Forum för leverantörer av betrodda tjänster och e-legitimationer

Tisdagen den 7 maj 2024

PTS

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Agenda

9.05-9.15	Aktuellt från Digg och PTS Sarah Amandusson, Digg Isabelle Westerlund, PTS
9.15-9.45	Aktuellt på EU-nivå Åsa Barton, EU-kommissionen
9.45-10.15	Aktuella frågor nationellt Ylva Wide, Regeringskansliet
10.15-10.45	**PAUS**
10.45-11.15	Ackreditering och certifiering - en allmän orientering Magnus Pedersen, Swedac Mats Engqvist, FMV
11.15-11.45	Auktorisationssystem Roger Fagerud, Digg
11.45-13.00	**Lunch på egen hand**
13.00-13.30	Nyheter eID och plånboken Anneli Hagdahl och Roger Fagerud, Digg
13.30-14.00	Large Scale Pilot Sarah Amandusson, Digg
14.00-14.30	Nya betrodda tjänster eIDAS2 Björn Scharin och Anna Amundberg, PTS
14.30-15.00	**PAUS**
15.00-15.30	Hur påverkas leverantörer av NIS2? Emma Wirf och Catherine Persson, PTS
15.30-16.00	Öppen frågestund & Avslut Emelie Björkengren Näslund, PTS

Aktuellt på PTS

Isabelle Westerlund

Enheten för digitala och betrodda tjänster

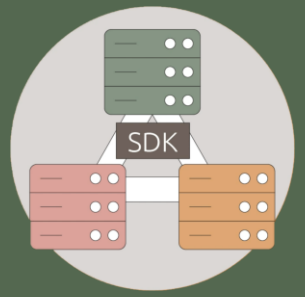
- Vi arbetar med betrodda tjänster genom att bedriva tillsyn och hantera rapporterade incidenter. Vi samverkar också med andra tillsynsmyndigheter inom EU kring tolkning och tillämpning av förordningen.
- Enheten är också ansvarig för tillsyn enligt NIS-lagen. Den 1 januari 2025 väntas en ny cybersäkerhetslag träda i kraft och även betrodda tjänster kommer att omfattas.

Aktuellt på PTS

- Analys och förberedelse inför eIDAS2 och ett utökat uppdrag
- Analys och förberedelse inför den nya Cybersäkerhetslagen (NIS2)
- Kommunikationsinsatser
- Deltagande i internationella arbetsgrupper

Aktuellt på Digg

Lotta Hämäläinen

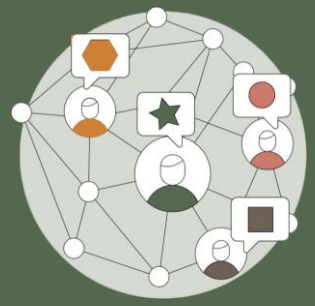


Ta över och förvalta säker digital kommunikation (SDK)

Införa auktorisationssystem

Utveckla och förvalta tekniskt system för bevisutbyte (SDG)

Utveckla och införa statlig e-legitimation



Utveckla identitets- och behörighetshantering för offentlig sektor

Delta i large scale pilot om digital plånbok

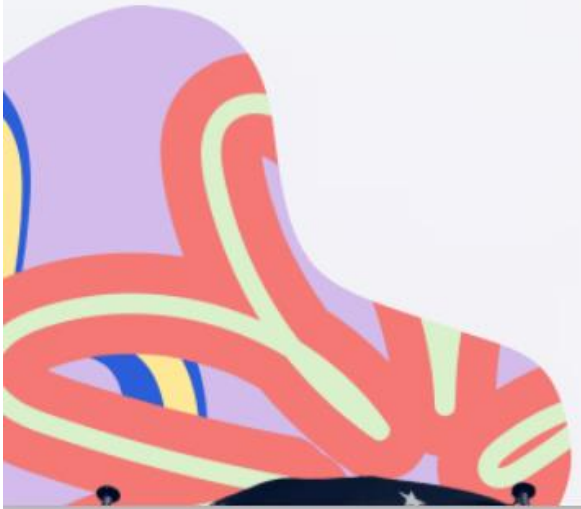
E-legdagarna

16-17 oktober 2024

European Commission

EU Digital Identity Wallet

The EU Digital Identity Wallet



Åsa Barton

7 May 2024

Imagine life in Europe in 2030

A secure, simplified, reliable and fast digital society

- Digital access knows **no age limits**
- Collaborating and converging **innovative infrastructure**
- **Lightning-speed** internet, anywhere you go
- **Safe and secure** digital world
- Seamless **EU-wide access** to digital public services

Introducing you to

EU Digital Identity Wallet

The personal digital wallet for EU citizens, residents & businesses, the EU Digital Identity Wallet.

Your Data, Your Story.

What is EU Digital Identity Wallet?

Identification is how we prove who we are; think of your passport or driver's license. With more and more private and public services becoming digital; a **safe, reliable, and privacy enhancing** means of digital identification is needed for **everyone in Europe.**

The EU Digital Identity Wallet

- is the **European Commission's response** to the challenges of digital identification.
- will allow you to **securely identify yourself** online when accessing a wide range of public and private services,
- will let you **store, present and share electronic attestations** (which include everything from university diplomas to train tickets).
- will let you **sign digital documents** swiftly and easily
- will be made available in **every EU Member State for all citizens, residents and businesses.**

The Benefits

How will citizens, governments and relying parties benefit from the wallet? Securely store and share your digital identity — discover the many ways EU Digital Identity Wallet will benefit both individuals and organizations.

Citizens

Protect personal data
Simplify paperwork and admin
Access public and private services across borders

Governments

Improve access to digital services
Enhance fraud prevention improves security

Relying Parties

Improve security and privacy
Reduce cost of authentication
Avoid relying on competing big platforms

Society

Increased online transactions
Resource reallocation
New business opportunities
Economic growth

The EU Digital Identity Wallet certification

Legal requirements (Article 5c)

Mandatory certification of the EU Digital Identity Wallet by accredited conformity assessment bodies

Certification against **level of assurance "high"** requirements as defined in the Regulation

Certification covers both **cybersecurity and non-cybersecurity** (functional, operational, interoperability) requirements

Certification is **valid for up to 5 years**, with a **2 years vulnerability assessment**

Optional certification against Regulation (EU) 2016/679.

Cybersecurity certification

The EU Digital Identity Wallet certification scheme shall **reference available and relevant CSA certification schemes** in order to ensure **harmonization**

For now, only the **EUCC scheme** is available covering ICT products

Transitory national certification schemes

For non-cybersecurity requirements and when cybersecurity certification schemes do not, or only partially, cover cybersecurity requirements, **Member States shall establish national certification schemes following the requirements set out in the revised Regulation implementing acts**

Member States shall **transmit their draft national certification schemes** to the European Digital Identity Cooperation Group which may issue opinions and recommendations.

EU Digital Identity Wallet Milestones

Legislative Process
Adoption - Ongoing work on Implementing Acts (IAs)

Publication of the Regulation in the Official Journal on April 30 and entry into force on 20 May 2024

Wallet technical specification
Published ARF 1.3, pending ARF 1.4

Published the Architecture Reference Framework (ARF) 1.3, on **GitHub** for public feedback - to be followed by version 1.4. in May

Wallet Prototype (Template)
Released first libraries and software components

Published first release of libraries and software components on GitHub, to be followed by regular releases based on feedback from pilots and updates to the ARF

Large-Scale Pilots
Approaching 1-year milestones and deliverables

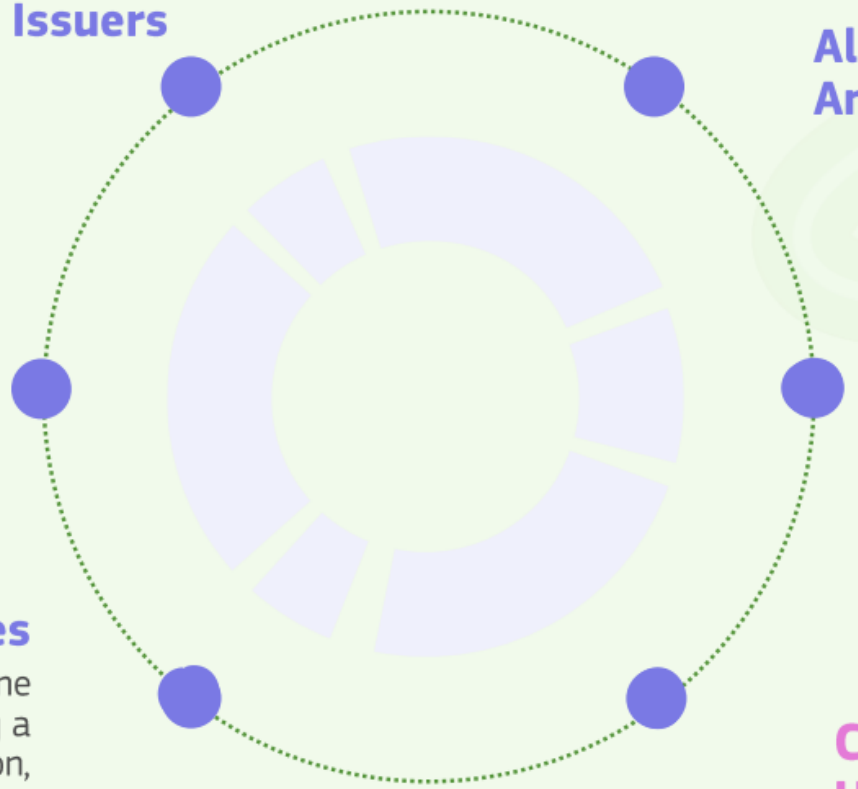
The 4 LSPs are **working towards 1-year milestones and deliverables**

Wallet Prototype Codes published 7 March (GitHub)

Main Functionalities

APPs for Verifiers and Issuers

All Mobile Platforms – Android & iOS



Identification and Authentication

Proximity and Remote

Support for Pilot Use Cases

Mobile Driving License, accessing online public and private services, opening a bank account, SIM registration, payments authorization, authenticating a third-party service to sign documents ..

Continuous Feedback and Updates

Piloted

Piloted by Large Scale Pilots

NOBID CONSORTIUM

A set of Nordic and Baltic countries who, together with Italy and Germany, who are developing a large-scale pilot for the payment use case in the EU Digital Wallet.

 # PAYMENTS

Potential
For European Digital Identity

Potential is a secure digital ID that will allow citizens to quickly and securely prove their identity as part of their online citizenship procedures.

 # MOBILE DRIVING LICENSE

 # ACCESS GOV SERVICES

 # OPEN BANK ACCOUNT

 # HEALTH

 # CONTRACTS

 # SIM REGISTRATION

EWC

The EWC aims to harness EU digital identity benefits for Digital Travel Credentials across Member States, building on the Reference Wallet Application for this specific use case.

 # PAYMENTS

 # TRAVEL

 # ORGANISATION ID

DC4EU

DC4EU supports the education and social security sectors by integrating cutting-edge digital services across Europe within a cross-border trust framework.

 # EDUCATION

 # SOCIAL SECURITY

New Call Publication

New use-cases to be piloted

Focused on 4 key areas:

1. **Wallets for Businesses** – Business-to-business and business-to-government scenarios including regulatory compliance, company registration, and power of attorney
2. **Wallets for Travel** – National and Cross-border travel scenarios including local public transport (metro/bus), long-distance travel (aviation/rail/sea/bus), shared mobility (e.g. car sharing, bike sharing), border control, hotel check-in
3. **Wallets for Payments & Banking** – Payment and banking scenarios including a standardised process for Know-Your-Customer, Strong Customer Authentication, and offline transactions and processes
4. **Wallets for Age Verification** – Age verification scenarios including the issuance of a pseudonymous attestation containing only age information by a trusted third party

Key Details	
Call Budget	20 MEUR
Co-funding rate	50%
Implementing Agency	HaDEA
Action Duration:	24 months
Timelines and deadlines (indicative)	
Call Publication	7 May 2024
Call Opening	14 May 2024
Call Deadline	24 September 2024 – 17:00:00 CEST (Brussels)
Evaluation	October-November 2024
Information on Evaluation Results	December 2024
Signature of Grant Agreements	June 2025

The EU Digital Identity Wallet timelime

The Large Scale Pilots are currently testing prototype wallets building on the specifications detailed in the Architecture and Reference Framework (ARF). After the legislation and specifications are finalised, each Member State will be obligated to offer at least one wallet to citizens, residents, and businesses.

