JANUARY 26, 2018 9:00-12:00

DISCUSSION ON THE FUTURE REGULATION OF REMOTE ELECTRONIC IDENTIFICATION AND ONBOARDING

WATCH ONLINE

AT COBALT
LEGAL
FACEBOOK PAGE

HTTP://EJ.UZ/
DISCUSSION2601

Association of Latvian Commercial Banks

LATVIJAS UNIVERSITATE
ANNO 1919

COBALT

Microsoft

9:00 – 9:05

Welcome by

SANDA LIEPIŅA

CHAIRMAN OF THE MANAGEMENT BOARD OF THE ASSOCIATION OF THE LATVIAN COMMERCIAL BANKS (ALCB)

Development

Technology

Compliance

KEYNOTE DEMOS: REMOTE IDENTIFICATION AND AUTHENTICATION TOOLS AS EXPERIENCED BY USERS AND PROVIDERS

9:05-9:40

ANKE ULRICH, LL.M

Senior Legal Counsel, Head of Anti Financial Crime & AML N26 Bank, Germany

JĀNIS BOKTA

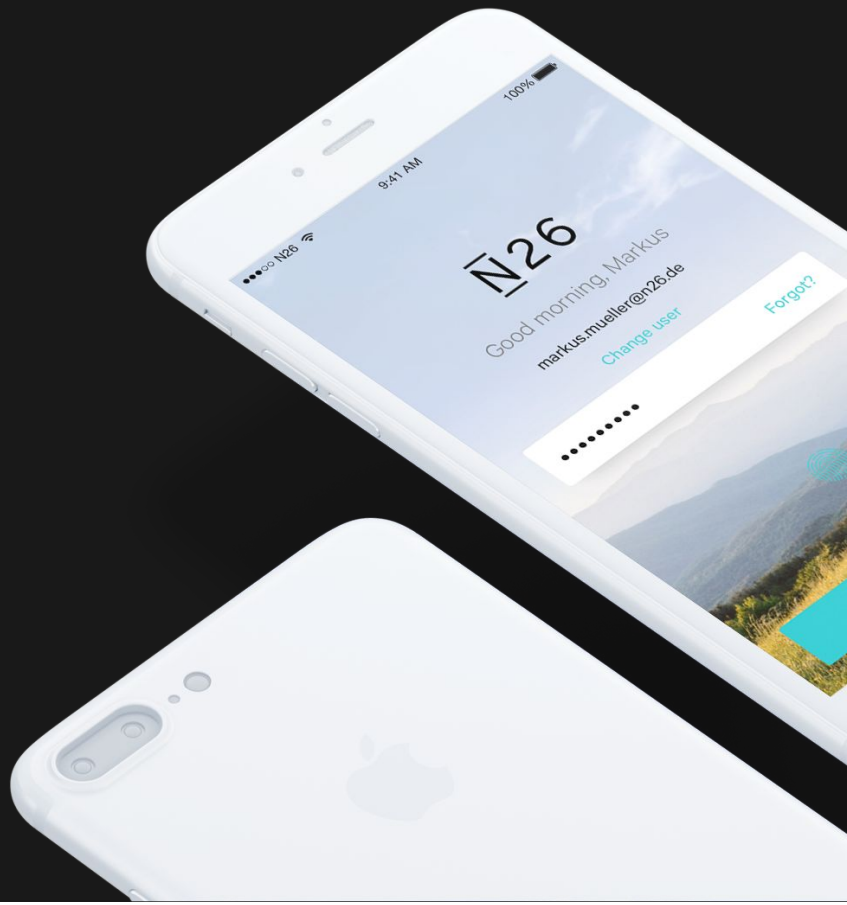
Chairman of the Management Board of Latvia State Radio and Television Centre (LVRTC)

DMITRIJS KAČANOVS

Chairman of the Association of Latvian Payment Service Providers and Electronic Money Institutions (LMENA)

N26

Remote Identification
Video-Identification



Anke Ulrich, N26 Bank GmbH

January 26th, 2018

Agenda

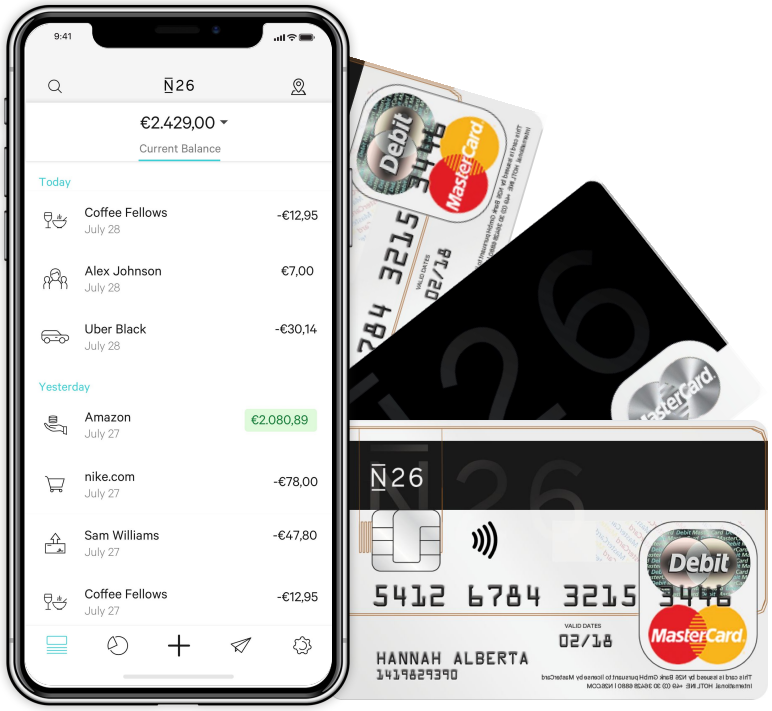
- N26 Vision & Facts
- Legal implementation Video-KYC
- Requirements for Video-KYC
- Practical experience
- Outlook

N26 Vision & Facts

N26 Solution

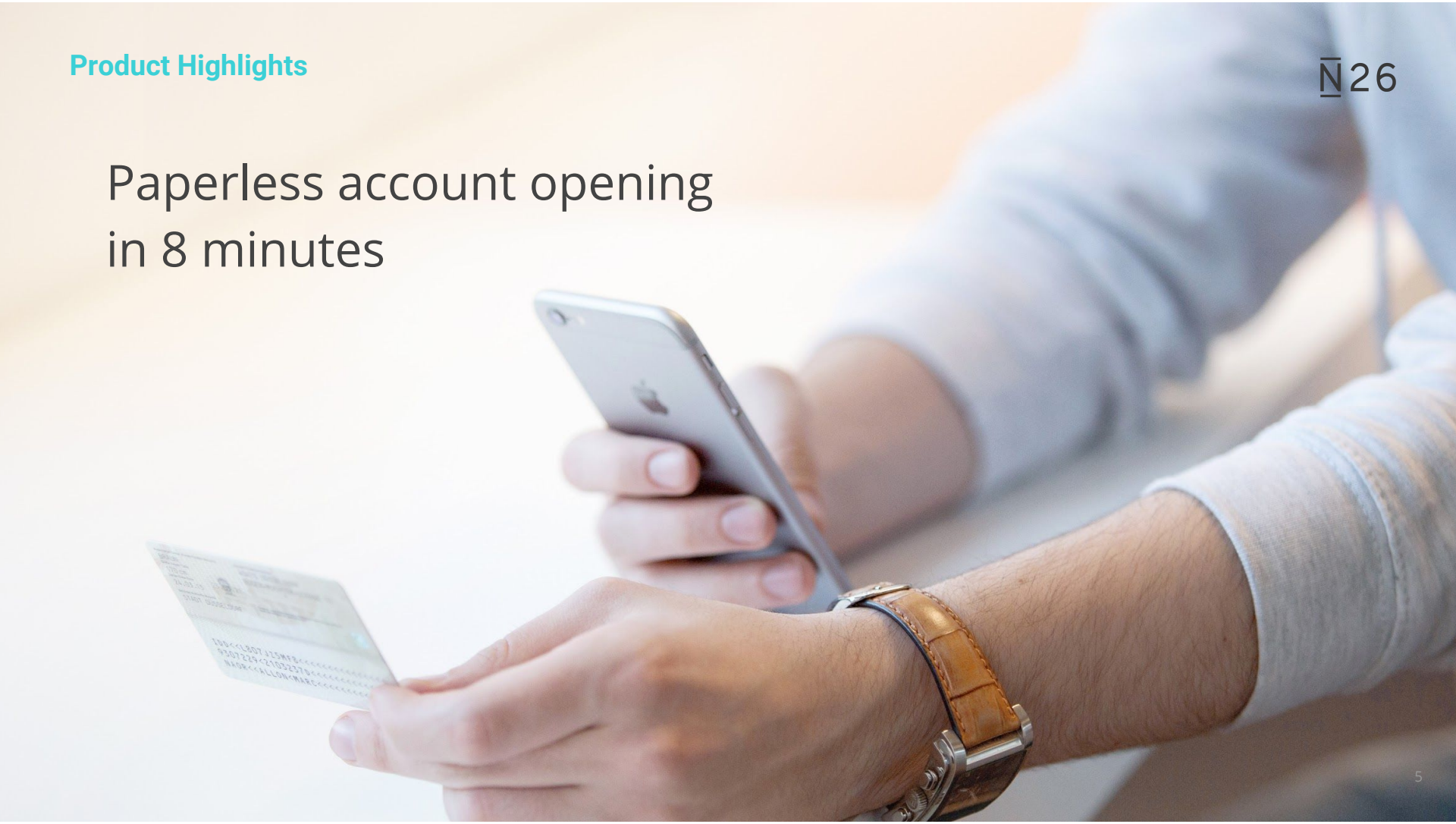
A bank the world loves to use

- Scalable, modern infrastructure
- First fully mobile bank account
- Superior user experience



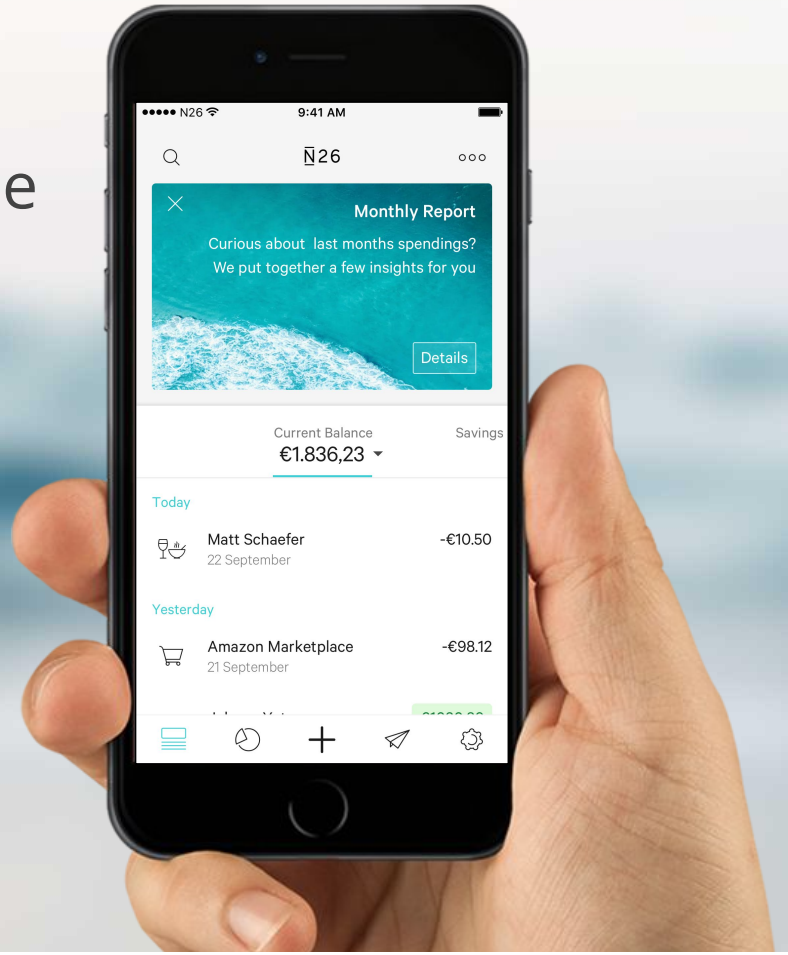
N26

Paperless account opening in 8 minutes



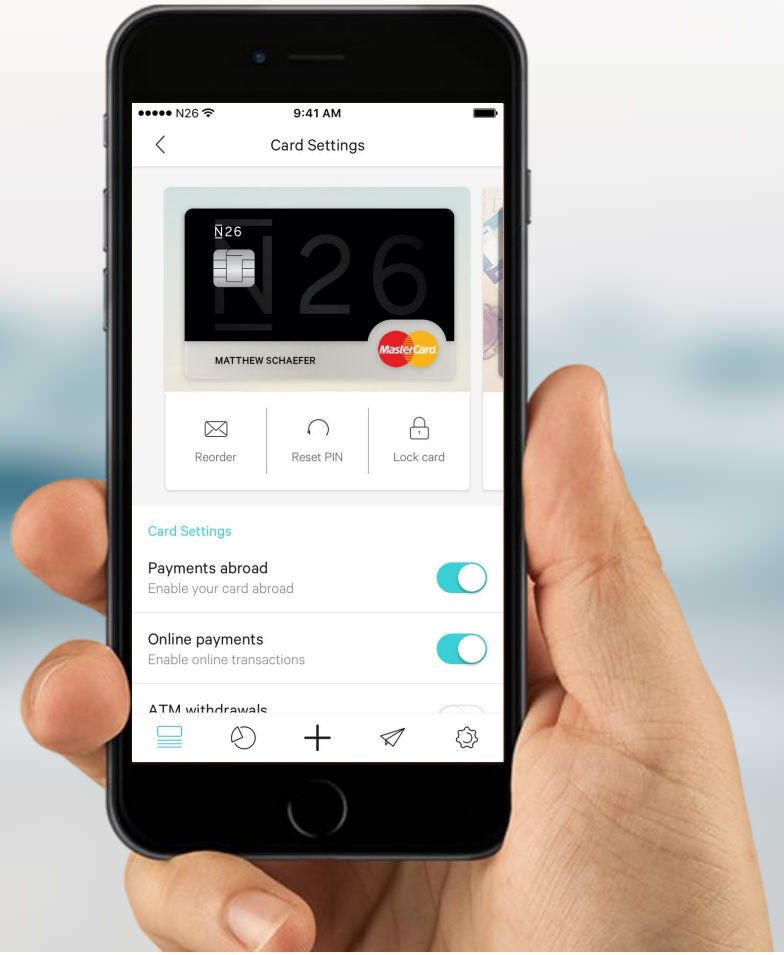
Product Highlights

Complete Bank account with real-time statistics and insights



Product Highlights

Full control
over N26 cards
directly in the app



Strategy of N26

Building a FinTech hub

... providing the best products either in-house or in cooperation with innovative partners

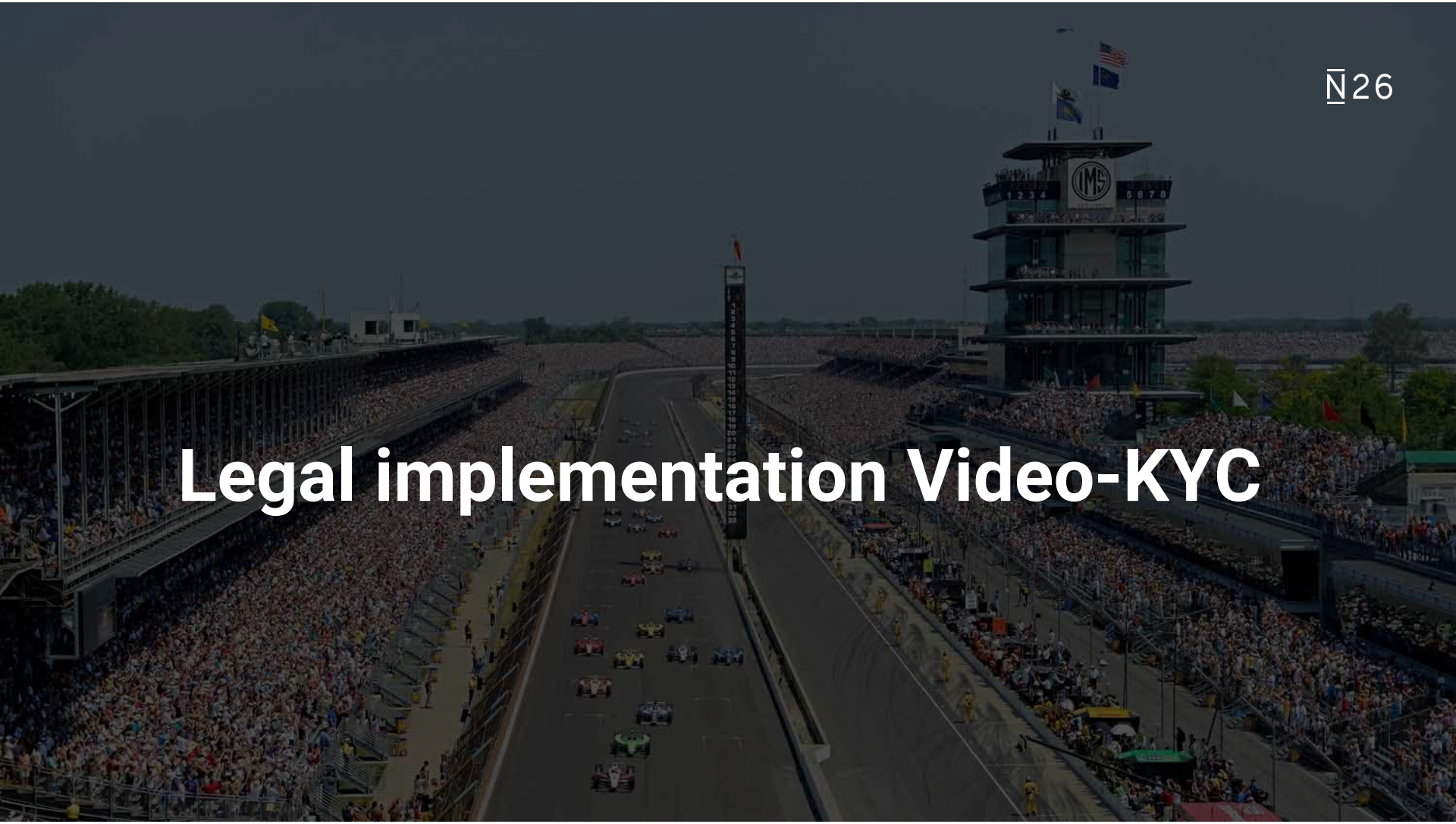
Becoming the first pan-European Bank

… successive expansion by passporting across the European Economic Area

Founding History

Most important milestones

January 2015:	Launch of N26 Account in collaboration with Wirecard Bank AG in Germany and Austria
April 2015:	$10m Series A Investment led by Valar Ventures
October 2015:	Application for full banking license handed in at BaFin
May 2016:	$40m Series B Investment led by Horizons Ventures
July 2016:	Granting of banking license from the ECB (Depository, Credit, Investment Brokerage)
August 2016:	Passporting of banking license to 16 €-currency markets, including Spain specifically for cross border services
October 2016:	Launch of N26 Bank



Legal implementation Video-KYC

Legal implementation Video-KYC

Identification & Verification Procedure

- Identification of a natural person (Sec. 11 (4) No. 1 German AML Act):
  - first name and surname,
  - place and date of birth,
  - nationality and
  - address;
- Verification of a natural person (Sec. 12 (1) No. German AML Act):
  - valid official identification card which includes a photograph of the holder and satisfies German requirements for identification cards and passports, including, in particular, German passports, personal identification cards or their substitutes, or passports, personal identification cards or their substitutes recognised or accepted under German provisions on foreign nationals

Legal implementation Video-KYC

Accepted KYC-methods before 4. AML Directive

- Face to Face, natural person is physically present (sec. 4 German AML Act)
  - Verification with personal presence of customer providing ID-document
- Non Face to Face, natural person is physically not present (sec. 6 (2) No. 2 German AML Act, EDD)
  - a certified copy of a document and 1st incoming transaction*
  - electronic identification function referred to in sec. 18 of the Personal Identification Act
  - Qualified Digital Signature (QES) as defined in 2 no. 3 of the German Signature Act and 1st incoming transaction
  - Performance of third parties, KYC Reliance through regulated entity or outsourcing partner (sec. 7 German AML Act)

*transaction carried out directly from a payment account as defined in section 1(3) of the Payment Services Supervision Act held in the name of the contracting party with an institution as defined in section 2 (1) no. 1 or 2a or with a credit institution domiciled in an equivalent third country

Legal implementation Video-KYC

Accepted KYC-methods after 4. AML Directive

- Face to Face, natural person is physically present
  - Verification with personal presence of customer providing ID-Document (Sec. 13 (1) No. 1) German AML Act)
  - Other procedures which provide the same security standard as defined in No. 1 (Sec. 13 (1) No. 2) German AML Act) LEGAL FOUNDATION for Video-KYC !!!
- Non Face to Face (natural person is physically not present)
  - electronic identification function referred to in section 18 of the Personal Identification Act
  - Qualified Digital Signature (QES) as defined in Art. 3 Nr. 12 Regulation (EU) Nr. 910/2014* and 1st incoming transaction and validation as defined in Art. 32 Regulation (EU) Nr. 910/2014
  - Notified Electronic Identification-System acc. Art. 8, 9 Regulation (EU) Nr. 910/2014
  - Performance of third parties, KYC Reliance through regulated entity or outsourcing partner (Sec. 17 German AML Act)

*Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)


Requirements for Video-KYC

Requirements for Video-KYC

BaFin Circular 01/2014 before 4th AML Directive

- Video KYC not yet implemented in the AML Act.
- BaFin implemented a code of conduct for video KYC via interpretation of Sec. 6 (2) No.2) German AML Act (old version)
- “Personal presence” (Sec. 6 (2) no.2 German AML Act) is fulfilled under the following requirements
  - Prior consent of the customer
  - Trained employees in a secure and separated location to conduct the video KYC
  - ID Check and screenshotting
    - Visual requirements of the ID (optical and holographic security features, ID photo, etc.)
    - Double check ID data and customer data
  - Interaction with customer for security reasons (ID serial no. read & TAN/PIN entered by customer,)
  - KYC process needs to be audio recorded
- Exclusion criteria: inadequate light or insufficient picture quality due to poor transmission quality

Requirements for Video-KYC

BaFin Circular 03/2017 after 4th AML Directive

- BaFin Circular 01/2014 is enhanced
- Trained auditors: instruction of test methods, forgery possibilities and AML & data protection
- Technical and organizational requirements
  - Random allocation of customers to auditors
  - End-to-end encryption (German Federal Office for Information Security (BSI) TR 02102 standard)
  - Transmission quality sufficient to secure doubtless identification
- ID verification (three random security features must be fulfilled)
  - Appropriate ID; forgery-proof, hologram, identigram etc.;
  - Correct spelling of numbers and writings
- Video & audio recording and storage for five years

N26 Practical experience

N26 Practical experience

Video KYC in everyday use - initial challenges

- Developing, implementing and maintaining a software-based guideline for the specialists is time consuming and costly
  - Gathering all applicable IDs data into a database
  - Understanding all specific safety features of the different IDs
  - Maintaining all safety features and applicable IDs in the ID database
- Instruction and training of the specialist/agents
  - Guarantee availability of multilingual agents
  - Making agents aware for multiple “creative” fraudsters
  - Preparing agents for difficulties which can occur in the verification process (e.g. third person in the same room, weird acting customers)

N26 Practical experience

Advantages of Video KYC

- Complete mobil identification of customer possible via smartphone
- Fast and easy way of verification once the process is implemented
- Good photo and video quality of user and verification documents in banks database (downloadable)
- Recording of the customer, which can be provided to the policy & federal agencies on demand for possible prosecution
- Current and detailed data of all customers available
- Video KYC is the only working verification method at the moment for mobile banks in Germany

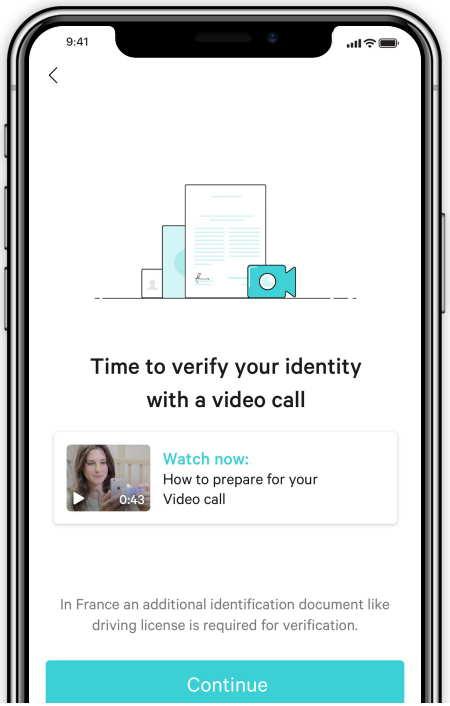
N26 Practical experience

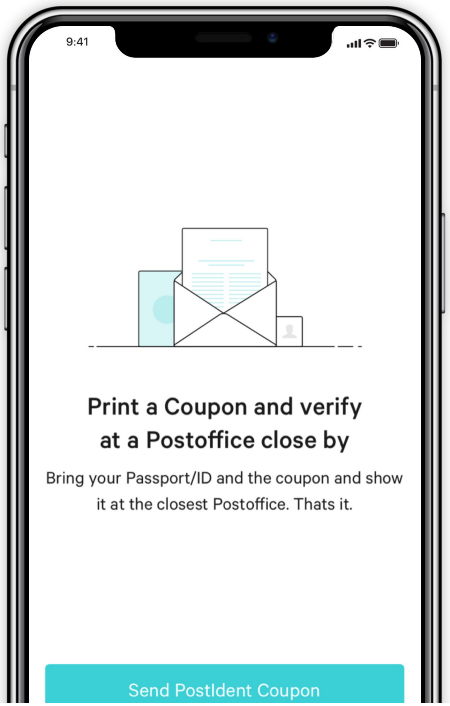
Disadvantages of Video KYC

- Multiple IDs are not suitable for Video KYC due to missing safety features
- High number of failure points (e.g. bad WIFI signal or other technical limitations) resulting in maximum 35% conversion (65% of Video KYC fail)
- Some customers dislike to be filmed and therefore to not use Video KYC
- Language barrier since only key languages are provided
- Discrimination of disabled people (blind, deaf and mute), by making it very difficult for them to complete the process


