

Virksomhetslommebok

Norstella 17.september 2026



Fakta om Buypass



Blant Norges største fagmiljøer innen sikkerhet og ID

Fordelt i Oslo og på Gjøvik sitter et sterkt team av utviklere og sikkerhetsekspert med spesialkompetanse innenfor eID og tillitstjenester



Tungt sertifisert nasjonalt og internasjonalt

Sertifisert ihht ISO 27001/9001, PCI-DSS og europeisk ETSI-sertifisering som inkluderer eIDAS tillitstjenester. QTSP under eIDAS-forordningen.



Norsk, 60 medarbeidere, etablert i 2001, eid av Total Specific Solutions (TSS)

Vi muliggjør effektiv og bærekraftig digitalisering ved å levere brukervennlige og trygge ID-, e-signatur og betalingsløsninger



Virksomhetslommebok

Kort introduksjon

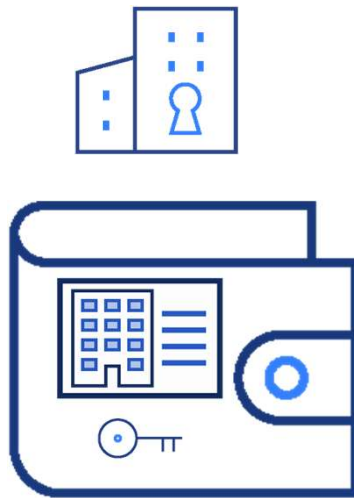
Virksomhetslommebok



- Forslag til ny EU-forordning publisert november 2025
- Bygger på eIDAS 2.0 og skal sameksistere med identitetslommeboken innenfor samme økosystem
- Tilby «lommebøker» til virksomheter under et enklere regelverk enn identitetslommeboken

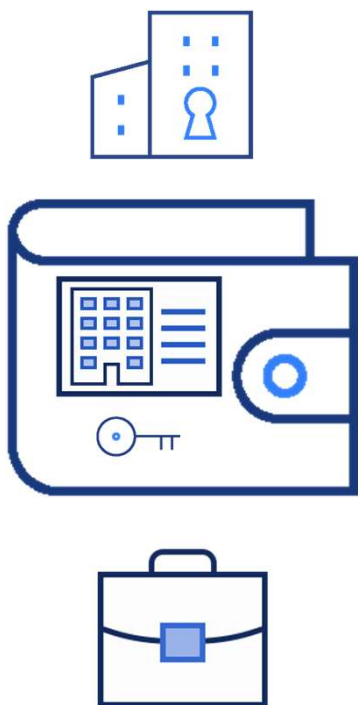
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0838>

Virksomhetslommebok - formål



- *‘European Business Wallet purposes:’*
 - to **authenticate** and provide the **verified proofs** required by a relying party;
 - to access and use **electronic attestations of attributes, electronic signatures, electronic seals, electronic registered delivery services, and electronic time stamps;**
 - to enable the creation, management and delegation of mandates to **authorised representatives;**

Virksomhetslommebok



- Utstedes til virksomheter
- Identifisering/autentisering av virksomheten i kommunikasjon med andre aktører
- «Dokumentmappe» med støtte for innhenting og deling av relevante dokumenter
 - Elektronisk attesterte attributter (EAA)
- Teknisk administrasjon av roller og rettigheter
- Støtte for elektronisk segl
- Utveksling av dokumenter via kvalifisert elektronisk tjeneste for registrert sending (QERDS)



Identifisering av virksomhet

- En virksomhet identifiseres (minst) med virksomhetens offisielle navn og **en unik identifikator**
 - *European Unique Identifier* i hht Directive 2017/1132
 - Også omtalt som *European Business Wallet Organization Identifier (EBWOID)*
 - For norske virksomheter vil identifikatoren være basert på organisasjonsnummeret i Brønnøysundregistrene
- Virksomhetens identitet skal være registrert som bevis i form av a) QEAA utstedt av en QTSP eller b) PUB_EAA utstedt av en offentlig myndighet
- Dette er en sentral del av tilliten til virksomhetslommeboken

