Namirial DTM

Identifying requirements for E-Signing
Agenda

• Brief Introduction Namirial
• Key goals and mission for e-signature implementation
• Signature terminology – legal and technical
• Typical use cases and their requirements – legal and technical
• Process orchestration and results
• Qualified e-signatures – requirements and processes
• ... and much more ...
Q&A “on the go” – Ask anytime!
**Qualified Trust Service Provider**
conform to EU-Regulation 910/2014 eIDAS

Headquarters in Senigallia, Italy

**20** Offices – also in Austria, Brazil, Germany and Romania

**430** Employees (August 2019)

**43 Mio Euro** Consolidated Turnover (FY 2018)

Certified according to
**ISO 27001:2013** – Information Security
**ISO 9001** – Quality Management
Experience horizon in banking, insurance, automotive

Banking and Finance
- UniCredit
- Rocheifen
- Poste Italiane
- Intesa Sanpaolo
- Moneta
- BNL
- BNP Paribas
- Regia Bank
- BIL
- TBI Bank
- Pireaus Bank
- Eurobank
- Fineco
- Summilinking Benefit
- Credito Comm.
- MTS
- Bred
- MutuOnline.it
- Gruppo Banca Carige
- Belfius
- Handelsbanken
- Cofidis
- MoneyGram

Insurance
- Reale Group
- HDI
- Allianz
- Foyer
- SwissLife
- Helvetia
- Öster
c<br>icheische
b
- E
- V
d
- MetLife
- Triglav
- Pramerica

Telecommunication
- T-Mobile
- Vodafone
- Orange
- Sky
- kpn Bel Company
- The Phone House
- Cellcom
- melta
- Wind
- Summer Mobile
- Mtn
- MTN
- NASHUA Mobile
- Turk Telekom
- Vivacom

Automotive
- Daimler
- BMW
- Ducati
- FCA
- Skoda
- Jaguar

Utilities
- ZSE
- RWE Group
- Latvenergo
- Russian Railways
- MetLife
- SNAM
- E-Work Wels
- Citgo
- Pubblacqua

Government
- Department for Work & Pensions
- INSEEC
- AVEPA
- Botanic
- CONAD
- BOC
- Olympus
- Maquet
- Medicon
- Vaillant
- Orange
- It Working
- Lenovo
- Business Software
- Vaillant

Retail
- Swatch
- L'Oréal
- Marionnaud
- Eismann

Other Industries
Namirial – Key Numbers in Digital Transaction Management

> 800 Mio. Transactions per year executed with Namirial SaaS solutions

> 1 Mio. Electronic certificates per year as basis for eSignature / eSeal

> 3 Mio. Signatures created on peak days with Namirial SaaS solutions

> 385,000 Workplaces equipped for handwritten signature capture – incl. biometric characteristics

> 5 Mio. Biometric signature user profiles handled by Namirial customers

~ 180 Mio. Documents securely stored in Long Term Archive

> 500,000 Active accounts of electronic registered delivery service

> 120,000 Customers of electronic invoicing platform

100+ Partners in business area of Digital Transaction Management

50+ Countries with customers using Namirial solutions

Numbers above as of August 2019
Key goals & mission for e-signature implementation

**GOALS**
- **Reduced Process Costs**
  - Respond to falling margins

- **Accelerated closures**
  - Stay ahead of competition

- **Compliant Processes**
  - AMLD, GDPR, PSD2, etc.

- **Delighted customers**
  - “Harvest” good reviews

**MISSION**
- **Remotely (external / internal)**
  - easy and trustworthy

- **In-person (branch office / field)**
  - with appropriate legal level and evidence (eIDAS)

- **According to a defined workflow and ceremony**
  - Anywhere, anytime, on any device
Signature terminology - Legal & technical terms

Legal terms
from EU Regulation 2014/910 eIDAS

Natural person
Electronic signature

Legal person
Electronic seal

in levels
basic – advanced – qualified

Applicability regulated
in national legislation

Technical terms

Digital signature
Electronic signature creation based on cryptography using an e-signing certificate

Remote certificate
(Qualified) e-signing certificate that a QTSP manages on behalf of its holder to simplify the creation of (qualified) e-signatures

In-person vs remote e-signing
Scenario describing how e-signatures from clients are captured

Biometric signature, Click2Sign, etc
Various signature capture methods
**Signature Capture Methods**

**Native capture (of handwritten signatures)**
- Makes use of native pens (e.g. signature pads, Apple Pencil, Samsung S Pen) for high data rate and palm detection
- Captures behavioral biometrics for verification against samples (by handwriting experts or verification software)
- Requires a native capture app and a pen (like on paper) – best used for in-person e-signing
- Satisfies the requirements for advanced e-signature

**HTML5 capture**
- Click („click-to-sign“), text entry (e. g. name, „type-to-sign“) or drawing („draw-to-sign“)
- Directly in the Web browser without native app – best used for remote e-signing
- Requires additional authentication to become an advanced e-signature

**PKI certificate capture** – issued to the signatory, typically used for qualified e-signatures in eIDAS
- Local certificate – requiring native app and local qualified signature creation device (QSCD)
- Remote certificate – simply accessed from a Web browser
  - Disposable (or short-term) certificates for simplified usage within one user session
  - Standard (or long-term) certificates for recurring use
Use Cases – Example Namirial Customer Allianz

IDENTIFIED USE CASES FOR E-SIGNATURE ACROSS DOMAINS

Sales & Distribution
- Intermediary contracts
- Intermediary authorizations
- New policy applications
- Customer advisory protocols

Policy Management
- Risk surveys
- Coverage rejections
- Policy and billing document deliveries
- Payment authorizations
- Changes (account, address, beneficiary)
- Medical releases
- Power of attorneys
- Statement of loss

Claims & Assistance Management
- Questionnaires
- Payment forms
- Service and assistance order creations, cancellations, dispositions
- Litigation management forms

Provider & Partnership Network Management
- Service provider & partner contracts (e.g. consulting contracts)
- Procurement paperwork (e.g. NDAs)
- Cooperate benefits contracts

Finance
- Approvals
- Budget shifts
- Delegations of authority

Human Resources
- Candidate NDA
- Offer letters
- Employee policy distribution and signature
- Expat paperwork

Legal & Compliance
- Individual agreements, contracts, non-disclosures
- Compliance instructions

Other Functions
- Audit signoff
- Finance agreements
- Investment contracts
- Reinsurance contracts
- Facility management contracts

Source: Presentation „Taking Signatures Seriously - Accelerate digital adoption while meeting global requirements “ – Hermann A. Lammer – Allianz, Efma Insurance Summit Vienna; June 13, 2019
<table>
<thead>
<tr>
<th><strong>Use cases – eSignatures for proof of intent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact with ...</strong></td>
</tr>
<tr>
<td>Customers B2C</td>
</tr>
<tr>
<td>- Contract - purchase, maintenance, service, repair, ...</td>
</tr>
<tr>
<td>- Order</td>
</tr>
<tr>
<td>- Protocol - consultation, testing, production steps</td>
</tr>
<tr>
<td>- Proof - rendered service, delivery</td>
</tr>
<tr>
<td>- Application - Account Opening, Insurance ...</td>
</tr>
<tr>
<td>- SEPA Direct Debit Mandate</td>
</tr>
<tr>
<td>- Damage reports</td>
</tr>
<tr>
<td>- Power of attorney</td>
</tr>
<tr>
<td>- <strong>Finance contracts (credit and leasing)</strong></td>
</tr>
<tr>
<td>- <strong>Rental agreements</strong></td>
</tr>
<tr>
<td><strong>Business Partners B2B</strong></td>
</tr>
<tr>
<td>- Contract - partnership, resale of goods</td>
</tr>
<tr>
<td>- <strong>Non-Disclosure Agreement (NDA)</strong></td>
</tr>
<tr>
<td><strong>Employees B2E</strong></td>
</tr>
<tr>
<td>- Employment contracts <strong>(temporary employment)</strong></td>
</tr>
<tr>
<td>- Taking note - working instructions on data protection (GDPR), ...</td>
</tr>
<tr>
<td>- Test report - process documentation, ....</td>
</tr>
<tr>
<td>- Release / approval</td>
</tr>
</tbody>
</table>

*Blue = use cases - at least partially - requiring to integrate qualified e-signatures (QES) in some EU countries*
### How to e-sign?

| **Who**       | Customer, business partner, employee, ...  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One or more signers – sequentially or parallel?</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Presented (in branch and/or in field) or signers own device (remote/self-service)</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Synchronous (sales assisted) or asynchronous (software assisted / unassisted)</td>
</tr>
<tr>
<td><strong>What</strong></td>
<td>Document, transaction – file type e. g. PDF?</td>
</tr>
<tr>
<td><strong>Why</strong></td>
<td>Legal (written form) and/or business requirement (proof of intend)</td>
</tr>
</tbody>
</table>

### How to implement?

<table>
<thead>
<tr>
<th><strong>Integration</strong></th>
<th>Standalone UI, Standard Connectors or Custom API Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delivery</strong></td>
<td>On-premise or SaaS application</td>
</tr>
</tbody>
</table>
Major legal requirements

Form Requirements

• Written Form Requirements in Commercial Law or Civil Law – e.g. German BGB
• Regulations defined by industry organizations / bodies

Privacy Requirements

Process Steps: Consent – Processing – Archiving
• General Data Protection Regulation (GDPR)
  -> Conflict potential with US Clarifying Lawful Overseas Use of Data (CLOUD) Act

Know Your Customer (KYC) Requirements – Identification

• Anti-Money Laundering Directive (AML) or application for telecommunication services
  o Account Opening, Applying for Life Insurance
  o SIM card registrations for mobile phones
• Implemented by national law and monitored by financial supervisory authorities
## Scenario – Direct vs. indirect contact

### WHO & WHERE?

<table>
<thead>
<tr>
<th>WHO &amp; WHERE?</th>
<th>Direct / on-site contact</th>
<th>Online / remote contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>face-to-face</td>
<td>via video (LiveID), eID</td>
</tr>
<tr>
<td>(if required – e.g. for QES or AML)</td>
<td>in office / in field</td>
<td>via smartphone, tablet, laptop...</td>
</tr>
<tr>
<td>Authentication</td>
<td>Behavioral biometrics</td>
<td>PIN and/or SMS-OTPs</td>
</tr>
<tr>
<td>(if required)</td>
<td>PIN and/or SMS-OTPs</td>
<td>3rd party identity provider</td>
</tr>
<tr>
<td>Capture of intend</td>
<td>on employee device</td>
<td>on customer device</td>
</tr>
<tr>
<td>(signature)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Namirial – All rights reserved
Integration of e-signing in business processes

Pre-Signing
auto-created
& auto-presented

Post-signing
auto-post processed
auto-archived

Powerplay – Fast forward: Acquire signatures in minutes instead of days anywhere, on any device, signing in-person or remote
Evidence in the signed document itself

- Digital signature / seal*
- Digital certificate for signing/sealing* (AATL compliant, opt. qualified)
- Proof about the validity of the used signature certificate at signing time (OCSP / CRL)
- (Trusted) signing time
- Digital signature imprint

Additional Evidence

- Geolocation
- Behavioral biometrical data from the handwritten signature

Evidence in the corresponding sealed process documentation (audit trail)

- Envelope ID with hashes of embedded documents
- Sent notifications and recipient addresses
- Authentication protocol (e.g. PIN, SMS-OTP, etc)
- Accepted agreement dialogs
- Reader IP address
- Reader location (optional)
- Date & time of action
- All actions such as
  - Pages opened
  - Confirmations
  - Form field edits
  - Signatures incl used signing method

* of customer systems or Namirial Trust Services – depending on use case and regulation per geography

** capable of handling digital signature fields in PDF files according to ISO 32000
Significant differences in the approval of procedures for the identification of users of qualified certificates according to Art. 24 eIDAS in Europe
**Holder identification** through Local Registration Authority (LRA)

<table>
<thead>
<tr>
<th>Identification</th>
<th>Certificate</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Contact</td>
<td>Virtual Contact online</td>
<td></td>
</tr>
</tbody>
</table>

**Citizens**
- AML directive
- Face 2 Face
- eID via ID Card
- QES
- Trusted 3rd party
  - Notary
- AML directive (national ruling)
  - eKYC (video ID) through agent/robot
  - Giro ident (fall back of AML done by other institute)
- Video ID – Namirial ViSI process
- QES
- eID via ID Card - via card reader or NFC

**Employees**
- Employer
Certificate request from the holder
QES execution using the issued certificate

Identification

Certificate

Signature

Disposable Certificate

SMS-OTP authentication

Long-term Certificate

2-factor authentication

Automatic signature / seal

Access PIN is defined in the Org Settings
Digital process in direct contact at POS

**Customer**

Sam Smith

ID Card / Passport
Smartphone

**Customer Service Agent at Dealership**

Terminal / Tablet with POS system access

**Trust Service Provider**

Namirial

Server Platform with Hardware Security Module (HSM)

Identification according to AML*

Certificate request form

Authentication via TAN entry

Transmission One-Time Password (OTP) via SMS

Request certificate

Customer copy

ECM archive of captive

Start certificate provisioning process for “Disposable”

Provisioning & execution of Qualified Electronic Signature (QES)

* Existing customer: No identification required

Start Namirial-Workflow Orchestration Signature Process

© Namirial – All rights reserved
E-Signature vendor selection check list

- Truly meeting global compliance (GDPR) and security requirements
- In-house one-stop offering of eIDAS certified Trust Service Provider
- Support of all channels – remote via internet and in-person (POS)
- Full white-labeling and integration of an organization’s own digital certificates
- Flexible deployment - SaaS (public, private, managed) or on-premise
- Multiple options for core system integration and virtualized IT environments
- Taking handwritten signatures seriously (not just click-to-sign and PKI) including certified signature capture device support
- Vendor flexibility in terms of integration support (new features & connectors)
- Fully committed personal support - also for new product and business development

Enable customers, dealers and employees to sign fast, efficient and legally binding