fiskaly.
receipts made simple

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

v1.3 (06.11.2025)

fiskaly SIGN FR Service

This document describes the fiskaly SIGN FR service (hereinafter *SIGN FR*), designed to help Point of Sale (POS) providers (hereinafter *Customer*) comply with new French fiscalization rules, particularly Article 286 of the General Tax Code (hereinafter *CGI*), which mandates certification by LNE or Infocert (hereinafter *Certifier*). Together with the fully integrated *fiskaly SAFE service* (hereinafter *SAFE*) for archiving, and the optional *fiskaly Certification Support France* (hereinafter *CONSULTING*), these services aim to address the most complex technical and documentation requirements to meet the conditions of inalterability, security, conservation and archiving: signing, journaling, and archiving.

1. Product description

1.1. The Service provides a clear, structured framework to simplify the certification process for the Customer. SIGN FR and SAFE offer a cloud-based API solution that covers the three main aspects of French fiscalization: signing, journaling, and archiving. These services will be based on fiskaly's existing unified API technology (hereinafter *API*), utilizing a raw scheme where fiskaly will sign the customer's payload without verifying its format in the initial phase. Core aspects provided by fiskaly:

1.1.1. **Signing:** SIGN FR handles the cryptographic signing of a broad scope of data required by French legislation. This includes all data, defined in Article 286 of the General Tax Code. Fiskaly is highly effective at managing the large volume of signatures. The service uses cryptographic chaining of signatures for authenticity and traceability.

1.1.2. **Journaling:** The system continuously signs transactions including all relevant fiscal data. This data is maintained in chronological order, which helps to immediately expose any attempts to delete, alter, or back-date data.

1.1.3. **Archiving:** SAFE ensures the secure storage of the fiscal data. While the legislation mandates a 6-year retention period, certifiers typically demand 7 years to prevent issues with fiscal and calendar year overlaps. fiskaly provides long-term compliant storage and archiving, with full data export functionality for auditing and compliance.

2. Value proposition & benefits

2.1. SIGN FR, SAFE and CONSULTING address the most complex technical and documentation requirements from CGI: signing, journaling, and archiving.

2.1.1. SIGN FR is fully cloud-based and requires no hardware. It is directly integrated with API and the fiskaly HUB (hereinafter *HUB*), but features an API-first architecture for seamless POS integration.

2.1.2. SIGN FR provides cryptographic chains of signatures, comprehensive journaling of sales and system events, and tamper-proof cloud logs to ensure authenticity, traceability, and audit readiness.

2.1.3. SIGN FR provides a free testing environment to streamline integration.

2.1.4. SAFE offers long-term compliant storage with full data search and export capabilities, enabling easy access to audit-ready information and supporting compliance requirements.

2.1.5. CONSULTING helps the customers through the entire initial certification phase and subsequent annual audits by providing Documentation and Certification and Audit Support.

3. Functionalities

3.1. SIGN FR is a JSON-based RESTful Software-as-a-Service solution. A full documentation of the service is provided in the API description (https://developer.fiskaly.com/api) and integration guides are provided in the fiskaly developer page (developer.fiskaly.com). A Quick-Start guide in the form of a Postman collection is also available. Integration and operation of the service requires:

- a contractual relationship with fiskaly that permits the use of the service
- an internet connection
- an integration of the API

3.2. SAFE is a JSON-based RESTful Software-as-a-Service solution. A full documentation of the service is provided in the API description (https://developer.fiskaly.com/api/safe/v0) and integration guides are provided in the fiskaly developer page (developer.fiskaly.com). A Quick-Start Guide in the form of a Postman collection is also available. For additional information, please refer to the Service Description for fiskaly SAFE services, which contains further details on the type and scope of SAFE (the solution presented here is currently based on fiskaly SAFE, and fiskaly SAFE Flex is not supported). In the event of any discrepancies, the information provided in this document shall take precedence over the general service description for fiskaly SAFE services. Integration and operation of the service requires:

- a contractual relationship with fiskaly that permits the use of the service
- an internet connection
- an integration of the API

3.3. SIGN FR offers robust functionalities primarily focused on data security, integrity, and long-term retention, based on CGI requirements.

3.3.1. Core functionalities provided by the services:

3.3.1.1. **Secure data signing:** The service is designed to sign fiscal data with cryptographic mechanisms to ensure inalterability, security and conservation. This is achieved through mechanisms for data authenticity and integrity.

