Der findes kun én – identitet

Bjarke Alling

Koncerndirektør i Liga ApS,

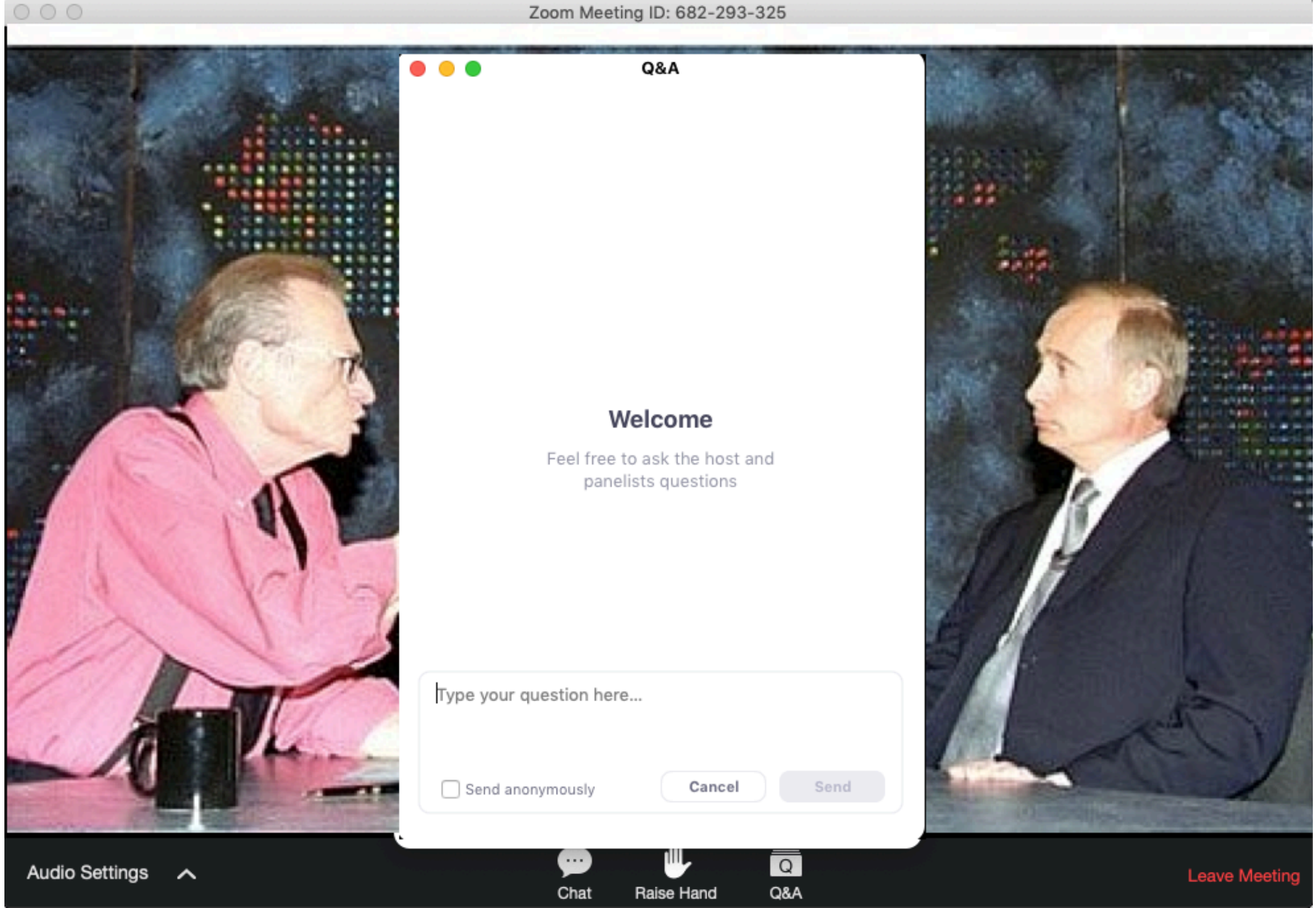
Derudover Formand IT Branchens it-sikkerhedsudvalg

Formand for Det Nationale Cybersikkerhedsråd.

De 5 webinar råd

- Find et lokale hvor du er uforstyrret
- Hav friske forsyninger klar [vand, kaffe, et stk. Frugt]
- Luk alle applikationer andre og sæt Zoom til fuld skærm
- Brug headset med mikrofon
- Tag noter og engagér dig gennem Q&A og håndsoprejsning


Zoom Meeting ID: 682-293-325
Audio Settings
Chat
Raise Hand
Q&A
Leave Meeting


Zoom Meeting ID: 682-293-325
Q&A
Welcome
Feel free to ask the host and panelists questions
Type your question here...
Send anonymously
Cancel
Send
Audio Settings
Chat
Raise Hand
Q&A
Leave Meeting

Zoom Meeting ID: 682-293-325

Chat

To: All panelists

Your text can only be seen by panelists

Audio Settings

Chat

Raise Hand

Q&A

Leave Meeting

God fornøjelse

Der kan kun være én

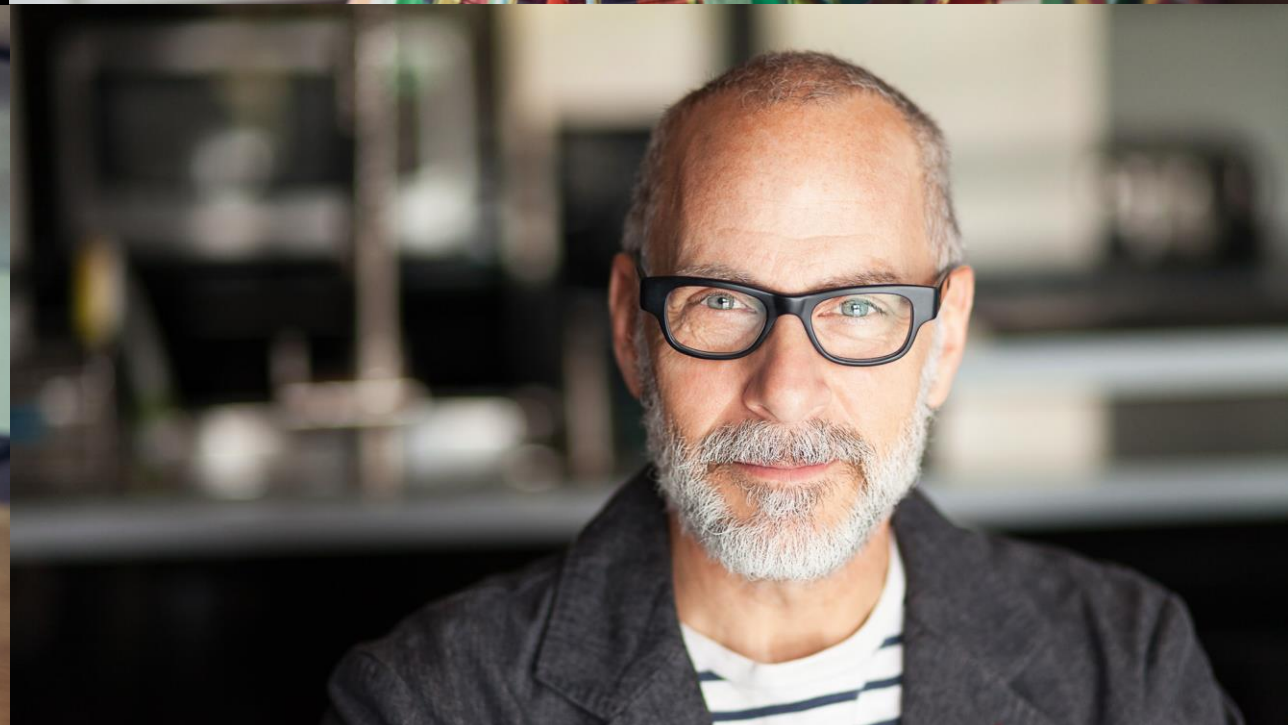
LIGA

Der kan kun være én

identitet

LIGA



Der kan kun være én ”identitet”

Bjarke Alling

Koncerndirektør i Liga

Formand IT Branchens it-sikkerhedsudvalg

Formand Det Nationale Cybersikkerhedsråd

LIGA

10 år med cybersikkerhed


RANSOMWARE
BØDER
INSIDER
DATATYVERI

Afstemning

Sorter truslerne efter den du mener udgør den største risiko
1 er den største – 4 er den mindste

