FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia

Perfil de Confiabilidade RCTS – P2

Federação de Identidade RCTS

Este documento é um extrato autónomo do perfil RCTS-P2, derivado do documento-mestre "Perfis de Confiabilidade de Identidade RCTS - Documento Consolidado" (a fonte primária mantida pela Federação de Identidade RCTS), alinhado com o REFEDS Assurance Framework v2.0 (RAF 2.0, 5 de dezembro de 2023).

RCTS | Federação de Identidade | Perfis de Confiabilidade
Data: 20 de agosto de 2026
Elaborado por: Esmeralda Pires
Revisto por: João Guerreiro e António Coucelo

Índice

Índice....2
1. Terminologia....3
2. Termos e Definições....3
3. Introdução....5
3.1. Âmbito....5
4. Conformidade e Verificação....6
4.1. Procedimento de Verificação....6
5. Requisitos da Organização....6
6. Requisitos Operacionais....7
6.1. Identificadores....7
6.1.1. Identificadores Permitidos....7
6.1.2. Pessoa Física....7
6.1.3. Pessoa Física Contactável....7
6.1.4. Reatribuição....7
6.2. Controlo e Verificação de Identidade e Gestão de Credenciais....8
6.2.1. Registo e Acreditação....9
6.2.2. Controlo e Verificação de Identidade - RCTS-P2....9
6.2.3. Emissão, Entrega e Ativação - RCTS-P2 e RCTS-P3....9
6.2.4. Integridade do Processo de Verificação e Registo - RCTS-P2 e RCTS-P3....10
6.2.5. Suspensão, Revogação e Reativação....10
6.2.6. Renovação e Substituição - RCTS-P0, RCTS-P1 e RCTS-P2....10
6.3. Qualidade dos Atributos....11
6.4. Autenticação....12
6.4.1. Autenticação de Fator Único....12
6.4.2. Autenticação MultiFator....13
7. Referências....15
Anexo B - Critérios Normativos Aplicáveis (Nível IAP high)....16

1. Terminologia

As palavras-chave “DEVE”, “NÃO DEVE”, “NECESSÁRIO”, “RECOMENDADO”, “TEM DE”, “PODE”, “NÃO PODEM”, “SERÁ” e “OPCIONAL” no presente documento devem ser interpretadas como descrito no RFC2119, consultar http://tools.ietf.org/html/rfc2119.

2. Termos e Definições

Federação Uma federação é um grupo de organizações que concordam em interoperar com base num conjunto de regras bem definidas.

Operador da federação A FCCN, Unidade Orgânica da FCT – Fundação para a Ciência e a Tecnologia, a operar como FCT|FCCN.

Gestor da Federação Membro do Conselho Diretivo da FCT responsável pela Computação Científica Nacional.

Federação de Identidade RCTS Federação de Identidade Portuguesa para Educação e Investigação.

Membro Um Membro da Federação de Identidade RCTS é um participante da rede RCTS que atua como Fornecedor de Identidade (fornece a infraestrutura necessária para a autenticação de utilizadores) e/ou Fornecedor de Serviço (fornece serviços a outros membros da federação ou permite acesso a recursos).

Utilizador Uma pessoa singular com vinculação a um Membro e que utiliza um serviço da Federação de Identidade RCTS através de um Fornecedor de Identidade responsável pelas suas credenciais.

Fornecedor de Identidade Componente que permite a transferência de dados necessários para a autenticação e autorização de um utilizador a um Fornecedor de Serviço.

Fornecedor de Serviço Componente que disponibiliza o acesso a serviços ou recursos aos utilizadores na Federação de Identidade RCTS.

Declaração de Práticas de Gestão de Identidade Descreve o ciclo de vida da gestão de identidades, incluindo os processos de inscrição, manutenção e remoção de informação de identidade no sistema de gestão de identidades, bem como o conjunto de processos administrativos, procedimentos e tecnologias relevantes usadas nesse ciclo de vida.

AUP Política de Utilização Aceitável.

Shared Secret Informação que é compartilhada exclusivamente entre as partes envolvidas numa comunicação segura.

Credenciais Combinação de informações, software e/ou hardware criptográfico que um Utilizador comprova possuir para se autenticar no Fornecedor de Identidade de uma organização Membro. Pode ser, por exemplo, uma combinação de nome de utilizador e palavra-chave ou um nome de utilizador e um dispositivo criptográfico.

Emissão de Credenciais Processo de emissão de um conjunto de credenciais para um Utilizador, que podem ser usadas pelo Utilizador para se autenticar no Fornecedor de Identidade de uma organização Membro. Inclui também o processo em que um Membro emite um conjunto adicional de credenciais para o mesmo Utilizador.

