Trask ZenID

Information from personal documents (ID card, driving license, passport, etc.) remains a key element in the client identity verification process. The usual procedure of having clerks manually copy details is laborious, lengthy, and error-prone. In addition, the human eye cannot detect high-quality counterfeits. A shift of client interaction to the mobile and online environment requires new approaches to personal identification, including reliable text recognition in digital images. Advances in optical character recognition (OCR) technologies, from special-purpose devices to multi-purpose interactive systems, have lowered the cost of data capture and fostered the development of more reliable solutions.

Functionalities and Methods

Example:
Online loan application with ZenID client verification
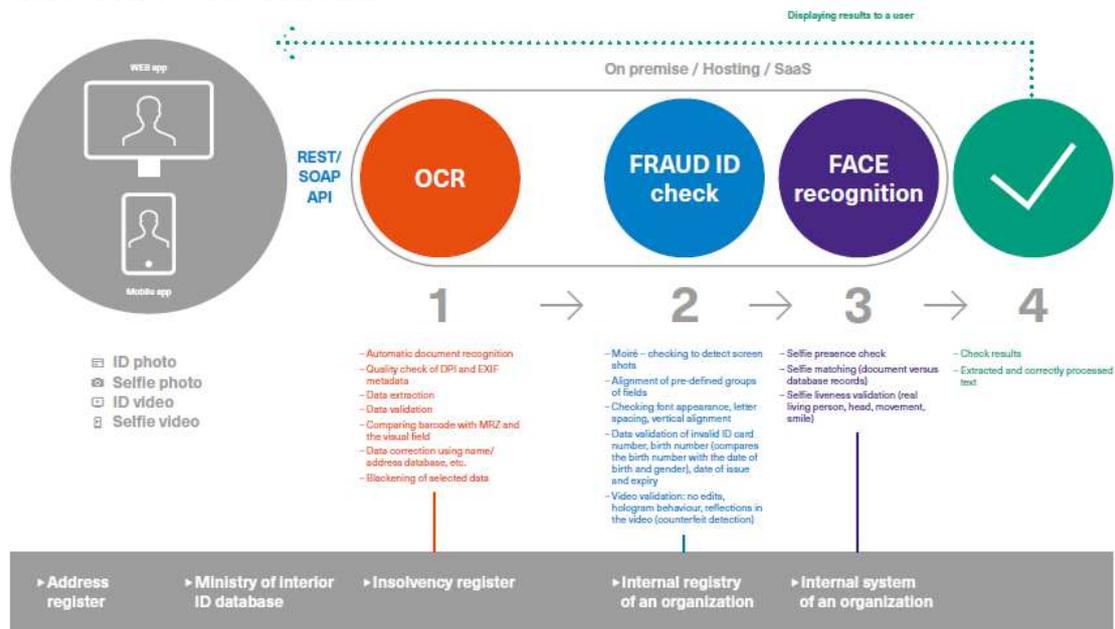
Security and Compliance

1. ZenID complies with data security requirements under applicable legislation including GDPR

ZenID is protected not only against an external attack and abuse, but the solution also complies with applicable legislation, in particular, the General Data Protection Regulation (GDPR). It provides for the data subject's right of access to personal data, the right to be forgotten and other rights guaranteed by the regulation. Processing of personal documents via OCR simplifies access to personal data upon request. Digitization improves the security of personal data over physical copies and reduces the risk of data theft, leakage or loss. ZenID meets the GDPR requirement to protect personal data with due regard to the state of the art by implementing measures such as secure storage and access control.

2. Malicious code protection

The greatest risk in automated systems for the processing of digital documents provided by the client is associated with corrupted or intentionally modified files with the potential to crash the application, or files containing malicious code aimed at the verification system or other systems of the service provider. Trask ZenID is protected against such risks with a range of security measures that prevent processing of damaged or altered files and activation of harmful code.

Implementation Schedule

A specific project implementation plan depends on the number of modules selected. In the example below, we provide a schedule for a single server implementation on the client's own infrastructure in the multitenant mode. Upon signing a contract, a typical implementation would proceed as follows:

: