FCCN UNIDADE DA FCT

Tecnologia para o Conhecimento

Federação de Identidade RCTS

Perfil de Confiabilidade RCTS – P3

FCT Fundação para a Ciência e a Tecnologia

ÍNDICE

índice 2
1. Terminologia 3
2. Termos e Definições 3
3. Introdução 5
4. Ambito, Objectivo e Sumário 5
5. Conformidade e Verificação 6
5.1 Procedimento de Verificação 6
6. Requisitos da Organização [= P0 P1 P2 P3] 6
7. Requisitos Operacionais 7
7.1 Identificadores [= P0 P1 P2 P3] 7
7.1.1 Identificadores Permitidos 7
7.1.2 Pessoa Física 7
7.1.3 Pessoa Física Contactável 8
7.1.4 Reatribuição 8
7.2 Controlo e Verificação de Identidade e Gestão de Credencias 8
7.2.1 Registo e ACREDITAÇÃO [= P0 P1 P2 P3] 8
7.2.2 Controlo e Verificação de Identidade 8
7.2.3 Emissão, Entrega e Ativação [= P2 P3] 8
7.2.4 Suspensão, Revogação e Reativação [= P0 P1 P2 P3] 8
7.2.5 Renovação e substituição 9
7.3 Qualidade dos ATRIBUTOS [= P0 P1 P2 P3] 9
7.4 Autenticação [= P2 P3] 10
7.4.1 Autenticação de Fator Único [= P0 P1 P2 P3] 10
7.4.2 Autenticação MultiFator [= P0 P1 P2 P3] 11
8. Referências 13
ANEXO A – Representação dos valores do Perfil de Confiabilidade RCTS-P3 14

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 uma organização que opera FORNECEDORES DE IDENTIDADE e/ou FORNECEDORES DE SERVIÇO e que adere à FEDERAÇÃO DE IDENTIDADE RCTS através do processo de adesão definido no presente documento.

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
Esta declaração 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. A declaração descreve o conjunto de processos administrativos, procedimentos e tecnologias relevantes usadas no ciclo de vida da gestão de identidades.

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 a possuir para se autenticar no *FORNECEDOR DE IDENTIDADE* de uma organização *MEMBRO*. Pode ser por exemplo, 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.* Também inclui 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 recebeu *CREDENCIAIS* (ex.: a substituição de um dispositivo criptográfico com defeito ou permitir que o *UTILIZADOR* possa redefinir 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 *MEMBRO* invalida um conjunto de *CREDENCIAIS* atualmente emitidas para um *UTILIZADOR* (ex.: revogar credenciais por existir suspeita de que as mesmas estejam comprometidas ou se *UTILIZADOR* já não pertence a uma organização *MEMBRO*).

CAPTCHA
Um teste de desafio-resposta usado como uma tentativa de garantir que a resposta seja gerada por um ser humano.

LOOK-UP SECRET AUTHENTICATOR
Registo físico ou eletrónico que guarda um conjunto de segredos partilhados entre o requerente e a sua entidade. O requerente utiliza este registo para procurar segredos que são necessários para responder num processo de verificação. É adequado para uma autenticação de backup em situações de perda, roubou ou problemas de funcionamento na autenticação primária.

ONE-TIME PASSWORD (OTP)
Código único enviado ao utilizador, geralmente composto por 4 a 6 carateres que o utilizador deve inserir para verificar a sua identidade. O código só pode ser utilizador uma vez e expira após um determinado período. Podem ser enviadas ao utilizador por e-mail, chamada telefónica, uma aplicação (ex: Google Authenticator ou Microsoft Authenticator) ou SMS. São frequentemente utilizadas como fator de autenticação complementar, mas também pode ser utilizado como método único de autenticação.

SEQUENCE BASED ONE-TIME PASSWORD
A geração do código OTP é realizada através de função de hash criptográfica que combina uma chave secreta (chave simétrica estática) e um contador. A chave secreta e o contador encontram-se no token e o servidor que valida os códigos OTP. No caso do token o contador é incrementado cada vez que selecionamos o botão para gerar um novo código. No servidor, o contador é incrementado apenas quando um código OTP é verificado.

