

# SIKKER DIGITAL IDENTITET

# SmartSignatur®

## 1 Opret

Automatisering af brugeroprettelse inklusiv integreret tildeling af roller og rettigheder og synkronisering af brugerdata i tilknyttede it-systemer.



## 2 Udsted

Selvbetjening for brugerne til kontoaktivering, password reset og ændringer i rettigheder - alle ugens dage, døgnet rundt

## 3 Anvend

Brugervenlig og sikker digital 2-faktor adgang, single sign-on og ægte digital underskrift i hverdagen

## 4 Revidér

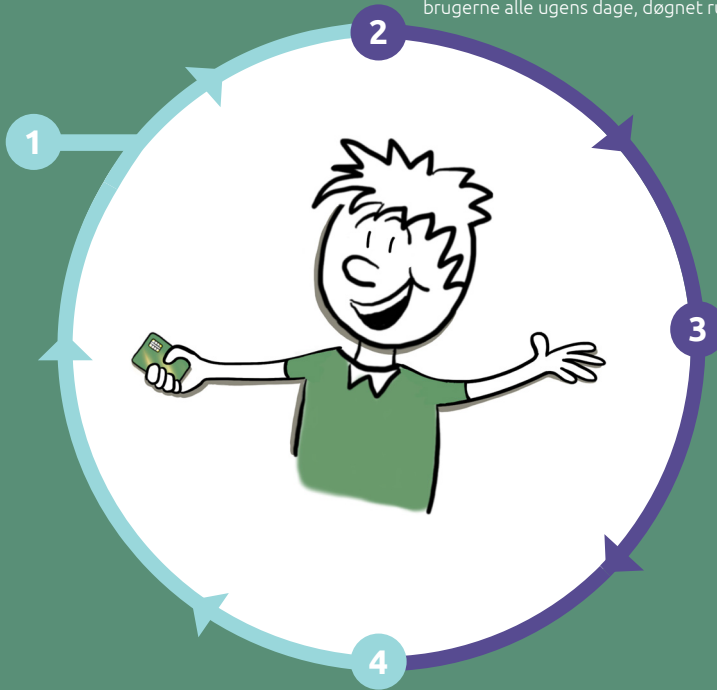
Kontrol af og dokumentation på overholdelse af interne regler og eksterne lovkrav

## Udsted

Selvbetjening for brugerne alle ugens dage, døgnet rundt.

## 1 Opret

Integreret og automatiseret brugeroprettelse.

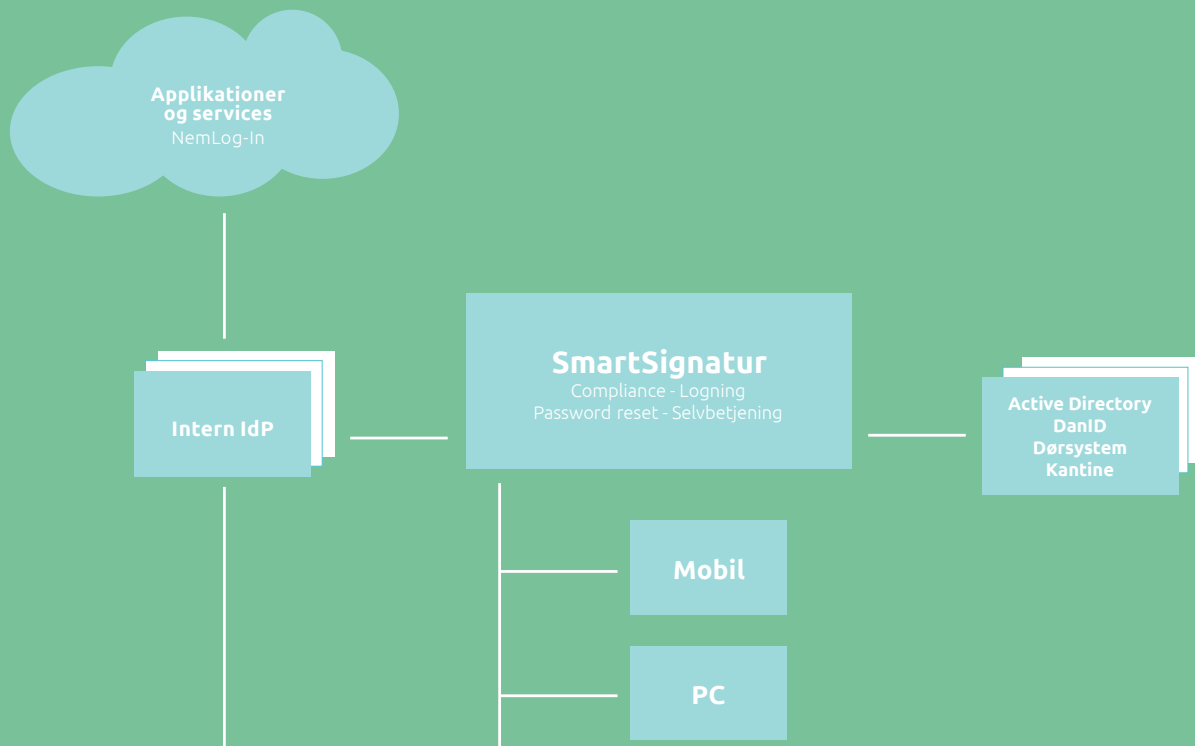


## 3 Anvend

Brugervenlig og sikker digital 2-faktor adgang i hverdagen.

