Regula

Webinar transcript: Understanding Electronic IDs and Digital IDs

 Kate Volskaya:

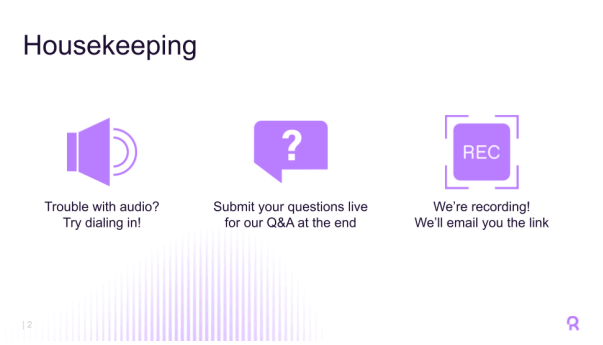
Hello, and thank you for making the time to join us for this Regula webinar. Today, we will talk about electronic IDs and digital IDs.

 Kate Volskaya:

Before we begin, a few housekeeping items:
If there are any audio issues, please try dialing in using the numbers provided in your invitation.

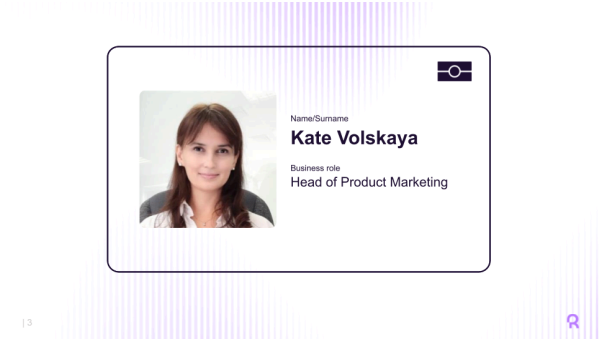
Also, feel free to submit your questions live in the chat during our presentation. We'll answer them in the Q&A session at the end, or our team will address them as we go.

This webinar is being recorded, and we'll send out the link over the next few days.



 Kate Volskaya:

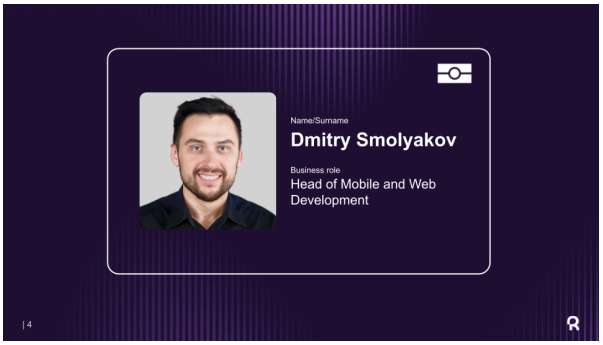
So, let's get started!
My name is Kate, and I'm the Head of Product Marketing at Regula.



 Kate Volskaya:
My co-host today is Dmitry, the Head of Mobile and Web Development at Regula.

 Dmitry Smolyakov:

Thank you, Kate! Hello everyone!
At Regula I'm responsible for the technical development of Mobile and Web products. I'm very glad to present



for you today.

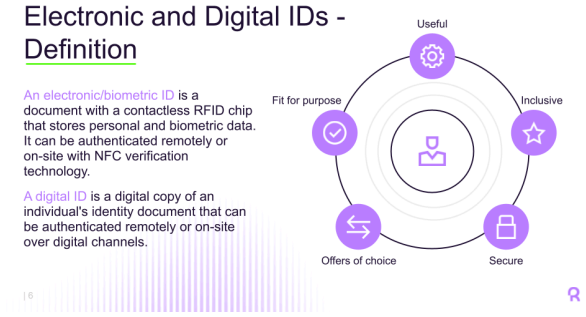

Kate Volskaya:
Today we're going to dive deeper into electronic and digital IDs. And I would like to begin by defining what electronic/biometric IDs and digital IDs are in simple words. Also, it's important to note that this presentation is based on Regula's knowledge and expertise.


Kate Volskaya:

An electronic/biometric ID is a document with an RFID chip that stores personal and biometric data, and it can be authenticated remotely via smartphone or on-site via a passport reader device with built-in NFC verification technology. The chip contains the personal data from the passport and the biometric facial image as well as information that helps to validate it. In simple words, an electronic ID is a physical passport with an RFID chip inside.

A digital ID is the electronic equivalent of an individual's physical ID, for example a driver's license. It is stored in a digital wallet and can be presented electronically to prove an individual's identity and their right to access information or services online. The World Economic Forum defined the following core principles of Digital ID:

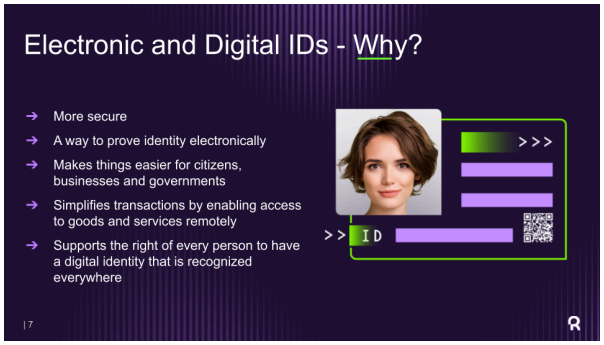
It needs to be Useful, Inclusive, Secure, Offer choice, and be Fit for Purpose.




Kate Volskaya:

Why do we need this type of identity document? Well, in today's world, where many interactions are online, we need a secure and reliable way to prove an identity electronically while keeping the choice of when and where to do it.