TIME-BASED ONE-TIME PASSWORD
A geração do código OTP é realizada através de uma função de hash criptográfica que combina uma chave secreta (chave simétrica estática) e tempo em vez de um contador, ou seja, usa incrementos de tempo chamados “timestep” que são geralmente de 30 ou 60 segundos, o que significa que o código OTP é valido durante esse intervalo de tempo.

SINGLE-FATOR OTP DEVICE

Dispositivos de hardware ou software (ex.: aplicações instaladas em dispositivos móveis) que estão na posse do utilizador e que geram códigos OTP's. O código OTP é exibido no dispositivo e inserido manualmente no verificador comprovando a posse e o controlo do dispositivo.

MULTI-FATOR OTP DEVICE
Dispositivos semelhantes aos dispositivos SINGLE-FATOR OTP DEVICE, mas que requer uma ativação por algo que o utilizador conhece (ex.: segredo memorizado) ou que o utilizador é (ex.: através de biometria para obter uma senha única).

OUT OF BAND AUTHENTICATION (OOBA)
Processo de autenticação que utiliza um canal de comunicação separado do canal comunicação primário de duas entidades que pretende estabelecer uma ligação na autenticação. A utilização de um canal de comunicação separado torna mais difícil intercetar e subverter o processo de autenticação (ex.: ataque "man-in-the-middle") porque exige que sejam comprometidos os dois canais de comunicação. Exemplo desta forma de autenticação OOB são os códigos enviados para um dispositivo móvel via SMS onde o requerente pode receber o segredo e digita o mesmo (normalmente um código de 6 dígitos) na sua sessão de autenticação ou por exemplo o requerente pode visualizar o segredo na sua sessão de autenticação e digitá-lo num aplicativo do seu dispositivo móvel ou usar uma tecnologia como código QR para efetuar a transferência.

3. INTRODUÇÃO

Este documento define um conjunto de regras que permite validar e afirmar a qualidade da identidade digital dos *UTILIZADORES* da *FEDERAÇÃO DE IDENTIDADE RCTS*.

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 no *REFEDS Assurance Framework* [RAF], nos níveis de garantia definidos pelo REGULAMENTO DE EXECUÇÃO (UE) 2015/1502 DA COMISSÃO 2015/1502 [eIDAS -LoA] e *Entity Authentication Assurance Framework* [ITU-T X.1254 09/2020]. Os componentes encontram-se divididos da seguinte forma:

- Identificadores: define os requisitos inerentes ao processo de atribuição de um identificador único e permanente que representa uma pessoa física.
- Verificação de Identidade e Gestão de *CREDENCIAIS*: define os requisitos inerentes ao processo de identificação, credenciação dos indivíduos, atribuição de *CREDENCIAIS* e respetiva renovação e substituição realizado por uma organização.
- Qualidade dos Atributos: define os requisitos relativos ao processo de atribuição de determinados níveis de qualidade e atualização dos atributos transmitidos pela organização.

Os componentes que definem a robustez do processo de autenticação são baseados no *REFEDS Single Factor Authentication Profile* [REFEDS-SFA], no *REFEDS Multi-Factor Authentication Profile* [REFEDS-MFA] e no documento de diretrizes para a identidade digital *Authentication and Lifecycle Management NIST* [NIST 800-63B].

4. AMBITO, OBJECTIVO E SUMÁRIO

Neste documento são definidas as regras do perfil de confiabilidade RCTS-P3.

O Perfil de Confiabilidade RCTS-P3 significa o seguinte:

- O perfil é uma extensão do RCTS-P2;
- O individuo é afiliado a um membro da Federação de Identidade RCTS;
- A organização membro identificou e confirmou o individuo;
- O individuo tem um identificador único e permanente;
- Atributos/Informações associadas à conta do utilizador são da responsabilidade da organização Membro;
- Autenticação Multifator é Obrigatória

Os *FORNECEDORES DE SERVIÇO* PODEM exigir níveis de garantia de identidade superiores e DEVEM garantir métodos que permitam avaliar o grau de confiabilidade recebido.