3.3.1.2. **API**: The fiscal data is being provided via API by the Customer. Therefore, the Customer needs to set up Organizations, Subjects, Assets, Entities, and Systems to perform Records, as described in the instructions and API documentation.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

3.3.1.3. **Chronological journaling:** The signing mechanism links each record cryptographically to the preceding one, preventing deletion or alteration. All data that forms the basis for calculating the hash algorithm/condensate and the electronic signature for invoices, receipts, proofs of payment, duplicates and grand totals.

3.3.1.4. **Signature:** The signature is encoded as Base64URL.

3.3.1.5. **Audit-ready data:** fiskaly SIGN FR provides tamper-proof cloud logs, making the data audit-ready. All user actions, such as file uploads, access, views, and exports, are logged and cryptographically hashed for full transparency and auditability.

3.4. SAFE ensures the secure storage of the fiscal data and long-term retention as mandated by French fiscalization.

3.4.1. **Core Functionalities provided by the services:**

3.4.1.1. **Compliant archiving:** SAFE supports the compliant archival of electronic accounting records.. The data is archived in certified Google Cloud data centers in Germany. Archives are stored in an open format. The following data is being archived:

3.4.1.1.1. The data defined in requirement n°3, the corrective data defined in requirement n°4, the test-school mode data defined in requirement n°5, the cumulative and summary data defined in requirement n°7, the traceability data for printing/reprinting of receipts defined in requirement n°9, the data defined in requirement n°15 for the traceability of data purging, archiving and restoration operations, the data defined in requirement n°18 for the traceability of POS data transmission to the centralization system.

3.4.1.2. **Traceability**: SAFE provides traceability and allows the user to export fixed and time-stamped cash data.

3.4.1.3. **Access:** SAFE functionality allows the customer, at any date, to access or generate archives for any past period of less than 7 years via HUB or API.

3.4.1.4. **Consistency:** The data contained in the archive is consistent with the original data in the cash register system, sent by the Customer.

3.4.1.5. **Reliability:** SAFE provides a reliable mechanism to ensure and verify its integrity, even after the Customer has stopped using the cash register system.

3.4.1.6. **Security:** SAFE utilizes an audit mechanism that writes an audit log for every operation in the system. There is an independent audit trail for each organizational unit. The audit logs are chained together using a cryptographic hash.

fiskaly Germany GmbH, Zeilweg 42, D - 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

3.4.1.7. **Data Export functionality:** Supports full data export functionality for auditing and compliance. Customers can search and retrieve data directly from the HUB or via API.

3.5. CONSULTING offers initial certification and subsequent annual audits support.

3.5.1. **Core Functionalities provided by the services:**

3.5.1.1. **Documentation:** The service includes certification documentation for fiskaly related parts (including 1. General design file, 2. Functional specifications file, 3. Technical architecture file, 4. Organizational file, 5. Maintenance file, 6. Operating file, and 7. User file).

3.5.1.2. **Certification and audit support:** The service includes recurring support on the API integration combined with advising on your documentation work, proof-reading service of the English version of the customer's documentation (Documentary admissibly review phase, prior to initial assessment audit), Fiskaly's presence during the in initial in-person audit with InfoCert or LNE, and assistance for the continuous compliance with future fiscal regulation updates (certification is valid yearly).

4. System requirements

4.1. A contractual relationship with fiskaly that permits the use of the service is required.

4.2. An internet connection is necessary for integration and operation.

4.3. Integration of the API is required for customers to access the service via API. Detailed documentation and integration guides are provided.

4.4. A compatible POS system capable of providing the necessary data for signing, journaling, and archiving is fundamental.

5. Security features

5.1. fiskaly prioritizes the security and integrity of the fiscal data provided by the Customer.

5.2. Customer identification & authentication: Customers are uniquely identified via customer-specific API credentials or an authorized user at the HUB. Access to functional service endpoints is conditional upon a valid token created through these credentials.

5.3. Data ownership & segregation: All data provided by a fiskaly customer remains the property of that customer, and no other customer has rights or the possibility to view, retrieve, or alter this data.

5.4. The service ensures the Inalterability of data once received, making deletion or modification of data (stored artifacts or metadata) impossible. Changes can only be documented by creating new independent files.

5.5. Data is stored on fiskaly servers for the necessary contractual and legal retention periods. The data is archived in certified Google Cloud data centers in Germany.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

5.6. It is the customer's responsibility to secure access to their data on their end through appropriate user management and up-to-date information security measures.

6. Maintenance and support

6.1. fiskaly is committed to maintaining and updating SIGN FR and SAFE.