These documents make it easier for users, as there's no need for them to go somewhere with a physical ID. They are much more handy, and at the same time, they are more secure for businesses and governments. eIDs are also easier to process, because with traditional IDs, you need to rely on the security elements they have. If they are poorly protected, then the potential for fraud is higher.



Regula

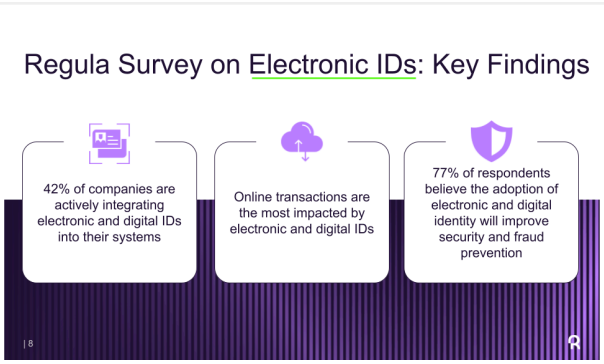
It's also worth mentioning that electronic IDs enable significant economic value by facilitating easier access to goods and services.


Kate Volskaya:

In January 2024, Regula commissioned Forrester Consulting to survey decision-makers responsible for their organization's ID verification solutions. For the research, we focused on organizations from Aviation, Finance, Government, and other industries from Europe, North America, and the Middle East.

The figures from the survey confirm the importance of these IDs:

- 42% of companies are actively integrating digital and electronic IDs into their systems.
- Online transactions will be most impacted by them.
- 77% of respondents expect these IDs to improve their security infrastructure and fraud prevention capabilities.

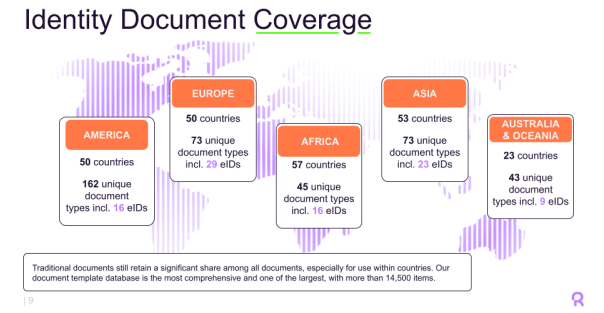



Kate Volskaya:

Today, electronic documents are the most secured and used identity documents globally. Almost every country issues an electronic ID. Of course, electronic ID coverage is not the same as the number of documents. This is due to the fact that in each country there are a lot of different document types.

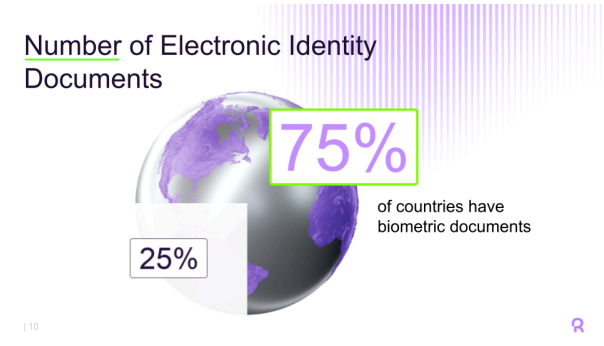
Also, the adoption of e-IDs is not the same across all countries. However, many of them are taking steps to phase out traditional documents.

At Regula, our technologies currently cover biometric documents from 178 countries and territories, and we actively add new ones as they become available.




Kate Volskaya:

It is important to note that even though 75% of countries have started issuing biometric documents, there are very few statistics available on the split between traditional documents and biometric documents that are currently in use. But this figure may vary from country to country, as in some the adoption is less than 50%. From past experience, these types of initiatives tend to have quite a long tail that may take many years to completely switch.



Regula


Kate Volskaya:

And now, I would like to pass the microphone to Dmitry. He'll guide you through in-depth details on these IDs.


Dmitry Smolyakov:

Thank you, Kate! Let's see how eIDs and Digital IDs evolved.


Dmitry Smolyakov:

Let's take a step back. The evolution of identity documents from traditional to electronic forms has been shaped by technological advancements, societal needs, and security concerns. Not long ago, there were documents that didn't even have photos. They exist now, but they're still paper-based documents like birth certificates, social security cards, and government-issued ID cards.

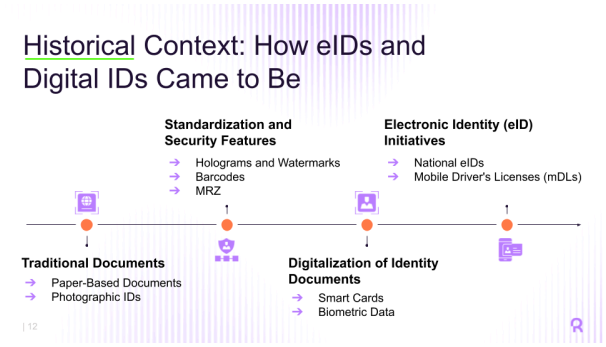
In the middle of the 20th century, a layer of security was added, and photographic IDs appeared, making it harder to impersonate someone.

The next step to consider is, once the standardization and security features are in place, such as holograms and watermarks, to enhance the authenticity of identity documents.
And barcodes, allowing for quick scanning and verification.

Another step was digitalization of identity documents:

Smart Cards and Biometric Data: These plastic cards contained embedded microchips that could store digital information securely.

And finally, there is electronic identity (eID):
National eIDs and mobile driver's licenses (mDLs) that can even be stored on smartphones.



Regula


Dmitry Smolyakov:

Now, let's all focus on what we call Biometric Identity documents.

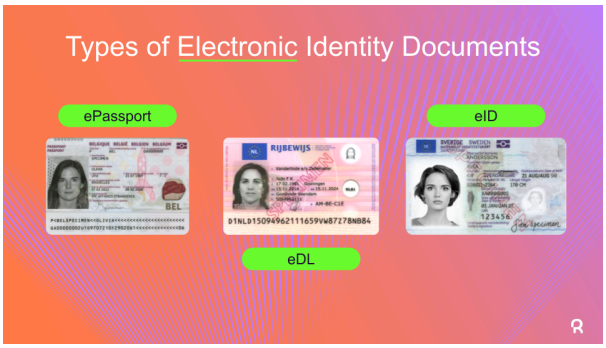
Since 1980, the International Civil Aviation Organization has been standardizing travel documents to ensure their international integration. The first attempt to use RFID technology in identity documents was a Malaysian electronic passport issued almost 30 years ago. At that time, there weren't even any specifications for this technology.

In 2003, ICAO updated its standard for countries issuing machine-readable travel documents, including printing and physical details. Additionally, it also specifies the details of the embedded chip so an identity document carries the symbol displayed on this slide. The terms for this include ePassport, biometric passport, electronic ID, or biometric ID. The eMRTD chip symbol now appears on many passports, IDs, and residence permits that have an embedded contactless RFID chip. It enables wireless NFC communication between the identity document and compatible devices, allowing swift and contactless data exchange.


Dmitry Smolyakov:

There are three main types of electronic identity documents:

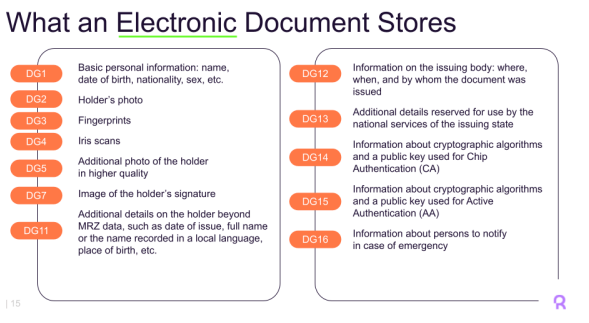
- ePassport
- eDL
- eID




Dmitry Smolyakov:

The content of RFID chips varies depending on the type of identity document. However, different data is always stored separately, and each file has its own unique identifier, which is used to provide access to it. This segregation contributes to RFID chip security.

Typically, there are informational and service data packages. For instance, a biometric passport's chip includes the data groups (DG) you can see on the slide: DG1 contains basic personal information such as name, date of birth, nationality, etc., the same data that is encoded in the document's MRZ. Then there's



biometric information, information about cryptographic algorithms, and a key used for chip or active authentication and other service data groups

Some data groups are reserved for further standard development. This structure makes it possible to set different access levels to the data recorded on the chip. For instance, the DG2 file with the document holder's photo is checked during routine verification sessions like customer onboarding in a bank. But only authorized entities like border control or police officers can access biometric data, such as iris scans or fingerprints stored in DG4 and DG3 data groups.

 Dmitry Smolyakov:

When issuing electronic documents, each issuing state signs every electronic identity document with certificates and at least two types of key pairs: a Country Signing Certification Authority (CSCA) key pair and a Document Signer Certificate (DSC) key pair. The CSCA private key digitally signs the DS Certificate, and the DS private key digitally signs the ePassport.

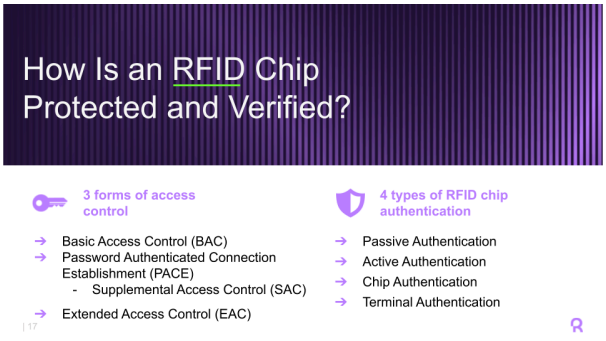
A digital signature on an ePassport is derived from the issuing state's security certificates, each of which contains the public key that can be used to verify its authenticity—the CSCA Certificate and the DSC Certificate.

Together, the signature and certificates form a trust chain wherein one end is securely anchored in the authority of the issuing state, and the other end is securely stored in the chip of the ePassport as the Document Security Object. The document signer must be validated against the CSCA to validate the digital signature to complete the whole chain of trust regarding the signatures.

 Dmitry Smolyakov:

All information stored on an RFID chip is secured with an access control mechanism. It prevents data from being read unless the inspection system can prove its authorization. This helps prevent unauthorized interception of the "dialog" between the chip and the reader, e.g., a smartphone, and stops fraudsters from skimming the data.

There are three forms of access control currently used in electronic IDs:
Basic Access Control is one of the earliest methods,



based on symmetric keys to secure communication between chip and reader, but it's still in use today. Password Authenticated Connection Establishment is a replacement of BAC, and it provides stronger protection Supplemental Access Control is not actually an access control mechanism in itself; it is just a term used to describe ePassports that have both BAC and PACE. Extended Access Control is optional and can be used to read biometric data (fingerprint or iris).

The RFID verification flow is determined by the issuing country, the specific use case, and the identity verification software in use. There are four methods to authenticate the chip:

- Passive Authentication
- Active Authentication
- Chip Authentication, and
- Terminal Authentication. This one, most of the time, can be used only by authorities to access sensitive data.

 Dmitry Smolyakov:

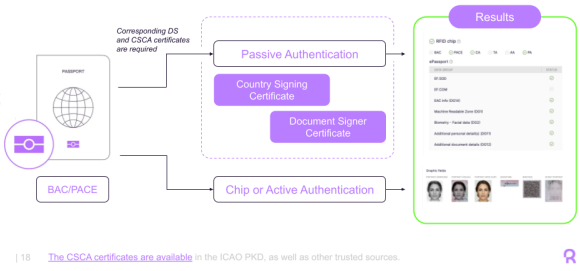
Have a look at the flow when conducting ePassport validation.

The first part is performing PACE or BAC procedures.

Then chip or active authentication checks that the chip was not cloned.

Passive authentication is the process of validating the chip by verifying the digital signature on the document, which uses the public keys of the issuing State.

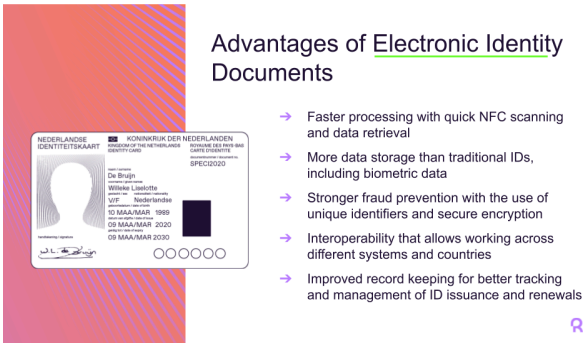
When the appropriate infrastructure and systems are in place, this process verifies that the electronically stored information in the ePassport is authentic, was issued by the given country, and has not been tampered with. The certificates are available in the ICAO Public Key Directory, as well as other trusted sources.



 Dmitry Smolyakov:

Electronic IDs that incorporate RFID technology, such as electronic passports, driver's licenses, and ID cards, offer several benefits:

Faster Processing: RFID technology allows for quick scanning and data retrieval, which can significantly reduce wait times at airports and other checkpoints. Data Storage: Electronic IDs can store more



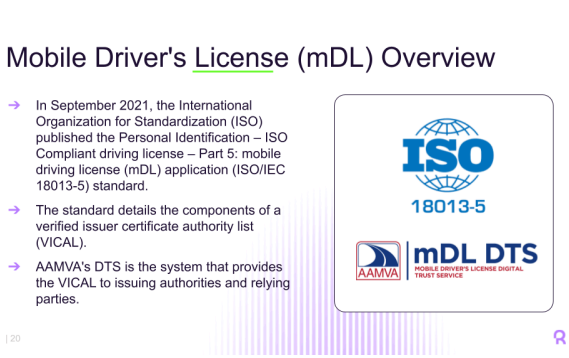
information than traditional IDs, including biometric data and additional personal details that can be accessed securely.
Fraud Prevention: The use of unique identifiers and secure encryption helps reduce identity theft and fraud, as it is more difficult to replicate or forge RFID-enabled IDs.
Interoperability: Many electronic IDs are designed to work across different systems and countries, facilitating international travel and identification.
Improved Record Keeping: The use of RFID technology allows for better tracking and management of ID issuance and renewals, leading to improved administrative efficiency.
Overall, the integration of RFID technology into electronic IDs enhances security, efficiency, and user experience. They also support modern needs for digital identity management.

 Dmitry Smolyakov:

Another type is the mobile driver's license (mDL).
In September 2021, the International Organization for Standardization (ISO) published a new standard—the whole name is presented on the slide. It's a standard for mDL application. It encompasses the entire lifecycle of digital driver's licenses, from their issuance by authorities to their use in everyday scenarios.

Also, it sets the framework for how mDLs should be formatted, transmitted, and authenticated.
The standard details the components of a verified issuer certificate authority list through which a list of legitimate issuing authority public keys can be shared with relying parties.

Similar to ICAO, the American Association of Motor Vehicle Administrators Digital Trust Service is the system that provides the Verified Issuer Certificate Authority List (VICAL) to issuing authorities and relying parties. Participating issuing authorities provide the organization with the public keys used to issue their mDLs, which are then loaded into the system.

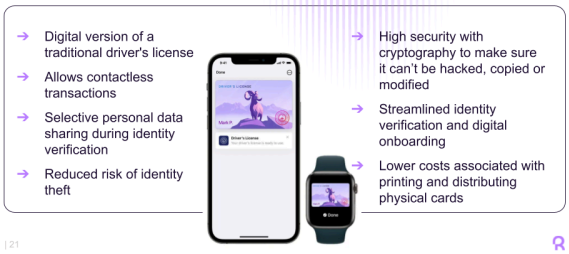


Regula


Dmitry Smolyakov:

A mobile driver's license is a digital version of a traditional driver's license. It can be stored on a smartphone or other mobile device. mDLs offer several benefits over traditional physical driver's licenses.

- Digital version of a traditional driver's license
- Allows contactless transactions
- Selective personal data sharing during identity verification
- Reduced risk of identity theft
- High security with cryptography to make sure it can't be hacked
- Streamlined identity verification and digital onboarding, and lower costs associated with printing and distributing physical cards

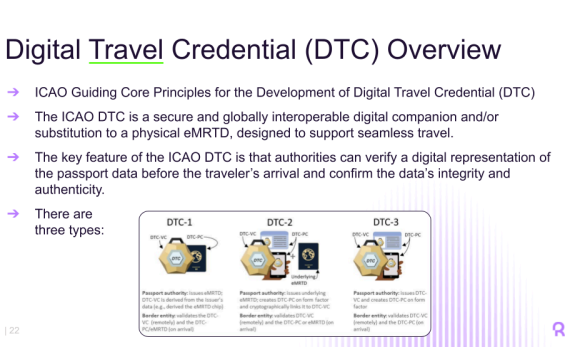



Dmitry Smolyakov:

Another type of digital ID is the quite new Digital Travel Credential. The DTC is a secure digital solution that streamlines travel experiences. ICAO sets the frameworks and standards for it with their Guiding Core Principles for the Development of DTC.

