



EUROPEAN
TLD ISAC

EPP Security Best Practices Guidelines

FOR EUROPEAN TLD OPERATORS

TLP:CLEAR



EPP SECURITY BEST PRACTICES GUIDELINES 2025

ABOUT THE EUROPEAN TLD ISAC

The European Top-Level Domain Information Sharing and Analysis Centre (European TLD ISAC) is a collaborative initiative dedicated to strengthening the cybersecurity posture of country code top-level domain (ccTLD) registries across Europe. It serves as a trusted platform for sharing threat intelligence, promoting best practices and fostering cooperation among ccTLD operators, security experts and other stakeholders. For more information: <https://www.tld-isac.eu>.

CONTACT

To contact the European TLD ISAC or for media enquiries about this report, please send an e-mail to info@tld-isac.eu.

LEGAL NOTICE

The European TLD ISAC is a special Working Group within CENTR ASBL/VZW. This publication represents the views and interpretations of CENTR. CENTR has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain CENTR and the European TLD ISAC as its source. Third-party sources are quoted as appropriate. CENTR is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither CENTR nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. CENTR maintains its intellectual property rights in relation to this publication.

Table of Contents

TABLE OF CONTENTS	3
1. LIST OF ABBREVIATIONS	4
2. INTRODUCTION	5
2.1 Scope	5
2.2 Target audience	6
2.3 Classification	6
2.4 Overview of the guideline development approach	6
2.5 How to read and work with these guidelines	6
3. CONVENTIONS	7
3.1 Keyword definitions (RFC2119)	7
3.2 Description of the security requirements' structure	7
3.3 Overview of TLD ISAC asset IDs	8
4. EPP GUIDELINES – SECURITY REQUIREMENTS	11
4.1 Network infrastructure	11
4.1.1 TLD-EPP-NET-1	11
4.1.2 TLD-EPP-NET-2	12
4.2 Operating system	13
4.2.1 TLD-EPP-OS-1	13
4.3 Authentication	14
4.3.1 TLD-EPP-AUTHE-1	14
4.3.2 TLD-EPP-AUTHE-2	15
4.3.3 TLD-EPP-AUTHE-3	15
4.3.4 TLD-EPP-AUTHE-4	16
4.3.5 TLD-EPP-AUTHE-5	16
4.4 Authorisation	17
4.4.1 TLD-EPP-AUTHO-1	17
4.4.2 TLD-EPP-AUTHO-2	17
4.5 Cryptography	18
4.5.1 TLD-EPP-CRYPTO-1	18
4.5.2 TLD-EPP-CRYPTO-2	19
4.5.3 TLD-EPP-CRYPTO-3	19
4.6 EPP SSDLC	20
4.6.1 TLD-EPP-SSDLC-1	20
4.7 Security monitoring	21
4.7.1 TLD-EPP-MON-1	21

1. List of abbreviations

ccTLD	Country Code Top-Level Domain (registry operator)
DAST	Dynamic Application Security Testing
DNS	Domain name system
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
EPP	Extensible Provisioning Protocol (EPP), an XML based text protocol.
IaaS	Infrastructure as a Service
IETF	Internet Engineering Task Force
PA	Primary Asset
PaaS	Platform as a Service
RFC	Request for Comments
SaaS	Software as a Service
SAST	Static Application Security Testing
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SSDLC	Secure Software Development Lifecycle
VPN	Virtual Private Network

2. Introduction

In January 2023, the “NIS2” Directive, (EU) 2022/2555¹ on measures for a high common level of cybersecurity across the Union), came into force. Under NIS2, the European Commission adopts implementing acts, which set out the technical and methodological requirements for cybersecurity risk management measures and contain technical and methodological rules as well as sector specific rules.

