



**CONCURSO PÚBLICO N.º 118/20/DCP/DTD/ GOVERNAÇÃO,
PROCEDIMENTOS E INFRA-ESTRUTURA DE SEGURANÇA
PLATAFORMAS 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 Gestor do Contrato	8
Cláusula 13.ª Foro competente	8
Cláusula 14.ª Legislação aplicável	8
Cláusulas Técnicas	10
Cláusula 15.ª Descrição técnica do contrato	10
Cláusula 16.ª Perfis técnico dos recursos a afetar aos serviços	22
Cláusula 17.ª Substituição das equipas	23
Cláusula 18.ª Entregáveis e documentação	24
Cláusula 19.ª Mecanismos Formais de Acompanhamento	24
Cláusula 20.ª Outras condições	25
Cláusula 21.ª Requisitos específicos de implementação para o tratamento de dados pessoais	Erro! Marcador não definido.





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 evolução de mecanismos de governação, procedimentos e infraestrutura de segurança de plataformas 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, ou remotamente a partir de qualquer local à escolha do adjudicatário.

Cláusula 3.ª

Duração

O contrato terá a duração estimada de 12 meses a contar da sua celebração, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço base

1. O preço base é de € 40.000 (quarenta mil 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, como por exemplo:
 - 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 previsto na subalínea i), da alínea a), do n.º 1 da Cláusula 18ª do presente caderno de encargos, mediante aceitação pela AMA;
 - b) 20% do preço contratual com a entrega e aceitação dos documentos previstos na alínea b) do n.º 1 da cláusula 18:ª do presente caderno de encargos, mediante aceitação pela AMA;
 - c) 20% do preço contratual com a entrega e aceitação dos documentos previstos na alínea c) do n.º 1 da cláusula 18:ª do presente caderno de encargos, mediante aceitação pela AMA;
 - d) 20% do preço contratual com a entrega e aceitação dos documentos em na alínea d) do n.º 1 da cláusula 18:ª do presente caderno de encargos, mediante aceitação pela AMA;
 - f) 20% do preço contratual com a entrega e aceitação de todos os serviços objeto do presente procedimento.
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 poderão revestir a forma eletrónica, caso em que deverão ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o endereço fornecedores@ama.pt.
 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.

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

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.
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.





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. 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:

$$P=V*A/500$$

em que:

P - Corresponde ao montante da penalidade;

V - Corresponde ao valor do contrato; e,

A - Corresponde ao número de dias em atraso.

2. Pela não comparência do Cocontratante em qualquer reunião, independentemente da parte que a convocou, poderá ser aplicada uma sanção de 250 €.
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 12ª

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





CLÁUSULAS TÉCNICAS

Cláusula 15.ª

Descrição técnica do contrato

1. Enquadramento

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

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

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS. Tendo por base a importância da experiência de utilização, conjugado com as novas possibilidades de assinatura eletrónica qualificada “server-side” previstas no regulamento europeu 910/2014, e em alterações legislativas nacionais, a CMD foi alvo de credenciação enquanto mecanismo de assinatura eletrónica qualificada “server-side”.

Neste contexto é central a continua aferição e melhoria de procedimentos de segurança na solução de assinatura da chave móvel digital.

Por outro lado, tendo por base a infraestrutura do Cartão de Cidadão foi implementado o Sistema de Certificação de Atributos Profissionais (SCAP). Através do SCAP permite-se que os detentores de CC possam autenticar-se e assinar nas qualidades profissionais que estejam disponíveis, potenciando investimentos efetuados e desmaterializando a identificação eletrónica profissional. Sobre esta infraestrutura possibilita-se aos dirigentes públicos autenticarem-se e assinarem eletronicamente usando o seu Cartão de Cidadão, certificando as suas atribuições, nos termos do artigo 10.º do Decreto-Lei n.º 83/2016, de 16 de dezembro. Disponibiliza-se ainda aos administradores, dirigentes e trabalhadores das empresas a possibilidade de autenticação e assinatura em representação da empresa. Para o efeito, o Sistema de Certificação de Atributos Profissionais permite a criação





do perfil da empresa, desmaterializando o pacto social e atos permitidos aos administradores, utilizando o Cartão de Cidadão para autenticação e assinatura na qualidade respetiva.

Neste contexto, é igualmente fundamental a contínua melhoria das políticas e procedimentos subjacentes à gestão desta infraestrutura (SCAP) tendo em consideração a necessidade de assegurar elevados níveis de segurança e confiabilidade dos atos certificados pela mesma.

2. Plataformas Tecnológicas Relevantes para os Serviços a Prestar

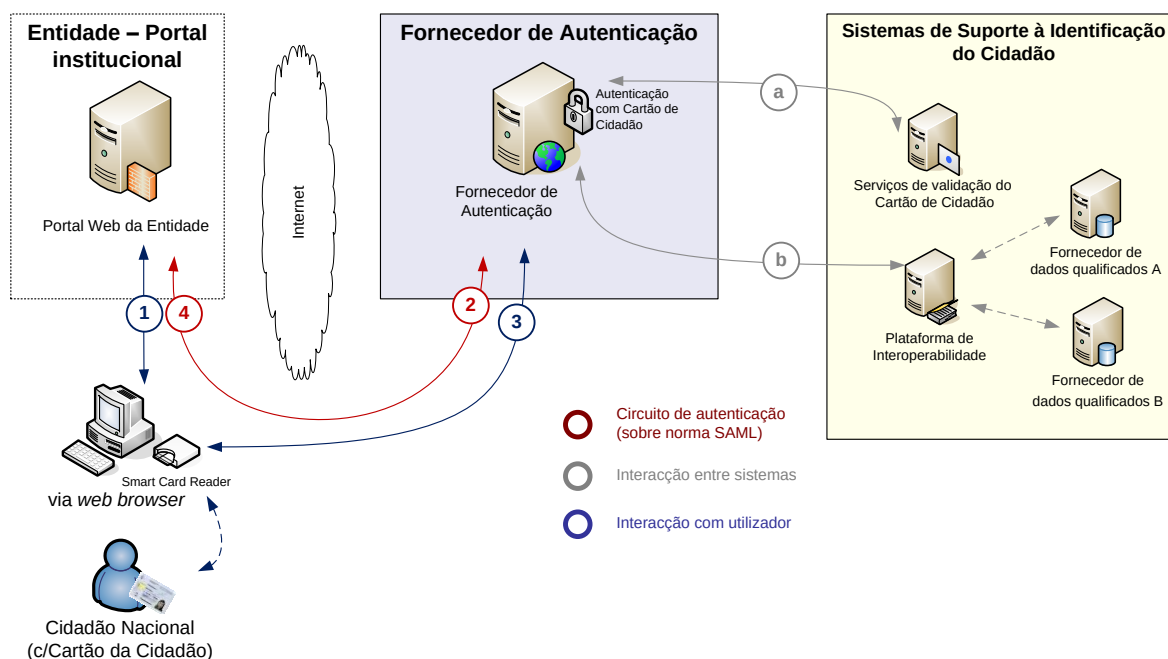
Nesta secção apresenta-se uma descrição sucinta de projetos já realizados ou em curso que se consideram relevantes no âmbito deste procedimento.

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 transaccional, 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.