Kjernefunksjoner



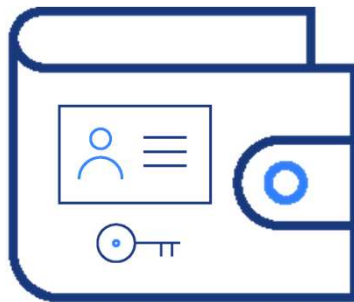
(virksomhetsinformasjon, attester, lisenser, sertifiseringer mm)



To lommebøker – ett økosystem

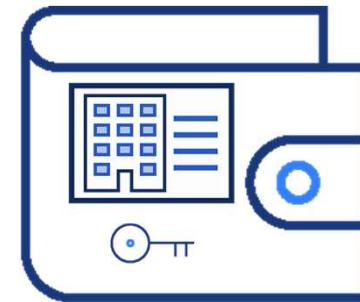
• Identitetslommebok

- For privatpersoner
- eID på sikkerhetsnivå Høyt
- App på smarttelefon
- Tilgang til kvalifisert elektronisk signatur
- Lagre og dele dokumenter og bevis
- Sertifisert løsning



• Virksomhetslommebok

- For virksomheter
- eID på sikkerhetsnivå Betydelig
- Skybasert tjeneste
- Tilgang til kvalifisert elektronisk segl
- Lagre og dele dokumenter
 - Dokumentmappe, distribusjon via QERDS
- «Notifisert» løsning



Virksomhetslommebok

Bruk av andre tillitstjenester

Kvalifisert elektronisk segl

- Hentet fra dokument vi har fått fra en offentlig myndighet



- En slik kommentar er i prinsippet verdiløst for å bevise at dokumentet er autentisk og ikke endret
- Her kan et (kvalifisert) elektronisk segl med fordel brukes
- Med tilgang til slik funksjonalitet fra en virksomhetslommebok kan vi enkelt øke tilliten til slike dokumenter
- Kommer også som krav fra andre regulerte områder
 - For eksempel Digital Product Passport (DPP) Register

Kvalifisert elektronisk signatur

- Forslaget krever at virksomhetslommeboken skal kunne brukes for å generere en kvalifisert elektronisk signatur
 - For eksempel ved at en autorisert representant signerer elektronisk på vegne av virksomheten
- Virksomhetslommeboken i seg selv vil ikke kunne brukes direkte for dette formålet
- Men dersom den autoriserte representanten bruker sin identitetslommebok eller en annen eID på sikkerhetsnivå Høyt vil dette kunne være en god løsning

Kvalifisert elektronisk tidsstempel

- Virksomhetslommeboken skal kunne knytte et kvalifisert elektronisk tidsstempel til ulike data for å sikre at disse er merket med et korrekt og pålitelig tidspunkt
- Dette kan brukes på data som utveksles med andre virksomheter eller offentlige myndigheter som en garanti for at disse er generert i hht relevant regelverk (for eksempel innenfor definerte tidsfrister)

Kvalifisert leveringstjeneste

- En kvalifisert elektronisk tjeneste for registrert sending (QERDS) vil gi garanti for levering av digitale forsendelser
- Tjenesten støtter også kryptering, noe som kan benyttes for ende-til-ende kryptering av meldinger
 - Virksomhetssertifikater har vært brukt for tilsvarende funksjoner i helsesektoren (ref Adresseregisteret) og finanssektoren (ref CertPub) i flere år
- Et nytt europeisk register over virksomhetslommebøker kan brukes for å slå opp den digitale adressen til mottakeren av meldingen
 - Dokumenter kan deretter sendes til denne adressen med bruk av QERDS, eventuelt kryptert

eIDAS 2.0 tillitstjenester

- En rekke nye tillitstjenester som er en del av det nye økosystemet rundt eIDAS 2.0 skal også støttes av virksomhetslommeboken
 - Utstedelse av kvalifiserte attesterte attributter (QEAA)
 - Utstedelse av offentlige attesterte attributter (PUB_EAA)
 - Utstedelse av attesterte attributter (EAA)
- Virksomhetslommeboken skal kunne operere innenfor økosystemet som er definert rundt identitetslommeboka
 - Mer detaljer vil bli bedre definert i gjennomføringsrettsakter, ARF-en og andre standarder når den endelige reguleringen foreligger

