

# Code of Practice for the Digital Trust Label

Version 3 – Valid since April 2024



SWISS   
DIGITAL  
INITIATIVE

**Swiss Digital Initiative**

Campus Biotech

Chemin des Mines 9

1202 Geneva

Switzerland



## Digital Trust Label Pricing

Level of complexity	Swiss Digital Initiative (SDI) Label Fee	Audit (SGS)	Total CHF
1	8,000	10,140	18,140
2	8,000	15,210	23,210
3	8,000	20,280	28,280
4	8,000	25,350	33,350

## PART I: CERTIFICATION PROCESS AND RULES

### 1. AUDIT PROCESS

#### 1.1 Scoping

During the scoping, all information needed to prepare a joint offer from SDI and the auditor (SGS) is collected. The client receives a Scoping questionnaire to be filled in and returned to SDI. This is the basis for estimating the scope and therefore the complexity (levels 1-4). If requested, a Non-Disclosure Agreement (NDA) is signed before

The Swiss Digital Initiative has the right to deny any digital service not aligned with the ethical values and spirit of the label the right to begin a Digital Trust Label audit

#### 1.2 Offer issuance and contract signing

The client receives a joint offer containing the total cost of the Digital Trust Label (DTL). After accepting the offer, the client signs the SDI contract before the audit starts.

#### 1.3 Audit steps

##### **STAGE 1**

The auditor kicks off the audit together with the client. The audit checklist is completed with client-specific data and where needed supported with the client's documents to prove fulfillment of the specific criteria.

The process for sharing data and files with the auditor is mutually agreed during the scoping call to ensure the security of the data.

The auditor reviews the audit checklist in a **document review** and thereafter completes an audit report. If needed, minor or/and or major findings/nonconformities are highlighted. Major nonconformities shall be removed before Stage 2 Audit can be started.



## Code of Practice for the Digital Trust Label (DTL)

### Version 3 – Valid since March 2024

**STAGE 2** Stage 2 Audit takes place as a virtual meeting (or at the client's premises if so requested) and includes the following topics:

- Opening meeting
- Formal closing of findings out of Stage 1 Audit
- Verification of the records according to the audit checklist
- Evaluation among the auditors
- Final meeting: Disclosure of the audit result and agreement on the next steps.

#### 1.4 Label Issue

The final audit report is forwarded to SDI for technical review together with the Label Certification Committee. When approved, the label is awarded and valid for three years.

#### 1.5 Surveillance audits

- Surveillance audits take place after one and two years respectively to ensure the maintenance of the relevant procedures and associated documents (templates and records) to comply with the label.

#### 1.6 Early Renewal

Early renewal is due in case of a new release of the product (major changes of the features). Stage 1 audit might be required if the changes are to be considered substantial.

## 2. DUE DATES

The audits shall be completed within the following timeframe:

- Stage 2 Audit: Not later than three months after Stage 1 Audit;
- Surveillance Audit: +/- 2 months from the Due Date (= date of the last Stage 2 Audit date);
- Renewal Audit:  $\leq 3$  months before the Due Date; (= date of the last Stage 2 Audit date);
- Closing of nonconformities: 90 days after the last audit day.

## 3. NONCONFORMITIES

### 3.1 Types of Nonconformities (NCs)

- MAJOR NC: Failure which impacts critical risk related to the criteria (or categories) in the DTL Criteria Catalogue (missing system elements, lack of implementation etc.);
- MINOR NC: Failure which impacts a limited risk related to the criteria (or categories) in the DTL Criteria Catalogue.

### 3.2 Closing of Nonconformities

- MAJOR NC: Action plan to be issued within 30 days; Follow-Up-Audit to be performed within 90 days;



## Code of Practice for the Digital Trust Label (DTL)

### Version 3 – Valid since March 2024

- MINOR NC: Action plan to be issued within 90 days; the implementation of the actions will be checked during the next following regular audit.

Overdues cause a warning of withdrawal of the DTL which lasts 30 days at maximum. Afterwards the label will be withdrawn unless the client takes action.

## PART II: AUDIT DURATION

The certificate is valid for 3 years, provided the annual surveillance audits are passed. The audit duration (number of audit days) is calculated based on the complexity of the product.