The DTC consolidates key personal information into a single virtual document that travelers can store on their mobile devices or upload to their digital wallets and share whenever needed. The main goal of the DTC is to facilitate travel and ensure that people are eligible to enter their destination before they board a flight.

There are three types of DTC: DTC-VC, a virtual copy bound with a physical ePassport; DTC-PC, which is a physical copy but also bound with a physical ePassport; and finally, a standalone document.

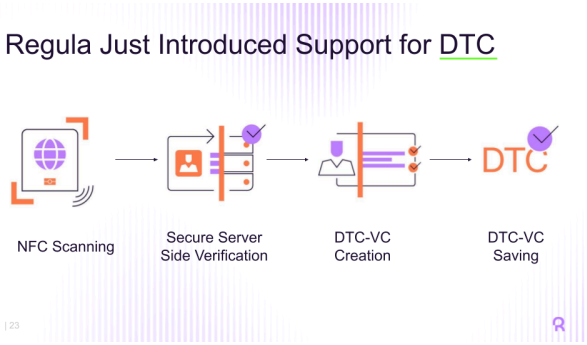



Dmitry Smolyakov:

We at Regula just introduced full support for the DTC.

Now, with Regula Document Reader SDK, a user can create and reprocess the DTC-VC out of an ePassport, as well as verify it by passing DTC-VC data as input. Also, support for handling the DTC-PC has been introduced. In particular, the updated Regula Document Reader SDK can:

- read the document's RFID chip with a smartphone, verify it, and create a DTC-VC;
- recognize, read, and verify the DTC-VC with a smartphone, passport reader, or via server



retrieval;
- read the DTC-PC with a smartphone or passport reader, parse its data, and verify it.

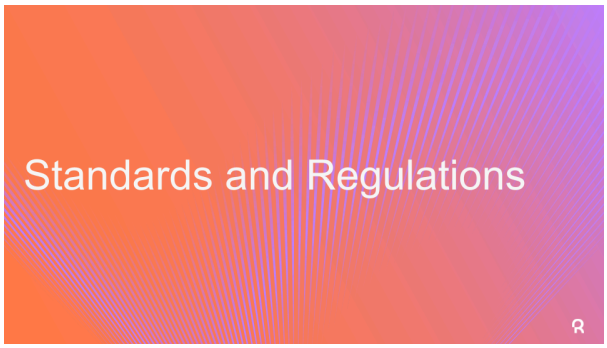
More about Regula's DTC support
https://regulaforensics.com/news/regula-launches-full-support-for-digital-travel-credentials-in-latest-software-update/

ICAO's Digital Travel Credentials: An Expert Breakdown
https://regulaforensics.com/blog/digital-travel-credentials-dtc/

Now Kate, I'd like to pass it back to you.

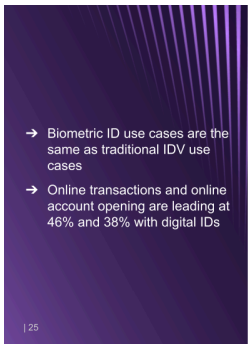

Kate Volskaya:

Thank you, Dmitry! That was a comprehensive story. Now, let's have a closer look at how digital IDs are regulated.




Kate Volskaya:

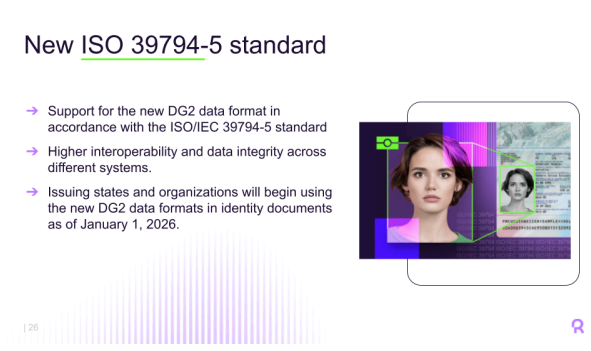
But first, I would like to highlight another insight from our survey. It shows that digital IDs revolutionize various industries that rely heavily on secure and efficient identity verification—especially in online transactions (46%), which are becoming more common for many industries and online account opening (38%). This trend not only streamlines onboarding but also bolsters security, illustrating the new ways we interact with services daily. And of course it should be standardized and regulated, especially to eliminate compatibility issues.




Kate Volskaya:

This new standard defines the requirements for biometric data exchange formats and protocols to ensure interoperability and data integrity across different systems. In simple words, it regulates how the biometric data and photo should be stored in the chip and further processed.

It is important to begin updating your systems now to support the new standard and be able to process such



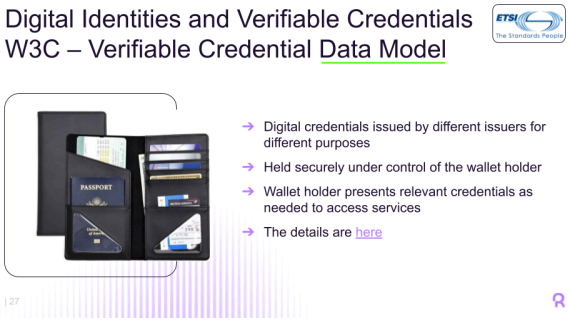
documents, as issuing states and organizations will begin using the new DG2 data formats in identity documents as of January 1, 2026.


Kate Volskaya:

Back to digital IDs. It all started with the World Wide Web Consortium developing a new data model for identity called the credential model.

One of the key challenges is that the existing standards in different countries issue digital credentials for different purposes, and they are not connected. This is a huge problem in making digital ID unified.