RANSOMWARE

BØDER

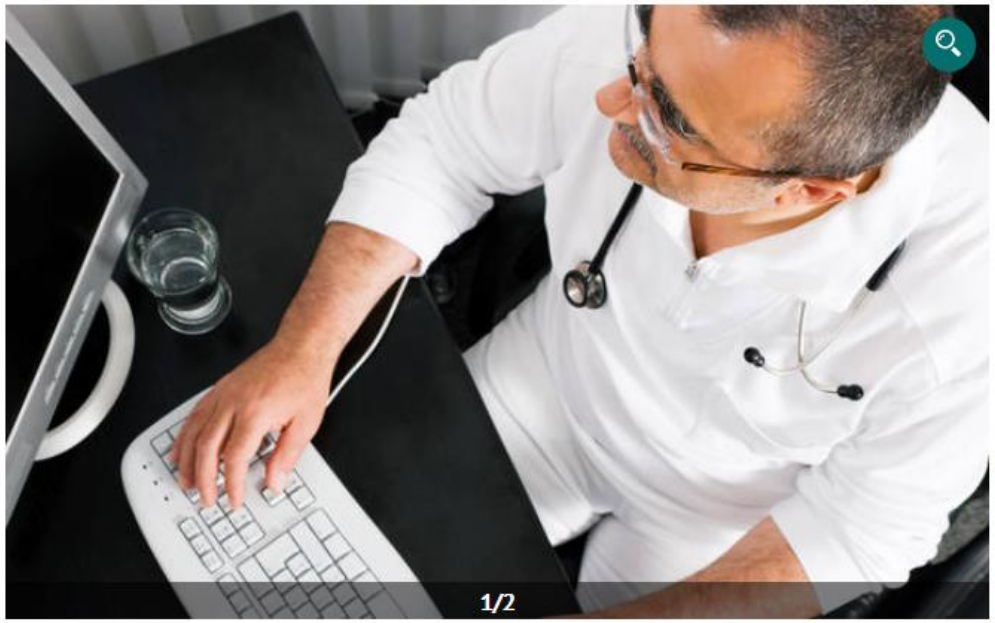
INSIDER

DATATYVERI

DANMARK

Region Midt lagde fælde for medarbejderne - næsten hver anden faldt i

AF: JESPER BECH PEDERSEN , JBPE@VIBORGFOLKEBLAD.DK
Publiceret 15. juni 2019 kl. 08:01



Næsten 1200 tilfældigt udvalgte medarbejdere i Region Midtjylland har modtaget en snydemail, som typisk kommer fra svindlere. Denne var dog sendt af regionen selv. I mailen blev de bedt om at indtaste deres adgangskode og brugernavn. Det gjorde 42 procent af de intetanende testpersoner. Modelfoto: Scanpix/Iris

"This changing environment doesn't mean that the security perimeter has disappeared. Instead, it has shifted to the users and their multiple endpoints. **As a result, identity has become the new perimeter"**


WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

The Cybersecurity Guide for Leaders in Today's Digital World

October 2019

weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf

LIGA

Minimumskrav - sikkerdigital.dk

GDPR

ISO/IEC 27001

NIS

PSD2

Ledelsesbekendtgørelsen
1. sep 19 - risikovurdering - it-sikkerhedspolitik

”Der er generelt brug for, at virksomhederne prioriterer cybersikkerhed højere og i den forbindelse skal ledelsen gå forrest.
Alle bestyrelser
bør læse denne vejledning”

Industriens Fond - Bestyrelsesforeningen med flere

www.industriensfond.dk/bestyrelsens-guide-til-cybersikkerhed

To faktor login

2 –faktor login skal være fra to kategorier

Krav til **2-faktor login** findes i NSIS (eIDAS), ISO27001, PSD2 med flere

GDPR og NSIS - standarden

National Standard for Identiteters Sikringsniveauer (NSIS 2.0.1)

NSIS (eIDAS) definere niveauerne: ”lav”, **”betydelig”** og ”høj”.

- **artikel 9** Behandling af særlige kategorier af personoplysninger
- **artikel 10** Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser

Der skal fremover anvendes **2-faktor login** til alle IT systemer med **GDPR** data

Microsoft adgangskodefri strategi

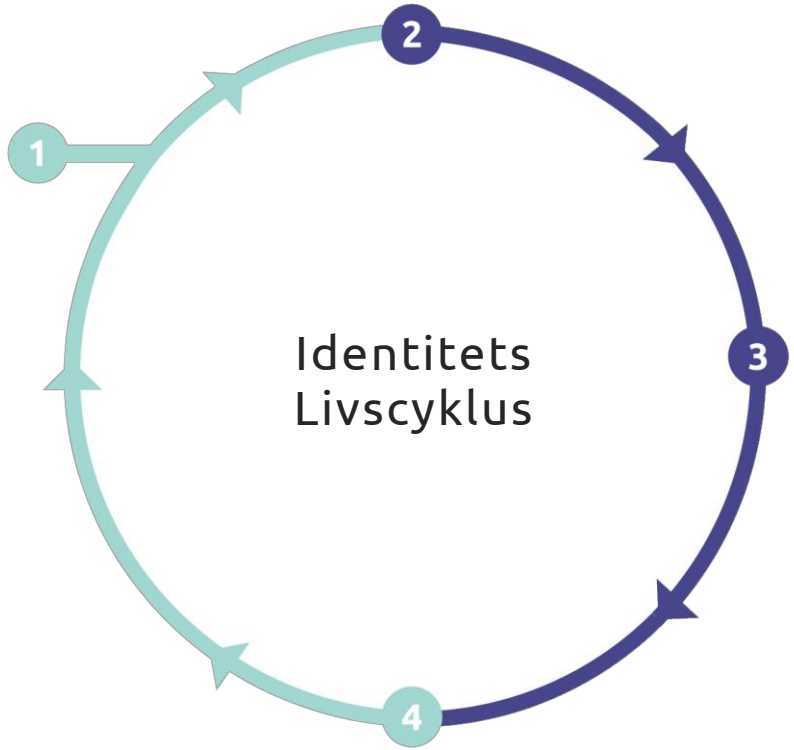
De fire trin til fuldstændige frihed for adgangskoder