2023

- Trilogue negotiations concluded on EU Digital Identity Wallet Regulation
- European Parliament ITRE Committee vote on the regulation

2024

- 29 Feb - Plenary vote and approval by European Parliament
- 26 Mar – European Council Approval
- 30 Apr – Publication in the Official Journal of the European Union
- Adoption and publication of the Wallet Implementing Acts

2025

- First Member States Wallets made available

2026

- Wallets widely available in all Member States

Regulation

Implementing acts

Piloting

Implementation by Member States

Ready ?

Visit our website and discover how the Wallet works.

Reviderade eIDAS-förordningen

Regeringskansliet och eIDAS

- RK ansvarar för förhandling och implementering av eIDAS-förordningen i Sverige
- RK blir förordnad i genomförandekommittén för eIDAS
- RK förordnar experter från myndigheter att delta i grupperingar kopplat till eIDAS, ex. expert group
- RK skriver instruktioner till de personer som är representanter för Sverige på expertgruppsmöten

Reviderade eIDAS-förordningen

- Plånboken ska möjliggöra för *fysiska och juridiska* personer att på ett *säkert* sätt bl.a. begära, erhålla, lagra och använda *personidentifieringsuppgifter* och digitala bevis för autentisering online och offline samt att skriva under med kvalificerade elektroniska underskrifter.
- Introducerar nya betrodda tjänster som elektroniska attributsintyg och en elektronisk arkiveringstjänst.
- Förordningen träder i kraft 20 maj 2024.

Krav på medlemsstaterna

- Tillhandahålla en digital identitetsplånbok
- Register över förlitande parter
- Utse en tillsynsmyndighet
- Utse ett organ som ansvarar för certifiering av plånboken
- Utse en gemensam kontaktpunkt

Krav på offentlig sektor

- Tillåta användning av digitala identitetsplånböcker vid inloggning på myndigheten/regionen/kommunens digitala tjänster
- Digitala attributsintyg – ny betrodd tjänst
  - Utfärda, verifiera och ta emot digitala attributsintyg
  - Attributsintyg innehåller vissa uppgifter om personen, exempelvis adress, ålder, kön, utbildningsmeriter

Krav på privat sektor

- När stark autentisering krävs i författning eller avtal så måste privata aktörer acceptera plånboken som ett medel för identifiering.
- Om användaren kräver det så måste stora onlineplattformar acceptera plånboken.

Nationella initiativ

- Utredningen om säker och tillgänglig digital identitet tillsattes 2022
- Digg fick i årets regleringsbrev uppdraget att utveckla en statlig e-legitimation

En säker och tillgänglig statlig e-legitimation (SOU 2023:61)

- Digg utfärdar en e-legitimation och antingen Polismyndigheten eller Skatteverket utför grundidentifieringen.
- Svenskt personnummer eller styrkt samordningsnummer krävs för att kunna få en statlig e-legitimation
- E-legitimationen ska tillhandahållas på ett kontaktlöst aktivt kort men bör så snart som möjligt tillhandahållas på ett statligt utfärdat identitetskort
- Det ska ställas krav på offentliga aktörer att tillåta identifiering med e-legitimationer som är anslutna till auktorisationssystemet för elektronisk identifiering och digital post

Utredningens slutbetänkande

Utredningen lämnar sitt slutbetänkande 17 juni 2024. Uppdraget är att bl.a. utreda:

- hur en kostnadseffektiv digital identitetsplånbok ska utfärdas,
- hur en digital plånbok kan användas för största möjliga nationella effektivitet och nytta,
- ta ställning till vilken myndighet som bör utses till tillsynsorgan och vilken myndighet som bör ha ansvar för ett register över förlitande parter.

Aktuella frågor nationellt

- Omhänderta utredningen om säker och tillgänglig digital identitets delbetänkande
- Bemanna och förordna experter som kan delta i utformandet av genomförandeakter
- Omhänderta Utredningen om säker och tillgänglig digital identitets slutbetänkande

Implementera den reviderade eIDAS-förordningen

Översyn av digitaliseringspolitiken

Säkerhet och resiliens

AI och andra tekniker

Data

Tack!

PAUS

SWEDAC

Styrelsen för ackreditering och teknisk kontroll
Swedish Board for Accreditation and Conformity Assessment

2024-05-07

Swedac – kvalitetssäkrar för ökad tillit och konkurrenskraft

Magnus Pedersen

SWEDAC

Utrikesdepartementet

Biståndsminister och utrikeshandelsminister,
Johan Forssell.

SWEDAC ACKREDITERING

SWEDAC

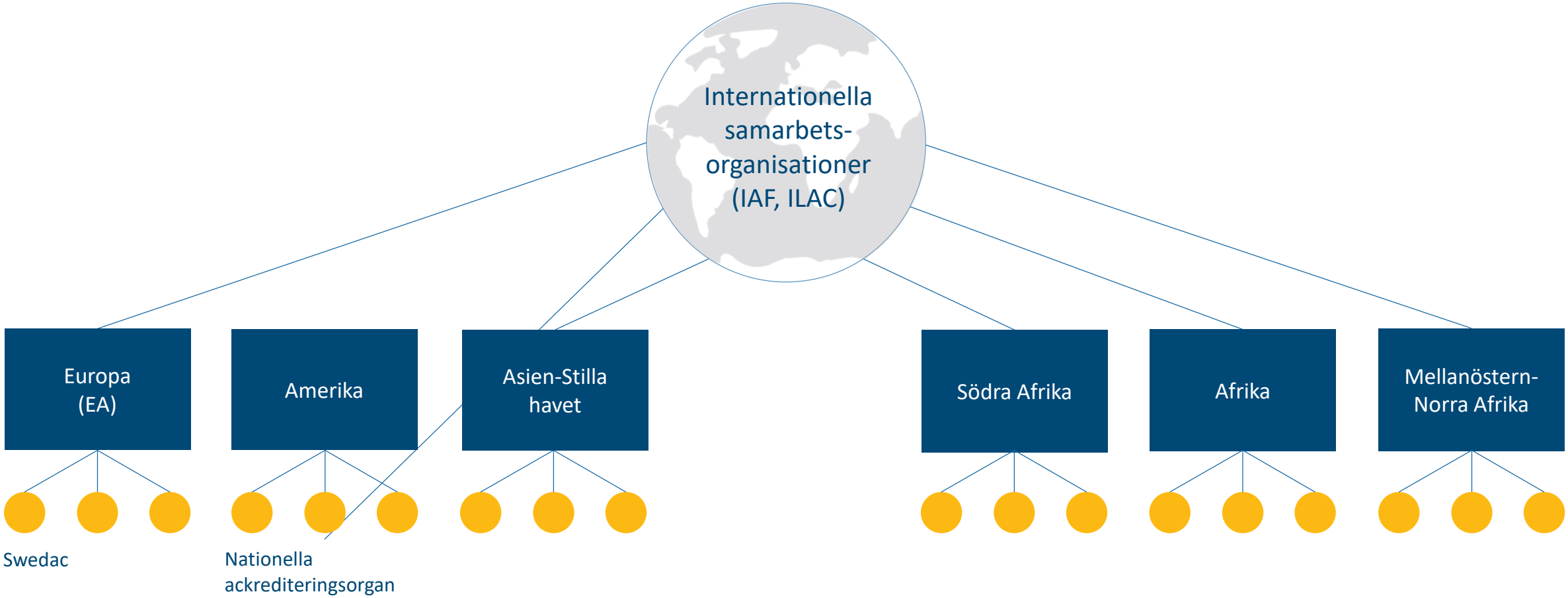
Omfattar:
Bedömning av kompetens och ledningssystem för att säkerställa att alla krav uppfylls

Baseras på:
- → Opartiska aktörer
- → Svensk samt europeisk lagstiftning
- → Nationell och internationell nivå
- → Standard

Bidrar till:
- → Stärkt konsumentskydd
- → Stärkt konkurrenskraft
- → Ökad hållbarhet
- → Ökad kvalitet och säkerhet

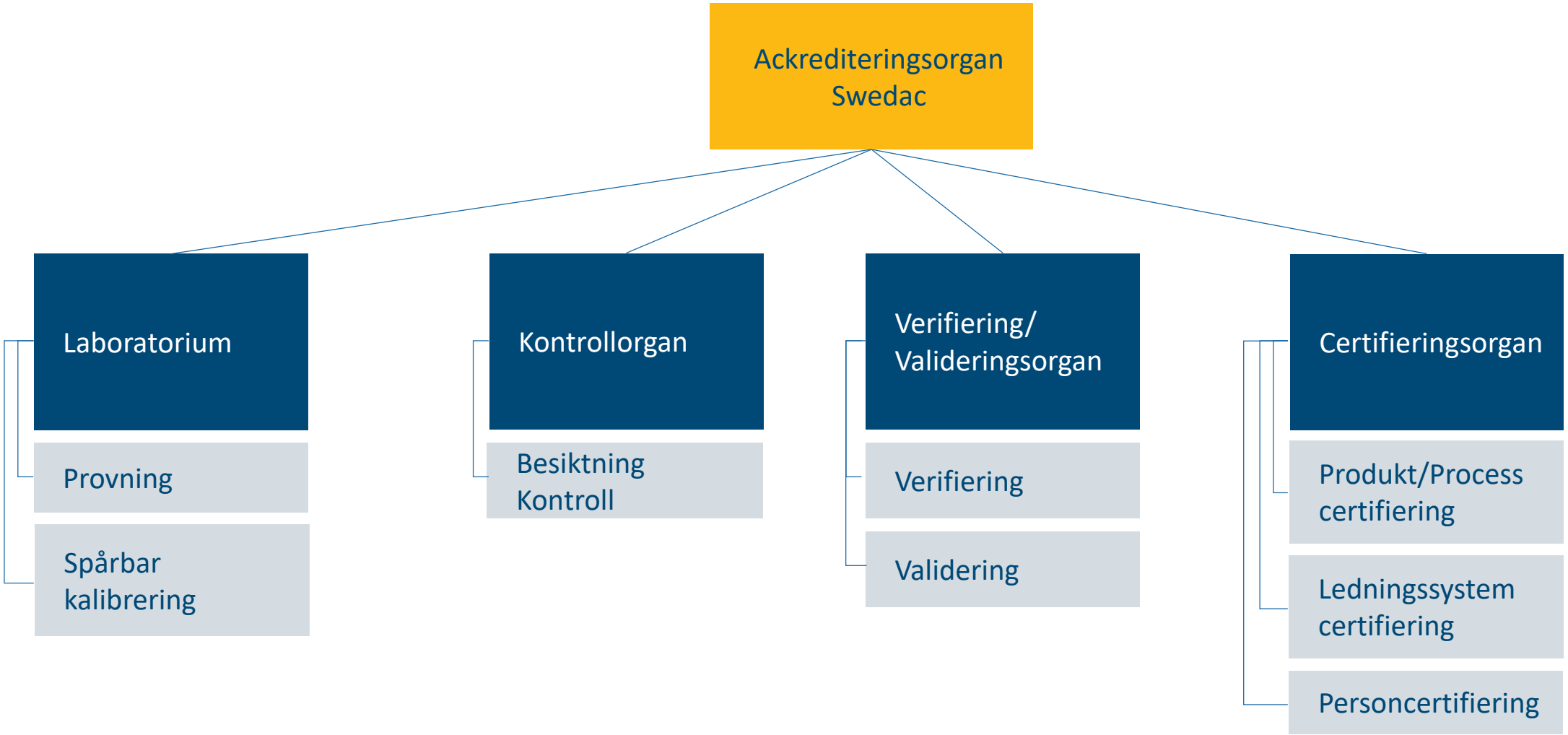
Referens: Förordning EG 765(2008)

Internationellt samarbete



EA = European co-operation for Accreditation,
IAF = International Accreditation Forum
ILAC = International Laboratory Accreditation Cooperation

SWEDAC


Ackrediteringsorgan
Swedac
Laboratorium
Provning
Spårbar kalibrering
Kontrollorgan
Besiktning
Kontroll
Verifiering/
Valideringsorgan
Verifiering
Validering
Certifieringsorgan
Produkt/Process certifiering
Ledningssystem certifiering
Personcertifiering

Ackreditering

SWEDAC

Krav:
Eu regelverk
Implementerande akt
Standard

Ägare av en ordning:
- Kommissionen
  - ENISA
- Myndighet

Hur certifieringen ska gå till
(Certifieringsordning/scheme)

Det som skall certifieras

Certifieringsorgan

Swedac ackrediterar

Tack

Magnus Pedersen

E-post: magnus.pedersen@swedac.se

eIDAS – identitetsplånbok – Certifiering
Cybersäkerhet – en kort introduktion

FÖRSVARETS MATERIELVERK | FMV

Kort om innehållet

- Kort om mig och FMV
- Ansvar för certifiering
- Krav på certifiering
- Tidsperspektiv
- Certifieringens egenskaper
- Utvecklingen i Sverige
- Om ni har frågor - kontaktuppgifter

Kort om mig och FMV

Mats Engquist, Operativ chef på Sveriges certifieringsorgan för IT-säkerhet (CSEC) som finns på Försvarets materielverk.