Outlook

Where we are now





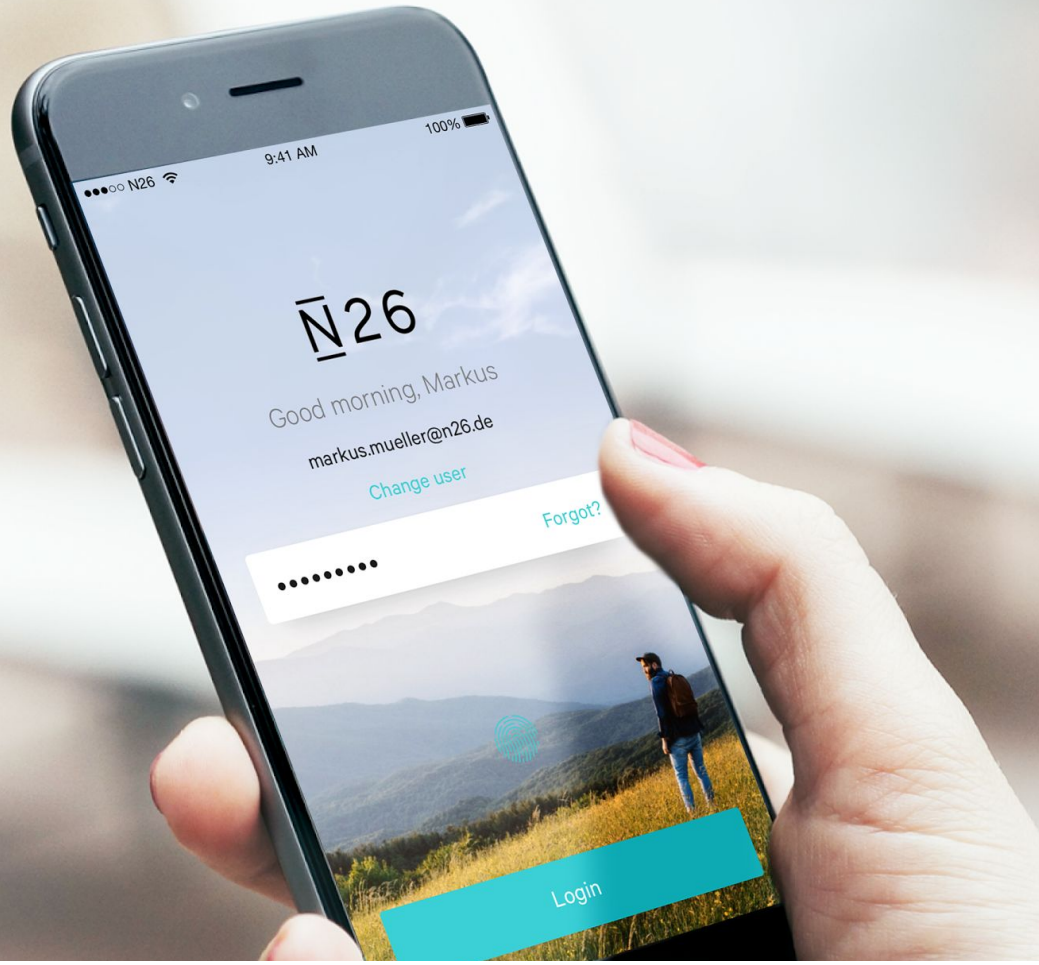
Outlook

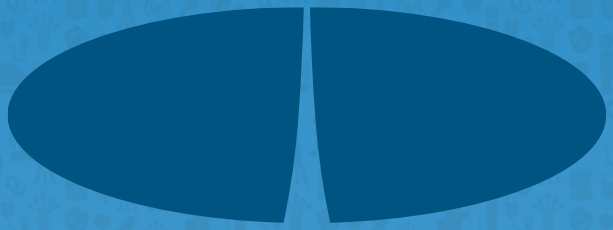
Legislators to encourage multiple KYC verifications

- Current Video KYC process is working but not the most suitable and functioning solution for KYC challenges
- Complex regulations inhibit innovation and practical solutions
- Other EU Member States transposed 4th AML Directive more flexible due to implementing of risk-based approach for NON Face-to-Face (F2F) verification
    - Netherlands: Passport + Selfie etc.
    - France: Passport + ID + Selfie
- Fraudsters will always find their way in - in F2F and non F2F verification
- Multi-factor Authentication services provide practical and safe solutions
- Legislators should create an environment where multiple KYC verifications are enabled
- Making governmental databases available for checkups can increase safety standards

Thank you!

Anke Ulrich, LL.M.
Senior Legal Counsel
Head of Anti Financial Crime & AML
N26 Bank GmbH | N26 Group
Klosterstraße 62 | 10179 Berlin | Germany
https://n26.com/
E-Mail: anke.ulrich@n26.com





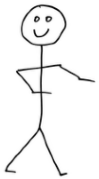
LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS

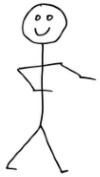
REMOTE ID
BUZZWORD OR TREND LINE

JĀNIS BOKTA

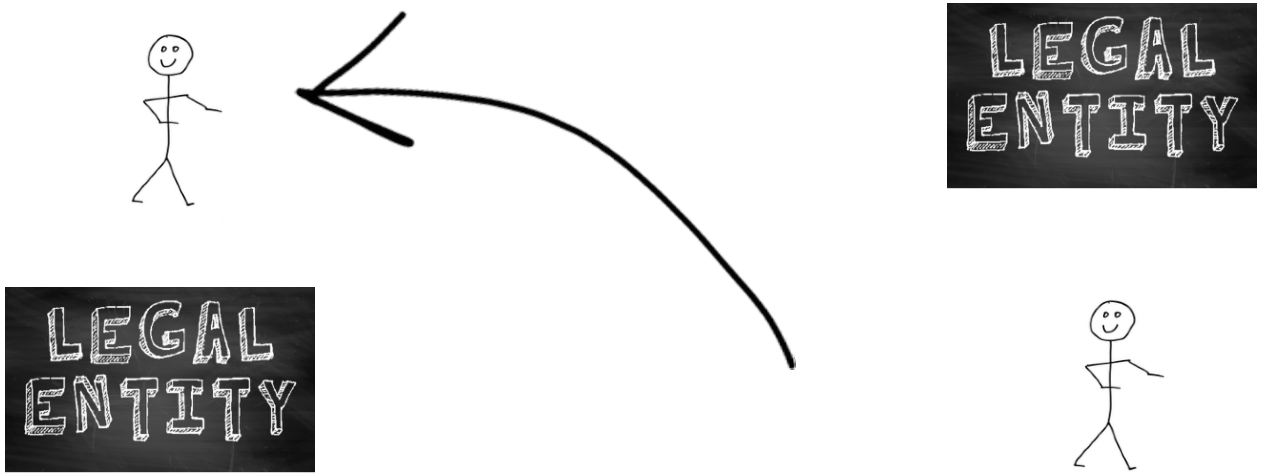
janis.bokta@lvrtc.lv

BEHIND IDEA

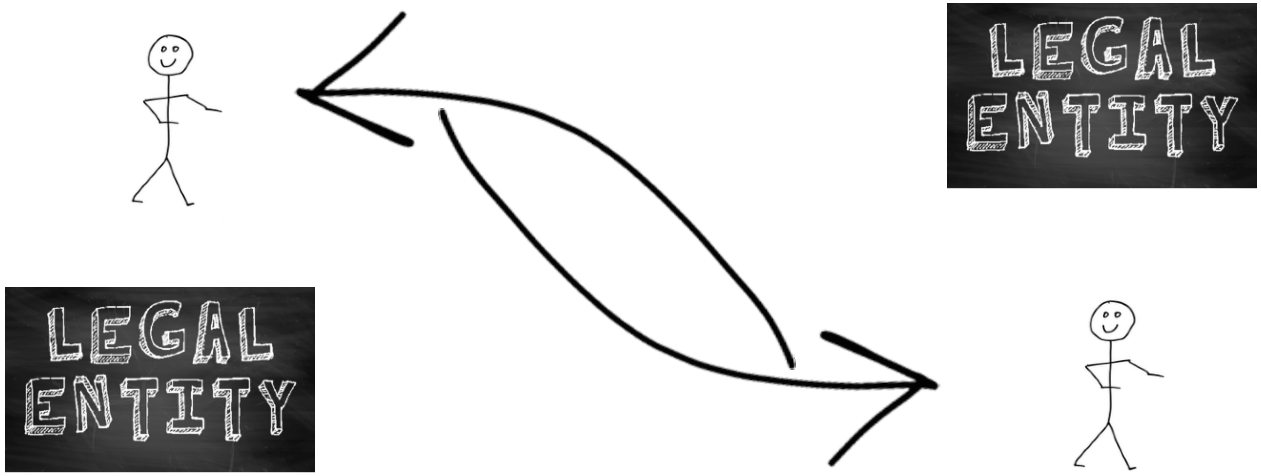




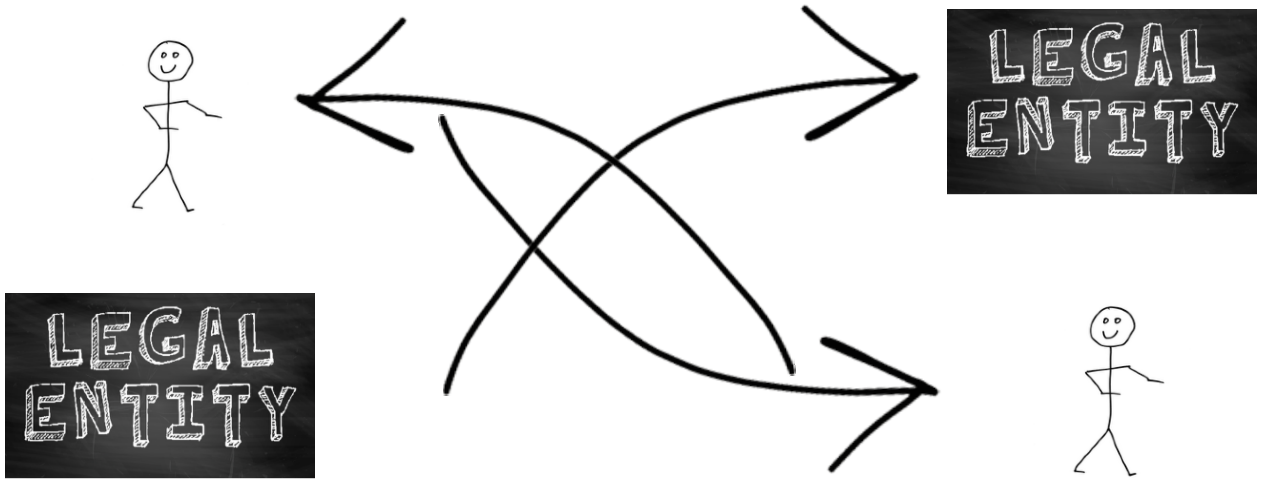
BEHIND IDEA



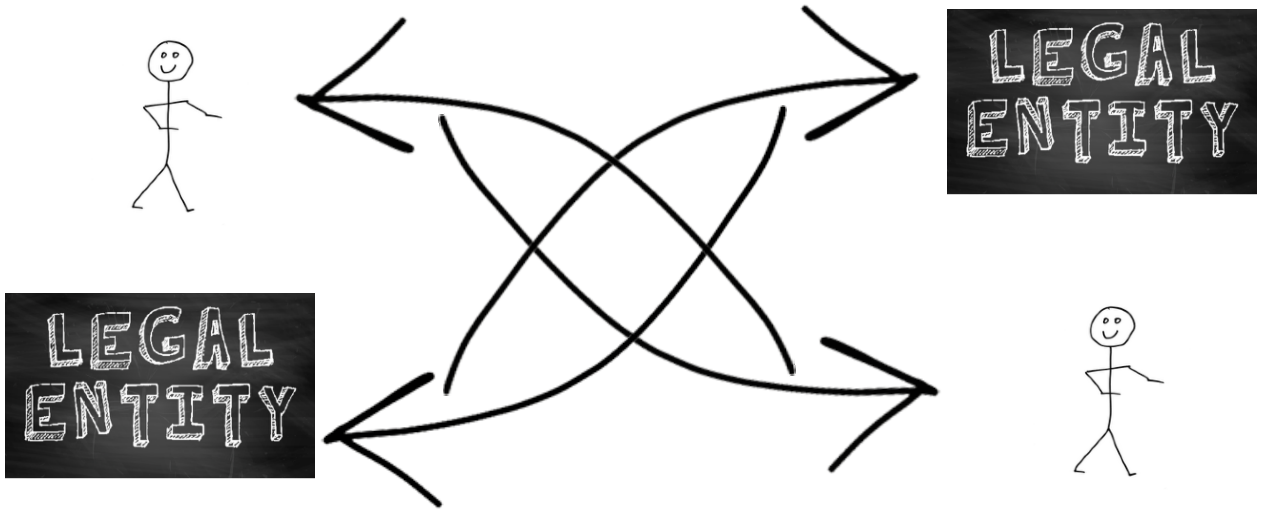
BEHIND IDEA



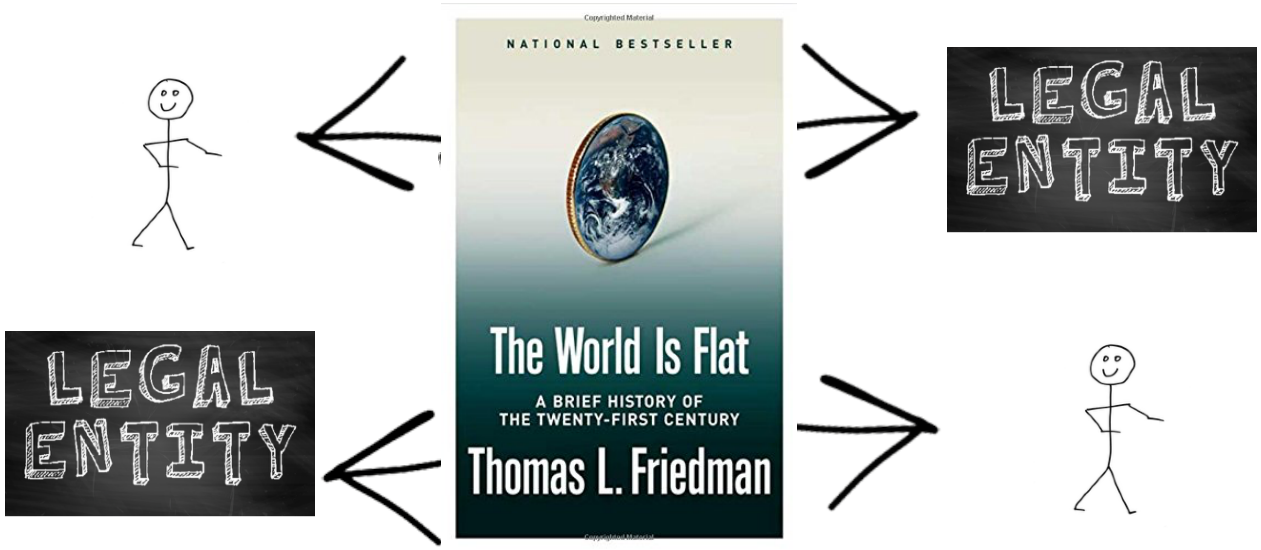
BEHIND IDEA



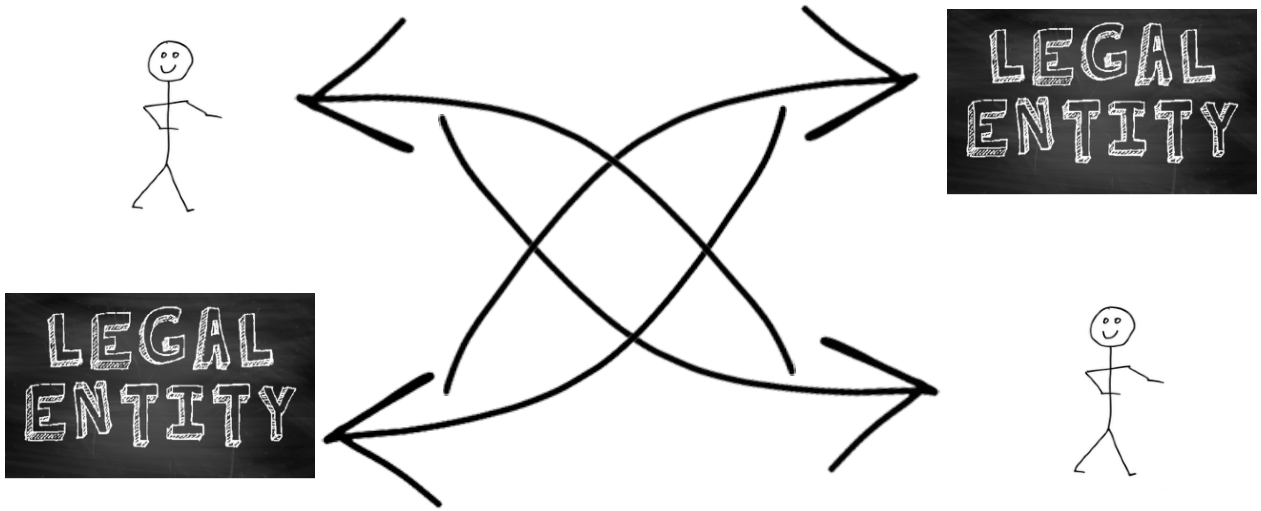
BEHIND IDEA



BEHIND IDEA

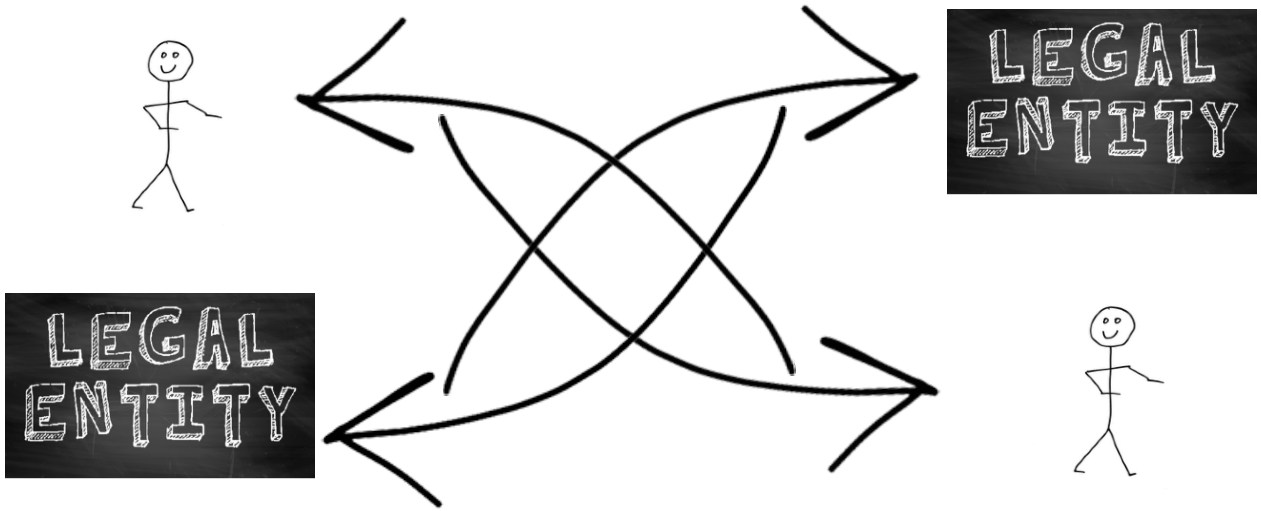

NATIONAL BESTSELLER
The World Is Flat
A BRIEF HISTORY OF
THE TWENTY-FIRST CENTURY
Thomas L. Friedman
LEGAL ENTITY
LEGAL ENTITY