1. Tilbyd brugerne en adgangskodefri erstatning
2. Begræns der hvor brugerne skal anvende adgangskoder
3. Overgå til adgangskodefri udrulninger
4. Fjern adgangskoderne fra selve identitetsdatabasen

docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy

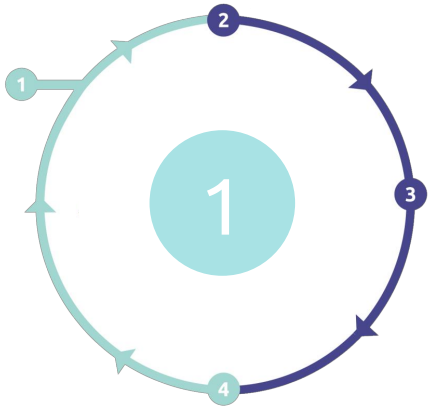
Proces

1. **Opret**
   Integreret og automatiseret brugeroprettelse
2. **Udsted**
   ID validering NFC- og nøglekonfiguration, print
   Selvbetjening for brugerne alle ugens dage, døgnet rundt
3. **Anvend**
   Brugervenlig og sikker digital 2-faktor adgang i hverdagen
4. **Revider**
   Hændelsesindsamling, analyser og kontroller
   Overholdelse af interne regler og eksterne lovkrav



Opret

Dannelse af dit digital “jeg”



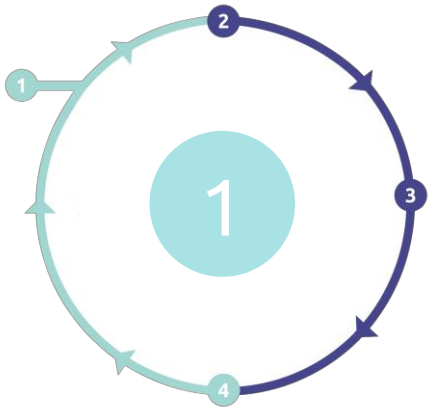
IT-afdeling

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

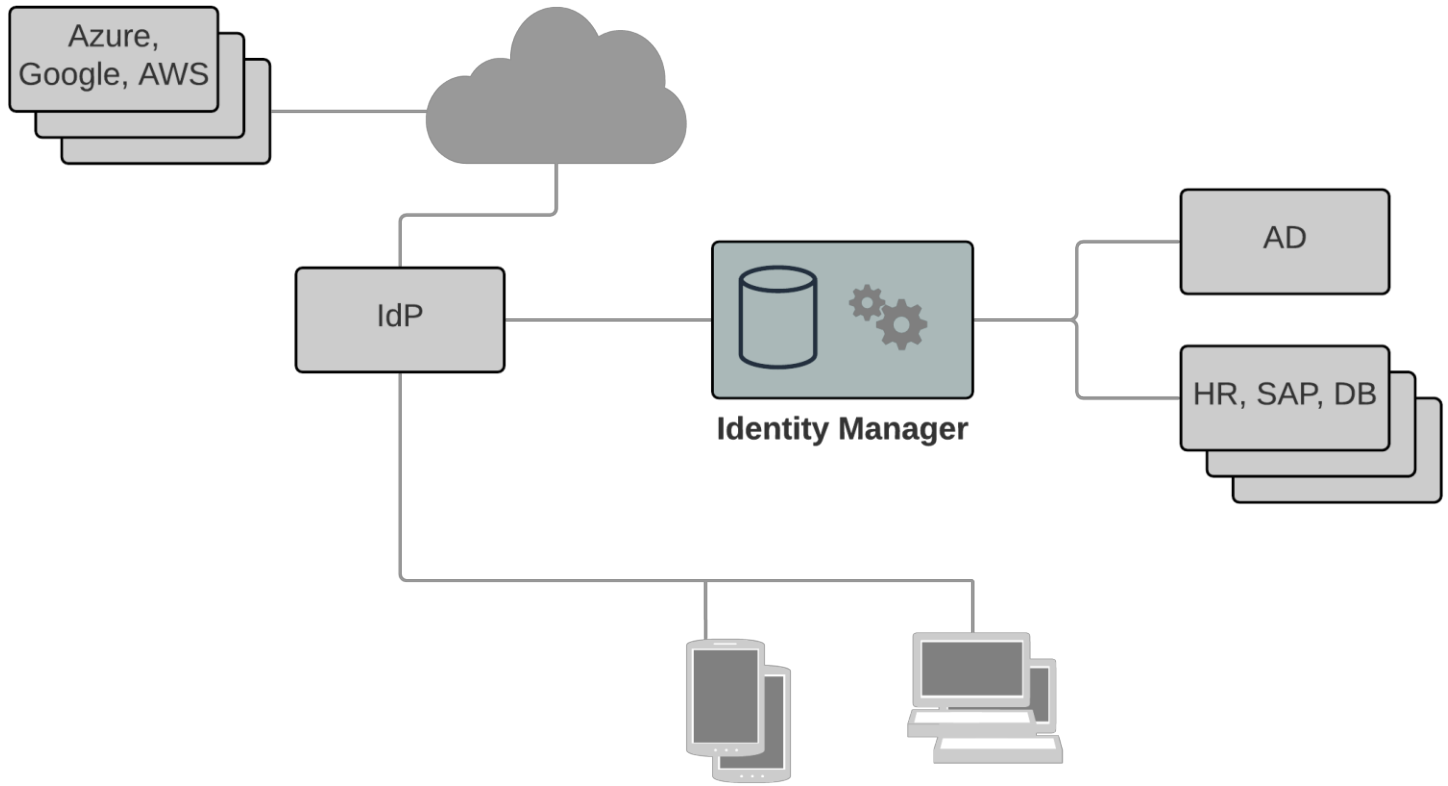
- Minimal manuel indtastning – i alle systemer
- Identitet dannes automatisk ud fra kendte stamdata - opslag i CPR
- Berigelse af stamdata fra eksterne systemer - Kombit, Lessor, SAP
- Automatisk tilføjelse af roller og rettigheder
- Mange roller – men stadig blot én enkelt identitet
- Realtids opdatering i tilsluttede interne og eksterne systemer

Opret

Identity Management (IDM)

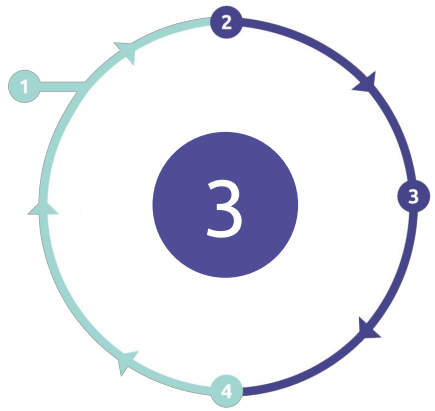


IT-afdeling



Anvend

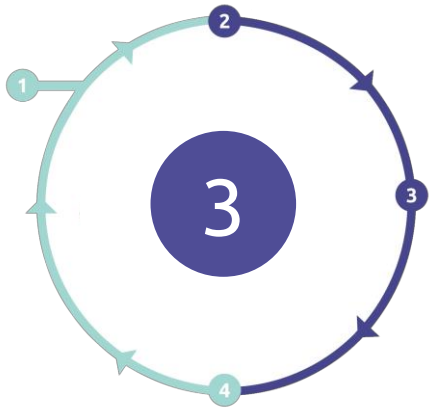
Værktøjer til adgangsstyring



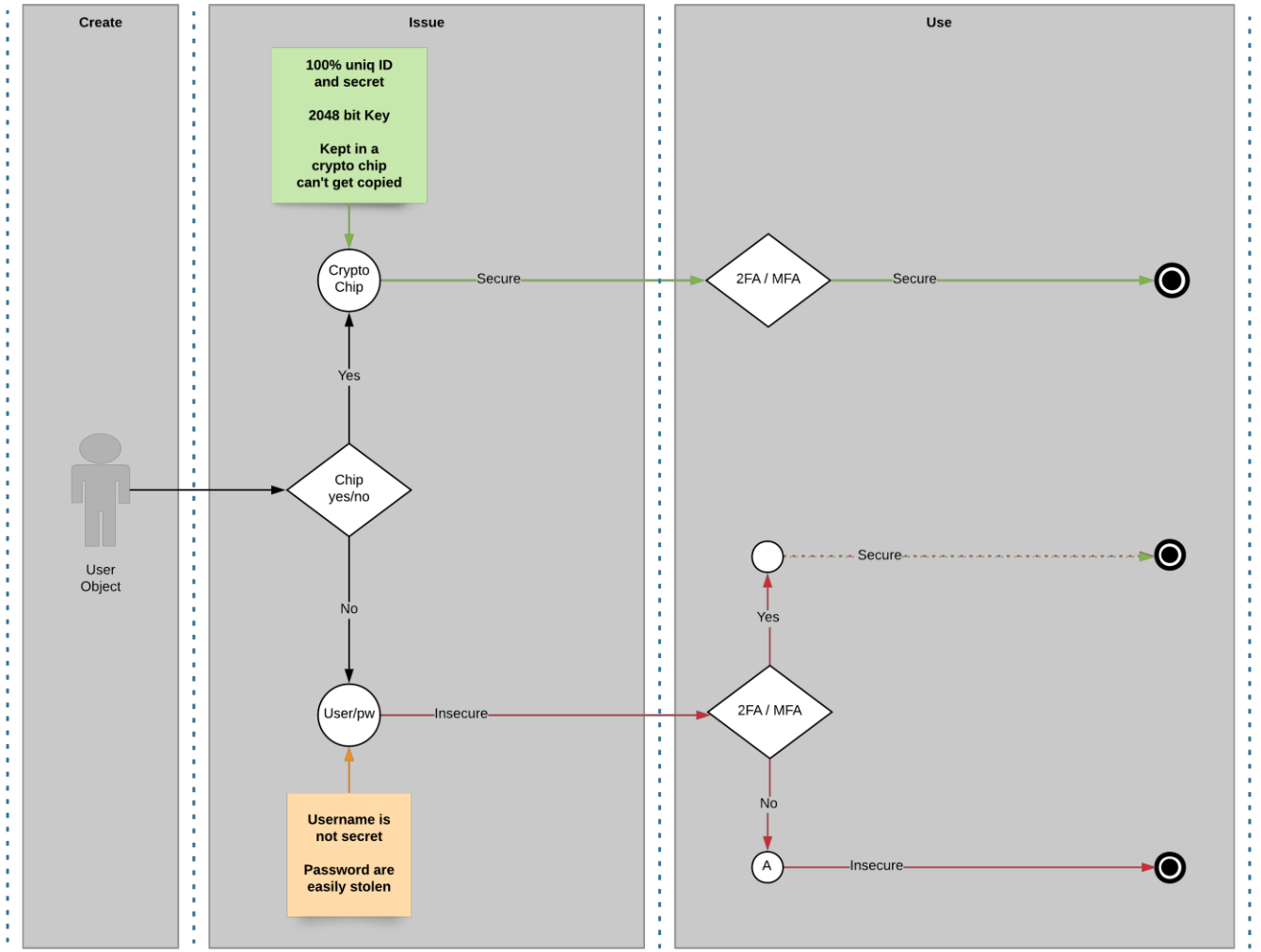
- **Operativsystem (Microsoft og Mac OS)**
  - AD understøtter user/password eller digitale certifikater (x509).
  - Patch hurtigt og undgå lokale ændringer i standardregler og kode.
  - Chip kort og certifikater er standard.
  - Sikkerhed bygger på standarder og genkendelighed.
- **Identity Provider (IdP)**
  - Skal være egnet til både federering og proxy.
  - Windows login metode fremgår i Kerberos ticket.
  - Åbne protokoller: SAML2/OIOSAML3 - OAuth/OpenID Connect.
  - Erhvervsidentiteter med Nemlog-In3 er et solidt professionelt valg.
- Fido-nøgler er til personligt og privat.

Anvend

Loginproces med to faktorer

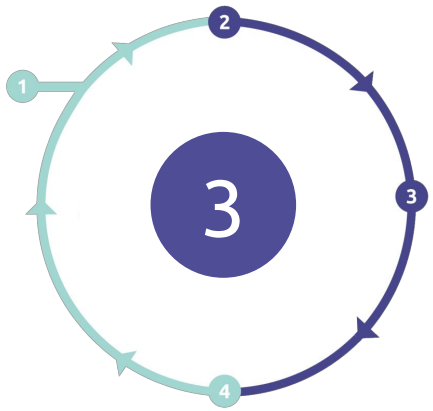


Bruger

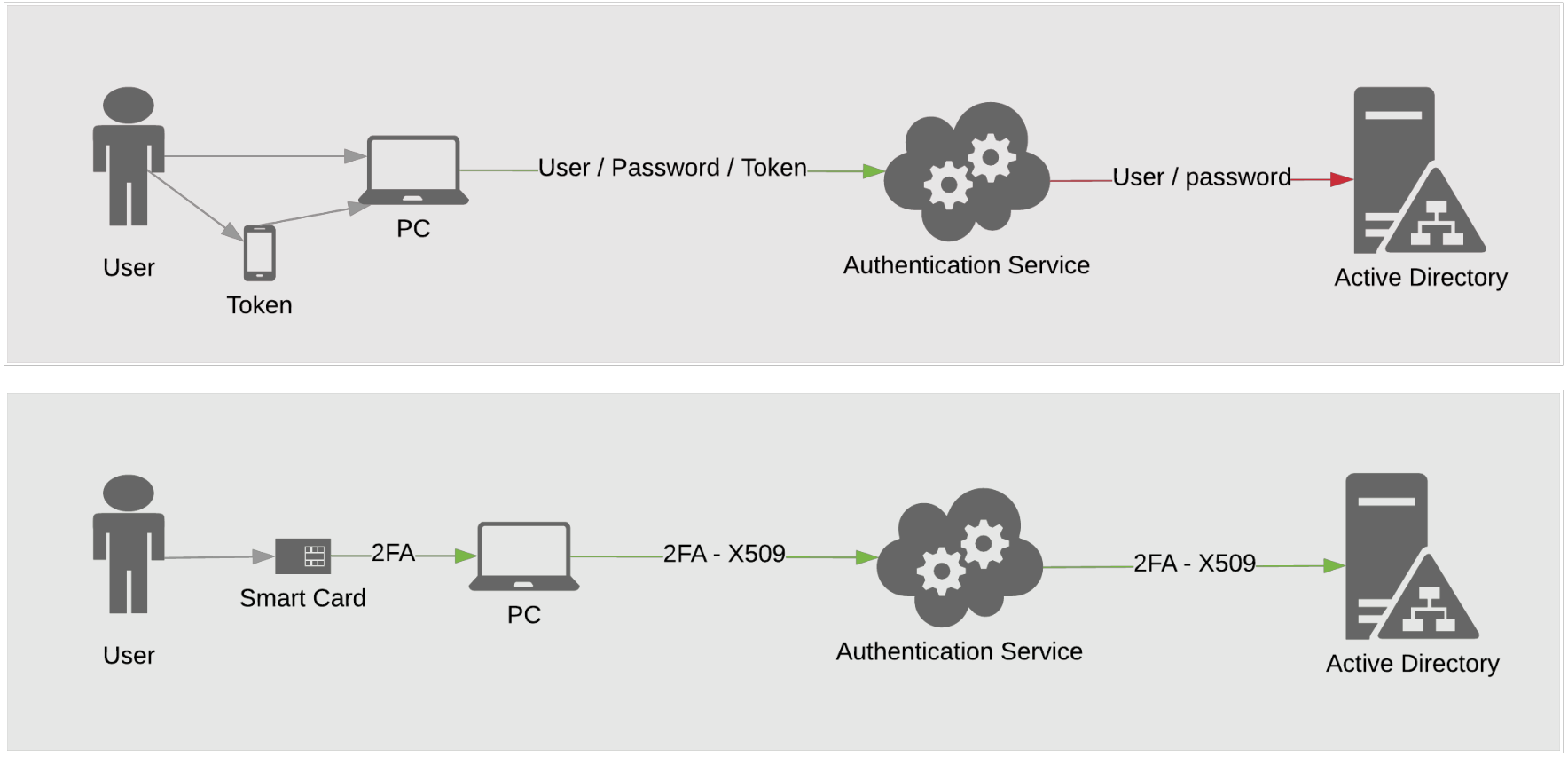


Anvend

Login proces efter NSIS niveau ”betydeligt”

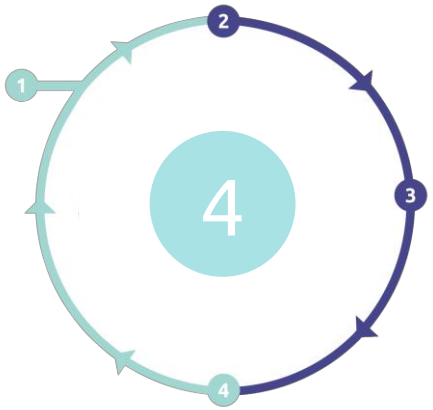


Bruger



Revider

Kontinuerlig kontrol og dokumentation



IT-afdeling

- Intern tilsyn med både fysiske- og digitale adgange
  - Dynamiske analyser af adfærds- og brugsmønstre
  - Automatisk de-aktivering ved gentagne fejllogin i forbudne systemer
- Regulatorisk kontrol og dokumentation
  - Specifik kontrol af rettighedstildelinger
  - Certificeringer af rettighedstildelinger af reel rettighedsejer
- System til password reset via selvbetjening
- Realtids opdatering i tilsluttede interne og eksterne systemer
- Nødvendig kapacitet til at modstå nye trusler