As part of its activities, the European TLD ISAC established an internal project to develop security best practices guidelines for environments of top-level domain (TLD) registry operators using the Extensible Provisioning Protocol (EPP). The initial EPP RFC 5730 was standardised in 2009 by the Internet Engineering Task Force (IETF). Since then, technology and the state of the art with respect to IT-security has continuously evolved resulting in additional security measures. Any vulnerability related to EPP implementations and their infrastructure have a direct impact on the related domain name system (DNS) infrastructure.

The idea behind a baseline is to define measurements that should be considered basic and that there should not be any further alignment or risk analysis necessary. You should just apply them. In addition, you should apply additional individual security measures to your EPP environment.

2.1 Scope

In scope

The purpose of this document is to provide guidelines for EPP security best practices and security recommendations to be adopted by TLD registries. All provided security recommendations are described in a generic way and are intended to be adopted by the TLD operators and integrated into their IT policy frameworks.

Out of scope

This document provides EPP-specific security recommendations – it does not provide a comprehensive and complete list of security requirements to protect an entire organisation. NIS2 and other local laws must be considered separately.

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

2.2 Target audience

The primary target group of these EPP security guidelines are people related to TLD registries and registrars who are within the following groups:

- CISOs
- Admins & Developers
- Auditors

2.3 Classification

These guidelines are public and classified as TLP:CLEAR.

2.4 Overview of the guideline development approach

TLD ISAC project team was tasked with developing a security baseline specific to EPP in the form of guidelines. The project team worked closely with the TLD ISAC community to identify and document a set of mutually agreed norms which registry operators of any size should implement. These norms support operating a secure EPP infrastructure. After drafting the guidelines and a final feedback round, the guidelines were validated in a test environment and then finalised.

2.5 How to read and work with these guidelines

In order to use these guidelines effectively, we suggest starting with chapters “3.1 Keyword definitions (RFC2119)”, “3.2 Description of the security requirements’ structure”, “3.3 Overview of TLD ISAC asset IDs” and then reviewing chapter “4 EPP Guidelines – Security Requirements”.

In a next step, we recommend integrating these guidelines into your existing IT security policy framework. Lastly, evaluate if you can set up automatic controls that continually monitor your infrastructure for misconfigurations and violations against these guidelines (e.g., in case someone deactivates strong authentication).

3. Conventions

3.1 Keyword definitions (RFC2119)

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [\[RFC2119\]](#).

3.2 Description of the security requirements' structure

Each section provides an overview of EPP-related security requirements and acts as a guideline for recommended tasks how to secure EPP-related environments.

For each requirement the following structure is used:

ELEMENT	ELEMENT
REQUIREMENT ID	A unique identifier using the following naming convention: TLD-EPP-<Area>-<Incremented-Digits>
SECURITY REQUIREMENT	A description of the security requirement.
TYPE	The type of security requirement in alignment with the conventions (see RFC2119 and section “Conventions”), e.g. “MUST”, “SHOULD”, etc.
RISK	A description of risks if the requirement is not or only partially fulfilled
RECOMMENDATION	A practical recommendation
ASSET (PA)	A link to the TLD ISAC Asset ID (see section 3.3) with a focus to EPP impact
SECURITY OBJECTIVE ID	A reference to related IDs of the “NIS2 Directive – Commission implementing Regulation C(2024) 7151 – ANNEX” (see https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks). Fulfilling the EPP security requirement does not imply that all referenced Security Objective IDs from NIS2 are fully addressed.
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

3.3 Overview of TLD ISAC asset IDs

NIS2 requires organisations to perform risk assessments. If you are a registry or registrar entity within the scope of NIS2 you will have to perform risk assessments. As risk assessments typically use an asset-based approach, we decided to map each security requirement against a primary asset (PA). Unfortunately, every organisation may have a different definition and classification of their information security related assets. Therefore, we decided to use the definition for primary asset by the European Union Agency for Cybersecurity (ENISA) as shown in the document "[METHODODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS September 2021](#)" on page 15, whereas primary assets are defined as:

Primary assets

- Business processes & activities
- Functional assets
- Information assets

To have a common asset structure we provide an exemplary TLD primary asset categorisation. This can be taken as a starting point depending on the maturity of your asset management. Your own organisation may have additional or different categories, therefore feel free to adopt the list to your own needs. As a reminder, this document aims to provide EPP-specific security requirements. Therefore not all provided primary asset IDs are mapped to a security requirement.

Explanation of columns

- ID: Unique ID with the following structure:
- PA-<two digit PA category (BP,FA,I)>-<digit>
- Primary Asset Category: Indicates whether the asset is a Business Process, Functional Asset, or Information Asset (see ENISA definition)
- Primary Asset Title and Description: The asset name and a brief description (e.g., its role in the domain registrar's operations)
- EPP Examples: Specific EPP-related examples for each primary asset, where applicable. Otherwise filled with "N/A".

ID	PRIMARY ASSET CATEGORY	PRIMARY ASSET TITLE	PRIMARY ASSET DESCRIPTION	EPP EXAMPLES
PA-BP-1	Business Process	Domain Registration Process	The process of provisioning, updating, transferring, and renewing domains.	EPP commands for domain create, update, transfer, and delete
PA-BP-2	Business Process	Billing and Payment Process	The process for generating invoices, processing payments, and managing financial transactions.	EPP transaction logs for billing
PA-BP-3	Business Process	Customer Support and Service Process	Handling customer inquiries, troubleshooting, and managing interactions.	EPP API logs for troubleshooting
PA-BP-4	Business Process	Compliance and Regulatory Management Process	Ensuring adherence to NIS2, GDPR, and other regulatory and compliance requirements.	EPP-related IT security processes (e.g., establish a secure software development lifecycle for your EPP environment, or conducting risk assessment for your EPP environment)
PA-BP-5	Business Process	Business Continuity and Disaster Recovery Process	Strategies and actions to ensure uptime and recovery from failures or incidents.	EPP backups and EPP configuration related to availability.
PA-F-1	Functional Asset	Domain Management Systems	Tools and platforms for managing domain lifecycle activities, including EPP integration.	EPP server software & configuration, EPP client tools
PA-F-2	Functional Asset	DNS Infrastructure	Authoritative and recursive DNS servers for domain resolution.	N/A
PA-F-3	Functional Asset	Registrar Interaction Platforms	Web portals, APIs, and mobile apps for registrar access to domain and DNS management, Registrar Support Portal	EPP external API for registrar interactions
PA-F-4	Functional Asset	Monitoring and Systems	Systems for tracking performance, availability, and DNS metrics, including firewalls, IDS/IPS, log concentrators, SAST and DAST solutions.	Monitoring of EPP servers and transactions, like response times, EPP log integration into SIEM (without analytics that is covered in PA-F-5)

ID	PRIMARY ASSET CATEGORY	PRIMARY ASSET TITLE	PRIMARY ASSET DESCRIPTION	EPP EXAMPLES
PA-F-5	Functional Asset	Security Analytics and Management Systems	Tools for protecting systems and data based on input from PA-F-4 related solutions and SIEM systems	Correlating EPP events, e.g., EPP specific application log alerting
PA-F-6	Functional Asset	Key Management Systems	Systems for generating, managing, and storing any cryptographic material like keys (DNSSEC, SSL/TLS, SSH, VPN)	EPP uses cryptography to ensure IT security goals. Can be an HSM, cryptographic software or a vault system
PA-F-7	Functional Asset	Identity and Access Management Systems (IAM)	Platforms for controlling user authentication and authorisation.	Role-based access for EPP applications and systems
PA-F-8	Functional Asset	Backup and Recovery Systems	Tools for safeguarding and restoring critical data and configurations.	Backups of EPP configurations and logs
PA-F-9	Functional Asset	Development and Testing Environments	Infrastructure for building, testing, and deploying software and services.	EPP testing tools and EPP develop environments
PA-I-1	Information Asset	Customer Data and Credentials	Registrant information, authentication credentials, and domain ownership data.	EPP transactional data and registrant details, EPP related cryptographic keys and credentials
PA-I-2	Information Asset	Domain and DNS Records	Zone files, DNS records, and domain-specific configurations.	N/A
PA-I-3	Information Asset	Operational Logs	Logs from EPP transactions, DNS queries, and system operations.	EPP transaction logs
PA-I-4	Information Asset	Policies and Compliance Documentation	Operational policies, service agreements, and regulatory compliance documents.	EPP related policies, e.g. a policy to fulfil the security requirements in these guidelines
PA-I-5	Information Asset	Organisational Knowledge and Training Materials	Internal guides, training resources, and operational best practices.	Training for EPP systems, IT security hardening guides and EPP related operating procedures

