Enable Secure and Trustworthy Online Identity Verification with the MOBILE CHIP SDK
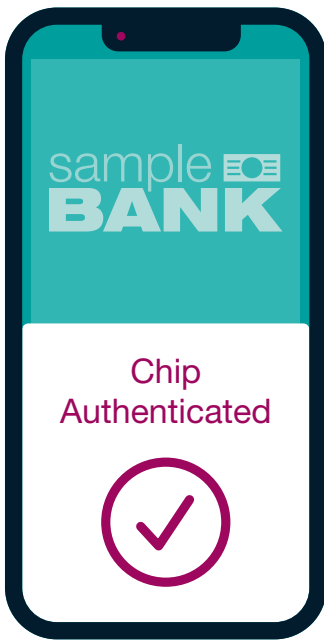
eMRTD Connector | Apps & App Clips | eMRTD Verification Server

MOBILE CHIP SDK – any**time,** any**where,** any **connection**

The Trusted Anchor for Your Customer Identification

sample BANK

Chip Authenticated ✓

Empowering Mobile Security – The MOBILE CHIP SDK securely and reliably reads and verifies chips of electronic machine-readable travel documents (eMRTDs, i.e., e-passports and electronic identity cards). The checks are conducted remotely via a secure server (SaaS) or on premise on your company's infrastructure.

Individually Adaptable Solutions – The MOBILE CHIP SDK consists of various components and can seamlessly be integrated into any identification process. It is compatible with iOS, Android or web-based browser solutions.

Information, Biometry, Document – The MOBILE CHIP SDK serves as the cornerstone of identity verification, as it reliably reads the personal data and picture of the holder from the chip of an eMRTD. These credentials can then be used to populate the identity and for biometric comparison.

# Addressing the Challenges of Digital Identity Verification

Remote Optical Document Inspection is Vulnerable

Optical document inspection is suspect to mistakes and manipulations. In live scenarios, untrained personnel may misidentify counterfeits as genuine; in remote situations, cameras may fail to capture all necessary details or be wrongly operated by the individual that needs to identify himself.

Digital Image Manipulation Risks Data Reliability (morphing, deep fakes)

