EUROPEAN TLD ISAC

Diretrizes sobre as Melhores Práticas de Segurança do EPP

PARA OPERADORES TLD EUROPEUS

TLP:CLEAR

DIRETRIZES SOBRE AS MELHORES PRÁTICAS DE SEGURANÇA DO EPP 2025

SOBRE O TLD ISAC EUROPEU

O European Top-Level Domain Information Sharing and Analysis Centre (TLD ISAC Europeu) é uma iniciativa de colaboração dedicada a fortalecer a postura de cibersegurança dos registries de top-level domain com código de país (ccTLD) em toda a Europa. Funciona como uma plataforma fiável para a partilha de informações sobre ameaças, promovendo as melhores práticas e fomentando a cooperação entre operadores de ccTLD, peritos em segurança e outras partes interessadas.
Para mais informações, aceda a https://www.tld-isac.eu.

CONTACTO

Para contactar o TLD ISAC Europeu ou para questões de imprensa sobre este relatório, envie um e-mail para info@tld-isac.eu.

AVISO LEGAL

O TLD ISAC Europeu é um Grupo de Trabalho especial do CENTR ASBL/VZW. Esta publicação representa os pontos de vista e as interpretações do CENTR. O CENTR reserva-se o direito de alterar, atualizar ou remover a publicação ou qualquer um dos seus conteúdos. Destina-se apenas a fins informativos e deve ser acessível gratuitamente.
Todas as referências à publicação ou à sua utilização, no todo ou em parte, devem indicar o CENTR e TLD ISAC Europeu como fonte. As fontes de terceiros são citadas quando necessário. O CENTR não é responsável pelo conteúdo das fontes externas, incluindo websites externos, referenciadas nesta publicação. Nem o CENTR nem qualquer pessoa que atue em seu nome é responsável pela utilização passível de ser feita das informações contidas nesta publicação. O CENTR detém os seus direitos de propriedade intelectual relativamente a esta publicação.

NOTA DA VERSÃO PORTUGUESA

Este documento é uma tradução para português do documento original publicado pelo TLD ISAC Europeu. A tradução apresentada foi realizada no âmbito do programa de capacitação digital da LusNIC e CDA/ICANN, sendo esta fornecida apenas para fins informativos. Em caso de divergência, inconsistência ou dúvida de interpretação, a versão original prevalece.

A LusNIC agradece ao TLD ISAC Europeu, entidade responsável pelo documento original, pela produção e disponibilização destes conteúdos, que serviram de base à presente tradução para português, realizada com o objetivo de apoiar a capacitação e a partilha de conhecimento entre os membros da comunidade LusNIC.

Índice

1. Lista de abreviaturas:

ccTLD	Top-Level Domain com Código de País (operator registry)
DAST	Teste Dinâmico de Segurança de Aplicações
DNS	Sistema de Nome de Domínio
DoS	Denial of Service
ENISA	Agência da União Europeia para a Cibersegurança
EPP	Extensible Provisioning Protocol (EPP), um protocolo de texto baseado em XML.
IaaS	Infraestrutura como Serviço
IETF	Internet Engineering Task Force
PA	Ativo Primário
PaaS	Plataforma como Serviço
RFC	Request for Comments
SaaS	Software como Serviço
SAST	Teste Estático de Segurança de Aplicações
SIEM	Gestão de Informações e Eventos de Segurança
SOC	Centro de Operações de Segurança
SSDLC	Ciclo de Vida de Desenvolvimento Seguro de Software
VPN	Rede Privada Virtual

2. Introdução

Em janeiro de 2023, entrou em vigor a Diretiva "NIS2" (UE) 2022/2555 [1], relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia. Ao abrigo da Diretiva NIS2, a Comissão Europeia adota atos de implementação que estabelecem os requisitos técnicos e as metodológicos para as medidas de gestão dos riscos de cibersegurança e contêm regras técnicas e metodológicas, bem como regras setoriais específicas.

No âmbito das suas atividades, o TLD ISAC Europeu criou um projeto interno para desenvolver diretrizes sobre as melhores práticas de segurança para ambientes de operadores de registry de Top-Level Domains (TLD) que utilizam o Extensible Provisioning Protocol (EPP). O EPP RFC 5730 inicial foi normalizado em 2009 pela Internet Engineering Task Force (IETF). Desde então, a tecnologia e o estado da arte no que respeita à segurança informática têm evoluído continuamente, dando origem a medidas de segurança adicionais. Qualquer vulnerabilidade relacionada com as implementações do EPP e respetiva infraestrutura tem um impacto direto na infraestrutura do sistema de nomes de domínio (DNS).

A ideia subjacente a uma linha de base é definir medidas consideradas básicas e que não devem necessitar de qualquer alinhamento ou análise de risco adicional. Devem ser simplesmente aplicadas. Para além disso, deve aplicar medidas de segurança individuais adicionais ao seu ambiente EPP.

2.1 Âmbito

Incluído no âmbito

O objetivo do presente documento é fornecer diretrizes para as melhores práticas de segurança de EPP e recomendações de segurança a adotar pelos registries de TLD.
Todas as recomendações de segurança fornecidas são descritas de forma genérica e destinam-se a ser adotadas pelos operadores de TLD e integradas nos seus quadros de política informática.

Excluído do âmbito

O presente documento fornece recomendações de segurança específicas para o EPP - não fornece uma lista exaustiva e completa de requisitos de segurança para proteger uma organização completa. A NIS2 e outras legislações locais devem ser consideradas separadamente.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

2.2 Público-alvo

O principal grupo-alvo destas diretrizes de segurança do EPP são as pessoas relacionadas com os registries e registrars de TLD dos seguintes grupos

- CISOs
- Administradores e Programadores
- Auditores

2.3 Classificação

Estas diretrizes são públicas e classificadas como TLP:CLEAR.

2.4 Visão geral da abordagem de desenvolvimento das diretrizes

A equipa do projeto TLD ISAC foi incumbida de desenvolver uma base de segurança específica para o EPP sob a forma de diretrizes. A equipa trabalhou em estreita colaboração com a comunidade TLD ISAC para identificar e documentar um conjunto de normas mutuamente acordadas que os operadores de registry de qualquer dimensão devem implementar. Essas normas apoiam a operação de uma infraestrutura segura de EPP. Após a elaboração das diretrizes e uma ronda final de comentários, as diretrizes foram validadas num ambiente de teste e, em seguida, finalizadas.

2.5 Como ler e trabalhar com estas diretrizes

Para utilizar estas diretrizes de forma eficaz, sugerimos que comece pelos capítulos "*3.1 Definições de palavras-chave (RFC2119)*", "*3.2 Descrição da estrutura dos requisitos de segurança*", "*3.3 Visão geral da identificação de ativos TLD ISAC*" e, em seguida, reveja o capítulo "*4 Diretrizes EPP - Requisitos de segurança*".

De seguida, recomendamos a integração destas diretrizes na sua estrutura de política de segurança informática existente. Por último, avalie a exequibilidade de definir controlos automáticos que monitorizem continuamente a sua infraestrutura para detetar configurações incorretas e violações destas diretrizes (por exemplo, caso alguém desative a autenticação forte).

3. Convenções

3.1 Definições de palavras-chave (RFC2119)

As palavras-chave “DEVE”, “NÃO DEVE”, “REQUER”, “DEVERIA”, “NÃO DEVERIA”, “PODERIA”, “NÃO PODERIA”, “RECOMENDÁVEL”, “PODE”, e “OPCIONAL” contidas neste documento devem ser interpretadas conforme descrito em [RFC2119].

3.2 Descrição da estrutura dos requisitos de segurança

Cada secção apresenta uma visão geral dos requisitos de segurança relacionados com o EPP e funciona como uma orientação para as tarefas recomendadas para proteger os ambientes relacionados com o EPP.

Cada requisito utiliza a seguinte estrutura:

ELEMENTO	ELEMENTO
IDENTIFICAÇÃO DO REQUISITO	Identificador único que utiliza a seguinte convenção de nomenclatura: TLD-EPP-<Area>-<Incremented-Digits>
REQUISITO DE SEGURANÇA	Descrição do requisito de segurança.
TIPO	Tipo de requisito de segurança em conformidade com as convenções (vrt RFC2119 and secção “Convenções”), p.ex., “DEVE”, “PODERIA”, etc.
RISCO	Descrição dos riscos caso o requisito não seja cumprido ou seja apenas parcialmente cumprido
RECOMENDAÇÃO	Recomendação prática
ATIVO (PA)	Ligação à identificação do ativo TLD ISAC (ver secção 3.3), com destaque para o impacto do EPP
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	Referência a identificações relacionadas com a “Diretiva NIS2 - Regulamento de Execução da Comissão C (2024) 7151 - ANEXO (ver https:// digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks). O cumprimento do requisito de segurança do EPP não implica que todas as identificações de objetivos de segurança referenciadas da NIS2 sejam plenamente satisfeitas.
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

3.3 Visão geral da identificação de ativos TLD ISAC

A NIS2 exige que as organizações realizem avaliações de risco. Caso se trate de um registry ou registrar abrangido pela NIS2, terá de realizar avaliações de risco. Dado que as avaliações de risco costumam utilizam uma abordagem baseada em ativos, decidimos mapear cada requisito de segurança em relação a um ativo primário (PA). Infelizmente, cada organização pode ter uma definição e uma classificação diferentes dos seus ativos relacionados com a segurança da informação. Neste sentido, decidimos utilizar a definição de ativo primário da Agência da União Europeia para a Cibersegurança (ENISA), conforme consta do documento "METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS September 2021", página 15, na qual ativos primários estão definidos como:

Ativos primários

- Processos e atividades empresariais
- Ativos funcionais
- Ativos de informação

Para ter uma estrutura de ativos comum, fornecemos, a título de exemplo, uma categorização dos ativos primários do TLD. Esta pode ser tomada como ponto de partida, dependendo da maturidade da sua gestão de ativos. A sua própria organização pode ter categorias adicionais ou diferentes, pelo que pode adotar a lista de acordo com as suas necessidades. Recordamos que o presente documento tem como objetivo fornecer requisitos de segurança específicos do EPP.
Por conseguinte, nem todas as identificações de ativos primários fornecidas estão associadas a um requisito de segurança.