Rather than having a single identifier, you have to use a set of credentials for different purposes, for example passports, ID cards, driver's licenses, and payment cards. And in practice, you don't want to present your full physical identity information every time. So the Verifiable Credential Data Model is very user-centric, with different forms of credentials representing your identity. Plus, it is under control of the wallet holder, so you can present the relevant credentials for various services. The W3C standard is shaping different approaches to using digital credentials.



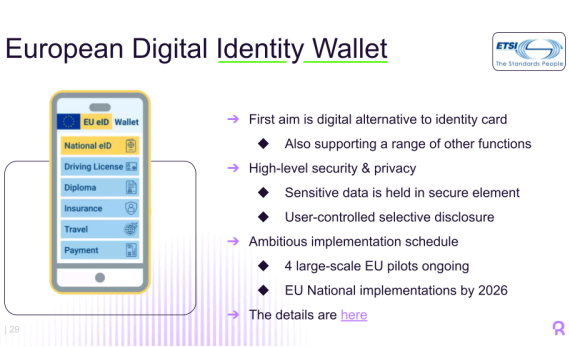

Kate Volskaya:

When it comes to holding your credentials on a mobile device, the ISO has provided a series of standards and frameworks for managing and interoperating your smartphone for mobile based digital wallets and credentials. This work was based on the standard for mobile driver's licenses. The experience has been generalized in this ISO standard, and has been further adapted for use with the W3C Credential Model.


Kate Volskaya:

Another one is the European Digital Identity Wallet. The regulation entered into force in May 2024. The wallet supports the principles outlined in the EU Declaration on Digital Rights and Principles, and will help fulfill the Digital Decade Policy Programme target of 100% of EU citizens having access to Digital ID by 2030. Currently, there are 4 large-scale EU pilots ongoing. All implementations should be done by 2026.

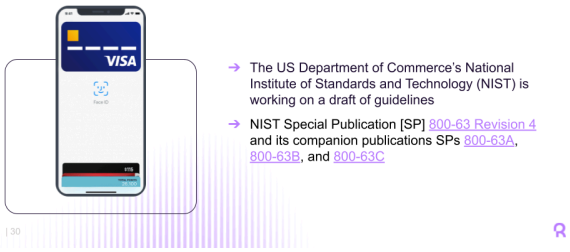
The European Digital Identity Framework amends the eIDAS (electronic identification, authentication, and



trust services) regulation, with the goal of creating a unified approach to electronic identification that works across every member state.


Kate Volskaya:

As for the US, The National Institute of Standards and Technology (NIST) has released updated guidance on a wide range of methods people use to prove their identity, from digital wallets and passkeys to physical IDs. The draft guidelines aim to help organizations manage risks associated with digital interactions while making it easier for individuals to use digital identities successfully, including when applying for government services.



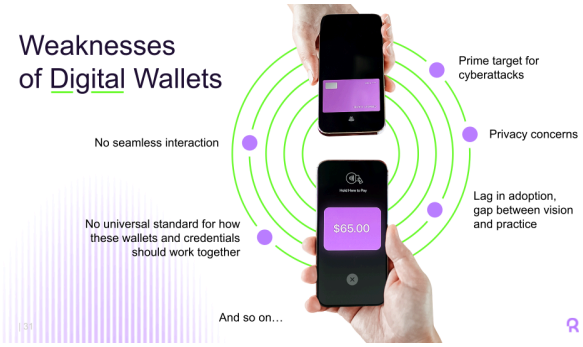

Kate Volskaya:

As we see, there's no universal standard for how these wallets and credentials should work together. One wallet may store a digital driver's license, while another might hold a vaccination record, but if they can't interact seamlessly, the user experience falls short.

With digital identity wallets, you store highly sensitive information like IDs, certificates, and financial records. This makes them a prime target for cyberattacks. If a wallet is compromised, the damage can be extensive, making security a paramount concern.

Many people are unfamiliar with the concept of verifiable credentials or the intricacies of managing their digital identity. Without user-friendly designs and a clear understanding of the benefits, adoption may lag.

One of the biggest promises of digital identity wallets is better privacy. Yet, they can also raise concerns about surveillance and data tracking. In a world where many people are already worried about their data being monitored, introducing a new identity tool can create apprehension.



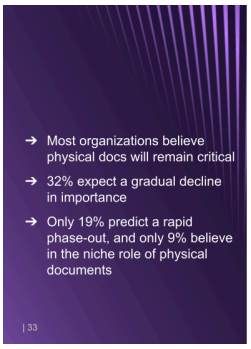
Regula

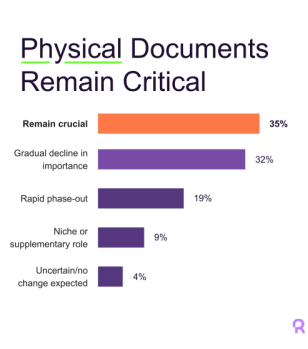

Kate Volskaya:

But how quick will the transition be? Are organizations around the globe ready to shift to the new formats, or do they prefer to work with physical documents?


Kate Volskaya:

Despite the initiatives on issuing new digital formats of IDs, physical documents remain critical. This is confirmed by our survey: the vast majority of organizations believe that physical documents are crucial at the moment, and will continue to be in the near future.






Kate Volskaya:

The advantages of electronic IDs cannot be overestimated. They include:

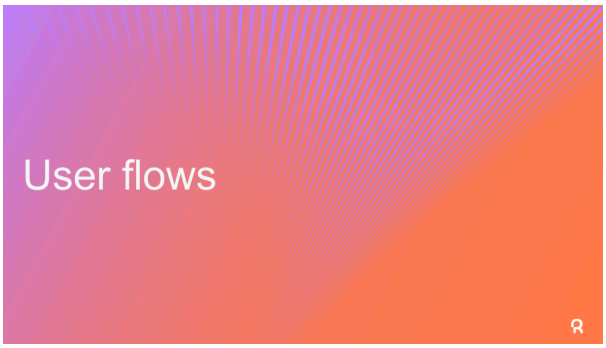
- Enhanced security
- Streamlined onboarding process
- Compliance with regulations
- Improved customer experience
- Cost savings by avoiding manual checks


Kate Volskaya:

And since we're talking about the benefits, Dmitry, let's talk about user flows.


Dmitry Smolyakov:

With pleasure.



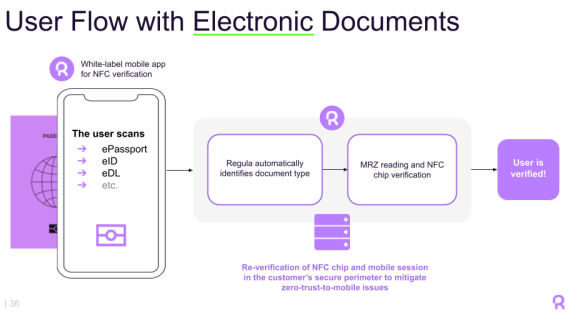
Regula


Dmitry Smolyakov:

Here’s how the flow looks with an electronic passport.

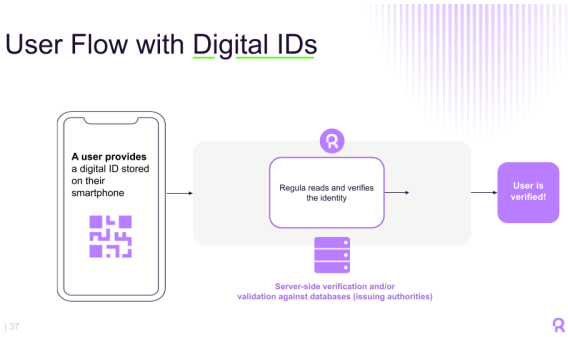
A user scans an electronic ID with an NFC-enabled smartphone with the help of an app, which can be customized in line with your branding. Then, Regula automatically identifies the document type, reads the MRZ, and performs NFC chip verification. In 1-2 seconds, the user is verified.

In addition, you can re-verify the NFC chip on your backend. This ensures higher security and addresses zero-trust-to-mobile issues.



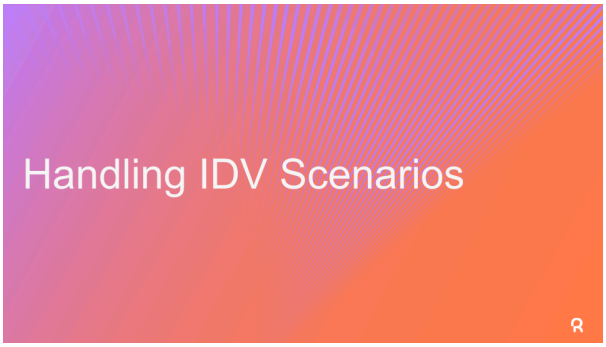

Dmitry Smolyakov:

And here’s an example of the Digital ID flow. A user applies with a digital ID stored on their smartphone. Regula reads and verifies the identity, and checks all the certificates and data. Here, you can also re-verify it on your backend.




Dmitry Smolyakov:

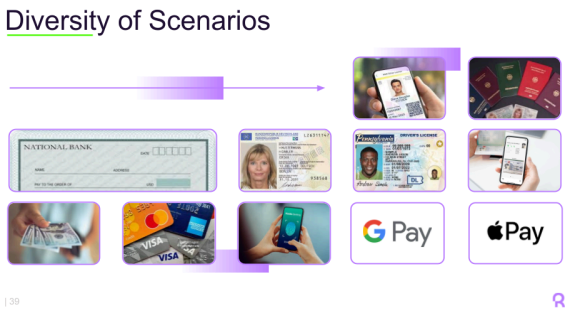
As a company, it may be challenging to handle diverse IDV scenarios, different mechanisms, solutions, and regulations. What a nightmare! :)




Dmitry Smolyakov:

In our daily life, we have various payment options such as cash, bank checks, Apple Pay, Samsung Pay, Google Pay, physical or virtual credit cards, even biometric payments, etc. And a shop, for example, should be able to accept any form of payment.

It’s the same way with identity documents: there are people with traditional documents, electronic passports, driver’s licenses, electronic IDs, mDLs and so on, and no one should be discriminated against, so you should



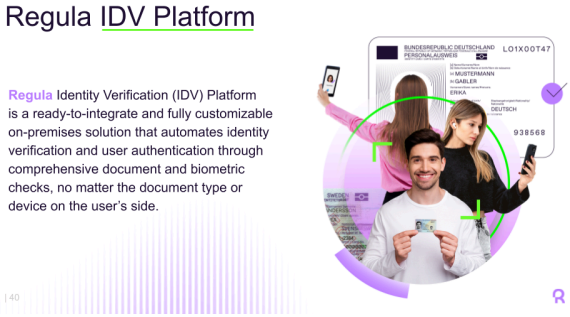
Regula

be able to process and verify each type of ID.


Dmitry Smolyakov:

So, to eliminate the hassle of supporting different solutions for every document type or scenario, we provide Regula IDV Platform.

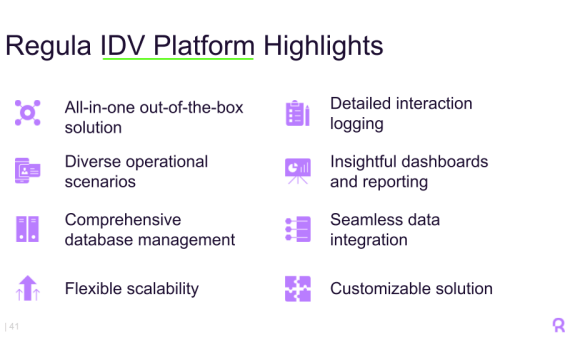
As an all-in-one solution, it mutually supports all the necessary components to perform the required tasks for document and biometric verification, just like with Regula hardware and software, and also with existing 3rd-party hardware components and services as well.




Dmitry Smolyakov:

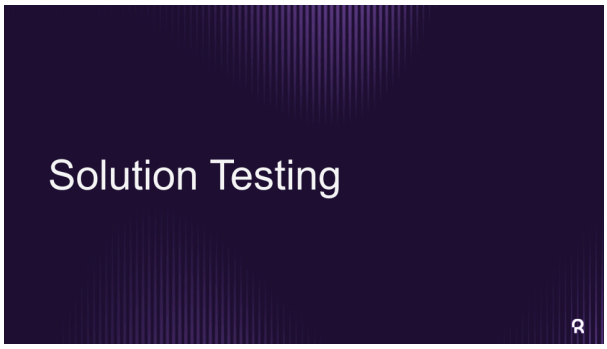
There's a wide range of benefits, including the following:

- Enabling user enrollment, identification and verification through different work scenarios.
- Maintaining a robust database of individuals, including their personal information and biometric data.
- Providing detailed logs of all interactions with individuals in the database for further audit.
- Seamless data integration to easily export and receive data from third-party systems via connectors or API calls for enhanced interoperability.
- Flexible scalability as load and/or data volumes grow without sacrificing performance.
- Customization: client UI with predefined templates that can be presented with any text in any language, images and video; plus a multi-language backoffice UI.
- Also it can be delivered in any way: on-premises or in the cloud, giving you wide flexibility to serve any customer needs.




Dmitry Smolyakov:

Additionally, before full implementation, you can test your solution using mockups to evaluate its functionality, usability, and potential issues. This allows for early detection of design flaws, security vulnerabilities, and user experience challenges. By testing on mockups, you can gather feedback, make necessary adjustments, and ensure a more seamless transition to real-world deployment, ultimately improving the efficiency and reliability of the final implementation.



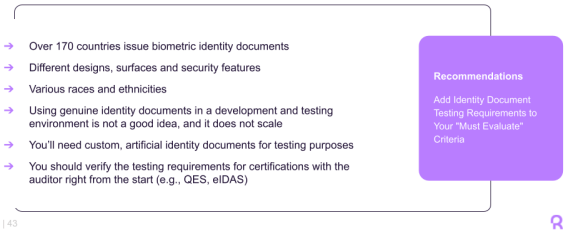
Regula


Dmitry Smolyakov:

For example, say you have to support more than 100 issuing countries. Your employees or project participants will not be able to receive specimens of these passports, ID cards or other documents. And in reality, you don't want to use real passports in an engineering or test environment for data security and privacy reasons. Therefore, you must use artificial ID documents equipped with real NFC chips for verification. These should be test documents, not fake ones.

And you have to check all the error conditions, such as passport expiration date, signature verification failure, etc. You cannot check these things with real ID documents.

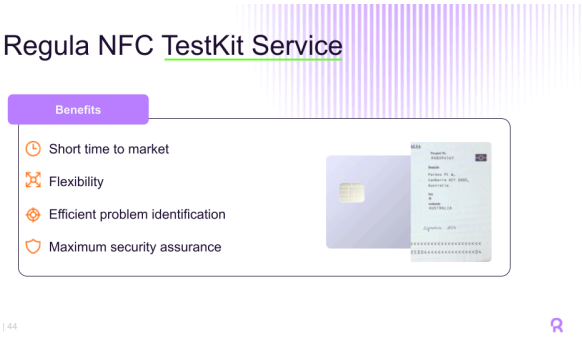
We regularly see our clients encounter such problems. We always listen very carefully to our customers' needs and try to help and develop solutions where possible. We released a new service in response to these needs called Regula NFC TestKit.




Dmitry Smolyakov:

Regula NFC TestKit helps you identify and prevent potential problems in an IDV solution during the testing phase, ensuring system reliability. From a business perspective, I think the most important benefit is that our customers can significantly reduce time to market and accelerate the implementation process.
More about Regula NFC TestKit Service
https://regulaforensics.com/news/regula-introduces-innovative-testing-service/

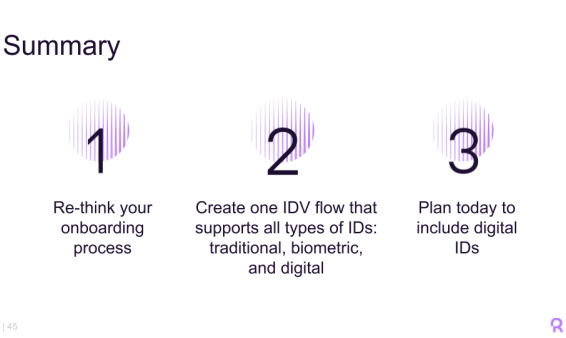
Thanks, Kate. That's all from my side.




Kate Volskaya:

Thank you, Dmitry! That was very interesting. Just to sum up, today, in the era of numerous types of IDs, AI, and deepfakes, it is crucial for us all to know how to deal with these types of IDs. And we consider three pillars:

- Re-think your onboarding process to include digital IDs.
- Create a unified IDV flow to support all types of IDs: traditional, electronic and digital.
- Plan today to include new types of IDs.



Regula

Thank you everybody for your attention!