AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Next Generation of National Digital Identity and Signing

Information meeting for potential contractors

June 27th 2016

AGENDA

1. **Visions for Next Generation of National Digital Infrastructure**

   By Head of Division Charlotte Jacoby

2. **Next Generation of National Digital Identity and Signing - Current infrastructure and future citizens' solution**

   By Solution Architect Anders Højbjerg

3. **Next Generation of National Digital Identity and Signing - for Businesses**

   By Solution Architect Rasmus Frederiksen

4. **Next Generation of NemLog-in – The Public Sector Log-in Solution**

   By Solution Architect Rasmus Frederiksen

5. **Next step – The Upcoming Procurement Procedure**

   By Senior Project Manager Per Faarup

6. **Questions**

Networking

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Visions for Next Generation of National Digital Infrastructure

DANISH PUBLIC SECTOR – DIGITAL FORERUNNER

- **Strong tradition of joint public sector digitisation**
- **Multi-year joint government eGovernment strategies since 2001, include central, regional, and local government**
  - Digital self-service made mandatory 2012-2015
  - Mandatory use of digital letter box
    - November 2013 for businesses
    - November 2014 for citizens

- **Digital strategy 2016-2020: A Stronger and More Secure Digital Denmark**
  - Strong focus on data and digital infrastructure
- **High degree of internet penetration, usage and skills in population**
  - 87 pct. aged 16-74 use internet every day
  - 88 pct. aged 16-74 have interacted online with public authorities within past 12 months

(source: European Commission. Digital Scoreboard, 2015)

DIGITAL INFRASTRUCTURE TODAY

NemID – for citizens (national eID since July 2010)

- 4.5 million citizens have a NemID (92 pct. of citizens aged 15+)
- High degree of satisfaction (85 pct.) and trust (81 pct.)
- NemID used as secure eID and eSignature in both public and private sector (e.g. banking and private service providers, Digital Post, recording of a deed)

NemID – for businesses (since November 2011)

- 1.1 million NemID employee-ID used by employees in public sector (e.g. accessing data within the public health service) and private sector (e.g. when interacting with the public sector)

NemLog-in

NEM LOG-IN

- Single sign-on to public sector solutions, digital self-service, Digital Post, etc.

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

THREE TENDERS COMING UP…

Next generation National Digital Identity and Signing (NDIS) must be user-friendly and adaptive to new technologies – and used across sectors as today

NDIS – the citizens´ solution

- Multiple levels of security
- Multiple log-in factors (e.g. biometrics)
- Modularity – separation of eID and eSignature

NDIS – the business solution

- More flexibility focused on different groups of users
- Better administrative solutions for businesses (managing identities and access rigths)

Next generation single sign-on (NemLog-in)

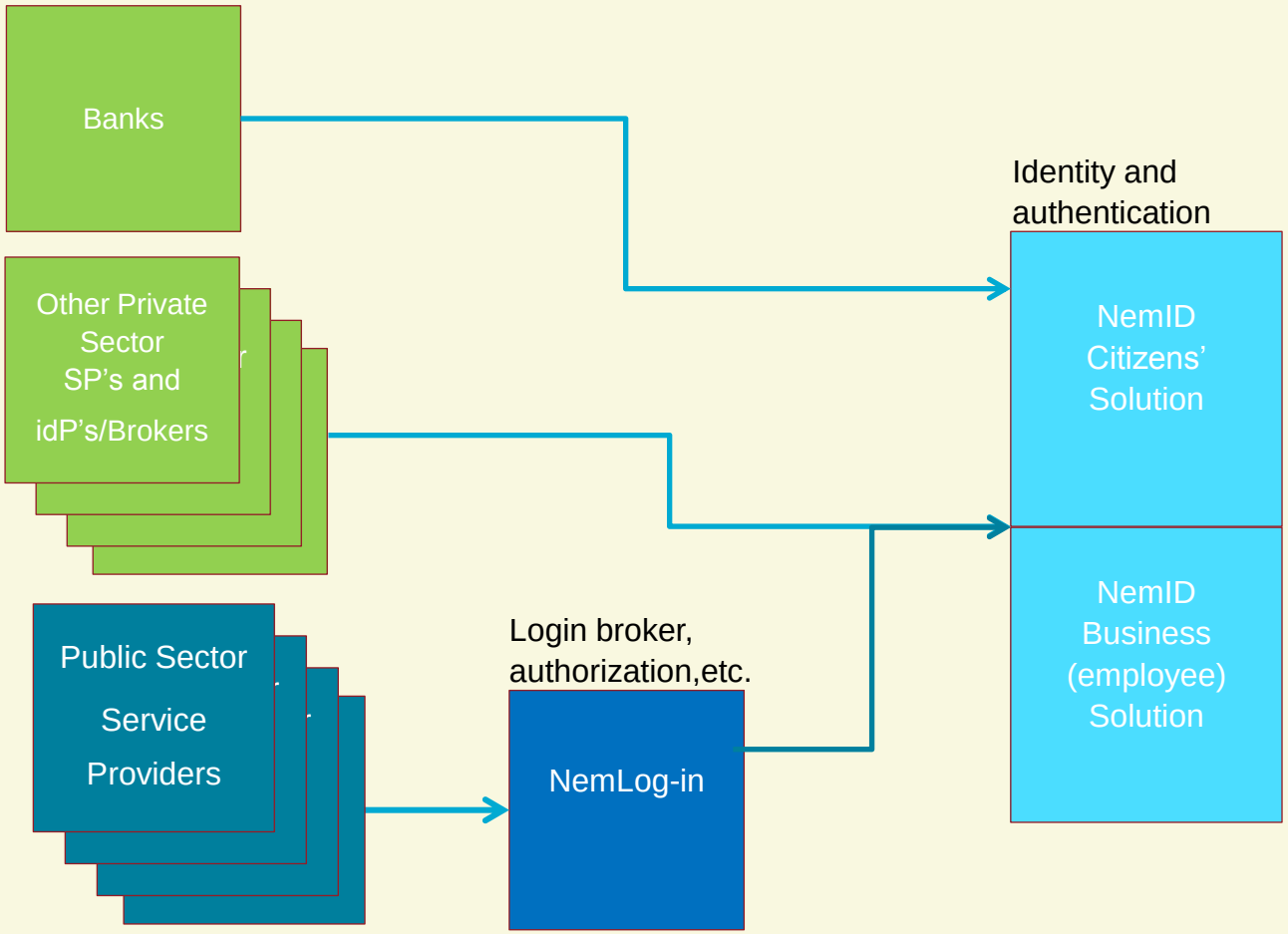
- More granular options for user administration for public authorities, private companies and citizens
- The creation of seamless user travels across domains

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Next Generation of National Digital Identity and Signing

Current infrastructure and future citizens' solution

”IT LANDSCAPE” DESCRIPTION
PUBLIC SECTOR CORE SECURITY COMPONENTS



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

NEMID
– CURRENT VERSION CHARACTERISTICS

- **NemID (”Easy ID”):**
  - Two parts: Citizens solution and business (employee) solution
  - Identity Lifecycle Handling (citizens and business users)
  - Credentials: Username-password + “Cardboard OTP cards”
  - Authentication based on “PKI-bourne”, centrally stored keys (”OCES”)
  - Advanced Electronic Signature
  - Current solution IPR owned by the supplier (Nets DanID)
  - Used by: Public Sector, all Danish banks, private sector service providers

NATIONAL DIGITAL IDENTITY AND SIGNING SOLUTION – NDIS – GENERAL INFO

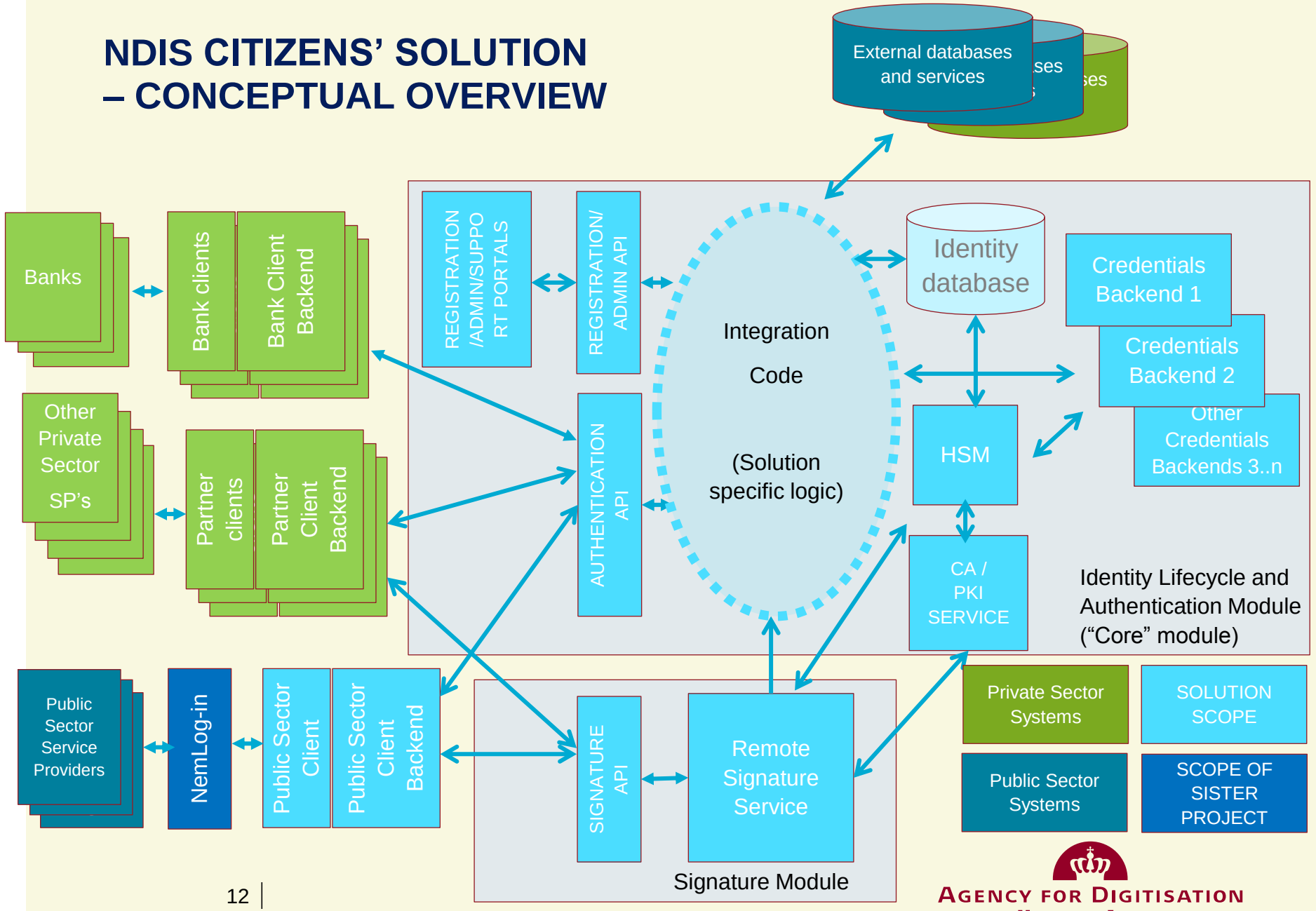
- **Same overall focus as NemID: Identity handling and authentication**

- **Split in two separate projects:**
  - Citizens' solution
  - Business (employee) solution
- **Parts of the Citizens' solution potentially to be procured in cooperation with the Danish Bankers Association**
- **Current "walk-through" is to be considered as a conceptual snapshot of the ongoing analysis/specification process**
  - This process will continue during the coming period and can lead to changes to what is being presented in this document.
  - We still need input from the market

FUTURE CITIZENS' SOLUTION

- **Modular architecture, extendable and with high level of flexibility**
  - Separated functionality modules, e.g. signature and authentication
- **No centrally stored "PKI-bourne" keys**
- **Project partners allowed to build their own client solutions**
- **Higher degree of ownership to the solution IPR**
- **Usage-based billing for Service Providers**

NDIS CITIZENS' SOLUTION – CONCEPTUAL OVERVIEW



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

CONCEPT FOR CITIZENS SOLUTION ”CORE” (IDENTITY LIFECYCLE HANDLING AND AUTHENTICATION)

- **Standard API to be called by multiple clients (API open to partners)**
  - Generic, agnostic to different credentials solutions
- **Based on standard credentials platforms to the degree possible**
  - Plug’n’play process for adding new credentials to the solution?
- **HSM protection of core identity and credentials data**
- **To be mapped to eIDAS Level of Assurance (LoA) substantial or high**
- **Support for 1-factor authentication for services handling non-sensitive data.**

CREDENTIALS BACKENDS

- **Support for multiple separate credential types preferred**
- **Needs to support end users with disabilities, e.g. blind and visually impaired people**
- **Focus on standardized credentials solutions**
  - OATH?
  - FIDO UAF/U2F?
  - Others?
- **Desire to include mobile phone based (non-physical) credentials in solution**
  - Possible to base it on Secure element / TEE technology?

INTEGRATION

"The code that glues standard components together to a full solution"

- **Transform user data and credentials data to "generic" API format**
- **Integrate with national Danish citizen registry and passport databases**
- **Integrate with external services used by the solution (print, SMS, etc.)**
- **Audit logging**
- **Data collection for billing and statistics purposes**
- **Business logic for different kinds of authentication**
- **Business logic for end user registration processes**
- **Business logic related to Service Provider registration & lifecycle handling**
- **Integration with Hardware Secure Module (HSM)**
- **Etc…**

CLIENTS AND CLIENT BACKENDS

- **End user authentication/signature clients will communicate with “Core”, Signature and other modules via standardised API’s**
- **Integrating both authentication and signature functionality**
- **Supposed to work in close cooperation with the NemLog-in platform**
- **Should support both web and (multiple) mobile platforms**

SIGNATURE MODULE

- **Expected to be based on upcoming CEN standard EN-419241**
- **Signatures to be issued based on user authentication from "Core" module**
- **Support for advanced electronic signature and possibly qualified signature.**
- **Expected to be based on short-lived (single usage) certificates**

CERTIFICATE AUTHORITY

- **PKI certificates for**
  - Signature needs (qualified/non-qualified, short term certificates)
  - System-to-system communication (SP's, public infrastructure, etc.)
- **Support for standard enrollment protocols (SCEP?, EST?)**

Questions?

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Next Generation of National Digital Identity and Signing – for Businesses

CURRENT: THE MOCES PLATFORM

Current MOCES infrastructure:

- PKI-based with private keys stored centrally
- Authentication and signing are inter-connected

Different end user solutions:

- CSS/LSS – Central Signature Server/Local Signature Server
- Downloadable Software Keys
- OTP Cards
- Hardware Token

FUTURE: THE MOCES PLATFORM

Future MOCES infrastructure:

- PKI-based without central storage of private keys
- Document signing is done via the signing module in the citizen solution
- CA API facilitates local solutions with custom credentials and processes for specialized use-cases
- Optionally used alongside the citizen credentials, one business identity – many ways to access

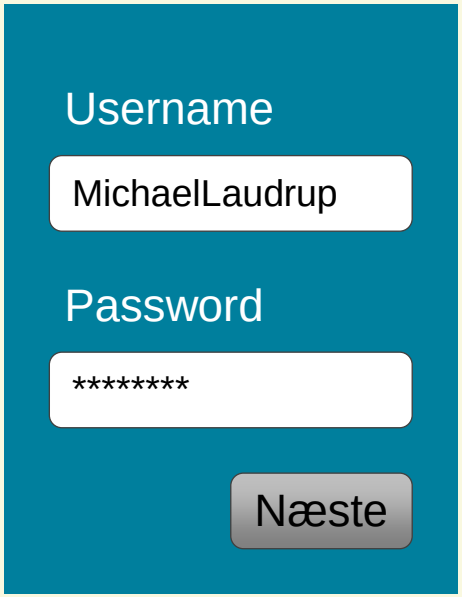
End user Solutions

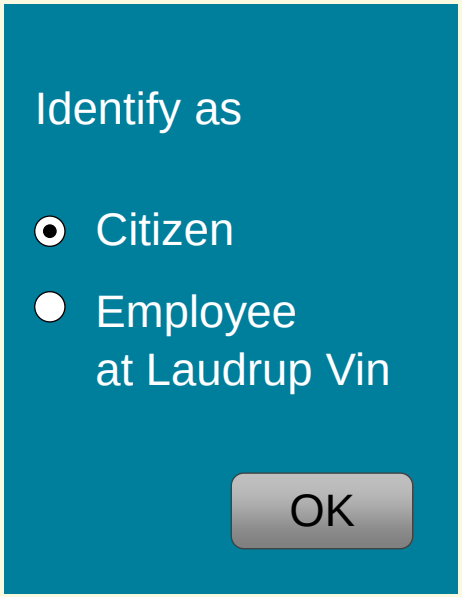
- CSS/LSS – Central Signature Server/Local Signature Server
- Downloadable Software Keys
- QSCDs (hardware tokens)

ADDITIONAL SIMPLE BUSINESS SOLUTION BASED ON THE CITIZEN IDENTITY

To most business users,
the difference between the two solutions will be invisible

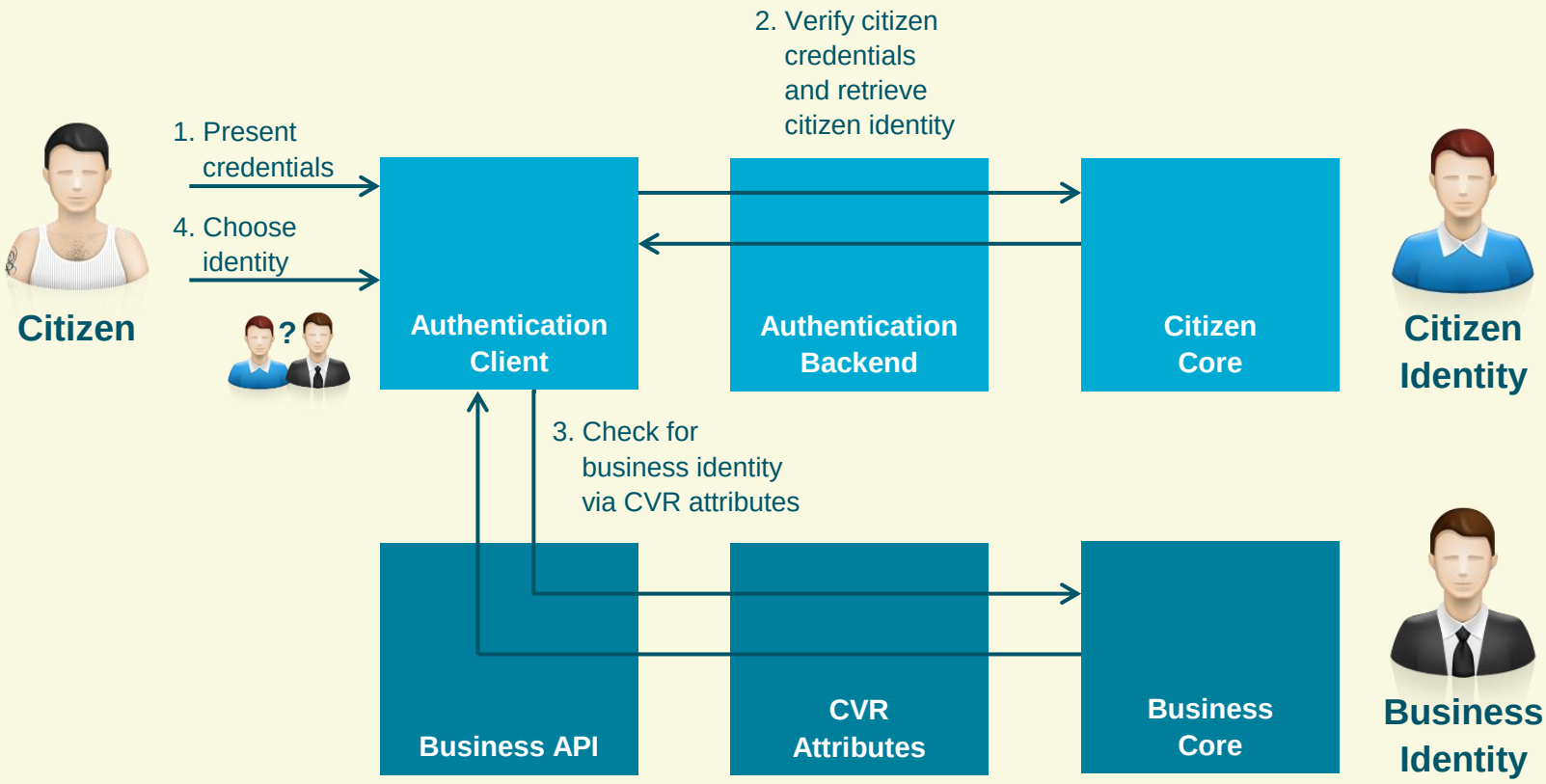
- Re-uses the credentials from the citizen identity
- Same interaction, same credentials
- Select whether to act as citizen or business identity after authentication





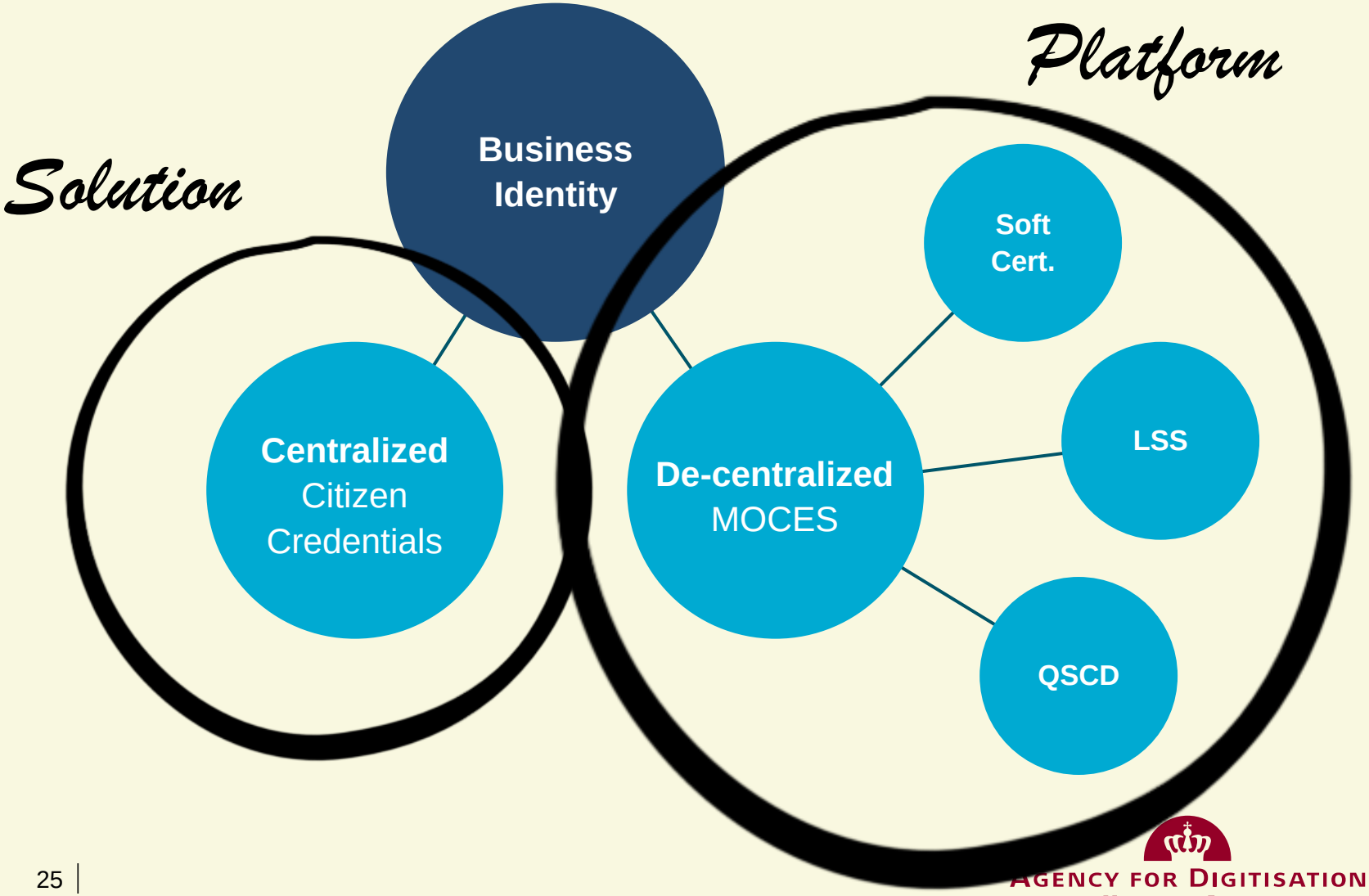
AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

SIMPLE BUSINESS SOLUTION DATA FLOW



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

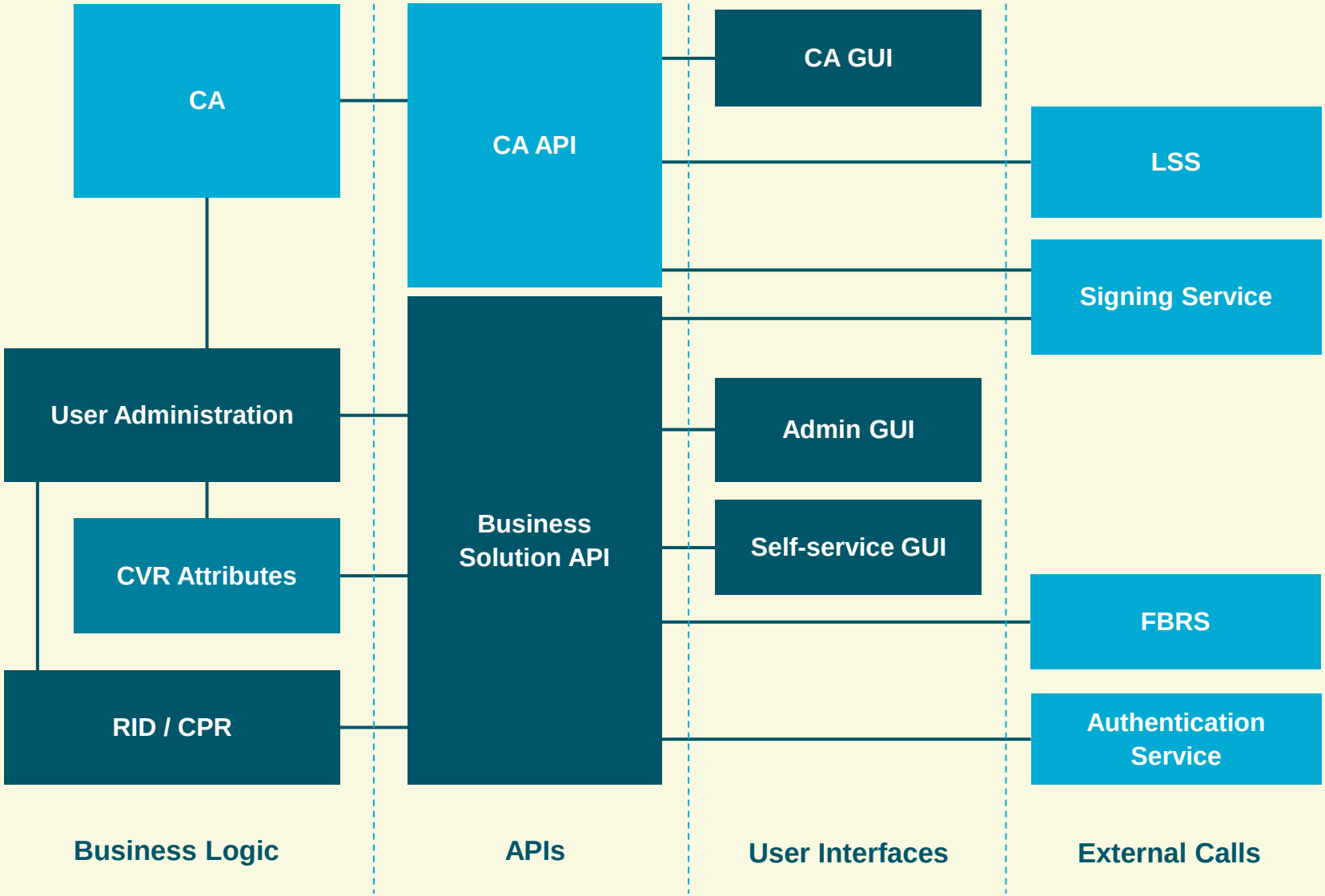
A FLEXIBLE BUSINESS SOLUTION



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

ADVANTAGES OF THE SIMPLE BUSINESS SOLUTION

- **The users of the business solution will benefit from additions made to the citizen solution, including new types of credentials and processes as they develop over the coming years**
- **Any valid citizen authentication can be used as a valid business authentication (LoA permitting)**
- **Low administration overhead for small to medium-sized businesses**
- **Low friction process when hiring/firing – no waiting for new credentials. CVR attribution can be set up quickly via mutual agreement and removed unilaterally by both parties**



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

INTEGRATION SERVICE

Registration and administration

- National CPR register
- National CVR register
- Integration to local administrative solutions

Issuance and renewal

- CA services in the citizen solution

Usage

- CVR attribute service
- NemLog-in
- Authentication services
- Signing services

Questions?

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Next Generation of NemLog-in

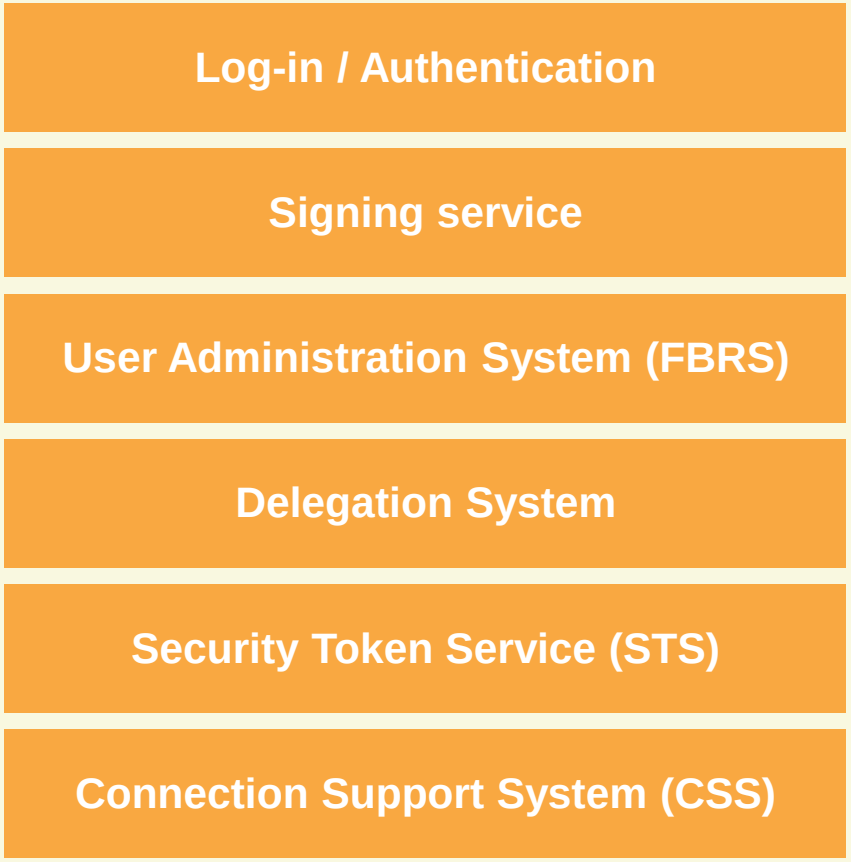
The Public Sector Log-in Solution

NEMLOG-IN AS IS

The Danish national platform for login and user administration

Primary functions:

- Reduced costs for public service providers
- Same security model across domains (same integration to NemID)



AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

THE LOG-IN AND SSO COMPONENT

- **Used by public authorities and portals (borger.dk, virk.dk) to authenticate users**
- **Functions: Sign-in, Single Sign-On, Single Logout, AttributeQuery**
- **The foundation is the OIOSAML profile**
- **SSO is the foundation for the portals Borger.dk, Virk.dk and Sundhed.dk**
- **Detaches eID / log-in mechanisms from the service provider**

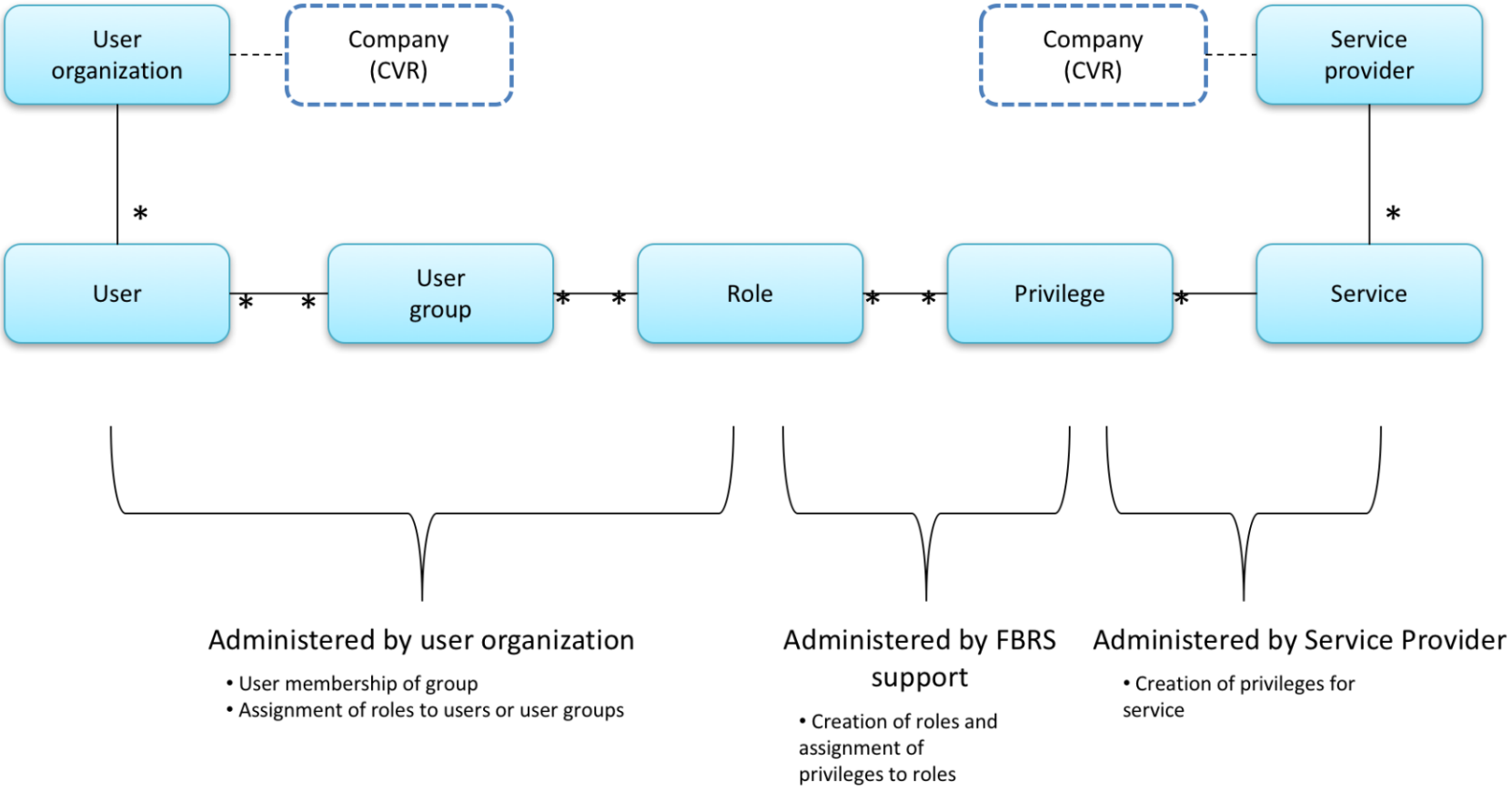
SIGNING SERVICE

- **Supports signing documents in online services**
- **Supports the legal integrity of electronic signatures through logging, system evidence and signature validity evidence**
- **Supports validation of signatures inside third party applications**
- **Secure validation and storing of signatures**

USER ADMINISTRATION

- **Central administration of business identity authorisation in self-service solutions**
- **Single destination for companies and public authorities to manage authorisations across the public sector**
- **Service providers do not have to build and maintain their own authorisation management solutions**
- **Delegation of rights**
- **More than 250.000 user organisations in FBRS**

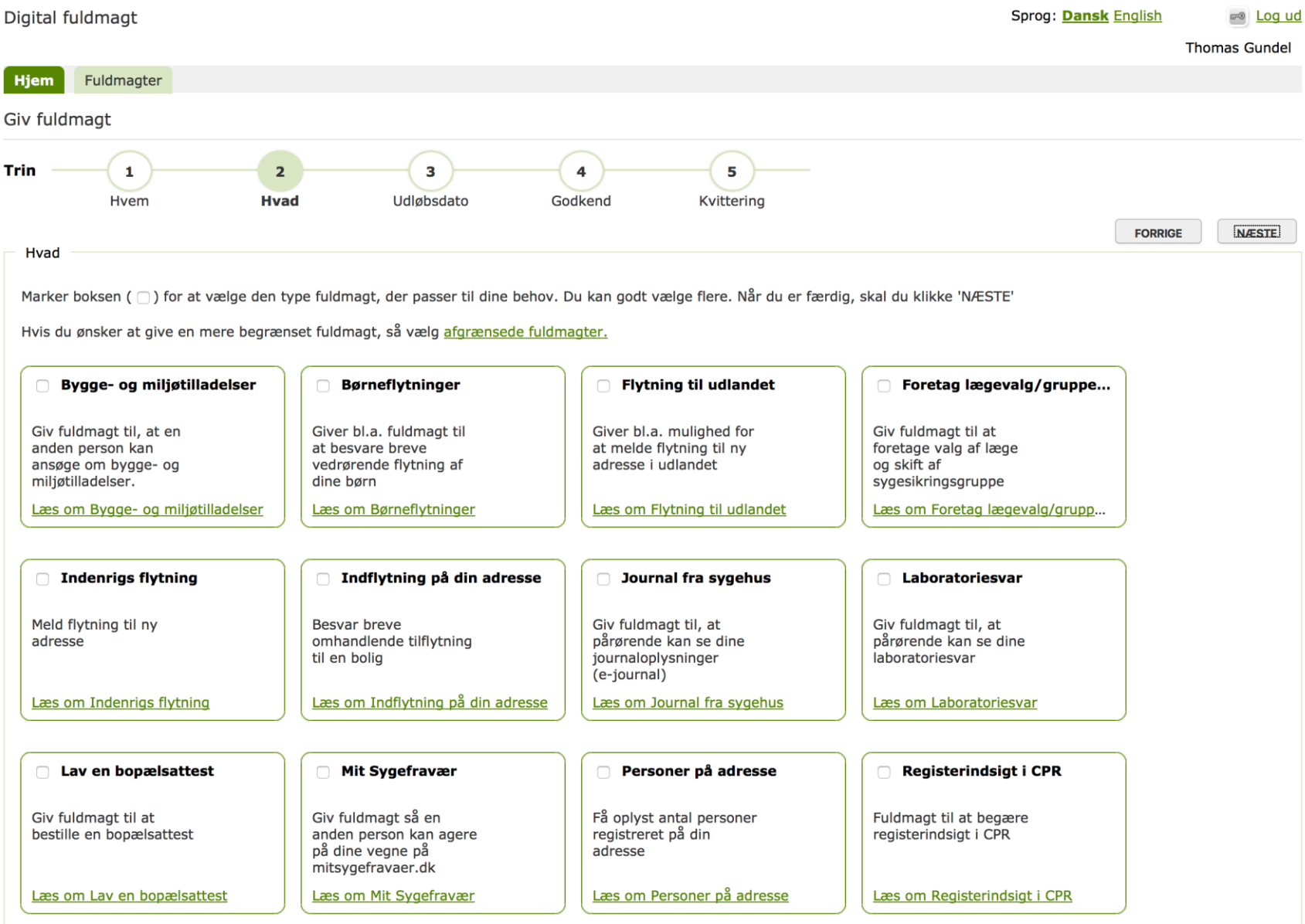
AUTHORISATION MODEL



DELEGATION SYSTEM (FOR CITIZENS)

- **Citizens can delegate rights to other party's who can act on their behalf in public self-service solutions**
- **Rights can be given to another citizen, a company or an employee of a company**
- **Citizens have a dashboard of given rights across self-service solutions**

EXAMPLE


Digital fuldmagt
Sprog: Dansk English
Log ud
Thomas Gundel
Hjem
Fuldmagter
Giv fuldmagt
Trin
1 Hvem
2 Hvad
3 Udløbsdato
4 Godkend
5 Kvittering
FORRIGE
NÆSTE
Hvad
Marker boksen ( ) for at vælge den type fuldmagt, der passer til dine behov. Du kan godt vælge flere. Når du er færdig, skal du klikke 'NÆSTE'
Hvis du ønsker at give en mere begrænset fuldmagt, så vælg afgrænsede fuldmagter.
Bygge- og miljøtilladelser
Giv fuldmagt til, at en anden person kan ansøge om bygge- og miljøtilladelser.
Læs om Bygge- og miljøtilladelser
Børneflytninger
Giver bl.a. fuldmagt til at besvare breve vedrørende flytning af dine børn
Læs om Børneflytninger
Flytning til udlandet
Giver bl.a. mulighed for at melde flytning til ny adresse i udlandet
Læs om Flytning til udlandet
Foretag lægevalg/gruppe...
Giv fuldmagt til at foretage valg af læge og skift af sygesikringsgruppe
Læs om Foretag lægevalg/grupp...
Indenrigs flytning
Meld flytning til ny adresse
Læs om Indenrigs flytning
Indflytning på din adresse
Besvar breve omhandlende tilflytning til en bolig
Læs om Indflytning på din adresse
Journal fra sygehus
Giv fuldmagt til, at pårørende kan se dine journaloplysninger (e-journal)
Læs om Journal fra sygehus
Laboratoriesvar
Giv fuldmagt til, at pårørende kan se dine laboratoriesvar
Læs om Laboratoriesvar
Lav en bopælsattest
Giv fuldmagt til at bestille en bopælsattest
Læs om Lav en bopælsattest
Mit Sygefravær
Giv fuldmagt så en anden person kan agere på dine vegne på mitsygefravaer.dk
Læs om Mit Sygefravær
Personer på adresse
Få oplyst antal personer registreret på din adresse
Læs om Personer på adresse
Registerindsigt i CPR
Fuldmagt til at begære registerindsigt i CPR
Læs om Registerindsigt i CPR

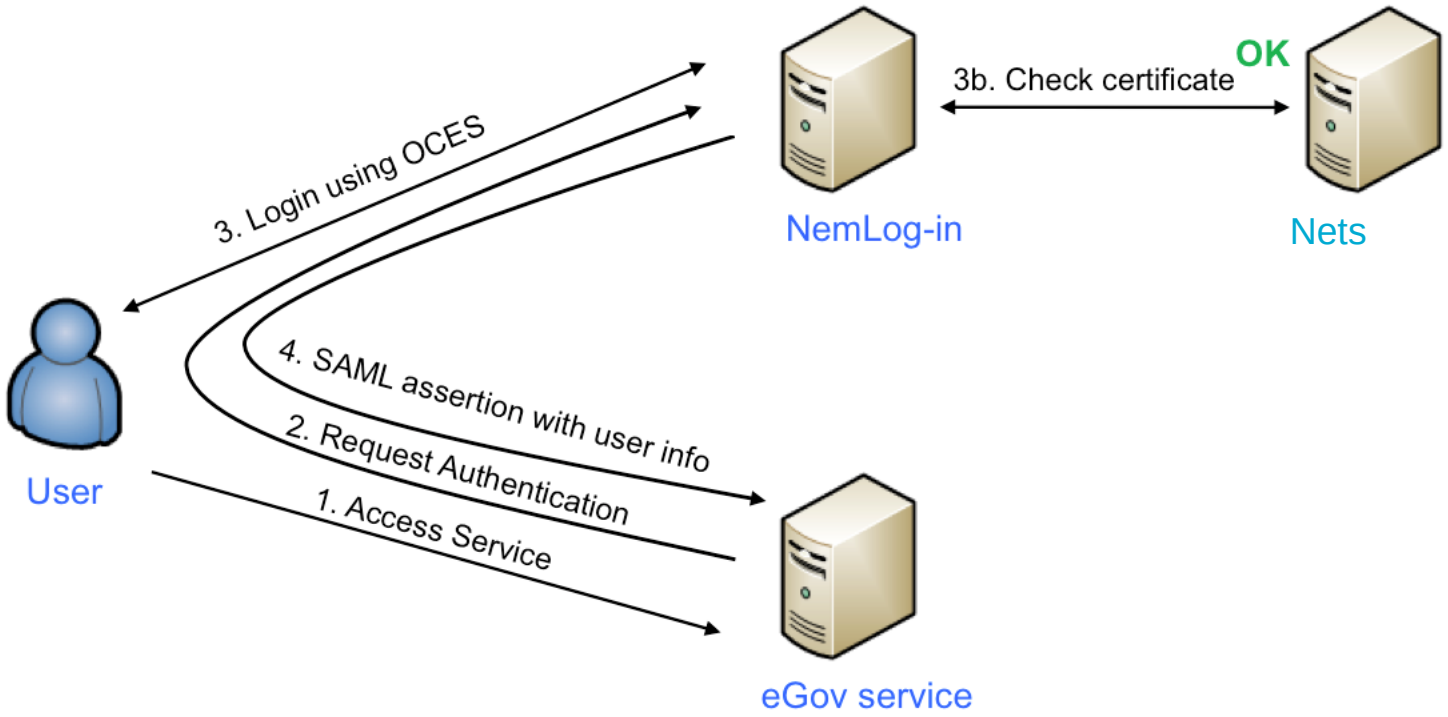
SECURITY TOKEN SERVICE

- **Provides access to web services based on a SAML token**
- **Based on the OIO WebService Trust profile**
- **Two main forms:**
  - Identity based web services
  - “Systembrugermodellen” – an identity framework used in the municipalities
- **Security Token Services is commonly used within the health sector and in the municipalities**

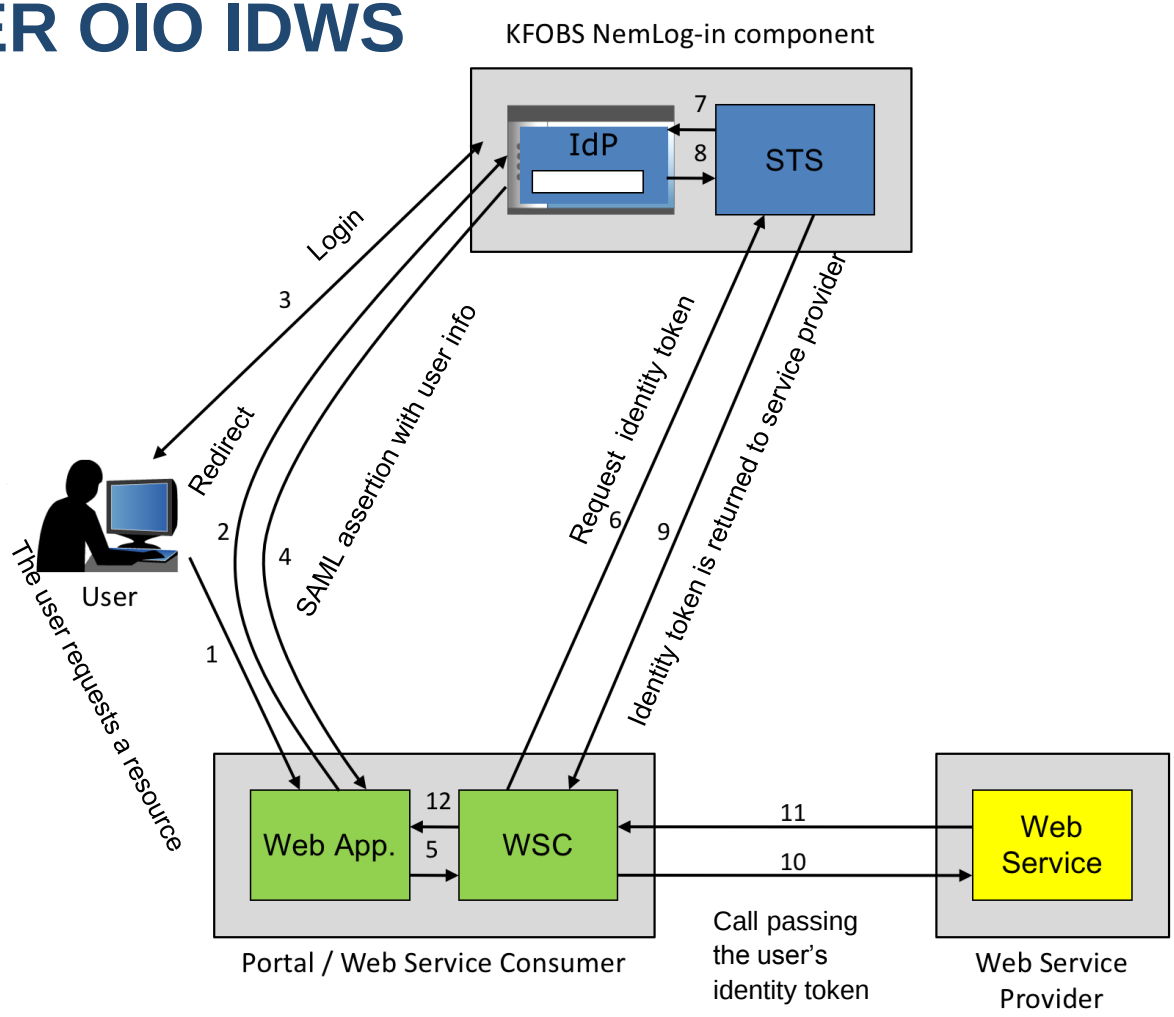
CONNECTION SUPPORT SYSTEM (CSS)

- **The administration of federation through self-service**
- **Public authorities (1151) connect their solutions and point out their it-vendor**
- **It-vendors (937) connect to the solution (850) and maintain technical information like certificates and metadata**
- **Companies connect as user organisations (>250.000)**

CURRENT ARCHITECTURE
FLOW: SAML LOG-IN
USER OIOSAML



CURRENT ARCHITECTURE FLOW: SECURITY TOKEN SERVICE USER OIO IDWS



NEXT GENERATION NEMLOG-IN: PRIMARY NEW BUSINESS NEEDS

- **Increased usability**
- **More granular user rights in FBRS**
  Detailed targeting of rights against various business types
- **Further use and granulated using a delegation** - e.g. read-only access to specific cases, but not necessarily to all types of cases
- **Federation between local user right domains.** Options for exchanging information between different domains as well as options to use local ADs or other IdM systems
- **Creating seamless user travels across domains**
  Looking into widening the scope for private service providers
- **Integration to the NDIS and eID gateway**
  Development of new integrations
- **Technological update and looking ahead**
  e.g. updating OIOSAML and better mobile support

Questions?

AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Next step: The Upcoming Procurement Procedure

PROCUREMENT PROCEDURE NEXT GEN NEMID CITIZEN, NEMID BUSINESS AND NEMLOG-IN

- **TED announcement for technical dialogue for NemID Citizen and NemID Business is excepted to be published in the beginning of July 2016**
- **Technical dialogue is expected to take place in the fall of 2016**
- **Assessment of risk profile by the Danish Council for IT Projects fall / winter 2016**
- **Announcement of tenders is expected to be published in spring / late spring 2017**
- **The procurement procedure is expected to contain**
  - Prequalification and appointment of prequalified bidders
  - Tenders and dialogue concerning the tenders
  - Tender evaluation and appointment

TECHNICAL DIALOGUE AUTUMN 2016

- **The purpose of the technical dialogue is to give the Danish Agency for Digitisation relevant knowledge to prepare the tender documents**
- **The technical dialogue will consist of individual dialogue meetings between the Danish Agency for Digitisation and a number of the IT vendors that submit a request to participate**
  - The guidelines for participation in the technical dialogue will be apparent from the TED-announcement of the technical dialogue
- **Some of the key issues for the dialogue will be:**
  - IT architecture, modularity and integration
  - IT operations
  - Contract principal deliveries
  - IT security and privacy
  - Accessability

FURTHER INFORMATION

Further information concerning procurement, IT solution development and migration, will be published regularly at

- http://www.digst.dk/
- http://www.digst.dk/Servicemenu/English

Subscribe to our newsletters (Danish and English) and get information about upcoming tenders etc.

- http://www.digst.dk/

Questions regarding the procurement procedure can be submitted to:

- ndis@digst.dk

Questions?