6.2. fiskaly undertakes to maintain and regularly update the service to ensure its security, availability, and compliance with CGI requirements.

6.3. The service will be versioned according to semantic versioning, with significant changes resulting in new major releases. The initial LIVE version shall be 1.0.0. Migration guides will be published to assist customers with transitions to new major releases. All customer-facing changes shall be documented in a public changelog.

6.4. Maintenance activities may result in the temporary outage of the SIGN FR. As far as possible, these activities shall be announced at least two (2) weeks in advance so that customers may schedule their use of the service accordingly. Emergency maintenance activities may deviate from this. Customers are encouraged to refer and subscribe to the fiskaly status page (status.fiskaly.com) for relevant information.

6.5. fiskaly shall provide assistance to customers in the form of the fiskaly support portal (support.fiskaly.com). The portal hosts FAQs and how-to guides regarding all fiskaly services. The support team can be contacted via dev-support@fiskaly.com, or via Web Widget from the fiskaly HUB, Support Page and Developer Page.

7. Testing

7.1. Test environment: SIGN FR and SAFE provides a TEST environment that is a fully functional cloud-based storage system with the same properties as the LIVE system. New versions of the service are available in the TEST environment before LIVE release.

7.2. No real data in test: fiskaly is not responsible if real data is provided by the customer in the TEST environment.

7.3. Free testing is available for developers.

8. Availability

8.1. SIGN FR and SAFE are designed for high availability (99,5% annual average).

8.2. Data resilience: No data is typically lost in the event of an incident. The Recovery Point Objective (RPO) is a maximum of 5 seconds. A synchronously replicating architecture is used and regularly audited.

8.3. Service restoration: The Recovery Time Objective (RTO) is a maximum of 24 hours, meaning full service is restored no later than 24 hours after a disruption.

9. Integration and compatibility

9.1. SIGN FR and SAFE are directly integrated into HUB.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

9.2. SIGN FR is compatible with SAFE and CONSULTING.

9.3. SIGN FR and SAFE are built with an API-first architecture for easy POS integration, following the same API model as other fiskaly services.

9.4. The Customer's POS systems connect directly to the API. The Customer's user creates an API key, authenticates it to receive an access token, and can then transmit files for signing, journaling and archiving.

9.5. Annotations**:** Customers will provide additional information (annotations) when uploading files, which are metadata attached to content for processing or categorization. The system validates transferred data against the annotation schema if set by the customer.

10. User and administration functions

10.1. Usage of SIGN FR is permitted on the basis of an authorized user at the HUB and the API.

10.2. Usage of SAFE is permitted on the basis of an authorized user at the HUB and the API.

10.3. Authorized users have the right to upload and manage all necessary data via provided endpoints and export all submitted data.

10.4. Administrative rights: fiskaly reserves the right to perform scheduled or ad-hoc administrative or maintenance actions to ensure service correctness, stability, performance, restrict access for non-compliance, and address customer requests.

11. Service Limitations

11.1. No semantic validation. SIGN FR and SAFE facilitates data collection in compliance with applicable laws and regulations but does not provide any semantic validation of the data.

11.2. The completeness and correctness of the data provided to the service are the sole responsibility of the customer.

11.3. Changes in applicable laws and regulations may result in significant changes to fiskaly services at any time. fiskaly will try to limit the impact of such changes on the service by bundling them into major releases. These releases will affect the API schema and will be reflected in the service URLs, e.g. v1 will be replaced by v2, etc. Resources created under the previous version(s) should not be affected, and will be available to the new major release, unless regulatory changes dictate otherwise. fiskaly will publish migration guides to inform and assist customers in transitioning to a new major release.

11.4. fiskaly aims to keep the number of major releases low, with at most one major release per year. However, as changes may reflect regulatory innovations that are time-critical, such a timeline may not be always possible. The release or deprecation of major versions shall be announced to all service customers well in advance.

12. Customer obligations

12.1. The Customer is responsible for integrating the API into their POS system.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

12.2. The Customer is responsible for staying updated and integrating new major releases as they are announced and made available in the TEST environment.

12.3. The comprehensive nature of SIGN FR and SAFE is its interplay with Customer responsibilities to ensure compliance with French CGI requirements. The following requirements are in the responsibility of the Customer or the Customer's POS system.

12.4. The Customer is responsible for ensuring the information on receipts is consistent with the recorded cash data, including, but not limited to the following information and applicable to the customers use cases:

12.5. **General Obligation:** Any VAT-taxable person supplying goods/services to private customers and recording payments with a cash register system must use a system that satisfies conditions of inalterability, securitization, conservation, and archiving of data for tax control. This applies to software with cash functionality, including "free" or internally developed software.