Various technologies are available to criminals to attack identity verification processes from the outside. In particular, they can introduce falsified information, for example manipulated or wrong photographs. This danger posed by third parties is a serious problem in remote identity check scenarios.
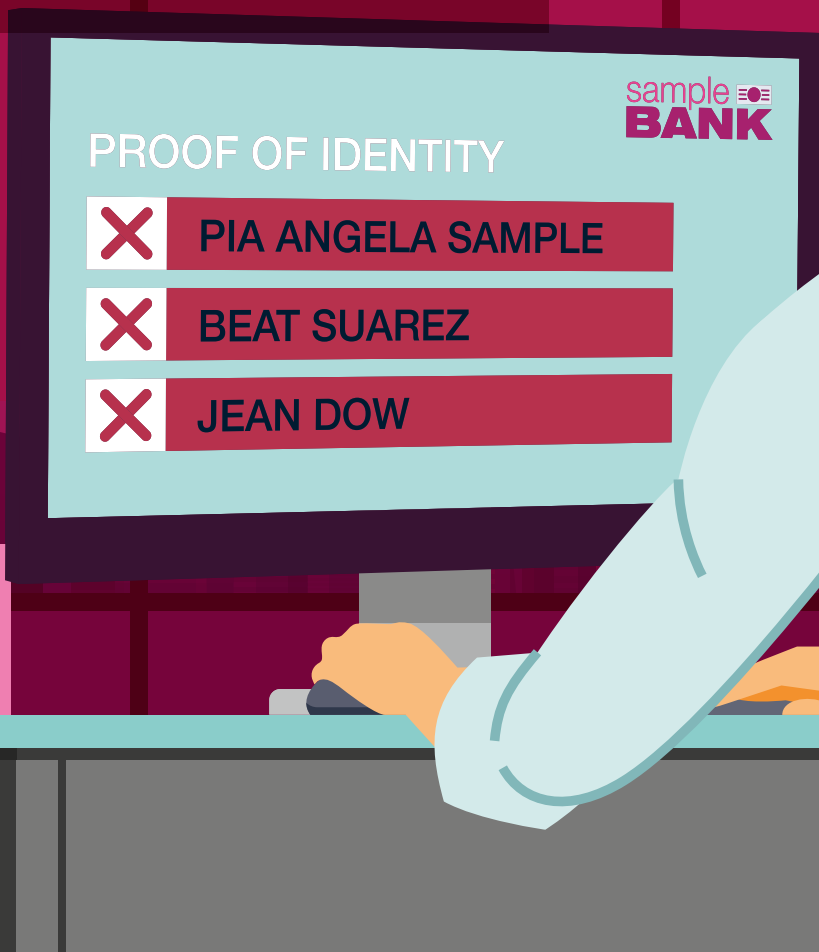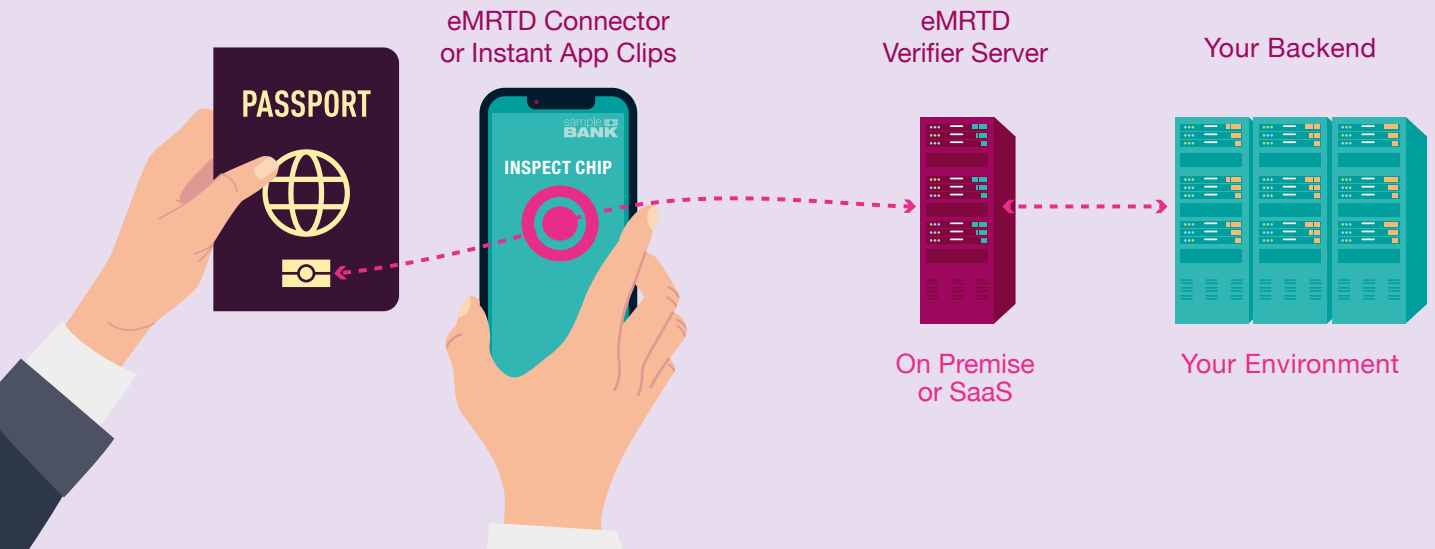
Consumer Devices Cannot be Trusted

The private devices of individuals or citizens who are the subject of the verification process are not trustworthy. Information received from these devices can be manipulated and it is easy for users with malicious intent to submit falsified information – both chip data as well as uploaded images.

Redundancies and Process Inefficiency Cause Frustration

The manual entry of data is cumbersome for users and can lead to mistakes. It is especially frustrating and inconvenient if the same information has to be typed up multiple times at different process steps. In the case of scans, poor image or data quality creates reliability and efficiency issues.

eMRTD Connector
or Instant App Clips

PASSPORT

sample BANK

INSPECT CHIP

eMRTD
Verifier Server

Your Backend

On Premise
or SaaS

Your Environment

Features and Advantages of MOBILE CHIP SDK

The chip of an eMRTD is the trustworthy cornerstone to doubtlessly establish identities online.

The MOBILE CHIP SDK is an essential toolkit for securely and flexibly verifying electronic identity documents. It enables the trustworthy and highly secure check of e-passports and electronic identity cards, creating conve-

nience and security in remote ID check scenarios, mobile and web-based identity verification, as well as during on-the-spot document checks. In full compliance with ICAO 9303 regulations, it provides confidence in an individual's document, biometrics and the available information.

Chip Offers Maximum Security in ID Verification
Reading and verifying the chip of an eMRTD offers maximum security in any ID verification scenario. The MOBILE CHIP SDK verifies a chip's digital signatures as well as its authenticity and integrity. It can even assist in cloning checks, making it the method of choice for secure identity verification.

Chip Provides a Trusted Photograph
The photograph contained in an eMRTD's chip is a trustworthy basis for identity checks. It can be used as a reference for selfies, video identification or for comparisons to the live person.

Secure Server Overcomes End Device Issues
The MOBILE CHIP SDK consists of several components that enable a secure and seamless document verification process. The secure server offers a trusted and ICAO-compliant check environment.

