Impact Report
eIDAS 2

Versie 1.0 | November 2025

Davinci
CONCLUSION

Voorwoord

Enkele jaren geleden sprak Ursula von der Leyen in haar State of the Union de ambitie uit dat iedere Europese burger en onderneming zou beschikken over een eigen digitale identiteit. Een identiteit waarmee je eenvoudig, veilig en onder eigen regie digitale transacties kunt uitvoeren en persoonlijke gegevens kunt delen. Die ambitie krijgt nu concreet vorm.

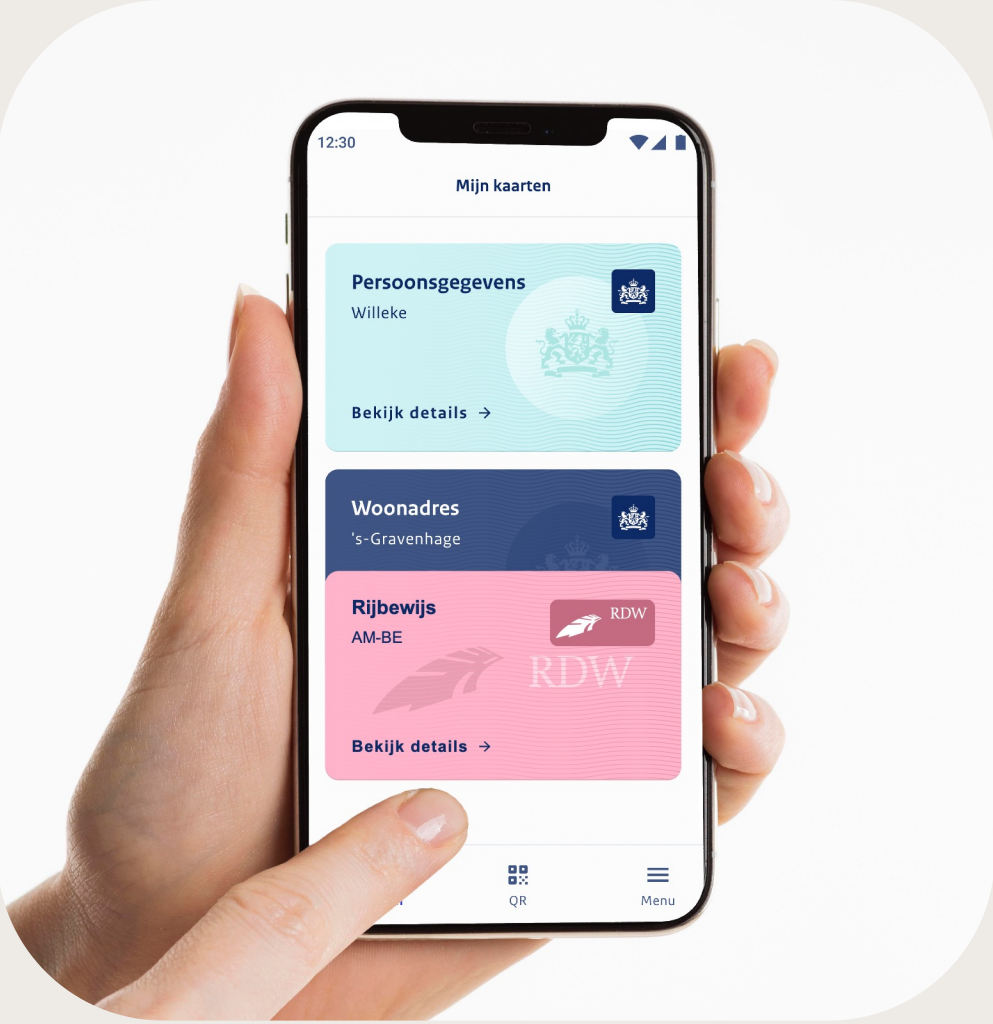
Met de inwerkingtreding van eIDAS 2 (EU 2024/1183) ontstaat een juridisch en technisch fundament voor de Europese Digitale Identiteitswallet (EUDI Wallet). Vanaf november 2026 moet iedere lidstaat minimaal één digitale wallet beschikbaar stellen. Een jaar later, in november 2027, zijn bedrijven en publieke instellingen in tal van sectoren verplicht om deze wallets te accepteren.