Virksomhetslommebok

Tillitsbasert KI

Tillitsbasert KI - kilder

European Business Wallets as the Legal Control Plane for Zero Trust AI Agents

An action and policy whitepaper on trusted AI and the role of business wallets for AI
adoption in regulated industries

Dr. Carsten Stöcker
CEO, Spherity GmbH
carsten.stoecker@spherity.com

1 June 2026

*Prepared for EU policy makers, the European Business Wallet workstream, the EU AI Office, cyber agencies,
national digitalisation authorities, frontier AI platforms, and regulated industrial buyers*

Zero Trust for AI Agents

A security framework for deploying
autonomous AI agents in the enterprise.

 Claude



Generert med bruk av KI

Fra «hvem er brukeren» til «hvem er ansvarlig»

- Autonome AI-agenter tolker mål, velger verktøy og samhandler med andre agenter
- Endrer sikkerhetsspørsmålet: fra «har brukeren tilgang?» til «har agenten fullmakt til å handle på vegne av en juridisk person?»
- Kjøretidssikkerhet kan begrense teknisk skade — den kan ikke skape juridisk myndighet



Teknisk Zero Trust svarer ikke på det juridiske spørsmålet

- Kryptografisk agent-ID beviser at en arbeidslast eksisterer — ikke hvem som er juridisk ansvarlig
- Én autentisert sesjon kan romme mange handlinger med ulik juridisk betydning
- Et loggført verktøykall viser hva som skjedde — ikke om det lå innenfor et gyldig mandat
 - *Utgangspunkt for analysen: Anthropic's rammeverk «Zero Trust for AI Agents» (2026)*



Anthropics modenhetsmodell – og gapet som gjenstår

Foundation

Kryptografiske ID-er per agent, kortlevde autentiseringsbevis, deny-by-default-tilgang.

Enterprise

Sertifikatlivssyklus, mTLS, sandboxing, sporbare revisjonsspor på tvers av tjenester.

Advanced

Maskinvarebundet identitet, kontinuerlig autorisasjon per handling, full proveniens, drift-deteksjon.

Selv på Advanced-nivå gjenstår ett gap: å bevise juridisk myndighet på tvers av selskapsgrenser.



Generert med bruk av KI

Digitale mandater: fullmakt for agenter, ikke bare mennesker

- Samme byggeklosser som identifiserer virksomheten i dag — EBVOID/EUID, attesteringer, roller og rettigheter — gir nå fullmakt til en AI-agent.
- Mandatet fastsetter hvem som delegerer, hvilke handlinger og ressurser som er tillatt.
- Formål, tidsvindu og geografisk/juridisk domene inngår i mandatet.
- Delegeringsdybde og eskaleringsregler er eksplisitte.
- En tydelig tilbakekallingsmekanisme er alltid del av mandatet.



Prinsippet: minste nødvendige fullmakt. En agent arver aldri full selskapsmyndighet — kun det mandatet som eksplisitt er gitt.