High Quality Data for Highly Efficient Processes
The MOBILE CHIP SDK's capacity to extract and process the chip-stored photograph and personal data eliminates the need for manual, let alone multiple data entries and handling. The obtained high-quality data can be directly used for further purposes.

Flexible Individualization Options

The MOBILE CHIP SDK is highly customizable to any identity verification scenario and use case. It can be provided as an SDK, as a complete app for mobile devices, or as a component for web-based verification

solutions. Based on the individual requirements, the look and feel of MOBILE CHIP SDK can be freely determined to seamlessly integrate into the respective environment, process, app, or user experience.
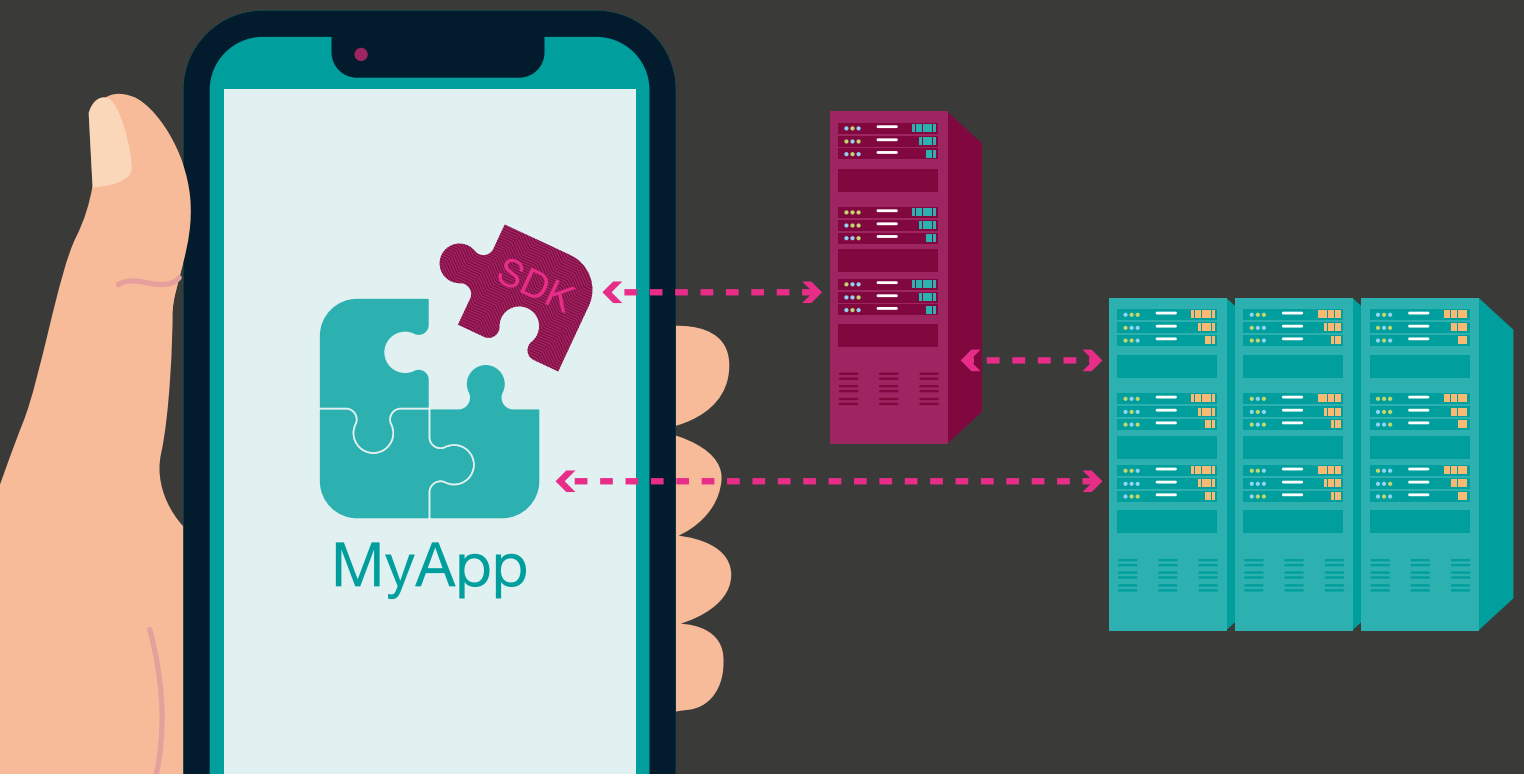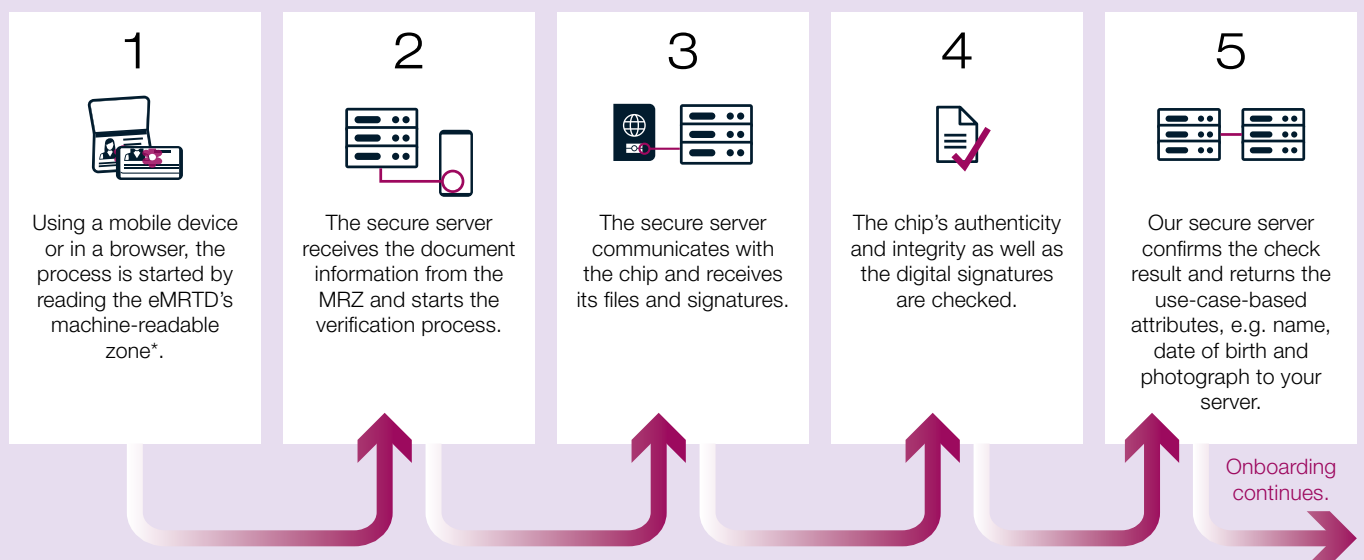
Technicalities of MOBILE CHIP SDK