4. EPP Guidelines – Security Requirements

This chapter divides the security requirements into the following areas: Network, Operating System, Authentication, Authorisation, Cryptography, EPP SSDLC and Security Monitoring.

4.1 Network infrastructure

4.1.1 TLD-EPP-NET-1

REQUIREMENT ID	TLD-EPP-NET-1
SECURITY REQUIREMENT	EPP components with different functions MUST each be hosted in a dedicated firewall zone .
TYPE	MUST
RISK	An attacker may be able to access or manipulate sensitive data if the EPP services are not sufficiently protected through network segregation. E. g., if multiple non EPP-related services are hosted with the EPP environment in the same firewall zone, then a compromise of one of these non EPP services allows an attacker to bypass restrictions and have direct access to the EPP infrastructure through relaying traffic across the compromised machine.
RECOMMENDATION	Any access from untrusted networks to EPP components MUST be protected by a firewall. Different EPP components with different functions MUST be separated, e. g., the billing application and custom support tools SHOULD NOT be in the EPP infrastructure zone. And in addition, the production EPP firewall zone MUST be separated from the non-production environment. Any service or server that is not required for the EPP infrastructure SHOULD NOT be hosted in an EPP-related firewall zone. These rules apply for cloud, on-premise and hybrid scenarios. In cloud and hybrid environments virtual networks, host-based firewalls, and web application firewalls MAY be used to fulfil the recommendations.
ASSET (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
SECURITY OBJECTIVE ID	3.2.1, 3.2.2, 3.2.3
TLD ISAC THREAT ID	TH46

4.1.2 TLD-EPP-NET-2

REQUIREMENT ID	TLD-EPP-NET-2
SECURITY REQUIREMENT	Server operators SHOULD take steps to minimise the impact of a denial-of-service (DoS) attack using combinations of DoS protection solutions, such as deployment of firewall technology, TCP-stack-hardening, and border router filters to restrict inbound server access to known and trusted clients.
TYPE	SHOULD
RISK	Attackers could perform denial-of-service attacks on the EPP environment affecting the availability of the ccTLD services. Attackers often try to attack the weakest element of a chain and will therefore investigate all attack vectors such as network, operating system, and application-level weaknesses for denial-of-service attacks.
RECOMMENDATION	Denial-of-service attacks are common. You SHOULD evaluate your options based on your hosting scenario, e. g., on-premise, hybrid, or cloud. Each component SHOULD be protected. You SHOULD evaluate firewalls, web-application-firewalls and reverse-proxies, BGP filtering, traffic-scrubbing, and TCP-stack hardening. If you rely on a cloud scenario you SHOULD ensure and validate that your cloud provider (e. g., IaaS, PaaS, or SaaS) has the aforementioned denial-of-service protection mechanisms in place.
ASSET (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
SECURITY OBJECTIVE ID	4.1.3, 4.2.4
TLD ISAC THREAT ID	TH02, TH05, TH06, TH07, TH25, TH31, TH32, TH34, TH37, TH38, TH39, TH41, TH43, TH44, TH47, TH50