## 4 Revidér

Overholdelse af interne regler og eksterne lovkrav.



# Lovgivning

Sikker digital identitet er særdeles vigtigt i forbindelse med de seneste lovkrav der stilles til både private og offentlige virksomheder og organisationer. Disse krav findes i de europæiske GDPR, eIDAS, NIS, PSD2 regler og den danske NSIS standard.

Her stilles krav om hvorledes digitale identiteter skal dannes, men også administreres og anvendes af brugerne.

Der veksles mellem mere tekniske krav så som fysiske ID krav i forbindelse med brugeroprettelse og 2-faktor validering til login og mere administrative krav, såsom der er truffet passende tekniske foranstaltninger og om der foretages kontinuerlige risikovurderinger.

# Arkitektur

Sikker digital identitet kræver, at ens interne it-systemer er godt forbundne, og at de automatisk - og gerne i realtid - bidirektionalt synkroniserer data om brugerne.

Den primære brugerdatabase skal udover de elementære brugerdata også kunne håndtere både roller og tilhørende rettigheder og ekstra udvidede brugeroplysninger, certifikater og login-credentials.

En bruger kan have flere roller i ens organisationer og det underliggende it-system skal kunne rumme denne udfordring. Det bliver særligt vigtigt hvis fokus er at opnå niveau "betydelig" eller "høj" jf. NSIS/eIDAS.

I tillæg til en avanceret brugerdatabase skal der også være en "Identity Provider (IdP)" til at varetage single sign-on (SSO) forbindelser til både interne og eksterne it-systemer. Endeligt skal der være central logging kombineret med og compliance værktøjer til analyser og rapportering.

# Livscyklus

Mange brugere begynder deres relation med deres organisation med en registrering i løn- og personalsystemet. Dette er et godt udgangspunkt, men ikke tilstrækkeligt til at brugeren er oprettet på niveau "betydelig" eller "høj". Brugeren skal selv bekræfte sin identitet med 2 faktorer fra mindst 2 forskellige kategorier. I hverdagen skal de anvende 2-faktor metoder til digital adgang.

Ofte ændrer ens opgaver sig og man har behov for ændringer i måske ens overordnede roller, men også i de mere specifikke rettigheder. Sådanne ændringer skal kunne varetages direkte af brugerne med efterfølgende godkendelse af en rettighedsejer.

Fratræder man sin stilling skal systemet automatisk sikre, at alle digitale og fysiske adgange lukkes eller deaktiveres. Med nationale og internationale krav til niveauet af brugeridentiteten er det centralt, at hele livscyklus forvaltes og administreres på samme eller højere niveau.

# Dagligdagen

Hverdagen for den digitale bruger skal være brugervenlig og overholde de it-mæssige sikkerhedskrav. Det er to kræfter der ofte trækker hver sin vej.

En sikker digital identitet kan rumme disse krav og medfører, at brugeren i dagligdagen har en let og sikker digital adgang med fuld 2-faktor adgang, kan underskrive dokumenter og e-mails med digitalt blæk, kan kryptere og dekryptere data når det kræves og endelig oplever, at adgang til andre it-systemer sker med single sign-on.

For at hverdagen opleves let og smidig, er det bedst, når både den fysiske og digitale adgang er kombineret. Det forbygger at adgangskort deles og at print kan ses af andre brugere. Samtidig betyder det også, at ens PC låses automatisk når man forlader sin PC.

# SMARTSIGNATUR PRODUKTER

	PersonalID	LocalID Standard	LocalID Advanced	CardID	GlobalID Standard	GlobalID Advanced
Minimum antal brugere	1	1	10	500	500	100
Chipkort til PC	✓	✓	✓		✓	✓
Dørkort og follow-me print				✓	✓	✓
Rolle- og rettighedsstyring						✓
Password reset system		Tilkøb	Tilkøb		Tilkøb	✓
Selvbetjeningskiosk				✓	✓	✓
Mail kryptering og signering	✓	✓	✓		✓	✓
Kyptering af filer og diske	✓	✓	✓		✓	✓
Signering af Office dokumenter	✓	✓	✓		✓	✓
Windows & MacOS 2-faktor login		Kun Windows	✓		✓	✓
Automatisk skærmlås		✓	✓		✓	✓
NemID medarbejdersignatur	✓		✓		✓	✓
Microsoft Active Directory			✓	✓	✓	✓
KMD Nexus & Systematic Cura					✓	✓
Nemlog-in	✓				✓	✓
Aula			Via IdP		Via IdP	Via IdP
PwC - Kombit Støttesystemerne (STS)					Tilkøb	Tilkøb
OS2faktor & OS2rollekatalog			Q4 2019		Q4 2019	Q4 2019
NSIS niveau	Betydelig	Betydelig	Betydelig		Høj	Høj
Relevant lovgivning	NSIS, NIS, eIDAS, GDPR & PSD2					



## LIGA

Deltag selv i eller gense et webinar på [liga.com/smartsignatur/webinar](https://liga.com/smartsignatur/webinar)

Download whitepaper på [liga.com/sikkerdigitalidentitet](https://liga.com/sikkerdigitalidentitet)

post@liga.dk  
Tel. 35 36 95 05

I samarbejde med:

