Namirial DTM

Identifying requirements for E-Signing

Klaus Fellner
VP Sales & Alliances

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!

Namirial Facts & Figures

Qualified Trust Service Provider
conform to EU-Regulation 910/2014 eIDAS

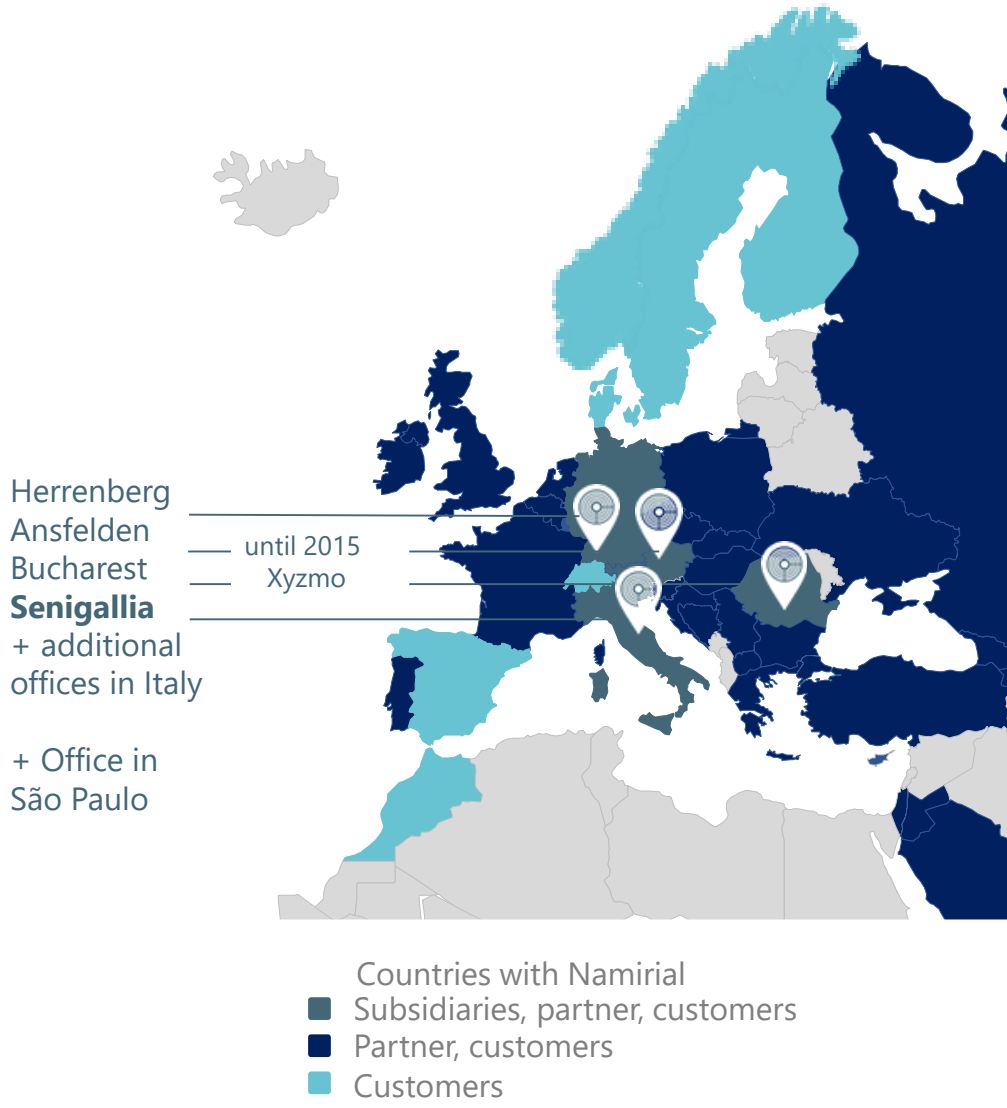
Headquarters in Senigallia, Italy

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



© Namirial – All rights reserved

Experience horizon in banking, insurance, automotive

Banking and Finance

Insurance

Telecommunication

Automotive

Utilities

Government

Retail

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

© Namirial – All rights reserved

Key goals & mission for e-signature implementation

GOALS

Reduced Process Costs

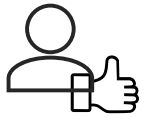
Respond to falling margins

Accelerated closures

Stay ahead of competition

Compliant Processes

AMLD, GDPR, PSD2, etc.



