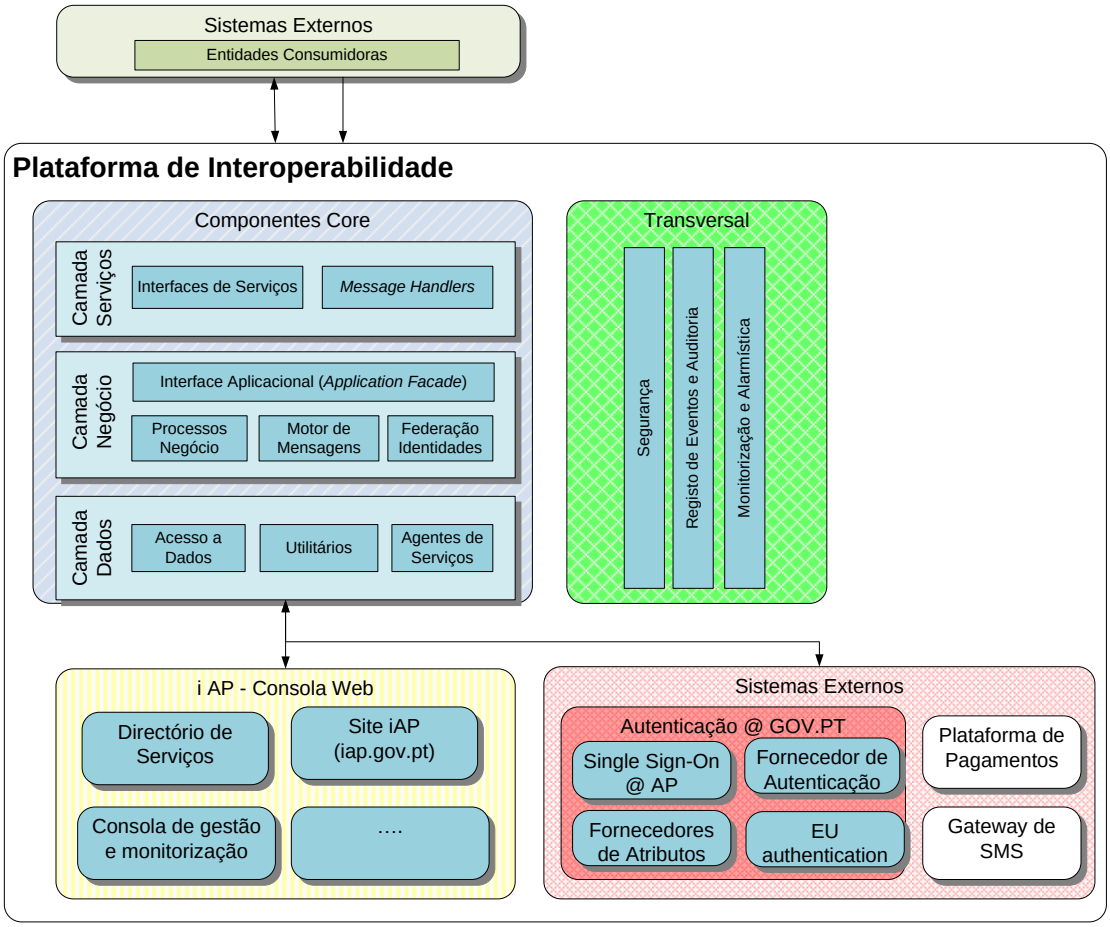
Dado que no processo de autenticação poderão ser solicitados mais dados que os presentes no certificado digital do Cartão de Cidadão (Nome e Número de Identificação Civil), mostra-se necessário a obtenção destes dados junto de fornecedores de atributos qualificados para o efeito.

2.2. 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.



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.

2.3. 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;

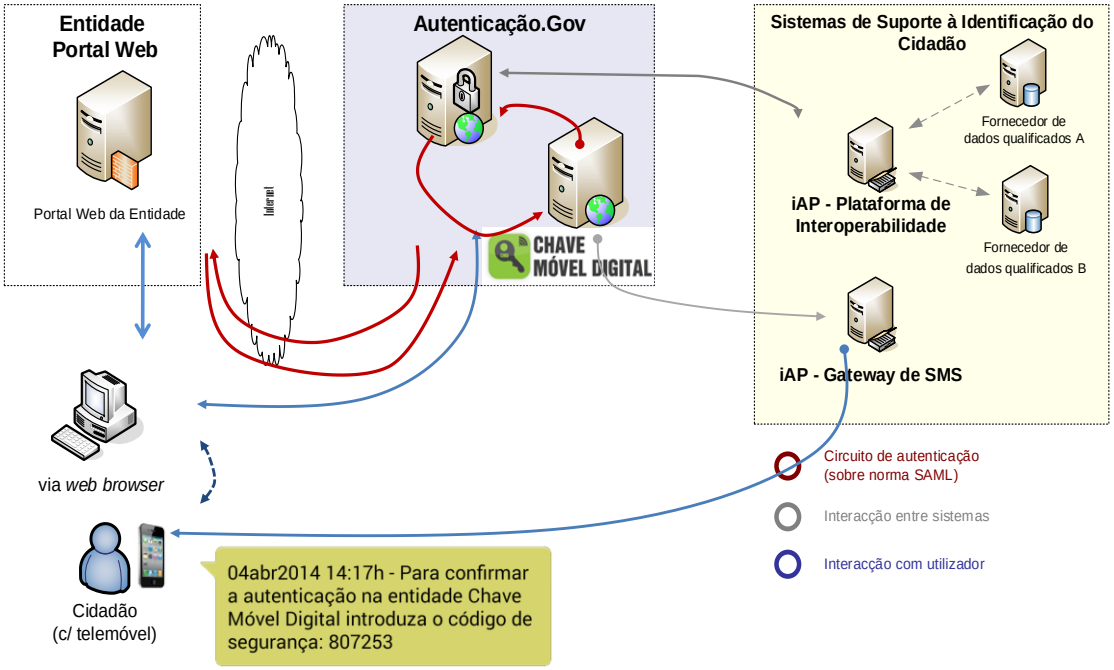
5 – O cidadão faz Login.

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.