BEHIND IDEA

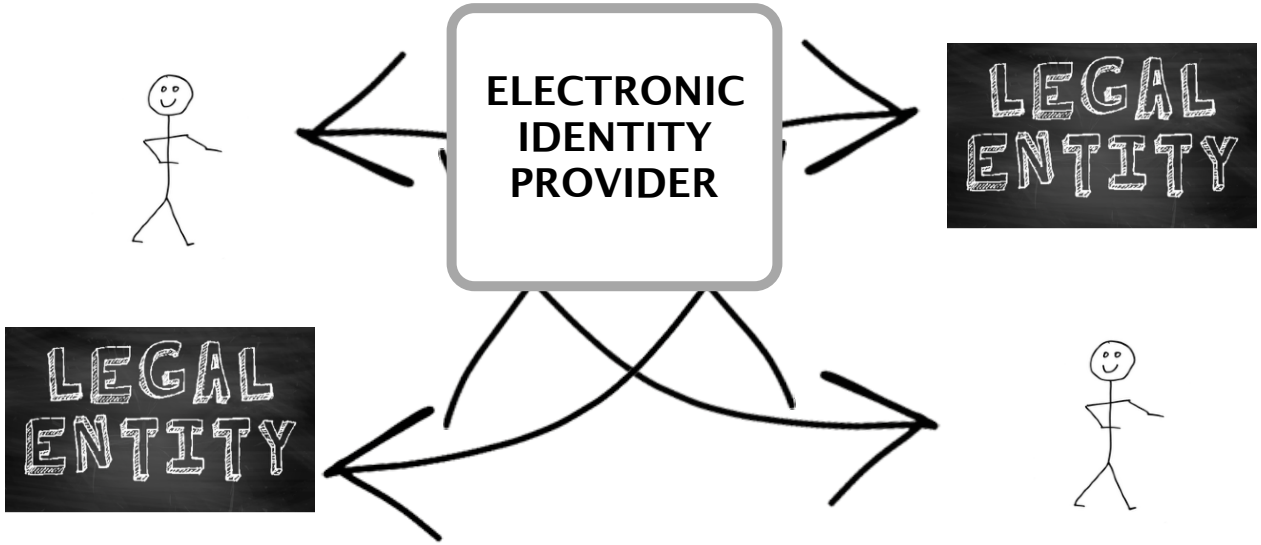


BEHIND IDEA

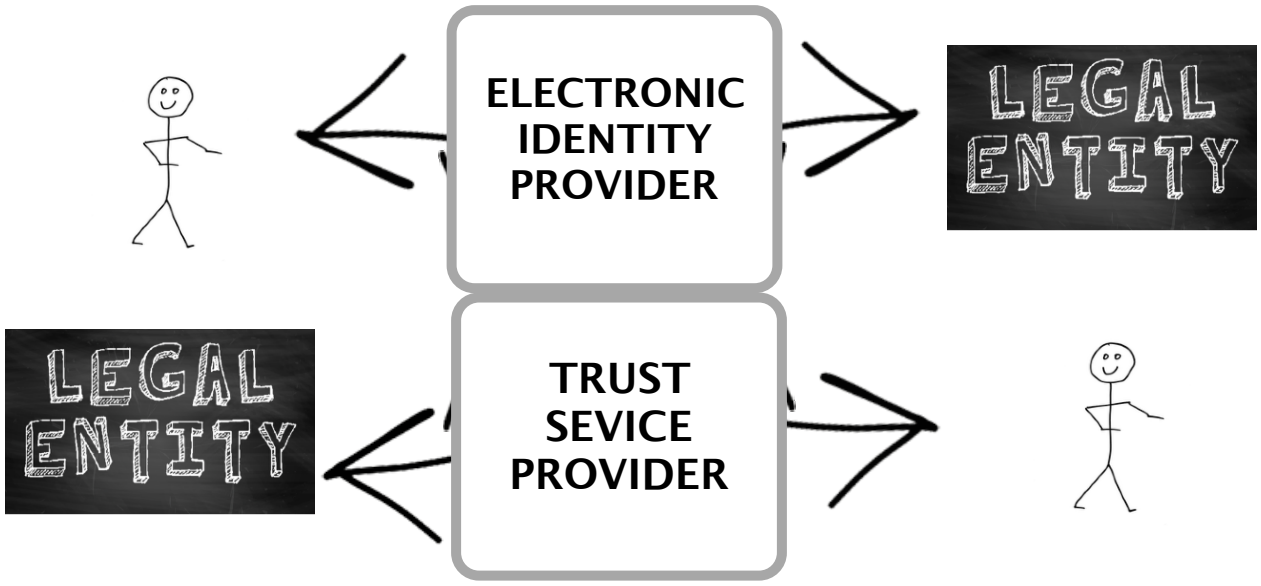
BEHIND IDEA



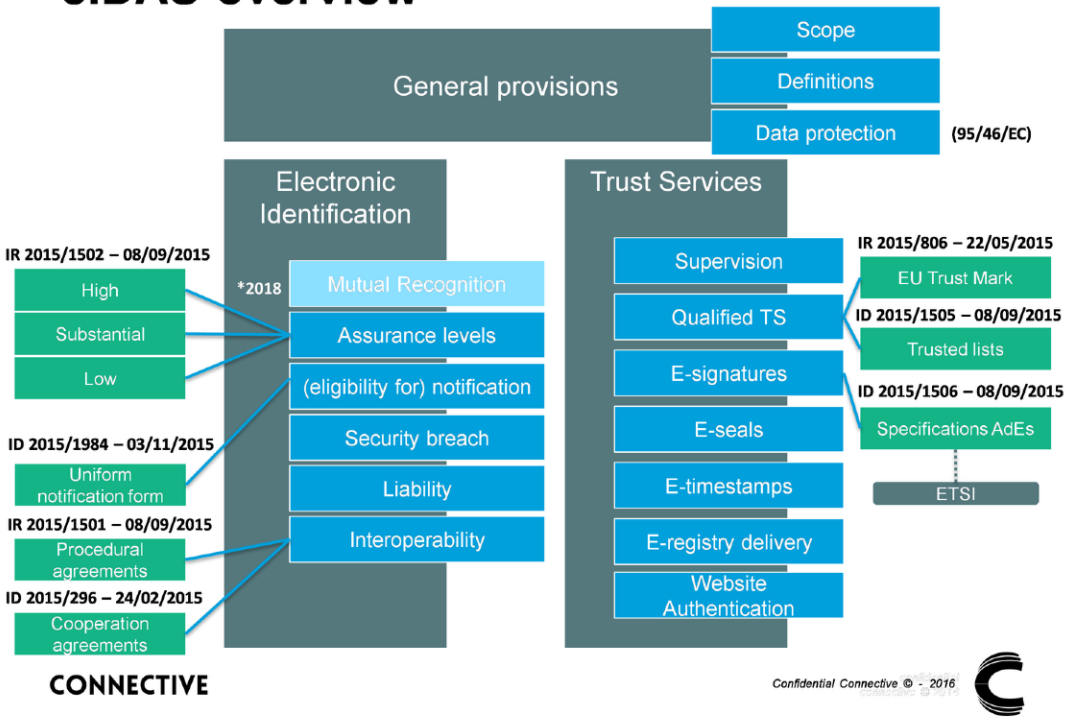
BEHIND IDEA



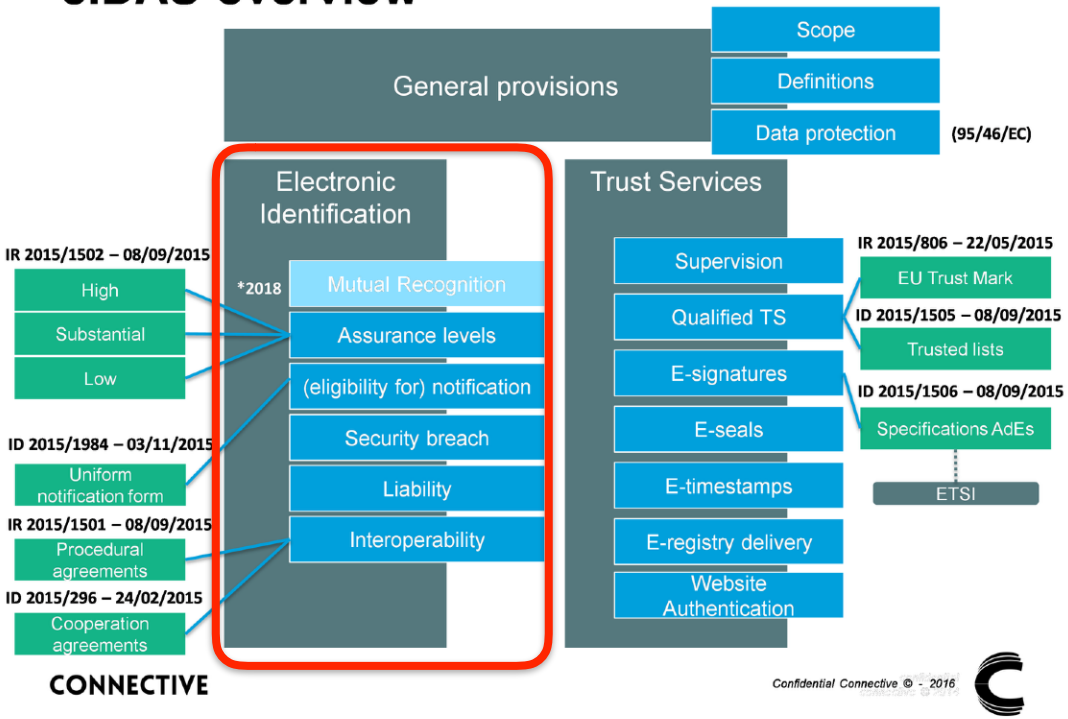
BEHIND IDEA


ELECTRONIC IDENTITY PROVIDER
TRUST SEVICE PROVIDER
LEGAL ENTITY
LEGAL ENTITY

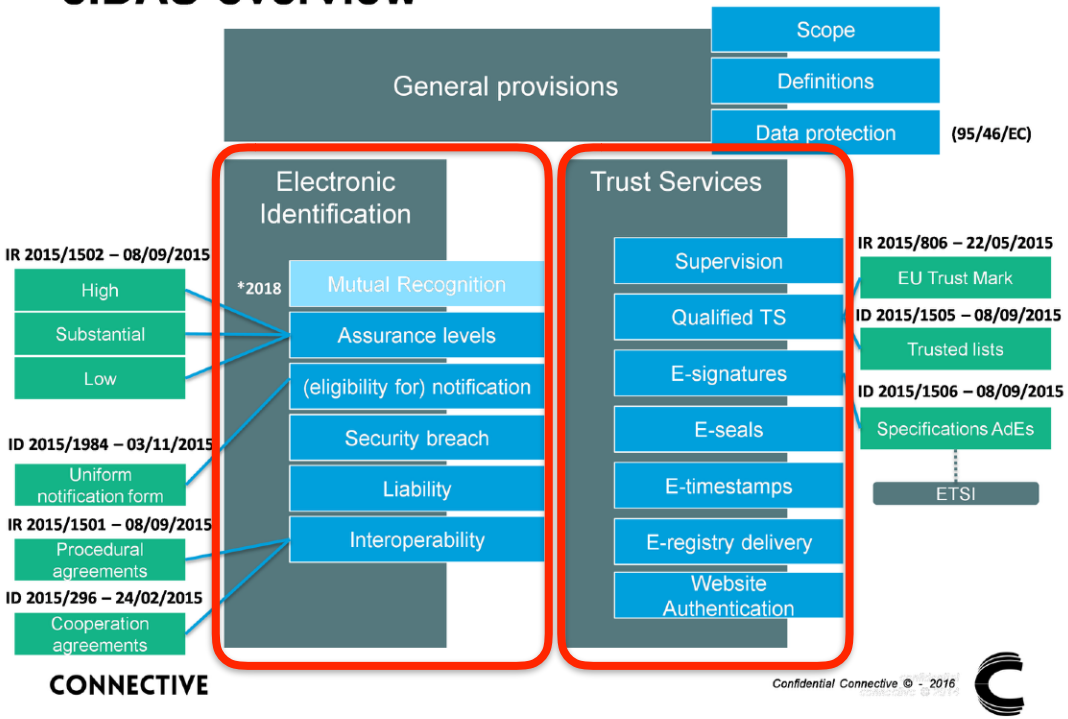
eIDAS overview



eIDAS overview



eIDAS overview




STOCKHOLM
DIET.COM

IS ‘REMOTE' NEW?

IS ‘REMOTE' NEW?

IS ‘REMOTE' NEW?

I

II

IS ‘REMOTE' NEW?

I

II

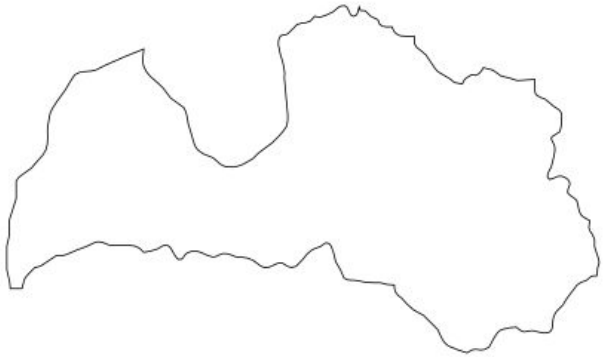
III

IS ‘REMOTE' NEW?

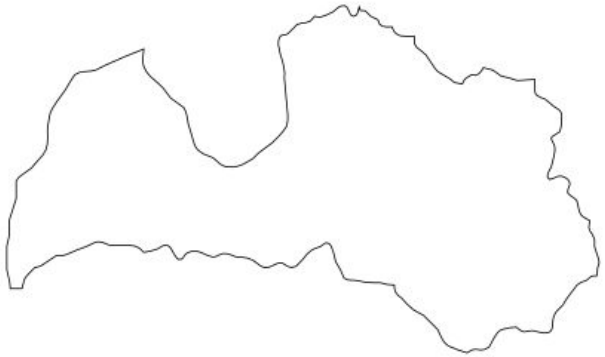
I	II	III	IV
			
			

STATE AS THE STAKEHOLDER

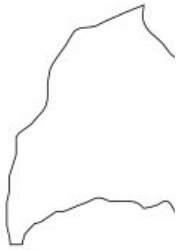
STATE AS THE STAKEHOLDER



STATE AS THE STAKEHOLDER

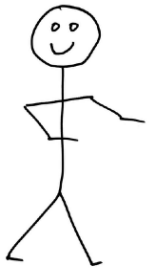


STATE AS THE STAKEHOLDER

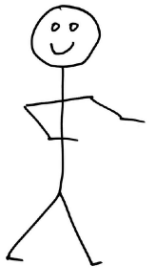


Rule of 3 (writting)

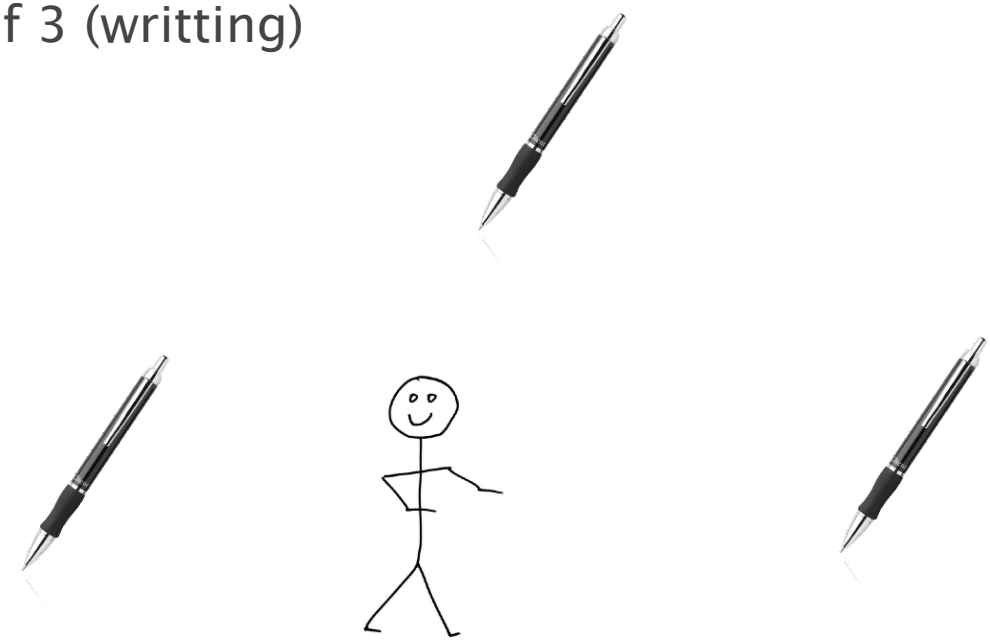
Rule of 3 (writting)



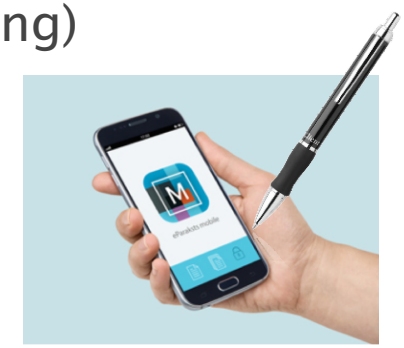
Rule of 3 (writting)

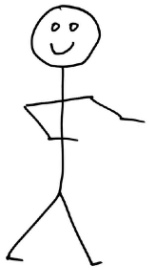


Rule of 3 (writting)



Rule of 3 (writting)





GREATEST CHALLENGE = COMPLIANCES

GREATEST CHALLENGE = COMPLIANCES

Signature Creation and Validation

TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation

TS 119 101 v1.1.1 on Policy and security requirements for applications for signature creation and signature validation

Technical requirements

- EN 319 122-1 v1.1.1 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
- EN 319 122-2 v1.1.1 CAdES digital signatures; Part 2: Extended CAdES signatures
- TS 119 122-3 V1.1.1 CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) in CAdES
- EN 319 132-1 v1.1.1 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
- EN 319 132-2 v1.1.1 XAdES digital signatures; Part 2: Extended XAdES signatures
- EN 319 142-1 v1.1.1 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- EN 319 142-2 v1.1.1 PAdES digital signatures; Part 2: Additional PAdES signatures profiles
- TS 119 142-3 v1.1.1 PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- EN 319 162-1 v1.1.1 Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers
- EN 319 162-2 v1.1.1 Associated Signature Containers (ASiC); Part 2: Additional ASiC containers
- EN 319 102-1 v1.1.1 Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- TS 119 172-1 Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents

Test specifications

- TR 119 124-1 v1.1.1: CAdES digital signatures Testing; Part 1: Overview
- TS 119 124-2 v1.1.1: CAdES digital signatures Testing; Part 2: Test suites for testing interoperability of CAdES baseline signatures
- TS 119 124-3 v1.1.1: CAdES digital signatures Testing; Part 3: Test suites for testing interoperability of extended CAdES signatures
- TS 119 124-4 v1.1.1: CAdES digital signatures Testing; Part 4: Testing conformance of CAdES baseline signatures
- TS 119 124-5 v1.1.1: CAdES digital signatures Testing; Part 5: Testing conformance of extended CAdES signatures
- TR 119 134-1 v1.1.1: XAdES digital signatures Testing; Part 1: Overview
- TS 119 134-2 v1.1.1: XAdES digital signatures Testing; Part 2: Test suites for testing interoperability of XAdES baseline signatures
- TS 119 134-3 v1.1.1: XAdES digital signatures Testing; Part 3: Test suites for testing interoperability of extended XAdES signatures
- TS 119 134-4 v1.1.1: XAdES digital signatures Testing; Part 4: Testing Conformance of XAdES baseline signatures
- TS 119 134-5 v2.1.1: XAdES digital signatures Testing; Part 5: Testing Conformance of extended XAdES signatures
- TR 119 144-1 v1.1.1: PAdES digital signatures Testing; Part 1: Overview
- TS 119 144-2 v2.1.1: PAdES digital signatures Testing; Part 2: Test suites for testing interoperability of PAdES baseline signatures
- TS 119 144-3 v1.1.1: PAdES digital signatures Testing; Part 3: Test suites for testing interoperability of additional PAdES signatures
- TS 119 144-4 v1.1.1: PAdES digital signatures Testing; Part 4: Testing Conformance of PAdES baseline signatures
- TS 119 144-5 v1.1.1: PAdES digital signatures Testing; Part 5: Testing Conformance of additional PAdES signatures
- TR 119 164-1 v1.1.1: ASiC containers Testing; Part 1: Overview
- TS 119 164-2 v2.1.1: ASiC containers Testing; Part 2: Test suites for testing interoperability of ASiC baseline containers