Details of the four complexity levels:

Complexity	Definition
Level 1	Regular system or device, for example this can be <ul style="list-style-type: none"> <li>- A server/client infrastructure which consists of one backend service (e.g. Application and Database) and one to two frontend services (e.g. Client Application, Web Application, mobile App, API)</li> <li>- A connected device (e.g. IoT) with one companion application (mobile, PC application) and one Backend Service</li> </ul> The service also should rely on not more than one additional external third-party service, e.g. for payments or authentication.
Level 2	Larger systems, in which more backend and/or frontend services are involved, or which consist of more than one device or multiple companion apps or backends: <ul style="list-style-type: none"> <li>- A server/client infrastructure with either two backend services or 3-4 frontend services</li> <li>- Either two coupled connected devices or 2-3 companion apps or 2 backend services</li> </ul> The service can rely on up to three additional external third-party services, e.g. for payments or authentication.
Level 3	Complex systems, in which more backend and/or frontend services are involved, or which consist of more devices, companion apps or backends: <ul style="list-style-type: none"> <li>- A server/client infrastructure with two backend services and 3-4 frontend services</li> <li>- A server/client infrastructure with three backend services</li> <li>- A server/client infrastructure with 5-6 frontend services</li> <li>- Two coupled connected devices and/or 2-3 companion apps and/or 2 backend services (2 out of 3)</li> </ul> The service can rely on up to five additional external third-party services, e.g. for payments or authentication.
Level 4	Very complex systems, which go beyond the limitations of Complexity Level 3

## 4. PRICING

### 4.1 Pricing

The pricing is provided in a joint offer upfront and includes everything for the three years validity: initial audit fee, label fee, and two surveillance audit fees.

Code of Practice for the Digital Trust Label (DTL)

Version 3 – Valid since March 2024

Level of complexity	Swiss Digital Initiative (SDI) Label Fee	Audit (SGS)	Total CHF
1	8,000	10,140	<b>18,140</b>
2	8,000	15,210	<b>23,210</b>
3	8,000	20,280	<b>28,280</b>
4	8,000	25,350	<b>33,350</b>

4.2 Audit Fees

Charged by auditing firm (SGS).

Initial Audit

Performed before the label is awarded.

level of complexity	Stage 1	Stage 2	CHF
1	2	2	<b>6,760</b>
2	3	3	<b>10,140</b>
3	4	4	<b>13,520</b>
4	5	5	<b>16,900</b>
>4	to be calculated in case-by-case		

Surveillance Audit (x2)

Performed second and third year of the label validity.

level of complexity	Duration (day)	CHF
1	1	<b>1690</b>
2	1.5	<b>2535</b>
3	2	<b>3380</b>
4	2.5	<b>4225</b>
>4	Case-by-case	

The following aspects cause some reduction/increase of the standard audit duration. The % shall be defined case-by-case at the scoping meeting.

Increase of audit duration (10-30%):

- The hosting infrastructure (often provided by a third party and not the company itself) is not certified against ISO 27001 by an acknowledged Certification Body;
- There are multiple (independent) development teams involved.



Reduction of audit duration (10-30%):

- The company is certified against ISO 27001, 27017, 27018 and/or ISO 22301 by an acknowledged Certification Body. Also ISO 42001 will become relevant in the future;
- There are outsourced processes/parts (e.g. data storage), provided an ISO 27001 certificate or supplier audit is available;
- Compliance with other standards such as PCI DSS, SOC 2/ 3 , BSI Cloud Computing Standards (CS) and FINMA compliance audits.

4.3 Label Fee

Charged once by SDI.

Label fee	CHF	8,000.00
-----------	-----	----------

The SDI label fee is a fixed fee regardless of the complexity of the digital service. The SDI label fee is a one-time, fixed fee paid for the 3-year validity of the label.

The fee will be invoiced in two equal parts:

- CHF 4,000 : To be paid upfront, non-refundable in case of an unsuccessful audit
- CHF 4,000 : To be paid upon the successful audit, non-refundable

Please note that all prices are excl. VAT. 7.7%.

**Disclaimer:** *This document has been prepared only for purposes of the use of the recipient and only serves for the scope and the terms agreed. This document may not be reproduced or circulated without the Swiss Digital Initiative's prior written consent. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else. © 2024 Swiss Digital Initiative. Digital Trust Label. All rights reserved.*