Os *FORNECEDORES DE IDENTIDADE* TEM DE ter a capacidade de recorrer a regras claras e partilhadas para implementar processos e métodos de gestão de identidade de acordo com o grau de confiabilidade exigido ou esperado.

5. CONFORMIDADE E VERIFICAÇÃO

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

1. A organização *MEMBRO* é aprovada para este perfil de confiabilidade, ou superior, pela equipa de *OPERAÇÃO DA FEDERAÇÃO;*
2. Foi provada de identidade do Utilizador de acordo com este perfil de confiabilidade ou superior; e
3. Todas as *CREDENCIAIS* utilizadas durante a autenticação são emitidas em conformidade com este perfil de confiabilidade ou superior.

Um *UTILIZADOR* que cumpre com este perfil de confiabilidade também cumpre com o perfil de confiabilidade RCTS P0, P1, P2. O Fornecedor de Identidade DEVE afirmar conformidade do perfil de confiabilidade RCTS P0, P1, P2 e P3 para o *UTILIZADOR*.

Orientação: Perfis com requisitos mais elevados inclui automaticamente perfis com requisitos mais baixos, como por exemplo a declaração de conformidade do perfil RCTS P2 inclui automaticamente os perfis RCTS-P0 e RCTS-P1

5.1 PROCEDIMENTO DE VERIFICAÇÃO

1. Provas de conformidade com este perfil são OBRIGATORIAMENTE parte da *DECLARAÇÃO DE PRÁTICAS DE GESTÃO DE IDENTIDADE*, mantidas como parte do processo de integração na FEDERAÇÃO DE IDENTIDADE RCTS. A *DECLARAÇÃO DE PRÁTICAS DE GESTÃO DE IDENTIDADE*, DEVE descrever como a organização cumpre as partes normativas deste documento.

2. A equipa de *OPERAÇÃO DA FEDERAÇÃO* ou outra parte aprovada pela *EQUIPA DE GESTÃO DA FEDERAÇÃO* realiza uma auditoria com base na *DECLARAÇÃO DE PRÁTICAS DE GESTÃO DE IDENTIDADE* enviada. A auditoria inclui uma ou mais reuniões onde a equipa de *OPERAÇÃO DA FEDERAÇÃO* verifica que a organização *MEMBRO* compreendeu os requisitos do perfil de confiabilidade sendo realizado um documento que reflete a avaliação realizada durante a auditoria.

3. A organização *MEMBRO* DEVE confirmar anualmente que a sua *DECLARAÇÃO DE PRÁTICAS DE GESTÃO DE IDENTIDADE* se encontra atual e em conformidade com o perfil. A organização membro TEM DE enviar uma *DECLARAÇÃO DE PRÁTICAS DE GESTÃO DE IDENTIDADE* atualizada antes de realizar alterações ao processo/tecnologia de gestão de identidade de forma a renovar a auditoria.

4. A equipa de *GESTÃO DA FEDERAÇÃO* PODE impor uma auditoria adicional da organização *MEMBRO* realizada pela equipa de *OPERAÇÃO DA FEDERAÇÃO*, ou outra parte aprovada pela equipa de *GESTÃO DA FEDERAÇÃO.*

6. REQUISITOS DA ORGANIZAÇÃO [= P0 P1 P2 P3]

[=] Os requisitos desta secção são válidos e comuns para 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 terá de estar sob contrato com uma organização que seja membro da FEDERAÇÃO DE IDENTIDADE RCTS.

2. Todas os MEMBROS que fazem parte DA FEDERAÇÃO DE IDENTIDADE RCTS que emitem e realizam a gestão de *CREDENCIAIS* DEVEM:

   - Registar todas as informações relevantes para o processo de provisionamento, gestão de *CREDENCIAIS* e fatores de autenticação, conservá-las na medida permitida pela legislação nacional e disponibilizá-las em caso de investigações e verificações da segurança das *CREDENCIAIS* e dos dados dos titulares dos dados.