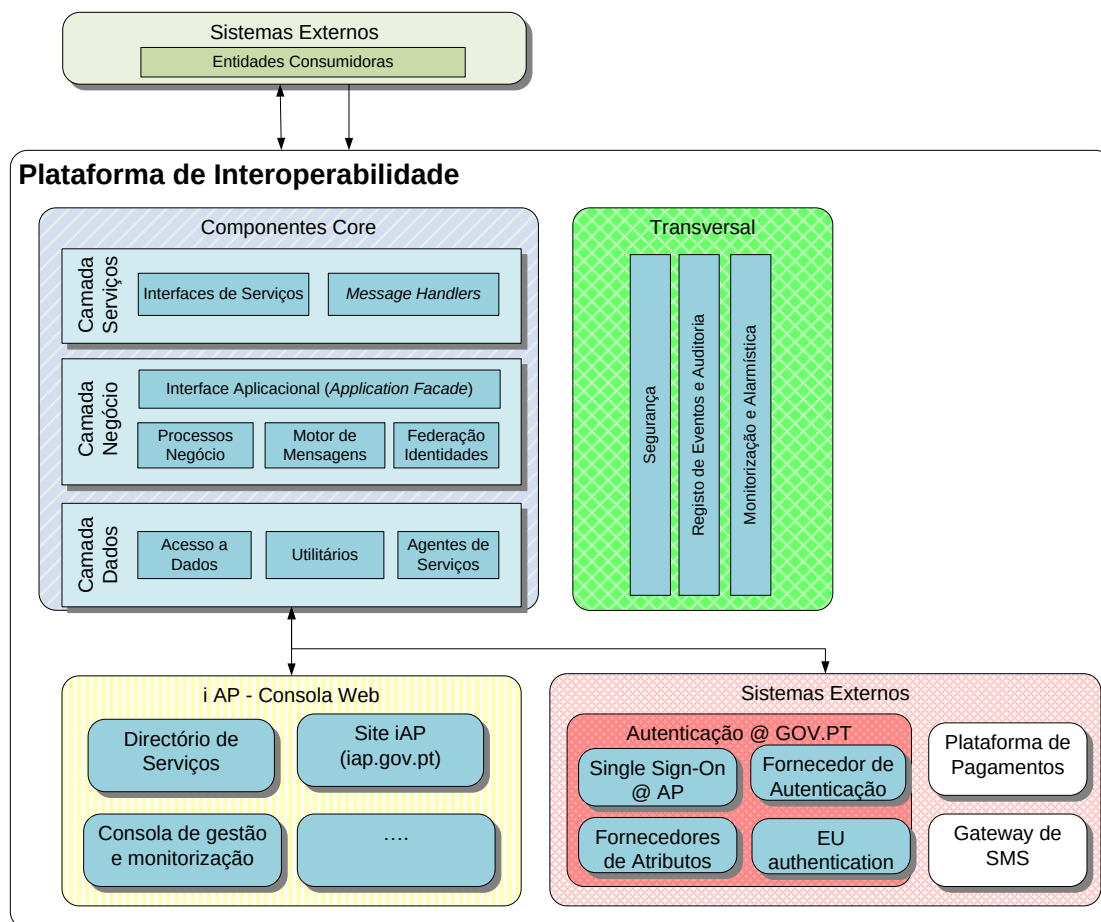


Figura 1 – Arquitetura lógica

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 Identities;
- **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.

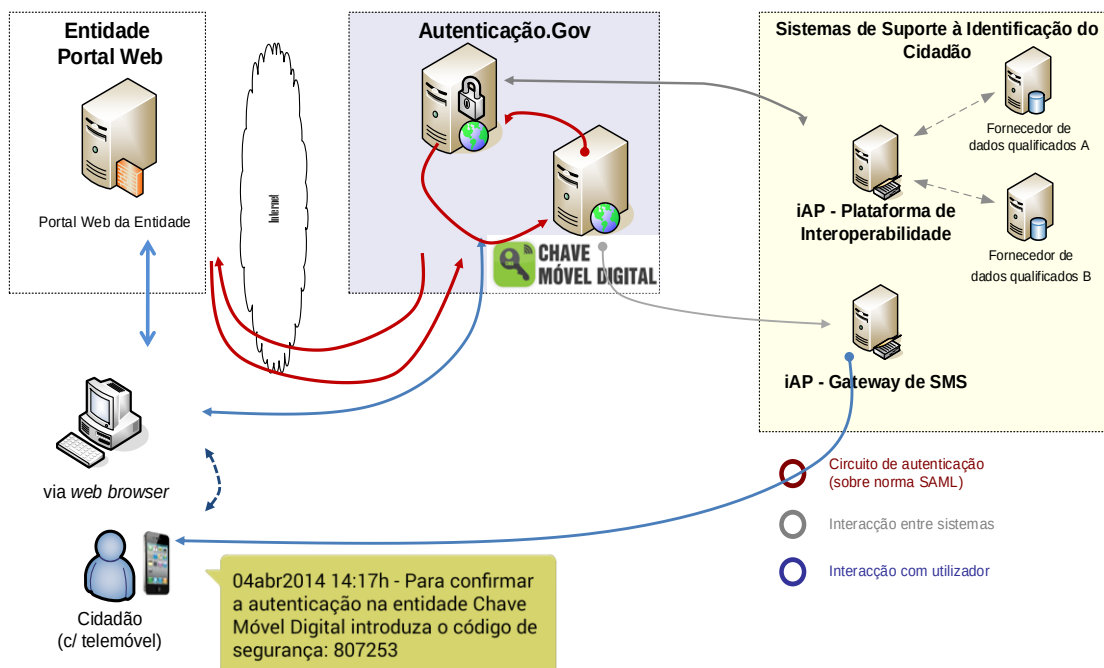
A CMD encontra-se já disponível em vários portais e sistemas (como eportugal.gov.pt (Portal do Cidadão), Portal do Utente, entre outros), assegurando:

- 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

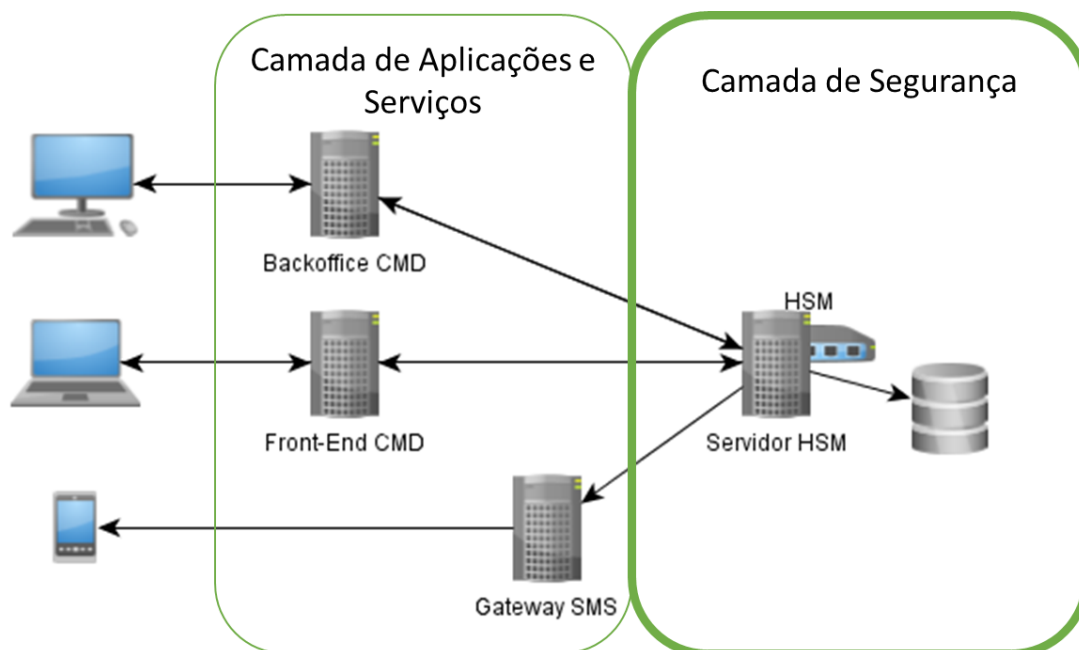


a autenticação com CMD num portal, basta incluir no atual pedido ao serviço “Autenticação.Gov” um parâmetro que indica que o portal também aceita Chave Móvel Digital.

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:





2.4. 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.