Afstemning

Sorter indvendinger efter den du mener passer bedst
1 er mest – 4 er mindste

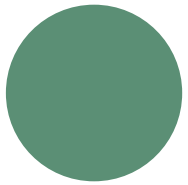
Vi følger de andre

Det er dyrt

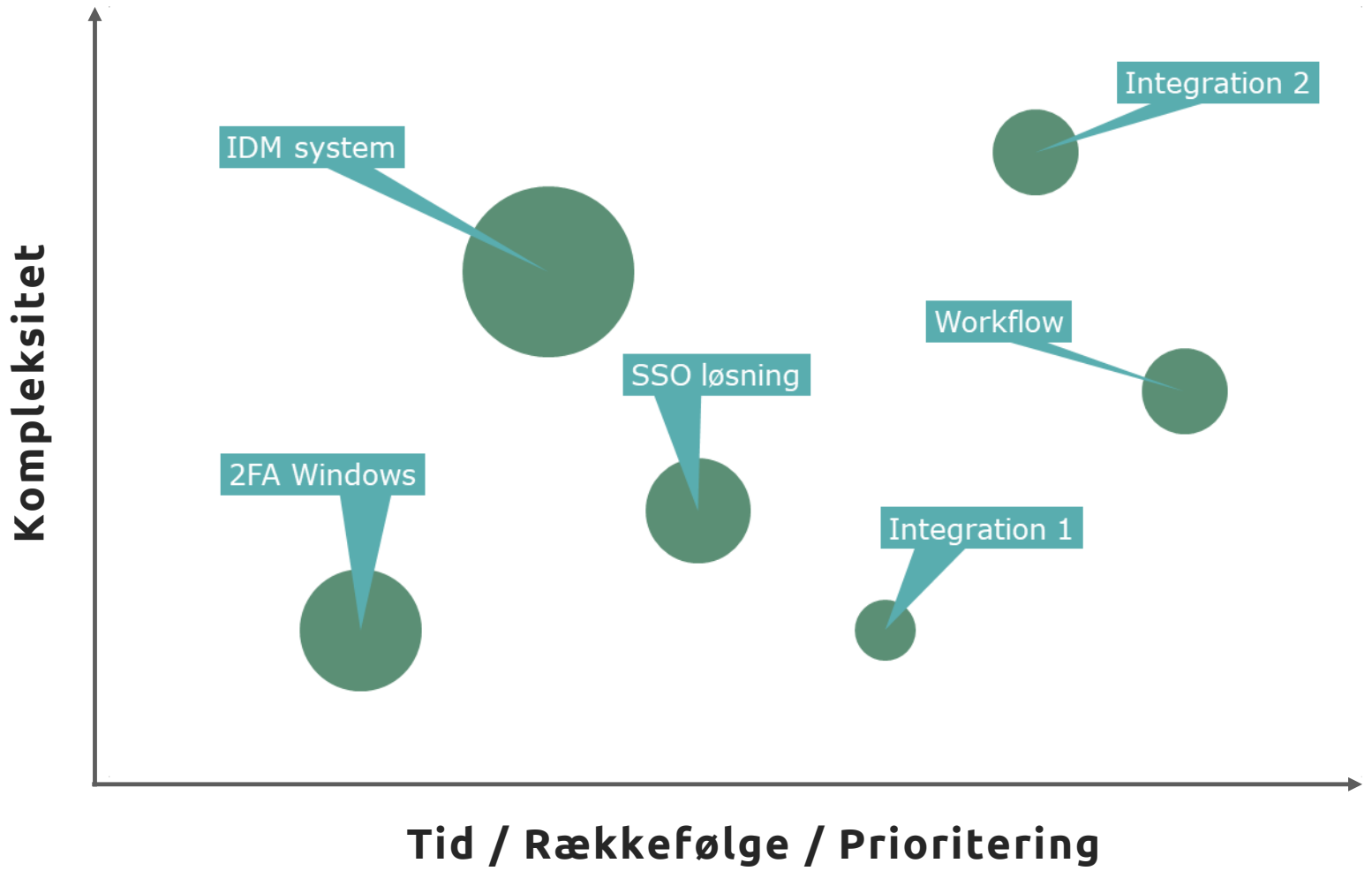
Vi har ikke tid

Mangler kompetencer

Trinvis



Omkostning



Læring

Fremtid – Sikkerhed, Compliance og Identitet

	SMB virksomhed	Faaborg Midtfyn	Region Midt
Størrelse af organisation	Lille 250 brugere 1,5 i IT	Mellem 3.400 brugere 22 i IT	Stor 26.000 brugere 350 i IT
Øjebliksbillede	Kun AD Ingen IDM Ingen 2FA	IDM Delvis SSO Ekstern 2FA	IDM SSO Ekstern 2FA
Proces	2FA > SSO > IDM	IDM > 2FA > SSO	IDM > SSO > 2FA

FAABORG-MIDTFYN KOMMUNE

midt regionmidtjylland

LIGA

Kort bane

Hvor er vi nu?

- Mange danske virksomheder oplever at de er ude af drift i flere uger!
- Hvordan vil din virksomhed / organisation opleve et sådan angreb?

Hvordan kommer vi i gang og hvor skal vi lave indsatserne?

- Hvor skal vi sætte ind, så vi kommer bedst fra start?
- Hvor er vi mest udsat?
- Hvilke kritiske services skal vi beskytte bedst og er vores ansvar?

Hvordan gør vi på den korte bane?

- **Start i IT afdelingen, her er risikoen størst**
- Prioritere de services som mindst kan undværes eller som giver størst tab
- Planlæg og gennemfør realistiske øvelser

Hvad kan vi langsigtet opnå?

- Sikre at brugerne har både korrekt og sikker adgang til de rigtige systemer

Der kan kun være én - identitet

Ransomware

Væk med lokaladministrator

Patch, patch & patch + backup

Datatyveri

Brug 2-faktor adgang

Dynamiske analyser af adgang

Svindel

Brug roller

Kontrol og rapportering

liga.com/sikkerdigitalidentitet

Bjarke Alling | ba@liga.com

linkedin.com/in/bjarkealling/

Liga ApS
Center Boulevard 5
DK – 2300 Copenhagen S

+45 35 36 95 05 | liga.com

LIGA