Deltar i:

- Samverkansgrupp eIDAS
- EU:s ad-hoc grupp för peer reviev

CSEC är en del av den nationella myndigheten för cybersäkerhetscertifiering (NCCA) enligt EU:s cybersäkerhetsakt.

Deltar i flera arbetsgrupper som tangerar detta ämne, speciellt i:

- EU:s ”eIDAS subgroup for certification"

Jag är hyggligt välorienterad om certifiering men är på intet sätt expert på arkitektur eller infrastruktur för t.ex. identitetsplånböcker eller e-legitimationer.

Ansvar för certifiering

FMV (CSEC) ansvarar för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter och anordningar för kvalificerade elektroniska stämplar enligt artikel 30 och 39 i eIDAS – men det har inte resulterat i några certifieringar.

FMV föreslås eventuellt även få ett övergripande ansvar för certifiering av europeiska digitala identitetsplånböcker i Sverige. Detta är inte klart och vad ansvaret betyder återstår att reda ut.

Detta följer naturligt av FMV:s roll som Nationell myndighet för cybersäkerhetscertifiering (NCCA) enligt EU:s cybersäkerhetsakt.

Krav på certifiering

När eIDAS2 träder ikraft kommer certifiering av identitetsplånboken att bli obligatorisk. Certifieringen skall ske inom Cybersäkerhetsaktens ramverk.

Delar av certifieringen antas göras på hög assuransnivå enligt en europeisk certifieringsordning som är under framtagande.

I väntan på den europeiska ordningen skall medlemsstaterna ta fram egna nationella certifieringsordningar (*som uppfyller kraven i kommissionens genomförandeakt till förordningen om ett ramverk för elektronisk identifiering*) som kan verka under mellantiden.

Tidspespektiv

EIDAS2 publicerades i EU:s Official journal den 30-04-2024 och träder ikraft 20 dagar därefter.

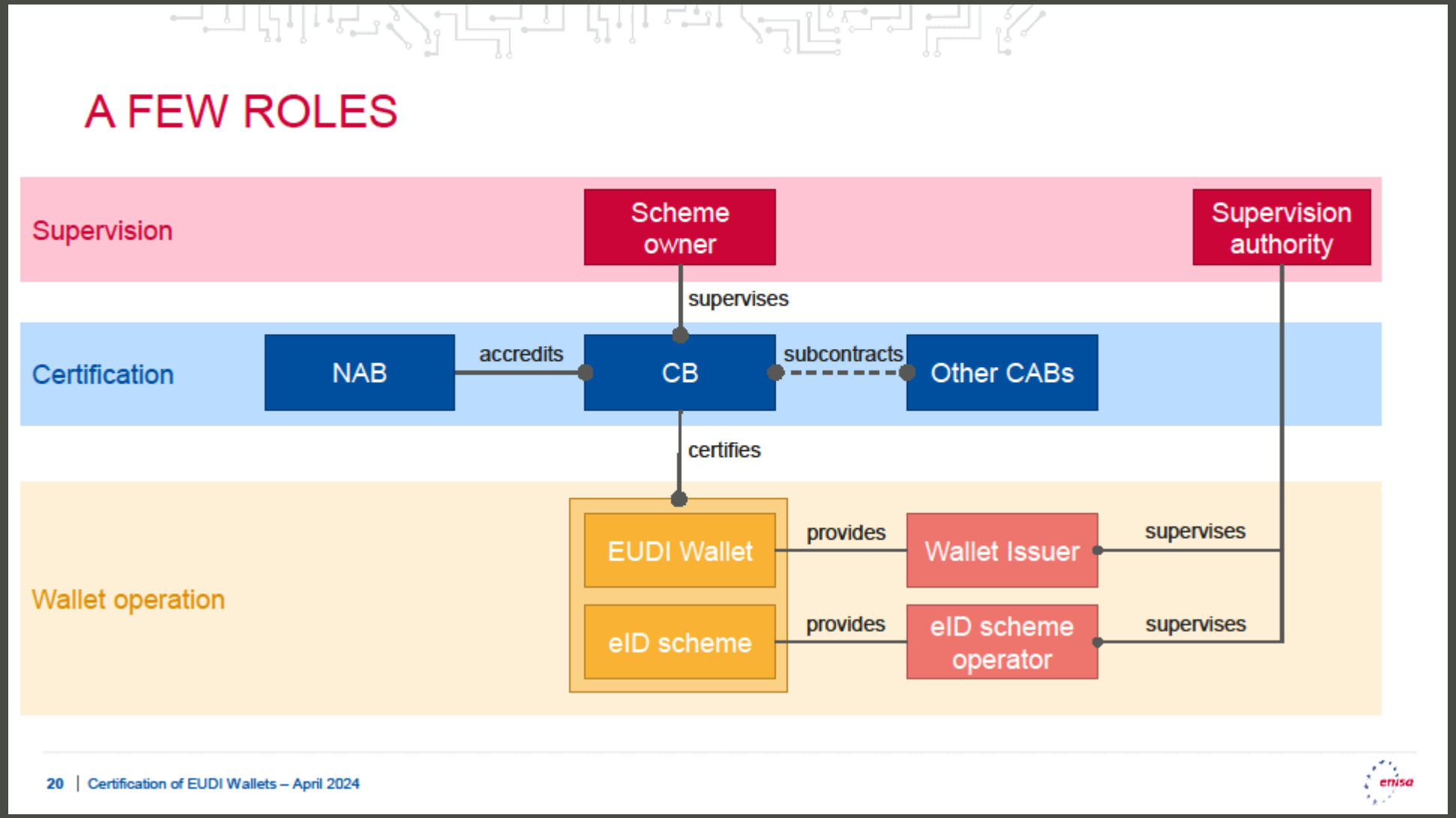
De första genomförandeakterna skall vara klara efter 6 månader. Detta gäller bland annat reglerna för certifiering.

Därefter har MS 2 år för införande av plånboken (plånböckerna)

När en europeisk certifieringsordning för eIDAS2 kan vara klar är oklart. Tidigare certifieringsordningar har tagit flera år.

Tidsplanen är optimistisk.

Roller


A FEW ROLES
Supervision
Scheme owner
Supervision authority
supervises
Certification
NAB
accredits
CB
subcontracts
Other CABs
certifies
Wallet operation
EUDI Wallet
provides
Wallet Issuer
supervises
eID scheme
provides
eID scheme operator
supervises
20 | Certification of EUDI Wallets – April 2024
enisa

Certifiering - egenskaper

Certifieringen kommer att innehålla olika delar som kan utgå från redan befintlig certifieringsordning (EUCC) inom EU:

- WSCD (secure device) skall certifieras på hög assuransnivå (AVA_VAN.5)
- WSCA (secure application) skall certifieras på lämplig nivå, viket också antas vara AVA_VAN.5.
- Allt annat är öppet…

Certifieringen skall utföras på tillräckligt hög nivå för att täcka de högnivårisker som identifierats för EUDI-plånboken.

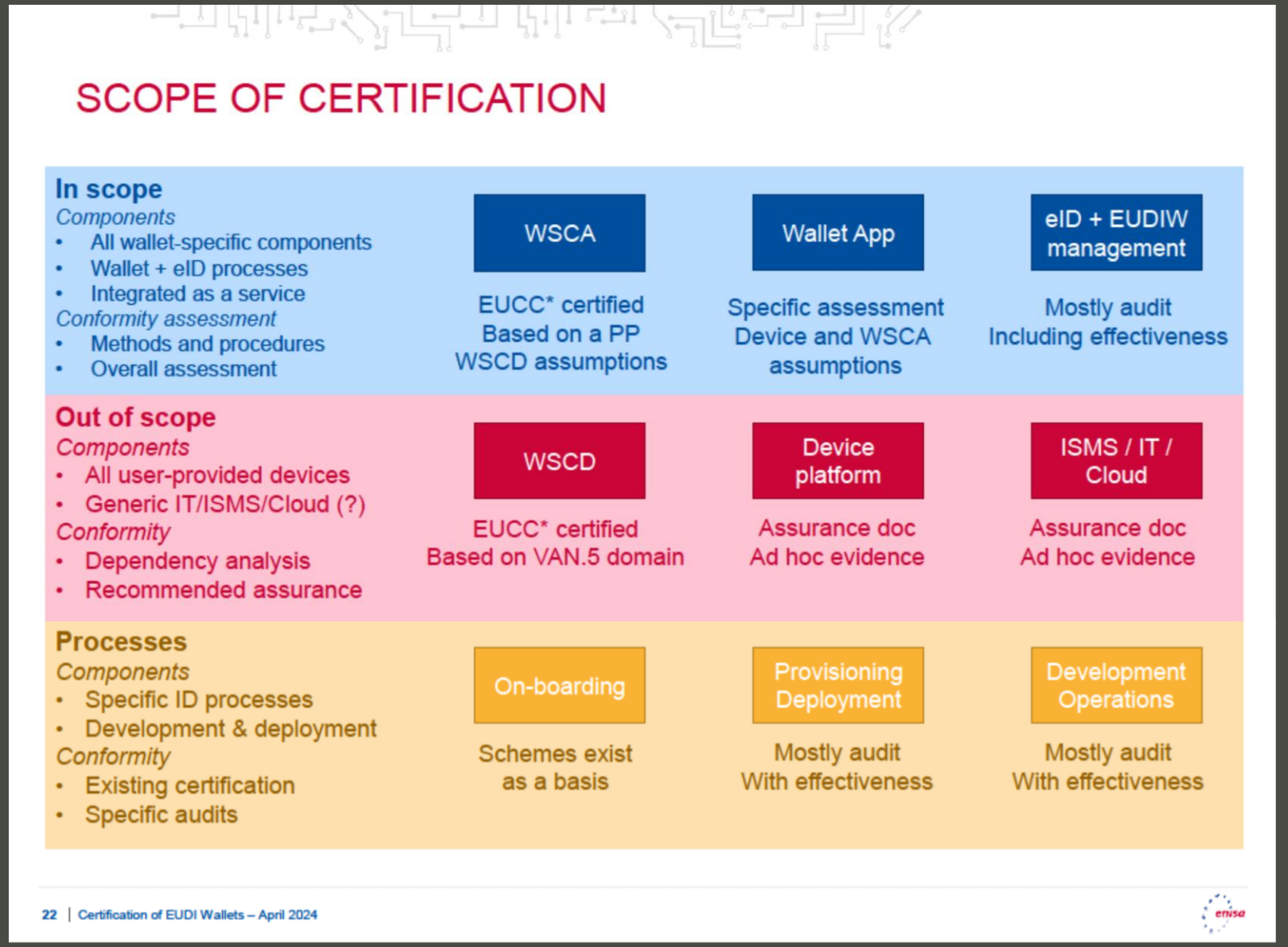
Medarbetare från FMV/CSEC deltar i arbetet med den gemensamma certifieringsordningen.

