

eID scheme: SMART-ID

Version 3.0

Version History			
Date	Version	Version info	Author
19.10.2021	3.0	Amended biometric identification registration method and added Smart-ID for Electronic identification	SK ID Solutions
01.04.2020	2.0	Added biometric identification as a new registration method	SK ID Solutions
26.08.2019	1.0	Public version	SK ID Solutions

1. Introduction

Smart-ID solution is an electronic ID solution to take advantage of the smart capabilities of the mobile devices and offering the high level of security to users and equipping online service providers with a reliable and secure end-user access management tool. Smart-ID has reached over 3 million users in Baltic countries. Smart-ID is being operated and developed by SK ID Solutions AS (SK) in collaboration with Cybernetica AS.

A technology has been used in this product for which Cybernetica AS has filed a patent application or a patent has been granted.

Smart-ID enables end-users to utilise their existing mobile devices to register securely and later use the mobile device to authenticate to service provider's systems (such as websites, apps and call centres) and to give electronic signatures according to the EU legislation and therefore recognised in across EU.

From November 2018, Smart-ID is recognised as a QSCD (Qualified Signature Creation Device). It means that signatures given with Smart-ID have the same legal standing as signatures given by hand (QES level).

On February 2020, SK ID Solutions revealed a new registration method for Smart-ID. The option of using a biometric identity document to create an account was added. The new option was made available to users who had previously used Smart-ID. The new addition to the Smart-ID service was created as a result of the cooperation between multiple international companies. In addition to SK ID Solutions, InnoValor from the Netherlands and iProov from the UK were also involved in the development process. The solution was evaluated by the German certification company TÜV Informationstechnik GmbH. In May 2021, the requirement that in case of Automated Biometric Identity Verification (ABIV), the Subscriber must have or have had Smart-ID account was replaced by Secondary Subscriber Authentication sub-process.

Smart-ID solution is based on the known and proven principles of the public key cryptography, electronic signature schemes and PKI (Public Key infrastructure). The private key of the user is never generated or combined in a single place of location. Instead, a distributed protocol is used that generates, processes, stores and protects the private key. It splits the key between the app and the secure server and separates their physical locations. Smart-ID complies with the highest international standards (eIDAS, PSD2).

Smart-ID is deployed in high-availability and fault-tolerant setup and is designed to be used in systems and applications with extensive number of users and user operations (e-government and financial systems, large-scale commercial platforms etc.). Smart-ID is fast, as it enables user authentication and digital signing at the speed of instant messaging.

Smart-ID is easy to use and free of charge for the end users. The users can have Smart-ID always with them in their smartphone, tablet or other smart device with Android or iOS operation system. Smart-ID is not dependable on a SIM card, and can be used in multiple devices.

Advantages of Smart-ID:

- High level of security – the PKI and digital signature technology combined with modern smart devices and process controls can mitigate many security risks and defeat cyber-attacks and fraud attempts.
- Signatures recognised all over the EU – electronic signatures given with Smart-ID are accepted in the EU member states, because Smart-ID complies with eIDAS AES and QES requirements.
- Strong authentication – the PKI based Smart-ID solution is compliant with European Central Bank's requirements for strong customer authentication.

- Innovative technology – Smart-ID uses split key technology for implementing transactions, where user's private key is equally stored in the server and in the app, making it non-replicable and non-stealable.
- SIM independence – Smart-ID is developed using the smart device's software security module, meaning that the app is not SIM card dependent and the communication between app and server takes place over the internet using secure HTTPS connection.
- Non-repudiation of operations – the digital signature-based authentication protocol links the user's private key to the authentication outcome and therefore nobody else could perform authentication for him.
- Easy integration to e-services – easy and secure access via Smart-ID will attract more customers to use e-services. Smart-ID solution is based on simple REST API that can be easily used from all modern development frameworks.
- Single-Sign-On solution – Smart-ID can be used as a Single-Sign-ON solution to different e-services using unique external identifier (for example national id code). This increases the convenience for end-users by not having to remember multiple usernames and passwords.
- Cross-usage – in addition to cross-sector use, Smart-ID is created for using on different operating systems (Android, iOS), as well as multiple devices per person.
- The end-user app is user-friendly, intuitive and easy to operate, even for those users who lack digital confidence.
- Easy remote on-boarding – registration process is flexible and versatile as different authentication methods are available and it takes just couple of minutes.

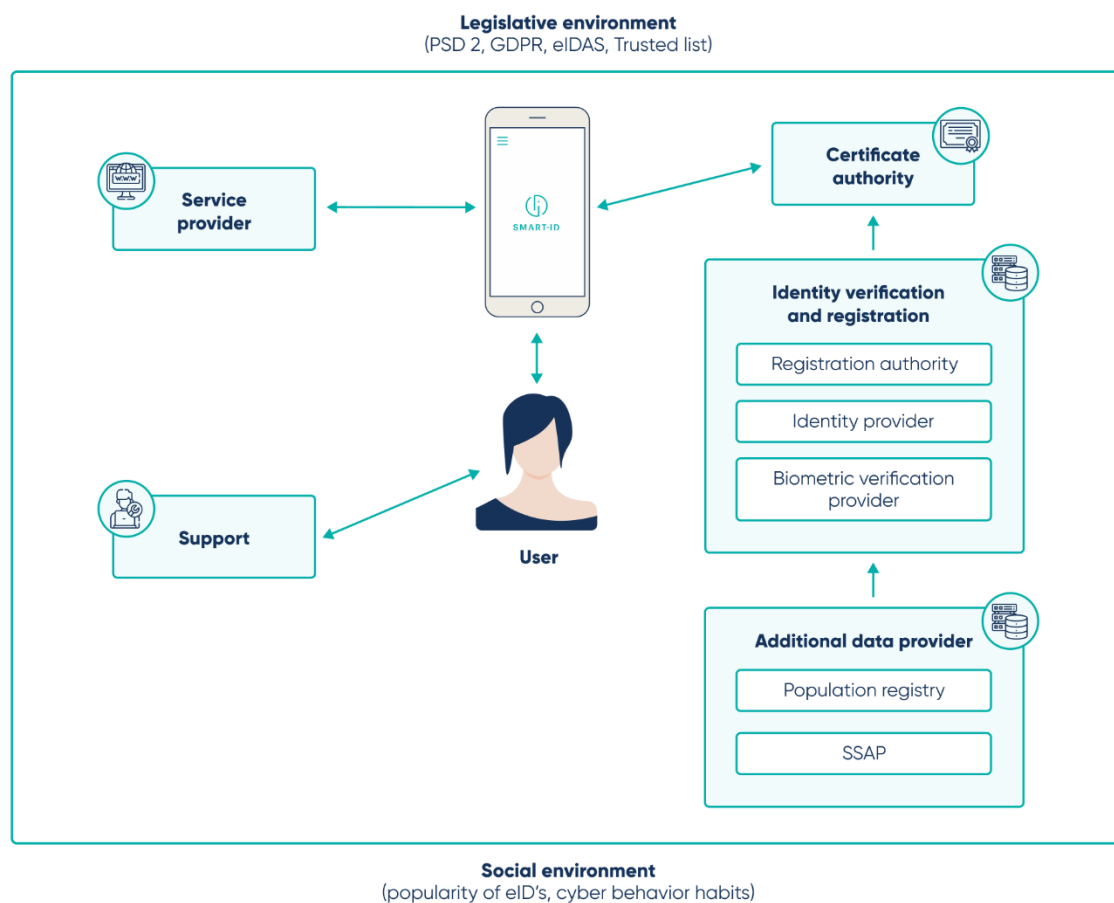
1.1. Smart-ID ecosystem

Smart-ID has been designed as user-centric ecosystem to offer seamless authentication in a secure way for end-users and service providers.

Smart-ID ecosystem consists of the following parties:

- Smart-ID service – audited and certified Smart-ID core service
- Identity provider for Smart-ID solutions – Smart-ID is based on an existing identity (ID-card, Mobile-ID).
- Biometric verification provider - an organisation who offers eMRTD (electronic Machine Readable Travel Documents following ICAO Doc9303 specifications) reading and validation services, service for biometric verification and liveness detection of Subscriber during Automated Biometric Identity Verification (biometric identity document).
- Service provider – integrates Smart-ID web interface to an existing e-service and enables secure access to the end-user.
- Registration authority – audited issuer of Smart-ID in branches or customer service points based on existing national identity document.
- Technical support - provides customer support for users during registration and day-to-day usage.

- **Certification Authority** - Issues certificates for Smart-ID based on identity derived from Identity provider, Biometric verification provider or Registration Authority. Issued certificate is used for Smart-ID transactions
- **Population Registry** - Identity derived from Identity provider, Biometric verification provider or Registration authority is verified against national population registry to minimize errors caused by name change and etc.
- **Secondary Subscriber Authentication Provider (SSAP)** - facilitates or performs Secondary Subscriber Authentication during enrolment process for assurance of Subscriber awareness by either delivery of authentication message to Subscriber or requesting Subscriber to perform authentication with electronic identification mean.



1.2. Using Smart-ID

Usability and ease of usage have been part of the core values during development of Smart-ID.

Smart-ID allows end-users to use their existing mobile devices to register for a securely verified Smart-ID account and later use the mobile device to authenticate themselves quickly, easily and

securely in different e-services (via websites, apps and call centers) and to give electronic signatures according to the eIDAS regulation, which is recognized in EU member states. Day-to-day usage of Smart-ID is carried out by simple and user-friendly smart device application, making it easy and intuitive even for users who lack digital confidence (e.g. elderly people). Onboarding is flexible and versatile as different authentication methods are available and it takes just couple of minutes.

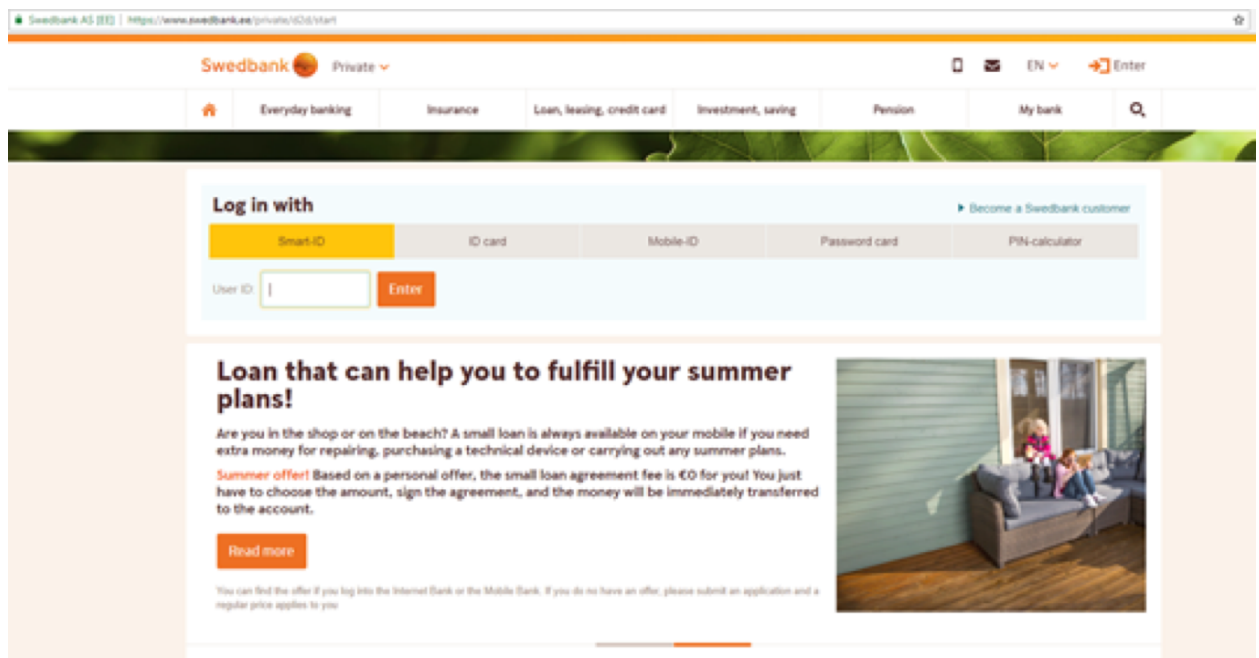
Compared to physical token-based authentication methods such as Fido token or national ID card, the everyday usage is much more convenient as for most people smart device is always at hand and there's no need to carry something additionally along. Smart-ID is flexible supporting Android and iOS smartphones, tablets and even smart watches. There's a long backwards compatibility for supported operating systems. User can have Smart-ID set up on multiple devices and use them in parallel, whereas each device will have an unique account per device.

Using Smart-ID does have high requirements for internet connection of the smart device but uses only limited amount of bandwidth so even the most basic internet connection (either wifi or mobile internet) is sufficient and would therefore not generate significant indirect costs to users.

Using Smart-ID for authentication

To use Smart-ID for authentication, the end users need to follow these steps:


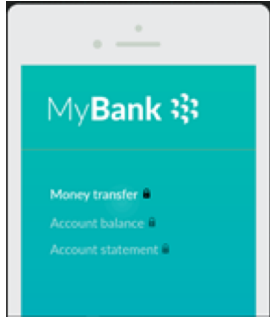
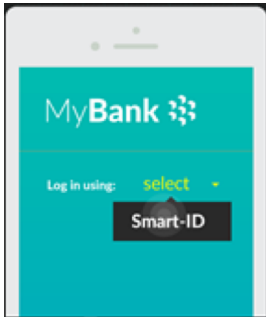
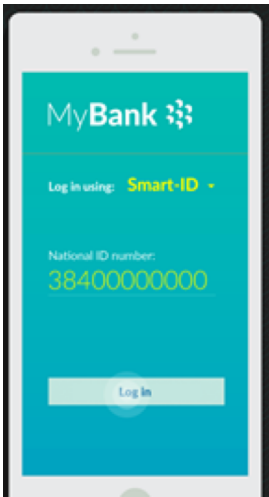

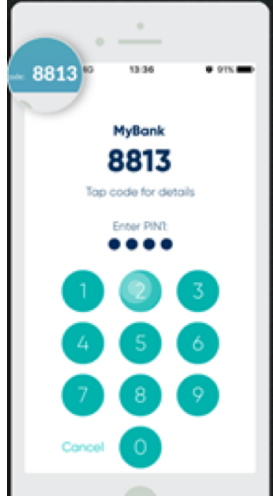

- Enter the website of an e-service provider in the smart device and choose for authentication Smart-ID. Example of log in option in the online banking system of Swedbank:

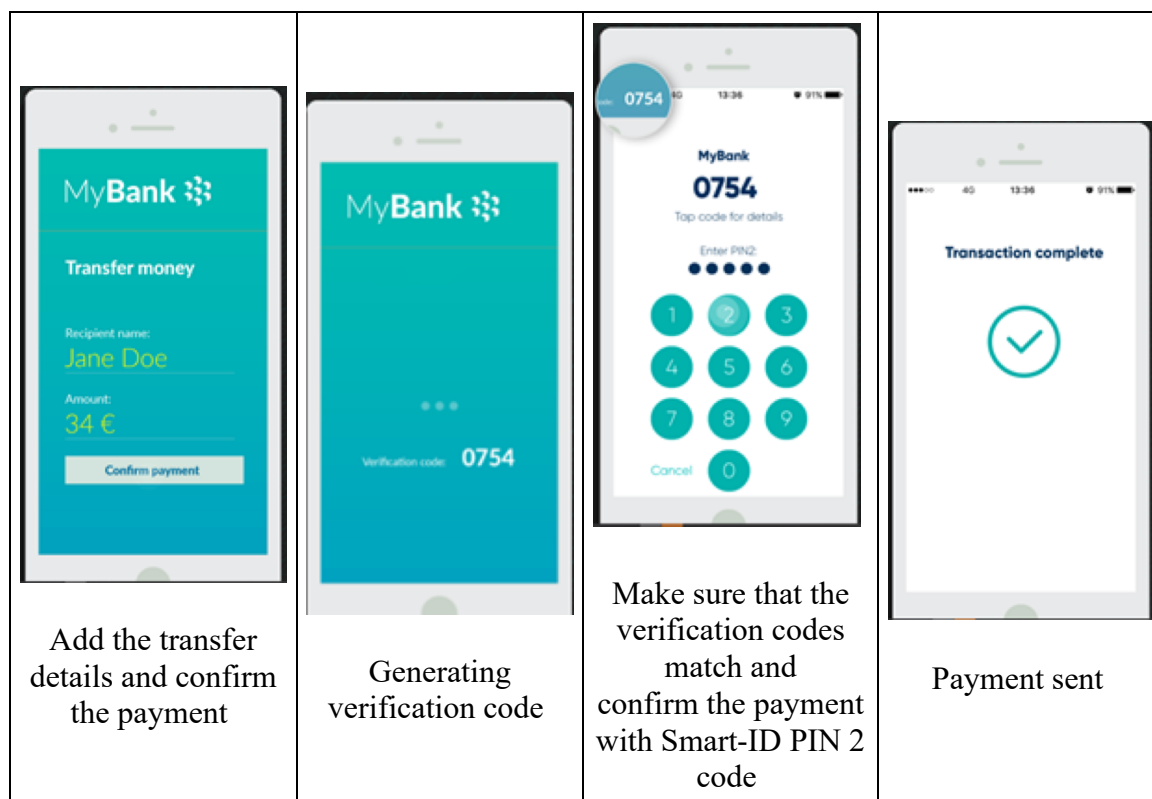
The image is a screenshot of the Swedbank online banking login page. At the top, there's a navigation bar with the Swedbank logo and a 'Private' dropdown menu. Below this is a horizontal menu with various banking services: 'Everyday banking', 'Insurance', 'Loan, leasing, credit card', 'Investment, saving', 'Pension', and 'My bank'. The main content area is titled 'Log in with' and features five buttons: 'Smart-ID' (highlighted in yellow), 'ID card', 'Mobile-ID', 'Password card', and 'PIN-calculator'. Below these buttons is a 'User ID' input field and an 'Enter' button. A promotional banner for a 'Loan that can help you to fulfill your summer plans!' is displayed below the login section, featuring text about a summer offer and a 'Read more' button. To the right of the text is an image of a person sitting on a sofa.

- Enter username (for this e-service or for Smart-ID) and receive a notification to the device connected with Smart-ID.

- Check the verification code and e-service name in the e-service portal and Smart-ID app notification to ensure that they match and enter PIN 1.

Example on using Smart-ID for bank authentication and transaction signing on mobile device:

 <p>Open the bank application on the mobile device</p>	 <p>Choose the preferred action</p>	 <p>Choose Smart-ID is the authentication option</p>	
 <p>Insert your national ID number</p>	 <p>Generating verification code for authentication</p>	 <p>Make sure that the verification codes match in your bank and the Smart-ID app</p> <p>Enter PIN 1 code in the Smart-ID app to log in to your bank</p>	 <p>You are now logged in to your bank</p>



1.3. Registering for Smart-ID

After downloading the app from app stores (see more information smart-id.com) a one-time account registration must be completed to start using Smart-ID. Registration is necessary to verify the identity of the user and generate the private-public key pairs. From the user's perspective, the registration process may have some differences depending as an example on the authentication method used or the age (under age of 18 users have special registering flow) of the user, but the overall process follows same basic steps.

The app asks the user to start the registration after downloading. The registration process consists of the following steps.

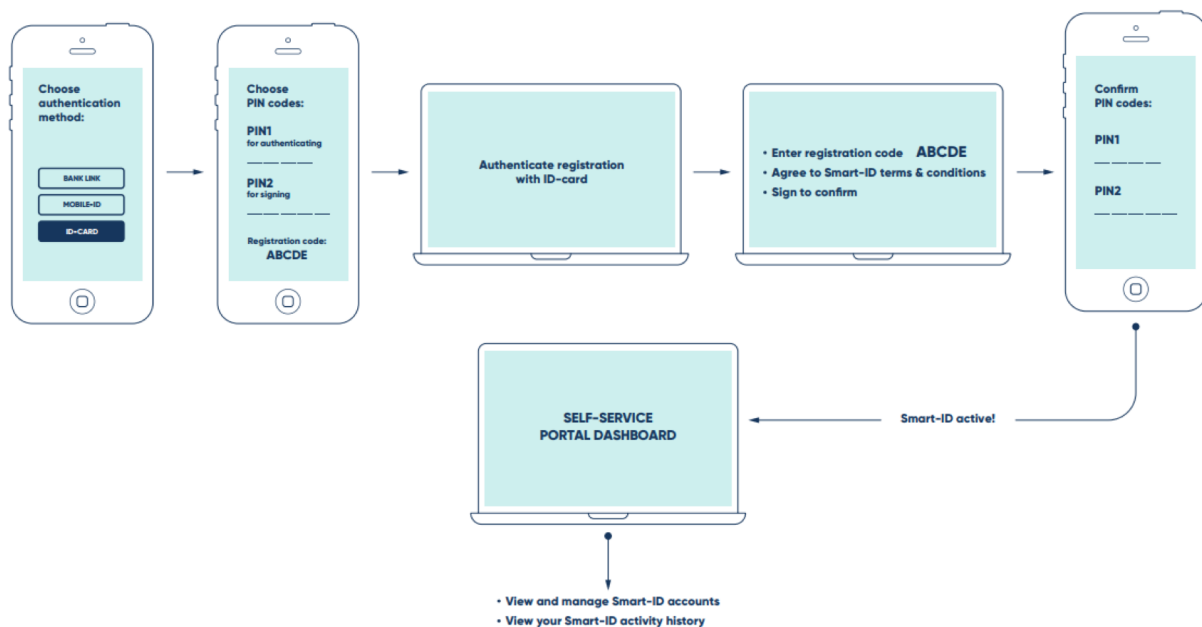
- Choosing country of residence
- Choosing identification method:
 - Using Mobile-ID – registration can be carried out on the smart device. App initiates the Mobile-ID authentication process and user will verify identity with Mobile-ID PIN code.
 - Using ID-card – user is asked to start a desktop browser session and authenticate himself in Smart-ID self-service portal.
 - Using (existing) Smart-ID – user performs registration of new Smart-ID account within Smart-ID app and signs application with existing Smart-ID.
 - Using biometric identification - registration can be carried out on the smart device. User's phone must have a working camera and must support NFC, and the user

must own a biometric identity document. Verification of the Subscriber's identity performed based upon face matching and liveness detection through a deep learning algorithm. In the course of ABIV, comparison is made between a snapshot taken from a selfie video stream against the image of the person read from the eMRTD chip. Secondary Subscriber Authentication process will be performed for assurance of user awareness about ongoing Smart-ID registration..

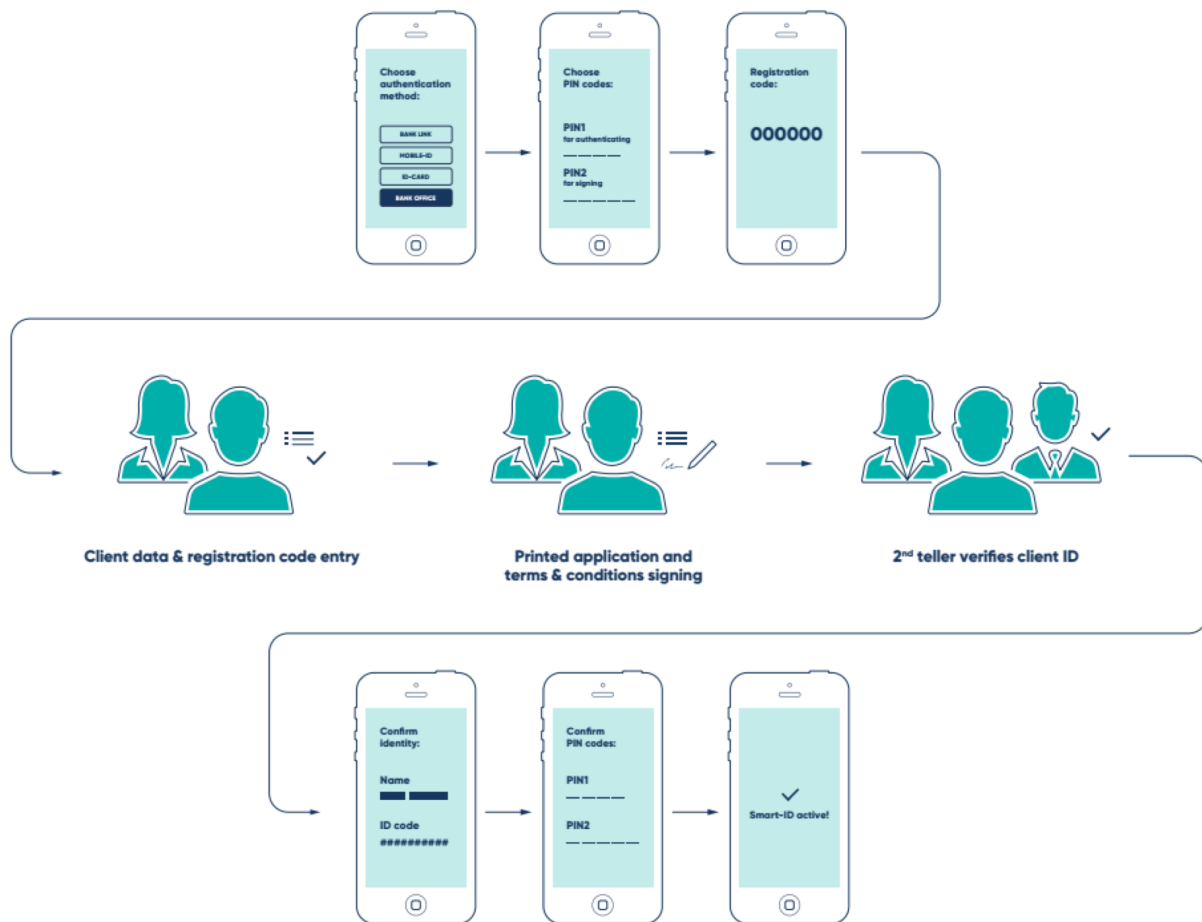
- Via registration authority (such as bank). In service provider's point-of-service where registration authority's representative verifies the identity of the user, terms and conditions and application are signed.
- Accept terms and conditions for use of Smart-ID certificates and in addition with ABIV consent to process biometric personal data
- Enter contact information (phone number and e-mail address)
- Creating PIN codes for the Smart-ID app. It's possible to create custom PIN codes or generate random PIN codes:
 - PIN 1 code for authentication in e-services (e.g. online banking, e-school, etc.)
 - PIN 2 code for signing documents and confirming transactions (e.g. bank transfers).
- Confirm identity - user must check if the identity and personal information is correct.
- Re-enter PIN codes to sign the certificate requests to conclude the registration.

After these steps the app is ready to use for authentication. Simplified flow of the registration process is shown on figures below.

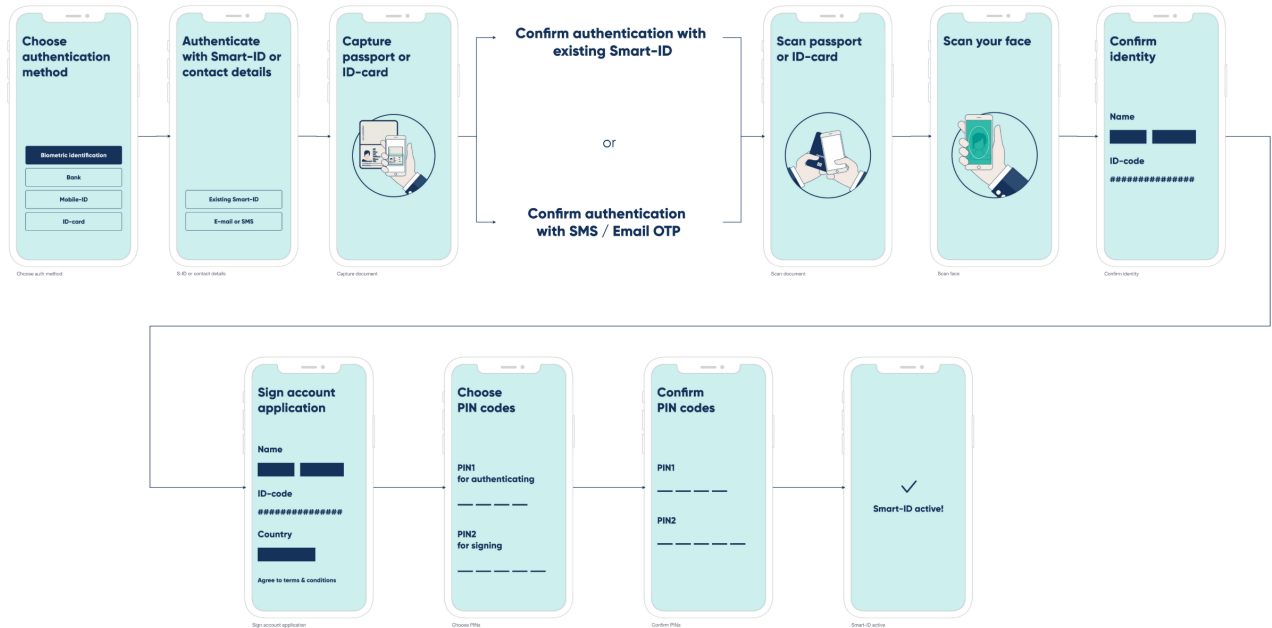
Registration process if ID-card is used for authentication:



Registration process if registration authority's point-of service authentication is used:



Registration process if biometric identification is used:



1.4. Usability for Service Providers

Smart-ID is offered as a service, hence there's no extra hardware required for the e-service provider and technical support for the service provider and end user is managed by SK. The usage of common JSON/REST API in Smart-ID ensures a fast and easy integration to the service providers website. Furthermore, SK provides free client libraries and open demo environment to further ease the process by providing useful guidance. Smart-ID provides fast and flexible integration. Transaction-based subscription model offers easy to manage and transparent day-to-day usage.

Smart-ID is convenient to use for service providers who wish to authenticate users. Using API's allows service providers to customise the authentication dialog and better integration with their web-page. Service provider can customise the design and user experience.

1.5. Reliability

The reliability of Smart-ID is assured by the solution's track record to date as well as by the compliance with leading regulations in the field of authentication and digital signatures. In terms

of electronic authentication and digital signatures, the European Telecommunications Standards Institute (ETSI) and electronic transactions in the internal market (eIDAS) are the most comprehensive frameworks that a product can satisfy. Smart-ID solution and set requirements correspond to ETSI standards stated under European Union regulation N°910/2014 on electronic identification and trust services for eIDAS.

Smart-ID is a reliable and trustworthy solution as it satisfies requirements of eIDAS and ETSI standards. Reliability of Smart ID is achieved by:

- Server-side services run on a high availability infrastructure composed of multiple nodes across two datacentres to maintain availability while maintenance is conducted.
- Smart-ID environment is separated into Live (Production), Demo, Test and Development sections, segmented according to the industry practices.
- Change and maintenance activities are carried out following the established rules based on ITIL.
- Security aspects of the infrastructure are under constant logging and monitoring.
- Due to Smart-ID architecture, replay attacks are caught by the system and therefore effectively prevented.
- SK is an established company offering a variety of trust services. Therefore, SK as a company is a constant subject of extensive compliance requirements. The company is familiar and confident with the CA and eID requirements at eIDAS QES level.
- Smart-ID is developed and operated by experienced companies specialising in trust services and security and constant subjects of extensive compliance requirements. The related parties that have developed Smart-ID – SK ID Solutions and Cybernetica AS – have a long history and extensive experience in technological innovations and solutions which adds to the credibility of Smart-ID.

From the standpoint of an information technology solution, the following aspects are of elevated interest:

- Everyday activity of SK is regulated by numerous outside regulations and internal policies and practices (<https://www.skidsolutions.eu/en/repository/>).
- SK is being regularly audited as a mandatory precondition of being certified against ETSI requirements, having status as qualified trust service provider under eIDAS and belonging to the Trusted List of Estonia (<https://sr.riik.ee/en.html>).
- SK is a member of the European Cyber Security Organisation (ESCO), Digital Trust and Compliance Europe (DTCE), Estonian Association of Information Technology and Telecommunication (officially abbreviated as ITL), European Telecommunications Standards Institute (ETSI) and CAB Forum, thus participating in several professional networks.
- The architecture and design of the Smart-ID solution is published and available at: <https://github.com/SK-EID/smart-id-documentation/wiki/Technical-overview>. These measures, standards and procedures ensure the actual technical solution is accomplished on a level suitable for certification, attestation and audit. Smart-ID server-side services run on a high availability infrastructure composed of multiple nodes across two datacentres to maintain availability while maintenance is conducted.

SK has been audited by relevant authorities and the audit (see latest and valid eIDAS certificate for creation EID-SK qualified electronic signature certificates from: <https://www.skidsolutions.eu/en/repository/audit/>) certifies Smart-ID as a qualified signature, the highest eIDAS level for signatures (since same CA is used for authentication certificates, then this certification applies for authentication as well). The development process is regulated, and the code is audited. For the most important and critical components, an additional layer of protection against manipulation of the code is used that is evaluated under QSCD. The assessment concluded that controls performed by SK during Smart-ID automated biometric verification enrolment process are rated to be stronger controls regarding the identity verification of the person than the controls provided by a typical average human based face to face identify verification.

1.6. Security

Smart ID's security is based on an implementation of a split key RSA scheme, and on proven principles of public key infrastructure and threshold cryptography. Smart-ID's underlying split key solution is a modification of threshold cryptography of a previous state-of-the-art RSA scheme and combines set of properties:

- The server alone is unable to create valid signatures.
- Having the client's share, it is not possible to create a signature without the server.
- Smart-ID application does not store any passwords which means that the account is safe even if the smart device itself is lost.
- The server detects cloned client's shares and blocks the service.
- Having the password-encrypted client's share, the dictionary attacks cannot be performed without alerting the server.
- The composite RSA signature "looks like" an ordinary RSA signature and verifies with standard crypto-libraries.

There are additional security measures:

- Protocol includes control code, which allows user to verify is the PIN request. Control code is computed from the data to be signed (DTBSR) by Smart-ID app and by the service provider itself.
- Service provider must verify the end users' signature and verify that hash is the same as service provider used to start authentication.
- Entries of wrong PIN codes is limited and after too many entries of wrong PIN in a row the account will be blocked without possibility to recover it to protect it from dictionary attacks.
- Smart-ID uses a clone detection protocol around signature protocol that allows the server to detect multiple instances of the client for detection of fraud.
- Development security measures ensure that the source code and its associated design information are protected from interference or disclosure.

- Thorough testing of the security functionality is conducted by the development team. The requirements for designing and conducting the testing are stated in the Common Criteria standard.

SK has been certified in the field of information security (certificate ISO/IEC 27001:2013) after passing the ISO audits in the fields of certification and digital signature technology and applications development. This states that Smart-ID, a product provided by SK, is following the international security standards and uses the highest security measures available in providing the service to the clients. Cybernetica AS, the technology developer, has been certified in the field of information security (certificate ISO/IEC 27001:2013) and in the field of quality management (certificate ISO/IEC 9001). This states that the development practices are following the international security standards and uses the highest security measures available.

1.7. Audits

The certification body of TÜV Austria has confirmed with certificate (see latest and valid eIDAS certificate for creation EID-SK qualified electronic signature certificates from: <https://www.skidsolutions.eu/en/repository/audit/>) that SK ID Solutions AS, the developer of Smart-ID, trust service EID-SK qualified certificates for electronic signatures fulfil all the relevant requirements defined in regulation Reg. (EU) No. 910/2014 (eIDAS) for creation of qualified certificates for electronic signatures. Audit was based among other documents on Certificate Policy for Qualified Smart-ID. The audit is carried out every 24 months.

It is confirmed also with conformity assessment that a new identification method – universal automated biometric identity verification implemented by SK ID Solutions AS fulfills above listed requirements. The assessment concluded that controls performed by SK ID Solutions AS during Smart-ID automated biometric identity verification enrolment process are rated to be stronger controls regarding the identity verification of the person than the controls provided by a typical average human based face to face identify verification. The NPL, the official national UK research lab, specialized and recognized for evaluation of biometric methods, consider that the methodology for testing and reporting (error rates specified, etc.) biometric verification performance conforms to the relevant requirements of ISO/IEC 19795-1:2006, and that the methodologies for testing and reporting presentation attack detection sufficiently conform to ISO/IEC 30107-3:2017 to support the iProov performance claims. iProov is the SK's partner for providing facial recognition service.

In terms of registration authority, the requirements come from eIDAS and ETSI standards. Firstly, SK carries out an initial audit of the registration authority to make sure the institution in fact meets the aforementioned requirements. From there onwards, registration authority has to hire an independent IT auditor every 24 months. In addition, SK carries out checks of service every year based on a random sample of e-service providers.

According to audit carried out by KPMG in 2017 Smart-ID application is considered a solution for strong authentication. Smart-ID meets the Regulatory Technical Standards (RTS) requirements and is capable of guaranteeing the high security of the electronic authentication. SK's information systems, organisation, processes and work methods comply with PSD2, other

technical requirements and the online payment legislative requirements of Estonia, Latvia and Lithuania.

The Smart-ID QSCD evaluation was conducted based on standard „Common Criteria for Information Technology Security Evaluation”, version 3.1 revision 5. The evaluation of the Smart-ID backend system component (SecureZone) is done according to the document "[Smart-ID SecureZone Security Target](#)", the evaluation corresponds to Common Criteria EAL4 level, augmented with AVA_VAN.5. This means that during the evaluation it is assured that Smart-ID QSCD components are resistant to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the Smart-ID QSCD. Certificate 9263.18 is available at TÜVIT [website](#).

The evaluation of the Smart-ID App library component (Threshold Signature Engine) is done according to the document "Smart-ID App Threshold Signature Engine", version 10.3.3 the library component is evaluated according to Common Criteria EAL 2 level. Certificate 9264.19 is available at TÜVIT [website](#).

Smart-ID QSCD evaluation finished in October 2018. Certificate TUVIT.9801.QSCD.12.2018 is available at TÜVIT [website](#).

For informational purposes Smart-ID SecureZone, version 10.3.5 is also published in [Compilation of Member States notification on SSCDs and QSCDs](#) by European Commission.