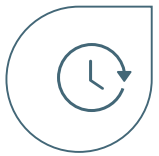
Delighted customers

"Harvest" good reviews

MISSION

Remotely (external / internal)

In-person (branch office / field)



According to a defined workflow and ceremony

easy and trustworthy

with appropriate legal level and evidence (eIDAS)

Anywhere, anytime, on any device

© Namirial – All rights reserved

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

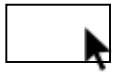
Biometric signature, Click2Sign, etc
Various signature capture methods

© Namirial – All rights reserved

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

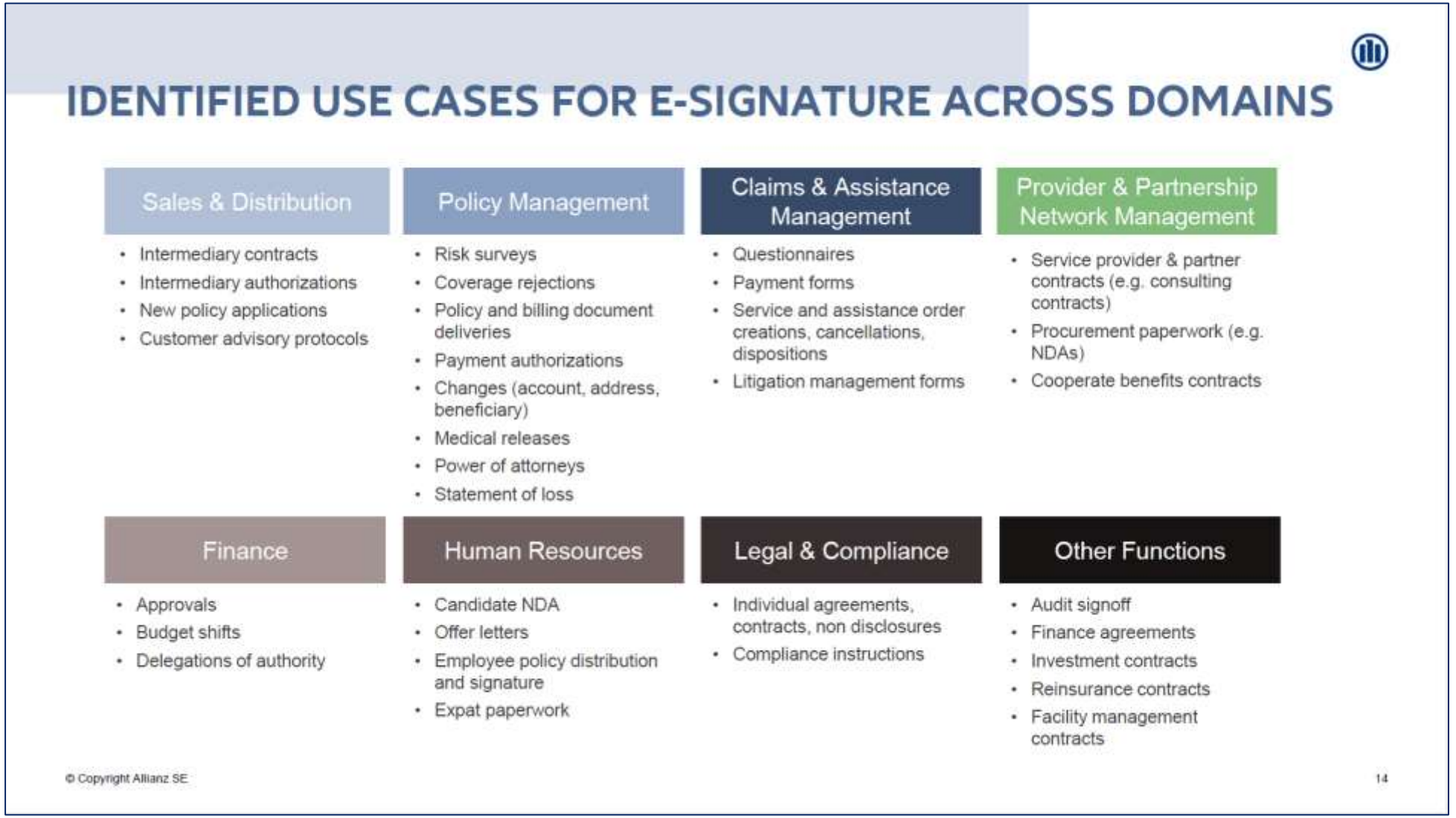
- Click („click-to-sign“), text entry (e. g. name, „type-to-sign“) or drawing (“draw-to-sign”)
- Directly in the Web browser without native app – best used for remote e-signing
- Requires additional authentication to become an advanced e-signature

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

© Namirial – Alle Rechte vorbehalten

Use Cases – Example Namirial Customer Allianz



Source: Presentation „Taking Signatures Seriously - Accelerate digital adoption while meeting global requirements " – Hermann A. Lammer – Allianz, Efma Insurance Summit Vienna; June 13, 2019

© Namirial – All rights reserved

Use cases – eSignatures for proof of intent

Contact with …	
Customers B2C	▪ Contract - purchase, maintenance, service, repair, … ▪ Order ▪ Protocol - consultation, testing, production steps ▪ Proof - rendered service, delivery ▪ Application - Account Opening, Insurance … SEPA Direct Debit Mandate ▪ Damage reports ▪ Power of attorney ▪ Finance contracts (credit and leasing) ▪ Rental agreements
Business Partners B2B	▪ Contract - partnership, resale of goods ▪ Non-Disclosure Agreement (NDA)
Employees B2E	▪ Employment contracts (temporary employment) ▪ Taking note - working instructions on data protection (GDPR), … ▪ Test report - process documentation, …. ▪ Release / approval

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

© Namirial – All rights reserved

Lead question for requirements identification

How to e-sign?

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

How to implement?

Integration	Standalone UI, Standard Connectors or Custom API Integration
Delivery	On-premise or SaaS application

© Namirial – All rights reserved

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

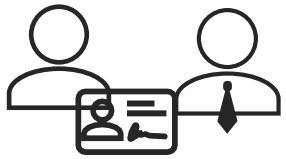
- General Data Protection Regulation (GDPR)
  -> Conflict potential with US Clarifying Lawful Overseas Use of Data (CLOUD) Act

Know Your Customer (KYC) Requirements – Identification

- Anti-Money Laundering Directive (AML) or application for telecommunication services
  - Account Opening, Applying for Life Insurance
  - SIM card registrations for mobile phones
- Implemented by national law and monitored by financial supervisory authorities

© Namirial – All rights reserved

Scenario – Direct vs. indirect contact

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

© Namirial – Al rights reserved

Integration of e-signing in business processes

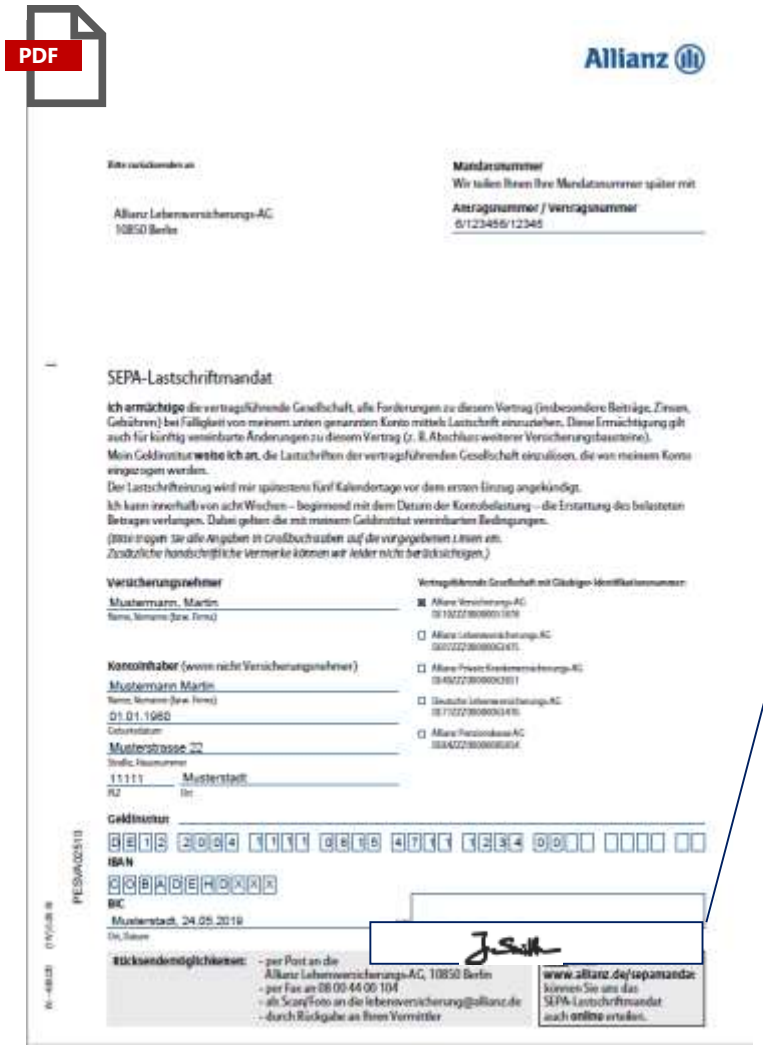
Pre-Signing
auto-created
& auto-presented