Explicação das colunas

- ID: Identificação única com a seguinte estrutura:
- PA-<categoria de PA de dois dígitos (BP,FA,I)>-<dígito>
- Categoria do Ativo Primário: indica se o ativo é um processo empresarial, um Ativo Funcional ou um Ativo de Informação (ver definição da ENISA)
- Título e Descrição do Ativo Primário: nome do ativo e breve descrição (p. ex., a sua função nas operações do Registrar de domínios)
- Exemplos de EPP: exemplos específicos relacionados com o EPP para cada ativo primário, quando aplicável. Caso contrário, preencher com "N/A".

ID	CATEGORIA DO ATIVO PRIMÁRIO	TÍTULO DO ATIVO PRIMÁRIO	DESCRIÇÃO DO ATIVO PRIMÁRIO	EXEMPLOS DE EPP
PA-BP-1	Processo Empresarial	Processo de Registo de Domínios	Processo de aprovisionamento, atualização, transferência e renovação de domínios.	Comandos EPP para criação, atualização, transferência e eliminação de domínios
PA-BP-2	Processo Empresarial	Processo de Faturação e Pagamento	Processo de geração de faturas, processamento de pagamentos e gestão de transações financeiras.	Registos de transações do EPP para faturação
PA-BP-3	Processo Empresarial	Apoio ao Cliente e Processo de Serviço	Tratamento de pedidos de informação de clientes, resolução de problemas e gestão de interações.	Registos da API do EPP para a resolução de problemas
PA-BP-4	Processo Empresarial	Processo de Gestão da Conformidade e da Regulamentação	Garantir a adesão à NIS2, ao RGPD e a outros requisitos regulamentares e de conformidade.	Processos de segurança informática relacionados com o EPP (p. ex., estabelecer um ciclo de vida de desenvolvimento seguro de software para o seu ambiente EPP ou realizar uma avaliação dos riscos para o seu ambiente EPP)
PA-BP-5	Processo Empresarial	Processo de Continuidade de Negócios e Recuperação de Desastres	Estratégias e ações para garantir o tempo de funcionamento e a recuperação de falhas ou incidentes.	Cópias de segurança do EPP e configuração do EPP relacionadas com a disponibilidade.
PA-F-1	Ativo Funcional	Sistemas de Gestão de Domínios	Ferramentas e plataformas para gestão de atividades do ciclo de vida do domínio, incluindo a integração do EPP.	Software e configuração do servidor EPP, ferramentas de cliente EPP
PA-F-2	Ativo Funcional	Infraestrutura DNS	Servidores DNS autoritativos e recursivos para resolução de domínios.	N/A
PA-F-3	Ativo Funcional	Plataformas de Interação com Registrars	Portais Web, API e aplicações móveis para acesso dos registrars à gestão de domínios e DNS, Portal de Apoio aos Registrars	API externa EPP para interações com registrars
PA-F-4	Ativo Funcional	Monitorização e Sistemas	Sistemas para acompanhar o desempenho, a disponibilidade e as métricas de DNS, incluindo firewalls, IDS/IPS, concentradores de logs, soluções SAST e DAST.	Monitorização de servidores e transações EPP, como tempos de resposta, integração de registos EPP no SIEM (sem análise, que é abordada no PA-F-5)

