SWISS DIGITAL INITIATIVE

Interpretation Guidelines for the Digital Trust Label Criteria Catalog

Version 1 - Valid since April 2024

Swiss Digital Initiative

c/o Campus Biotech

Chemin des Mines 9

1202 Geneva

Switzerland

Introduction

The Digital Trust Label (DTL) was launched in 2022 after a thorough development process. It was developed in a multi-stakeholder process and is constantly evolving. The DTL is awarded to digital solutions after a third-party audit described in the DTL Code of Practice The audit is based on the Digital Trust Criteria Catalogue. The purpose of these Interpretation Guidelines is to transparently communicate how the criteria should be interpreted in the audit. This document therefore clarifies for the auditors how to interpret the criteria in the label process, supports the Label Certification Committee (LCC) in the label award nomination and summarizes inputs and decisions from the Digital Trust Expert Group (DTEG).

As part of Swiss Digital Initiative's non-profit mission on digital trust and transparency we support collaboration and therefore welcome any feedback to: info@sdi-foundation.org

Category: Security

Criteria	No	Specification	Interpretation Guideline
Secure communication, data transmission and storage	1	The service shall apply best practice cryptography to data in transit, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all transmitted data and is appropriate to the properties of the technology, risk, and usage. All data in transit over open communication lines such as the internet must be encrypted.	*Best practice guidance can be found in e.g. government provided standards, Owsap Cheatsheet or NIST Chapter 4.*
	2	The service shall apply best practice cryptography to data at rest, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all sensitive and applicable data at rest and is appropriate to the properties of the technology, risk, and usage.	*Best practice guidance can be found in e.g. government provided standards, Owsap Cheatsheet or NIST Chapter 4.*
	3	Privacy-enhancing technologies such as Anonymization and Pseudonymization shall be used according to best practices in order to adequately protect the user's data.	Privacy-enhancing technologies should be used. An example guidance to best practice anonymization and pseudonymization techniques can be found in the IAPP Guide. Example use cases where anonymization should be in place are - Anonymization of PII after expiration of the retention period - Anonymization of customer/production data or synthetic data should be used for development/testing environment
Secure User Authentication	4	All passwords used for the service shall be subject to a state-of-the-art authentication policy, which includes requirements applicable to the service and ensures that no hard-coded passwords are used, best practice	State-of-the-art authentication policies should follow a risk-based approach and may include - Password requirements - Storage of passwords (hashed, random salt, computationally expensive algorithms)

		authentication is in place and ensures that brute-force attacks on authentication mechanisms are not feasible.	- Ban common passwords - Brute-force protection (e.g., rate limiting) - Offer MFA or argue why not necessary (risk assessment) - Usage of password managers - Education of employees - Regular review of changes in regulatory/legal/industry requirements Further guidance can be found in NIST Appendix A, UK National Cyber Security Centre, Enterprise authentication policy, OWASP Authentication Cheat Sheet, Microsoft Password Guidance.
Criteria. Secure service set up, maintenance and update	5	Guidance for secure installation, configuration, and updates shall be in place and updated for each release if necessary. Guidance shall be available in a manner that is easy to access and understand. Any major changes shall lead to a communication to the users in an easy-to-understand format.	Checking of descriptions on how to accomplish installation, configuration, and updates for the web service - Internal documents: Focus on security-relevant parts (e.g., deployment of service to different environments (dev, test, production), configuration of secure channel, configuration of security parameters) - Public documents: Only required/checked in case service needs security-relevant installation, configuration, and updates done by end user
	6	All software components shall be updatable in a secure manner, and verification of security updates shall be in place.	It shall not be possible for attackers to do any modifications in the context of the web service update process. For instance, this can be achieved by - Controlling the access to the update process: only authorized employees are allowed to do updates - Updates/patches are digitally signed and verified such that any modification would be detected - Updates automatically done by authorized deployment machines - no direct human interaction

	7	Updates shall be timely. Updates addressing critical security vulnerabilities must be available as soon as possible.	There shall be a process for patch/vulnerability management in place - Initial risk assessment of vulnerability (affected assets, business impact, etc.) - Decide on severity of vulnerability (critical, high, ..., low) - Define response times for each severity level - Take actions based on severity - Documentation of decisions
	8	Hard-coded critical security parameters in service software source code shall not be used.	How is this prevented? Examples are - Usage of Static Code Analysis tools - Following Secure Development Lifecycle (SDLC) - Manuel review (4-eye principle)
	9	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated service software shall be unique per service and shall implement security measures to protect the integrity and confidentiality of critical security parameters.	
	10	The service provider shall follow secure management processes for critical security parameters that relate to the service.	Critical security parameters may include (privileged) account credentials, API keys, cryptographic keys, certificates, etc. A secure management process covers creation, storage, rotation, deletion, of security parameters. Best practice guidance can be found in e.g. government provided standards, NIST 800-57 or OWASP Key Management Cheatsheet
Criteria: Vulnerability/ breach monitoring/reporting	11	The service provider shall continually monitor, identify, and rectify security vulnerabilities and/or breaches, and shall provide a public point of contact as part of a vulnerability disclosure policy so that security researchers and others are able to report issues.	The reported vulnerabilities should not be lost internally - Process on how to deal with reported vulnerabilities - Responsible/educated personal, e.g., dedicated email address similar to security@company.com - Ticketing system - Following vulnerability management process

			A public point of contact can be - Dedicated area on website (“Report Vulnerability”) - Put security.txt online (NCSC, Securitytxt.org)
	12	Critical security vulnerabilities shall be communicated to relevant authorities within 72 hours if not corrected, and the impacted users shall be timely and adequately informed if there is an update to be installed.	Initial notification within 72h, this should be clearly stated in the process document. If not, “timely/as fast as possible” must be stated in the process and the customer needs to process and needs to prove via evidence that they were consistently capable in the past to communicate within 72h. Details in log 21.06.2023.
	13	Personal data breaches that create high risks for users shall be communicated to relevant authorities and impacted data subjects within 72 hours.	

Category: Data Protection

Criteria	No	Specification	Interpretation Guideline
User Consent	14	The user shall be informed about the purpose of the processing and / or the legal basis for processing of their personal data in clear and plain language. Where there is more than one purpose and /or legal basis, they need to be listed separately in a way that the user is able to easily distinguish between one purpose and / or legal basis and another.	Information to the user in Terms & Conditions is not sufficient. The information must be done in a transparent and easily accessible form e.g. in the privacy policy. A legal basis is only needed where legally required (e.g. GDPR countries) and does not need to be mapped to the individual data collections. Details in log 21.02.2023.
	15	Where user consent is sought for the processing of personal data, such consent shall be expressly collected from the user for each of the purposes and / or legal basis listed by the service provider and obtained separately from the terms and conditions of use of the services.	Criteria 15-16 only applies IF an organization is actively asking for consent. Otherwise particular attention needs to be paid to criteria 14. Organizations that do not seek consent need to make information according to criteria 14 easily available. Details in log 20.12.2022. Example guidelines for Cookie Banners: ● A Cookie Banner must allow on the first layer for the user to opt-out, e.g. "Reject All". ● All options that are given on the Cookie Banner must be presented to the user in a way that does not severely influence the decision-making: ○ Buttons and fonts must have the same size. ○ Colors can be different as long as contrasts still allow users to quickly identify all options. ○ Clear wording of button text, text shall not be misleading More guidelines can be found in the European Cookie Banner task force report and PWC Switzerland Cookie Banner report.. More details in log 28.11.2023.

	16	Where initial user consent is sought for the processing of personal data, the user shall be provided with the option of either opting in, or opting out, expressed through a valid and affirmative action. If checkboxes are used, they shall not pre-ticked. The user shall also be given the possibility of requesting additional information.	See interpretation for Criteria 14.
	17	The user shall be provided with a separate, easy, and accessible way of the right to object.	See interpretation for Criteria 14.
Data retention and data processing	18	The user shall be informed of the definite time period for which the personal data will be stored. If that is not possible, the user shall be informed of the criteria and reasons used to determine the indefinite period, and a regular timeframe for which a review will be undertaken.	No requirement for a specific duration but digital service providers should consider reducing the duration as much as possible..
	19	In cases in which the service provider anonymises personal data, upon a request by the user, such service provider shall provide a detailed explanation of how personal data is being anonymised, and the safety measures used to prevent de-anonymisation. The service provider shall also update the user on the anonymisation status of any personal data held by the provider at the time of the request.	a process that describes how to answer user requests must be in place. If available, examples will be checked
	20	Once the data retention period lapses, the service provider shall either anonymise or delete the personal data. In case of indefinite data retention periods where regular reviews are to be undertaken (criteria 17), the user shall be informed of the outcomes of the review within 30 days.	
	21	The service provider shall ensure that the user can access their data. Any requests for access need to be acceded to within 30 days. Together with a copy of the personal data, a user is to be provided with names of third parties with whom such personal data has been shared, together with the legal basis under which such data is being held.	