Voor publieke instellingen en bedrijven betekent dit een fundamentele verandering. Niet alleen in hoe klanten zich identificeren of transacties uitvoeren, maar ook in hoe u zich kunt positioneren in nieuwe digitale ketens en ecosystemen. Wie eIDAS 2 slim benut, kan sneller klanten onboarden, operationele kosten verlagen en nieuwe proposities ontwikkelen. Maar wie wacht, loopt het risico op complianceproblemen, reputatieschade en concurrenten die de markt betreden met innovatieve oplossingen.

In dit rapport bieden wij u een overzicht van de impact van eIDAS 2 per bedrijfsfunctie. Met als doel: u inzicht geven in waar de grootste kansen én risico’s liggen voor uw organisatie - zowel publiek als privaat - en hoe u zich hierop kunt voorbereiden.

Wij nodigen u uit om dit rapport te gebruiken als startpunt voor strategische keuzes.

eIDAS 2



- Digitale identiteit
- Digitale handtekening
- Gewaarmerkte brongegevens
- EU Identity Wallet

Verplichtingen
voor sectoren

- Transport
- Gezondheidszorg
- Onderwijs
- Nutsvoorzieningen
- Overheid
- Postdiensten
- Financiële dienstverlening
- Digitale infrastructuur
- Sociale zekerheid
- Telecommunicatie

eIDAS *impact*

- Technology
- Information
- Operations
- Human Resources
- Risk & Compliance
- Strategy
- Commercial

IMPACT

Technology

Technology (1/2)

De herziene eIDAS-verordening (2024/1183) heeft grote impact op de IT-architectuur en roadmap. Als CTO krijgt u te maken met nieuwe verplichtingen én kansen:

Digitale wallet-integratie in kernprocessen

Vanaf 2026 moeten alle lidstaten minimaal één wallet aanbieden die door instellingen uit de aangewezen sectoren verplicht geaccepteerd moet worden. Dat raakt processen rond onboarding, identificatie en authenticatie en klantcommunicatie. Integratie vereist aanpassingen in zowel frontend als back-end systemen.

Samenwerking met Trust Service Providers (TSP's)

Er zal intensieve samenwerking nodig zijn met gecertificeerde partijen die gekwalificeerde handtekeningen, seals en attestaties leveren. Belangrijke aandachtspunten zijn daarbij de continuïteit in dienstverlening, integratie in IT-beheerprocessen en het opdoen van voldoende kennis om dergelijke diensten correct te integreren.

Interoperabiliteit en standaardisatie cruciaal

Uw systemen moeten kunnen koppelen met een nog onbekend aantal Europese wallets en meerdere vertrouwensdiensten. Dat vraagt om flexibile architecturen, standaardisatie in data(modellen) en een robuuste IT-landschap. Dit voorkomt vendor lock-in en faciliteert snelle adoptie van nieuwe nieuwe middelen die ter beschikking komen.

Compliance en ketenintegriteit

Met het toevoegen van nieuwe, externe, services aan het IT-landschap groeit de complexiteit en afhankelijkheid. Effectief en efficiënt regie voeren is hierbij essentieel, evenals het inzichtelijk maken en houden van integriteit en compliancy van de gehele keten.

Technology (2/2)

De herziene eIDAS-verordening (2024/1183) heeft grote impact op de IT-architectuur en roadmap. Als CTO krijgt u te maken met nieuwe verplichtingen én kansen:

Langetermijn archivering

Digitale documenten met gekwalificeerde handtekeningen of zegels moeten integer en raadpleegbaar blijven, ook over tientallen jaren. Dit vraagt om de mogelijke vervanging of aanpassing van bestaande oplossingen, (veranderende) eisen aan processen.

Digitale onboarding personen én bedrijven

eIDAS verplicht instellingen om zowel personen als bedrijven digitaal te identificeren. Dit vergt naast integratie ook een herziening van achterliggende processen, user interfaces en logging en archivering. Daarvoor is samenwerking tussen de business als Legal en Compliance een absolute must.

Datadistributie als strategische kans

Deze veranderingen biedt de mogelijkheid om als organisatie attestaties van gegevens uit te geven. Gegevens die op gekwalificeerd niveau, bij wet gelijkgesteld zijn aan het papieren equivalent. Dit leidt tot kansen en uitdagingen op gebied van data governance, distributiemechanismen en business modellen. IT is hierbij de enabler voor Commercial en Strategy.

IMPACT

Operations

Operations (1/2)

De invoering van de Europese Digitale Identiteitswallet verandert fundamenteel hoe bedrijven en overheden klantprocessen inrichten. Voor de COO biedt dit zowel operationele voordelen als structurele uitdagingen:

Efficiëntere dienstverlening

Dankzij de Wallet kunnen klanten uit alle EU-lidstaten zich digitaal identificeren. Dit verkort de onboardingstijd aanzienlijk en maakt digitale, automatische verificatie van essentiële gegevens mogelijk. De COO kan workflows stroomlijnen, wat leidt tot hogere kwaliteit, lagere operationele kosten en een soepeler klantproces.

Laagdrempelige centralisatie

De Wallet introduceert uniforme standaarden waarmee klantidentificatie en -authenticatie in alle EU-lidstaten op dezelfde wijze kan plaatsvinden. Dit biedt een unieke kans om grensoverschrijdende processen te harmoniseren, schaalvoordelen te behalen en operations te centraliseren. Voor de COO betekent dit een reductie van complexiteit en hogere operationele efficiëntie.

KYC-processen automatiseren

Door gebruik te maken van gevalideerde digitale identiteiten en attestaties uit betrouwbare bronnen kan Know Your Customer (KYC) sneller en consistenter plaatsvinden. Dit reduceert foutkansen en vereenvoudigt compliance, terwijl het operationele werk voor medewerkers aanzienlijk afneemt. De COO kan hierdoor resources vrijspelen en compliance-risico’s beperken.

Afname afhankelijkheid externe bronnen

Waar voorheen externe partijen nodig waren om identiteits- of bevoegdheidschecks uit te voeren, biedt eIDAS 2 nu attestaties uit authentieke, digitale bronnen. Dit vermindert kosten, verkort processen en verkleint de afhankelijkheid van derde partijen. Tegelijk ontstaan nieuwe uitdagingen rond integratie en governance van deze digitale gegevensstromen.

Operations (2/2)

De invoering van de Europese Digitale Identiteitswallet verandert fundamenteel hoe bedrijven en overheden klantprocessen inrichten. Voor de COO biedt dit zowel operationele voordelen als structurele uitdagingen:

Versnelling van dienstverleningsprocessen

Met digitale identiteiten kunnen klanten sneller zelf acties uitvoeren, zoals documenten ondertekenen of rechten aantonen, waardoor doorlooptijden bij aanvragen of transacties aanzienlijk korter worden. Dit verhoogt de klanttevredenheid én vergroot de capaciteit van operationele teams. Voor de COO ligt hier een kans om processen opnieuw te ontwerpen met snelheid als uitgangspunt.

Beheersing van operationele risico's

Hoewel digitale identiteiten veel huidige risico's reduceren, ontstaan er nieuwe afhankelijkheden, zoals uitval van digitale services of verschillen in implementatie per lidstaat. De COO moet daarom investeren in robuuste fallbackscenario's en monitoringmechanismen om continuïteit te waarborgen. Het risicoprofiel verschuift, maar blijft significant.

Ketensamenwerking voor ultieme klantreis

eIDAS 2 opent de deur voor intensieve samenwerking met partners om samen één naadloze klantreis vorm te geven. Dit vraagt om goed afgestemde processen, gezamenlijke standaarden en heldere afspraken over rollen en verantwoordelijkheden. De COO speelt hierin een sleutelrol om de operationele uitvoering van deze ecosystemen effectief te organiseren.

IMPACT

Risk & Compliance

Risk & Compliance (1/2)

De introductie van eIDAS 2 verandert risicobeheersing rondom digitale identificatie en authenticatie. Tegelijk ontstaan nieuwe ecosysteemrisico's, afhankelijkheden en compliance-uitdagingen. Een aantal belangrijke aandachtspunten zijn:

Veiligere digitale identificatie

De Wallet en inzet van vertrouwensdiensten verhogen de zekerheid over wie een klant is en welke bevoegdheden hij heeft, waardoor traditionele fraude- en identiteitsrisico's significant afnemen. Dit versterkt de fundamenten onder risicomodellen en Customer Due Dilligence-processen – mits goed uitgevoerd, want digitale onboarding en wallets brengen nieuwe risico's met zich mee.

Risico-gestuurd gebruik van attestaties

Het gebruik van digitale attestaties uit authentieke bronnen ondersteunt risicobeheersing in onboarding, dienstverlening en monitoring – door besluiten te baseren op objectieve, integere brondata. Dit vraagt om een herijking van interne risicomodellen waarbij herkomst, kwaliteit en juridische waarde van deze bronnen nieuwe factoren worden. Voor de CRO biedt dit kansen, maar ook noodzaak tot scherpe integratie in beleid en processen.

Dataminimalisatie

eIDAS 2 biedt invulling aan dataminimalisatie, waardoor bedrijven alleen die gegevens mogen opvragen en verwerken die strikt noodzakelijk zijn. Dit verlaagt privacyrisico's en vergemakkelijkt aantoonbare compliance, maar vereist ook dat risicomodellen en procedures opnieuw worden afgestemd op beperkte datasets. De CRO moet ervoor zorgen dat dit niet leidt tot informatiegaten in risicobeoordelingen.

Nieuwe ecosysteemrisico's

Met eIDAS verschuift risicobeheersing deels naar externe partijen zoals walletproviders en Trust Service Providers (TSP's), waardoor nieuwe ketenrisico's ontstaan met impact op compliance en dienstverlening. Incidenten daar kunnen klantprocessen verstoren of leiden tot juridische aansprakelijkheid. Voor de CRO betekent dit dat risicomanagement ook de externe keten moet omvatten, met duidelijke afspraken en monitoring.

Risk & Compliance (2/2)

De introductie van eIDAS 2 verandert risicobeheersing rondom digitale identificatie en authenticatie. Tegelijk ontstaan nieuwe ecosysteemrisico's, afhankelijkheden en compliance-uitdagingen. Een aantal belangrijke aandachtspunten zijn:

Compliance en ketenintegriteit

Nieuwe digitale processen moeten vanaf de start voldoen aan eIDAS, GDPR, NIS2 en sectorale regels zoals DORA, waarbij de verantwoordelijkheid voor compliance niet ophoudt bij de eigen organisatiegrenzen. Dit vereist nauwe samenwerking tussen risk, legal, technology en operations, én robuuste audittrails die bewijs leveren van juiste procesvoering. De CRO moet hier als regisseur optreden om alle partijen op één lijn te krijgen.

Verhoogde complexiteit in implementatie

Onduidelijke tijdslijnen voor uitvoeringswetgeving en uiteenlopende interpretaties per lidstaat vergroten de complexiteit en onzekerheid bij de implementatie van eIDAS 2. Dit kan leiden tot compliance-risico's of vertragingen die directe impact hebben op klantprocessen. De CRO moet scenario's ontwikkelen voor non-compliance of operationele verstoringen door externe factoren.

Ketenmonitoring en signalering

Met de groeiende afhankelijkheid van externe partijen is het cruciaal om continu zicht te houden op de prestaties, compliance en incidenten binnen de keten. Moderne risk teams zullen datagedreven monitoring en alerts moeten implementeren om snel in te grijpen bij afwijkingen. Voor de CRO wordt ketenmonitoring een strategisch speerpunt om integriteits- en continuïteitsrisico's vroegtijdig te signaleren.

IMPACT

Commercial

Commercial (1/2)

eIDAS 2 verandert niet alleen de manier waarop klanten zich identificeren en transacties uitvoeren, maar opent ook de deur naar snellere onboarding, grensoverschrijdende dienstverlening en geheel nieuwe proposities. Voor de Chief Commercial Officer betekent dit:

Betere ervaring in digitale klantreis

Met digitale identiteiten kunnen klanten zich sneller en eenvoudiger identificeren en transacties afronden, wat leidt tot minder frictie en een hogere conversie. Dit verkort processen zoals onboarding, productaanvragen of digitale handtekeningen aanzienlijk. Voor de CCO biedt dit een kans om klantervaring en concurrentiepositie tegelijkertijd te verbeteren.

Nieuwe proposities op basis van attestaties

eIDAS 2 maakt het mogelijk om als bank zelf digitale attestaties uit te geven, bijvoorbeeld over bezittingen, producten of digitale machtigingen. Dit opent deuren naar nieuwe commerciële diensten en trusted solutions waarmee instellingen zich kunnen onderscheiden. De CCO moet bepalen welke attestaties commerciële waarde toevoegen en hoe die slim gepositioneerd kunnen worden.

Toegang tot nieuwe markten en diensten

Uniforme Europese standaarden maken het eenvoudiger om digitale producten en diensten grensoverschrijdend aan te bieden zonder per land aparte verificatie-infrastructuur op te bouwen. Dit verlaagt de drempel voor markttoetreding en versnelt groei. De CCO kan hierdoor internationale expansie realiseren en nieuwe klantgroepen bedienen.

Partnerschappen voor trusted services

Samenwerking met gekwalificeerde vertrouwensdienstverleners (QTSP’s) biedt instellingen de mogelijkheid om white-label of embedded trusted services aan te bieden, bijvoorbeeld in platformen van partners of bij zakelijke klanten. Dit creëert nieuwe commerciële kansen en distributiekanalen. De uitdaging voor de CCO ligt in het slim regisseren van partnerships en (her)ontwikkelen van business modellen.

Commercial (2/2)

eIDAS 2 verandert niet alleen de manier waarop klanten zich identificeren en transacties uitvoeren, maar opent ook de deur naar snellere onboarding, grensoverschrijdende dienstverlening en geheel nieuwe proposities. Voor de Chief Commercial Officer betekent dit:

Positionering binnen ecosystemen

eIDAS 2 maakt het mogelijk om als onderneming een leidende rol te spelen in ecosystemen en sectoren, bijvoorbeeld als Orchestrator of Trusted Hub. Door de regierol te pakken, kan een instelling zich onderscheiden én nieuwe inkomstenstromen aanboren. Voor de CCO is het cruciaal om deze positie te definiëren, en de organisatie daarop in te richten.

Dataminimalisatie versus klantinzicht

Hoewel dataminimalisatie verplicht wordt onder eIDAS, blijft het essentieel om voldoende klantinzicht te behouden voor gepersonaliseerde dienstverlening en risicobeoordeling. Dit vraagt om slimme ontwerpen van klantreizen waarbij alleen strikt noodzakelijke gegevens worden gebruikt, zonder commerciële slagkracht te verliezen. Voor de CCO ligt hier de uitdaging om privacy en commerciële belangen in balans te brengen.

Versterken van het merk als digitale leider

Door eIDAS 2 proactief te omarmen, kan een instelling zich profileren als innovatieve en betrouwbare digitale speler. Dit versterkt niet alleen de merkpositie, maar trekt ook klanten en partners aan die waarde hechten aan digitale zekerheid en gemak. Voor de CCO is dit een kans om het merk strategisch te laden en onderscheidend te maken.

IMPACT

Information

Information (1/2)

De implementatie van eIDAS 2 stelt nieuwe eisen aan datakwaliteit, -beveiliging en -uitwisseling. Voor de CIO betekent dit een stevigere regierol op het gebied van gegevensbeheer en compliance:

Uniform en centraal databeheer

De verordening vraagt om harmonisatie van hoe identiteitsdata en bijbehorende gegevens uit klantdossiers worden opgeslagen en beheerd. Dat geldt zowel voor de initiële verwerking als voor latere uitgifte van attestaties.