ID	CATEGORIA DO ATIVO PRIMÁRIO	TÍTULO DO ATIVO PRIMÁRIO	DESCRIÇÃO DO ATIVO PRIMÁRIO	EXEMPLOS DE EPP
PA-F-5	Ativo Funcional	Sistemas de Análise e Gestão da Segurança	Ferramentas para proteção de sistemas e dados com base em informações provenientes de soluções relacionadas com o PA-F-4 e sistemas SIEM	Correlação de eventos EPP, p. ex., alerta de registo de aplicações específicas EPP
PA-F-6	Ativo Funcional	Sistemas de Gestão de Chaves	Sistemas para gerar, gerir e armazenar qualquer material criptográfico, como chaves (DNSSEC, SSL/ TLS, SSH, VPN)	O EPP utiliza a criptografia para garantir os objetivos de segurança informáticos. Pode ser um HSM, software criptográfico ou um sistema de cofre
PA-F-7	Ativo Funcional	Sistemas de Gestão de Identidade e Acesso (IAM)	Plataformas para controlar a autenticação e a autorização dos utilizadores.	Acesso baseado em funções para aplicações e sistemas EPP
PA-F-8	Ativo Funcional	Sistemas de Cópia de segurança e Recuperação	Ferramentas para salvaguardar e restaurar dados e configurações críticos.	Cópias de segurança de configurações e registos EPP
PA-F-9	Ativo Funcional	Ambientes de Desenvolvimento e Teste	Infraestrutura para criar, testar e implantar software e serviços.	Ferramentas de teste EPP e ambientes de desenvolvimento EPP
PA-I-1	Ativo de Informação	Dados e Credenciais do Cliente	Informações do registrant, credenciais de autenticação e dados de titularidade do domínio.	Dados transacionais do EPP e detalhes do registrant, chaves e credenciais criptográficas relacionadas com o EPP
PA-I-2	Ativo de Informação	Registos de Domínios e DNS	Ficheiros de zona, registos DNS e configurações específicas do domínio.	N/A
PA-I-3	Ativo de Informação	Registos Operacionais	Registos de transações EPP, consultas DNS e operações do sistema.	Registos de transações EPP
PA-I-4	Ativo de Informação	Políticas e Documentação de Conformidade	Políticas operacionais, acordos de serviços e documentos de conformidade regulamentar.	Políticas relacionadas com o EPP, p. ex., uma política para cumprir os requisitos de segurança das presentes diretrizes
PA-I-5	Ativo de Informação	Conhecimento Organizacional e Materiais de Formação	Guias internos, recursos de formação e melhores práticas operacionais.	Formação para sistemas EPP, guias de reforço da segurança informática e procedimentos operacionais relacionados com o EPP

4. Diretrizes EPP - Requisitos de Segurança

Este capítulo divide os requisitos de segurança nos seguintes domínios: Rede, Sistema Operativo, Autenticação, Autorização, Criptografia, EPP SSDLC e Monitorização da Segurança.

4.1 Infraestrutura de Rede

4.1.1 TLD-EPP-NET-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-NET-1
REQUISITO DE SEGURANÇA	Os componentes do EPP com funções diferentes DEVEM ser alojados numa zona da firewall dedicada.
TIPO	MUST/DEVE
RISCO	Um cibercriminoso pode conseguir aceder ou manipular dados sensíveis se os serviços EPP não estiverem suficientemente protegidos através da segregação da rede. Por exemplo, se vários serviços não relacionados com o EPP estiverem alojados com o ambiente EPP na mesma zona da firewall, o comprometimento de um desses serviços não relacionados com o EPP permite que um cibercriminoso contorne as restrições e tenha acesso direto à infraestrutura do EPP através da retransmissão do tráfego pela máquina comprometida.
RECOMENDAÇÃO	Qualquer acesso de redes não fiáveis a componentes EPP DEVE ser protegido por uma firewall. Os diferentes componentes do EPP com funções diferentes DEVEM ser separados, p. ex., a aplicação de faturação e as ferramentas de apoio personalizadas NÃO PODERIA estar na zona da infraestrutura do EPP. Para além disso, a zona da firewall do EPP de produção DEVE ser separada do ambiente de não produção. Qualquer serviço ou servidor que não seja necessário para a infraestrutura EPP NÃO PODERIA estar alojado numa zona da firewall relacionada com o EPP. Estas regras aplicam-se a cenários em nuvem, no local e híbridos. Em ambientes em nuvem e híbridos, as redes virtuais, as firewalls baseadas no host e as firewalls de aplicações Web PODEM ser utilizadas para cumprir as recomendações.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3, 3.2.1, 3.2.2, 3.2.3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	3.2.1, 3.2.2, 3.2.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	TH46

4.1.2 TLD-EPP-NET-2

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-NET-2
REQUISITOS DE SEGURANÇA	Os operadores de servidores PODERIAM tomar medidas para minimizar o impacto de um ataque de negação de serviço (DoS) utilizando combinações de soluções de proteção DoS, tais como implementação de tecnologia de firewall, reforço da pilha TCP e filtros de router de fronteira para restringir o acesso de entrada ao servidor a clientes conhecidos e de confiança.
TIPO	SHOULD/PODERIA
RISCO	Cibercriminosos podem efetuar ataques de negação de serviço no ambiente do EPP, afetando a disponibilidade dos serviços ccTLD. Os cibercriminosos tentam frequentemente atacar o elemento mais fraco de uma cadeia, investigando todos os vetores de ataque, como a rede, o sistema operativo e os pontos fracos ao nível da aplicação, para ataques de negação de serviço.
RECOMENDAÇÃO	Os ataques de negação de serviço são comuns. PODERIA avaliar as suas opções com base no seu cenário de alojamento, p. ex., no local, híbrido ou em nuvem. Cada componente PODERIA ser protegido. PODERIA avaliar firewalls, firewalls de aplicações Web e proxies inversos, filtragem BGP, filtragem de tráfego e reforço da pilha TCP. Se depender de um cenário em nuvem, PODERIA assegurar e validar que o seu fornecedor de nuvem (p. ex., IaaS, PaaS ou SaaS) dispõe de mecanismos de proteção contra a negação de serviço acima referidos.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	4.1.3, 4.2.4
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	TH02, TH05, TH06, TH07, TH25, TH31, TH32, TH34, TH37, TH38, TH39, TH41, TH43, TH44, TH47, TH50