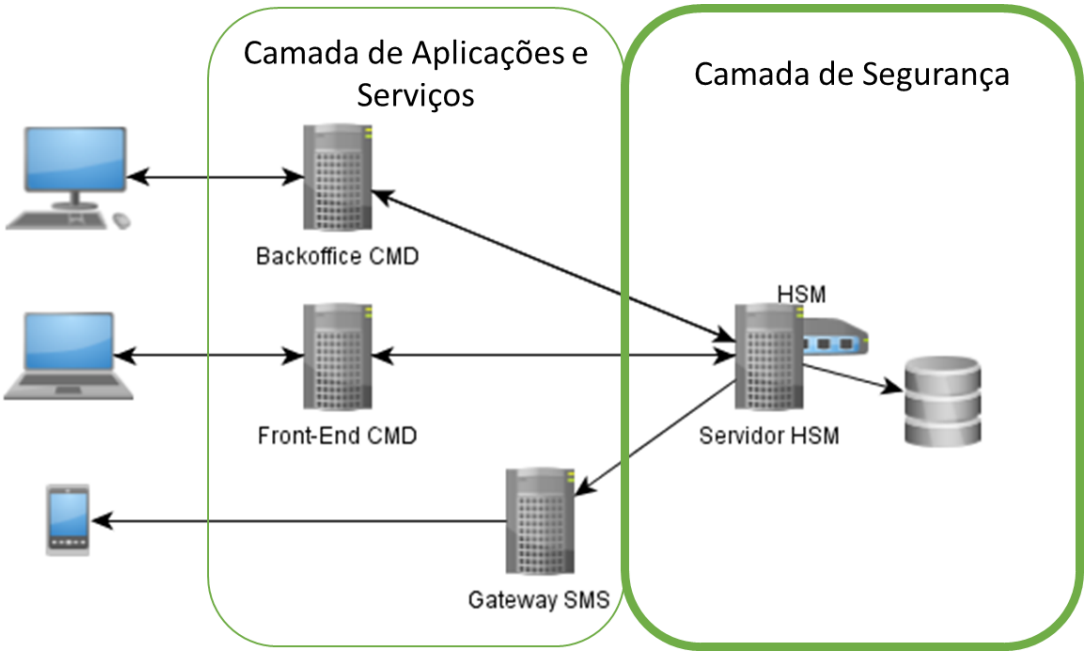
A CMD encontra-se já disponível em vários portais e sistemas (como o eportugal.gov.pt , Portal do Utente, entre outros), assegurando:

- 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.gov.pt (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.



Está também disponível mecanismo de assinatura associado à CMD, conforme arquitetura patente na figura seguinte:



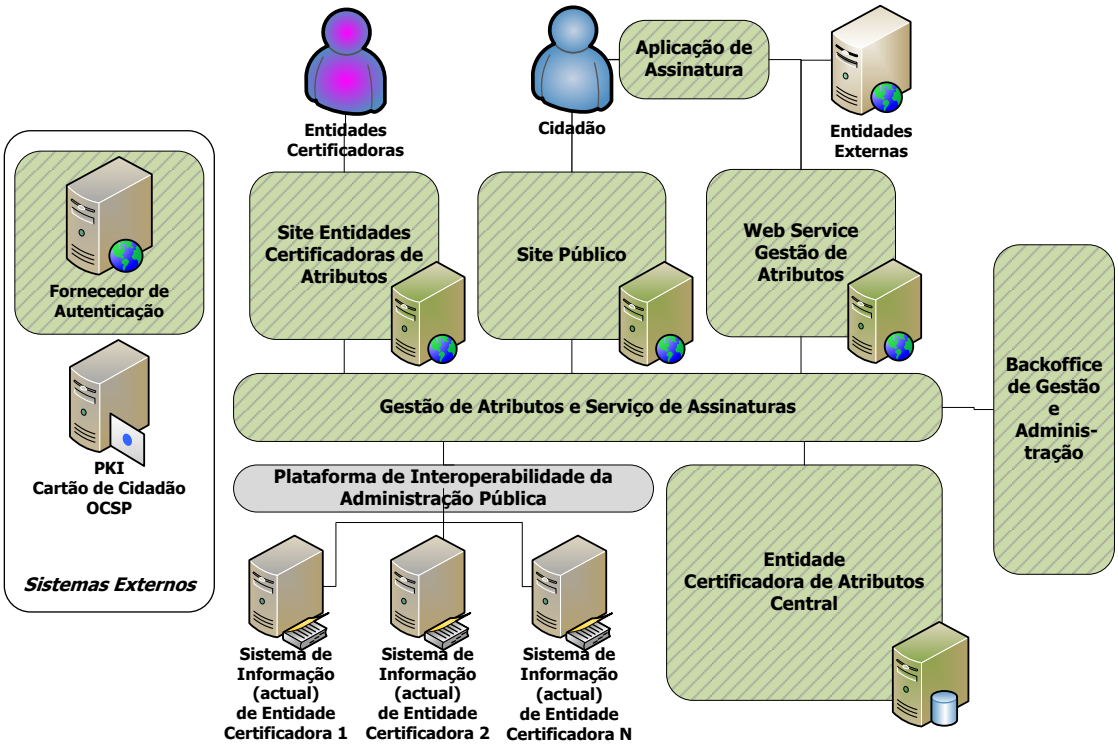
2.4. Sistema de Certificação de Atributos Profissionais com Cartão de Cidadão

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

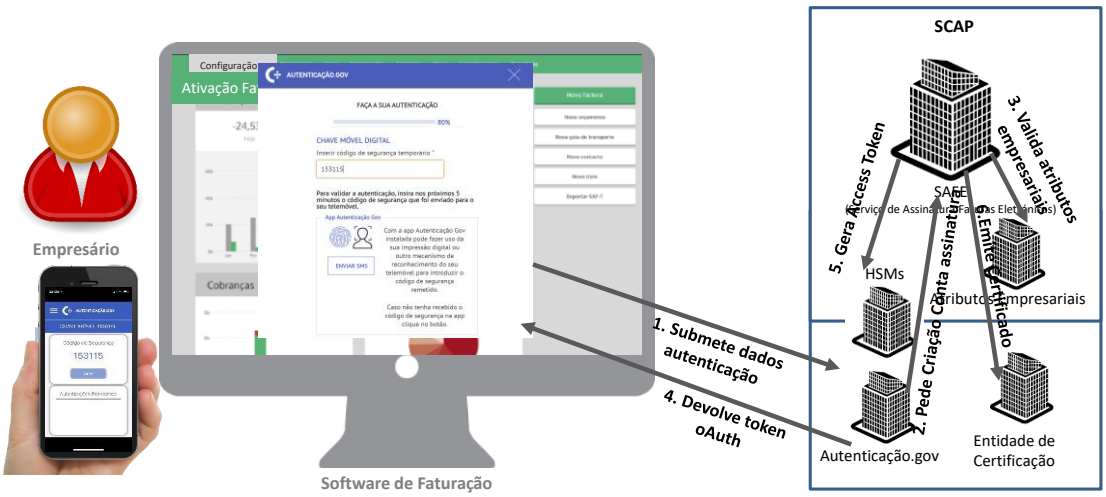
Suportado no SCAP a AMA disponibiliza o Serviço de Assinatura de Faturas Eletrónicas (SAFE). O SAFE surge com o objetivo de suportar este processo de desmaterialização, designadamente no que respeita à assinatura eletrónica qualificada das faturas, estando conforme com o artigo 12º do DL 28/2019 de 15 de fevereiro.