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

© Namirial – Alle Rechte vorbehalten

Evidential weight in document & audit trail



Evidence in the signed document itself

Digital Signature Field (PAdES)**

- 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)
- Document history
- (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

© Namirial – All rights reserved

eIDAS Qualified Trust Services - Supervision & Authorization

Supervision of trust services
by national authorities, e. g.
Agenzia per l'Italia digitale (AgID)

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Assessing conformity
to requirements of eIDAS
in Italy on behalf of AgID

in case of Namirial: Bureau Veritas

BUREAU VERITAS
Certification

EU Trusted List (EUTL)
listing through AgID

https://webgate.ec.europa.eu/tl-browser/#/

Significant differences in the approval of procedures for the identification of users of qualified certificates according to Art. 24 eIDAS in Europe

© Namirial – All rights reserved

Holder identification through Local Registration Authority (LRA)

	Physical Contact	**Virtual Contact** online

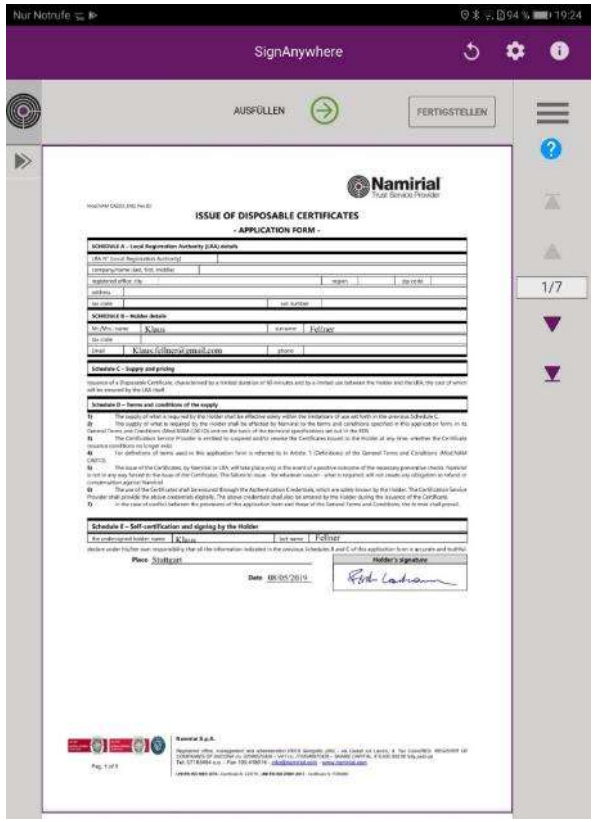
Citizens	• **AML directive**
	• **Face 2 Face**
	• **eID via ID Card**
	• **QES**
	• **Trusted 3rd party**
	  • Notary
		• **AML directive (national ruling)**
		  • eKYC (video ID) through agent/robot
		  • Giro ident (fall back of AML done by other institute)
		• **Video ID – Namirial ViSI process**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