Värt att betänka att assuransnivå ”hög” enligt cybersäkerhetsakten – inte direkt motsvarar tillitsnivå ”hög” inom eIDAS.

Det finns röster som även pekar på att andra certifieringsordningar kan spela en roll:

- EU5G – Certifiering av mobil kommunikation
- EUCS – Certifiering av molntjänster

Scope


SCOPE OF CERTIFICATION
In scope
Components
• All wallet-specific components
• Wallet + eID processes
• Integrated as a service
Conformity assessment
• Methods and procedures
• Overall assessment
WSCA
EUCC* certified
Based on a PP
WSCD assumptions
Wallet App
Specific assessment
Device and WSCA
assumptions
eID + EUDIW management
Mostly audit
Including effectiveness
Out of scope
Components
• All user-provided devices
• Generic IT/ISMS/Cloud (?)
Conformity
• Dependency analysis
• Recommended assurance
WSCD
EUCC* certified
Based on VAN.5 domain
Device platform
Assurance doc
Ad hoc evidence
ISMS / IT / Cloud
Assurance doc
Ad hoc evidence
Processes
Components
• Specific ID processes
• Development & deployment
Conformity
• Existing certification
• Specific audits
On-boarding
Schemes exist
as a basis
Provisioning Deployment
Mostly audit
With effectiveness
Development Operations
Mostly audit
With effectiveness
22 | Certification of EUDI Wallets – April 2024
enisa

Utvecklingen i Sverige

Idag är det CSEC som utför certifieringar inom Common Criteria-området i Sverige.

I och med att certifieringsordningar inom cybersäkerhetsakten träder ikraft ser vi en utveckling mot att privata certifieringsorgan tar över ansvaret för all certifiering.

Detta gäller även assuransnivå ”hög” där cybersäkerhetsakten annars öppnar för statliga organ.

Detta gäller även certifieringar för eIDAS.

Frågor

En hel del kring detta är ännu ganska otydligt.

Vi saknar såväl certifieringsordningar som standarder att certifiera mot samtidigt som både regleringar och marknad är lite otydliga.

Den som är intresserad av certifieringsfrågor är alltid välkommen att kontakta oss på FMV:

- Mig: mats.engquist@fmv.se
- CSEC: csec@fmv.se (www.csec.se)
- NCCA: icc@fmv.se (https://www.fmv.se/verksamhet/ovrig-verksamhet/ncca/)

Auktorisationssystem

7 maj 2024

Information om pågående arbete

Digg har påbörjat en rad informations och samverkans möten

Det är via dessa era frågor och synpunkter huvudsakligen kommer behandlas

Dagens presentation är tänkt att ge som en översikt om förändringen

- Repetition för er som deltog i förra veckan
- men kanske av visst intresse även för leverantörer som inte direkt berörs

Presentationens delar

1. Inledning
2. Lagstiftningen
3. Vad blir skillnaden?
4. Beskrivning av Diggs arbete

Lagstiftningen

Vad är auktorisationssystem?

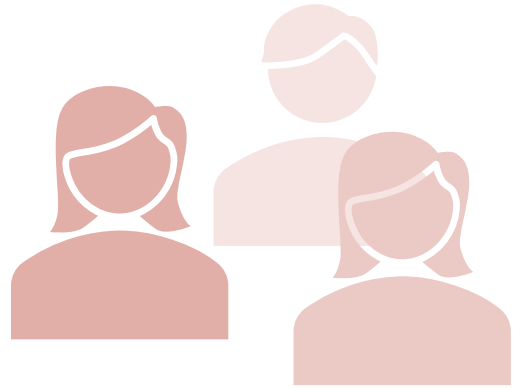
Med ett auktorisationssystem avses ett system där

- Digg *godkänner* att leverantörer av tjänster för elektronisk identifiering av enskilda *eller* för digital post får ingå ett avtal inom systemet och *ingår avtal* med var och en av de godkända leverantörerna om utförande av sådana tjänster,
- en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning, och
- en offentlig aktör kan använda tjänsterna i sin verksamhet enligt avtal med Digg.

Offentliga aktörer

Leverantörer

Tillhandahållande myndighet
Digg



Enskilda

Vad blir skillnaden?

Bild utifrån arbetshypotes

Förändringar kring digital post

Nuläge	Nyläge
För offentliga aktörer	Ingen förändring
Valfritt att ansluta	Ingen förändring
Fler aktörer tillkommer efter hand	Ingen förändring
Digg formulerar krav och granskar	Ingen förändring
Avgiftsfritt för anslutna offentliga aktörer	Digg tar in avgift från offentliga aktörer
Ingen ersättning till leverantörer av digital brevlåda	Digg betalar ersättning till leverantörer av digital brevlåda

Bild utifrån arbetshypotes

Förändringar kring e-legitimation

Nuläge	Nyläge
För upphandlande myndigheter	Även privata aktörer (ex. skola, hälso- och sjukvård)
Valfritt att ansluta	Obligatoriskt för statliga myndigheter (valfritt för övriga)
Fler aktörer tillkommer efter hand	Ingen förändring
Digg formulerar krav och granskar	Ingen förändring
Oklart om alla e-legitimationer erbjuds i praktiken i e-tjänsterna	Obligatoriskt erbjuda alla ingående e-legitimationer
Leverantörerna av e-leg fakturerar offentliga aktörer direkt	Digg tar in avgift från offentliga aktörer och betalar ersättning till leverantörerna av e-leg
Fastpris per e-legitimering	Annan ersättningsmodell

Vad gör Digg nu?

- Analysarbete och framtagning av krav och villkor som ska gälla för leverantörer och dess tjänster för respektive auktorisationssystem
- Kunskapsinhämtning och analys kring avgift- och ersättningsmodell, både med offentliga aktörer, leverantörer och nordiska länder

Områden att samverka kring

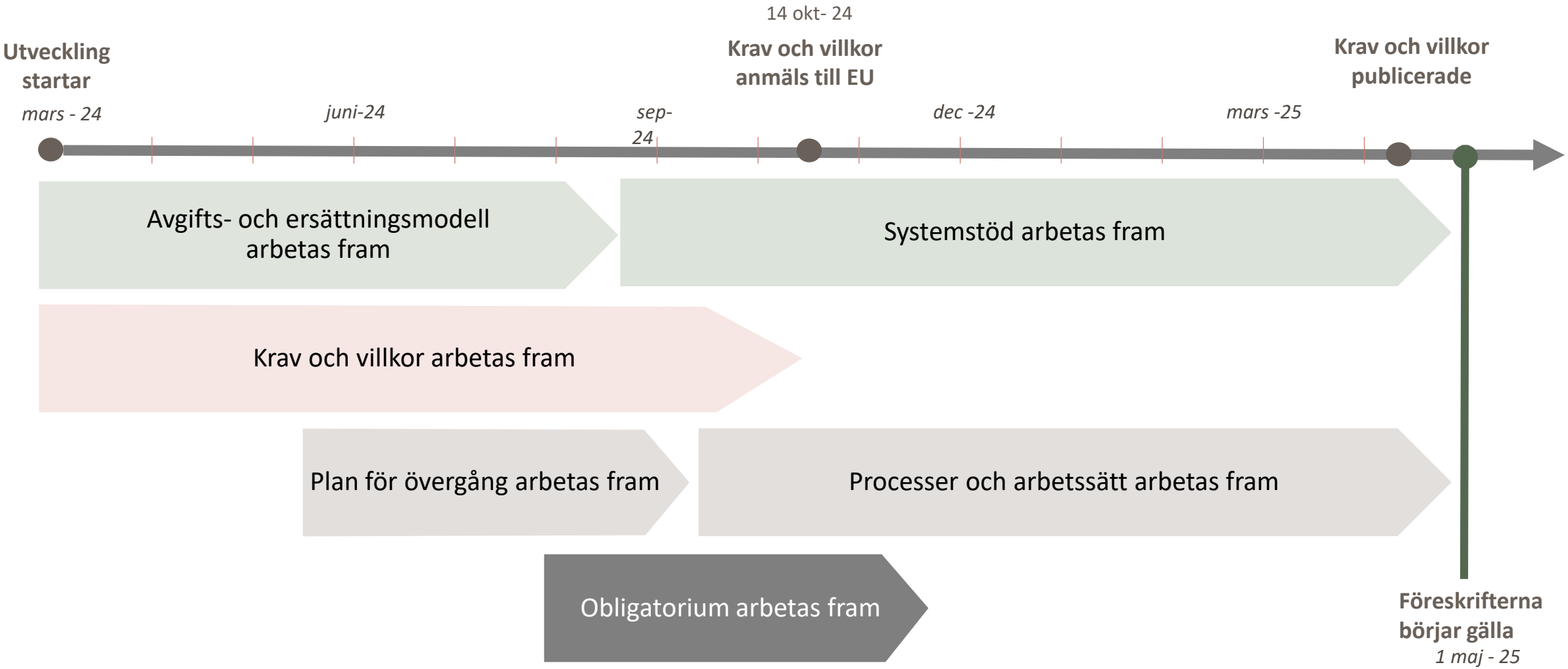
Avgift/ersättning

Krav, villkor och obligatorium (e-leg)

Övergång

Granskning och redovisning

Planering


14 okt- 24
Utveckling startar
mars - 24
juni-24
sep-24
Krav och villkor anmäls till EU
dec -24
mars -25
Krav och villkor publicerade
Avgifts- och ersättningsmodell arbetas fram
Systemstöd arbetas fram
Krav och villkor arbetas fram
Plan för övergång arbetas fram
Processer och arbetssätt arbetas fram
Obligatorium arbetas fram
Föreskrifterna börjar gälla
1 maj - 25

Samverkan

- Digg avser samverka med leverantörer av tjänster för e-legitimering och digital post.

- Inbjudningar till samverkan annonseras på digg.se där även resultatet kommer publiceras

För mer information

Auktorisationssystem | Digg

https://www.digg.se/digitala-tjanster/auktorisationssystem

Lunch på egen hand

Återsamling kl. 13.00

Agenda

9.05-9.15	Aktuellt från Digg och PTS Sarah Amandusson, Digg Isabelle Westerlund, PTS
9.15-9.45	Aktuellt på EU-nivå Åsa Barton, EU-kommissionen
9.45-10.15	Aktuella frågor nationellt Ylva Wide, Regeringskansliet
10.15-10.45	**PAUS**
10.45-11.15	Ackreditering och certifiering - en allmän orientering Magnus Pedersen, Swedac Mats Engqvist, FMV
11.15-11.45	Auktorisationssystem Roger Fagerud, Digg
11.45-13.00	**Lunch på egen hand**
13.00-13.30	Nyheter eID och plånboken Anneli Hagdahl och Roger Fagerud, Digg
13.30-14.00	Large Scale Pilot Sarah Amandusson, Digg
14.00-14.30	Nya betrodda tjänster eIDAS2 Björn Scharin och Anna Amundberg, PTS
14.30-15.00	**PAUS**
15.00-15.30	Hur påverkas leverantörer av NIS2? Emma Wirf och Catherine Persson, PTS
15.30-16.00	Öppen frågestund & Avslut Emelie Björkengren Näslund, PTS

MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government

Nyheter eID och plånboken

Anneli Hagdahl, strateg

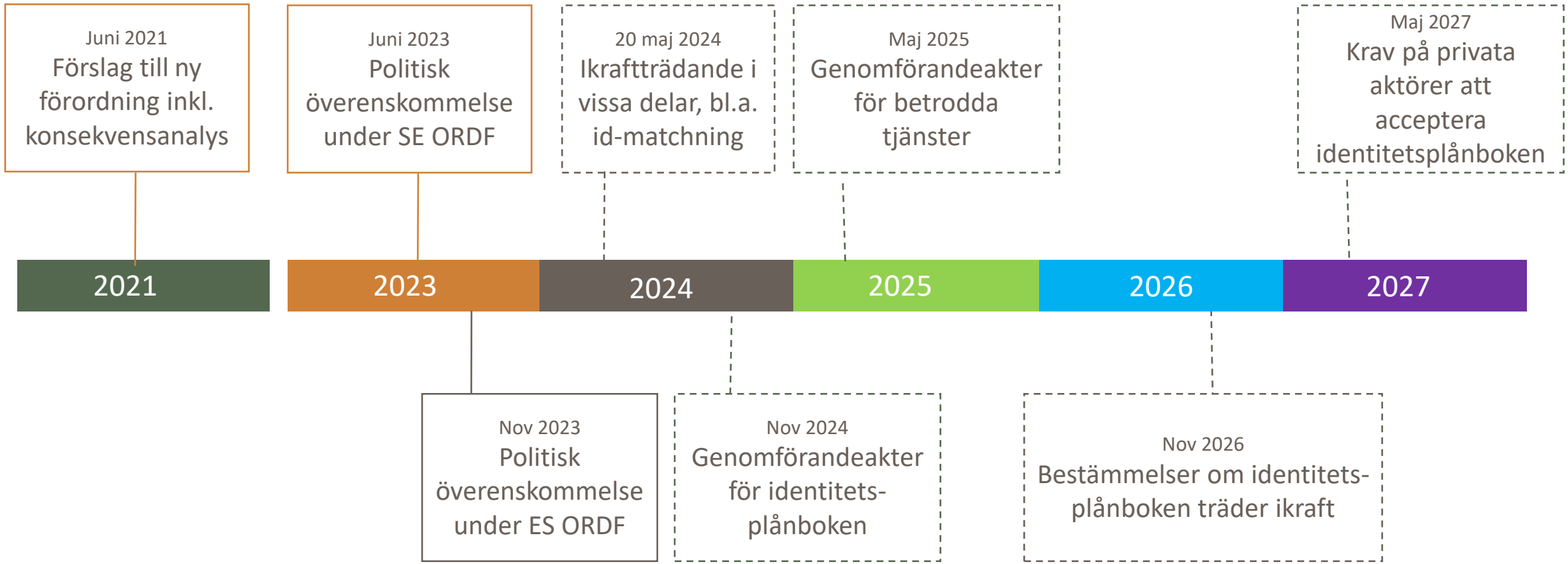
Roger Fagerud, strateg

Enheten för Identitet och Auktorisation

Varför uppdateras förordningen?

- EU-kommissionens analys visar att syftet inte har uppnåtts
  - eIDAS I var tänkt att
    - Stärka den digitala inre marknaden
    - Öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen
  - Men spridningen har gått för sakta:
    - För få medborgare har eller använder en e-legitimation
    - För få digitala tjänster tillåter gränsöverskridande e-legitimering
    - Privat sektor har i för låg grad inkluderats
  - Förstärka användarens kontroll över sina data

Tidslinje för ikraftträdande



eID: förändringar i korthet

- Nuvarande eID-system finns kvar
- Pseudonymer *valda av användaren*
- Certifiering av eID-system alternativ till sakkunnig-granskningar
- Gränsöverskridande identitetsmatchning
- Införande av EUDIW - Europeiska digitala identitetsplånboken
  - PID – personidentifieringsuppgifter
  - Attesterade attribut
  - Certifiering

Gränsöverskridande identitetsmatchning

- När medlemsstaterna agerar som förlitande parter för gränsöverskridande tjänster ska de **säkerställa otvetydig identitetsmatchning** för fysiska personer som använder anmälda medel för elektronisk identifiering eller europeiska digitala identitetsplånböcker.
- Medlemsstaterna ska vidta åtgärder för att säkerställa en **hög skyddsnivå för personuppgifter** som används för identitetsmatchning och för att förhindra profilering av användare.

Europeiska digitala identitetsplånboken

- Medel som låter användaren
  - E-legitimera sig på högsta tillitsnivå
  - Kontrollera motpartens identitet
  - Dela personuppgifter på ett integritetssäkert sätt
  - Underteckna med kvalificerad elektronisk underskrift
- Online och off-line
- Funktioner för validering, återkallelse och spärr

Nya uppgifter för Sverige

Ge ut svenska digitala identitetsplånböcker

- under ett eID-system på tillitsnivå Hög

- Modell för utgivning:
  1. Medlemsstat (MS)
  2. På uppdrag av MS (upphandling)
  3. Oberoende men godkänd av MS
- Plånböcker ska certifieras och meddelas till KOM
- Plånboksutfärdaren ska intyga att varje enskild plånboksinstans är en av Sverige godkänd plånbok
- Funktioner för validering, spärr och återkallelse

Nya uppgifter för Sverige

Ge ut personidentifieringsuppgifter (PID)

- PID består av attribut som unikt identifierar en fysisk eller juridisk person
- Plånboksprogramvara + PID = identitetsplånbok
- PID kan utfärdas fristående från plånboksutfärdaren
- Validera, spärra och återkalla PID

Nya uppgifter för Sverige

Registrera aktörer som vill förlita sig på plånboken

Förlitande part: en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst

- Förlitande parter ska anmäla sin avsikt att ta emot personuppgifter från plånboken
- Vilka uppgifter man avser att ta del av och vilken rätt man har att ta del av de uppgifterna
- Detta ska ske på ett kostnadseffektivt sätt

Utökade uppgifter för Sverige

Delta i det utökade eIDAS-samarbetet

- Representera SE i EU:s samarbetsorgan för plånboken
- Tillhandahålla utbildning och support
- Delta i framtagandet av genomförandeakter
- Cybersäkerhetsfrågor ska hanteras enligt cybersäkerhetsakten under ledning av ENISA
  - Framtagande av krav och specifikationer för certifiering
- *Kan kräva bredare deltagande, förutom Digg och PTS*

Nya uppgifter för Sverige

- Obligatoriskt även för privata aktörer att acceptera plånboken, där så kallad stark autentisering krävs i författning eller avtal
- Infrastruktur som e-tjänster behöver för att verifiera användarnas plånböcker mm måste därför erbjudas till alla
- Stora onlineplattformar ska acceptera plånboken om användaren kräver det
- (art. 5f.2 och 5f.3)

Nya uppgifter för offentlig sektor

Ge ut attesterade attributsintyg

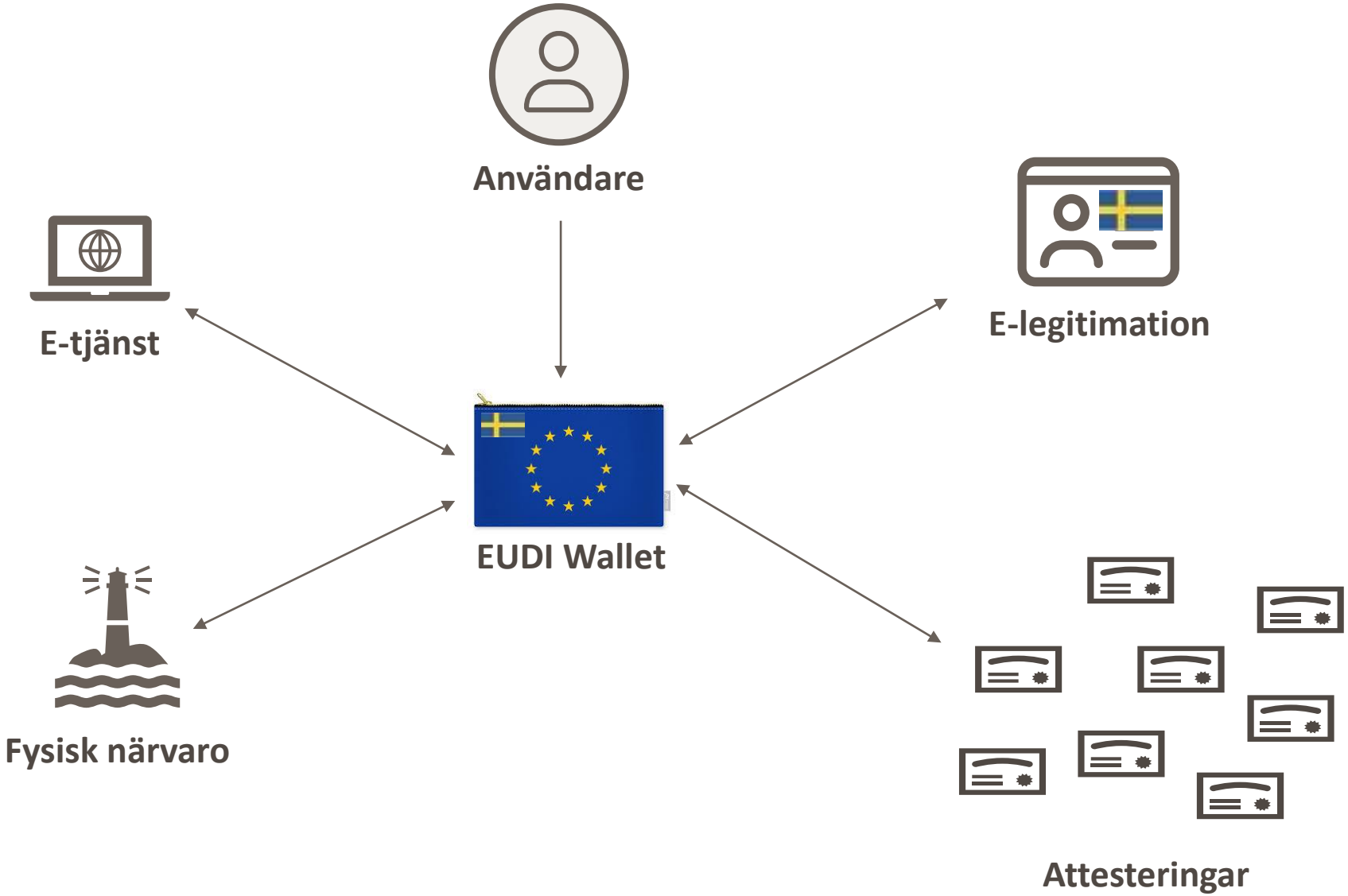
- Attribut = utdrag ur register eller beslut
- Attribut som intygar någonting om användaren
- Förordningen likställer det rättsliga värdet för kvalificerade attesterade attribut med motsvarande pappersdokument
- Funktioner för validering, spärr och återkallelse
- Betrodd tjänst under tillsyn av PTS

