

1. Objetivo

O presente documento tem como objetivo definir o serviço de acreditação para o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE, adiante designado por Regulamento eIDAS, em complemento do estabelecido no DRC001, DRC006 e documentos conexos.

2. Entidade competente

O Gabinete Nacional de segurança (GNS) atua como entidade supervisora no âmbito do Regulamento eIDAS, encontrando-se informação relevante para a atuação dos organismos de certificação no seu sítio internet (www.gns.gov.pt).

3. Norma de Acreditação

Considerando o referencial de certificação em causa, este serviço está incluído no esquema de acreditação de Organismos de Certificação de Produtos, cujo referencial de acreditação é a ISO/IEC 17065.

4. Documentos Normativos

Consideram-se como documentos normativos (de cumprimento obrigatório) específicos os seguintes:

- Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;
- ETSI EN 319 403 - Trust Service Provide Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 401 - General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 - Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 - Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 412-1 - Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 - Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-3 - Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-4 - Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations;
- ETSI EN 319 412-5 - Certificate Profiles; Part 5: QC Statements;
- ETSI EN 319 422 - Time stamping protocol and electronic time-stamp profiles.
- Documentos normativos disponibilizados pelo Gabinete Nacional de Segurança nomeadamente quanto a requisitos dos auditores, duração das auditorias e modelo de relatório de auditoria;

Devem ser usadas as versões vigentes e válidas dos documentos normativos acima citados respeitando os prazos e processos de transição que possam ser estabelecidos.

5. Condições de Acesso

Para que possa ser aceite a candidatura de um organismo de certificação (OC), deve o mesmo:

- Não estar em estado de falência, liquidação ou de cessação de atividade, ou ter pendentes processos correspondentes;
- Não ter sido condenado, por sentença transitada em julgado, por qualquer delito que afete a honorabilidade profissional, nomeadamente fraude, ou ter sofrido punição disciplinar por falta grave em matéria profissional, se entretanto não tiver ocorrido a reabilitação;
- Não enviar, de forma consciente ou intencional, informação falsa, incompleta ou omissa com indução de dolo ao IPAC ou às autoridades competentes;
- Dispor de pelo menos um auditor qualificado para cada unidade de acreditação incluída ou a incluir no seu âmbito de acreditação.

6. Descrição do Âmbito de Acreditação

A descrição dos âmbitos de acreditação é feita com base nos âmbitos de auditoria e categorias indicadas na tabela abaixo, considerando-se cada categoria como uma unidade de acreditação:

1 - Serviço qualificado de confiança - Assinaturas eletrônicas
2 - Serviço qualificado de confiança - Selos eletrônicos
3 - Serviço qualificado de confiança - Selos temporais
4 - Serviço qualificado de confiança - Autenticação de sítios web
5 - Serviço qualificado de confiança - Serviço de envio registado eletrónico

7. Procedimento de Acreditação

O procedimento de acreditação aplicável encontra-se descrito no DRC001 - Regulamento Geral de Acreditação e no DRC006 - Procedimento para Acreditação de Organismos de Certificação, os quais são complementados pelo conteúdo do presente documento.

Para a concessão da acreditação será necessária a realização de uma avaliação nas instalações do OC, complementada pela realização de pelo menos de 1 testemunho presencial em cada um dos âmbitos de acreditação atrás identificados.

Poderão ser avaliadas várias categorias num único testemunho, caso as atividades testemunhadas do prestador de serviços de segurança e do organismo de certificação o justifiquem.

Para a manutenção da acreditação, e tendo em conta as categorias para as quais o OC possua acreditação, será realizado pelo menos 1 testemunho presencial em cada um dos âmbitos acima identificados em cada ciclo de acreditação. Estes testemunhos serão complementados pela(s) correspondente(s) avaliação(es) nas instalações do OC.

8. Requisitos para o processo de certificação

8.1 Qualificação de auditores

O procedimento de qualificação de auditores do OC que atuam neste âmbito deve cumprir o estabelecido no capítulo 6 da Norma EN 319 403 e documentos normativos disponibilizados pelo Gabinete Nacional de Segurança.

8.2 Frequência das auditorias

As auditorias aos prestadores de serviços de confiança são efetuadas de acordo com os seguintes referenciais:

- Legislação nacional em vigor;
- Regulamento eIDAS.

8.3 Duração das auditorias

A duração das auditorias deve cumprir os critérios estabelecido no capítulo 7.4 da Norma EN 319 403 e documentos normativos disponibilizados pelo Gabinete Nacional de Segurança.

8.4 Modelo de relatório

Os relatórios de auditoria serão elaborados seguindo os padrões definidos em documento normativo disponibilizado pelo Gabinete Nacional de Segurança.