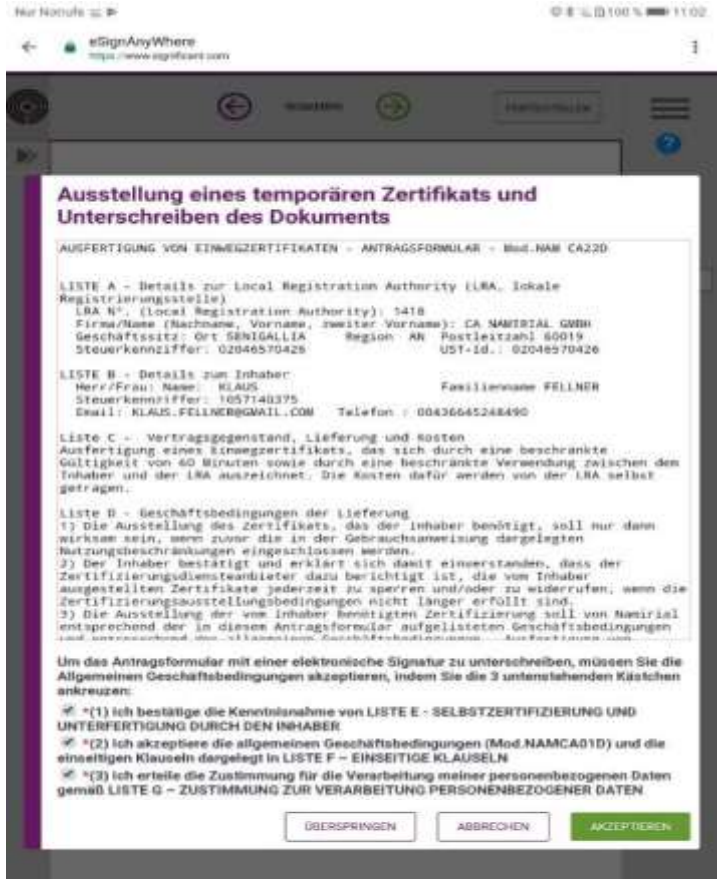
Employees	• **Employer**	

© Namirial – All rights reserved

Certificate request from the holder

Identification → Certificate → Signature



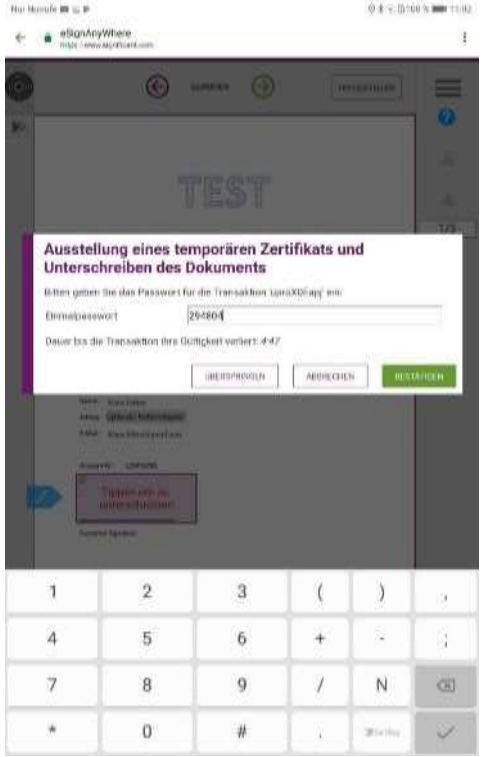


© Namirial – All rights reserved

QES execution using the issued certificate

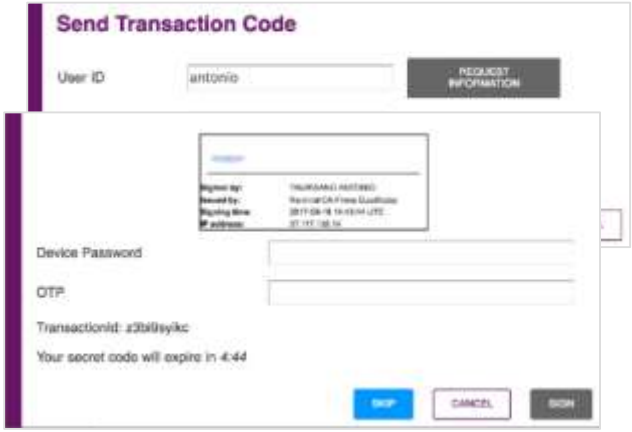
Identification → Certificate → Signature