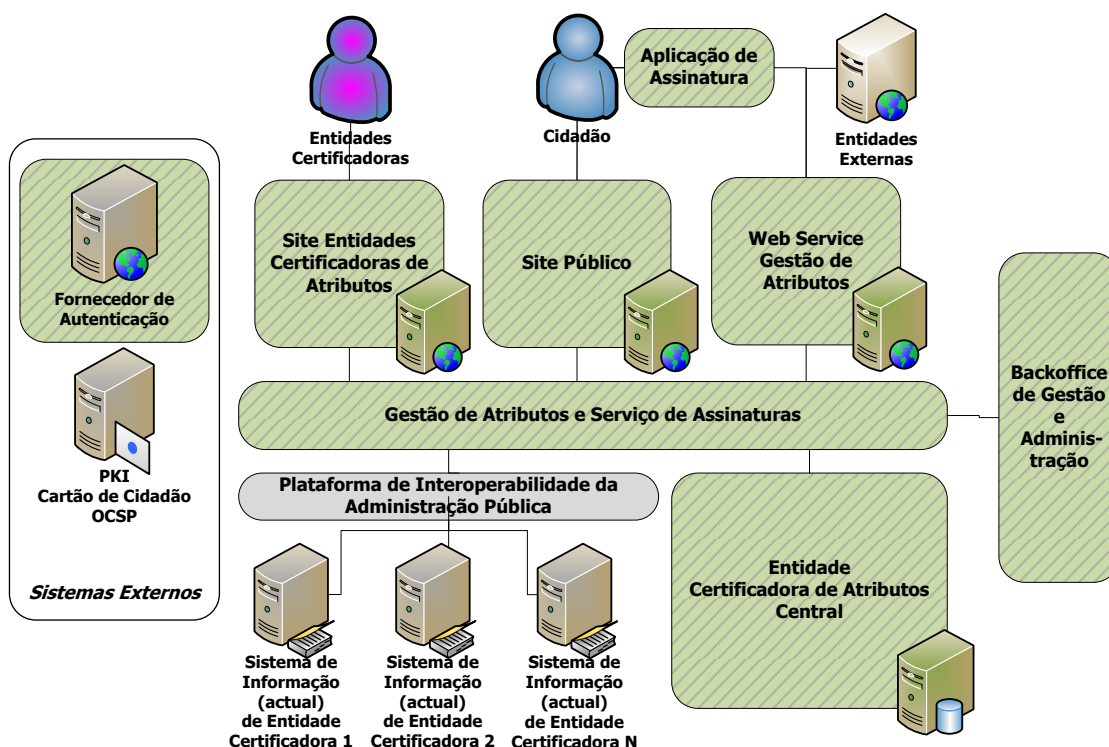
O principal enfoque deste procedimento é a gestão global das várias iniciativas tecnológicas e de negócio para implementação deste sistema que possibilite a utilização do Cartão de Cidadão para a criação de assinaturas digitais e a autenticação em diferentes qualidades, nomeadamente as qualidades profissionais – 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>



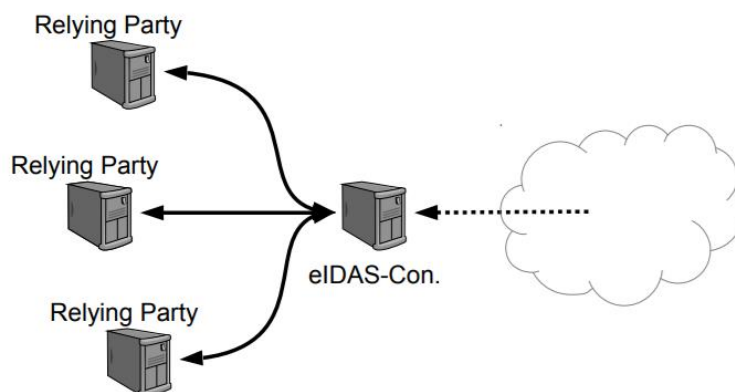


Figura

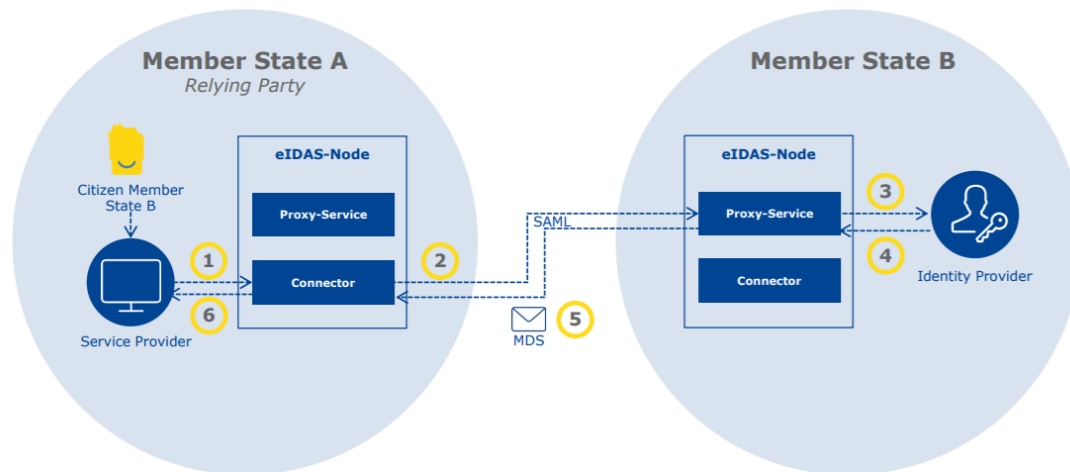
2 – Arquitetura Global da Solução

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).

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. Políticas, Procedimentos e instalações CMD

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

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



- 3.1.1.8. Política de Ambientes - concretização dos Ambientes e artefactos;
- 3.1.1.9. Política de Recursos Humanos - concretização dos RH baseado nas Regras de Recursos Humanos;
- 3.1.1.10. Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento do CMD;
- 3.1.1.11. Políticas e procedimentos para sub-CA CMD da PKI do CC – incluindo revisão das políticas, procedimentos e documentação da PKI do CC;
- 3.1.1.12. Elaboração de documentação para credenciação nos termos da especificação técnica CEN/TS 419241;
- 3.1.1.13. Outros documentos, ou diagramas referentes a políticas e procedimentos que se revelem necessários para a concretização da eventual certificação;
- 3.1.1.14. Verificação das políticas, infraestruturas e procedimentos implementados na CMD;
- 3.1.1.15. Recomendação de melhorias a implementar;
- 3.1.1.16. Segunda verificação das políticas, infraestruturas e procedimentos CMD após implementação de melhorias;
- 3.1.1.17. Acompanhamento de auditorias externas a solução CMD assinatura.

3.1.2. Políticas, Procedimentos e instalações SCAP

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

- 3.1.2.1. Regras de Documentação;
- 3.1.2.2. Regras de Recursos;
- 3.1.2.3. Regras de Ambientes;
- 3.1.2.4. Política de Identificadores a usar no SCAP;
- 3.1.2.5. Política de gestão de Certificados
- 3.1.2.6. Declaração de Práticas;
- 3.1.2.7. Política de Cerimónias;
- 3.1.2.8. Política de Ambientes;
- 3.1.2.9. Política de Recursos Humanos;
- 3.1.2.10. Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento do SCAP;
- 3.1.2.11. Outros documentos, ou diagramas referentes a políticas e procedimentos que se revelem necessários para a concretização da eventual certificação.
- 3.1.2.12. Verificação das políticas, infraestruturas e procedimentos implementados no SCAP;
- 3.1.2.13. Recomendação de melhorias a implementar;





- 3.1.2.14. Segunda verificação das políticas, infraestruturas e procedimentos SCAP após implementação de melhorias.
 - 3.1.2.15. Definição de Requisitos segurança da infraestrutura de armazenamento, comunicações e processamento dos fornecedores de atributos;
 - 3.1.2.16. Definição de *orientações*, políticas e procedimentos transversais que deverão ser asseguradas por Fornecedores de Atributos;
 - 3.1.2.17. Verificação do cumprimento de políticas e procedimentos em Fornecedores de Atributos;
 - 3.1.2.18. Verificação do cumprimento de políticas e procedimentos em Fornecedor de Atributos 2;
 - 3.1.2.19. Verificação do cumprimento de políticas e procedimentos em Fornecedor de Atributos 3;
 - 3.1.2.20. Acompanhamento de auditorias externas a solução SCAP.
- 3.1.3. eIDAS
- 3.1.3.1. Atualização informação em relação a infra-estrutura eIDAS e sistemas de Identificação Digital nacionais
- 3.1.4. Pareceres técnicos, assessments, e esclarecimento de Dúvidas decorrentes dos trabalhos de auditoria ou credenciação por entidades externas**

3.2. Planeamento

Os serviços supra referidos deverão ser iniciados após a celebração do contrato e integralmente concluídos num prazo de **12 meses**.

Espera-se que o cocontratante apresente em fase de propostas um calendário para o desenvolvimento dos serviços apresentados no ponto 3.1, com indicação clara da alocação dos recursos e sua alocação às diferentes fases e entregáveis do projeto.

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 16.^a

Perfis 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 a partir de qualquer local à escolha do adjudicatário.
2. Para a execução dos serviços de consultadoria supra-referidos deverá ser prevista uma equipa de pelo menos 1 pessoa a 40%, com os perfis e níveis de afetação que em seguida se indicam:





- Um Consultor tecnológico que desenvolverá as atividades descritas no CE, com experiência superior a 15 anos, e:
 - Experiência anterior em projetos relacionados com o Cartão de Cidadão, preferencialmente com sistema de certificação de atributos profissionais ou CMD;
 - Formação superior em Informática ou Engenharia Informática sendo valorizada formação complementar em gestão;
 - Licenciatura em engenharia, informática ou equivalente;
 - Credenciação do Gabinete Nacional de Segurança ou demonstrar que iniciaram o processo de credenciação junto da referida entidade;
 - Experiência em execução de pelo menos 5 projetos de credenciação de ICP:

O local da prestação de serviços será nas instalações da AMA , ou remotamente a partir de qualquer local à escolha do adjudicatário.

3. Informação a fornecer sobre os recursos

Os curricula vitae apresentados 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 17.^a

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 comumente expectável, poderá a AMA exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

Cláusula 18.ª

Entregáveis e documentação

1. O cocontratante entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital (.pdf e .odf):
 - a) Gestão projeto
 - i. Plano detalhado do Projeto;
 - ii. Atas e apresentações de suporte a reuniões;
 - iii. Relatórios de gestão de projeto, planeamento e reporting.
 - b) Relatório AS-IS infra-estrutura de identificação digital;
 - c) Relatório melhorias infra-estrutura de identificação digital;
 - d) Documentação para credenciação de soluções CMD e SCAP;
 - e) Relatório de verificação e de recomendações referente a políticas e procedimentos no CMD.
2. O cocontratante deverá apresentar o documento “Requisitos de conformidade com o RGPD” de acordo com o nº 3 da Cláusula 21ª.
3. A AMA poderá proceder à reprodução de todos os documentos referidos no número anterior (para os fins que assim o entender).

Cláusula 19.ª

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 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 20.ª

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 21.ª

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) Mascaram dados sensíveis de acordo com o nível de permissões do utilizador;
 - ii) Apagamento, consulta, alteração/atualização, exportação/portabilidade dos dados;
 - iii) Encriptação de dados sensíveis.
 - c) Estruturas de dados que permitam:
 - i) Implementação de um modelo de dados que contemple categoria, finalidade, consentimento, fundamento, bem como outros atributos relacionados, e permita estabelecer as relações necessárias;
 - ii) Registo dos tempos de retenção por finalidade.
 - d) Desenho de interface que permita:
 - i) Pesquisas por dados isolados assegurando a segregação por titular dos dados e/ou atributos;
 - ii) Informação e recolha de consentimento de forma contextualizada com a funcionalidade/página que procede à utilização dos dados pessoais.
 - e) Mecanismos de registo de utilizador/data/hora de atividades CRUD (*Create, Read, Update, Delete*)



- sobre dados pessoais;
- f) Procedimentos automáticos para garantir que findo o período de retenção, os dados serão anonimizados, eliminados, encriptados ou renovado o período de retenção, e recolhido o consentimento caso seja aplicável, dependendo da finalidade ou fundamentação existente para a sua retenção;
 - g) Segurança de redes e sistemas de informação em conformidade com os requisitos obrigatórios previstos no anexo da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, sempre que aplicáveis;
 - h) Uma estrutura multicamada, composta pelas camadas de Apresentação ou *Front-end* (FE), Apicacional (APP) e Base de dados (BD).
2. A arquitetura da solução de acordo com estes e restantes requisitos deverá ser apresentada e detalhada nos entregáveis das várias fases que compõem o projeto, sujeitos à aprovação da AMA.
3. Nos entregáveis deverá estar incluído um documento de “Conformidade com o RGPD”, no qual o cocontratante deve incluir o inventário de dados pessoais sujeitos a tratamento pela solução e sua categorização, funcionalidades, estruturas de dados e mecanismos de segurança implementados, bem como, a forma de cumprimento dos requisitos estabelecidos como obrigatórios previstos na alínea g), justificando os casos de não aplicabilidade.
4. Os seguintes requisitos serão assegurados pela AMA:
- a) Análise de vulnerabilidades no contexto da cibersegurança, sendo a sua correção da responsabilidade do cocontratante;
 - b) Implementação de protocolos de segurança TLS (*Transport Layer Security*) fornecendo os certificados digitais, desde que o alojamento do sistema/aplicação/portal seja em infraestrutura gerida pela entidade contratante;
 - c) Detecção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas 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

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 ou 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 anti-virus 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.