   - Implementar controles de engenharia proporcionais ao risco de segurança das *CREDENCIAIS* para garantir a confidencialidade, integridade e disponibilidade das *CREDENCIAIS*.

   - Permitir o acesso aos sistemas de gestão de *CREDENCIAIS* e ao material criptográfico associado apenas a pessoal explicitamente autorizado e adequadamente treinado.

   - Certifique-se de que nenhum segredo (armazenado ou gerado) seja mantido sem criptografia nos seus sistemas.

7. REQUISITOS OPERACIONAIS

7.1 IDENTIFICADORES [= P0 P1 P2 P3]

[=] Os requisitos desta secção são válidos e comuns para 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.

7.1.1 IDENTIFICADORES PERMITIDOS

1. Cada FORNECEDOR DE IDENTIDADE TEM DE ter um identificador Global Único
2. O identificador do UTILIZADOR transmitido pelo FORNECEDOR DE IDENTIDADE TEM DE ser pelo menos um dos seguintes:

   - SAML 2.0 persistent name identifier [OASIS SAML]
   - SAML 2.0 subject-id ou pairwise-id [OASIS SIA]
   - OIDC sub con type public o pairwise [OpenID.Core]
   - eduPersonUniqueId [eduPerson]
   - eduPersonPrincipalName [eduPerson]

3. Caso o UTILIZADOR possua mais do que um identificador único no FORNECEDOR DE IDENTIDADE, TEM DE garantir que UTILIZADOR pode escolher com qual pretende realizar a autenticação.

7.1.2 PESSOA FÍSICA

O identificador do UTILIZADOR TEM DE representar uma pessoa física afiliada com a ORGANIZAÇÃO com o qual o FORNECEDOR DE IDENTIDADE está associado.

7.1.3 PESSOA FÍSICA CONTACTÁVEL

A ORGANIZAÇÃO com o qual o FORNECEDOR DE IDENTIDADE está associado TEM DE ser capaz de entrar em contacto com a pessoa a quem o identificador é atribuído.

7.1.4 REATRIBUIÇÃO

Os identificadores atribuídos aos UTILIZADORES NUNCA PODEM ser reatribuídos.

7.2 CONTROLO E VERIFICAÇÃO DE IDENTIDADE E GESTÃO DE CREDENCIAS

Esta seção tem como objetivo definir os requisitos referente aos procedimentos de identificação e acreditação dos UTILIZADORES, emissão, renovação e substituição de CREDENCIAIS que uma ORGANIZAÇÃO tem de garantir.

7.2.1 REGISTO E ACREDITAÇÃO [= P0 P1 P2 P3]

[=] Os requisitos desta subsecção são válidos e comuns para todos os perfis RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3

1. A organização DEVE tornar públicos e acessíveis aos interessados 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.

7.2.2 CONTROLO E VERIFICAÇÃO DE IDENTIDADE

1. A ORGANIZAÇÃO TEM DE realizar o controlo e verificação de identidade para que possa emitir *CREDENCIAIS* ao UTILIZADOR.

2. Para o Perfil RCTS-P3 a ORGANIZAÇÃO TEM DE implementar um sistema de verificação de identidade de acordo com o Regulamento eIDAS [eIDAS] para nível de confiança Elevado.

7.2.3 EMISSÃO, ENTREGA E ATIVAÇÃO [= P2 P3]

1. Uma vez emitidas, as *CREDENCIAIS* TEM DE ser entregues através de um mecanismo que garante que as mesmas são recebidas apenas pelo destinatário pretendido.

2. 2. As *CREDENCIAIS* PODEM ser ativadas através do envio de links via e-mail ou SMS, caso em que TEM DE cumprir os requisitos estabelecidos posteriormente no Ponto 2 da secção 7.4.1 Autenticação de Fator Único.