Semantische interoperabiliteit

Het uitwisselen van gegevens in ketens vereist dat alle betrokken partijen een gemeenschappelijk begrip hebben van de betekenis van data. De CIO dient ervoor te zorgen dat middels het gebruik van taxonomieën en ontologiën, gegevens correct geïnterpreteerd en verwerkt worden over systeem- en landsgrenzen heen.

Databehoefte granualiseren

eIDAS 2 dwingt instellingen om alleen die data uit te vragen en te verwerken die strikt noodzakelijk zijn voor een specifieke dienst of proces. Dit principe van dataminimalisatie vraagt een fijnmazige inrichting van dataflows en autorisaties. Voor de CIO betekent dit balanceren tussen compliance en het behoud van voldoende informatie voor operationele en commerciële processen.

Interoperabiliteit over landsgrenzen heen

Systemen moeten gegevens uit verschillende lidstaten kunnen verwerken, die mogelijk verschillen kennen in implementatie, technische specificaties en juridische implicaties. Voor de CIO betekent dit investeringen in en testen op het snijvlak van data, operatie en juridica.

Information (2/2)

De implementatie van eIDAS 2 stelt nieuwe eisen aan datakwaliteit, -beveiliging en -uitwisseling. Voor de CIO betekent dit een stevigere regierol op het gebied van gegevensbeheer en compliance:

Duurzame beschikbaarheid

Transactie- en dossiergegevens moeten duurzaam beschikbaar en verifieerbaar blijven. Het gebruik van Trust Services waaronder digitale handtekeningen vereist herziening van de procedures en voorzieningen voor langdurige opslag en beschikbaarheid. De CIO zal hier in samenwerking met de CTO passend beleid en processen voor moeten ontwikkelen.

Integriteit en actualiteit

De CIO, als verantwoordelijke voor het organisatie-brede informatiebeleid staat voor de uitdaging om vertrouwensdiensten correct toe te passen en de benodigde informatievoorziening daarop te ontsluiten. Incorrecte toepassing of ontsluitingen kunnen leiden tot juridische problemen of reputatieschade.

IMPACT

Human Resources

Human Resources (1/2)

De implementatie van eIDAS 2 raakt niet alleen klanten, maar ook medewerkers en interne processen. Voor de CHRO betekent dit nieuwe verantwoordelijkheden, maar ook kansen om de *employee experience* te verbeteren:

Digitale onboarding en authenticatie

Met de Wallet kunnen nieuwe medewerkers eenvoudig en veilig hun identiteit aantonen, waardoor het onboardingproces sneller, consistenter en grensoverschrijdend kan plaatsvinden. Dit verlaagt de administratieve druk en geeft HR ruimte om zich meer te richten op de menselijke kant van instroom. Voor de CHRO betekent dit een kans om de *employee experience* direct vanaf dag één te verbeteren.

Veilig digitaal toegangsbeheer

Digitale identiteiten maken het mogelijk om medewerkers precieze toegangsrechten te geven tot systemen, locaties en gevoelige data, afhankelijk van hun rol en functie. Dit vergroot de security en maakt toegangsbeheer eenvoudiger en flexibeler, ook bij hybride werken. De CHRO krijgt hiermee een belangrijke rol in het borgen van digitale veiligheid en compliance.

Check op diploma's en referenties bij de bron

Digitale attestaties maken het mogelijk om diploma's, certificaten en werkervaring direct bij de bron te verifiëren, zonder papieren documenten of tijdrovende checks. Dit versnelt werving en selectie en vermindert de kans op fraude of vervalste informatie. Voor HR is dit een belangrijke stap richting een meer datagedreven en betrouwbare recruitmentpraktijk.

Efficiëntie in HR-administratie

Door digitale identiteiten en elektronische handtekeningen te integreren in HR-processen kunnen veel documenten en workflows volledig digitaal en veilig worden afgehandeld. Dit vermindert papierwerk, versnelt processen en verkleint fouten. Voor de CHRO betekent dit een slankere operatie en meer focus op strategische HR-thema's.