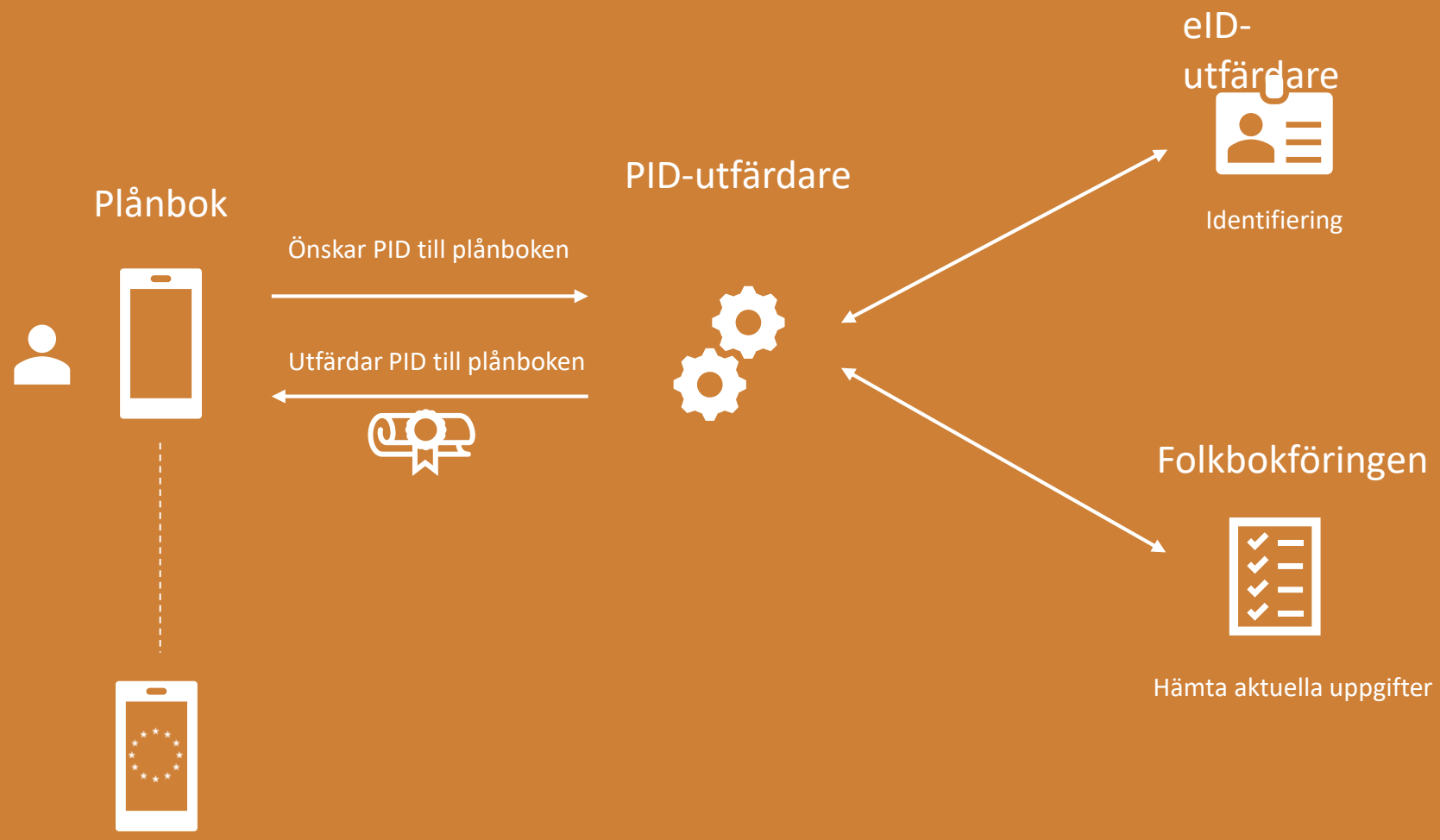
Nya uppgifter för offentlig sektor

Agera som förlitande part

- Anpassa sina e-tjänster för att
  - Acceptera plånböcker som medel för e-legitimering
  - Kunna ta emot attesterade attribut
  - Nödvändig data
  - Användning av pseudonymer

Den europeiska digitala identitetsplånboken


Användare
E-tjänst
E-legitimation
EUDI Wallet
Fysisk närvaro
Attesteringar


eID-
utfärdare
Identifiering
PID-utfärdare
Plånbok
Önskar PID till plånboken
Utfärdar PID till plånboken
Folkbokföringen
Hämta aktuella uppgifter
Identitetsplånbok
utfärdad av SE

Plånbokens egenskaper

- Användaren ska kunna kontrollera:
  - vilka uppgifter som ska delas i en e-tjänst
    - bara de uppgifter som behövs i ett ärende ska behöva delas
  - vem uppgifter delas med
    - motpartens identitet ska kunna kontrolleras
    - delningen ska inte ”läcka”, exempelvis ska inte den som utfärdat uppgifterna kunna se vem uppgifterna delades med
- Uppgifter som lämnats vid olika tillfällen eller till olika mottagare ska inte kunna kombineras
  - attesteringen ska därför utformas så att den i sig inte ökar möjligheten att kombinera data

Utfärdarens skyldigheter

- Utfärdare av attesterade attribut eller plånbok inte får samla information om användaren
- Får inte veta var informationen används

Förlitande parts skyldigheter

- Inte begära mer information än som krävs
  - Acceptera pseudonymer
- Inte kombinera uppgifter lämnade vid olika tillfällen
- Inte verifiera uppgifterna genom att kontrollera hos utgivaren

Frågor?

EU:s storskaliga pilotprojekt

EU:s digitala identitetsplånbok

Finansieras av Europeiska unionen

EU Digital Identity Wallet

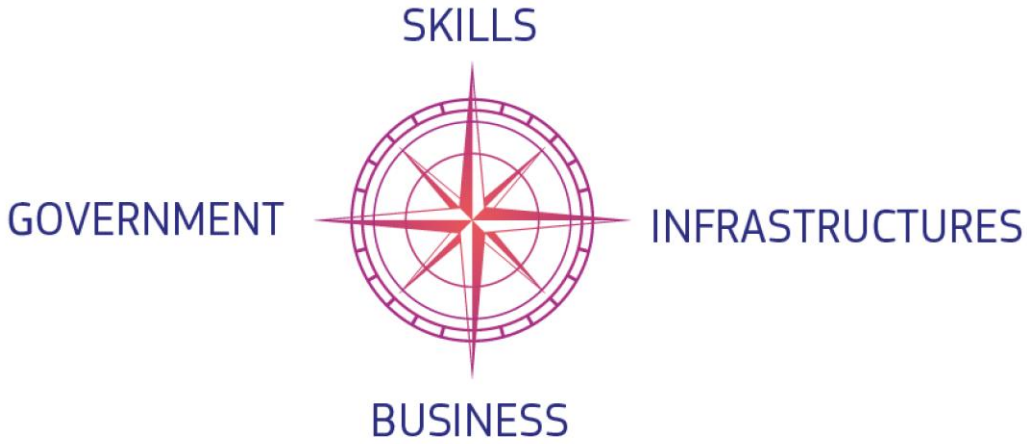
Om mig

- Sarah Amandusson
- Specialist, Digital identitet och auktorisation
- Storskaliga pilotprojekt (LSP) för EU:s digitala identitetsplånbok (EUDI Wallet)

EU:s digitala decenniur

- Vägleder EU:s digitala omställning med konkreta mål för 2030

- **Digital identitet**: alla i EU ska kunna skaffa en e-legitimation



Finansieras av Europeiska unionen

EU Digital Identity Wallet

Programmet för ett digitalt Europa (DIGITAL)

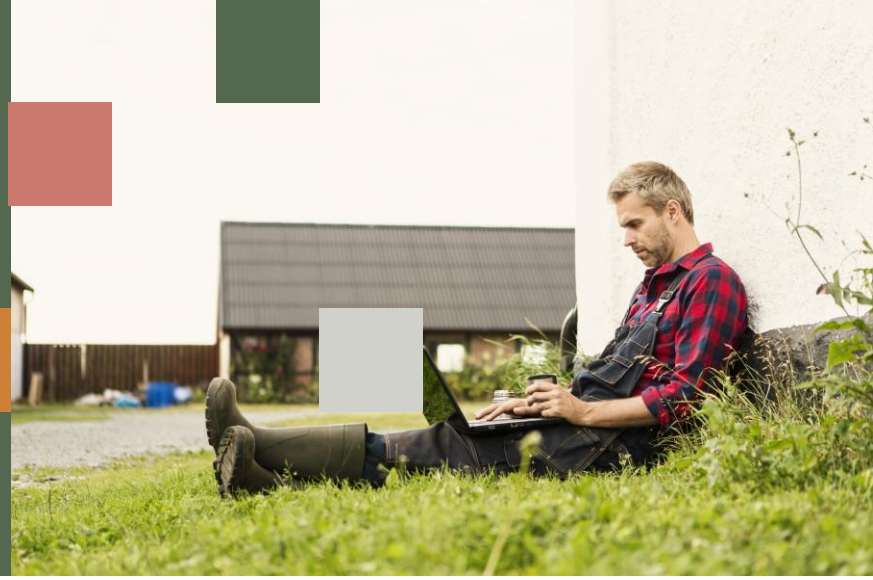
- DIGITAL är ett EU-finansieringsprogram som ska forma och stödja den digitala omvandlingen av Europas samhälle och ekonomi

- LSP EUDI Wallet delfinansieras av DIGITAL

Finansieras av Europeiska unionen

EU Digital Identity Wallet

Piloternas grundpelare



1

eIDAS2

2

Testfall

3

Teknisk verktygslåda och referensarkitektur

4

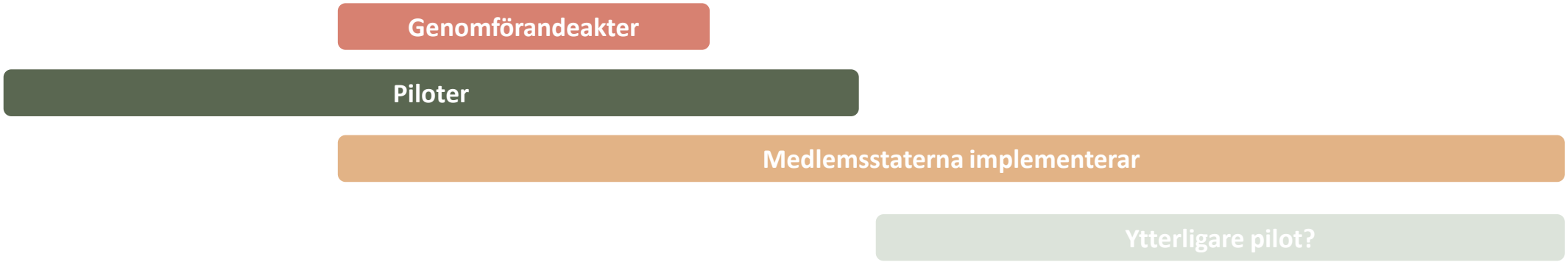
Prototyp-plånbok

Finansieras av Europeiska unionen

EU Digital Identity Wallet

Tidslinje - piloter

2023	2024	2025	2026	2027?
• Triloger, politiska överenskommelser • Pilotstart 1 april	• eIDAS2 • Prototypplånbok • ARF-uppdatering	• Piloter slut 1 april? • Mindre pilot?	• Medlemsstater ska ha identitets-plånböcker	• Andra pilotomgång slut?



Finansieras av Europeiska unionen

EU Digital Identity Wallet

Parter i ekosystemet

EU

Europeiska kommissionen
Europeiska parlamentet
European rådet

Förlitande part

Offentliga och privata organisationer som verifierar attesteringar och PID

Statliga organ

Myndigheter
Dataskydd
Ackrediteringsorgan

Plånboksutfärdare

Plånboksutvecklare
Hårdvarutillverkare
Tillhandahållare av betrodda tjänster

Utfärdare

Utfärdare av PID och attestateringar

Plånboks-användare

Europeiska medborgare, invånare och företag som hämtar och använder attesteringar

Finansieras av Europeiska unionen

EU Digital Identity Wallet

POTENTIAL
European Consortium for Digital Identity

- Tillgång till offentlig tjänst
- Öppna bankkonto
- Ansöka om SIM-kort
- Mobilt körkort
- Underteckna avtal
- E-hälsa

NOBID CONSORTIUM

- Initiering av betalningar

DC4EU

- Utbildningsuppgifter för att söka jobb
- Socialförsäkrings-förmåner

EWC

- Resor (pass, visum, resehandlingar)
- Juridisk person
- Initiering av betalningar

Finansieras av Europeiska unionen

EU Digital Identity Wallet

DC4EU

- Digg
- Vetenskapsrådet (Sunet)
- Finansiell ID-teknik AB
- Internetstiftelsen
- Ladok-konsortiet (via Umeå Universitet)
- Socialstyrelsen
- Försäkringskassan
- RISE

- Sunet projektleder ett arbetspaket för interoperabilitet och utveckling

EWC

- Digg
- Vetenskapsrådet (Sunet)
- Finansiell ID-teknik AB
- Internetstiftelsen
- Bolagsverket
- Tink AB (Visa)
- LCubed AB (iGrant.io/MyData)
- Yubico

- Bolagsverket är koordinator för EWC

Finansieras av Europeiska unionen

EU Digital Identity Wallet

DC4EU

Utbildning

- Yrkeskvalifikationer
- Bevis på behörigheter; examensbevis, intyg
- Underlättar att ansöka om jobb och vidareutbildning

Sociala förmåner

- Ge tillgång till socialförsäkringsinformation
- Sociala förmåner som pension eller invaliditet
- Sjukförsäkringskortet

Utveckling

- OS-komponenter för utfärdare och förlitande part (verifiering)
- Interoperabilitetslab

Co-funded by the European Union

EU Digital Identity Wallet

Resor

- Boka
- På flygplatsen
- Boarding, checka in på hotell

Juridisk person

- Organisationer behöver också smidig identifiering
- Interoperabilitet
- Upphandlingar, fullmakter, avtal, rättigheter, över gränserna

Betalningar

- Något många gör dagligen
- Sverige en föregångare som visar övriga länder hur viktigt betalningar är för att uppmuntra användning av eID.