4.2 Sistema Operativo

4.2.1 TLD-EPP-OS-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-OS-1
REQUISITO DE SEGURANÇA	O sistema operativo que aloja o serviço EPP DEVE ser seguro.
TIPO	MUST/DEVE
RISCO	Um cibercriminoso pode roubar informações sensíveis, modificar dados empresariais arbitrários ou perturbar processos empresariais relacionados com o EPP se os sistemas operativos da infraestruturo EPP não estiverem protegidos, o que irá resultar numa superfície de ataque maior. A título de exemplo, os componentes ou serviços desnecessários do sistema podem conter vulnerabilidades, estão expostos à rede ou são vulneráveis devido a definições de configuração inseguras.
RECOMENDAÇÃO	DEVE proteger o seu sistema operativo com base nas recomendações de segurança dos fornecedores de sistemas operativos ou dos CIS Benchmark (p. ex., https://www.cisecurity.org/cis-benchmarks)
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	2.2.2 (monitorização da conformidade)
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	TH02, TH03, TH14, TH26, TH38, TH46, TH47, TH49, TH50

4.3 Autenticação

4.3.1 TLD-EPP-AUTHE-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHE-1
REQUISITO DE SEGURANÇA	DEVE utilizar a autenticação forte mútua nas implementações EPP.
TIPO	MUST/DEVE
RISCO	Um cibercriminoso pode atacar a autenticação de fator único através de diferentes métodos, tais como força bruta, engenharia social, armazenamento de texto simples (p. ex., por administradores), reutilização de palavras-passe para diferentes serviços, credential dumping, malware ou phishing.
RECOMENDAÇÃO	Para ambientes EPP, a autenticação forte DEVE ser estabelecida utilizando, pelo menos, um dos seguintes métodos: • 1. O acesso ao EPP PODERIA utilizar listas de permissões de IP ponto a ponto que restringem o acesso a clientes e parceiros conhecidos, combinadas com uma palavra-passe (TLD-EPP-AUTHE-4). Se utilizar esta opção, DEVE utilizar o EPP sobre TLS (TLD-EPP-CRYPTO-2) para assegurar que o servidor pode ser identificado pelo cliente com o objetivo de evitar ataques man-in-the-middle. • 2. Rede privada virtual (VPN) ponto a ponto utilizando um dispositivo de identificação criptográfica (p. ex., TPM) combinado com uma palavra-passe (TLD-EPP-AUTHE-4). Neste caso, certifique-se de que a sua configuração VPN impõe a autenticação mútua. • 3. Certificados de cliente combinados com uma palavra-passe (TLD-EPP-6). Se utilizar esta opção, DEVE utilizar o EPP sobre TLS (ver TLD-EPP-CRYPTO-2) para assegurar que o servidor pode ser identificado pelo cliente com o objetivo de evitar ataques man-in-the-middle. • 4. Qualquer utilização da autenticação NIST SP 800-63B Authenticator Assurance Level 2 (AAL2) ou superior também é suficiente. Se utilizar esta opção, DEVE utilizar o EPP sobre TLS (ver TLD-EPP-CRYPTO-2) para assegurar que o servidor pode ser identificado pelo cliente com o objetivo de evitar ataques man-in-the-middle. Nota: A BSI alemã apresenta a seguinte definição de “autenticação forte” [ver ligação]: *Autenticação forte* *Combinação de duas ou mais técnicas de autenticação - por exemplo, uma palavra-passe e um número de transação (palavra-passe de uso único) ou um cartão com chip. Por este motivo, a autenticação forte é também frequentemente designada por autenticação de dois fatores ou autenticação multifatorial.*
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.6, 1.7.1, 11.7.2
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	TH02, TH07, TH17, TH27, TH35, TH41

4.3.2 TLD-EPP-AUTHE-2

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHE-2
REQUISITO DE SEGURANÇA	Qualquer cliente DEVE ser autenticado utilizando o comando EPP <login> antes de estabelecer uma sessão EPP
TIPO	MUST/DEVE
RISCO	Um cibercriminoso pode executar comandos arbitrários se não for necessário realiza a autenticação dos utilizadores.
RECOMENDAÇÃO	DEVE garantir que a sua aplicação EPP fornece um mecanismo de autenticação através de nome de utilizador e palavra-passe na camada EPP, ver RFC 5730, secção 2.9.1.1. A autenticação DEVE ocorrer antes de se poderem executar quaisquer operações EPP.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-3, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.1.2.(c). 11.6.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.3.3 TLD-EPP-AUTHE-3