4.2 Operating system

4.2.1 TLD-EPP-OS-1

REQUIREMENT ID	TLD-EPP-OS-1
SECURITY REQUIREMENT	The operating system hosting the EPP service MUST be secured.
TYPE	MUST
RISK	An attacker may steal sensitive information, modify arbitrary business data, or disrupt EPP-related business processes if the operating systems of the EPP infrastructure are not secured. This will result in an increased attack surface. As an example, unnecessary system components or services may contain vulnerabilities, are exposed to the network, or are vulnerable due to insecure configuration settings.
RECOMMENDATION	You MUST secure your operating system based on the operating system vendors security recommendations or the CIS Benchmark (e.g., https://www.cisecurity.org/cis-benchmarks)
ASSET (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
SECURITY OBJECTIVE ID	2.2.2 (compliance monitoring)
TLD ISAC THREAT ID	TH02, TH03, TH14, TH26, TH38, TH46, TH47, TH49, TH50

4.3 Authentication

4.3.1 TLD-EPP-AUTHE-1

REQUIREMENT ID	TLD-EPP-AUTHE-1
SECURITY REQUIREMENT	You MUST use mutual strong authentication in EPP implementations.
TYPE	MUST
RISK	An attacker may attack single-factor authentication through different methods, such as brute-force, social engineering, plain-text-storage (e.g., by admins), password reuse for different services, credential dumping, malware, or phishing.
RECOMMENDATION	<p>For EPP environments, strong authentication MUST be established by at least one of the following methods:</p> <ul style="list-style-type: none">• 1. Access to EPP landscape SHOULD use point to point IP allow lists restricting access to known clients, customers, and partners combined with a password (TLD-EPP-AUTHE-4). If you use this option, you MUST use EPP over TLS (TLD-EPP-CRYPTO-2) to ensure that the server can be identified by the client for the purpose of avoiding man-in-the-middle attacks.• 2. Point to point virtual private network (VPN) using a cryptographic identification device (e.g., TPM) combined with a password (TLD-EPP-AUTHE-4). In this case ensure that your VPN configuration enforces mutual authentication.• 3. Client Certificates combined with a password (TLD-EPP-6). If you use this option, you MUST use EPP over TLS (see TLD-EPP-CRYPTO-2) to ensure that the server can be identified by the client for the purpose of avoiding man-in-the-middle attacks.• 4. Any use of NIST SP 800-63B Authenticator Assurance Level 2 (AAL2) or higher authentication is also sufficient. If you use this option you MUST use EPP over TLS (see TLD-EPP-CRYPTO-2) to ensure that the server can be identified by the client for the purpose of avoiding man-in-the-middle attacks. <p>Remark: The German BSI defines "Strong authentication" [see link] as follows:</p> <p><i>Strong authentication</i></p> <p><i>Strong authentication refers to the combination of two or more authentication techniques – for example, a password plus a transaction number (a one-time password) or a chip card. For this reason, strong authentication is also often referred to as two-factor or multi-factor authentication.</i></p>
ASSET (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
SECURITY OBJECTIVE ID	11.6, 1.7.1, 11.7.2
TLD ISAC THREAT ID	TH02, TH07, TH17, TH27, TH35, TH41

4.3.2 TLD-EPP-AUTHE-2

REQUIREMENT ID	TLD-EPP-AUTHE-2
SECURITY REQUIREMENT	Any client MUST be authenticated using the EPP <login> command before establishing an EPP session
TYPE	MUST
RISK	An attacker can perform arbitrary commands if no authentication of users is in place.
RECOMMENDATION	You MUST ensure that your EPP implementation provides a mechanism to authenticate via username and password on the EPP layer, see RFC 5730 section 2.9.1.1 . The authentication MUST happen before any EPP operations can be executed.
ASSET (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
SECURITY OBJECTIVE ID	11.1.2.(c). 11.6.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.3.3 TLD-EPP-AUTHE-3