Human Resources (2/2)

De implementatie van eIDAS 2 raakt niet alleen klanten, maar ook medewerkers en interne processen. Voor de CHRO betekent dit nieuwe verantwoordelijkheden, maar ook kansen om de *employee experience* te verbeteren:

Faciliteren van mobiliteit

De uniforme standaarden van eIDAS maken het eenvoudiger om medewerkers te laten werken of overstappen tussen vestigingen in verschillende EU-landen, zonder steeds opnieuw identiteits- of bevoegdheidscontroles uit te voeren. Dit ondersteunt grensoverschrijdende werving en mobiliteit van talent. Voor de CHRO biedt dit nieuwe mogelijkheden om internationale loopbaanpaden te faciliteren.

Training bij gebruik van vertrouwensdiensten

Medewerkers moeten leren hoe ze veilig omgaan met de Wallet en vertrouwensdiensten, zowel in hun eigen werkprocessen als richting klanten. Dit vraagt om trainingen, communicatie en duidelijke richtlijnen om acceptatie en risicobewustzijn te vergroten. De CHRO speelt een sleutelrol in het managen van deze adoptie en het creëren van vertrouwen bij medewerkers.

Employee experience en vertrouwen

Digitale identiteit raakt medewerkers niet alleen technisch, maar ook emotioneel: hoe veilig voelt hun data, hoe transparant is het proces, en wat betekent dit voor hun privacy? De CHRO moet hier proactief communicatie en beleid op inzetten om vertrouwen en betrokkenheid te behouden. Dit is cruciaal voor draagvlak en succesvolle adoptie.

IMPACT

Strategy

Strategy (1/2)

De invoering van eIDAS 2 raakt de kern van de strategie van vele instellingen: vertrouwen, digitale wendbaarheid, compliance en marktkracht. Voor de CEO en CSO betekent dit niet alleen voldoen aan wetgeving, maar ook het benutten van een strategisch momentum:

Onderscheidend vermogen in de markt

Bedrijven die eIDAS 2 proactief omarmen, kunnen sneller nieuwe proposities lanceren, grensoverschrijdend opereren en digitaal vertrouwen uitstralen naar klanten en partners. Dit first mover advantage is essentieel in een markt waar snelheid en betrouwbaarheid bepalend zijn. Voor de CEO ligt hier de kans om concurrenten voor te blijven en de digitale strategie van de organisatie te versnellen.

Strategische positionering binnen ecosystemen

eIDAS 2 creëert ruimte voor overheden en bedrijven om niet alleen dienstverlener te zijn, maar ook regisseur van digitale ecosystemen, bijvoorbeeld als Orchestrator of Trusted Hub. Dit opent nieuwe verdienmodellen en samenwerkingen met partijen binnen en buiten de sector. Voor de CEO betekent dit keuzes maken over de rol die de organisatie wil spelen in de digitale economie.

Versneller voor digitalisering en efficiency

De uniforme standaarden van eIDAS maken processen als onboarding, machtigen en klantcommunicatie sneller en betrouwbaarder, wat direct bijdraagt aan lagere kosten en hogere klanttevredenheid. Dit biedt ruimte om digitale initiatieven te versnellen zonder steeds opnieuw integraties te bouwen. Voor de CEO is dit een kans om binnen de digitaliseringsagenda tastbaar resultaat te creëren.

Bestuurlijke verantwoordelijkheid

De verplichting om Wallets te accepteren raakt vrijwel alle onderdelen van de organisatie, van IT en risk tot commercie en HR. Dit vereist sterke bestuurlijke sturing, heldere visie en een geïntegreerde implementatie-aanpak. Voor de CEO betekent dit eigenaarschap nemen over de koers én de interne alignment.

