



iText 7 Core – Integrating remote electronic signatures for Swisscom Trust Services

Swisscom Trust Services is the leading trust service provider in Europe, enabling their partners to implement business models for efficient, location-independent and

completely digital processing with their customers. Read on to learn how they use iText 7 to integrate electronic signatures into legally valid and timestamped documents.

BACKGROUND

Swisscom is Switzerland's primary telecoms company and one of its leading IT companies. As part of the Swisscom organization, Swisscom Trust Services offers businesses its Signing Service; a remote service for the legally binding electronic signing and timestamping of documents.

HOW BUSINESSES USE SIGNING SERVICE

By using the Signing Service, Swisscom's business partners can offer their customers digital processes for document transactions. Numerous companies (especially from the banking sector) have already recognized this potential and integrated their remote signing service into their workflows to sign various types of PDF such as legal contracts, financial contracts, invoices etc.

A key benefit for their clients is that they are currently the only European provider that provides qualified electronic signatures in accordance with both the eIDAS (European Union's Electronic Identification Authentication, and Trust Services) and Swiss equivalent ZertES regulations.

The eIDAS regulation provides a framework for electronic identification and trust services for electronic transactions in the European single market. Since coming into effect on 1st July 2016, it offers a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

Similarly, ZertES is a Swiss federal law that regulates the conditions under which trust service providers may use certification services with electronic signatures. In addition, it provides a framework outlining the provider's obligations and rights relating to providing certification services.

Under these laws, qualified electronic signatures (a specific digital signature implementation which is the strictest form of electronic signature) are legally defined as being equal to a handwritten signature, thus promoting the use of secure services for electronic certification. Signers are required to use certificate-based digital ID issued by a qualified Trust Service Provider (QTSP) such as Swisscom Trust Services.

An additional factor for Swisscom's growth is the introduction of the European Green Deal, a roadmap for making the EU's economy sustainable by moving to a clean, circular economy, restoring biodiversity and cutting pollution. Naturally, this encourages the use of digital solutions like those of Swisscom Trust Services to reduce the impact on the environment by saving valuable resources, and similar regulations are likely to be introduced in other parts of the world.

GOALS

- ✓ To allow the addition of authenticated digital signatures into PDFs
- ✓ To enable their partners to provide digital signing of documents for their customer

CHALLENGES

Swisscom's Signing Service is a cloud service for the legally binding electronic signing and time stamping of documents and files. The electronic signature ensures the integrity and authenticity of files for a contractual partner or a regulating authority. Signature application scenarios are supported in accordance with the Swiss Signatures Act (ZertES) and electronic archiving (GeBüV).

Two versions of the service are available: one for personal on-demand signatures and one for mass signatures.

Some of the benefits of using the AIS:

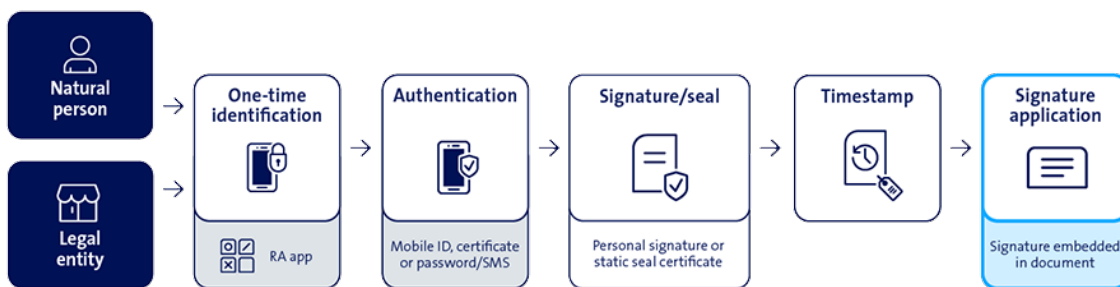
Electronic documents can be signed at any time without the installation of software on the user's side

High availability and security due to redundant operation in the Swisscom data centers

Increased efficiency and verifiability to reduce costs and save time

Partners benefit from the expertise of Swisscom as a legally recognized Certificate Service Provider (CSP)

Save paper by signing documents electronically, reducing environmental impact and increasing sustainability



An overview of the entire DABS solution

HOW DIGITAL SIGNING FOR PDF WORKS

When a PDF document is signed using Public Key Infrastructure (PKI), a hash is calculated using a cryptographic algorithm from all the bytes of the file, except the bytes of the signature itself. This hash is then signed using a private key and finally embedded into the PDF file. Essentially, this is achieved by adding an empty signature block to an existing PDF document that needs to be digitally signed.

Anyone with the corresponding public key can validate the signature, but if the PDF was altered, modified, or corrupted in any way, the signature will be invalidated as the document hash will not match the signed hash.

As it allows PDF documents to be programmatically signed, iText has always been at the forefront of digital signature technology in PDF thanks to its enterprise-grade capabilities for bulk generation of PDFs, huge userbase and reputation for standards-compliance.

Our free ebook “Digital signatures for PDF documents” has been seen as a reference in the field, and iText 7 adds support for PDF 2.0 and superior support for PAdES (PDF Advanced Electronic Signatures), along with a refined and reimplemented API and many more features. All of this continues to strengthen iText's position as a global leader in PDF technology.

