IN2120 – Informasjonssikkerhet

Brukerautentisering

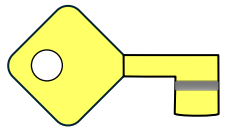
Janne Hagen



Universitetet i Oslo, høst 2026

Presentasjonsoversikt

- Autentikatorer for brukerautentisering



  - Noe du vet
    - Passord



  - Noe du har
    - Brikker og apper (f.eks. BankID)
    - Sekundære kanaler (f.eks. SMS og e-post)









  - Noe du er/gjør
    - Biometri



- Rammeverk for e-autentisering

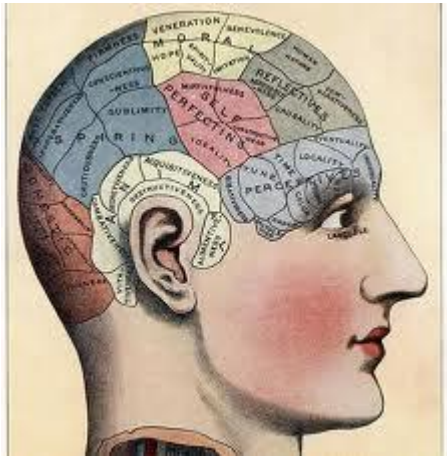
NIST National Institute of Standards and Technology U.S. Department of Commerce