Reemissão de Credenciais O processo em que um Membro reemite credenciais para um Utilizador que anteriormente as recebeu (ex.: substituição de um dispositivo criptográfico com defeito, ou redefinição de uma palavra-chave esquecida).

Renovação de Credenciais O processo em que um Utilizador altera voluntariamente as suas credenciais, comprovando a posse das credenciais atuais (ex.: alterar uma palavra-chave comprovando o conhecimento da palavra-chave atual).

Revogação de Credenciais O processo em que o Membro invalida um conjunto de credenciais atualmente emitidas a um Utilizador (ex.: por suspeita de compromisso, ou porque o Utilizador já não pertence a uma organização Membro).

CAPTCHA Um teste de desafio-resposta usado para tentar garantir que a resposta é gerada por um ser humano.

Registrar Pessoa ou entidade responsável por verificar a identidade do requerente durante o processo de registo, presencial ou remotamente.

Look-Up Secret Authenticator Registo físico ou eletrónico que guarda um conjunto de segredos partilhados entre o requerente e a sua entidade, usado para procurar os segredos necessários num processo de verificação. É adequado como autenticação de backup em caso de perda, roubo ou falha da autenticação primária.

One-Time Password (OTP) Código único enviado ao utilizador, geralmente com 4 a 6 caracteres, que este deve inserir para verificar a sua identidade. Só pode ser usado uma vez e expira ao fim de um determinado período. Pode ser enviado por e-mail, chamada telefónica, aplicação (ex.: Google Authenticator, Microsoft Authenticator) ou SMS, e é usado como fator complementar ou como método único de autenticação.

Sequence Based One-Time Password O código OTP é gerado por uma função de hash criptográfica que combina uma chave secreta (simétrica e estática) com um contador, mantido tanto no token como no servidor de validação. No token, o contador incrementa a cada geração de código; no servidor, incrementa apenas quando um código é verificado.

Time-Based One-Time Password O código OTP é gerado por uma função de hash criptográfica que combina uma chave secreta com o tempo em vez de um contador, usando intervalos (“timestep”) tipicamente de 30 ou 60 segundos, durante os quais o código é válido.

Single-Fator OTP Device Dispositivo de hardware ou software (ex.: aplicação móvel) na posse do utilizador, que gera códigos OTP exibidos no dispositivo e inseridos manualmente no verificador, comprovando a posse e o controlo do dispositivo.

Multi-Fator OTP Device Semelhante ao Single-Fator OTP Device, mas cuja ativação exige adicionalmente algo que o utilizador conhece (ex.: segredo memorizado) ou que o utilizador é (ex.: biometria).

Out of Band Authentication (OOBA) Processo de autenticação que utiliza um canal de comunicação separado do canal primário entre as entidades, dificultando a interceção e subversão do processo (ex.: ataque “man-in-the-middle”), pois exige comprometer ambos os canais. Exemplo: um código enviado por SMS a um dispositivo móvel e introduzido na sessão de autenticação, ou o inverso, incluindo o uso de código QR para a transferência.

3. Introdução

Numa federação de identidade, o Fornecedor de Serviço (SP) confia a gestão da identidade digital dos seus utilizadores ao Fornecedor de Identidade (IdP) da organização a que pertencem. O Fornecedor de Serviço precisa de saber o grau de confiança que pode depositar nessa identidade, proporcional à criticidade dos serviços e dados que disponibiliza, de forma a determinar o nível de risco aceitável. Este documento define um conjunto de regras que permite à Federação de Identidade RCTS validar e afirmar essa confiança, de forma consistente entre todos os seus Membros.

Os componentes que definem a qualidade da identidade digital em termos de processos de acreditação, verificação de identidade, gestão de Credenciais e qualidade de atributos baseiam-se em três referências normativas:

- **REFEDS Assurance Framework v2.0 [RAF]** - a norma principal, publicada pela comunidade internacional REFEDS, que define os níveis de garantia de identidade (IAP low, medium, high) e os perfis de assurance Cappuccino e Espresso.
- **Regulamento de Execução (UE) 2015/1502 da Comissão [eIDAS-LoA]** - a legislação europeia que define os níveis de garantia eIDAS (Baixo, Substancial, Elevado) usados por meios de identificação eletrónica reconhecidos entre Estados-Membros, como o Cartão de Cidadão ou a Chave Móvel Digital.
- **Entity Authentication Assurance Framework [ITU-T X.1254 09/2020]** - uma recomendação técnica internacional da ITU-T sobre a robustez do processo de autenticação em si, usada como referência de apoio.

Os componentes encontram-se divididos da seguinte forma:

- **Identificadores**: requisitos inerentes ao processo de atribuição de um identificador único e permanente que representa uma pessoa física.
- **Verificação de Identidade e Gestão de Credenciais**: requisitos inerentes ao processo de identificação e credenciação dos indivíduos, atribuição de credenciais e respetiva renovação e substituição, correspondendo ao nível de garantia de identidade (IAP low, medium ou high) definido pela RAF v2.0.
- **Qualidade dos Atributos**: requisitos relativos à atribuição de determinados níveis de qualidade e atualização dos atributos transmitidos pela organização.

