



Sikkerhetswebinar

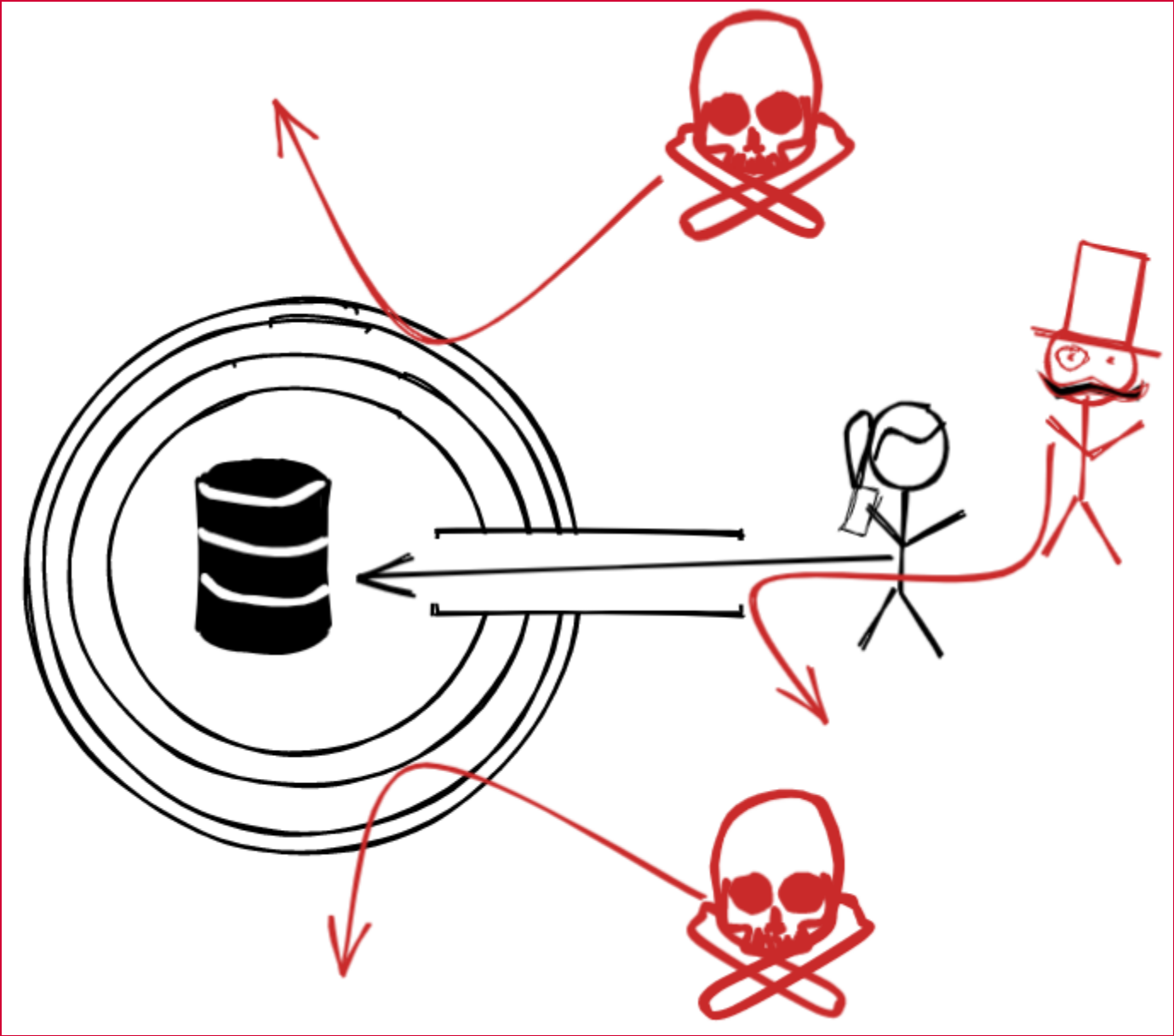
05.12.23

Tema

- Generelt om data sikkerhet
- Passord
- Vitec Planias tiltak for sikkerhet
- Plania 8.18: Hva er nytt?
- Autentifikasjons alternativer med Plania



Espen Sigmundstad
Prosjektleder BIM



Passord

Phishing - Nettfisking

- Lurer deg til å gi fra deg passordet
 - Via mail
 - Via telefon
 - Via SMS
 - Via annen nett tjeneste