O Serviço de Assinatura de Faturas Eletrónicas (SAFE) tem como objetivo de oferecer 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).

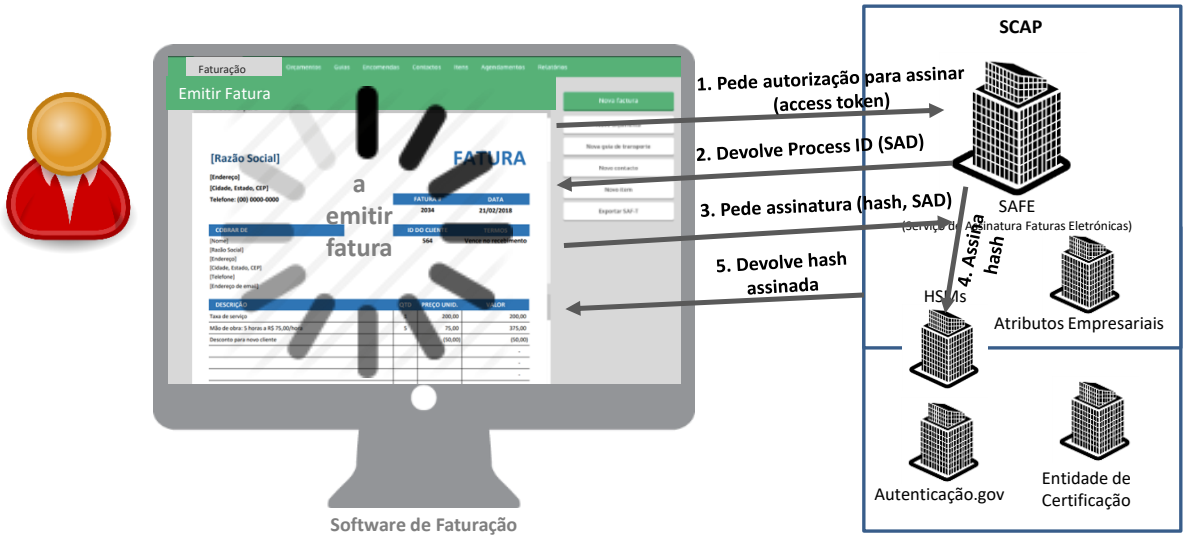
Este serviço permite ao cidadão, enquanto profissional de uma empresa, assinar digitalmente faturas eletrónicas, através de mecanismo automatizado pelo software de faturação.

Assim, o empresário aderente ao SCAP (em moldes similares aos atuais), passa a ter acesso a novo certificado qualificado específico para a assinatura de faturas. Este certificado tem uma duração máxima de 45 dias, podendo o empresário (registado no SCAP) proceder à sua emissão inicial e reemissão periódica (tipicamente mensalmente). Este processo é sumariado na figura seguinte.



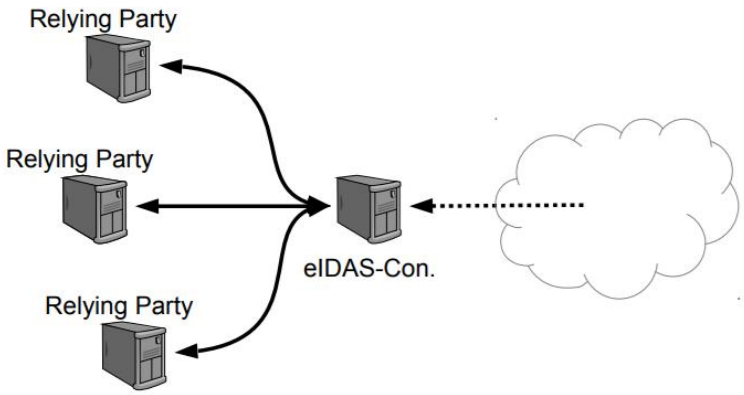
Assim, de forma a obter um certificado de assinatura de faturas SAFE, o empresário/comerciante autentica-se com o Cartão de Cidadão ou a Chave Móvel Digital e, após verificação da existência de poder associado (no SCAP) para assinatura de faturas, é gerado um código ("Access Token") que é guardado de 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 (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.

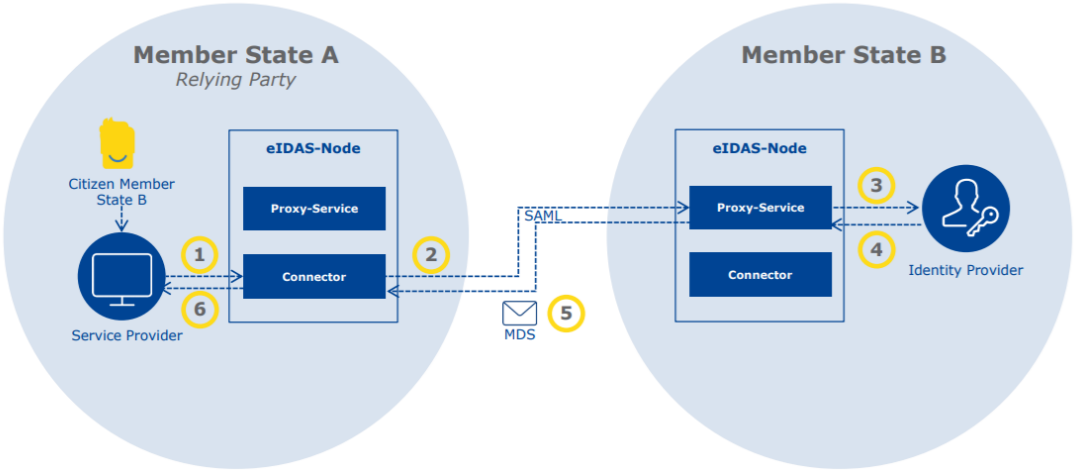


2.5 Nó eIDAS Nacional

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.



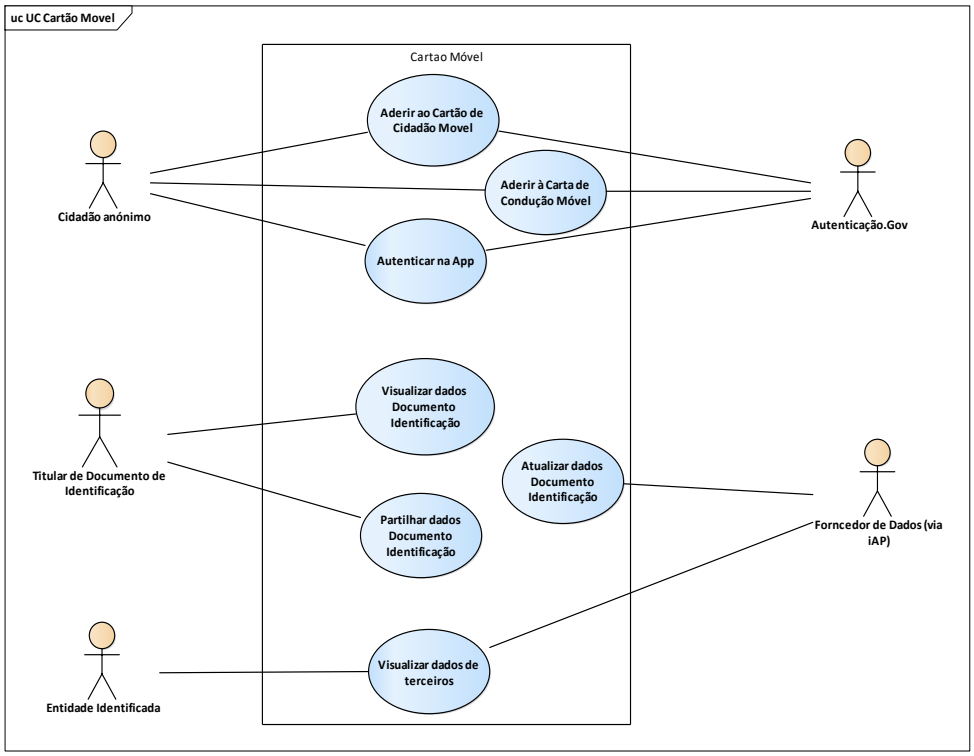
O nó eIDAS nacional suporta-se no serviço Autenticação.gov, disponibilizando os mecanismos de autenticação aí existentes (e.g., Cartão de Cidadão, Chave Móvel Digital e Sistema de Certificação de Atributos Profissionais).

2.6. Id.Gov.PT

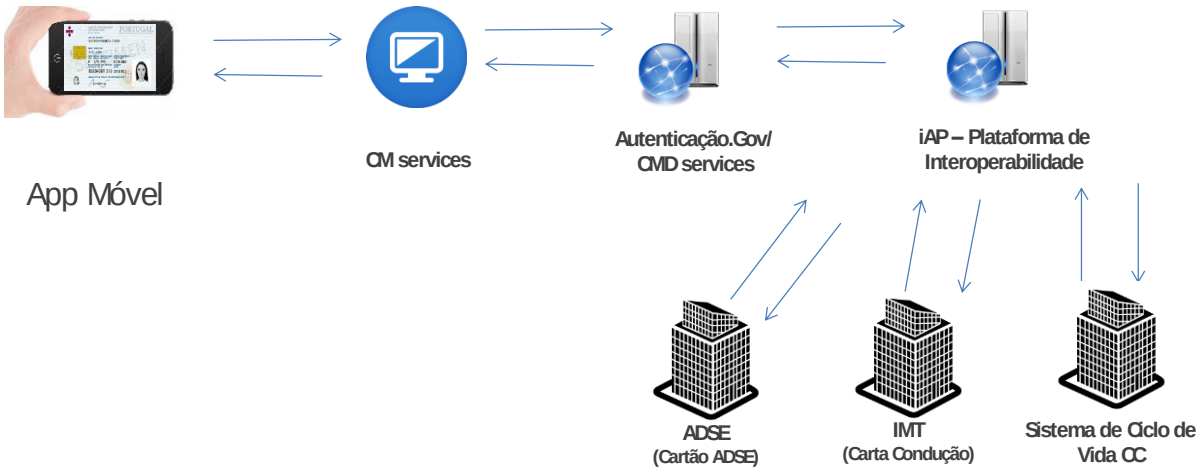
Aplicação Móvel que possibilita ao cidadão "transportar" os seus documentos de identificação no seu telemóvel, assegurando-se que os dados apresentados e validade dos mesmos é coincidente e dependente da informação residente nos sistemas de informação públicos, nomeadamente Cartão de Cidadão, Carta de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



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



Principais componentes aplicacionais:



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

3.1.1. No que concerne aos Atributos Profissionais (SCAP)

3.1.1.1. Análise ao AS IS da solução;

3.1.1.2. Evolução tecnológica de solução implementada em Java11 e Springboot para versões mais recentes Java, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.1.2.1. Submissão de pedidos de atributos empresariais;

3.1.1.2.2. Consulta de pedidos de atributos empresariais enquanto cidadão;

3.1.1.2.3. Cancelamento de atributos empresariais enquanto cidadão;

3.1.1.2.4. Consulta de atributos via portal AutGov;

3.1.1.2.5. Consulta de atributos via webService;

3.1.1.2.6. Consulta de fornecedores de atributos do SCAP via portal AutGov;

3.1.1.2.7. Consulta de fornecedores de atributos do SCAP via webService;

3.1.1.2.8. Consulta de atributos de um cidadão via portal AutGov;

3.1.1.2.9. Consulta de atributos de um cidadão via webService;

3.1.1.2.10. Assinatura de documento;

3.1.1.2.11. Assinatura de múltiplos documentos;

3.1.1.2.12. Consulta de pedidos de atributos empresariais enquanto mediador;

3.1.1.2.13. Aprovação/Recusa de pedidos de atributos empresariais;

3.1.1.2.14. Cancelamento de atributos empresariais enquanto mediador;

3.1.1.2.15. Algoritmo de verificação de pagamentos e distribuição de processos;

3.1.1.2.16. Assinatura com SCAP, com logotipo do fornecedor de atributos;

3.1.1.2.17. Disponibilização de **serviço público de selos**, em articulação com Serviço de Certificação de Atributos Profissionais (SCAP).