Os requisitos da secção de Autenticação nos documentos definem a robustez do processo de autenticação em si, um conceito distinto da garantia de identidade, de forma compatível com:

- **REFEDS Single Factor Authentication Profile [REFEDS-SFA]** - requisitos para autenticação de fator único.
- **REFEDS Multi-Factor Authentication Profile [REFEDS-MFA]** - requisitos para autenticação multifator.
- **NIST Digital Identity Guidelines: Authentication and Lifecycle Management [NIST 800-63B]** - guia técnico do NIST sobre níveis de garantia de autenticador.

3.1. Âmbito

Os Perfis de Confiabilidade definem requisitos sobre os processos de gestão de identidade da organização Membro, nomeadamente verificação de identidade, emissão, entrega, renovação e revogação de credenciais, e não sobre a tecnologia através da qual essas credenciais são utilizadas. Aplicam-se, por isso, a qualquer Fornecedor de Identidade na Federação de Identidade RCTS, independentemente do Perfil Tecnológico utilizado.

Quando as credenciais emitidas e geridas ao abrigo destes perfis são utilizadas em mais do que um Perfil Tecnológico, os requisitos aplicam-se a todos eles. A afirmação da conformidade

perante Fornecedores de Serviço, essa, depende do Perfil Tecnológico em causa e encontra-se definida nesse documento, podendo não estar prevista em todos.

4. Conformidade e Verificação

A autenticação num Perfil de Confiabilidade NÃO PODE ser afirmada, a menos que os seguintes critérios sejam garantidos:

1. A organização Membro é aprovada para o perfil de confiabilidade pretendido, pela equipa de Operação da Federação;
2. Foi provada a identidade do Utilizador de acordo com o perfil de confiabilidade pretendido; e
3. Todas as Credenciais utilizadas durante a autenticação são emitidas em conformidade com o perfil de confiabilidade pretendido.

Um Utilizador que cumpre um perfil de confiabilidade cumpre automaticamente também todos os perfis de nível inferior (ex.: a conformidade com RCTS-P2 inclui automaticamente RCTS-P0 e RCTS-P1). O Fornecedor de Identidade DEVE afirmar a conformidade de todos os perfis inferiores que o Utilizador também cumpre.

4.1. Procedimento de Verificação

1. As provas de conformidade com o perfil são OBRIGATORIAMENTE parte da Declaração de Práticas de Gestão de Identidade, elaborada no âmbito do processo de integração na Federação de Identidade RCTS. A Declaração DEVE descrever como a organização cumpre as partes normativas do perfil em causa.
2. O mecanismo de auditoria da Declaração é o seguinte: além da Declaração, a auditoria inclui uma ou mais reuniões, nas quais a equipa de Operação da Federação confirma que a organização Membro compreendeu os requisitos do perfil, produzindo um documento com o resultado da avaliação (Avaliação de Perfil de Confiabilidade).
3. A organização Membro DEVE confirmar anualmente que a Declaração se mantém atual e em conformidade com o perfil, e TEM DE submeter uma Declaração atualizada antes de alterar o processo ou a tecnologia de gestão de identidade, renovando assim a auditoria.
4. A Equipa de Gestão da Federação PODE exigir uma auditoria adicional à organização Membro, a realizar pela equipa de Operação da Federação ou por outra parte por esta aprovada.

5. Requisitos da Organização

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

1. A organização que opera o Fornecedor de Identidade tem de pertencer OBRIGATORIAMENTE a um membro da Federação de Identidade RCTS, ou estar sob contrato com uma organização que seja membro da Federação de Identidade RCTS.
2. O Fornecedor de Identidade TEM DE ser suficientemente fiável para ser utilizado no acesso aos sistemas internos da própria organização.
3. A organização Membro TEM DE publicar informação de contacto para o Fornecedor de Identidade e responder em tempo útil a incidentes e questões operacionais.
4. A organização Membro TEM DE garantir que os metadados registados na Federação estão completos, corretos e atualizados.
5. Todos os Membros da Federação de Identidade RCTS que emitem e gerem credenciais TEM DE:

1. Registar todas as informações relevantes para o processo de provisionamento, gestão de credenciais e fatores de autenticação, conservando-as na medida permitida pela legislação nacional e disponibilizando-as em caso de investigações e verificações de segurança das credenciais e dos dados dos titulares.
2. Implementar controlos de engenharia proporcionais ao risco de segurança das credenciais, garantindo confidencialidade, integridade e disponibilidade.
3. Permitir o acesso aos sistemas de gestão de credenciais e ao material criptográfico associado apenas a pessoal explicitamente autorizado e adequadamente treinado.
4. Garantir que nenhum segredo (armazenado ou gerado) é mantido sem criptografia nos seus sistemas.