7.2.4 SUSPENSÃO, REVOGAÇÃO E REATIVAÇÃO [= P0 P1 P2 P3]

[=] Estes requisitos são válidos e comuns para 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 das *CREDENCIAIS* se deve a um incidente de segurança, o MEMBRO TEM DE tomar precauções para evitar que o incidente ocorra novamente.

3. A reativação é realizada somente se os requisitos de garantia estabelecidos antes da suspensão ou revogação forem restabelecidos.

7.2.5 RENOVAÇÃO E SUBSTITUIÇÃO

1. Todos os UTILIZADORES TÊM 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 emissão de credenciais, ou seja, necessário garantir a confirmação por meio de identificação eletrónica através de uma fonte autoritativa idêntica à utilizada na verificação de identidade.

7.3 QUALIDADE DOS ATRIBUTOS [= P0 P1 P2 P3]

[=] Os requisitos desta secção são válidos e comuns para todos os perfis RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

Esta secção define os requisitos que determinam a qualidade dos atributos referentes à afiliação do UTILIZADOR que podem ser transmitidos pelo FORNECEDOR DE IDENTIDADE em conjunto com a identidade digital.

1. Os requisitos definidos nesta secção para os atributos referentes à afiliação do UTILIZADOR são exclusivos aos atributos *eduPersonAffiliation, eduPersonPrimaryAffiliation e eduPersonScopedAffiliation* e apenas para a afiliação de alunos, docentes e membros.

2. Os FORNECEDORES DE IDENTIDADE que transmitem a afiliação através dos atributos e valores acima mencionados DEVE indicar a qualidade, entendida como frequência de atualização.

3. O valor da afiliação DEVE ser atualizado após a mudança de função ou término da afiliação com a ORGANIZAÇÃO.

5. A ORGANIZAÇÃO DEVE indicar se podem garantir um tempo de atualização do valor do afiliado dentro de 1 mês a 1 dia do evento que desencadeou a mudança.

7.4 AUTENTICAÇÃO [= P2 P3]

1. O FORNECEDOR DE IDENTIDADE TEM DE autenticar o UTILIZADOR a pedido do FORNECEDOR DE SERVIÇO.

2. O Fornecedor de Identidade TEM DE garantir a Autenticação de Fator Único e TÊM DE garantir a Autenticação Multi Fator.

7.4.1 AUTENTICAÇÃO DE FATOR ÚNICO [= P0 P1 P2 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 72 caracteres diferentes ou TEM DE ter um tamanho mínimo de 12 caracteres quando escolhido de uma base entre 52 a 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 52 caracteres diferentes ou TEM DE ter um tamanho mínimo de 12 caracteres quando escolhido de uma base de 10 a 51 caracteres.

Tipo de Autenticação	Base	Tamanho Mínimo
Segredo gerado e utilização única (Conjunto *de caracteres gerados e enviado ao Utilizador para ser utilizado uma única vez)*	**≥ 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)

Segredo de utilização única TEM DE ter um tamanho mínimo de 4 caracteres quando escolhido de uma base com o mínimo 52 caracteres diferentes ou TEM DE ter um tamanho mínimo de 12 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/DAS**
  Chaves criptográficas RSA/DAS *TEM DE ter um tamanho mínimo de 2048 bit*

- **Chave criptográfica ECDSA**
  Chaves criptográficas 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 TEM DE ser válidos por um tempo máximo de 5 minutos.
   - Segredos comunicados e transmitidos por telefone ou SMS TEM DE ser válidos por um tempo máximo de 10 minutos.
   - Segredos comunicados e transmitidos por e-Mail TEM DE ser válidos por um tempo máximo de 24 horas.
   - Segredos comunicados por correio postal TEM DE ser válidos por um tempo máximo de 1 mês.

3. As especificações de autenticação do Perfil REFEDS SFA [REFEDS-SFA] são totalmente compatíveis com as especificações aqui indicadas.