Co-funded by the European Union

Läs mer

- EU-kommissionens sidor om plånboken, piloterna, kod till referensimplementationen osv

Finansieras av Europeiska unionen

EU Digital Identity Wallet

Uppdrag att ta fram en eller flera digitala plånböcker inom ramen för EU:s storskaliga pilotprojekt

Nya betrodda tjänster eIDAS2

Björn Scharin och Anna Amundberg

Enheten för digitala och betrodda tjänster

2024-05-07

Agenda

- Introduktion om de nya betrodda tjänsterna
- Fördjupning om de enskilda betrodda tjänsterna
- Avslutar med att svara på frågor

Introduktion

Betrodd tjänst: en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av något av följande:

a) Utfärdande av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplar, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.

b) Validering av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplar, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.

c) Skapande av elektroniska underskrifter eller elektroniska stämplar.

d) Validering av elektroniska underskrifter eller elektroniska stämplar.

e) Bevarande av elektroniska underskrifter, elektroniska stämplar, certifikat för elektroniska underskrifter eller certifikat för elektroniska stämplar.

f) Förvaltning av anordningar för skapande av elektroniska underskrifter på distans eller anordningar för skapande av elektroniska stämplar på distans.

g) Utfärdande av elektroniska attributsintyg.

h) Validering av elektroniska attributsintyg.

i) Skapande av elektroniska tidsstämplingar.

j) Validering av elektroniska tidsstämplingar.

k) Tillhandahållande av elektroniska tjänster för rekommenderade leveranser.

l) Validering av data som överförs via elektroniska tjänster för rekommenderade leveranser och tillhörande bevis.

m) Elektronisk arkivering av elektroniska uppgifter och elektroniska dokument.

n) Registrering av elektroniska uppgifter i en elektronisk liggare.

Nya betrodda tjänster i eIDAS2

- Elektroniska attributsintyg
- Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans
- Förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans
- Elektronisk arkiveringstjänst
- Elektroniska liggare

Elektroniska attributsintyg

Elektroniska attributsintyg

- Ett intyg i elektronisk form som möjliggör autentisering av attribut.

Attributen kommer att användas tillsammans med plånboken och kan tillhandahållas som

- Elektroniskt attributsintyg (icke kvalificerat) (art. 45 g och h)
- Kvalificerat elektroniskt attributsintyg (krav i art. 45d och Bil. V)
- Elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa (krav i art. 45f, g, h och Bil. VII)

Medlemsstaterna ska möjliggöra kontroll av attributen mot autentiska källor (art 45 e och Bil. VI)

- ”Medlemsstaterna säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera äktheten hos följande attribut gentemot den relevanta autentiska källan på nationell nivå eller via särskilt utsedda mellanhänder som är erkända på nationell nivå, i enlighet med unionsrätten eller nationell rätt och i de fall då dessa attribut utgår från autentiska källor inom den offentliga sektorn:”

Attributen enligt bil.VI

- Adress.
- Ålder.
- Kön.
- Civilstånd.
- Familjesammansättning.
- Nationalitet eller medborgarskap.
- Utbildningskvalifikationer, titlar och licenser.
- Yrkeskvalifikationer, titlar och licenser.
- Befogenheter och uppdrag att företräda fysiska eller juridiska personer
- Offentliga tillstånd och licenser
- För juridiska personer, finansiella uppgifter och företagsuppgifter.”

Kvalificerad anordning för skapande av elektroniska underskrifter eller stämplar på distans (QSCD)

Vad är en sådan anordning?

- anordning för underskriftframställning: en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.
- kvalificerad anordning för underskriftframställning: en anordning för skapande av elektroniska underskrifter som uppfyller kraven i bilaga II.
- kvalificerad anordning för skapande av elektroniska underskrifter på distans: en kvalificerad anordning för skapande av elektroniska underskrifter som förvaltas av en kvalificerad tillhandahållare av betrodda tjänster i enlighet med artikel 29a för undertecknarens räkning. (artikel 39 a för stämplar)

Krav på QSCD:er

- Ska uppfylla kraven i art. 30, bil II med tillhörande genomförandebeslut (EU) 2016/650
- Certifierade enligt common criteria och någon av de i genomförandebeslutet utpekade skyddsprofilerna
- Listade i eIDAS dashboard dit certifierade QSCD:er ska notifieras

De nya tjänsterna förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans

- Tillhandahålla QSCD i enlighet med art. 29a eller 39a

a) genererar eller hanterar uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning,

b) trots punkt 1 d i bilaga II, kopierar uppgifterna för skapande av elektroniska underskrifter endast för framställning av säkerhetskopior, förutsatt att följande krav uppfylls:

i) Säkerheten för de kopierade datauppsättningarna måste vara på samma nivå som för de ursprungliga datauppsättningarna.

ii) Antalet kopierade datauppsättningar får inte överskrida det minsta antal som krävs för att säkerställa tjänstens kontinuitet.

c) uppfyller alla krav som anges i certifieringsrapporten för den specifika kvalificerade anordning för skapande av elektroniska underskrifter på distans som utfärdats i enlighet med artikel 30

Elektronisk arkiveringstjänst

Artikel 3.48
Elektronisk arkiveringstjänst

En tjänst som

- säkerställer mottagande, lagring, hämtning och radering av elektroniska uppgifter och elektroniska dokument i
- syfte att säkerställa deras hållbarhet och läsbarhet samt att bevara deras
- integritet, konfidentialitet och ursprungsbevis under hela bevarandeperioden.

Artikel 45i
Rättslig verkan av elektroniska arkiveringstjänster

1. Elektroniska uppgifter och elektroniska dokument som bevaras genom en elektronisk arkiveringstjänst **får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte är bevarade genom en kvalificerad elektronisk arkiveringstjänst**.

2. Elektroniska uppgifter och elektroniska dokument som bevaras genom en **kvalificerad** elektronisk arkiveringstjänst ska omfattas av en **presumtion om deras integritet** och ursprung under hela den period som de bevaras av den kvalificerade tillhandahållaren av betrodda tjänster.

Artikel 45j
Krav på kvalificerade elektroniska arkiveringstjänster

- Ska använda **förfaranden och teknik som kan säkerställa** att elektroniska uppgifter och elektroniska dokument **håller och är läsbara** även efter den tekniska giltighetstiden och åtminstone under hela den rättsliga eller avtalsenliga bevarandeperioden, samtidigt som deras **integritet och korrekta ursprung bibehålls**.
- De ska säkerställa att dessa elektroniska uppgifter och elektroniska dokument bevaras på ett sådant sätt att de **skyddas mot förlust och ändring**, med **undantag för ändringar som rör deras medium eller elektroniska format**.

Elektroniska liggare

Artikel 3.52
Elektronisk liggare

- En sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i dessa loggars kronologiska ordning.

Artikel 45l.1
Krav på kvalificerade elektroniska liggare

- Ska skapas och förvaltas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.
- Ska fastställa ursprunget till dataloggarna i liggaren.
- Ska säkerställa unik sekventiell kronologisk ordning för dataloggarna i liggaren.
- Ska registrera data på ett sådant sätt att alla senare ändringar av uppgifterna omedelbart kan upptäckas, varvid deras integritet säkerställs över tid.

Avslut

Nya betrodda tjänster

- Elektroniska attributsintyg
- Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans
- Förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans
- Elektronisk arkiveringstjänst
- Elektroniska liggare

Frågor?

E-post: eIDAS@pts.se

pts.se/eidas
pts.se/e-underskrift

PAUS

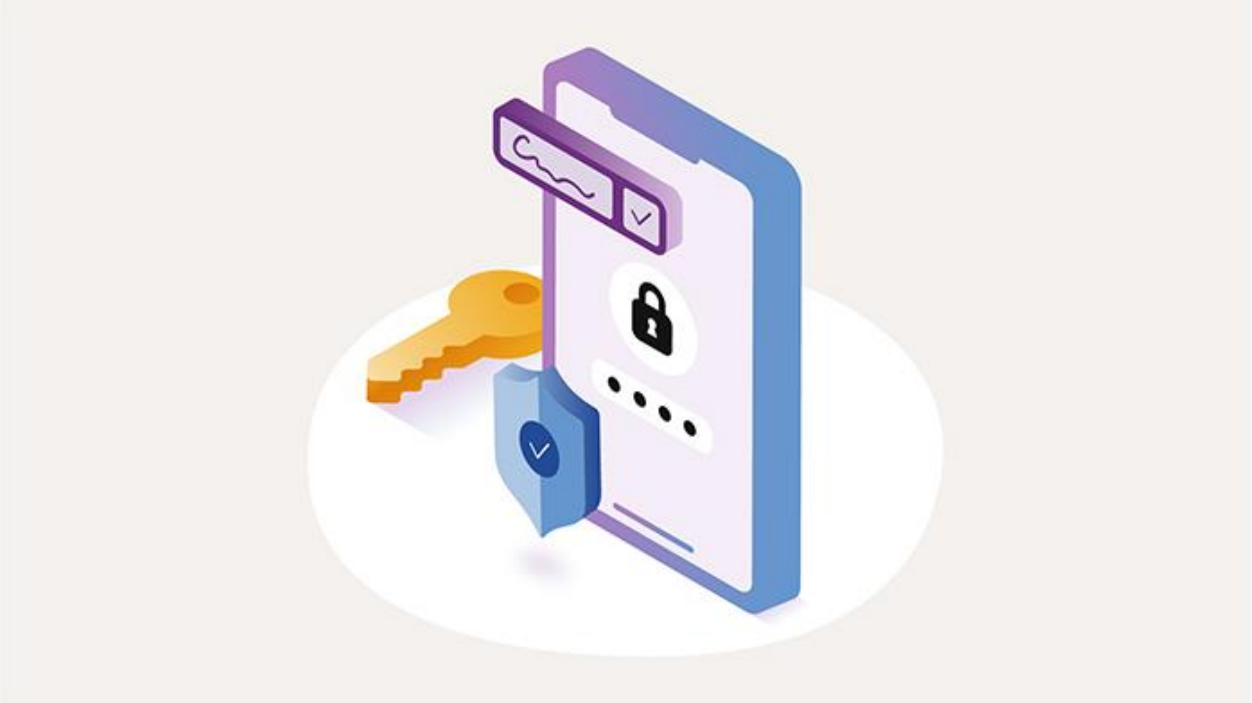
Hur påverkas ni som leverantörer av NIS2

7 maj 2024

Catherine Persson och Emma Wirf

Agenda

- Syftet med NIS2
- Nya krav och regler i NIS2 och eIDAS2
  - Väsentlig/viktig verksamhetsutövare
  - Anmälningsplikt
  - Riskhanteringsåtgärder
  - Incidentrapportering
  - Tillsyn
  - Sanktioner
  - Granskning kvalificerade tillhandahållare
- Vad händer framöver?