6. Requisitos Operacionais

6.1. Identificadores

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

A cada identidade digital é atribuído um identificador que TEM DE cumprir os requisitos definidos nesta secção.

6.1.1. Identificadores Permitidos

1. Cada Fornecedor de Identidade TEM DE ter um identificador Global Único.
2. Cada Utilizador TEM DE ser representado por um identificador único atribuído pelo Fornecedor de Identidade.
3. Caso o utilizador possua mais do que um identificador único no Fornecedor de Identidade, TEM DE garantir que o utilizador pode escolher com qual pretende realizar a autenticação.

Orientações: *Para o requisito 2, o Perfil Tecnológico SAML WebSSO aceita:*

- SAML 2.0 persistent name identifier [OASIS SAML]
- SAML 2.0 subject-id ou pairwise-id [OASIS SIA]
- eduPersonUniqueId [eduPerson]
- eduPersonPrincipalName [eduPerson]

Ver a representação técnica publicada no espaço RCTSaai para a lista completa e respetivas condições.

6.1.2. Pessoa Física

O identificador do utilizador TEM DE representar uma pessoa física afiliada à organização com a qual o Fornecedor de Identidade está associado.

6.1.3. Pessoa Física Contactável

A organização com a qual o Fornecedor de Identidade está associado TEM DE ser capaz de entrar em contacto com a pessoa a quem o identificador é atribuído.

6.1.4. Reatribuição

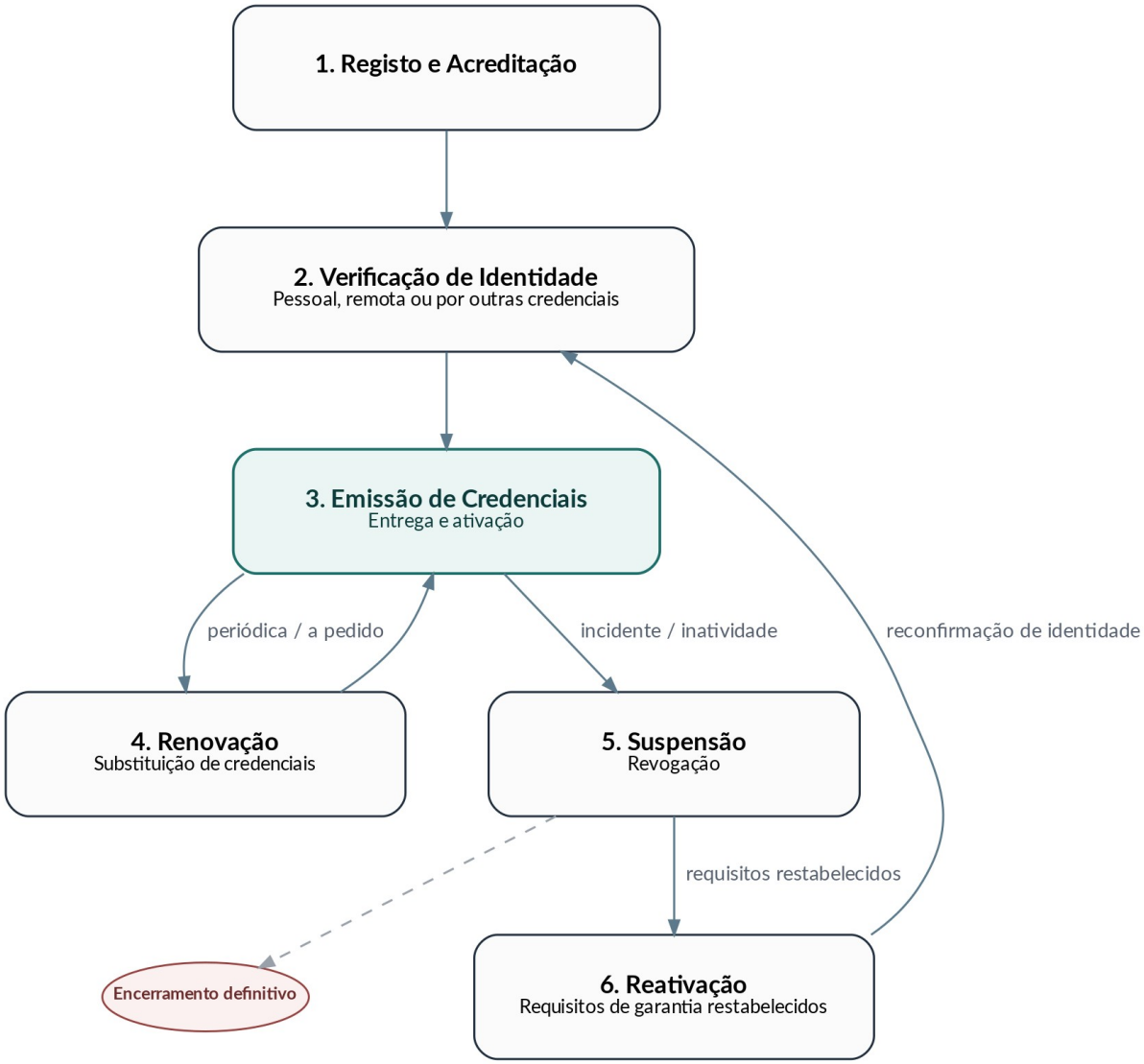
Os identificadores atribuídos aos utilizadores NUNCA PODEM ser reatribuídos.