GREATEST CHALLENGE = COMPLIANCES

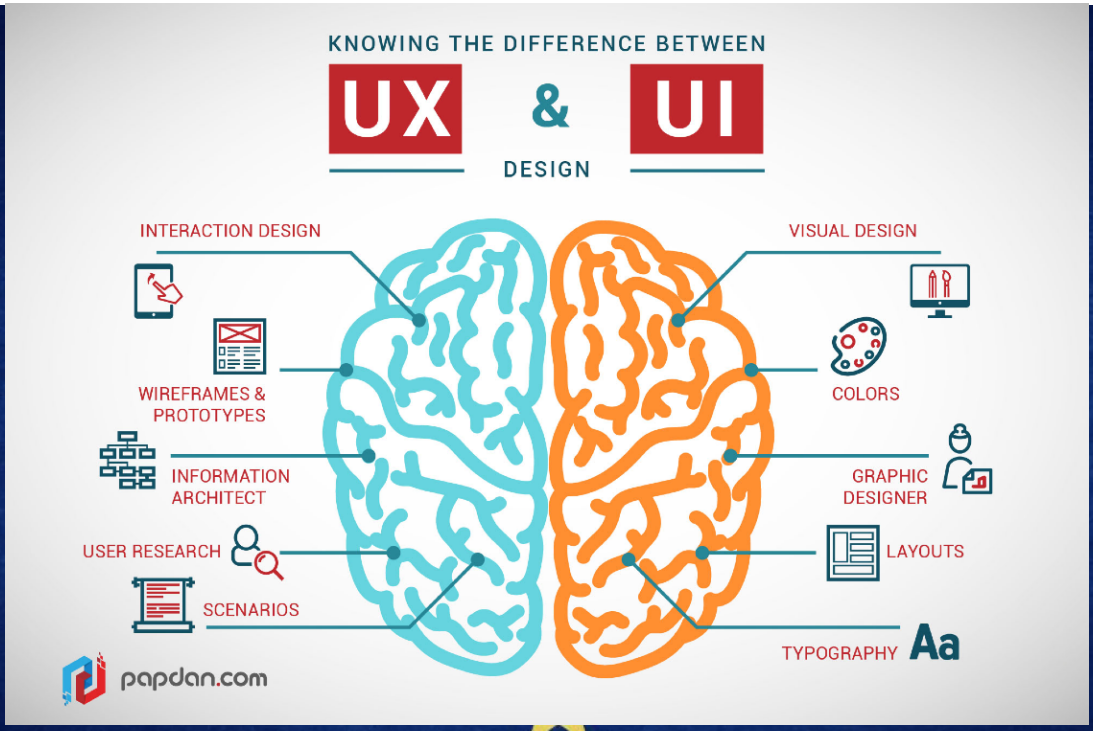
Signature Creation and Validation

TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation

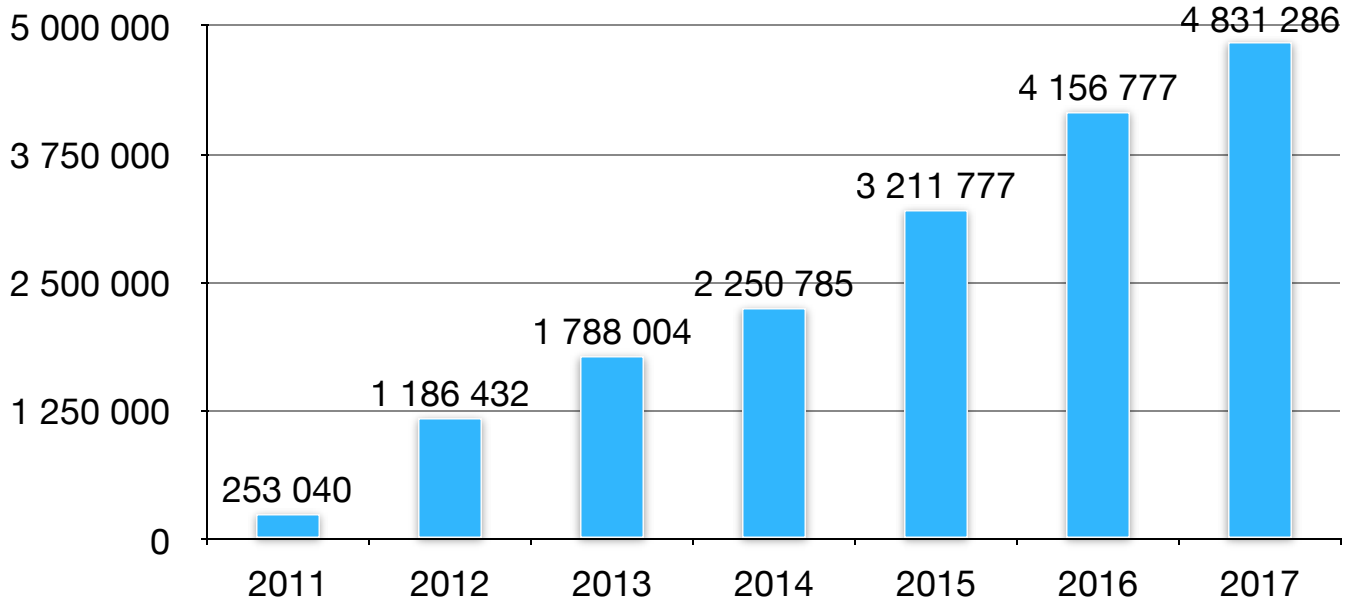
- TS 119 144-4 v1.1.1: PAdES digital signatures Testing; Part 4: Testing Conformance of PAdES baseline signatures
- TS 119 144-5 v1.1.1: PAdES digital signatures Testing; Part 5: Testing Conformance of additional PAdES signatures
- TR 119 164-1 v1.1.1: ASiC containers Testing; Part 1: Overview
- TS 119 164-2 v2.1.1: ASiC containers Testing; Part 2: Test suites for testing interoperability of ASiC baseline containers

GREATEST CHALLENGE = COMPLIANCES

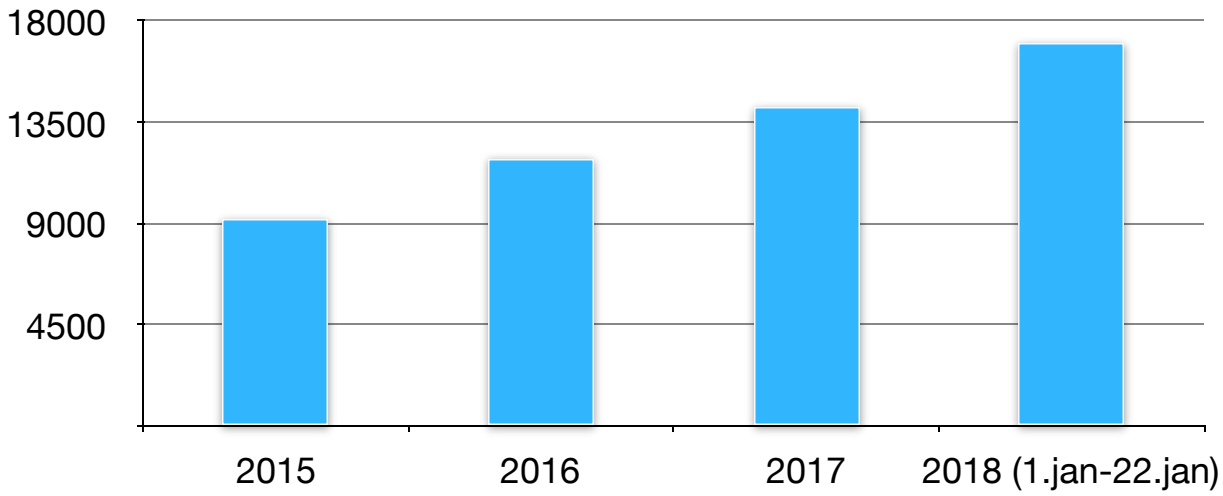
GREATEST CHALLENGE = COMPLIANCES

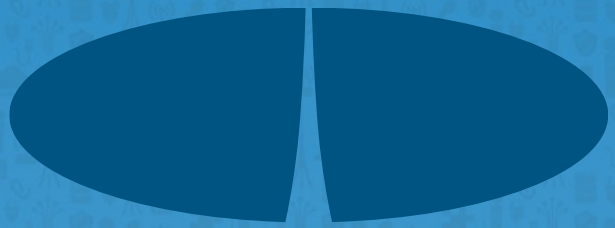


Time Stamps


5 000 000
3 750 000
2 500 000
1 250 000
0
253 040
1 186 432
1 788 004
2 250 785
3 211 777
4 156 777
4 831 286
2011
2012
2013
2014
2015
2016
2017

Time Stamps (best month/avg. per day)





LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS

Thank you!

www.lvrtc.lv

Remote identification - Dukascopy Group experience

26.01.2018 Riga

Dukascopy Bank SA

Bank

Dukascopy Bank – innovative Swiss online bank with HQ in Geneva, Switzerland.

Dukascopy Bank is a cornerstone of **Dukascopy Swiss Banking Group**, with companies providing financial services and having financial licenses in Switzerland, Japan and Latvia.

Bank has **representative offices** in Latvia, Ukraine, Russian Federation, Hong Kong, Malaysia and UAE.

Switzerland

Video and online identification – Dukascopy initiative

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circular 2016/7
Video and online identification

Due diligence requirements for client onboarding via digital channels

Reference:	FINMA-Circ. 16/7 "Video and online identification"
Date:	3 March 2016
Entry into force:	8 March 2016
Legal framework:	FINMASA Article 7 para. 1 let. b AMLO-FINMA Article 3 para. 2
Appendix:	Glossary

Addressees																														
BankA			ISA			SESTA	FINMA							CIBA								AMLA			Other					
Banks	Financial groups and congl.	Other intermediaries	Insurers	Insurance groups and congl.	Intermediaries	Securities dealers	Trading venue	Central counterparties	Central securities depositories	Trade repositories	Payment systems	Participants	Fund management companies	SICAVs	Limited partnerships for CISs	SICAFs	Custodian banks	Asset manager CISs	Distributors	Representatives of foreign CISs	Other intermediaries	SROs	DSFIs	SRO-supervised institutions	Audit firms	Rating agencies				
x	x		x	x		x		x	x		x		x	x	x	x		x					x		x					

- In December 2014, with active support of Swiss bankers association Dukascopy Bank SA has initiated discussion and implementation of video-identification for clients of Swiss banks.
- On 3rd of March, 2016 Swiss Financial Market Supervisory Authority (FINMA) has issued Circular 2016/7 Video and online identification, which has equal validity to in-person identification, provided the certain criteria are met.

Switzerland

FINMA Circ. 2016/7

DUKASCOPY
Swiss Forex Bank & Marketplace

Video-identification

Technical and organisational requirements	Identity verification	Stopping the video identification process
▪ Audio-visual real-time (live transmission) communication; ▪ Adequate technical equipment to ensure the secure video transmission; ▪ Reading and decryption of the information stored in the identification document's machine-readable zone (MRZ); ▪ The picture and sound quality must be adequate - the full duration of the interview must be audio-recorded; ▪ Specially trained employees; ▪ Procedure defining a process for conducting the identification interview and a dialogue guide for employees.	▪ Client registration form with identification data and BO data provided before video identification interview; ▪ Client's explicit consent to conduct the video identification and audio recording; ▪ Photos of the client and all the relevant pages in the identification document and checks whether photos match; ▪ The authenticity of the identification documents review by information decryption in the MRZ and optically variable features examination; ▪ Identity verification by means of a TAN or another similar method.	▪ The picture or sound quality does not enable unambiguous identification of the client; ▪ The financial intermediary identifies evidence of increased risks; ▪ There are any doubts regarding the authenticity of the identification document or the identity of the Client; ▪ The client asked to use conventional channels (i.e. opening an account in person or by correspondence) instead.

Switzerland

FINMA Circ. 2016/7

Documents **equivalent to a simple copy** of an identification document for client onboarding by correspondence:

- A photograph of the identification document provided by the contracting party is equivalent to a simple copy of an identification document. The photograph can be sent electronically to the financial intermediary for filing.
- Photographs of identification documents taken as part of the vide-identification process are also equivalent to a simple copy of an identification document, even if not all of the criteria are met.

ONLINE IDENTIFICATION

Online identification by electronic copy of an identification document - **equivalent to an authenticated copy of an identification document** if they are generated through one of the following processes:

- Electronic copy of an identification document authenticated by the financial intermediary;
- Electronic copy of an identification document with qualified electronic signature;
- Digital authentication;
- Legal entities and partnerships;

European Union

4th AML Directive

EUROPEAN COMMISSION

Press Release Database

European Commission - Press release

Strengthened EU rules to tackle money laundering, tax avoidance and terrorism financing enter into force

Brussels, 26 June 2017

The Juncker Commission has made the fight against tax avoidance, money laundering and terrorism financing one of its priorities.

Today, the Fourth Anti-Money Laundering Directive enters into force. It strengthens the existing rules and will make the fight against money laundering and terrorism financing more effective. It also improves transparency to prevent tax avoidance. This entry into force comes as discussions with the European Parliament and the Council on extra measures further reinforcing the Directive are already at an advanced stage.

Today the Commission also publishes a report which will support Member State authorities in better addressing money laundering risks in practice. As required by the new directive, the Commission assessed the money laundering and terrorist financing risks of different sectors and financial products. The report published today identifies the areas most at risk and the most widespread techniques used by criminals to launder illicit funds.

Frans **Timmermans,** First Vice-President said: *"Laundered money is oxygen to crime, terrorism and tax-avoidance. We need to cut off its supply as best we can. Today's stronger rules are a big step forward but we now need quick agreement on the further improvements the Commission proposed last July."*

Věra **Jourová**, Commissioner for Justice, Consumers and Gender Equality said: *"Terrorists and criminals still find ways to finance their activities and to launder illicit gains back into the economy. The new rules as of today are crucial to closing further loopholes. I urge all Member States to put them in place without delay: lower standards in one country will weaken the fight against money laundering and terrorist financing across the EU. I also call for quick agreement on the further revisions proposed by the Commission following the "Panama Papers" to increase transparency of beneficial ownership."*

Strengthening the existing rules

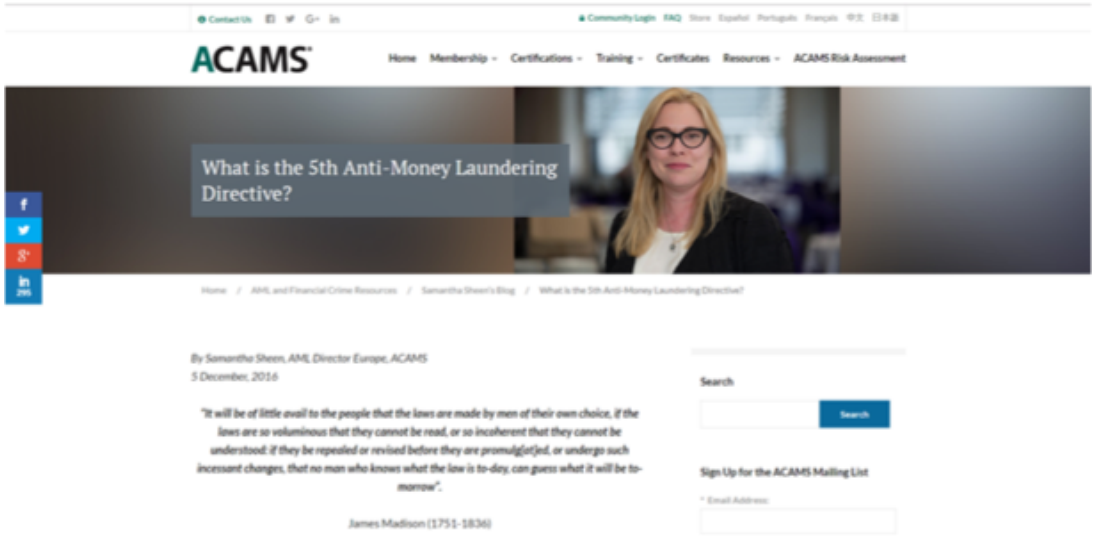
The Fourth Anti-Money Laundering reinforces the existing rules by introducing the following changes:

- reinforcing the risk assessment obligation for banks, lawyers, and accountants;
- setting clear transparency requirements about beneficial ownership for companies. This information will be stored in a central register, such as commercial registers, and will be available to national authorities and obliged entities
- facilitating cooperation and exchange of information between Financial Intelligence Units from different Member States to identify and follow suspicious transfers of money to prevent and detect crime or terrorist activities;

- When establishing business relationship financial institutions must apply customer due diligence measures («client due diligence» или «CDD»);
- CDD shall comprise various measure, including identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a liable and independent source;
- However, obliged entities may determine the extent of such measures on a risk-sensitive basis.