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHE-3
REQUISITO DE SEGURANÇA	DEVE aplicar regras de palavra-passe (p. ex., comprimento mais curto com elevada complexidade ou comprimento longo com menor complexidade) para as palavras-passe relacionadas com o EPP
TIPO	MUST/DEVE
RISCO	Se uma palavra-passe tiver uma complexidade insuficiente, pode ser espiada através de força bruta; tal pode ocorrer remotamente, adivinhando palavras-passe fracas, ou se o sistema for comprometido através de outra vulnerabilidade, atacando hashes de palavras-passe. Por exemplo, as palavras-passe com 6 caracteres podem ser quebradas instantaneamente e as palavras-passe com até 8 caracteres podem demorar menos de um minuto.
RECOMENDAÇÃO	DEVE aplicar, pelo menos, a política de palavras-passe da sua empresa na implementação e infraestrutura do protocolo EPP. PODERIA avaliar se a complexidade com maior entropia é imposta, uma vez que, por norma, o EPP é utilizado na comunicação máquina-a-máquina. A título de exemplo, a BSI alemã fornece a seguinte recomendação de melhores práticas: *12 caracteres de 4 tipos diferentes (minúsculas, maiúsculas, números, caracteres especiais) ou 25 caracteres com pelo menos 2 tipos diferentes (p. ex., minúsculas e especiais) - p. ex., isto permite concatenar 6 palavras separadas por um caracter especial (ver ligação).*
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-3, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.6.1, 11.6.2, 11.6.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.3.4 TLD-EPP-AUTHE-4

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHE-4
REQUISITO DE SEGURANÇA	O identificador de um cliente com uma palavra-passe inicial segura e aleatória DEVE ser criado no servidor antes de um cliente poder concluir com êxito um comando <login>.
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem facilmente reutilizar as palavras-passe predefinidas ou calcular palavras-passe geradas de forma fraca e previsível, como "Init1234" ou "$client-welcome-$clientid", etc.
RECOMENDAÇÃO	Utilizar uma palavra-passe inicial para autenticação, a qual DEVE ser protegida por geração aleatoriamente e com entropia suficiente. Um cliente DEVE alterar a palavra-passe inicial fornecida, mesmo num cenário de comunicação máquina-a-máquina. Tal PODE exigir o desenvolvimento de um serviço adicional de alteração de palavra-passe se a sua implementação EPP não o oferecer. Uma boa prática seria: um cliente obtém uma conta de utilizador geral numa interface Web onde pode gerir os seus tokens de acesso. Essa página de gestão pode ser utilizada para fornecer uma palavra-passe gerada aleatoriamente para a comunicação EPP.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-3, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.6.1, 11.6.2, 11.6.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.3.5 TLD-EPP-AUTHE-5

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHE-5
REQUISITO DE SEGURANÇA	Deve limitar o número de tentativas falhadas de início de sessão com palavra-passe EPP.
TIPO	SHOULD/PODERIA
RISCO	Cibercriminosos podem aplicar força bruta às credenciais das contas de utilizador, o que lhes permitiria aumentar os seus privilégios e comprometer a conta atacada.
RECOMENDAÇÃO	PODERIA limitar a quantidade de tentativas de início de sessão falhadas por um período de tempo definido. DEVE bloquear permanente ou temporariamente as contas de utilizador com demasiadas tentativas de início de sessão falhadas. A título de exemplo, pode definir para a sua implementação EPP que em 5 minutos não pode haver mais de 5 tentativas falhadas. Considera-se aceitável desbloquear contas após um período de tempo definido (p. ex., 24 horas) caso existam mecanismos de registo adicionais para detetar tentativas contínuas de início de sessão falhadas (por exemplo, SIEM TLD-EPP-16).
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-3, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.6.2.(d), 11.6.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.4 Autorização

4.4.1 TLD-EPP-AUTHO-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHO-1
REQUISITO DE SEGURANÇA	DEVE ser criada uma política de controlo do acesso para todos os componentes relacionados com o EPP. Esta política deve abranger o acesso e as autorizações para os clientes EPP e DEVE ser revista e atualizada regularmente, conforme necessário, com base em incidentes, riscos ou alterações operacionais.
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem conseguir um acesso não autorizado a sistemas relacionados com o EPP ou aumentar os seus privilégios.
RECOMENDAÇÃO	DEVE elaborar uma política de controlo do acesso que abranja cada comando EPP (p. ex., consulta, transferência, etc.). Esta política PODERIA ser revista e atualizada pelo menos uma vez por ano.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	6 .7.7.2.(b) + (c)
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.4.2 TLD-EPP-AUTHO-2

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-AUTHO-2
REQUISITO DE SEGURANÇA	Os registries DEVEM implementar autorizações no seu ambiente EPP para restringir operações de leitura e/ou de escrita relacionadas com o EPP relativas à “criação de objetos de domínio”, “transferência”, “consulta” e “objeto de contacto”, limitando o acesso dos clientes EPP aos seus próprios dados e carteira.
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem conseguir aumentar os seus privilégios e efetuar operações relacionadas com o EPP sem autorização.
RECOMENDAÇÃO	DEVE aplicar a sua política de controlo do acesso desenvolvida (TLD-EPP-SDLC-1) no seu ambiente EPP. O seu ambiente de implementação do EPP DEVE aplicar os controlos de autorização. PODE tratar as verificações de autorização num backend diferente, desde que não possam ser contornadas. A sua implementação do EPP DEVE garantir que qualquer cliente EPP só pode alterar os seus próprios dados e carteira.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-3, PA-I-1
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	11.1.2.(c) & 11.2.2.(a)
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.5 Criptografia