6.2. Controlo e Verificação de Identidade e Gestão de Credenciais

Esta secção define os requisitos referentes aos procedimentos de identificação e acreditação dos utilizadores, e à emissão, renovação e substituição de credenciais que uma organização tem de garantir. As secções seguintes de verificação de identidade e gestão de credenciais correspondem ao nível de garantia que a RAF v2.0 designa por IAP (Identity Assurance Profile), medindo o rigor com que a identidade do utilizador foi verificada no registo, através de três níveis crescentes: low, medium e high. A suspensão, revogação e reativação de credenciais não fazem parte deste conceito, sendo um requisito próprio do RCTS.

Adicionalmente, o Fornecedor de Identidade PODE afirmar o claim https://refeds.org/assurance/IAP/local-enterprise (RAF v2.0, secção 5.2.2), sempre que o mesmo processo de verificação de identidade e gestão de credenciais seja também considerado, pela organização, suficiente para o acesso aos seus sistemas internos críticos. Este claim é cumulativo, não substitui a afirmação do nível IAP correspondente, e só é aplicável a partir do nível IAP medium (perfis RCTS-P1, RCTS-P2 e RCTS-P3).

Orientações: *No Perfil Tecnológico SAML WebSSO, este claim é comunicado através do atributo eduPersonAssurance.*



Ciclo de vida da identidade na Federação RCTS

A Reativação após suspensão ou revogação (etapa 6) só é realizada quando os requisitos de garantia estabelecidos antes da suspensão ou revogação forem restabelecidos, o que pode implicar reconfirmar a identidade do utilizador junto da organização (ver “Suspensão, Revogação e Reativação” mais abaixo).

6.2.1. Registo e Acreditação

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

1. A organização DEVE tornar acessíveis, a quem demonstre interesse legítimo, os seus procedimentos de registo e acreditação para o fornecimento de identidade eletrónica.
2. A organização TEM DE certificar-se de que o titular dos dados está familiarizado com os termos e condições de uso da identidade digital fornecida.

6.2.2. Controlo e Verificação de Identidade - RCTS-P2

Para o Perfil RCTS-P2 a organização TEM DE implementar um dos seguintes sistemas de verificação de identidade:

1. **Verificação Pessoal**: a organização TEM DE verificar a identidade por meio de um documento de identidade reconhecido pelo Estado Português que tenha sido verificado para estabelecer a sua autenticidade, confirmando que a evidência apresentada aparenta pertencer ao próprio requerente (por exemplo, comparando a fotografia do documento com a pessoa presente). Caso o documento contenha elementos intrínsecos de segurança (ex.: holograma, marca de água, chip criptográfico), esses elementos TEM DE ser verificados. A organização TEM DE ainda confirmar, junto de uma fonte autorizada (por exemplo, a entidade emissora do documento), que a identidade reclamada existe e pertence a uma pessoa real.
2. **Verificação Remota**: a organização TEM DE verificar a identidade da pessoa remotamente através de um documento de identidade reconhecido pelo Estado Português, confirmando a sua autenticidade, e TEM DE ainda confirmar, junto de uma fonte autorizada, que a identidade reclamada existe e pertence a uma pessoa real:

    ◦ Supervisionada: o documento é confirmado ao vivo por um Registar, via videochamada.

    ◦ Não Supervisionada: a organização TEM DE ainda cumprir os dois requisitos adicionais seguintes:

        ▪ Confirmar, junto de uma fonte confiável, que pelo menos um dos contactos fornecidos pertence ao requerente.

        ▪ Realizar uma comparação entre uma fotografia (ou outro elemento biométrico) do documento validado e uma fotografia, vídeo ou outro elemento biométrico do requerente recolhido durante o processo remoto, manualmente pelo Registar, ou por um sistema automático reconhecido por uma autoridade nacional ou internacional.
3. **Verificação com Base em outras Credenciais**: a organização PODE optar por aceitar credenciais de outros serviços para verificação de identidade. Nesse caso, as credenciais TEM DE ter sido fornecidas de acordo com regras compatíveis ou superiores às do nível RCTS-P2, e o individuo TEM DE demonstrar que tem controlo sobre as credenciais utilizadas (por exemplo, fazendo login com essa credencial perante a organização).