Digdir

eIDAS

Kunnskapsbaserte autentikatorer

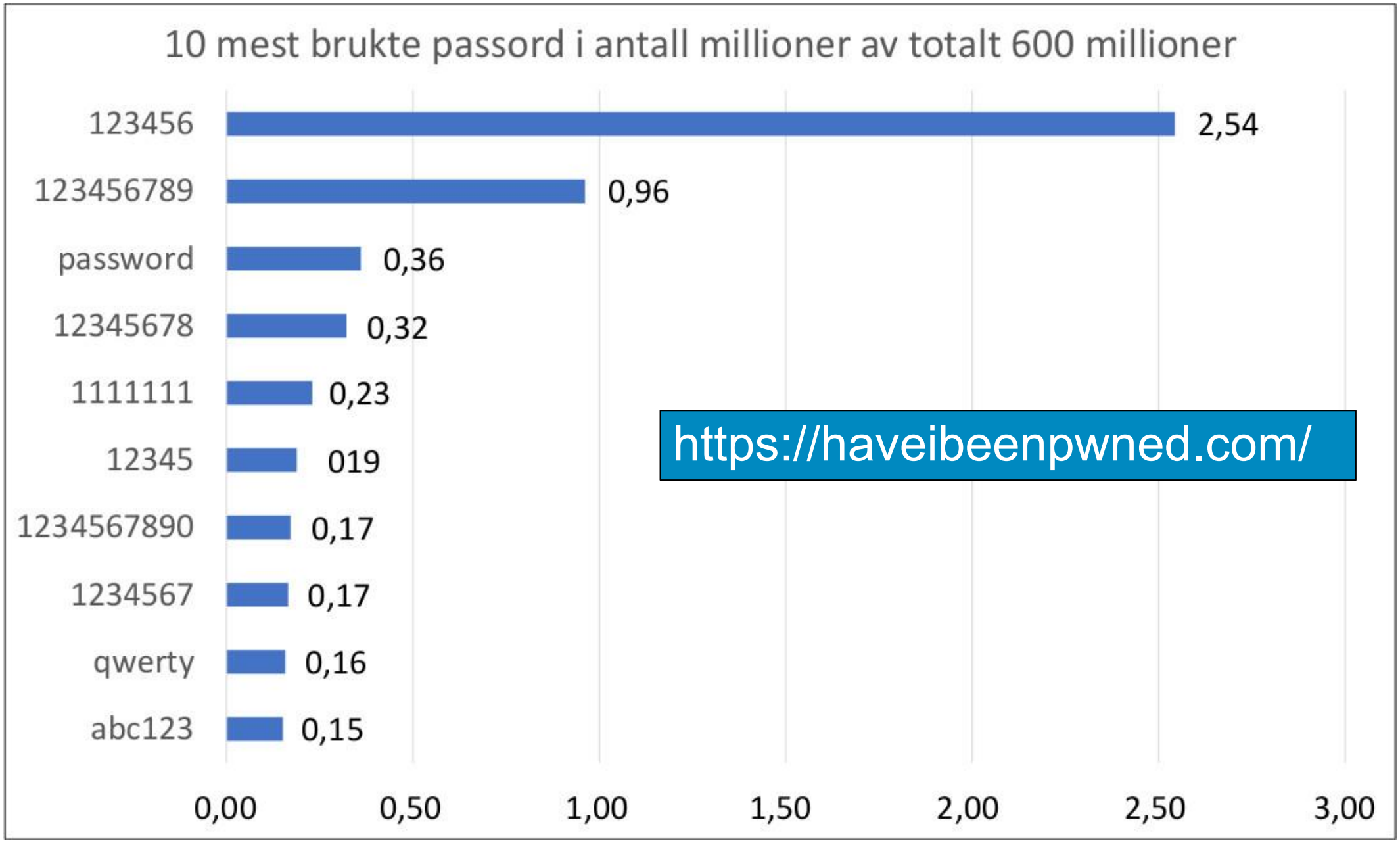
Noe du vet: Passord



Autentisering med statiske passord

123456

- Passord er den enkleste og vanligste autentikator
  - Noe brukeren vet
- Problemer:
  - Lett å dele (med vilje eller ikke)
  - Lett å glemme (kan bli belastning for help-desk)
  - Ofte lett å gjette (med kraftige cracke-verktøy)
  - Kan skrives ned (som er både bra og ikke bra)
  - Hvis nedskrevet, så er "det du vet" "hvor du finner det"
  - Forblir ofte i dataminnet og cachen, kan stjeles av skadevare


10 mest brukte passord i antall millioner av totalt 600 millioner
123456
2,54
123456789
0,96
password
0,36
12345678
0,32
1111111
0,23
12345
019
1234567890
0,17
1234567
0,17
qwerty
0,16
abc123
0,15
0,00
0,50
1,00
1,50
2,00
2,50
3,00
https://haveibeenpwned.com/

Råd om sikker håndtering av passord

- Passordlengde $\geq$ 13 tegn
- Bruk flere kategorier tegn
  - store, små, tall, spesialtegn
- Ikke bruk vanlige ord (fra ordbok), navn, dato, årstall, eller sekvensielle tall
- Endring av passord
  - Normalt sjelden ($\geq$ 2 år) eller aldri.
  - Umiddelbart ved mistanke om kompromittering eller hvis konto eksponert (haveibeenpwned.com/)
- Ikke gjenbruk
  - eller bare mellom kontoer med svært lav sensitivitet
- Oppbevar passord sikkert
  - i hodet
  - på papir, hvis du passer godt på papiret
  - i (online) passordbank (eng. password manager)
  - alltid kryptert i online digital enhet
  - kan lagres i klartekst i offline digital enhet

Lagring av passord i systemer/nettverk

- Linux/Unix: /etc/shadow –filen lagrer password. Tidligere versjon lagret den i /etc/passwd
  - Tekstformat
  - Må ha root-tilgang for å lese / endre
- Windows: Passord lagres lokalt i SAM-databasen (Security Account Manager) \windows\system32\config\sam
  - NTLM-format. Kun admin har tilgang.
  - Må ha admin-tilgang for å lese / endre
- Lagring av passord i nettverksmiljøer
  - AD (Active Directory) i Windows
  - Entra ID i Microsoft Azure (online versjon av AD)
  - LDAP app (Lightweight Directory Access Protocol) i Linux