REQUIREMENT ID	TLD-EPP-AUTHE-3
SECURITY REQUIREMENT	You MUST enforce password rules (e.g., either shorter length with high complexity or long length with less complexity) for EPP related passwords
TYPE	MUST
RISK	If a password has insufficient complexity, it may be spied out through brute-force. This may occur either remotely by guessing weak passwords or if the system is compromised through another vulnerability by attacking password hashes. E.g., passwords of 6 characters can be broken instantly, and up to 8 characters may take less than a minute.
RECOMMENDATION	<p>You MUST enforce at least your corporate password policy in your EPP protocol implementation and infrastructure. You SHOULD evaluate if complexity with higher entropy is enforced since EPP is typically used in machine-to-machine communication.</p> <p>As an example, the German BSI provides the following best practice recommendation:</p> <p><i>Either 12 characters of 4 different character types (small, capital, numbers, special chars) or 25 characters with at least 2 different types (e.g., small and specials) – e.g., this allows concatenating 6 words separated by a special character (see link).</i></p>
ASSET (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
SECURITY OBJECTIVE ID	11.6.1, 11.6.2, 11.6.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.3.4 TLD-EPP-AUTHE-4

REQUIREMENT ID	TLD-EPP-AUTHE-4
SECURITY REQUIREMENT	A client identifier with a secure and random initial password MUST be created on the server before a client can successfully complete a <login> command.
TYPE	MUST
RISK	Attackers can easily reuse default passwords or calculate weakly and predictable generated passwords such as "Init1234" or "\$client-welcome-\$clientid", etc.
RECOMMENDATION	An initial password is used for authentication and MUST be protected by generating it randomly and with sufficient entropy. A client or customer MUST change the provided initial password even in a machine-to-machine communication scenario. This MAY require you to develop an additional password change service if your EPP implementation does not offer this. A best practice would be: A client obtains a general user account in a web interface where he can manage his access tokens. That management page can then be used to provide a randomly generated password for the EPP communication.
ASSET (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
SECURITY OBJECTIVE ID	11.6.1, 11.6.2, 11.6.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.3.5 TLD-EPP-AUTHE-5

REQUIREMENT ID	TLD-EPP-AUTHE-5
SECURITY REQUIREMENT	You should limit the amount of failed EPP password login attempts.
TYPE	SHOULD
RISK	Attackers could brute force credentials of user accounts which would allow them to escalate their privileges and compromise the attacked account.
RECOMMENDATION	You SHOULD limit the amount of failed login attempts per a defined timeframe. You MUST either permanently or temporarily lock user accounts with too many failed login attempts. You could define for your EPP implementation, e. g., that in 5 minutes there cannot be more than 5 failed attempts. It is considered acceptable to unlock accounts after a defined timeframe (e. g., 24h), if additional logging mechanisms are in place to detect continuous failed login attempts (e. g., TLD-EPP-16 SIEM).
ASSET (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
SECURITY OBJECTIVE ID	11.6.2.(d), 11.6.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.4 Authorisation

4.4.1 TLD-EPP-AUTHO-1

REQUIREMENT ID	TLD-EPP-AUTHO-1
SECURITY REQUIREMENT	An access control policy for all EPP-related components MUST be created. This policy should cover access and authorisations for EPP clients and MUST be regularly reviewed and updated as needed based on incidents, risks or operational changes.
TYPE	MUST
RISK	Attackers may be able to get unauthorised access to EPP-related systems or elevate their privileges.
RECOMMENDATION	You MUST develop an access control policy that covers each EPP command (e.g., query, transfer, etc.). You SHOULD review and update this policy at least annually.
ASSET (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
SECURITY OBJECTIVE ID	6 .7.2.(b) + (c)
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.4.2 TLD-EPP-AUTHO-2