4.5.1 TLD-EPP-CRYPTO-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-CRYPTO-1
REQUISITO DE SEGURANÇA	Os registries DEVEM implementar e aplicar políticas criptográficas sólidas baseadas na classificação de ativos que garantam a adoção de protocolos e a aprovação de algoritmos criptográficos permitidos, força de cifra, soluções criptográficas e práticas de utilização (p. ex., manuseamento de certificados e tempo de vida). As políticas devem ser revistas regularmente para incorporar os últimos avanços criptográficos.
TIPO	SHOULD/PODERIA
RISCO	Cibercriminosos podem obter ou modificar dados sensíveis em trânsito ou em repouso, o que pode resultar no comprometimento total do sistema. Alguns exemplos desses tipos de ataque a soluções criptográficas são ataques man-in-the-middle, ataques de repetição, ataques de canal lateral, ataques de chave e algoritmo, ataques de dicionário e ataques de força bruta.
RECOMENDAÇÃO	O PCI-DSS define a criptografia forte da seguinte forma no seu glossário padrão (https://www.pcisecuritystandards.org/glossary/): *Criptografia Forte:* *A criptografia é um método usado para proteger dados através de um processo de encriptação reversível e é um primitivo fundamental utilizado em muitos protocolos e serviços de segurança. A criptografia forte baseia-se em algoritmos testados e aceites pela indústria, juntamente com comprimentos de chave que fornecem um mínimo de 112 bits de força de chave efetiva e práticas adequadas de gestão de chaves.* *A força efetiva da chave pode ser menor do que o comprimento real em "bits" da chave, o que pode levar a que os algoritmos com chaves maiores ofereçam menor proteção do que os algoritmos com chaves reais mais pequenas, mas com tamanhos efetivos maiores. Recomenda-se que todas as novas implementações utilizem um mínimo de 128 bits de força de chave efetiva.* *Exemplos de referências da indústria sobre algoritmos criptográficos e comprimentos de chave incluem:* *NIST Special Publication 800-57 Part 1,* *BSI TR-02102-1,* *ECRYPT-CSA D5.4 Algoritmos, Tamanho de Chave e Relatórios de Protocolos (2018), e* *ISO/IEC 18033 Algoritmos de Encriptação, e* *ISO/IEC 14888-3:2-81 Técnicas de Segurança Informática – Assinaturas digitais com anexo – Parte 3: Mecanismos baseados em algoritmos discretos.* DEVE desenvolver políticas criptográficas que abranjam a utilização segura da criptografia (ver Anexo 9.1.2 da NIS2). A utilização de algoritmos de encriptação e de modos de cifra é frequentemente regulamentada pela administração local. Por conseguinte, o utilizador PODERIA incorporar os requisitos do seu governo como base, caso contrário, PODERIA basear-se nas referências mais recentes da indústria para elaborar a sua política.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	9.1.1, 9.1.2, 9.1.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.5.2 TLD-EPP-CRYPTO-2

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-CRYPTO-2
REQUISITO DE SEGURANÇA	Os dados em trânsito DEVEM ser protegidos utilizando encriptação na camada de transporte ou de aplicação acima da camada de protocolo EPP. PODERIA implementar o EPP sobre TLS ou uma VPN ponto-a-ponto.
TIPO	MUST/DEVE
RISCO	Piratas informáticos podem roubar as informações através de escutas (p. ex., ARP-spoofing ou interceção de credenciais numa rede Wi-Fi pública) se se enviarem informações sensíveis sem encriptação como palavras-passe ou dados pessoais. As contas comprometidas permitiriam maiores privilégios, falsificação de comandos e injeções de comandos relacionadas com o EPP no contexto da conta da vítima.
RECOMENDAÇÃO	DEVE utilizar uma camada de encriptação ao nível do transporte ou da aplicação acima da camada do protocolo EPP. PODERIA recorrer ao TLS ou a uma VPN ponto-a-ponto. PODE utilizar uma alternativa, mas DEVE então assegurar a integridade, a confidencialidade e a autenticação mútua forte cliente-servidor na sua camada de encriptação (ver TLD-EPP-2). Referência da RFC 5730 (sec. 7): "As instâncias EPP DEVEM ser protegidas utilizando um mecanismo de transporte ou protocolo de aplicação que forneça integridade, confidencialidade e autenticação forte mútua cliente-servidor."
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	6.7.2.(i)
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.5.3 TLD-EPP-CRYPTO-3