Cracking

- Prøver å “beregne” ditt passord kombinasjoner
- Prøver typisk brukte password som “123456789”



Passord

CLOUD



Compute Service

Passord lengde:	Passord med: 0-9	Passord med: a-Z	Passord med: a-Z og 0-9	Passord med: a-Z, 0-9 og &%
1	Momentant!	Momentant!	Momentant!	Momentant!
2	Momentant!	Momentant!	Momentant!	Momentant!
3	Momentant!	Momentant!	Momentant!	Momentant!
4	Momentant!	Momentant!	Momentant!	Momentant!
5	Momentant!	Momentant!	Momentant!	Momentant!
6	Momentant!	2 sek	6 sek	20 sek
7	Momentant!	1 min	6 min	49 min
8	Momentant!	1 time	6 timer	5 dager
9	Momentant!	3 dager	15 dager	2 år
10	Momentant!	138 dager	3 år	330 år
11	Momentant!	20 år	162 år	50 000 år
12	2 sek	1 år	10 000 år	8X10 ⁶ år
13	16 sek	53 år	622 000 år	1X10 ⁹ år
14	3 min	3X10 ⁶ år	39X10 ⁶ år	176X10 ⁹ år
15	26 min	143X10 ⁶ år	2X10 ⁹ år	Laaang tid
16	4 timer	7X10 ⁹ år	148X10 ⁹ år	Laaang tid
17	2 dager	388X10 ⁹ år	Laaang tid	Laaang tid
18	18 dager	Laaang tid	Laaang tid	Laaang tid
19	183 dager	Laaang tid	Laaang tid	Laaang tid
20	5 år	Laaang tid	Laaang tid	Laaang tid

Passord

Credential stuffing

- Bruker navnet ditt er nødvendigvis ikke hemmelig
- Kan testes over mange tjenester

haveibeenpwned.com

Tiltak

- Unike sterke passord
- Skift passord med jevne mellomrom
- To-faktor autentifikasjon

3 Jysla Tåsjne Bisletutar

Passord

Tiltak

Password manager

- Samling av unike passord
- Tjenestene har strenge sikkerhets barrierer
- Kan ligge innenfor din organisasjons nettverk

Andre muligheter

- Windows Hello
- Passwordless

Vitec Planias tiltak for sikkerhet

Vitec IT

- Brannmur and IPS (Intrusion Protection System)
- Søker etter sårbarheter
- Kontinuerlig vedlikehold

Vitec Plania

- Penetrasjonstest
- Tilbyr forskjellige muligheter for autentisering
- Ny hovedrelease av Plania



Plania 8.18: Hva er nytt?

- Plania Web: **Internet Explorer** ikke lengre støttet
- Plania Web: Økt til **.NET Framework 4.8** (rammeverk for programmering)
- Mobil: Økt minimum plattform fra iOS 11 til **iOS 13**
- Mobil: Android **5.0**, med Chromium **60**, eller høyere
- Endring i **minimumskravene** til passordlengde og- kompleksitet.