7.4.2 AUTENTICAÇÃO MULTIFATOR [= P0 P1 P2 P3]

1. A Autenticação de 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 (definidos na subsecção 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

3. Os vários fatores utilizados numa autenticação Multifator TEM DE ser independentes.

4. A ativação de um novo fator de autenticação PODE ser realizada através de um fator já existente, neste caso a notificação de ativação DEVE ser transmitida pelos canais de contacto do Utilizador e TEM DE ser tomadas medidas de acordo com os requisitos mencionados no ponto 1 da secção 3.4 ou através de um processo supervisionado de forma a mitigar o risco. Em qualquer um dos casos, o novo fator NÃO

PODE ser acessível utilizando o fator já existente e TEM DE ser independente de todas as outras operações de gestão, como revogar, alterar ou reativar.

5. As especificações de autenticação do Perfil REFEDS MFA [REFEDS-MFA] são totalmente compatíveis com as especificações aqui indicadas.

***Orientações**: Fatores independentes significa que o acesso a um fator não garante, acesso ao outro fator. 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.*

8. REFERÊNCIAS

- [eIDAS-LoA]
  https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015R1502

- [ITU-T X.1254 09/2020]
  https://www.itu.int/rec/T-REC-X.1254

- [NIST 800-63B]
  https://doi.org/10.6028/NIST.SP.800-63b

- [RAF] REFEDS Assurance Framework
  https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

- [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. Referenced 9 February 2018
  https://wiki.refeds.org/display/GROUPS/Mapping+SAML+attributes+to+OIDC+Claims

ANEXO A – REPRESENTAÇÃO DOS VALORES DO PERFIL DE CONFIABILIDADE RCTS-P3

Todos os perfis de confiabilidade de identidade da Federação RCTS e os valores dos componentes de confiabilidade (Identificadores, Verificação de Identidade, Gestão de Credenciais e Qualidade dos Atributos) a eles associados, são expressos através do atributo SAML 2.0 *[eduPerson]* eduPersonAssurance ou por meio de uma declaração OIDC *[REFEDS OIDCre]* edu_person_assurance.

<table>
<tr><th colspan="3">Componente de Confiabilidade</th><th>Valores</th></tr>
<tr><td colspan="3">Identificadores</td><td>https://refeds.org/assurance
https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign</td></tr>
<tr><td colspan="2" rowspan="3">Qualidade dos Atributos [1]</td><td>Não Cumpre</td><td></td></tr>
<tr><td>Atualização em 1 Mês</td><td>https://refeds.org/assurance/ATP/ePA-1m</td></tr>
<tr><td>Atualização em 1 Dia</td><td>https://refeds.org/assurance/ATP/ePA-1d</td></tr>
<tr><td rowspan="2">Controlo e Verificação de Identidade e Gestão de Credenciais [2]</td><td rowspan="2">Tipo de Autenticação</td><td>Fator Único</td><td>https://refeds.org/assurance/IAP/low
https://refeds.org/assurance/IAP/medium
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P0
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P1
https://refeds.org/assurance/cappuccino</td></tr>
<tr><td>Múltiplo Fator</td><td>https://refeds.org/assurance/IAP/low
https://refeds.org/assurance/IAP/medium
https://refeds.org/assurance/IAP/high
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P0
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P1
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P2
https://rctsfederation.fccn.pt/policy/assurance/RCTS-P3
https://refeds.org/assurance/cappuccino
https://refeds.org/assurance/espresso</td></tr>
</table>

[1] Se o Fornecedor de Identidade não cumpre os requisitos do componente "Qualidade dos Atributos" não deve ser adicionado valor.

[2] Um utilizador que garante o **perfil RCTS-P3 deve ser sinalizado com RCTS-P1** quando **não estiver a utilizar a autenticação multi-factor**.

Caso de Uso I

- Acesso a serviços críticos ou altamente confidenciais onde é essencial a verificação da identidade dos acessos.
- Identificação verificada através de outras credenciais como por exemplo o Chave Móvel Digital ou Cartão de Cidadão; e
- Autenticação múltiplo fator.