

Standardisation in Financial Services for Switzerland & Liechtenstein with a Focus on Artificial Intelligence

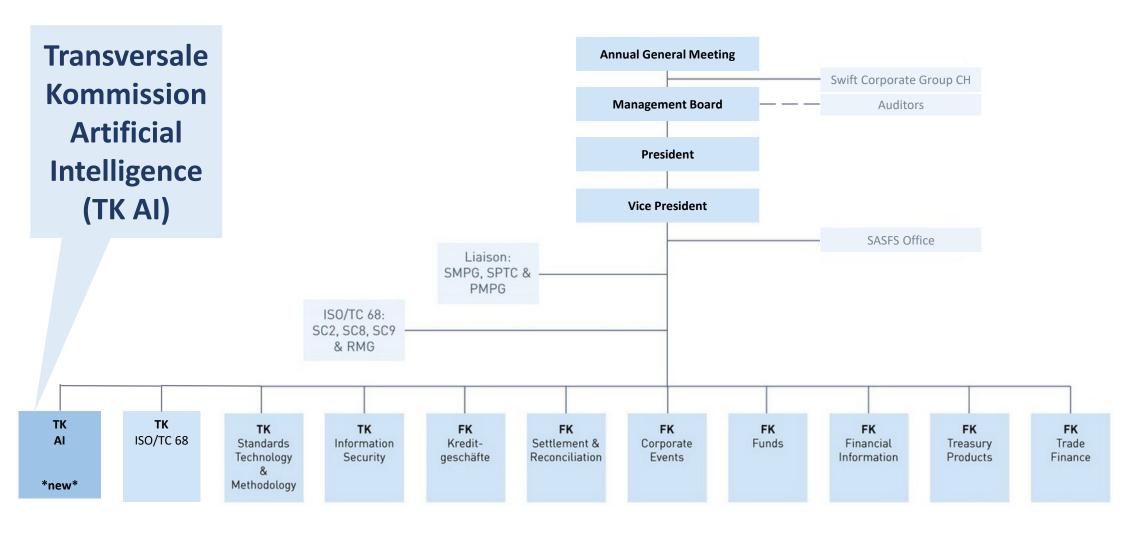
Plateforme Tripartite

Welle 7, Berne, 8 December 2025

Rainer Vogelgesang Torsten Schmidt (SASFS Executive Committee)
(Chair SASFS Transversal Commission Artificial Intelligence (TK AI))



SASFS - Who we are ...



8 December 2025 2



SASFS – How we are connected in Switzerland and internationally ...

Interlinking with Swift

The SASFS forms the Swift
National Member User
Group (Swift NMUG) for
Switzerland and
Liechtenstein and
represents the interests of
both countries vis-à-vis
the Society for Worldwide
Interbank Financial
Telecommunication (Swift)
based in La Hulpe,
Belgium. The Associations
president acts as
chairperson.



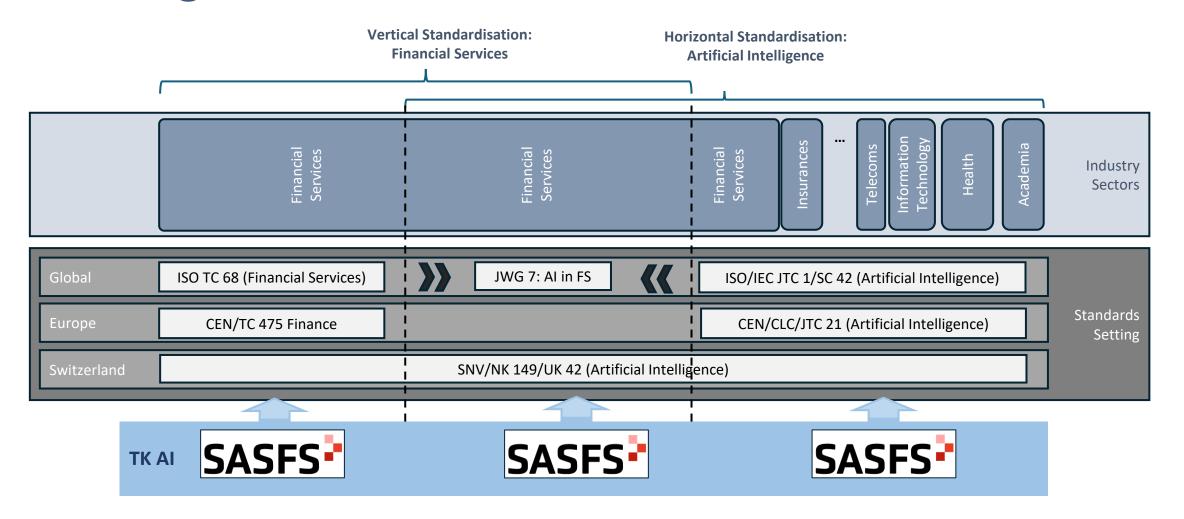
Interlinking with ISO

Based on the mandate agreement between the Swiss Association for Standardization (SNV) and the Swiss Banking Association, the SASFS represents the interests of Switzerland and Liechtenstein vis-à-vis the International Organization for Standardization (ISO) in the Technical Committee 68 (ISO/TC 68).