Nota: estes requisitos correspondem a IAP low + medium + high da RAF v2.0.

6.2.3. Emissão, Entrega e Ativação - RCTS-P2 e RCTS-P3

1. Uma vez emitidas, as credenciais TEM DE ser entregues através de um mecanismo que garante que são recebidas apenas pelo destinatário pretendido e entregues exclusivamente

na posse do próprio requerente a quem pertencem (por exemplo, entrega presencial com verificação de identidade no ato de entrega, ou envio para um endereço já validado durante o processo de verificação, com confirmação de receção pelo próprio).

2. As credenciais PODEM ser ativadas através de um link enviado por e-mail ou SMS. Na prática, esse link funciona como um segredo de utilização única, pelo que TEM DE cumprir os requisitos técnicos da secção “Autenticação de Fator Único” (ex.: mínimo de 6 caracteres alfanuméricos, válido até 10 minutos por SMS).

6.2.4. Integridade do Processo de Verificação e Registo - RCTS-P2 e RCTS-P3

1. A organização TEM DE garantir que o mesmo indivíduo conclui todas as etapas do processo de verificação de identidade e emissão de credenciais (ex.: a pessoa que apresenta os documentos de identidade é a mesma que recebe as credenciais emitidas).

2. Este processo TEM DE seguir procedimentos documentados que abrangem os requisitos aplicáveis a cada nível.

3. A organização TEM DE manter registo de:

   • Quando o indivíduo foi identificado e a que nível (ex.: data da verificação e perfil atribuído nessa data).

   • Alterações ao vínculo entre o titular e os seus autenticadores (ex.: password, chave FIDO, app de OTP) ou dados de contacto usados para comunicação e recuperação (ex.: e-mail, telefone) - por exemplo, sempre que um autenticador é substituído ou o contacto é atualizado (ver "Renovação e Substituição").

Estes registos devem ser conservados de acordo com as normas de retenção aplicáveis.

4. A organização TEM DE manter registo de quais atributos foram validados pelo processo de verificação de identidade (por exemplo, nome, data de nascimento e número do documento). TEM DE ainda manter registo do valor de pelo menos um atributo que identifique a pessoa de forma única (por exemplo, o número do documento de identidade).

Nota: estes requisitos correspondem a IAP high da RAF v2.0.

6.2.5. Suspensão, Revogação e Reativação

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

1. A organização Membro TEM DE poder suspender ou revogar credenciais de forma oportuna e eficaz, a pedido do Utilizador ou por decisão da organização Membro.
2. Quando a causa da suspensão ou revogação se deve a um incidente de segurança, o Membro TEM DE tomar precauções para evitar que o incidente ocorra novamente.
3. A reativação só é realizada se os requisitos de garantia estabelecidos antes da suspensão ou revogação forem restabelecidos.

6.2.6. Renovação e Substituição - RCTS-P0, RCTS-P1 e RCTS-P2

1. Todos os Utilizadores TEM DE ter permissão para renovar as suas credenciais.
2. O processo de renovação ou substituição TEM DE garantir os mesmos requisitos de verificação de identidade usados para a emissão de credenciais, ou TEM DE contar com um meio de identificação eletrónica com níveis de garantia equivalentes ou superiores aos da identidade em questão.

3. Sempre que a informação de contacto do Utilizador for atualizada, adicionada ou removida, a organização TEM DE aplicar os mesmos requisitos: nova verificação de identidade, ou confirmação através de um autenticador já vinculado à identidade verificada.

6.3. Qualidade dos Atributos

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

Esta secção define os requisitos de qualidade dos atributos de afiliação do Utilizador transmitidos pela organização em conjunto com a identidade digital, aplicáveis apenas às afiliações de aluno, docente, funcionário e membro.

1. Os Fornecedores de Identidade que transmitem a afiliação através dos atributos e valores acima mencionados DEVEM indicar a qualidade, entendida como frequência de atualização.
2. O valor da afiliação DEVE ser atualizado após a mudança de função ou término da afiliação com a organização.
3. A organização DEVE indicar se pode garantir um tempo de atualização do valor da afiliação dentro de 1 mês ou de 1 dia após o evento que desencadeou a mudança.

Orientações: *No Perfil Tecnológico SAML WebSSO, os atributos em causa são eduPersonAffiliation, eduPersonPrimaryAffiliation e eduPersonScopedAffiliation, com os valores student, faculty, employee e member.*

6.4. Autenticação

1. A organização TEM DE conseguir autenticar o Utilizador sempre que tal lhe seja solicitado, cumprindo os requisitos do perfil de confiabilidade que está a ser afirmado para esse Utilizador.

