TIS | Objektni Informacijski Sustavi
MEETING OF MINDS

TIS - Objektni Informacijski Sustavi d.o.o.
Heinzelova 33, 10 000 Zagreb, Hrvatska
OIB: 62434408100

TIS eSIG – Digital Signature Solution

Overview and Proposal

Tel: +385 1 23 55 700
Fax: +385 1 23 02 014
E-mail: info@tis.hr
www.tis.hr

TIS - Objektni Informacijski Sustavi d.o.o.
Heinzelova 33, 10 000 Zagreb, Hrvatska
OIB: 62434408100

Introduction

Digital Transaction Management (DTM) is a fast growing market which includes legally compliant electronic signatures, managing and tracking the flow of documents, conducting secure transactions and ensuring secure storage of data.

TIS eSIG solution is concieved around a single, comprehensive platform that can seamlessly support all use cases, signature types, and user experiences and can be deployed according to customer needs.

We support all most commonly used types of e-signatures. In addition to electronic signatures provided with Click-to-sign, Draw-to-sign and Type-to-sign mechanisms, eSIG allows also eIDAS compliant Advanced Electronic Signatures with Handwriting Biometrics, and eIDAS compliant Qualified Electronic Signatures with Remote and Local certificates.

TIS eSIG is being used in financial industry, transport industry, and is qualified and extendable to any other industry striving to achieve digital awareness and presence.

About Signatures

Advanced e-Signature

An advanced electronic signature (AdES) is an electronic signature that has met the requirements set forth under EU Regulation No 910/2014 (eIDAS-regulation) on electronic identification and trust services for electronic transactions in the internal market.

- Satisfies certain quality requirements => provides safe proof
    - Is uniquely linked to the signatory
    - Is capable of identifying the signatory
    - Is created using trusted creation data (usually a private key) that the signatory can, with high level of confidence, use under his sole control
    - Is linked to the data in such manner that any subsequent change of the data is detectable
- Created typically through
    - Pure biometric signature
    - HTML5 signature using an authentication method that identifies the signer
    - Cyptographic digital signature

Advanced electronic signatures that are compliant with eIDAS may be technically implemented through the AdES Baseline Profiles that have been developed by the European Telecommunications Standards Institute (ETSI):

- XAdES, XML Advanced Electronic Signatures is a set of extensions to XML-DSig recommendation making it suitable for Advanced Electronic Signatures.

- PAdES, PDF Advanced Electronic Signatures is a set of restrictions and extensions to PDF and ISO 32000-1 making it suitable for Advanced Electronic Signature.
- CAdES, CMS Advanced Electronic Signatures is a set of extensions to Cryptographic Message Syntax (CMS) signed data making it suitable for advanced electronic signatures.

Qualified e-Signature

A qualified electronic signature is an electronic signature that is compliant with EU Regulation No. 910/2014 (eIDAS Regulation) for electronic transactions within the internal European market. It enables authorship verification of a declaration in electronic data exchange over long periods of time. Qualified electronic signatures can be considered as digital equivalent to handwritten signatures.

- Equivalent to written legal form
- Non reputable
- Requires a personal qualified signing certificate issued to the signer
- Requires certain identity checks from the CA when issuing the certificate to the signer
- Must be stored and used with a secure signature creation device

Solution

TIS eSIG is built around one of worldwide leading signature platforms – Namirial SIGNificant. With almost unprecedented level of expertise and experience, this platform enables TIS eSIG to provide signature services tailored to particular customer needs, and remains compliant to all relevant standards and norms.

About Namirial

Namirial is uniquely positioned as a leading provider in the DTM market thanks to the breadth and depth of its products and services portfolio, designed around a single, holistic platform that can seamlessly support all use cases, types of signatures and user experiences and can be deployed as desired by the customer (on-premises, in cloud or hybrid). Namirial is best represented by the following figures:

- *More than 1 million customers,*
- *More than 375.000 installed handwritten biometric signature workplaces,*
- *More than 3 billion pages digitally signed and archived.*

TIS - Objektni Informacijski Sustavi d.o.o.
Heinzelova 33, 10 000 Zagreb, Hrvatska
OIB: 62434408100

Popular Use Cases

TIS eSIG solution can be utilized in several use cases. In many cases these are combined in order to provide comprehensive and integrated digital signature solution which covers all business needs.