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-CRYPTO-3
REQUISITO DE SEGURANÇA	A troca de informações de gestão relacionadas com a conta (p. ex., palavras-passe, certificados de cliente, tokens) DEVE utilizar um canal de comunicação fora de banda protegido adicional (p. ex., através de uma aplicação Web https).
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem conseguir intercetar credenciais se os canais de comunicação não estiverem protegidos, o que permitiria a um cibercriminoso comprometer contas relacionadas.
RECOMENDAÇÃO	Os certificados de cliente DEVEM ser gerados pelo cliente ou, se o certificado de cliente, incluindo a chave privada, for gerado pelo registry, a chave privada do certificado de cliente DEVE ser protegida com uma palavra-passe. Em ambos os casos, os certificados DEVEM ser trocados utilizando um canal de comunicação fora de banda, p. ex., através de https ou de um correio eletrónico encriptado (ver RFC 5734, secção 8). Por norma, os tokens de acesso são gerados no lado do servidor pelo registry e DEVEM ser protegidos por encriptação antes de serem enviados ao cliente.

	Tal como o serviço de alteração de palavra-passe descrito no TLD-AUTHE-4, este serviço também pode processar certificados de clientes ou fichas de acesso, cumprindo o requisito de segurança através da utilização de encriptação via https.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	9.1.1, 9.1.2, 9.1.3
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.6 EPP SSDLC

4.6.1 TLD-EPP-SSDLC-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-SSDLC-1
REQUISITO DE SEGURANÇA	DEVE garantir um ciclo de vida de desenvolvimento seguro da sua aplicação EPP (proteção contra vulnerabilidades de software)
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem abusar de vulnerabilidades de software em implementações EPP e código relacionado. As vulnerabilidades de software podem permitir que um cibercriminoso comprometa completamente o ambiente EPP de um TLD. A título de exemplo, em 2023, investigadores de segurança mostraram como um ataque XXE (injeção de entidade externa XML) a uma implementação do EPP resultou no comprometimento total de um TLD mais pequeno.
RECOMENDAÇÃO	A sua implementação do EPP será desenvolvida por si irá depender de uma implementação externa. Em ambos os casos, DEVE garantir a existência de um ciclo de vida de desenvolvimento seguro de software (p. ex., segurança da cadeia de fornecimento NIS2). DEVEM-se adotar medidas de segurança para evitar vulnerabilidades comuns do software, tanto no software desenvolvido pelo próprio como no software fornecido externamente. Exemplos: SSDLC, revisões de código e por pares, análise de código estático, testes de penetração e manutenção de um SBOM (p. ex., o Regulamento de Ciber-Resiliência da UE). O seu SSDLC PODERIA envolver uma componente de revisão manual (p. ex., revisão por pares ou auditoria de código). De notar que seria pouco provável que soluções de testes dinâmicos de segurança de aplicações (DAST) de fornecedores terceiros conseguissem descobrir vulnerabilidades específicas do EPP.
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3, PA-I-4, PA-I-5
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

4.7 Monitorização da segurança

4.7.1 TLD-EPP-MON-1

IDENTIFICAÇÃO DO REQUISITO	TLD-EPP-SSDLC-1
REQUISITO DE SEGURANÇA	A sua infraestrutura EPP DEVE fornecer registos de segurança. Estes registos PODERIAM ser transferidos e analisados num ambiente centralizado e separado de gestão de informações e eventos de segurança (SIEM).
TIPO	MUST/DEVE
RISCO	Cibercriminosos podem ocultar o seu ataque se os registos do servidor e da aplicação EPP não forem enviados para um ambiente SIEM de agregação de registos centralizado. Sem um ambiente de registo central, é difícil responder às ameaças em tempo real e, após um ataque, é muito provável que se demore a detetar um ataque ou que se detete, efetivamente, o referido ataque. Se o servidor for comprometido por um cibercriminoso, este poderá modificar ou eliminar os registos relacionados, impossibilitando a realização de uma investigação forense para compreender a causa e o impacto do ataque.
RECOMENDAÇÃO	DEVE garantir que o seu ambiente EPP está a gerar registos de aplicações relacionados com o protocolo EPP. Quando liga os seus servidores relacionados com o EPP a um ambiente SIEM, não é suficiente ligar apenas a camada do sistema operativo. Os registos de aplicações específicas do EPP PODERIAM também estar disponíveis. PODERIA desenvolver casos de utilização ou padrões específicos do EPP na sua solução SIEM/Centro de Operações de Segurança (SOC).
ATIVO (PA)	PA-BP-1, PA-BP-2, PA-BP-3, PA-BP-4, PA-BP-5, PA-F-1, PA-F-2, PA-F-3, PA-F-4, PA-F-5, PA-F-6, PA-F-7, PA-F-8, PA-F-9, PA-I-1, PA-I-2, PA-I-3, PA-I-4, PA-I-5
IDENTIFICAÇÃO DO OBJETIVO DE SEGURANÇA	3.2
IDENTIFICAÇÃO DA AMEAÇA TLD ISAC	Ligação às ameaças existentes identificadas no relatório do panorama de ameaças do TLD ISAC - o relatório pormenorizado apenas está disponível para membros do TLD ISAC.

EUROPEAN
TLD ISAC