2. A organização TEM DE garantir a Autenticação de Fator Único (secção 6.4.1).

3. Para os perfis RCTS-P2 e RCTS-P3, a organização TEM DE vincular ao Utilizador um segundo fator de autenticação, conforme os requisitos da secção 6.4.2 (Autenticação Multifator), e TEM DE ser capaz de o exigir sempre que necessário.

   Este requisito diz respeito à capacidade da organização de exigir autenticação multifator, não a uma obrigação de a exercer em todas as sessões. Uma organização aprovada para RCTS-P2 ou RCTS-P3 continua conforme mesmo que, num determinado momento, um Utilizador se autentique apenas com um único fator.

   O que muda de sessão para sessão é a afirmação do perfil, não a conformidade da organização. Uma sessão em que apenas o fator único foi utilizado só pode ser afirmada no máximo como RCTS-P1, ainda que a organização esteja aprovada para um nível superior.

Orientações: *No Perfil Tecnológico SAML WebSSO, a solicitação multifactor é feita pelo Fornecedor de Serviço através do AuthnContextClassRef. O Perfil Tecnológico eduroam não dispõe deste mecanismo; a autenticação multifator não é aí exercida, o que não afeta a conformidade da organização com o perfil.*

6.4.1. Autenticação de Fator Único

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

1. A Autenticação de Fator Único dos Utilizadores TEM DE ser realizada utilizando uma das seguintes opções:

- **Segredo Memorizado**

O segredo memorizado TEM DE ter um tamanho mínimo de 8 caracteres quando escolhido de uma base com o mínimo de 72 caracteres diferentes, ou TEM DE ter um tamanho mínimo de 12 caracteres quando escolhido de uma base entre 52 e 72 caracteres (a base NÃO PODE ser inferior a 52 caracteres).

Tipo de Autenticação	Base	Tamanho Mínimo
Segredo Memorizado (conjunto de caracteres tipicamente escolhido pelo utilizador, palavra-chave/password ou PIN)	≥ 72 caracteres (ex.: 52 letras + 10 dígitos + 10 caracteres especiais)	8 caracteres
	≥ 52 caracteres (ex.: 52 letras a-z, A-Z)	12 caracteres

- **Segredo Gerado e de Utilização Única** (Time Based OTP Device / Out-of-Band Device)

O segredo gerado e de utilização única TEM DE ter um tamanho mínimo de 4 caracteres quando escolhido de uma base com o mínimo de 52 caracteres diferentes, ou TEM DE ter um tamanho mínimo de 6 caracteres quando escolhido de uma base de 10 a 51 caracteres.

Tipo de Autenticação	Base	Tamanho Mínimo

Segredo gerado e de utilização única (conjunto de caracteres gerado e enviado ao Utilizador para uso único)	≥ 52 caracteres (ex.: 52 letras a-z, A-Z)	4 caracteres
	10-51 caracteres (ex.: 10 dígitos)	6 caracteres

- **Segredo de Utilização Única** (Look-Up Secret / Sequence Based OTP Device)

O segredo de utilização única TEM DE ter um tamanho mínimo de 6 caracteres quando escolhido de uma base com o mínimo de 52 caracteres diferentes, ou TEM DE ter um tamanho mínimo de 10 caracteres quando escolhido de uma base de 10 a 51 caracteres.

Tipo de Autenticação	Base	Tamanho Mínimo
Segredo de utilização única	≥ 52 caracteres (ex.: 52 letras a-z, A-Z)	6 caracteres
	10-51 caracteres (ex.: 10 dígitos)	10 caracteres

- **Chave Criptográfica RSA/DSA** - TEM DE ter um tamanho mínimo de 2048 bit.
- **Chave Criptográfica ECDSA** - TEM DE ter um tamanho mínimo de 256 bit.
- **Dispositivo de Software ou Hardware de Criptografia de Fator Único** em conformidade com as especificações [NIST 800-63B].

2. O tempo de validade do processo de comunicação de um segredo TEM DE cumprir os seguintes prazos:
    - Segredos gerados através de dispositivos Time Based OTP Device: máximo de 5 minutos.
    - Segredos comunicados por telefone ou SMS: máximo de 10 minutos.
    - Segredos comunicados por e-mail: máximo de 24 horas.
    - Segredos comunicados por correio postal: máximo de 1 mês.