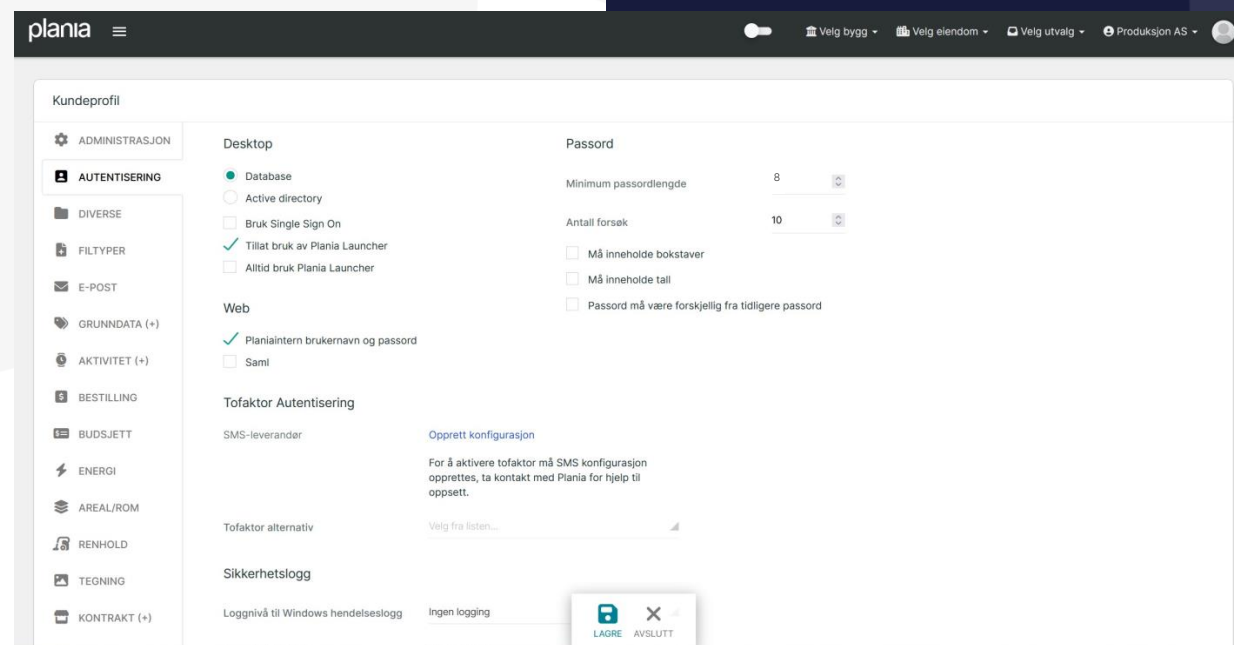
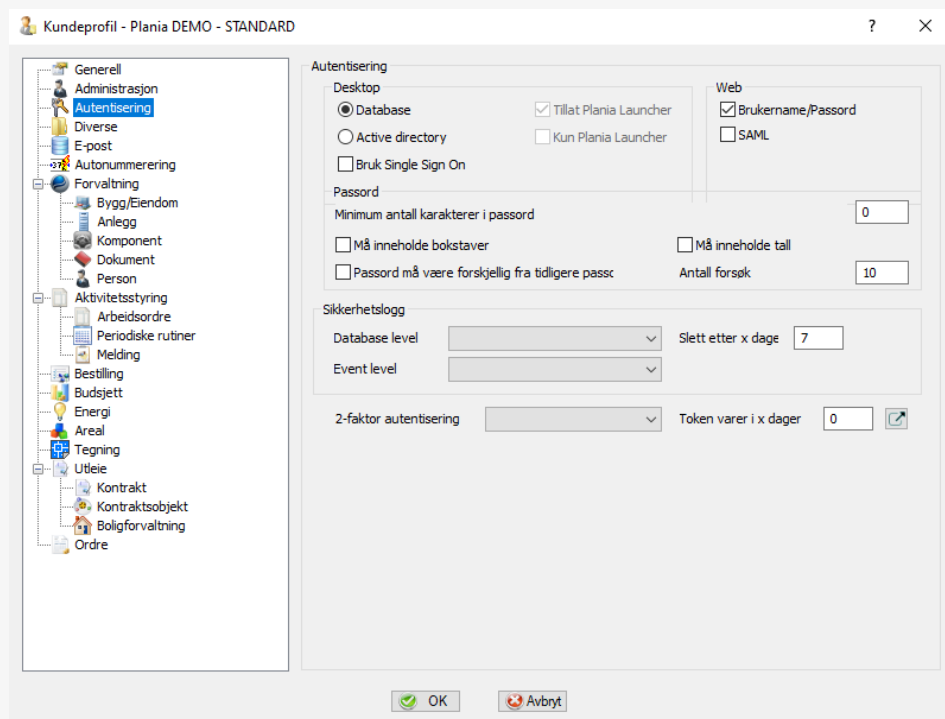
Velkommen!

 Brukernavn Passord[LOGG INN](#)[Glemt passord?](#)

Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon
3. Administrere innlogging via egen IT avdeling (SAML)

Autentifikasjons alternativer med Plania



Autentifikasjons alternativer med Plania

1. Sette passord krav

Kundeprofil - Plania DEMO - STANDARD

Autentisering

Desktop

☒ Database ☒ Tillat Plania Launcher

☐ Active directory ☐ Kun Plania Launcher

Web

☒ Brukernavn/Passord ☐ SAML

Passord

Minimum antall karakterer i passord

☐ Må inneholde bokstaver ☐ Må inneholde tall

☐ Passord må være forskjellig fra tidligere passc

Sikkerhetslogg

Database level Slett etter x dage

Event level

2-faktor autentisering Token varer i x dager

OK Avbryt

plania

Kundeprofil

ADMINISTRASJON

AUTENTISERING

Desktop

☒ Database ☐ Active directory

☐ Bruk Single Sign On

☒ Tillat bruk av Plania Launcher

☐ Alltid bruk Plania Launcher

Web

☒ Planiaintern brukernavn og passord

☐ Saml

Tofaktor Autentisering

SMS-leverander [Opprett konfigurasjon](#)

For å aktivere tofaktor må SMS konfigurasjon opprettes, ta kontakt med Plania for hjelp til oppsett.