Strategy (2/2)

De invoering van eIDAS 2.0 raakt de kern van de strategie van vele instellingen: vertrouwen, digitale wendbaarheid, compliance en marktkracht. Voor de CEO en CSO betekent dit niet alleen voldoen aan wetgeving, maar ook het benutten van een strategisch momentum:

Richting geven aan interne alignment

Omdat eIDAS 2.0 meerdere disciplines tegelijk raakt, moet de CEO zorgen dat alle C-level functies samenwerken vanuit één visie en tempo. Dit voorkomt versnipperde initiatieven en dubbele kosten. Het is de taak van de CEO om prioriteiten te stellen en duidelijke governance in te richten rondom dit strategische thema.

Reputatie en legitimiteit

eIDAS 2.0 draait niet alleen om technologie, maar ook om vertrouwen en de rol in een digitale samenleving. Klanten en toezichthouders kijken kritisch hoe zorgvuldig zowel overheden als bedrijven omgaan met digitale identiteit en privacy. Voor de CEO is dit een strategisch thema om reputatie te beschermen én maatschappelijke waarde zichtbaar te maken.

Self-assessment

Functie	Vragen
Chief Technology Officer (CTO)	▪ Hebben wij onze IT-roadmap aangepast op de verplichte acceptatie van Wallets vanaf 2027? ▪ Zijn onze systemen technisch voorbereid op interoperabiliteit met een onbekend aantal wallets en vertrouwensdiensten? ▪ Hebben wij een archiveringsstrategie voor digitale handtekeningen en attestaties die juridisch houdbaar is op de lange termijn?
Chief Operations Officer (COO)	▪ Hebben wij inzicht in welke operationele processen geraakt worden? ▪ Kunnen wij digitale klantidentificatie via de EUDI Wallet integraal ondersteunen in onboarding en serviceprocessen? ▪ Zijn er al ketenpartners waarmee we gezamenlijk processen willen digitaliseren met eIDAS-vertrouwensdiensten?
Chief Risk Officer (CRO)	▪ Zijn onze fraude- en CDD-processen aangepast op de mogelijkheden en beperkingen van eIDAS? ▪ Hebben we de risico's van vertrouwensdiensten waaronder attestaties binnen onze risicoraamwerken geanalyseerd? ▪ Weten we hoe afhankelijk we (willen) worden van externe TSP's en hoe we die ketenrisico's gaan beheersen?
Chief Commercial Officer (CCO)	▪ Zijn onze klantreizen geoptimaliseerd voor gebruik van Wallets (B2C én B2B)? ▪ Overwegen wij een actieve rol in het ecosysteem, zoals het uitgeven van attestaties of het orkestreren van ketenoplossingen? ▪ Weten we welke nieuwe proposities we nu kunnen ontwikkelen dankzij eIDAS?
Chief Information Officer (CIO)	▪ Kunnen wij attestaties technisch en juridisch correct verwerken? ▪ Zijn ons datamanagement en onze governance afgestemd op het gebruik van vertrouwensdiensten? ▪ Beschikken wij over een plan voor redundantie en duurzame opslag van digitale transacties?
Chief Human Resources Officer (CHRO)	▪ Kunnen wij digitale identiteiten veilig inzetten in onboarding, toegang en personeelsbeheer? ▪ Is onze HR-organisatie voorbereid op het beheren van digitale toegang en machtigingen via Wallets? ▪ Weten wij in welke mate het bedrijf ondersteuning nodig heeft bij het trainen en opleiden bij gebruik van de Wallet?
Chief Executive Officer (CEO)	▪ Hebben wij al een visie of strategie geformuleerd over de rol die wij in digitale ecosystemen willen spelen? ▪ Is er een integraal overzicht beschikbaar van alle domeinen en processen binnen onze organisatie die geraakt worden door de verplichte acceptatie van de Wallet per 2027? ▪ Hebben wij eIDAS 2 benoemd als strategisch thema binnen onze bestuursagenda of digitale transformatieprogramma's?

Meer weten of een *impactanalyse starten?*

Leon Roseleur

lroseleur@davinci-conclusion.nl

06-30 31 40 84

Cas Sunderman

csunderman@davinci-conclusion.nl

06-57 26 13 00

Samen *vooruit*

+31 (0)35 524 8901

info@davinci-conclusion.nl

Davinci Conclusion
Gooimeer 6-01
1411 DD Naarden

Davinci
CONCLUSION