Orientações: *No Perfil Tecnológico SAML WebSSO, as especificações de autenticação do Perfil REFEDS SFA [REFEDS-SFA] são totalmente compatíveis com as especificações aqui indicadas.*

6.4.2. Autenticação MultiFator

Comum a todos os perfis: RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

1. A Autenticação Multifator dos Utilizadores TEM DE ser realizada utilizando uma das seguintes opções:
    - Uma combinação de dois ou mais fatores que cumprem os requisitos indicados para autenticação de fator único (secção anterior).
    - Dispositivo de Software ou Hardware de Criptografia Multifator em conformidade com as especificações [NIST 800-63B].
2. Os vários fatores utilizados numa autenticação Multifator TEM DE ser de tipos diferentes e TEM DE ser independentes.
3. O registo inicial de um segundo fator de autenticação PODE ser realizado através de um fator já existente, desde que:
    - a notificação de ativação seja transmitida pelos canais de contacto do Utilizador; e
    - sejam tomadas medidas de mitigação de risco equivalentes às referidas para a comunicação de segredos, ou o registo seja feito através de um processo supervisionado.

4. Após o registo inicial, qualquer adição, substituição ou recuperação de fatores TEM DE ser realizada através de autenticação multifator, não bastando um único fator já existente. O novo fator NÃO PODE, em qualquer caso, ser acessível utilizando apenas o fator já existente, e TEM DE ser independente de todas as outras operações de gestão, como revogar, alterar ou reativar.

Orientações: *No Perfil Tecnológico SAML WebSSO, as especificações de autenticação do Perfil REFEDS MFA [REFEDS-MFA] são totalmente compatíveis com as especificações aqui indicadas.*

Fatores independentes significa que o acesso a um fator não garante o acesso ao outro. Por exemplo, uma chave de segurança FIDO usada em combinação com uma palavra-chave não pode, por si só, ser usada para redefinir a palavra-chave.

7. Referências

- **[eIDAS-LoA]** Regulamento de Execução (UE) 2015/1502 da Comissão, de 8 de setembro de 2015. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32015R1502
- **[ITU-T X.1254 09/2020]** https://www.itu.int/rec/T-REC-X.1254-202009-P/en
- **[NIST 800-63B]** https://doi.org/10.6028/NIST.SP.800-63b
- **[RAF]** REFEDS Assurance Framework v2.0 (RAF 2.0), 5 de dezembro de 2023. https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf
- **[REFEDS-SFA]** REFEDS SFA Profile https://doi.org/10.5281/zenodo.5113499
- **[REFEDS-MFA]** REFEDS MFA Profile https://doi.org/10.5281/zenodo.5113296
- **[eduPerson]** Internet2/MACE. eduPerson Object Class Specification (201602) http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html
- **[REFEDS OIDCre]** OpenID Connect for Research and Education Working Group. Mapping SAML attributes to OIDC Claims. https://wiki.refeds.org/display/GROUPS/Mapping+SAML+attributes+to+OIDC+Claims

Anexo B - Critérios Normativos Aplicáveis (Nível IAP high)

Critérios da RAF v2.0 (secção 5.2.1) que este perfil TEM DE cumprir. Para a tabela comparativa completa entre os quatro perfis, ver o Anexo B do documento-mestre "Perfis de Confiabilidade de Identidade RCTS - Documento Consolidado".

Critério	Descrição
[GR1]	A mesma pessoa conclui todas as etapas do processo de verificação e emissão
[GR2]	Processo documentado, cobrindo todos os critérios aplicáveis ao nível suportado
[GR3]	Registo de quando e a que nível a pessoa foi verificada, e de alterações à vinculação (AB5)
[GR4]	Registo dos atributos validados pelo processo de verificação
[GR5]	Registo dos valores de atributo(s) que identificam unicamente a pessoa
[IE2]	Evidência válida, com atributo(s) que identificam unicamente a pessoa, emitida por fonte nacionalmente reconhecida (ou atestação documentada de uma autoridade aceite pelo Registar)
[VA3]	Elementos intrínsecos de segurança da evidência (físicos ou criptográficos) TEM DE ser verificados, quando presentes
[VA4]	A evidência é confirmada junto de uma fonte confiável e autoritativa que ateste que a identidade existe
[VF1]	Confirmação de que o requerente é uma pessoa
[VF2]	A evidência apresentada aparenta pertencer ao requerente
[AB1]	O requerente fornece e comprova o controlo de pelo menos um contacto
[AB2]	O autenticador emitido é entregue de forma a só poder chegar ao requerente
[AB3]	O autenticador emitido é entregue exclusivamente na posse do requerente
[AB4]	Reutilização de um autenticador previamente emitido exige prova de controlo sobre ele
[AB5]	Após a verificação inicial, a vinculação entre identidade e autenticadores/contactos é mantida em cada renovação, novo registo ou alteração de contacto
[UR1]	Pelo menos um contacto é confirmado junto de uma fonte confiável
[UR2]	É exigido o cumprimento de [VA4]
[UR3]	Comparação biométrica entre a evidência validada e o requerente (manual pelo Registar, ou automática e reconhecida por autoridade nacional/internacional)