March 2021

MitID

Arkitektur og funktionalitet

Mogens Rom Andersen

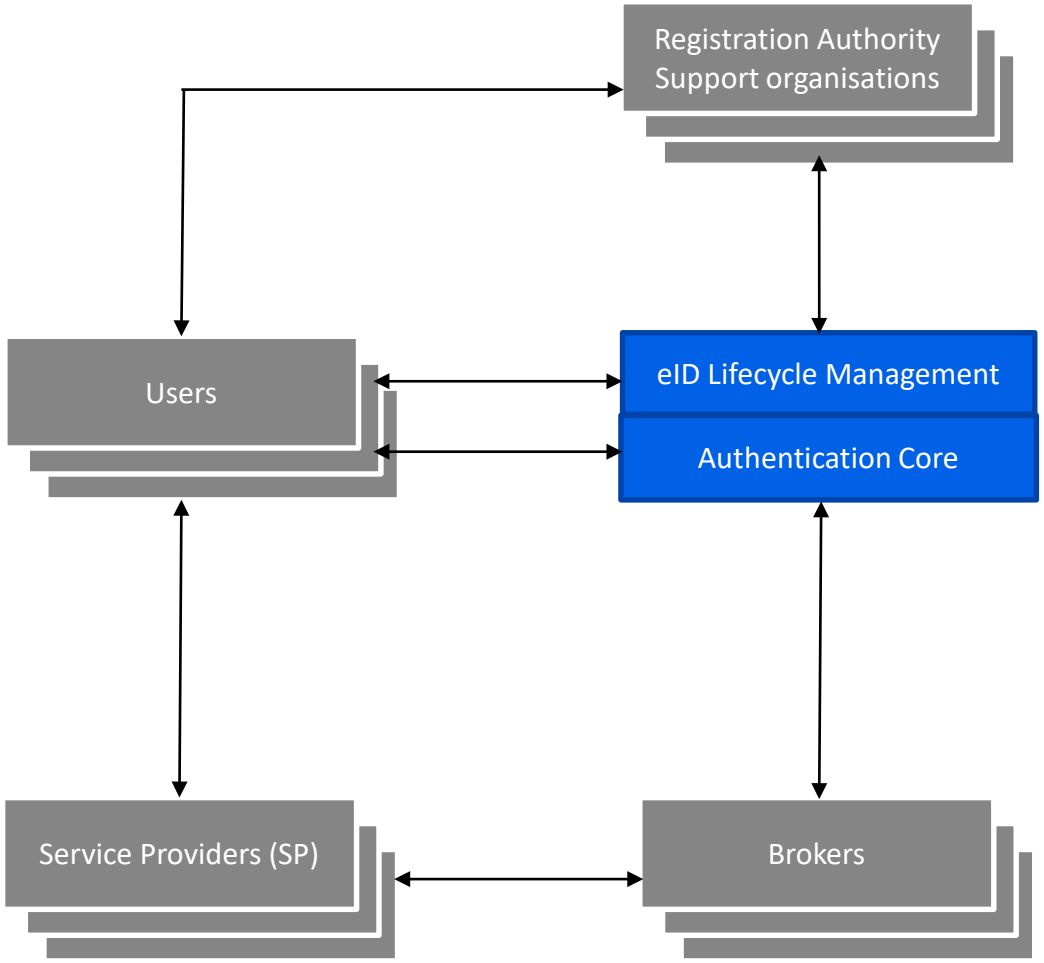
MitID – af partnerskabet mellem Digitaliseringsstyrelsen og de danske pengeinstitutter

Introduction

- 3’rd generation national eID
- Go-live in May 2021
- Migration start in Q3 2021
- Phased functionality approach until Q4 2021

- Mobile first but no exclusive approach
- Go-live, pilot users and establish Registration Authority (RA) and Support functionality
- Q3 functionality sufficient for normal usage
- Users can use both NemID and MitID in migration period
- Presentation describes the full functionality

MitID Ecosystem



eID Lifecycle Management

- Users register, enroll, manage identities and identification means online via self-service.

or

- Users register, enroll, manage identities and identification means via physical presence at registration authorities or request support via support organisations.

Authentication

- Users authenticate at Service Provider request using MitID identification means
- SP interacts with Brokers to perform MitID authentication
- Brokers manage the authentication request interacting with the authentication core
- The authentication itself is performed directly between user and authentication core

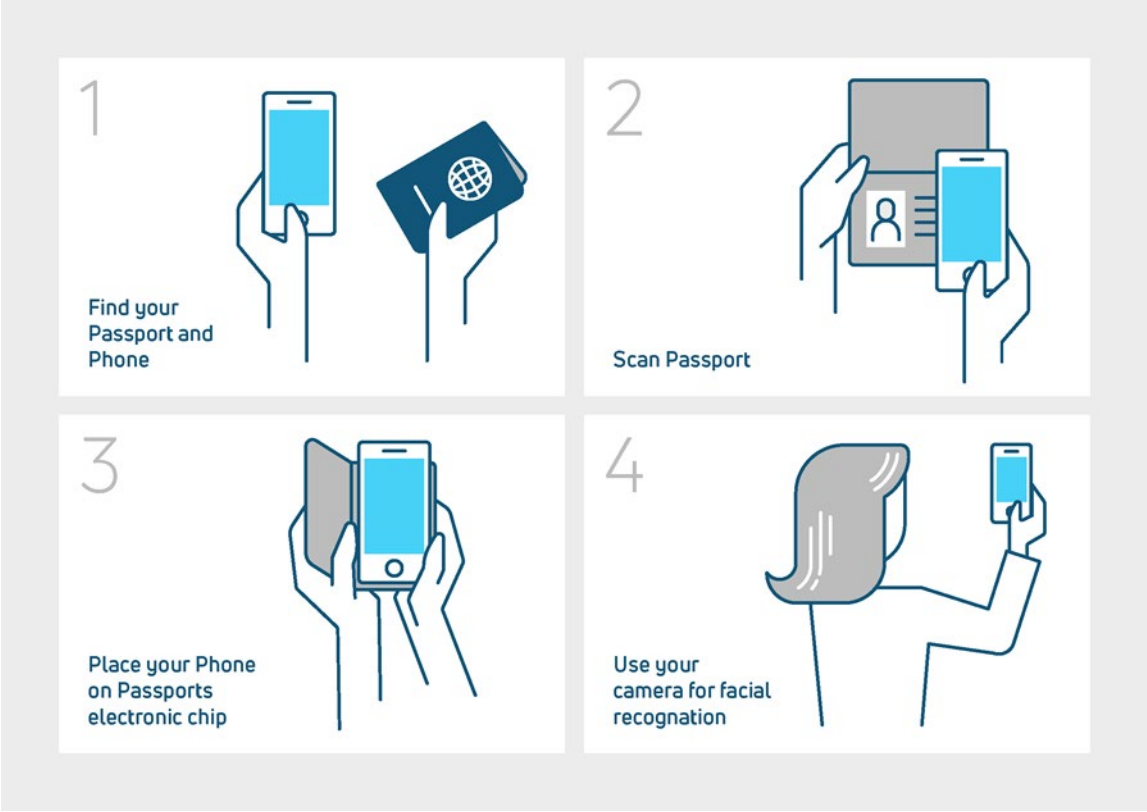
eID Lifecycle Management

- An Identification-app facilitates online user identification via data from passport chip
- Online eID lifecycle management provides options for self-service registration and enrolment on assurance level substantial and management of eID and identification means and retrieval of support tickets on assurance level substantial and high
- Registration, eID management is also available via physical presence at registration authorities
- Identification-app or a list of well defined legitimation documents can be used for identification during physical presence at registration authorities
- Support is available via phone provided the user can identify themselves to support organisations, e.g. using a support ticket.
- Physical presence is mandatory for registration on assurance level high

- Identification-app is Q4.21 functionality
- Users are encouraged to use Self-Service for identification to the widest possible extent

- Support organisations cannot perform registration
- Support organisations can offer alternative support channels, e.g. chat

Identification-app functionality



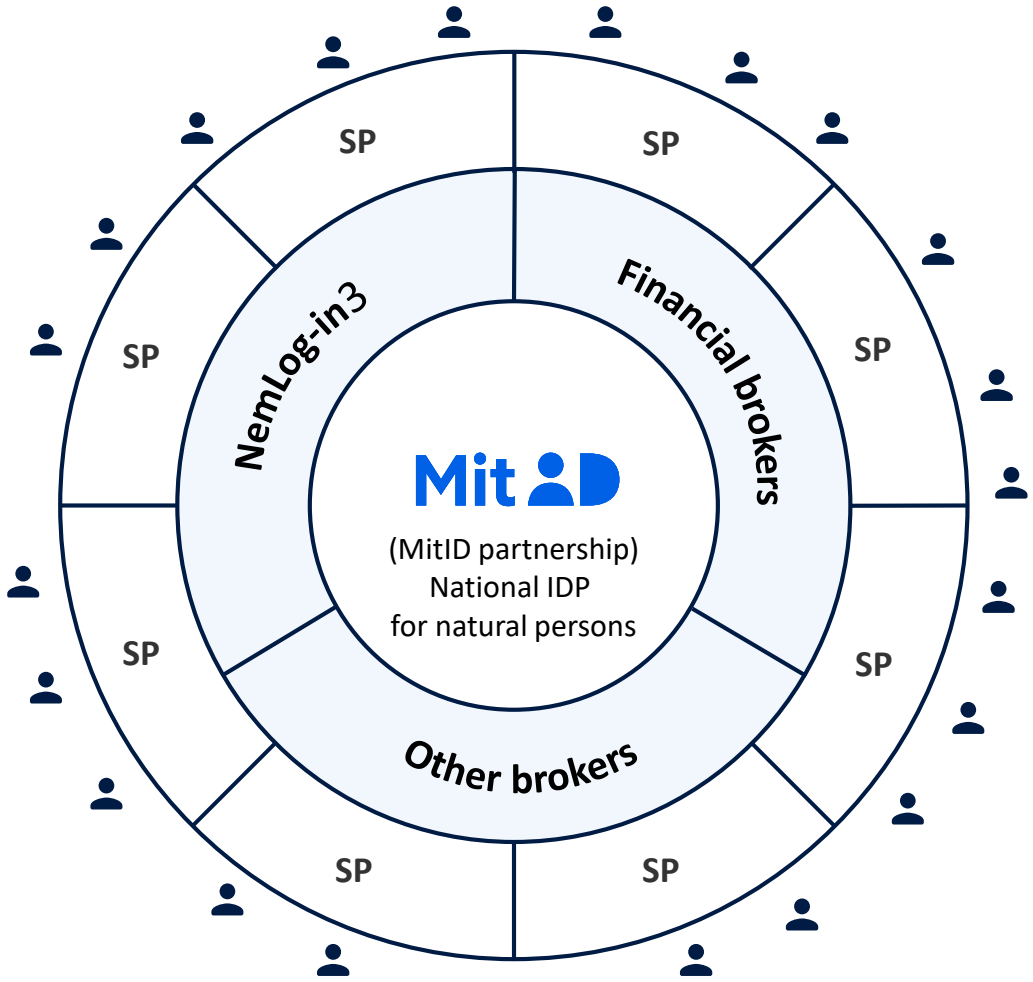
Scan passport in order to access chip content

Chip content is checked for autenticity and chip clone detection

Face recognition based on image from chip and liveness check on the physical person

Authentication

- Future-proof – flexible and modular
- Easier to develop
- One unified system



SP = Service Provider

- ”Authentication” is the proof that the user is in posession and control of the identification means associated with the user
- Users interact with Service Providers (= SP) using MitID eID
- SP gain access to MitID authentication through a broker of their choice.
- MitID is born with one broker for public SP (NemLog-in3), five brokers for financial SP and a number of brokers for private SP
- More brokers can be added during the lifetime of MitID

Brokers

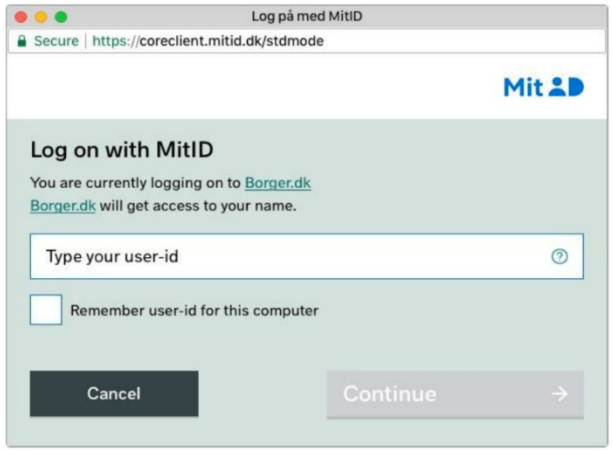
- Brokers play an important role in MitID; therefore the standards are set high:
  - All brokers must complete a basic certification - requirements and documentation of e.g. management systems for information security and various controls
  - The certified brokers must be further certified on security requirements and the UX scheme according to the three applicable usage models, chosen by the individual broker
  - Brokers add context to MitID eIDs and are expected to create sector specific solutions based on MitID eIDs, e.g. for insurance or education
  - Brokers create smooth SP connectivity to MitID as sector specific protocols can be used between SP and Broker
  - Brokers enforce part of the security model defined by MitID as the core functionality of the MitID IDP is shielded from SP

The Broker can choose between three usage models, providing various degrees of flexibility for brokers to create good and innovative solutions for the user and SP

The security requirements defines the set of security constraints that the Brokers must fulfill in order to become part of the MitID ecosystem

The UX scheme defines the set of graphical expressions that the Brokers must fulfill in order to become part of the MitID ecosystem

Identification means



- MitID facilitates a national eID and must embrace all citizens to the widest possible extent
- The expectation is that approx. 80-90% of the citizens can or will use App based authentication
- This implies a need for both App and hardware token based identification means

- At go-live a U2F (FIDO) token will be supported, conceptual named ”MitID Chip”

Assurance Levels and Identification means combinations

- MitID is based on NSIS with three Levels of Assurance (LoA) - Low, Substantial and High - for the combined strength of identification and authentication (IAL and AAL)
- The SP decides the required level of assurance for the user to access a digital self-service solution
- The valid combinations of identification means are predefined, but step-up is also supported
- MitID App comes in two flavors for assurance level substantial and high
- MitID App supports multiple users on assurance level substantial
- MitID App for assurance level substantial, without multiple users, can use device biometrics to release the knowledge element (App PIN code)
- MitID is PSD2 Strong Customer Authentication (SCA) compliant

Valid combinations

Assurance level High

- Password + MitID chip
- MitID App + MitID chip
- MitID App enhanced security

Assurance level Substantial

- MitID App
- Password + MitID code display
- Password + MitID code reader
- Password + MitID chip

Assurance level Low

- Password
- MitID chip
- MitID code display