E-Signing In-Shop / Branch

- Flexibility to use different document presentations & multiple signature capture devices
  - Signature pads / smartphones
  - Signature screens
  - Tablets
- Using signature device as a marketing & feedback channel (videos, pictures, questionnaires) when idle
- Support for Terminal Services
- Option to verify a signature in real time

Mobile Signing in the Field

- Sign on portable devices based on iOS, Android or Windows – tablets, smartphones or sign pads
- Complete PDF forms on the go
- Add scans of driver's license, passport, or any other photo

Send a Document for Signature to External Recipients

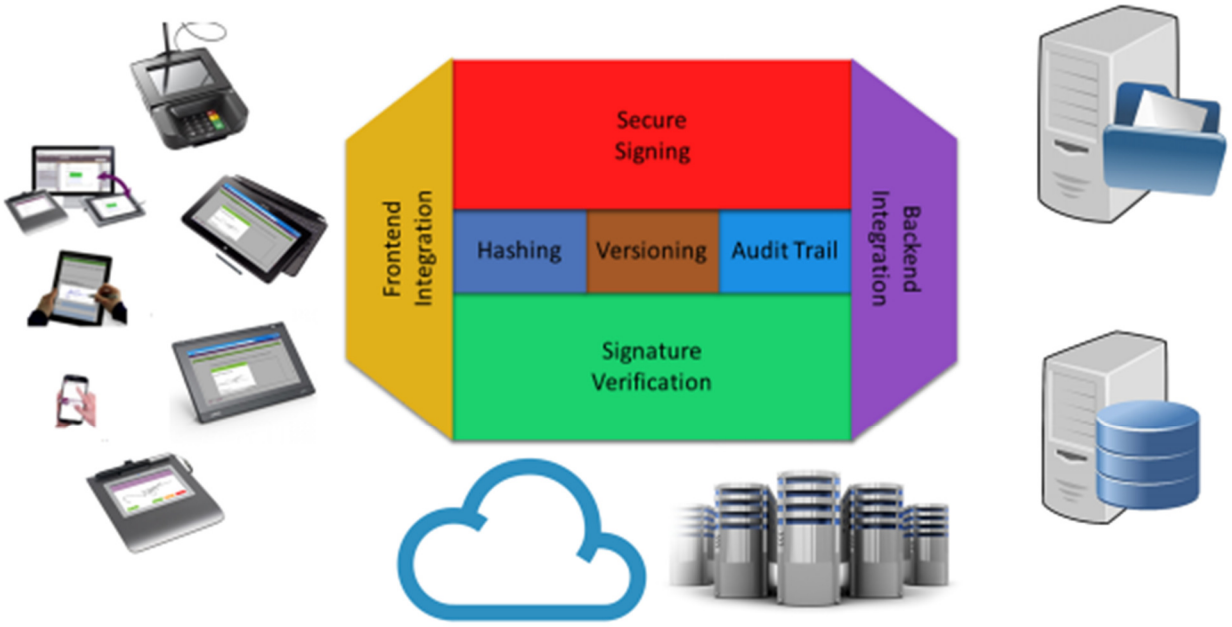
- Without installation on any HTML5 enabled device
  - PC, tablet, smartphone
- Onboarding & sales assistance through video collaboration
- Reuse of existing user authentications (Web portal)
- Email to involve external signers asynchronously

E-Signing within the Organization

- Single Sign On authentication and PKI integration
- Batch signing of documents for approval processes
- Send links to internal users to trigger a transaction

TIS - Objektni Informacijski Sustavi d.o.o.
Heinzelova 33, 10 000 Zagreb, Hrvatska
OIB: 62434408100

Architecture



TIS eSIG solution architecture is server-based in order to achieve highest possible security, monitoring, and auditing standards. During the process of signing the document, maximum effort has been made to protect documents as well as all important data. Document is kept firmly protected, with only rendered images being sent to signature devices, together with hash values, for reviewing and signing.

Services

Handwritten Biometric Signature

Capturing a handwritten signature is the best choice for getting documents signed when meeting clients face-to-face, either on your premises or on the go. In this scenario, you can present the client with the document on your own device (e.g., on a point-of-sale computer or a tablet) and the client can sign using whatever device you provide.

A forensically identifiable signature is much more than merely a digitized image of a handwritten signature. It requires recording the handwritten signature of a person using all available parameters; such as acceleration and speed - i.e. the writing rhythm. These dynamic parameters are unique to every individual and cannot be reproduced by a forger. That's why the digitized signature is forensically identifiable and far more reliable than just the signature image.

If someone claims, not to have signed a document, a forensic expert can perform a thorough manual signature verification, using specialized software to achieve an admissible result in the same way as the expert would with a signature on paper. Thus, the biometric signature fulfills the eIDAS Advanced Electronic Signature standard and has been widely adopted as the de-facto industry standard wherever applicable.

Local Signatures

We can issue Qualified Electronic Certificates stored on a Smart Card, USB token or a MicroSD card. Moreover, we use Client, SDK and Platform components to apply an electronic signature not only with our digital certificates but also in cases in which the signer already has a Local Certificate released by another Certification Authority or Trust Service Provider.

Automatic Signatures

Automatic signature is a special type of Qualified Electronic Signature that makes it possible to automatically execute a signature on a large number of documents from a customer application (e.g.: e-invoice signature, company contract acceptance, etc.).

Qualified Electronic Signatures

Some use cases, industries and countries demand certificate-based personal digital signatures. In those cases, the highest legal value of a signature – which is legally deemed to be equivalent to a wet ink on paper signature – can only be realized by using certificated based signatures. This generally applies to the so-called Qualified Electronic Signatures (QES) used in the European Union under the eIDAS Regulation.

Remote Signatures

A QES Remote Signature is essential in several scenarios, especially in cases where the document recipients need to sign remotely without the need to use USB tokens or Smart Cards with local certificates.
To execute a Remote Signature user needs to input a PIN and a One Time Password (OTP) to access his Digital Certificate stored on a tamperproof Hardware Security Module (HSM).
Namirial provides Qualified Certificates, Clients, Apps, SDKs and Platforms for Remote Electronic Signature that ensure proper process execution, maximizes automation of all steps, and only raise alerts and reminders if something goes wrong.

Remote Electronic Signing Trust Platform is based on digital certificates with keys stored in eIDAS compliant Hardware Security Modules.

With Remote Electronic Signing, the same architecture can be used to provide different level of signature strength and several OTP mechanisms are supported for two-factor authentication, including Biometric Authentication systems.

TIS - Objektni Informacijski Sustavi d.o.o.
Heinzelova 33, 10 000 Zagreb, Hrvatska
OIB: 62434408100

Video Identification

Activating a Qualified Certificate requires identification performed by a Registration Authority Operator. For highest levels of security and especially for onboarding face-to-face indentification is preferred. This is of utmost importance because the Qualified Certificate is the electronic equivalent of an ID document and it identifies and qualifies an individual or an entity in a digital way.

Video Security Identity (ViSI) Platform allows remote web identification where a user interacts with a Remote Operator in order to perform the identification procedures needed to release an eIDAS compliant Qualified Certificate. The ViSI platform provides security procedures approved by the National Supervisory Body to mitigate the risk of frauds and identity theft.

The User can be identified electronically using ViSI from any PC equipped with a webcam (no client installation required) or through the use of the ViSI app for iOS.

Once the identification process is complete, the Operator starts the enrollment to release a Qualified Certificate to the identified User.

Features

Document Manipulation

- Work with digital documents as with paper documents.
- Define signature fields, signing order, form fields. Automatically define signature field position based on document category and content.
- Fill Out the Document.
- Add temporary annotations and guide customer through the process.
- Add attachments and Scans.

Versioning

Document versioning is fully supported throughout the signing process. Hash value is assigned to each signature which, together with pdf versioning feature, enables clear visibility of all activities applied on the document. In more complex processes documents may be updated even after some signatures have already been applied. In such cases, existing signatures remain valid for related document version.

Signature flow

- Document ceremony per user
  - Obligatory and optional tasks (e.g. signature fields)
- Envelopes
  - Include multiple documents into one transaction
- Routing to multiple recipients
  - Sequentially for multi-step approvals

    - Bulk for parallel sign-offs
- Reminders & alerts
    - Automatically remind recipients
    - Automatically alert senders that recipients did not sign or access documents yet
- Document status overview
    - View document status (e.g. viewed, signed, rejected)
    - Organize documents (Inbox, Sent, Templates)
- Document archive
    - Integrated or external system

Biometric Authentication and Signature Verification

Biometric Authentication platform provides a signature verification that authenticates a signature against a pre-enrolled signature profile database in real time. This allows you to not only secure the execution of certain transactions, but also to provide a ready-to-use audit trail in case of a dispute, thus placing the burden of proof immediately on the signer.

Implementation/deployment

TIS eSIG can be deployed in private or public infrastructure without any loss of features and functionality. The choice is solely customers' and doesn't affect eSIG feature set.

Service in the Cloud

TIS eSIG solution can be provided as cloud service, eliminating needs for local resources. Cloud service is private for customer. We don't recommend multitenancy, even though we can support it.

On Premise

Usual and preferred deployment option is having it installed on premise, in private data center, with supervision provided by internal resources. It is still widely accepted that this way maximum level of security and autonomy is provided.

Hosted in Data Center of Choice

TIS eSIG can be deployed in any data center preferred by customer. We can provide list of permissions and other security settings which enable integration with any other system, either local or remote.