3.1.1.3. Fornecedor de Atributos de Funcionários (FAF):

3.1.1.3.1. Evolução de versão de SGBD (MySQL) para versão mais recente.

3.1.2. No que concerne ao Serviço de Assinatura de Faturas (SAFE)

3.1.2.1. Evolução tecnológica de solução implementada em Java11 e Springboot para versões mais recentes Java, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.2.1.1. Criação de conta via portal AutGov;

3.1.2.1.2. Criação de conta via webService;

3.1.2.1.3. Gestão de conta;

3.1.2.1.4. Gestão de tokens;

3.1.2.1.5. Assinatura.

3.1.3. No que concerne ao Autenticação.Gov (Fornecedor de Autenticação) e à Chave Móvel Digital (CMD)

3.1.3.1. Análise ao AS IS da solução;

3.1.3.2. Fornecedor de autenticação:

3.1.3.2.1. Melhoria da Ux associada ao processo de autenticação;

3.1.3.2.2. Melhoria no mecanismo de autenticação modal assegurando a compatibilidade com a evolução dos browsers e Ux adequada

3.1.3.2.3. Melhorias no Single Sign-On (SSO), nomeadamente com integração com mecanismo de autorizações;

3.1.3.2.4. Alargamento das normas abertas de integração suportadas.

3.1.3.3. Evolução tecnológica de componente CMD Assinatura implementada em Java 7 e para quarkus reactive, incluindo:

3.1.3.3.1. Evolução de versão MySQL;

3.1.3.3.2. Criação de conta;

3.1.3.3.3. Gestão de conta;

3.1.3.3.4. Assinatura;

3.1.3.3.5. Registo de secretKeys para aplicação móvel;

3.1.3.3.6. Gestão de secretKeys para aplicação móvel;

3.1.3.4. Evolução tecnológica de componente de registo na CMD implementada em Java 8 e para sringBoot, incluindo:

3.1.3.4.1. Evolução de versão MySQL;

3.1.3.4.2. Criação de CMD;

3.1.3.4.3. Pedido de CMD e envio por carta códigos.

3.1.3.5. Evolução tecnológica de componente de gestão dos serviços de HSM implementada em Java 11, incluindo:

3.1.3.5.1. Criação de chaves privadas;

3.1.3.5.2. Gestão de chaves privadas;

3.1.3.5.3. Assinatura;

3.1.3.5.4. Encriptações/Desencriptações.

3.1.3.6. **Portal Autenticação Gov – implementação de novo Portal com revisão de marca e imagem e Ux**

3.1.3.6.1. Evolução tecnológica para Liferay com react, nomeadamente front ends das seguintes funcionalidades:

3.1.3.6.1.1. Os meus Dados;

3.1.3.6.1.2. CMD;

3.1.3.6.1.3. SAFE;

3.1.3.6.1.4. SCAP;

3.1.3.6.1.5. Estatísticas;

3.1.3.6.1.6. Autorizações;

3.1.3.6.1.7. FAF;

3.1.3.6.1.8. CMD via Portal das Finanças.

3.1.3.7. **Nó eIDAS.**:

3.1.3.7.1. Atualização de nó eIDAS Nacional de acordo com especificações EU e implementações de referência EU que venham a ser disponibilizadas;

3.1.3.7.2. Integração com outros EU ou países com quem Portugal tenha protocolos no nó eIDAS Nacional.

3.1.4. **Serviços de interoperabilidade Biométricos**. Evolução de serviço de backend (servidor) que possa ser usados em aplicações terceiras, de forma a assegurar:

3.1.4.1. Validação de segurança do Documentos de Identificação (Nacionais e Internacionais), para cidadãos Portugueses e outra nacionalidade;

3.1.4.2. Verificação Facial (com a comparação de 2 ou mais fotografias);

3.1.4.3. Verificação da Presença de Vida

Estes serviços devem ser implementados tendo por base a integração com diferentes fornecedores de serviços de biometria, possibilitando a implementação de uma camada segura que permita a seleção do fornecedor de biometria mais adequado e dos dados biométricos (constantes de bases de dados públicas) que, com a devida autorização do titular, são usados na verificação biométrica.

3.1.4.4. Solução para adesão CMD via e-residency:

3.1.4.4.1. Gestão da adesão de cidadãos estrangeiros, nomeadamente no âmbito da iniciativa e-residency;

3.1.4.4.2. Recolha e gestão de informações e documentação adicional (e.g., comprovativos morada, dados profissionais);

3.1.4.4.3. Validação biométrica cidadãos estrangeiros.

3.1.4.5. Evolução de solução de renovação de **cartão de cidadão e passaporte em app móvel ou Portal**
Implementação de serviços de forma a possibilitar a renovação de Cartão de Cidadão e Passaporte em aplicação móvel ou Portal, com recolha e validação de nova fotografia, incluindo:

3.1.4.5.1. Verificação da validade e segurança de documento de cidadão;

3.1.4.5.2. Verificação biométrica (tendo por base serviços de biometria);

3.1.4.5.3. Verificação e tratamento de foto recolhida (Selfie) para novo documento (nomeadamente de acordo com requisitos ICAO);

3.1.4.5.4. Integração com sistemas de negócio (CVCC e SIPEP) responsáveis pelo ciclo de vida destes documentos.

3.1.5. No **que concerne à gestão de autorizações**

3.1.5.1. Análise ao AS IS da solução;

3.1.5.2. Evolução tecnológica de solução implementada em Java11 e Springboot para versões mais recentes Java, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.5.2.1. Autorizações por blocos de atributos;

3.1.5.2.2. Autorizações por JWT;

3.1.5.2.3. Autorizações de grupos de entidades;

3.1.5.2.4. Autorizações por QrCode;

3.1.5.2.5. Autorizações por telefone;

3.1.5.2.6. Usar 4 microserviços (springBoot e reactive):

3.1.5.2.6.1. JWT e Grupo de entidades em reactive;

3.1.5.2.6.2. QrCode em springBoot;

3.1.5.2.6.3. Blocos em springBoot;

3.1.5.2.6.4. Atendimento Telefónico em springBoot.

3.1.5.3. Evolução serviço de consumo de dados das autorização através de webservice seguro para permitir às entidades aderentes fazer um pedido de autorização através da internet.