Tofaktor alternativ [Velg fra listen...](#)

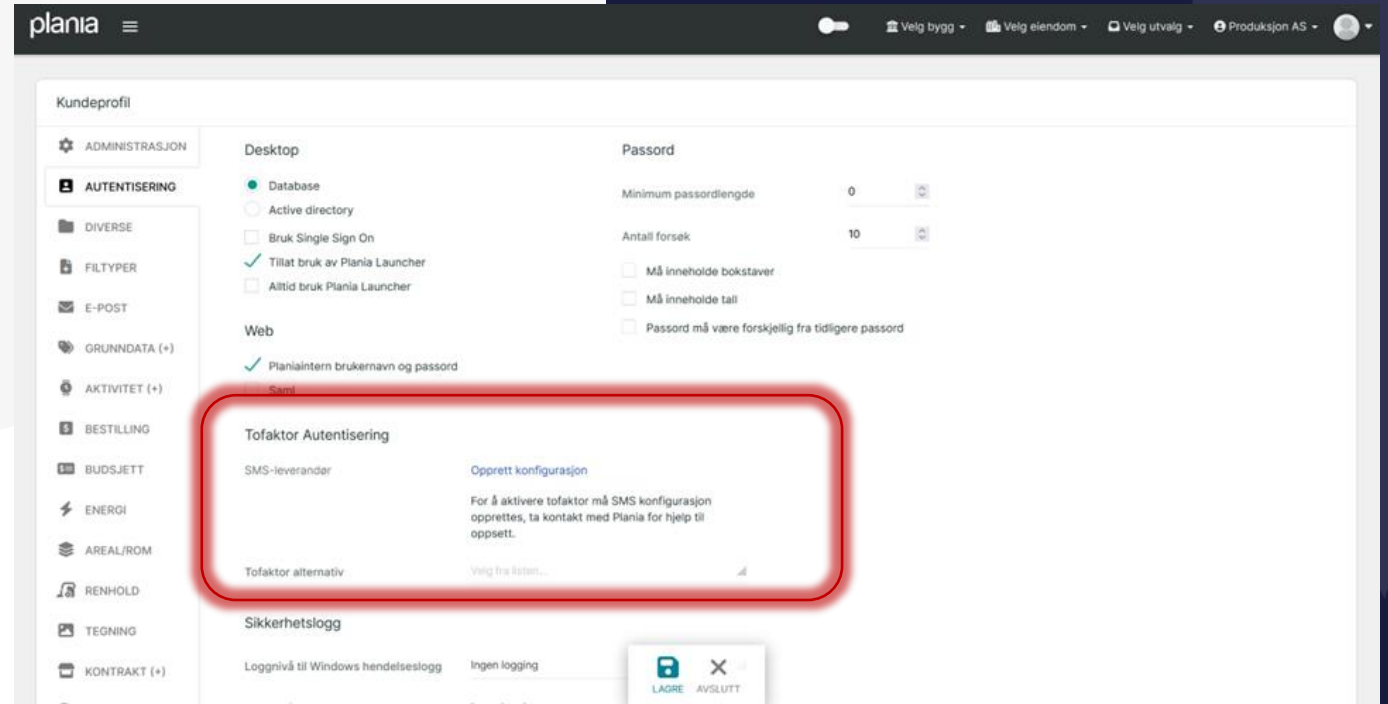
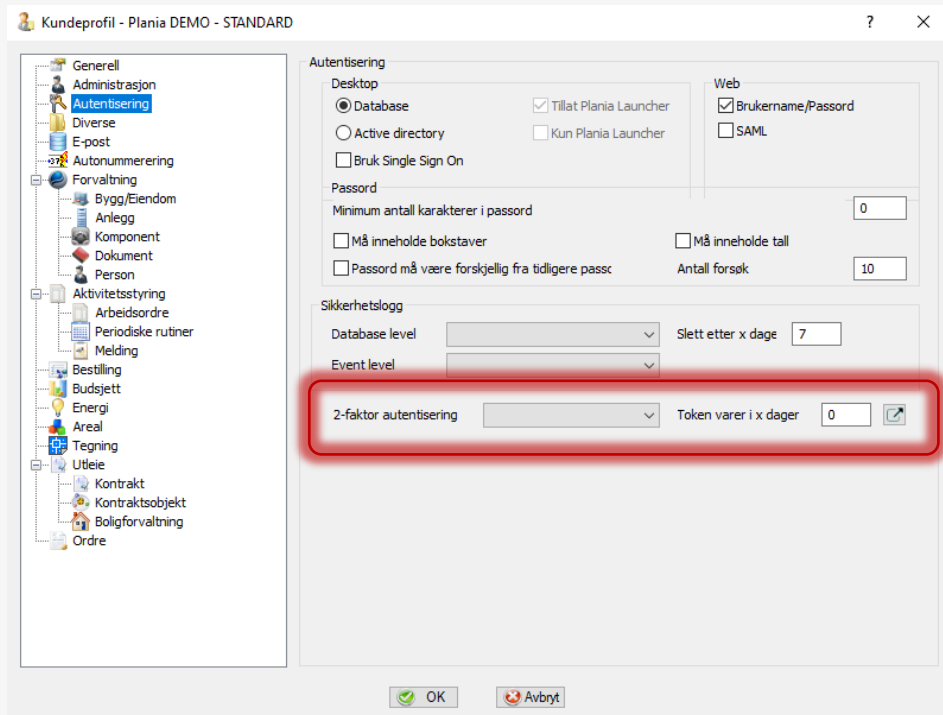
Sikkerhetslogg