12.5.1. **Documentation** (n°1,2): The POS system must be documented in terms of design, operation, maintenance, and use, with regulatory documents in French. Additional technical documentation can be in French or English.

12.5.2. **Data recording** (n°3): The POS system must record all cash data related to transactions and settlements, including receipt number, POS identifier, establishment unique identifier, transaction date/time, total amount with VAT, and detailed item/service lines (wording, quantity, unit price, total HT, VAT rate, etc.). All cash data must be stored as elementary data in hard, non-volatile memory.

12.5.2.1. **Transaction details (cash data)**

12.5.2.1.1. **Document header data**: Unique document identifier, document number, type of document (invoice, receipt, note, credit note, proforma invoice, proof of payment, correction, cancelation, reprint), date and time of transaction/registration/issue, references to other documents (e.g., quotations, purchase orders, delivery orders, previous receipts).

12.5.2.1.2. **Issuer data**: Name or corporate name, address, postcode, city, country, SIRET/SIREN number, NAF/APE code, VAT number, legal form, tax representative details, and payment options for VAT.

12.5.2.1.3. **Customer data**: Distinction between professional/individual, customer number, name/company name, address, postcode, city, country, VAT/SIRET/SIREN/Fiscal Identification numbers, RCS, and delivery address if different.

12.5.2.1.4. **Line item details**: Product code, wording/description, quantity, unit of measurement, unit price (excl. VAT and incl. VAT), discount rates/amounts, price increases/reductions, total amounts per line (excl. VAT and incl. VAT), applied VAT code/rate/wording, other taxes, additional information, and legal guarantee mentions.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

12.5.2.1.5. **Payment information**: Code/name/references of payment methods, amount of payment, occurrence of regulations, foreign currency.

12.5.3. **Corrections** (n°4): Corrections to transactions must be done via "plus" and "minus" transactions, not by direct modification of original cash data, and these operations must be recorded and inalterability guaranteed.

12.5.3.1. **Modifications and corrections**

12.5.3.1.1. Traces of all modifications and corrections made to recorded transactions must be included. Corrections are to be made by "plus" and "minus" operations, not by direct alteration of original data, and these correction operations must also be recorded and inalterable.

12.5.4. **Test/School mode** (n°5): Data generated in "school" or "test" mode must be recorded and secured like actual cash data but explicitly identified as such. The manager's identifier for this mode and all operations within it are part of cash data. Any vouchers issued must be marked "dummy" or "simulation," and the use of this mode must be visible on the system's display.

12.5.4.1. **Test/School mode data**

12.5.4.1.1. Data generated or simulated through a "school" or "test" mode must be recorded and secured like actual cash data, but explicitly identified as such. This includes the identifier of the manager allowing the record and all operations carried out in this mode.

12.5.5. **Securing supporting documents** (n°9): The POS must distinguish receipts issued before/after payment, mark reprinted receipts as "duplicate," ensure secure traceability of printouts/reprints (physical and electronic), ensure consistency of receipt info with recorded cash data, display "offline" mode on exports for centralizing systems, and mention LNE (“LNE certified cash register system”) or Infocert ("Infocert certified cash register system") on tickets. Procedures for electronic document issuance must be documented.

12.5.6. **Purging** (n°13,14): If the POS has a purge function, it must ensure an archive of all purged data is generated and retained beforehand. Cumulative and summary data, and transaction tracking data, must never be purged from the system.

12.5.7. **Traceability of operations** (n°15): The POS system must ensure secure traceability of archiving, purging, and restoration operations by recording their timestamp and POS identifier.

12.5.7.1. **Traceability data**

12.5.7.1.1. All data ensures the traceability and integrity of transactions.

12.5.7.1.2. Traceability of printouts and reprints of receipts (final or provisional), with reprints clearly marked "duplicate".

12.5.7.1.3. Traceability of archiving, purging, and restoration operations of application data, including time stamp and POS identifier.

12.5.7.1.4. Traceability of POS data transmission to a centralizing system, ensuring completeness of the transferred data flow, even during disconnections or offline modes. This includes identifying when the system operates in offline mode.

12.5.8. **Data retention** (n°16,17): Cumulative and summary data, as well as traceability data, must be kept within the system itself. Other cash data can be stored in the system or archive. The system must protect against physical storage failure or warn the user of their responsibility to retain data for 7 years. Archives must guarantee integrity and availability for 7 years.