European Union

5th AML Directive

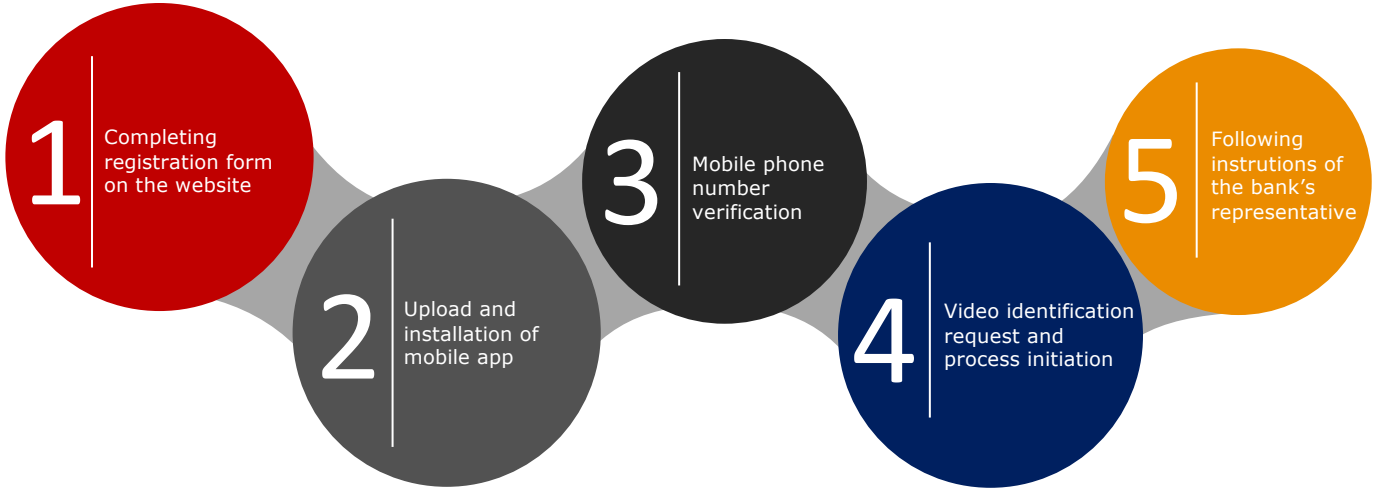


- Latest technical developments in the digitalisation of transactions and payments enable a secure remote or electronic identification (Recital (17));
- In Article 13(1), point (a) is replaced by the following:(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014*or national law.

Dukascopy Bank SA

Video-identification process

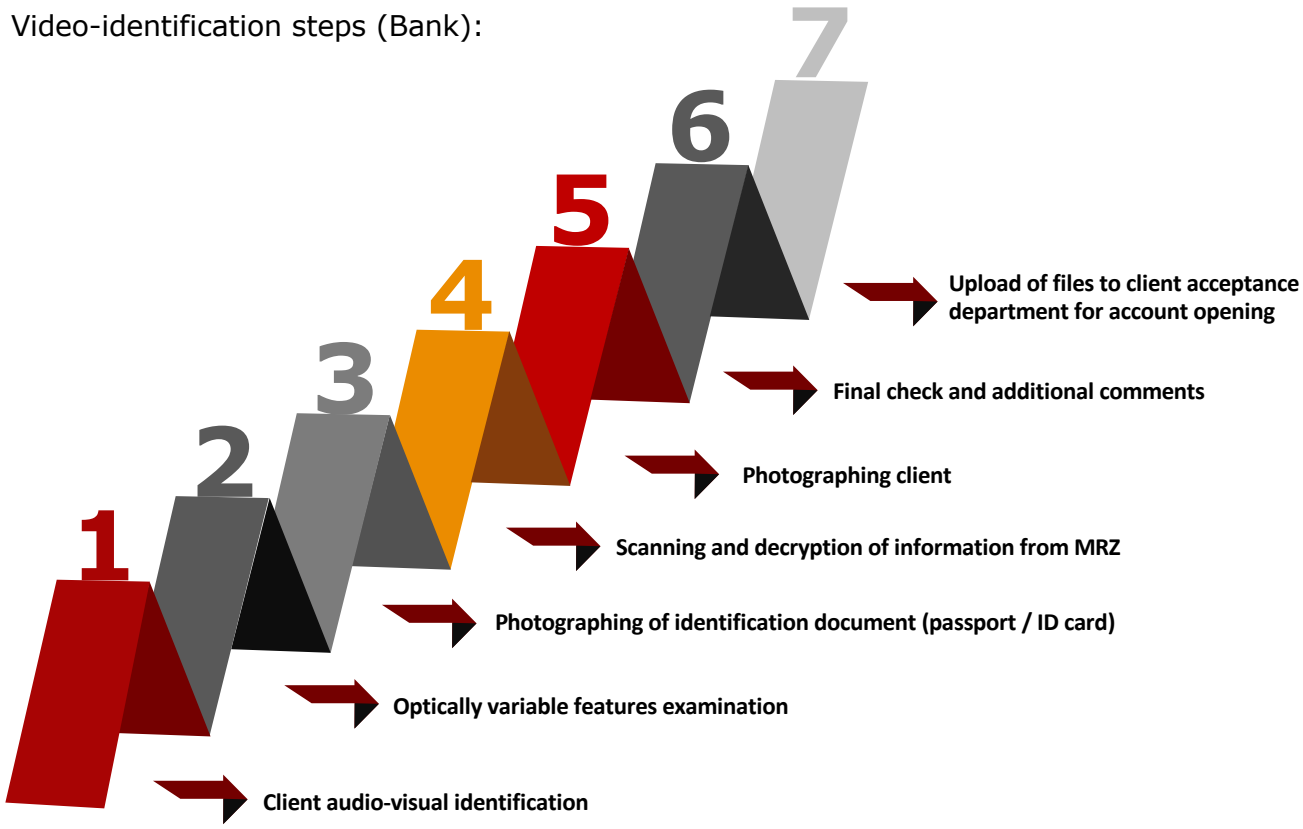
Video-identification steps (Client):



Dukascopy Bank SA

Video-identification process

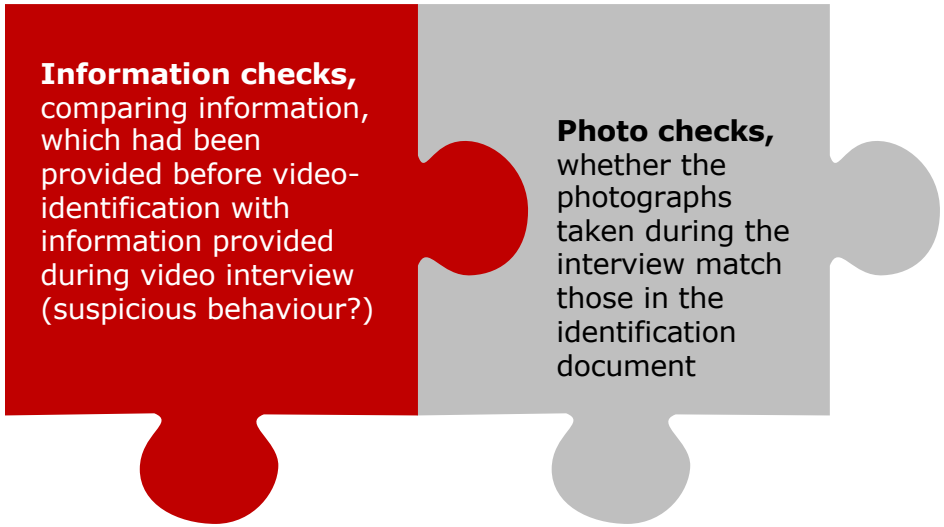
Video-identification steps (Bank):



Dukascopy Bank SA

Video-identification process

Client audio-visual identification:



Dukascopy Bank SA

Video-identification process

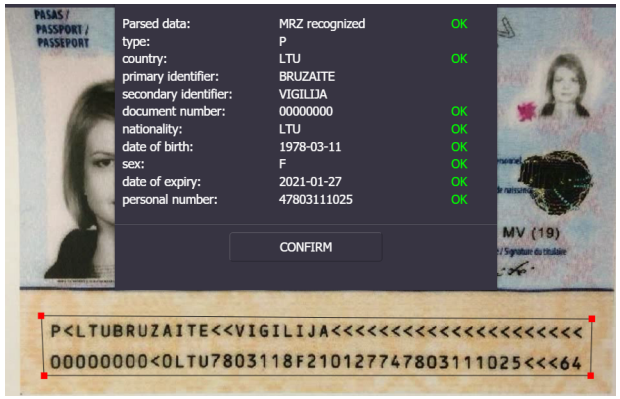
Inspection of optical security elements

Photographing of passport / ID card

Dukascopy Bank SA

Video-identification process

Scanning of machine readable zone



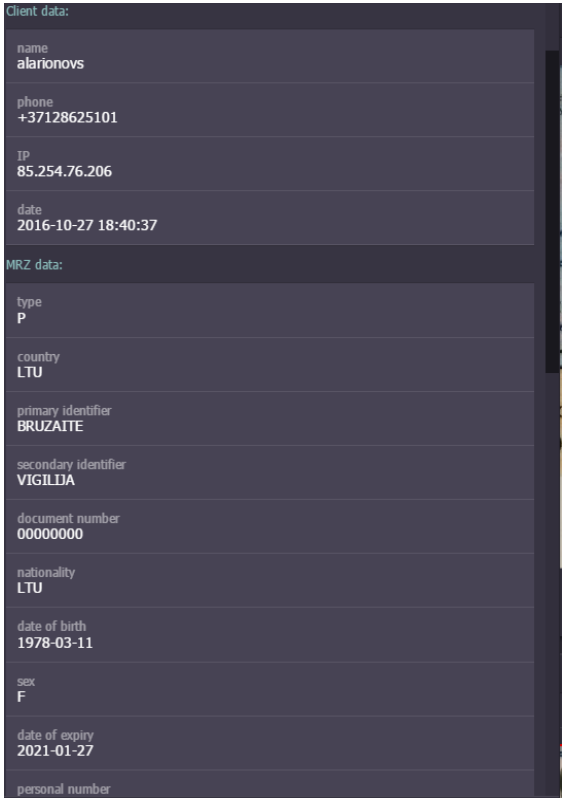
Supported MRZ encoding formats

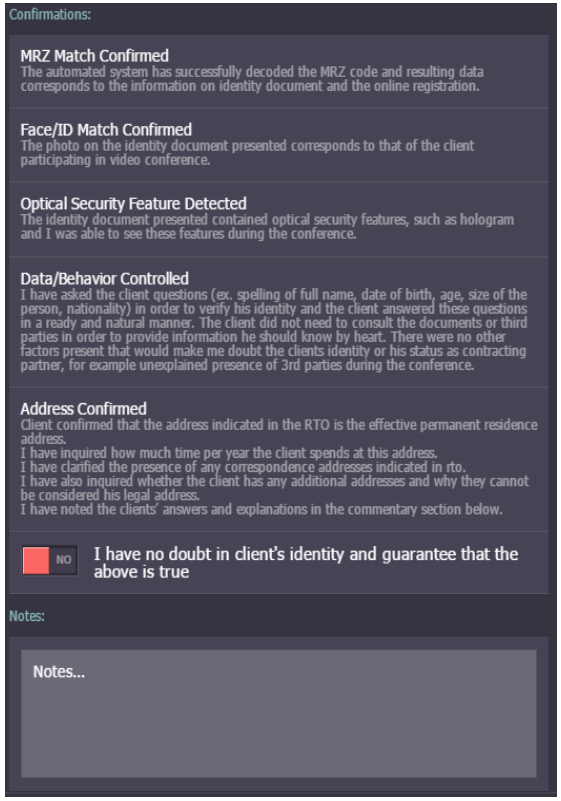
- Passports и ID cards, compliant with ICAO Document 9303 standard;
- Travel (International) passports and Internal passports (e.g., in Russia), issued starting in 2011 (MRZ) in modernized format.

Dukascopy Bank SA

Video-identification process

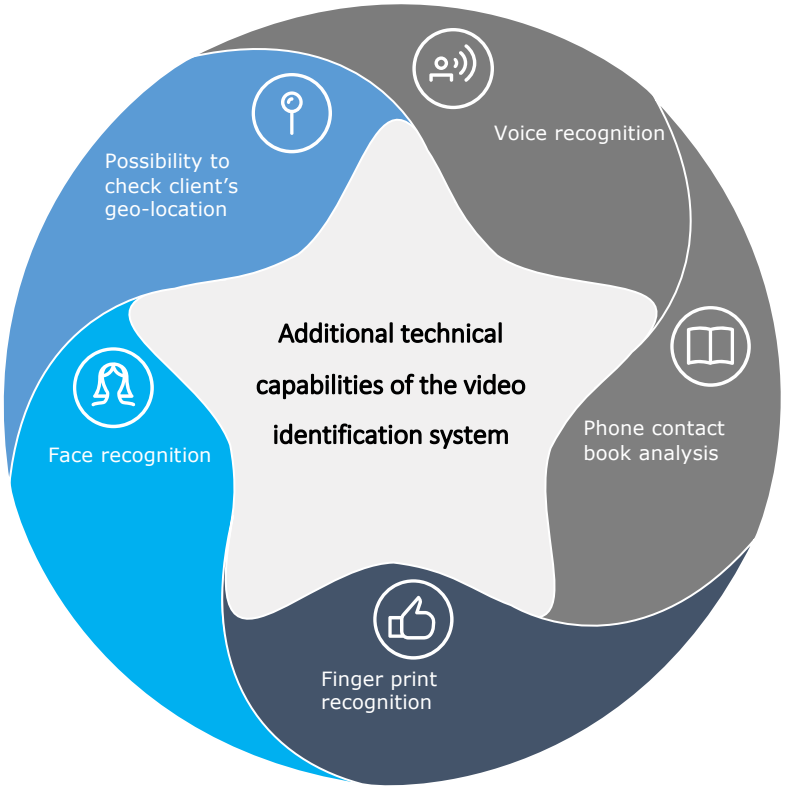
Video-identification verification and confirmation screen





Dukascopy Bank SA

Video-identification process



DUKASCOPY
Swiss Forex Bank & Marketplace

LMENA
Association of Latvian payment and electronic money service providers

Thank you!