Loggnivå til Windows hendelseslogg

LAGRE AVSLUTT

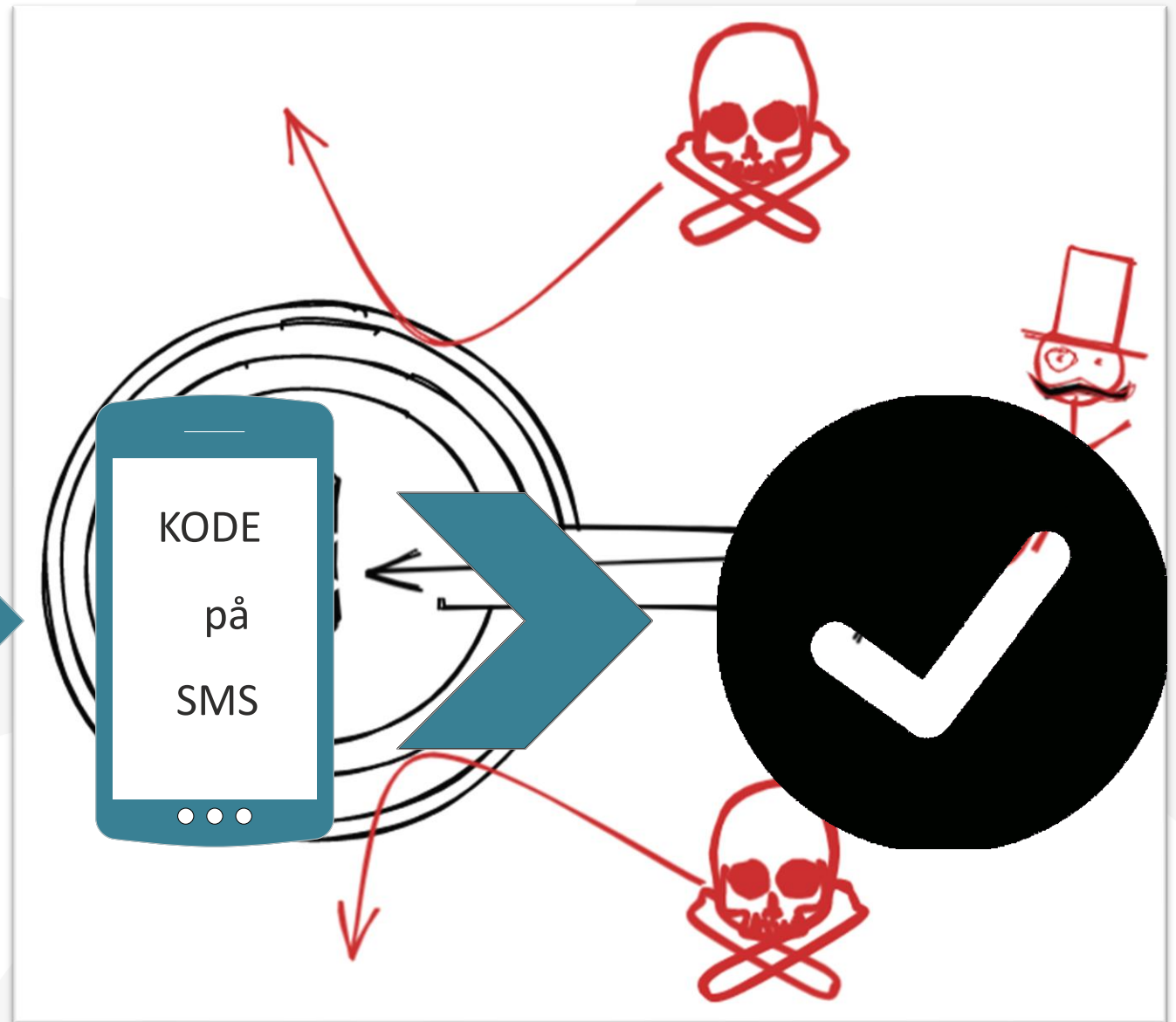
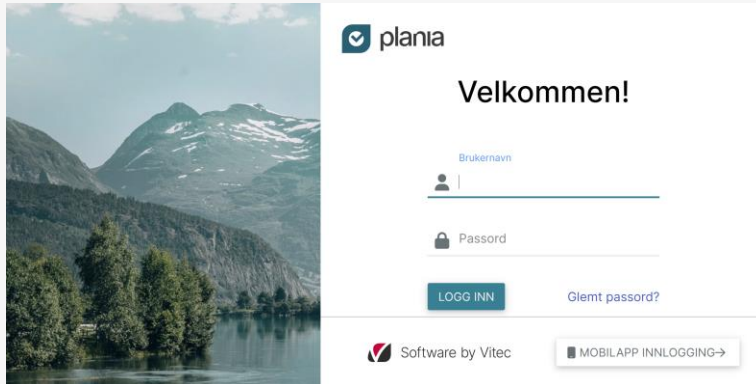
Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon



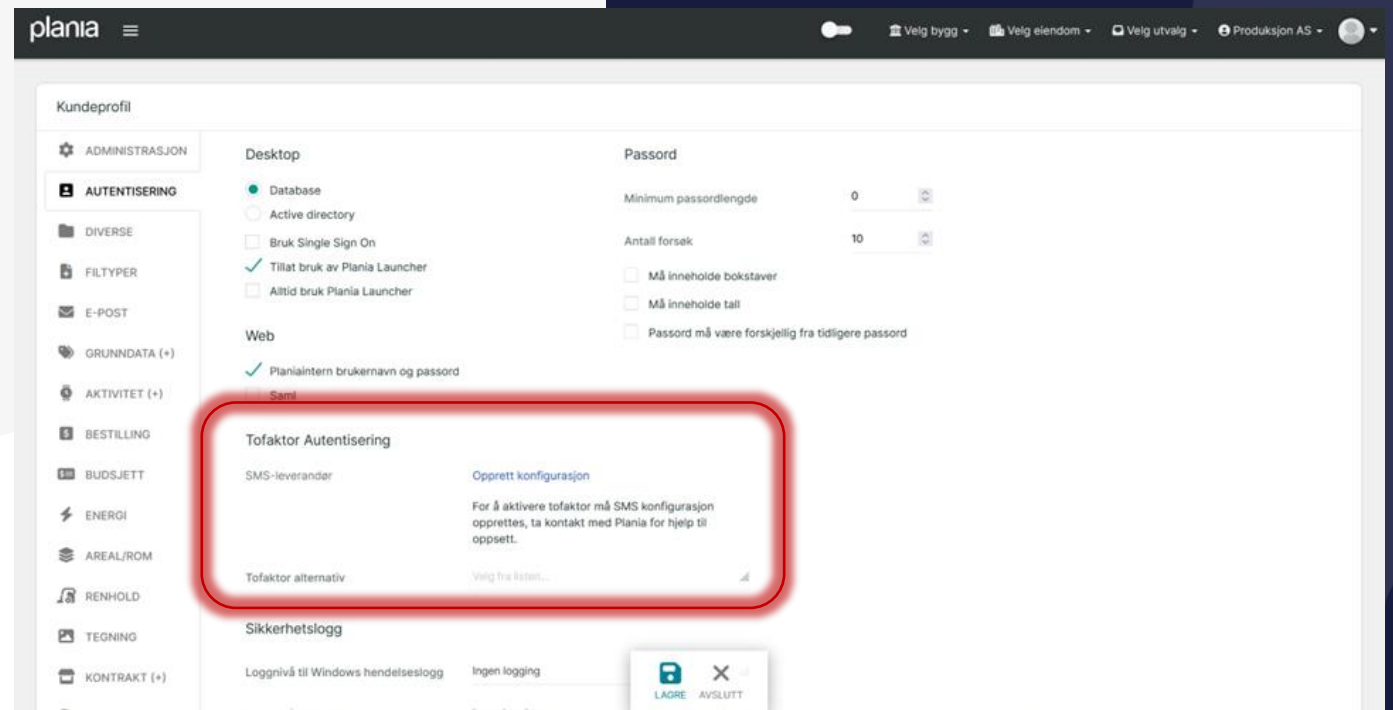
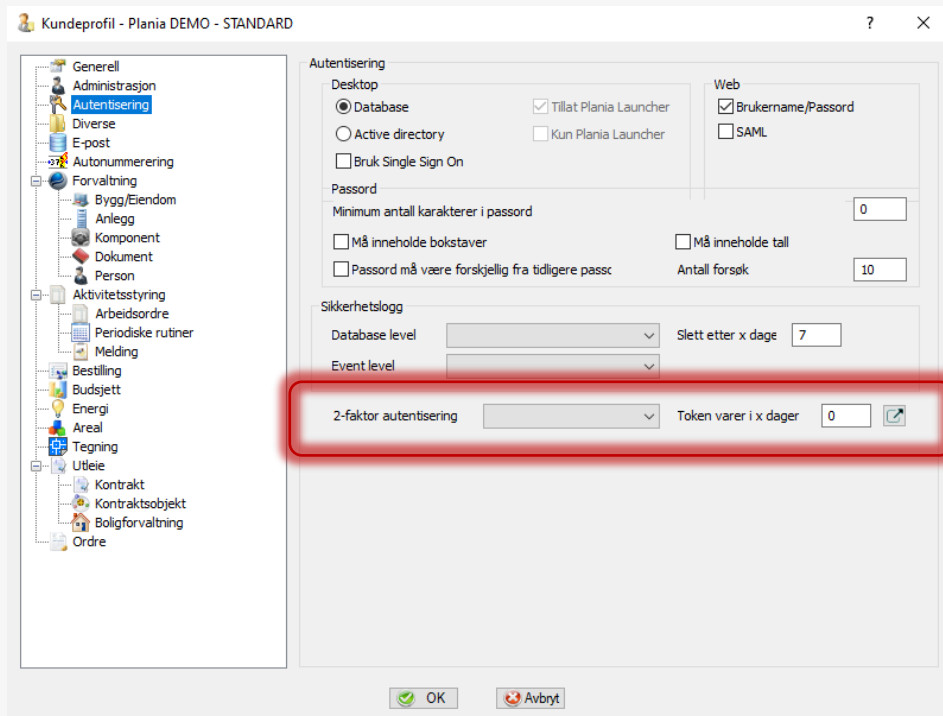
To-faktor autentisering