Category: Reliability

Criteria	No	Specification	Interpretation Guideline
Reliable service updates	22	The software version of the service shall be easy to access and understand.	Installable services (e.g., mobile apps) shall present software versions to end users and clearly show updates through a change log. In Web applications/SaaS typically no version is presented to end users as the same version runs for all users on the live system. However, internal version management shall exist.
	23	The service provider shall publish, in a way that is easy to access and understand for the user, the defined support period and the need for that support period.	Are the support periods (i.e., end of life) defined and implemented according to policy? Is the information in regards to the support periods clearly published and easily accessible to relevant stakeholders?
Resilience to service outrage	24	Disaster recovery, business continuity and data backup and restore policies and procedures shall be in place and regularly tested to ensure ongoing availability of the service and associated data.	
Functional reliability	25	The service shall provide its users with an extensive, easy-to-access, easy-to-understand description of its functionalities, and shall operate in strict accordance with this description.	The description of service functionalities should be aligned with the scoping negotiated for the audit and information about the scope of the label should be accessible to the end users.
	26	If relevant, the service shall provision for a secure, precise and efficient billing and payment system which employs two-factor authentication and adheres to local and regional norms.	This requirement only applies to digital billing and payments systems which are part of the solution in question. Invoicing of e.g. third parties that are not directly included in the audit scope are not considered.
	27	If relevant, the service shall provision for a delivery system which fulfills state-of-the-art conditions of the associated specific activity domain.	This requirement only applies to delivery systems which are part of the solution in question, e.g. in e-commerce solutions.

Accountability	28	The service shall provide its users with an easy-to-access, easy-to-understand, and easy-to-print service and service provider identification.	A clearly visible and easily understandable service provider identification must be provided, e.g. in the form of an imprint (“Impressum”). The main points to check are: 1.Is it easily understandable who is responsible for the service? While in the service it should be easy for users to understand who is the party behind the service, e.g. ‘Service name by company name’; company logo omnipresent; this service is offered to you by... + there should be more than a name (minimum imprint with company number and address) 2. Is this information easily accessible? The company imprint shouldn't be more than 1 click away from the service page and provided in accessible format (for visually and hearing impaired) 3. Is the information easy to print? There is a symbol or link to print and the printout features only the relevant info, so no website menus.
	29	The service shall document its compliance with all applicable laws and regulation and assign a contact representative for easy-to-access and easy-to-understand information about legislation that the service is subject to.	
	30	User inquiries and complaints shall be treated in a timely fashion, and relevant alternative dispute resolution mechanisms must be in place to facilitate these processes.	This criteria is completed by the organization being able to show some sort of dispute resolution process in place.

Category: Fair User Interaction

Criteria: Non-discriminating access

Criteria	No	Specification	Interpretation Guideline
Non-discriminating access	31	The system shall provide a non-discriminating access to all its potential users.	Non-discriminating access means that the digital solution should not exclude users or treat users differently based on attributes like nationality, race, gender, religion or other categories considered discriminatory. The solution being offered in certain markets and not in others is not considered discrimination. Also, restrictions based on laws (e.g. trade restriction laws, money laundering laws etc.) and corresponding restrictions are made individually and on a legal basis, is also not considered discriminatory.
Fair user interfaces	32	Service interfaces shall be designed so as not to deceive, nor to manipulate the users, and, in particular, shall exclude clearly manipulative techniques ("dark patterns") such as Interface Interference (Preselection, Obstruction), Aesthetic Manipulation (Toying with emotions, False Hierarchy), Disguised ads (Trick questions, Sneaking), Forced Actions (Social Pyramid, Gamification, Privacy Zuckering). In addition, the use of mildly manipulative techniques shall be clearly announced to the users and proportionate to the objectives of the service.	
	33	The service shall not be designed to exclusively cause user addiction and shall provide the users with an easy-to-access, easy-to-understand information about potential addiction risks during its set up.	
	34	Service providers whose services are illegal to users under the age of 18 shall take proportional steps to verify users' age and prevent under-18s from accessing those services.	

Fair use of AI-based algorithms	35	There shall be clear information to the user when interacting with AI-based algorithms and, especially, with automated decision-making algorithms. The service provider shall also indicate which user-related data is processed by the algorithms and its relationship to the objectives of the service, in addition to informing why an AI is used for the service. Any risks inherent to the algorithms must be clearly and concisely described to the user.	Question: What can be understood under AI-based algorithms with automated decision-making algorithms? Answer: Algorithmically controlled, automated decision-making or decision support systems are procedures in which decisions are initially – partially or completely – delegated to another person or corporate entity, who then in turn use automatically executed decision-making models to perform an action.
	36	If AI-based algorithms and, especially, automated decision-making algorithms, are used, the service shall provision for specific mechanisms to assess their robustness, resilience, and accuracy, as well as the risks associated with their exploitation, and shall provide the user with the possibility to request that a representative of the service provider, reviews and validates the outputs produced by the algorithm.	See interpretation for criteria 34.