Disposable Certificate



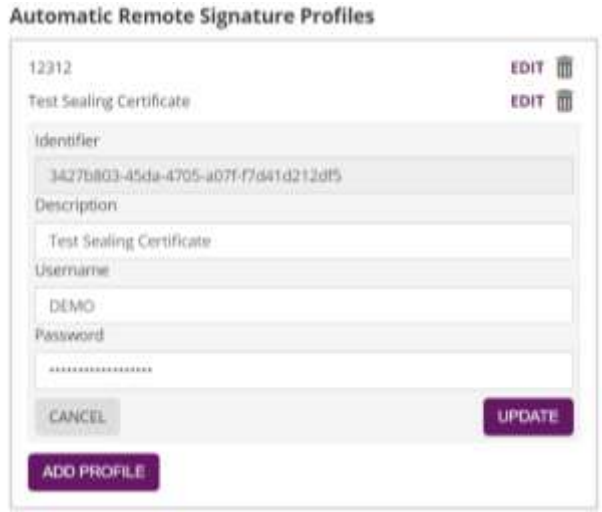
SMS-OTP authentication

Long-term Certificate



2-factor authentication

Automatic signature / seal



Access PIN is defined in the Org Settings

© Namirial – All rights reserved

Digital process in direct contact at POS

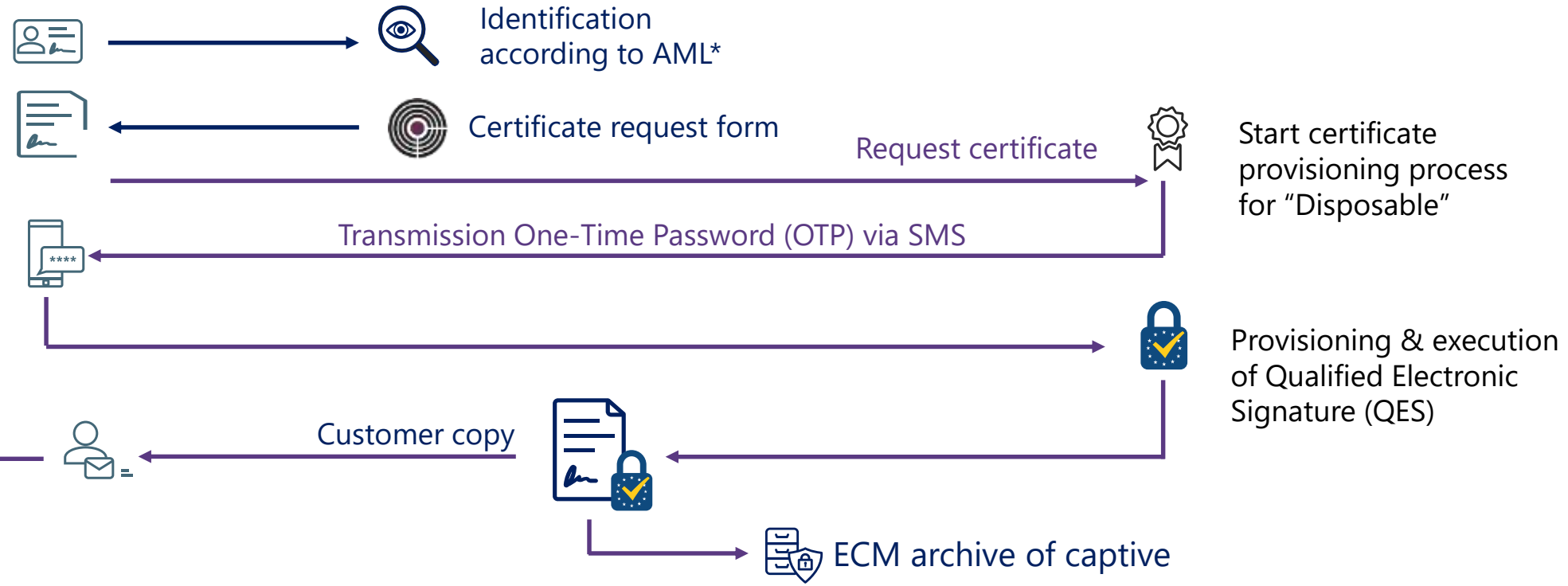
Customer
Sam Smith

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)



* 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

© Namirial – All rights reserved

Q&A

Klaus
Managing Director
Namirial Germany

TBD