- Noe man vet (passord)
- Noe man har (kodebrikke, enhet)
- Noe man er (biometri)



Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon



Autentifikasjons alternativer med Plania

1. Sette passord krav
2. To-faktor autentifikasjon
3. SAML

Kundeprofil - Plania DEMO - STANDARD

Autentisering

Desktop

☐ Database ☒ Tillat Plania Launcher ☐ Bruk Single Sign On

☐ Active directory ☐ Kun Plania Launcher

Web

☐ Brukernavn/Passord ☒ SAML

Passord

Minimum antall karakterer i passord

☐ Må inneholde bokstaver ☐ Må inneholde tall

☐ Passord må være forskjellig fra tidligere pass

Sikkerhetslogg

Database level Slett etter x dager

Event level

2-faktor autentisering Token varer i x dager

OK Avbryt

plania

HOVEDMENY

Hjem

Grunndata

Vedlikehold

Arbeidsordrer

Avvik

Budsjett

Kostnader/fakturaer

Bestillinger

Bestillingsobjekter

Meldinger

Driftsmeldinger

Periodiske rutiner

Reservat

Kundeprofil

ADMINISTRASJON

AUTENTISERING

DIVERSE

FILTYPER

E-POST

GRUNNDATA (+)

AKTIVITET (+)

BESTILLING

BUDSJETT

Desktop

☒ Database

☐ Active directory

☒ Bruk Single Sign On

☒ Tillat bruk av Plania Launcher

☐ Alltid bruk Plania Launcher

Web

☒ Planiaintern brukernavn og passord

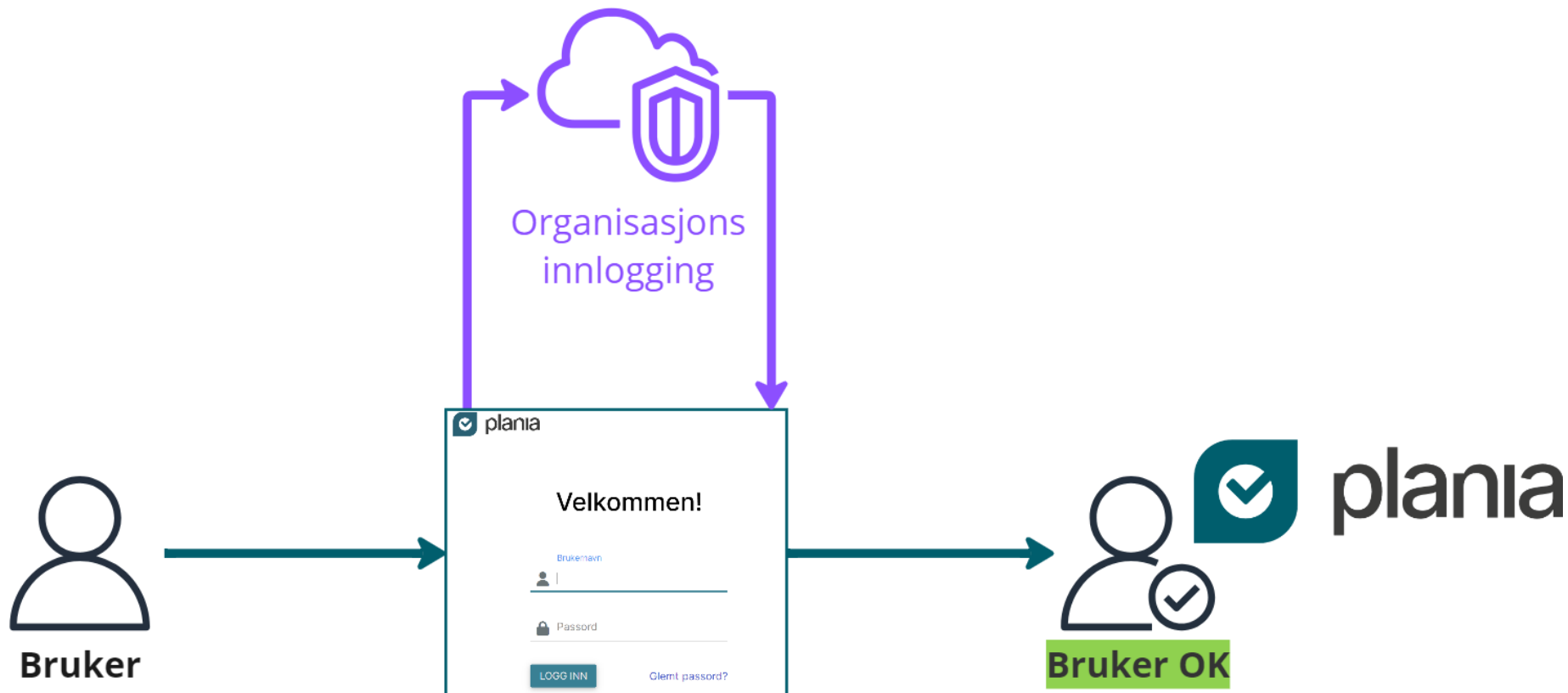
☒ SAML

☒ Single sign out

☐ Tving fersk pålogging

SAML

- Benytter din organisasjon tilgangsstyring.
- God sikkerhet, og enkelt for brukerne.
- Må ordnes gjennom organisasjonenes IT avdeling og Plania Support.



Oppsummering

- Generelt om data sikkerhet
- Passord
- Vitec Planias tiltak for sikkerhet
- Autentifikasjons alternativer med Plania

<https://kunde.plania.no/hc/no/articles/4758696472092-God-passordsikkerhet-i-systemet>

Spørsmål?



Espen Sigmundstad
Prosjektleder BIM