OVD Kinegram's MOBILE CHIP SDK is characterized by its reliability and flexibility. Offering online and offline functionality, it can be perfectly integrated into existing apps and processes, including app-clip solutions. Its highly secure server provides speedy and reliable verification of the chip data in eMRTDs according to ICAO 9303 standard.

A typical remote onboarding scenario using MOBILE CHIP SDK entails:

1
Using a mobile device or in a browser, the process is started by reading the eMRTD's machine-readable zone*.

2
The secure server receives the document information from the MRZ and starts the verification process.

3
The secure server communicates with the chip and receives its files and signatures.

4
The chip's authenticity and integrity as well as the digital signatures are checked.

5
Our secure server confirms the check result and returns the use-case-based attributes, e.g. name, date of birth and photograph to your server.

Onboarding continues.

* A suitable tool for reading the MRZ is necessary for this step and can either be provided by OVD Kinegram or may already be part of the customer's existing ID verification solution.

For further details on the technicalities of MOBILE CHIP SDK, refer to Knowledge Base of OVD Kinegram.

KINEGRAM is the world's most advanced security solution for the protection of government documents. More than 120 countries trust the innovative capacity of OVD Kinegram AG.
Experience the capabilities of OVD Kinegram's MOBILE CHIP SDK in advanced identity verification and join us in our mission of protecting identities!

Contact us for a DEMO

Learn how the MOBILE CHIP SDK can enhance your identity verification and customer onboarding. Contact us for a personalized consultation!

Stefan Gabriel
Head of Digital Solutions
stefan.gabriel@kinegram.com | www.kinegram.digital
Phone   +41 41 555 20 40

Stefan Gabriel is the Head of Digital Solutions at OVD Kinegram AG. With over a decade of experience in designing, developing, and implementing IT systems and digital products, he drives the company's efforts in identifying and delivering cutting-edge solutions. His work focuses on enhancing secure digital identity verification and ensuring reliable, user-friendly document authenticity checks. His passion lies in creating innovative, robust digital solutions that keep pace with the ever-evolving tech landscape. Stefan regularly shares his knowledge and expertise through presentations, workshops, and articles.

Contact

OVD Kinegram AG
Zählerweg 11 | 6300 Zug | Switzerland
www.kinegram.com

KINEGRAM DIGITAL POLICING is based on a cooperation with Dycom AG.
Some Swiss polices use MACS extended with OVD KINEGRAM document verification modules.