REQUIREMENT ID	TLD-EPP-AUTHO-2
SECURITY REQUIREMENT	Registries MUST implement authorisations in their EPP environment to restrict EPP-related read and/or write operation actions related to "creation of domain objects", "transfer", "query", and "contact object" limiting access for EPP clients to their own data and portfolio.
TYPE	MUST
RISK	Attackers may be able to elevate their privileges and conduct EPP related operations without authorisation.
RECOMMENDATION	You MUST enforce your developed access control policy (TLD-EPP-SDLC-1) in your EPP environment. Your EPP implementation environment MUST enforce the authorisation checks. You MAY handle authorisation checks in a different backend as long as they cannot be bypassed. Your EPP implementation MUST ensure that any EPP client is able to alter their own data and portfolio only.
ASSET (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
SECURITY OBJECTIVE ID	11.1.2.(c) & 11.2.2.(a)
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.5 Cryptography

4.5.1 TLD-EPP-CRYPTO-1

REQUIREMENT ID	TLD-EPP-CRYPTO-1
SECURITY REQUIREMENT	Registries MUST implement and enforce strong cryptographic policies based on the classification of assets that ensure the adoption of protocols, and the approval of allowed cryptographic algorithms, cipher strength, cryptographic solutions and usage practices (e.g., certificate handling and lifetime). The policies must be regularly reviewed to incorporate the latest advancements in cryptography.
TYPE	SHOULD
RISK	Attackers may obtain or modify sensitive data in transit or at rest, which can result in a complete system compromise. Some examples for those attack types on cryptographic solutions are man-in-the-middle attacks, replay attacks, side-channel attacks, key and algorithm attacks, dictionary attacks, and brute force attacks.
RECOMMENDATION	<p>PCI-DSS defines Strong Cryptography as follows in their standard glossary (https://www.pcisecuritystandards.org/glossary/):</p> <p><i>Strong Cryptography:</i> <i>Cryptography is a method to protect data through a reversible encryption process, and is a foundational primitive used in many security protocols and services. Strong cryptography is based on industry-tested and accepted algorithms along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices.</i></p> <p><i>Effective key strength can be shorter than the actual 'bit' length of the key, which can lead to algorithms with larger keys providing lesser protection than algorithms with smaller actual, but larger effective, key sizes. It is recommended that all new implementations use a minimum of 128-bits of effective key strength.</i></p> <p><i>Examples of industry references on cryptographic algorithms and key lengths include:</i></p> <p><i>NIST Special Publication 800-57 Part 1,</i> <i>BSI TR-02102-1,</i> <i>ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018),</i> <i>and</i> <i>ISO/IEC 18033 Encryption algorithms, and</i> <i>ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.</i></p> <p>You MUST develop cryptographic policies that cover the secure usage of cryptography (see NIS2 Annex 9.1.2). The usage of encryption algorithms and cipher modes is often regulated by your local government. Therefore, you SHOULD incorporate your government's requirements as a baseline, otherwise you SHOULD rely on the latest industry references to build your policy.</p>
ASSET (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
SECURITY OBJECTIVE ID	9.1.1, 9.1.2, 9.1.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.5.2 TLD-EPP-CRYPTO-2

REQUIREMENT ID	TLD-EPP-CRYPTO-2
SECURITY REQUIREMENT	Data in transit MUST be protected using encryption on the transport or application layer above the EPP protocol layer. You SHOULD implement EPP over TLS or a point-to-point VPN.
TYPE	MUST
RISK	An attacker could steal the information through eavesdropping (e.g., ARP-spoofing or intercepting credentials in a public Wi-Fi) if sensitive information like passwords or personal data are sent unencrypted. Compromised accounts would allow an elevation of privileges, command forgery, and EPP related command injections in the context of the victim's account.
RECOMMENDATION	<p>You MUST use an encryption layer on transport or application level above the EPP protocol layer. You SHOULD rely either on TLS or on a point-to-point VPN. You MAY use an alternative, but you MUST then ensure integrity, confidentiality, and mutual, strong client-server authentication in your encryption layer (see TLD-EPP-2).</p> <p>Reference from RFC 5730 (sec. 7): "EPP instances MUST be protected using a transport mechanism or application protocol that provides integrity, confidentiality, and mutual strong client-server authentication."</p>
ASSET (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
SECURITY OBJECTIVE ID	6.7.2.(i)
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.5.3 TLD-EPP-CRYPTO-3