Autorisasjon per handling — ikke per sesjon

En sesjon kan romme mange handlinger med ulik juridisk betydning. Hver regulert handling bør derfor følges av en egen autorisasjonsartefakt som binder sammen:



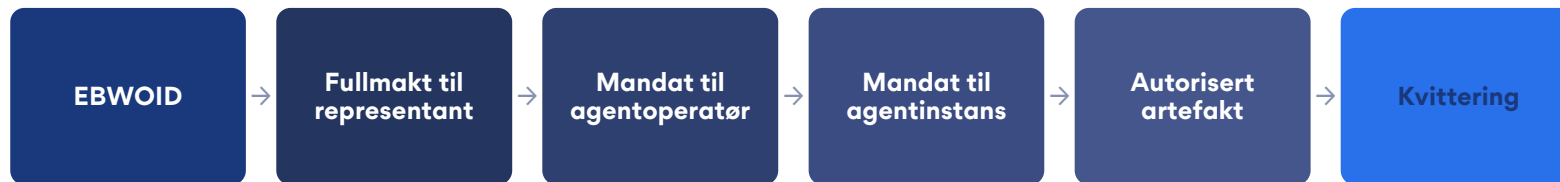
Resultatet er en signert kvittering («action receipt») som kan etterprøves av revisor, tilsyn eller domstol.



Generert med bruk av KI

Bevissikker delegering på tvers av agenter

En agent med høy tillit kan bli lurt til å bruke sin myndighet på vegne av en agent med lavere tillit («confused deputy»). Løsningen: en kjede der hvert ledd kun kan innskrenke — aldri utvide — myndighet.



Hvert ledd inneholder en hash av forrige ledd, tillatt omfang, ferskhetsregel og tilbakekallingsreferanse. Effektiv myndighet er alltid snittet av alle overordnede fullmakter.



AI-forordningen og AI Service Passport

AI-forordningens krav

- Risikostyring for høyrisiko AI-systemer
- Teknisk dokumentasjon og loggføring
- Åpenhet overfor tilbydere og brukere
- Menneskelig tilsyn ved høy risiko
- Nøyaktighet, robusthet og cybersikkerhet



AI Service Passport (AISP)

Et verifiserbart «pass» for AI-tjenesten: modellversjon, verktøysett, TEVV-bevis, driftskontroller og risikostatus knyttet til hver autorisasjonsbeslutning.

Uten gyldig AISP-status kan en handling avvises eller eskaleres automatisk.



Europas mulighet: tillitsinfrastruktur, ikke bare modellkapasitet

Det globale AI-kappløpet handler ofte om modellstørrelse, beregningskraft og data. Men B2B- og B2G-virksomheter tar ikke autonome agenter inn i kjerneprosesser før ansvar, revisjon og tilgangskontroll kan styres.

Web-PKI

autentiserer domener og endepunkter

Bedrifts-IAM

autentiserer brukere, arbeidslaster og leietakere

EBW

autentiserer juridiske personer, mandater og myndighet — på tvers av landegrenser



Generert med bruk av KI

Fra pilot til høy-sikkerhet: modenhetstrinn



Hovedpoenger å ta med seg

- Autonome agenter trenger et juridisk tillitslag i tillegg til det tekniske Zero Trust-laget
- EBW kan levere juridisk identitet, mandat, tillit og tilbakekalling på tvers av selskaps- og landegrenser
- Nøkkelmekanismen er autorisasjon per handling, med en sporbar bevis- og mandatkjede
- Dette kobler naturlig til AI-forordningen og gir regulerte bransjer en vei fra pilot til produksjon
 - *Foreløpig et policyutkast under forhandling — arkitekturen er infrastruktur- og protokollnøytral*