Geneva

Dukascopy Bank SA
ICC, Route de Pré-Bois 20,
CH-1215 Geneva 15, Switzerland
Tel: +41 (22) 799 4888
Fax: +41 (22) 799 4880

Riga

LMENA
Lacplesa iela 20a-1, Riga,
LV-1011, Latvia
Tel: +371 67 399 000
Fax: +371 67 399 025

TECHNOLOGY PERSPECTIVE

PANEL Q&A: REMOTE IDENTIFICATION AND AUTHENTICATION TOOLS – OPPORTUNITIES, RISKS, TECHNOLOGIES, FUTURE DEVELOPMENTS

9:40 – 10:30

MODERATED BY:

ĢIRTS BĒRZIŅŠ

Co-chairman of Digital transformation committee at ALCB; Head of Digital strategy, Swedbank group

ANKE ULRICH, LL.M

Senior Legal Counsel, Head of Anti Financial Crime & AML N26 Bank, Germany

JĀNIS BOKTA

Chairman of the Management Board of Latvia State Radio and Television Centre (LVRTC)

DMITRIJS KAČANOVS

Chairman of the Association of Latvian Payment Service Providers and Electronic Money Institutions (LMENA)

JĀNIS GRAUBIŅŠ

Business Developer & Co-founder at Notakey

JANUARY 26, 2018 9:00-12:00

DISCUSSION ON THE FUTURE REGULATION OF REMOTE ELECTRONIC IDENTIFICATION AND ONBOARDING

WATCH ONLINE

AT COBALT
LEGAL
FACEBOOK PAGE

HTTP://EJ.UZ/
DISCUSSION2601

Association of Latvian Commercial Banks

LATVIJAS UNIVERSITATE
ANNO 1919

COBALT

Microsoft

LEGAL PERSPECTIVE

TECHNOLOGY NEUTRAL REGULATION OF REMOTE IDENTIFICATION AND AUTHENTICATION IN LATVIA

10:45 – 11:00

LAURIS LIEPA

Managing parnter, COBALT
Latvia

TECHNOLOGY-NEUTRAL REGULATION OF REMOTE IDENTIFICATION AND AUTHENTICATION IN LATVIA

26 January 2018
Riga

Lauris Liepa
Managing Partner, COBALT

COBALT

IFLR WINNER BALTICS LAW FIRM OF THE YEAR 2016

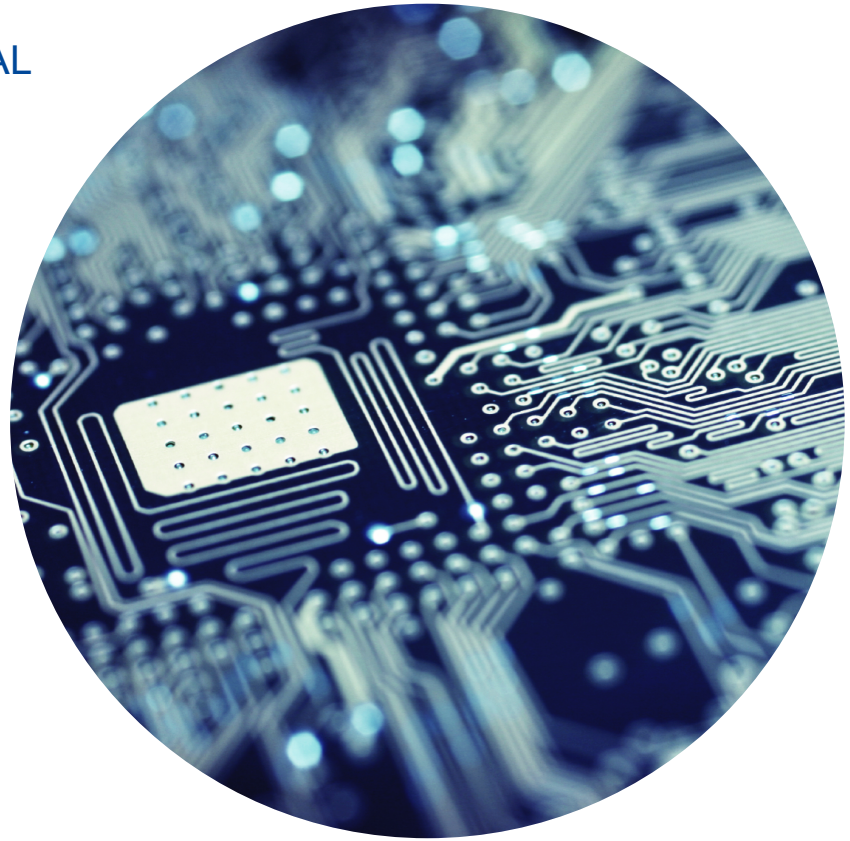
BALTIC-WIDE LAW FIRM OF THE YEAR

COMMON DENOMINATORS FOR DIGITAL CLIENT IDENTIFICATION

<u>AML/KYC provisions apply to:</u>

- Financial and credit institutions (bank and non-bank)
- Auditors and tax consultants
- Sworn attorneys and notaries
- Companies
  - Particularly real estate, gambling, debt recovery

Need for a digital solution that is as technology-neutral as possible

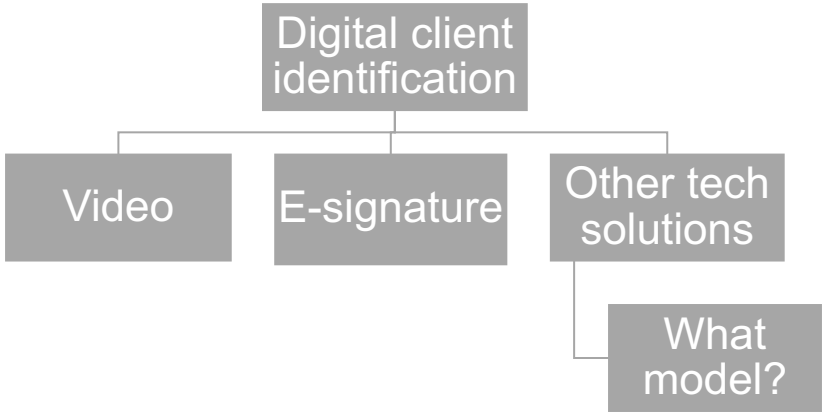


LEGAL FRAMEWORK APPLICABLE TO DIGITAL AUTHENTICATION

Latvian AML Law, Article 22(3):

- *"The Cabinet of Ministers shall determine the scope and procedure of identification of a client by means of technological solutions that include video identification, secure electronic signature or other technological solutions.*

Alternatively, the undertaking must carry out enhanced customer due diligence

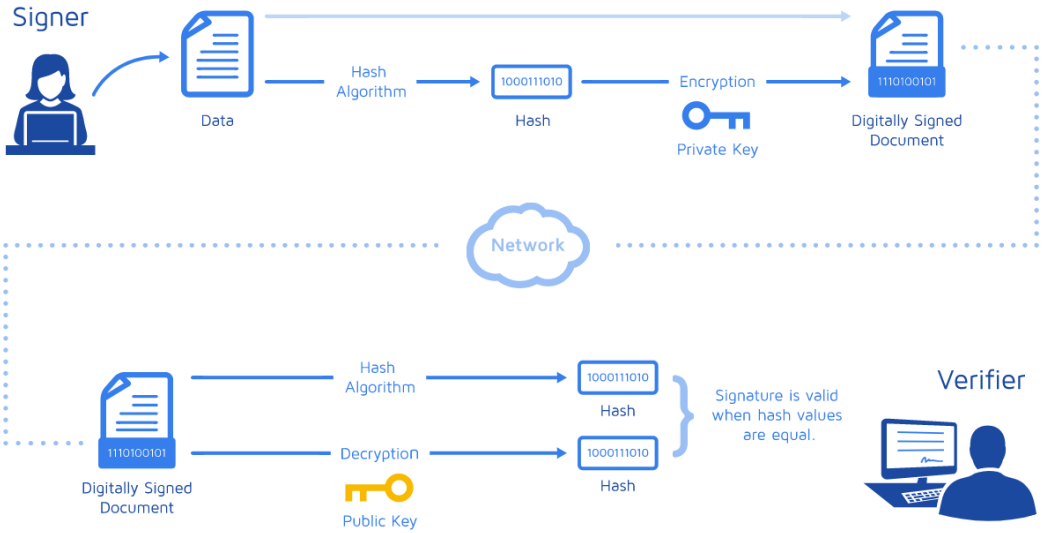


E-SIGNATURE

- Electronic Documents Law
  - Electronic signature of documents
  - Digital client authentication

While theoretically available, is of limited practical applicability/ popularity

- Prone to identity theft – no visual confirmation



Source

VIDEO IDENTIFICATION: GENERAL

(1) Login to video identification platform

(2) Connection via video hardware

(3) Video chat and authentication of document

(4) Video identification complete

- What technical solutions with respect to video identification in Latvia?

Source

VIDEO IDENTIFICATION: EE AND DE

	Estonia	Germany
ID card with reader/ mobile app	■	
Limited number of documents (ID card or passport only)		■
Webcam with audio	■	■
Computer or tablet with internet connection	■	■

Especially trained employees		■
Express client consent required	■	■
Client shows ID, maintains video, and answers questions	■	■
Technical standards required (video quality, audio)	■	■
Audio must be encrypted		■
Screenshots during video		■
Video must be recorded and safely stored	■	■
Skype/ FaceTime OK?	■	

OTHER TECHNOLOGICAL SOLUTIONS: ALGORITHMS

Algorithmic data (mathematical specification seeking data commonalities)

- Electronic copy of identification documents or other documents

- Automated identity verification via behavioural analysis of individual communications using dataset and algorithms

→ E.g. electronic banking identification
  - Authentication via banking credentials (invoices, bank statements, etc.)

→ E.g. identification via information received from third party databases, individual's online profiles, social networks, data from technological devices used, etc.

OTHER TECHNOLOGICAL SOLUTIONS: BIOMETRICS

Biometric data (pertaining to the biological analysis of the individual)

- Analysing and comparing an electronic copy of an identification document with a personality self portrait photo or video and audio recordings to determine authenticity
- Authentication via a scan of biometric data (e.g. fingerprint, facial recognition, retinal scan)

→ Becoming available in the UK

TOWARDS A DIGITAL SINGLE MARKET

Digital Single Market

- Digitalisation of the free movement provisions — enabling citizens and businesses seamless and fair online access to goods and services, irrespective of nationality or geographic location

EIDAS Regulation *on electronic identification and trust services for electronic transactions in the internal market*

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available
- creates a European internal market for electronic trust services (eTS) by ensuring that they will work across borders and have the same legal status as traditional paper based processes
  - Electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication

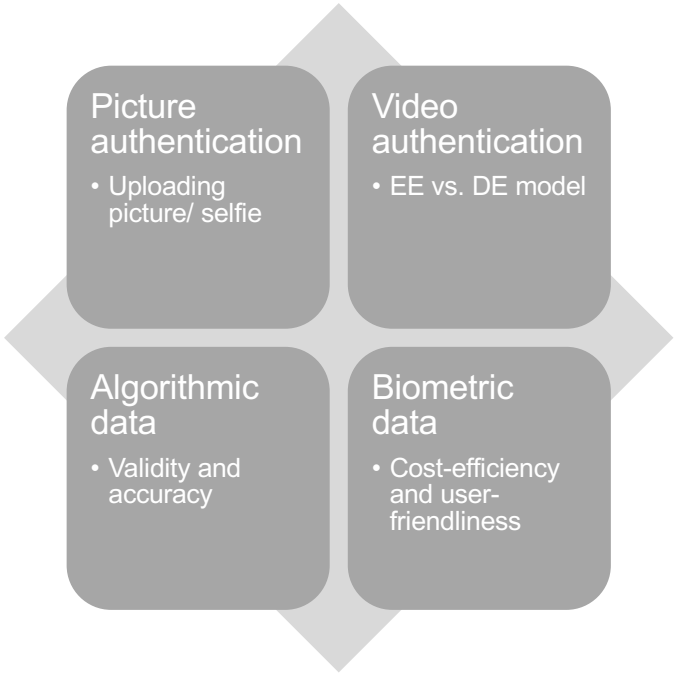
→ Mutual recognition of eIDs and eTSs – giving force to a Latvian electronic identification in another MS, and vice versa

POSSIBILITIES AND PITFALLS OF DIGITAL CLIENT IDENTIFICATION

Key question: what way forward?

Main building blocks:

- Sector-neutrality
- Technology-neutrality
- Cost-efficiency
- User-friendliness



COBALT

LAW FIRM

PANEL DISCUSSION: REGULATION OF REMOTE IDENTIFICATION AND AUTHENTICATION – WHAT? WHY? AND HOW?

11:00 – 11:50

MODERATED BY:

LAURIS LIEPA

Managing Partner, COBALT Latvia

ANKE ULRICH, LL.M

Senior Legal Counsel, Head of Anti Financial Crime & AML N26 Bank, Germany

LĪGA KĻAVIŅA,

Deputy State Secretary, Ministry of Finance

LAILA MEDIN

Deputy State Secretary, Ministry of Justice

KRISTAPS MARKOVSKIS

Head of Legislative and Regulatory Division, Compliance Control Department, Financial and Capital Markets Commission (FKTK)

JANA ORLOVA

Head of Commercial Unit at Group Legal, 4finance

WRAP UP

11:50 – 12:00

LĪGA KĻAVIŅA

Deputy State Secretary, Ministry of Finance

SANDA LIEPIŅA

Chairman of the Managment Board of the Association of the Latvian Commercial Banks (ALCB)

DISCUSSION ON THE FUTURE REGULATION OF
REMOTE ELECTRONIC IDENTIFICATION AND ONBOARDING

THANK YOU

Association of Latvian Commercial Banks
LATVIJAS UNIVERSITĀTE ANNO 1919
COBALT
Microsoft