REQUIREMENT ID	TLD-EPP-CRYPTO-3
SECURITY REQUIREMENT	The exchange of account-related management information (e.g., passwords, client certificates, tokens) MUST use an additional secured out-of-band communication channel (e.g., via an https web application).
TYPE	MUST
RISK	Attackers may be able to intercept credentials if communication channels are not protected. This would allow an attacker to compromise related accounts.
RECOMMENDATION	<p>Client certificates MUST either be generated by the client, or if the client certificate including the private key is generated by the registry, then the private key of the client certificate MUST be protected with a password. In both cases, the certificates MUST be exchanged using an out-of-band communication channel, e.g., via https or via an encrypted mail (see RFC 5734 section 8).</p> <p>Access tokens are typically generated on the server side by the registry and MUST be protected using encryption before sending them to the customer.</p>

Similarly to the password change service described in TLD-AUTHE-4, this service could also handle client certificates or access tokens, which fulfils the security requirement through using encryption via https.

ASSET (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
SECURITY OBJECTIVE ID	9.1.1, 9.1.2, 9.1.3
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.6 EPP SSDLC

4.6.1 TLD-EPP-SSDLC-1

REQUIREMENT ID	TLD-EPP-SSDLC-1
SECURITY REQUIREMENT	You MUST ensure a secure development lifecycle of your EPP implementation (protection against software vulnerabilities)
TYPE	MUST
RISK	Attackers could abuse software vulnerabilities in EPP implementations and related code. Software vulnerabilities may allow an attacker a complete compromise of the EPP environment of a TLD. This affects both self-deployed and supplied EPP software implementations, e.g., in 2023 security researchers showed how an XXE (XML external entity injection) attack on a EPP implementation resulted in a full compromise of a smaller TLD.
RECOMMENDATION	Your EPP implementation will either be self-developed or you rely on an external implementation. In both cases you MUST ensure that a secure software development lifecycle is in place (e.g., NIS2 supply chain security). Security measures MUST be in place to avoid common software vulnerabilities in both self-developed and externally supplied software. Examples are: SSDLC, code and peer reviews, static-code-analysis, penetration tests, and maintaining an SBOM (e.g., EU Cyber Resilience Act). Your SSDLC SHOULD involve a manual review component (e.g., peer review or code audit). Note that Dynamic Application Security Testing (DAST) solutions from 3rd party suppliers will likely not be able to discover EPP-specific vulnerabilities.
ASSET (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
SECURITY OBJECTIVE ID	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.

4.7 Security monitoring

4.7.1 TLD-EPP-MON-1

REQUIREMENT ID	TLD-EPP-SSDLC-1
SECURITY REQUIREMENT	Your EPP infrastructure MUST provide security logs. These logs SHOULD be transferred and analysed in a centralised and separate Security Information and Event Management (SIEM) environment.
TYPE	MUST
RISK	Attackers can hide their attack if server and EPP application logs are not sent to a centralised log aggregation SIEM environment. Without a central log environment, it is difficult to respond to threats in real time and upon an attack it is very likely that the attack detection is either delayed or not noticed at all. If the server is compromised by an attacker, then the attacker may be able to modify or delete related logs thereby making it impossible to conduct a forensic investigation to understand the root cause and impact of the attack.
RECOMMENDATION	You MUST ensure that your EPP environment is generating application logs related to the EPP protocol. When you connect your EPP-related servers to a SIEM environment it is not sufficient to just connect the operating system layer. EPP-specific application logs SHOULD be available too. You SHOULD develop EPP-specific use-cases or patterns in your SIEM / Security Operations Centre (SOC) solution.
ASSET (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
SECURITY OBJECTIVE ID	3.2
TLD ISAC THREAT ID	A link to existing threats identified in the TLD ISAC Threat landscape report – the detailed report is available to TLD ISAC members only.



EUROPEAN
TLD ISAC