Syftet med NIS2 och varför betrodda tjänster omfattas

- NIS2 reglerar åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion
  - Hög harmoniseringsgrad p.g.a. gränsöverskridande karaktär
- Tillhandahållare av betrodda tjänster ska kunna dra nytta av den rättsliga ram som inrättats genom NIS2
  - Utnämning av en CSIRT-enhet med ansvar för risk- och incidenthantering
  - Deltagande av berörda behöriga myndigheter i samarbetsgruppens och CSIRT-nätverkets verksamhet
- NIS2 börjar tillämpas 18 oktober 2024
- Cybersäkerhetslagen (CSL) träder i kraft 1 januari 2025 enligt nuvarande förslag

Väsentliga och viktiga entiteter - storlekskrav

- Samtliga tillhandahållare av betrodda tjänster omfattas av NIS2 – oavsett storlek och även icke-kvalificerade tillhandahållare.
- Kvalificerade tillhandahållare utgör väsentliga verksamhetsutövare.
- Icke kvalificerade, storlekskravet avgör (om större än medelstort företag = väsentligt).
- Om ej väsentlig = viktig.

Väsentliga och viktiga entiteter – utses särskilt

- Finns en möjlighet att särskilt utse en entitet som väsentlig
- Kritiska entiteter enligt CER = väsentliga entiteter enligt NIS2

Anmälningsskyldighet

- Anmälningsskyldighet till PTS
- Icke-kvalificerade och kvalificerade ska anmäla sig enligt CSL/NIS2
- Anmälan senast 17 januari 2025
- Ändringar ska anmälas inom 14 dagar
- MSB föreslås få föreskriftsrätt om de uppgifter som ska lämnas
- Utebliven anmälan – sanktionsavgift kan meddelas
- Kvalificerade tillhandahållare anmäler sig även till PTS enligt eIDAS2

Riskhanteringsåtgärder eIDAS vs. NIS2/CSL

eIDAS, Artikel 19, Säkerhetskrav på tillhandahållare - utgår	3 kap 1-3 §§ CSL, Riskhanteringsåtgärder	eIDAS2, Artikel 19 a (TSPs) och artikel 24 p. 2 fa-fb (QTSPs)
Hantera riskerna för **säkerheten hos de betrodda tjänster** som de tillhandahåller.	**Säkerheten i nätverks- och informationssystem**, dvs smalare scope. Allriskansats.	Hantera rättsliga, affärsmässiga, operativa och **andra direkta eller indirekta risker** för tillhandahållandet av betrodda tjänster.
	Innehåller mer detaljerade krav än eIDAS. Genomförandeakter ska tas fram för QTSPs. PTS föreslås få föreskriftsrätt för vår sektor.	Endast eIDAS2 tom NIS2 implementeras. Genomförandeakter ska tas fram som pekar ut referensstandarder.

Riskhanteringsåtgärder eIDAS vs. NIS2/CSL

3 kap. CSL, Riskhanteringsåtgärder	eIDAS2, Artikel 19 a (TSPs) och artikel 24 p. 2 fa-fb (QTSPs)
1 § Verksamhetsutövaren ska vidta **tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder** för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande: 1. Incidenthantering, 2. kontinuitetshantering, 3. säkerhet i leveranskedjan, 4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation, 5. strategier och förfaranden för användning av kryptografi och kryptering, 6. personalsäkerhet, 7. strategier för åtkomstkontroll och tillgångsförvaltning, 8. säkrade lösningar för kommunikation, och 9. lösningar för autentisering. 2 §Systematiskt och riskbaserat informationssäkerhetsarbete. 3 §Utbildning för ledning och anställda.	Tillhandahållare ska ha lämpliga policyer och vidta motsvarande åtgärder för att hantera *rättsliga, affärsmässiga, operativa **och andra direkta eller indirekta risker** för tillhandahållandet* av betrodda tjänster, som trots artikel 21 i direktiv (EU) 2022/2555, ska innefatta åtminstone åtgärder avseende i) registrerings- och anslutningsförfaranden för en tjänst, ii) förfarandemässiga eller administrativa kontroller som krävs för att tillhandahålla betrodda tjänster, iii) förvaltning och genomförande av betrodda tjänster.
	Tillhandahållare ska vidta åtgärder för att hantera XXX ”och andra direkta eller indirekta risker”. Vi har tolkat detta brett. Alla säkerhetsåtgärder som gäller enligt nuvarande bestämmelser kommer att omfattas även av eIDAS2.

Incidentrapportering eIDAS vs. NIS2/CSL

NIS2/CSL	eIDAS2
Incidenter rapporteras till **CSIRT-enhet** eller behörig myndighet inom 24 h. **Slutrapport inom en månad.**	Incidentrapportering **till tillsynsorganet** (PTS) avseende art 19 a och 24 inom 24 h, dvs tillhandahållaren behöver rapportera till två myndigheter.
Verksamhetsutövare ska rapportera betydande incidenter. Med **betydande incident** avses 1. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller 2. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.	Alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de säkerhetsåtgärder som finns i eIDAS2 och som har en **betydande inverkan** på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri ska anmälas till tillsynsorganet.
Genomförandeakt får tas fram. Arbete pågår. MSB föreslås få föreskriftsrätt avs. incidentrapportering och begreppet betydande incident. .	Vi uppfattar att rapporteringskraven i eIDAS2 är samma som dagens. ECATS arbetar med att uppdatera vägledning.

Tillsyn eIDAS vs. NIS2/CSL

2, 4 & 5 kap CSL	eIDAS2
Endast händelsestyrd tillsyn över viktiga entiteter. Händelsestyrd och planerad tillsyn för väsentliga.	Händelsestyrd tillsyn av TSPs. Händelsestyrd och planerad tillsyn över QTSPs. TO eIDAS kan begära hjälp i bedömningen av TO NIS avseende art. 21.
Register över samtliga viktiga och väsentliga entiteter.	Även kraven i NIS2/CSL bedöms vid nyanmälan samt vartannat år.
Utökade befogenheter inkluderat sanktionsavgifter.	Nyhet med sanktionsavgifter.

Skillnader i tillsyn

Väsentliga entiteter kan tillsynas planerat och händelsestyrt. Kan (minst) underställas:

1. inspektioner på plats och distansbaserad tillsyn,
2. regelbundna och riktade säkerhetsrevisioner,
3. ad hoc-revisioner inkl. efter betydande incidenter eller vid överträdelse av detta direktiv,
4. säkerhetsskanningar,
5. begäranden om information,
6. begäranden om tillgång till uppgifter, handlingar och information och
7. begäranden om bevis på genomförandet av cybersäkerhetsstrategier.

Viktiga entiteter kan endast tillsynas händelsestyrt Kan (minst) underställas:

1. inspektioner på plats och distansbaserad tillsyn i efterhand,
2. riktade säkerhetsrevisioner,
3. säkerhetsskanningar,
4. begäranden om information,
5. begäranden om tillgång till uppgifter, handlingar och information och
6. begäranden om bevis på genomförandet av cybersäkerhetsstrategier.

Sanktioner eIDAS vs. NIS2/CSL

	CSL	eIDAS2
Icke-kvalificerade och kvalificerade tillhandahållare		Högst 5 000 000 EUR (fysisk/juridisk person) eller 1 % av den totala globala årsomsättningen (juridisk person).
Viktig	Högst 7 000 000 EUR eller högst 1,4 % av den totala globala årsomsättningen.	
Väsentlig	Högst 10 000 000 EUR eller högst 2 % av den totala globala årsomsättningen.	

Granskning av kvalificerade tillhandahållare

- I artikel 20 eIDAS2 införs att den granskning som kvalificerade tillhandahållare genomgår vid anmälan samt vartannat år ska bekräfta att kraven i såväl eIDAS som artikel 21 i NIS2 uppfylls.
- Tillsynsorganet enligt eIDAS och nationell behörig myndighet enligt NIS2 föreslås samarbeta och bistå varandra.
- Genomförandeakter ska precisera förfarandemässiga arrangemangen för att främja samarbete mellan TO.

Vad händer framöver?

- Utredningen om säker och tillgänglig identitet (Dir 2022:142).
- Genomförandeakter NIS2 - riskhanteringsåtgärder och incidentrapportering.
- Ca 50 genomförandeakter – eIDAS2.
- ECATS vägledning incidentrapportering.
- Nyhetsbrev och kommande forum/webinarium.

Tack för oss!

E-post: eIDAS@pts.se

pts.se/eidas
pts.se/e-underskrift

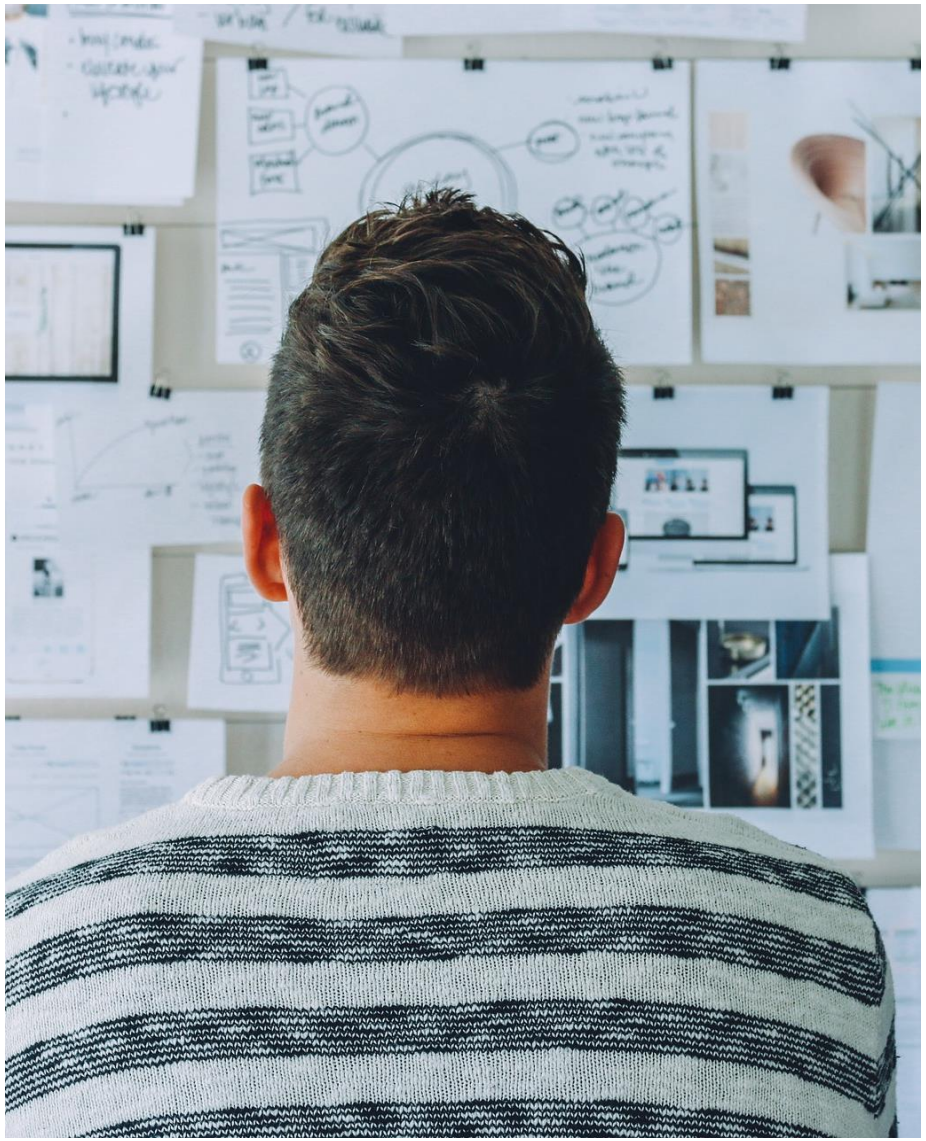
Öppen frågestund

PTS

DIGG MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Föranmälda frågor

- Nya tillkommande icke kvalificerade tjänster som exempelvis arkivtjänster. Hur kommer efterlevnad av eIDAS att följas upp innan det finns standarder för dessa tjänster?




Tack för ert deltagande!
PTS
DIGG
MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government