Sist, men ikke minst

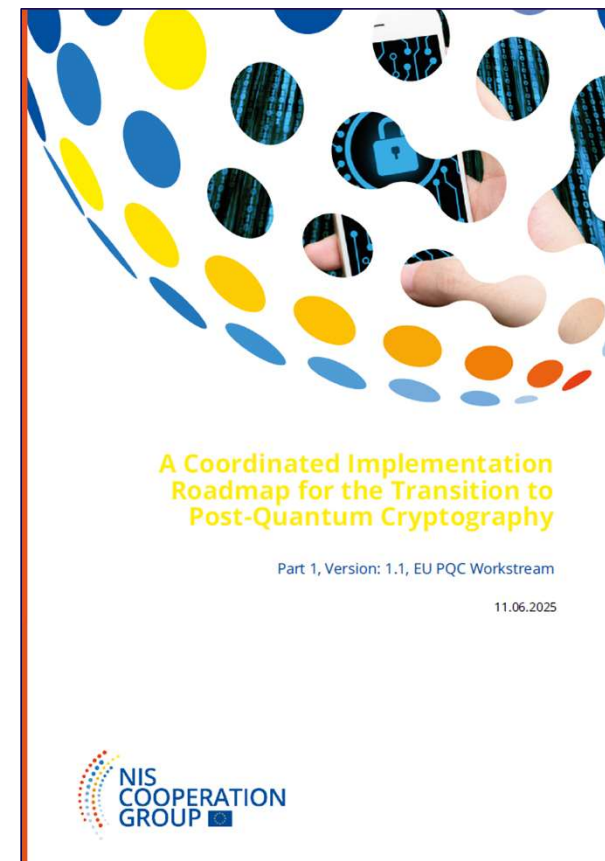
Planlegg for kvantesikker kryptografi

EU kommisjonen med roadmap



The screenshot shows the European Commission website with the headline "Shaping Europe's digital future". The navigation bar includes links for Home, Policies, Activities, News, Library, Funding, Calendar, Consultations, and AI Office. The main content area is titled "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography" under the "POLICY AND LEGISLATION" section, dated 23 June 2025. The text explains that the EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC). It also mentions that quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. The document is the first deliverable of a work stream on PQC with the NIS Cooperation Group, aimed at Member States, and includes a set of recommendations that Member States need to implement for a synchronised transition to PQC.

- DORA, NIS2, eIDAS, CRA etc



EU Roadmap for PQC

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Part 1, Version: 1.1, EU PQC Workstream

11.06.2025



Timeline for the transition to PQC

1. By 31.12.2026:
 - At least the *First Steps* have been implemented by all Member States.
 - Initial national PQC transition roadmaps have been established by all Member States.
 - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By 31.12.2030:
 - The *Next Steps* have been implemented by all Member States.
 - The PQC transition for high-risk use cases has been completed.
 - PQC transition planning and pilots for medium-risk use cases have been completed.
 - Quantum-safe software and firmware upgrades are enabled by default.
3. By 31.12.2035:
 - The PQC transition for medium-risk use cases has been completed.
 - The PQC transition for low-risk use cases has been completed as much as feasible.

Milestone 1: 31.12.2026

- **First Steps:**
 - Identify and involve stakeholders.
 - Support mature cryptographic asset management.
 - Create dependency maps.
 - Perform quantum risk analysis.
 - Include the supply chain.
 - Create a national awareness and communication program.
 - Share knowledge and get involved with the NIS CG work stream on PQC.
 - Develop a timeline and an implementation plan.
- **Main achievements:**
 - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
 - Initial national PQC transition roadmaps have been established by all Member States.

Milestone 2: 31.12.2030

- **Next Steps:**
 - Support cryptographic agility and a quantum-safe upgrade path.
 - Allocate resources for the transition.
 - Adapt certification schemes.
 - Evolve the rules.
 - Look for opportunities within the ecosystem.
 - Considering transversal activities throughout the creation and implementation of the roadmap.
 - Implement pilot use cases and contribute to testing centres.
- **Main achievements:**
 - The PQC transition for high-risk use cases has been completed.
 - PQC transition planning and pilots for medium-risk use cases has been completed.
 - Quantum-safe software and firmware upgrades are enabled by default.

Kvantesikker kryptografi

- En virksomhetslommebok som skal realiseres innen 2030, bør være forberedt for kvantesikker kryptografi
- En hybrid tilnærming med støtte for både klassisk og kvantesikker kryptografi kan være hensiktsmessig
- Man bør følge med på gjeldende anbefalinger innenfor området, det forventes å komme mer eksplisitte krav om dette i løpet i nær fremtid