3.1.5.4. Evolução de mecanismo de gestão de autorizações integrado com Fornecedor de Autenticação.

3.1.5.5. Previsualização de dados partilhados em formatos estruturas e não estruturados (e.g., pdf, imagens).

3.1.6. No que concerne a Pilotos de identificação digital

3.1.6.1. Suporte na implementação de pilotos de eID, incluindo o desenho, a adaptação e teste com sistemas de informação externos para suportar a integração com o serviço Autenticação.Gov (incluindo a Chave Móvel Digital);

3.1.6.2. Disseminar Iniciativas/projetos que façam uso de mecanismos de identificação eletrónica.

3.1.7. Área do developer

3.1.7.1. Evolução de funcionalidades dirigidas a implementadores, incluindo catálogo de componentes, kit de developer (em função das funcionalidades pretendidas) e respetivas comunidades de developers.

3.1.7.2. Melhoria nos procedimentos de subscrição dos serviços e funcionalidades de identidade digital por parte de parceiros.

3.1.8. No que concerne a Apps de Identificação Eletrónica para ambientes Móveis

3.1.8.1. Manutenção e evolução de componentes de backend de app Autenticação.gov/CMD incluindo:

3.1.8.1.1.1. Gestão de documento assinados e a partilha de link para documento;

3.1.8.1.1.2. Envio de documento para assinatura de outro e devolução do mesmo.

3.1.8.2. Carteira de Identidade Digital:

3.1.8.2.1. Implementação e evolução de componentes de backend (servidor) de mecanismos, baseados em blockchain, de guarda local segura, e gestão e partilha de atributos de identidade, implementando os princípios de uma identidade Soberana — Self-Sovereign Identity (SSI);

3.1.8.2.2. Participação em piloto de larga escala (LSP) de identidade digital, como integração com outros Estados Membros no contexto EU, nomeadamente tendo em vista a disponibilização dos seguintes casos de uso transfronteiriços e funcionalidades:

3.1.8.2.2.1. Abertura de Conta Bancária;

3.1.8.2.2.2. Autenticação;

3.1.8.2.2.3. Assinatura;

3.1.8.2.2.4. Gestão de atributos no contexto da saúde;

3.1.8.2.2.5. Gestão de atributos no contexto da educação e emprego;

3.1.8.2.2.6. Implementação de componentes comuns de identidade digital EU.

3.1.8.2.3. Implementação e evolução de componentes de backend (servidor) referente a novos cartões a implementar em aplicação id.gov :

3.1.8.2.3.1. Passaporte;

3.1.8.2.3.2. Titulo/Certificado de Residência;

3.1.8.2.3.3. Seguro automóvel;

3.1.8.2.3.4. Cartão do estudante;

3.1.8.2.3.5. Certificado COVID-19;

3.1.8.2.3.6. Cartão para cada fornecedor de atributos SCAP.

3.1.9. Arquivo e Preservação Temporal Assinaturas

3.1.9.1. **Implementação de serviço de Arquivo e Preservação Temporal Assinaturas de acordo com o Regulamento eIDAS e normas técnicas ETSI, , incluindo mecanismos de ré assinatura:**

3.1.9.1.1.1. Serviço de Validação, conforme Regulamento eIDAS e, standards ETSI TS 119 441, ETSI TS 119 442, ETSI TS 119 101, ETSI TS 119 102-1, ETSI TS 119 102-2 e ETSI TS 119 172-4. (Nota: (i) Antes de serem preservadas, as assinaturas têm de ser validadas. (ii) Assinaturas preservadas necessitam de ser validadas para garantir integridade da força probatória.);

3.1.9.1.1.2. Modo de funcionamento com e sem armazenamento central documentação;

3.1.9.1.1.3. Implementação de SDK/clientes locais que assegurem a preservação de documentos armazenados descentralizadamente.

3.1.10. Serviços Cartão de Cidadão, Alteração e Confirmação de Morada:

3.1.10.1. Evolução tecnológica **Serviço de Alteração de Morada** implementado em Java 8, Liferay 7.0, JSP para springBoot com versões mais recentes e react, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.10.1.1. Integração com a IAP para envio de mensagens às entidades;

3.1.10.1.2. Integração com plataforma de para envio de emails com os dados da nova morada às entidades;

3.1.10.1.3. Possibilidade de selecionar morada estrangeira e Portuguesa;

3.1.10.1.4. Integração com serviço de códigos-postais para obter moradas portuguesas;

3.1.10.1.5. Serviço para reenviar moradas apenas depois de securizadas;

3.1.10.1.6. Serviço para reenvio de processos de morada com erro de Integração;

3.1.10.1.7. Serviço que possibilite a consulta de processos de alteração de morada;

3.1.10.1.8. Integração com autenticação.Gov para login do cidadão;

3.1.10.1.9. Evolução de Fluxo, experiência do utilizador e Design.

3.1.10.1.10. Evolução de versão de MySQL.

3.1.10.2. Evolução tecnológica **Serviço de Confirmação de Morada** implementado em Java 8, Liferay 7.0, JSP para springBoot com versões mais recentes Java e react, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.10.2.1. Integração com a IAP para consulta de moradas em confirmação, confirmar morada e obtenção de nova morada;

3.1.10.2.2. Integração com autenticação.Gov para login do cidadão;

3.1.10.2.3. Evolução de Fluxo, experiência do utilizador e Design.

3.1.10.2.4. Evolução de versão de MySQL.

3.1.10.3. Evolução tecnológica **Serviço de Renovação CC** implementado em Java 8, Liferay 7.0, JSP para springBoot com versões mais recentes Java e react, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.10.3.1. Implementação de microserviços para Cancelamento, Renovação Próprio, Renovação Terceiro, Renovação operador;

3.1.10.3.2. Integração com a IAP para envio de renovações e cancelamentos de CC;

3.1.10.3.3. Integração com autenticação.Gov para login do cidadão;

3.1.10.3.4. Integração com serviço de códigos-postais para obter moradas portuguesas.

3.1.11. Evolução tecnológica de serviços de suporte de eID, nomeadamente com evoluções tecnológicas:

3.1.11.1. Serviço de **BlacklistIps**, implementado em quarkus e Java 11 com evolução de versão Java, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.11.1.1. Gerir Ips bloqueados, com criação de ficheiro .txt;

3.1.11.1.2. Recepção de pedidos de bloqueio de Ips de vários serviços.

3.1.11.2. Serviço de **Notificações**, implementado em .Net Core assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.11.2.1. Permitir envio de notificações por email, push e sms;

3.1.11.2.2. Permitir a recepção de pedidos de notificações de vários serviços;

3.1.11.3. Serviço de **ToptService**, implementado em Java 8 para springBoot, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.11.3.1. Criação e gestão de scret keys;

3.1.11.3.2. Validação de TOTPs.

3.1.11.4. Serviço de Testes IapDummyService implementado em Java 8 para springBoot e react, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.11.4.1. Consulta de dados dummys;

3.1.11.4.2. Serviços para criação de dados dummy por cidadão.

3.1.11.5. Backoffice de gestão de serviços de eID, implementado em Java 8, Liferay 7.0, JSP para versões mais recentes Java e react, assegurando funcionalidades atualmente existentes, nomeadamente:

3.1.11.5.1. Serviços por telefone (realização, criação, edição e estatísticas);

3.1.11.5.2. Estaísticas renovação e alteração de morada;

3.1.11.5.3. Realização de alteração de morada presencial;

3.1.11.5.4. Atendimento Telefónico;

3.1.11.5.5. Gestão SAM (Configuração, e sam presencial e pesquisa);

3.1.11.5.6. Gestão ServicosCC (pesquisa e estatísticas).

3.1.12. Monitorização e Resiliência

3.1.12.1. Revisão em todas as aplicações de identidade digital (descritas no cap 2) assegurando a existência de um endpoint de monitorização;

3.1.12.2. Disponibilização de sondas inteligentes em todas as aplicações de identidade digital que detetem variações de utilização significativas (e.g., número médio de autenticações nos últimos 10 minutos inferior a 25% da média do mês, no mesmo dia/período horário);

3.1.12.3. Anonimização e exportação diária dos dados de identidade digital para dados.gov e sistema externo de exploração de dados (power BI);

3.1.12.4. Upgrade do Liferay do Autenticação Gov para a versão enterprise;

3.1.12.5. Configuração de alta disponibilidade de aplicações, com eventuais adaptações de componentes de software;

3.1.12.6. Adaptação de arquitetura de aplicações para event driven (melhoria de performance e escalabilidade).

3.1.13. Suporte às equipas de 1.ª linha de suporte

A utilização dos mecanismos de autenticação por parte de cidadãos ou profissionais gera por vezes situações cuja análise carece de um conhecimento técnico da solução de forma a identificar problema, replicar erro e resolução do mesmo, produção de relatórios ou guiões para ajuda dos utilizadores. Neste sentido, é âmbito do presente procedimento garantir a realização do seguinte conjunto de atividades:

a) Atualização de guião para 1.ª linha documentar problema na primeira interação com cidadão;
b) Análise a problema identificado, replicação e resolução técnica para o mesmo;
c) Produção de documentação para apoio à resolução encontrada;
d) Produção, gestão e manutenção de sistema de gestão de incidentes;
e) Produção de relatórios estatísticos com pelo menos as seguintes informações:
   i. Tipologia de problema;
   ii. Tempo de resolução;
   iii. Complexidade da solução;
   iv. N.º de ocorrências do incidente após informação à 1.ª linha de suporte.

3.1.14. Acompanhamento de processos de passagem a ambiente de produção

Estas passagens acontecem em ambiente laboral e fora de ambiente laboral até 2 vezes por semana (após as 20h e até às 8h, nos dias úteis e aos fins de semana). Estas horas poderão ser compensadas em dobro, em horário útil, pelos recursos envolvidos.

Cláusula 15ª

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.
2. Para a execução dos serviços de consultadoria suprarreferidos deverá ser afeta uma equipa, com a composição indicada na proposta, de pelo menos 11 recursos, com os perfis mínimos e níveis de afetação da equipa mínimos que em seguida se indicam:

- Um Gestor de Projeto 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 nas funções subjacentes ao perfil em apreço superior a 10 anos, dedicação a 100% ao projeto e:
    - Experiência anterior em projetos relacionados com o Cartão de Cidadão ou Chave Móvel Digital;
    - Valorizada formação superior complementar em Informática ou Engenharia Informática ou em gestão (e.g.. Mestrado, Pós-graduação, cursos de especialização);
    - Licenciatura em engenharia, gestão ou economia;
    - Credenciação do Gabinete Nacional de Segurança ou demonstrar que iniciou 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 e 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.

- Dois consultores Tecnológicos, com experiência nas tecnologias e soluções descritas na secção 2 do presente caderno de encargos, em particular no desenho de arquiteturas de projetos em tecnologia .NET, nomeadamente na linguagem C#, ASP, ASPX, que serão responsáveis pela qualidade técnica das Soluções e dos testes e pela proposta das principais decisões tecnológicas, com experiência em

consultoria tecnológica superior a 5 anos, com uma dedicação ao projeto igual a 100%, com:

- Experiência anterior em projetos relacionados com o Cartão de Cidadão, plataformas descritas no presente caderno de encargos;
- Valorizada formação complementar nas tecnologias em apreço para a função (e.g.. Mestrado, Pós-graduação, cursos de especialização);
- 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*.

- Sete consultores Tecnológicos, com experiência nas tecnologias e soluções descritas na secção 2 do presente caderno de encargos, em particular no desenho de arquiteturas de projetos em tecnologia Java e Liferay, que serão responsáveis pela qualidade técnica das Soluções e dos testes e pela proposta das principais decisões tecnológicas, com experiência em consultoria tecnológica superior a 5 anos, com uma dedicação ao projeto igual a 100% (cada recurso), com:
  - Experiência anterior em projetos relacionados com o Cartão de Cidadão, plataformas descritas no presente caderno de encargos;
  - Valorizada formação complementar nas tecnologias em apreço para a função (e.g.. Mestrado, Pós-graduação, cursos de especialização);;
  - 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* (ou equivalente).

- Um especialista em Experiência de utilizador/webdesign responsável pelo design das interfaces de utilizador da App, com experiência superior a 5 anos nas funções de UX/webdesign, dedicação ao projeto superior ou igual a 50% e,
  i. Experiência anterior em projetos Mobile;
  ii. Formação superior;
  iii. Experiência comprovada (superior a 3 anos) em:
    - Interfaces com o utilizador;
    - Interfaces Mobile.

3. O cocontratante deverá prever a possibilidade de eventual participação de 1 a 2 elementos da AMA na equipa de projeto que terão por principal missão a aquisição de know-how nas funcionalidades implementadas, bem como a implementação de outras funcionalidades (que se terão de integrar com as descritas neste CE), sendo da responsabilidade do cocontratante a sua gestão e passagem de conhecimento.