12.5.9. **Centralizing system** (n°18): If data storage is centralized, the POS must provide a reliable data transfer mechanism ensuring completeness, even with disconnections. Offline mode use should be limited, specified, documented, and notified to the user.

12.5.10. **Tax Administration Access** (n°19): The POS must provide tax authorities access to all recorded cash data and an automated means to verify its integrity. A French user manual detailing data access and integrity verification tools must be provided, ensuring security is not jeopardized.

12.5.11. **Identification of fiscal scope & versions** (n°20,21): The editor must clearly define the fiscal perimeter (source code files, libraries, modules impacting compliance) and list them exhaustively. The POS system must be clearly identified by a major and minor version number, easily accessible from the user interface. Modifications to the fiscal perimeter or parameters affecting compliance must increment the major version number. The publisher must provide the footprint of each major release.

12.6. Customer obligations to SIGN FR

12.6.1. The customer is responsible for activation or deactivation of the service

12.6.2. The customer is responsible configuring the service

12.6.3. The Customer is responsible to provide the relevant data via API

12.6.4. The Customer is responsible for providing all necessary data during an fiscal audit based on the French regulations.

12.6.5. The customer must transmit all required tax-relevant data to fiskaly in the format and schema specified by fiskaly via the API.

12.6.6. Integration and ongoing transmission: The customer is responsible for properly integrating the API into its POS system and ensuring that each relevant business transaction is transmitted in a timely and continuous manner.

12.7. Customer obligations to SAFE

12.7.1. The customer is responsible for activation or deactivation of the service

12.7.2. The customer is responsible to individually define the storage period for the artifacts.

fiskaly Germany GmbH, Zeilweg 42, D – 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

12.7.3. The customer is responsible configuring the service

12.7.4. The Customer is responsible to provide the relevant data via API

12.7.5. The Customer is responsible to provide the cumulative and summary data to be archived, if the cash register system is changed.

12.7.6. The Customer is responsible for providing all necessary data during an fiscal audit based on the French regulations.

12.7.7. The Customer is responsible that the period, covered by an archive, may not exceed one year or one fiscal year.

12.7.8. The data contained in the archive must be consistent with the original data in the cash register system and must provide a reliable mechanism, independent of the medium, to ensure and verify its integrity, even after the user has stopped using the cash register system.

12.7.9. The customer must transmit all required tax-relevant data to fiskaly in the format and schema specified by fiskaly via the API.

12.7.10. Retrieval and verification obligations: Exports generated by the customer must be retrieved and retained by the customer and submitted to the competent tax authorities if required.

12.8. Customer obligations to CONSULTING:

12.8.1. The Customer shall provide fiskaly with all technical, operational, and organizational information reasonably required for the performance of the CONSULTING in a complete, accurate, and timely manner.

12.8.2. The Customer shall ensure the accuracy and completeness of all information, documentation, and data supplied to fiskaly.

12.8.3. The Customer shall promptly notify fiskaly of any changes to systems, processes, or organizational structures relevant to certification or audit requirements.

12.8.4. Access and Availability

12.8.4.1. The Customer shall grant fiskaly and its authorized consultants reasonable access to personnel, documentation, and systems necessary for providing the CONSULTING Services.

12.8.4.2. The Customer shall make responsible employees available for meetings, interviews, and follow-up clarifications as required during the consulting engagement.

12.8.5. Certification and Audit Preparation Responsibilities

12.8.5.1. The Customer shall implement, in a timely manner, fiskaly's recommended corrective or preventive actions necessary to achieve or maintain certification and compliance.

fiskaly Germany GmbH, Zeilweg 42, D - 60439, Frankfurt am Main, Germany
+43 1 9974459, fax.: +43 1 9974459 99, office@fiskaly.com, www.fiskaly.com

12.8.5.2. The Customer shall adhere to fiskaly's instructions related to certification preparation and audit support to avoid unnecessary delays or compliance risks.

12.8.5.3. The Customer shall maintain and preserve records of all documents relevant to the certification or audit process, including fiskaly's consulting outputs and implementation evidence, for the legally prescribed retention period.

12.8.6. Scope of Consulting Services

12.8.6.1. The Customer agrees that the allocated consulting hours and days shall be used solely for initial certification and subsequent annual audit support. Hours and days not consumed in the calendar year expire without compensation.

12.8.6.2. The Customer shall request and schedule consulting days with fiskaly at least four (4) weeks in advance to ensure fiskaly's resource availability.

12.8.6.3. The use of consulting days for purposes other than certification or audit support requires fiskaly's prior written approval.