8 December 2025



SASFS – How we drive standardisation in Artificial Intelligence



8 December 2025





SASFS – Swiss Association for SWIFT and Financial Standards - Executive Board

TK AI Chairs

TK AI Steering Committee

1# Definition, Terminology & Glossary

- Definition and scope of Artificial Intelligence
- Definition of and relation between Al System, Model and Al Use case
- Identification of AI & AI Inventory
- Al Lifecycle status & other Al Terminology: eg Al Oversight, explainability, traceability, toxicity
- Specific terminology: deployer vs provider of AI

2# Assessment & Evaluation of Al systems, models & use cases

- Al Governance , e.g. governance structure & bodies, roles & responsibilities
- Al Risks, e.g. identification, categorization and maintenance
- Al Risk & Lifecycle management, e.g. Inherent & residual risk assessments, documentation, evaluation, testing
- Incident detection & Management
- Al portfolio oversight roles & responsibilities

3# Third Party Management and Data Ethics & Privacy

- Requirements for legal accountability, intellectual property rights management and liability across the value chain
- Use of data & data accessibility by the third party
- Third Party Risk Management Monitoring & Control
- Data Privacy, Ethical use of data

4# AI Transparency and AI oversight, AI Literacy—training education

- Transparency requirements for disclaimers for the responsible use of AI
- AI Oversight human oversight,...
- Al Training & Education minimum standards taylored to roles & responsibilities

8 December 2025

TK AI – Example: Data Leakage & Third Party AI



Example – develop best practices for data leakage risk mitigation in third party AI solutions as inputs for standardization

TK AI

- Encryption: Encrypt data at rest and in transit
- Data Minimization & Anonymization: Share only what is strictly necessary.
- Federated Learning / On-Premise Processing: Keep raw data within your environment; only share model updates.
- Differential Privacy: Prevent reverse-engineering of sensitive data.
- Access Control & Monitoring: Role-based access for vendor systems.
- Data Leakage Prevention (DLP)

- **Encryption**: Implement at rest (AES-256) and in transit (TLS 1.3) encryption. Use customer-managed keys (KMS) for full control.
- Data Classification Before Sharing: Tag data by sensitivity level and apply sharing restrictions. Avoid sending unnecessary PII or confidential data.
- No Training on Customer Data Without Consent:
 Prohibit using data for model retraining unless opt-in is documented.
- Segregated Environments: Require tenant isolation and dedicated VPCs / private endpoints for API calls.
- Data Loss Prevention (DLP) Policies: Apply DLP filters on inputs and outputs to prevent sensitive data from being exposed in model responses. For LLMs, implement prompt sanitization and output redaction.
- **Secure Logging:** Redact sensitive fields in logs. Store logs in encrypted, access-controlled systems.

Standardisation (ISO,...) Working Groups

- ISO/IEC 27001 Information Security
 Management System (ISMS) covers
 encryption, access control, and security
 governance.
- **ISO/IEC 27002** Security Controls- detailed best practices for data protection.
- ISO/IEC 27701 Privacy Information
 Management extends 27001 for personal data protection (GDPR alignment).
- ISO/IEC 23894 AI Risk Managementaddresses AI-specific risks, including data leakage.
- ISO/IEC 42001 AI Management System -Governance framework for responsible AI, including data handling. {JCT1/}
- ISO/IEC 27018 Protection of PII in Cloud Services -critical when using third-party AI hosted in the cloud.

 Best practices (how)

Standards

8 December 2025

Data leakage

6



SASFS and TK AI - How to get involved





If you within your **financial institution** would like to be part of the exciting standardisation space, please reach out to the SASFS representative office at

SASFS GESCHÄFTSSTELLE

Swiss Association for Swift & Financial Standards (SASFS) Tannenstrasse 98 8424 Embrach

☑ geschaeftsstelle@sasfs.ch

Tel.: +41 79 941 30 87

We look forward to hearing from you!

8 December 2025 7