Cláusula 16ª

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, 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 17ª

Planeamento

1. Os serviços suprarreferidos deverão ser iniciados após a celebração do contrato e integralmente concluídos num prazo de **36 meses (33 meses de trabalho efetivo),** tendo por base metodologias de desenvolvimento ágeis, com sprints, tendencialmente quinzenais.

2. Espera-se que o cocontratante apresente em fase de propostas um calendário para o desenvolvimento dos serviços apresentados no número 3.1 da cláusula 14.ª do presente Caderno de Encargos, 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.
4. O cocontratante deverá apresentar uma metodologia de gestão de projeto e desenvolvimento assente nos valores e princípios ágeis. Deverá também propor a utilização de uma ferramenta online, para controlo de gestão de projeto e de issues, que obrigatoriamente terá que fornecer acesso aos elementos da AMA que irão efetuar o acompanhamento do projeto. A AMA tem uma instância do Tuleap (https://www.tuleap.org/) que também deverá ser utilizada.
5. Todos os desenvolvimentos ficarão alojados sistema de controlo de versões da AMA, baseada em Git, e deverão seguir a metodologia Twelve-Factor App (ou equivalente).

Cláusula 18ª

Entregáveis e documentação

1. O cocontratante deverá apresentar o documento "Requisitos de conformidade com o RGPD" de acordo com o nº 3 da Cláusula 21ª do presente Caderno de Encargos.
2. A solução deverá ser fornecida em conjunto com a documentação adequada a nível do projeto, do sistema e do código, para apoio da equipa responsável pela assistência ao sistema. A documentação deve identificar:
   - Os componentes críticos;
   - Procedimentos de instalação;
   - Procedimentos de gestão de alterações;
   - Dependência entre componentes;
   - Procedimentos de monitorização;
   - Procedimentos de recuperação;
   - Tempos de execução;
   - Características dos ambientes.
3. A documentação técnica seguirá a utilização de UML em toda a documentação produzida, sendo tipicamente complementada com outro tipo de artefactos que demonstrem expressar ideias ou conceitos de forma mais percetível ou que não sejam suportados de forma adequada pela linguagem UML.
4. Da referida documentação, o cocontratante entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital (.pdf e .odf):

4.1. Gestão projeto:

4.1.1. Plano detalhado do Projeto;

4.1.2. Descrição das Atividades do Projeto;

4.1.3. Work breakdown structure;

4.1.4. Modelo de Governance;

4.1.5. Registo de Riscos;

4.1.6. Log de Issues;

4.1.7. Relatório de status do projeto;

4.1.8. Matriz de Responsabilidades;

4.1.9. Gestão de documentação;

4.1.10. Pareceres e Análise funcional-técnica na implementação do projeto;

4.1.11. Documento de Especificação de requisitos e Arquitetura;

4.1.12. Atas e apresentações de suporte a reuniões;

4.1.13. Documento com Plano e Cenários de Teste;

4.1.14. Documento com resultados testes efetuados;

4.1.15. Relatórios de gestão de projeto, planeamento e reporting.

4.2. Chave Móvel Digital (CMD):

4.2.1. Relatório análise ao AS IS;

4.2.2. Desenho técnico;

4.2.3. Código Fonte desenvolvimentos;

4.2.4. Manuais de desenvolvimento, instalação e operação.

4.3. Fornecedor de Autenticação:

4.3.1. Relatório análise ao AS IS;

4.3.2. Desenho técnico;

4.3.3. Código Fonte desenvolvimentos;

4.3.4. Manuais de desenvolvimento, instalação e operação.

4.4. SCAP:

4.4.1. Relatório análise ao AS IS;

4.4.2. Desenho técnico;

4.4.3. Código Fonte desenvolvimentos;

4.4.4. Manuais de desenvolvimento, instalação e operação.

4.5. SAFE:

4.5.1. Relatório análise ao AS IS;

4.5.2. Desenho técnico;

4.5.3. Código Fonte desenvolvimentos;

4.5.4. Manuais de desenvolvimento, instalação e operação.

4.6. Pilotos Eid:

4.6.1. Relatório análise ao AS IS;

4.6.2. Desenho técnico;

4.6.3. Código Fonte desenvolvimentos;

4.6.4. Manuais de desenvolvimento, instalação e operação;

4.6.5. Relatório por cada implementação de piloto eID efectuada.

4.7. Serviços de Arquivo e Preservação Temporal:

4.7.1. Análise Funcional;

4.7.2. Desenho técnico;

4.7.3. Código Fonte desenvolvimentos;

4.7.4. Manuais de desenvolvimento, instalação e operação.

4.8. Serviços Cartão de Cidadão, Alteração e Confirmação de Morada:

4.8.1. Análise Funcional;

4.8.2. Desenho técnico;

4.8.3. Código Fonte desenvolvimentos;

4.8.4. Manuais de desenvolvimento, instalação e operação.

4.9. Serviços Biometricos:

4.9.1. Análise Funcional;

4.9.2. Desenho técnico;

4.9.3. Código Fonte desenvolvimentos;

4.9.4. Manuais de desenvolvimento, instalação e operação.

4.10. Serviços Gestão de Autorizações:

4.10.1. Análise Funcional;

4.10.2. Desenho técnico;

4.10.3. Código Fonte desenvolvimentos;

4.10.4. Manuais de desenvolvimento, instalação e operação.

4.11. Apoio na resolução de problemas reportados à 2.ª linha:

4.11.1. Relatório de incidentes e níveis de serviço.

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

Cláusula 19ª

Gestor do Contrato

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

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

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

Cláusula 20ª

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 mínimos:

- 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 21ª

Requisitos específicos de implementação para o tratamento de dados pessoais

1. A arquitetura da solução deverá obrigatoriamente 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 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) Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas firewall, *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 22.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 Selo Prata (https://selo.usabilidade.gov.pt/prata.html);

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

Cláusula 23ª

Acesso a informação da AMA

1. No decorrer do contrato o cocontratante terá acesso a informação interna da AMA que lhe será transmitida e a informação restrita, nomeadamente o código fonte da Plataforma.
2. O acesso à informação restrita é dada individualmente mediante atribuições de utilizadores individuais que terão acesso apenas aos recursos necessários para executar os serviços a prestar.
3. As alterações ao código fonte são objeto de logging.

Cláusula 24ª

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 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 Procedimento 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.