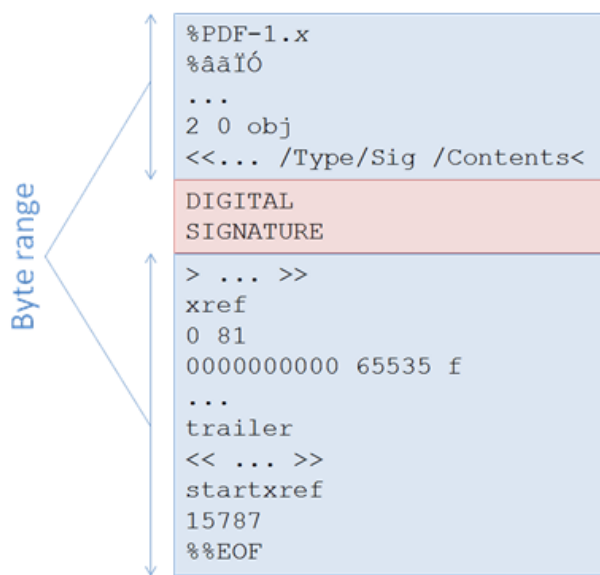
SOLUTION

Swisscom Trust Services developed the Signing Service by making use of the long-standing digital signing capabilities of iText. Their solution has been using iText as the backbone of its PDF signing engine for over 5 years.

Swisscom Trust Services chose iText thanks to its ease of use, flexibility, and wealth of digital signing documentation. Because of the way iText provides an abstraction layer for PDFs, Swisscom’s customers do not need to worry about the PDF standards and specifications. In a similar way, Swisscom provides their own abstraction layer for customers to use for their digital signing requirements.

Customers are enabled to add authenticated digital signatures to PDF documents by making use of iText’s advanced PDF editing and manipulation capabilities. A unique hash is generated from the PDF and sent to the Signing Service. The hash is then signed and returned, and then the customer can then add the authenticated digital signature into the signature block.

For security, hashes are generated using the Secure Hash Algorithm method; specifically the SHA-2 family of cryptographic functions. SHA-256, SHA-384, and SHA-512 digest algorithm methods are supported, and document hash values are encoded in a Base64 encoded binary form.



How a digital signature appears in the structure of a PDF

RESULT

Both Swisscom Trust Services and their partners are very happy with the functionality iText gives them to produce digitally signed PDFs. Being a highly-scalable PDF generation solution, it’s no problem for iText to handle however many documents are required. In fact, iText is integrated into other digital identity services developed by Swisscom Trust services, such as their Mobile ID and Smart Registration Service, proving its value to them.

Swisscom has also taken advantage of the support iText provides to its customers; being experts in the PDF field we can offer advice and assistance with the complexities of PDF specifications, implementation of different signing standards, encryption methods etc.

We chose iText to power the PDF signing part of AIS due to its ease of use and flexibility. Thanks to its provision of an abstraction layer for PDF, it enables our customers to produce digitally signed PDFs without having to know about the PDF specifications.

PETER AMRHYN - CTO TRUST SERVICES, SWISSCOM

Swisscom Trust Services

ABOUT SWISSCOM TRUST SERVICES

Swisscom Trust Services is the only European provider of qualified electronic signatures for EU (eIDAS Signature Ordinance) and Swiss (ZertES Signature Act) legal territories. As leading provider of trust services in Europe, Swisscom Trust Services enables partners to implement pan-European digital innovations by providing identity-based services that can run entirely on digital platforms, eliminating the need to change between media formats. The signature service easily enables partners to add an electronic signature to their own business solutions while taking industry-specific requirements and compliance regulations into account.

This provides end customers with a multitude of options which previously had to be completed on paper, such as signing contracts, buying insurance, signing an employment contract, applying for a credit card or signing acceptance protocols – digital and legally binding.

Swisscom is the leading telecommunications company and one of the leading IT companies in Switzerland. Swisscom offers mobile communications, fixed network, Internet and digital TV to business and private customers and is also one of the largest providers of IT services in Switzerland.

Swisscom Trust Services is one of the leading trust services providers on the market. We place the highest demands on our solutions and therefore only select partners and suppliers that we are convinced complement us at the appropriate level. iText is such a partner.

MARCO SCHMID - HEAD OF INTERNATIONAL EXPANSION STRATEGY, SWISSCOM

”

ABOUT US

iText is a global leader in innovative award-winning PDF software used by millions of users worldwide to create digital documents like invoices, credit card statements, mobile boarding passes, and more. The iText 7 Core library is available as open source, while commercial licensing provides professional support and release from AGPL requirements. The iText 7 Suite includes a wide range of add-ons for extra functionality, and we also develop iText DITO: a low-code, template-based PDF generator.

iText works and works well. Our customers choose iText because of our world-class software quality, and our reliable, mature, and proven technology. Our PDF solutions can be embedded into the document workflows of various industries and their applications to create and manipulate PDFs, tasks like secure content redaction, encryption, digital signatures, and ensuring documents are accessible and archivable.

Europe, Middle East, Africa & CIS

AA Tower
Technologiepark - Zwijnaarde 122
9052 Zwijnaarde
Belgium

✉ sales.isb@itextpdf.com
🌐 www.itextpdf.com
☎ +32 9 298 02 31

Americas

530 Harrison Ave,
Second Floor
Boston, MA 02118
United States

✉ sales.isc@itextpdf.com
🌐 www.itextpdf.com
☎ +1 617 982 2646

Asia & Oceania

Republic Plaza
9 Raffles Place, Level 6,
Republic Plaza 1
Singapore 048619

✉ sales.isa@itextpdf.com
🌐 www.itextpdf.com
☎ +65 6932 5062