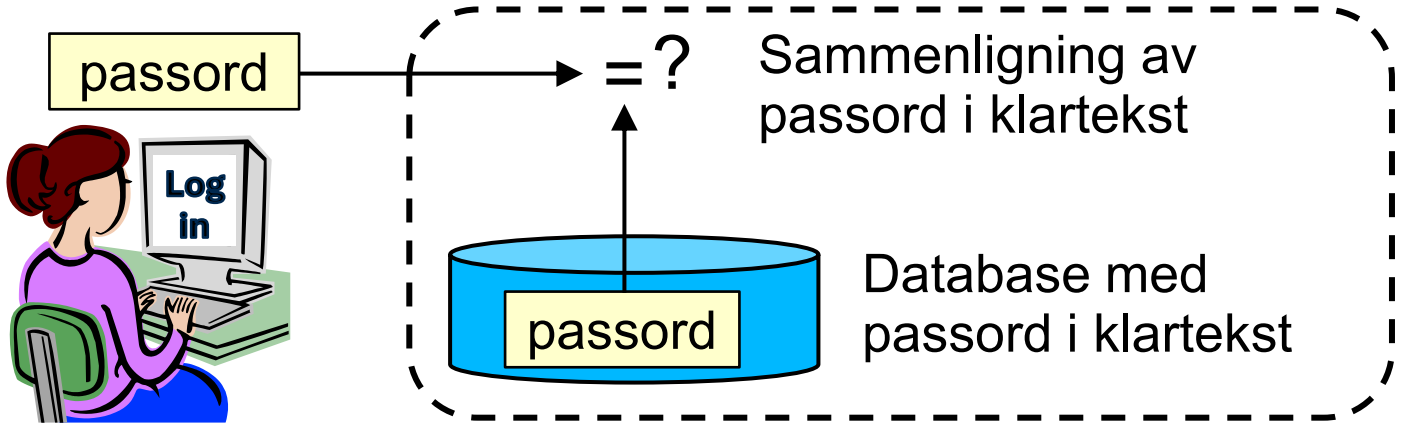






Database med passord i klartekst: Svak sikkerhet

- Database med passord i klartekst er en enkel løsning for autentiseringstjenere, der passord mottatt fra bruker sammenlignes med lagret passord.
- Men det er også en usikker løsning.
- Det er ikke uvanlig at passorddatabaser stjeles/lekkes, og hvis det skjer er alle passordene direkte tilgjengelig

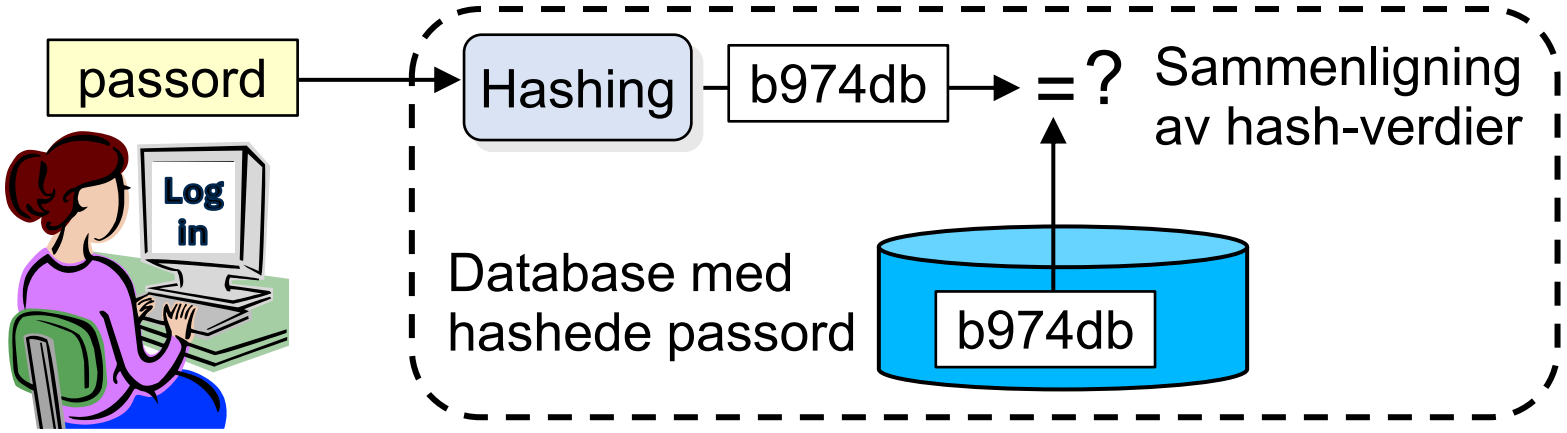




Svak sikkerhet ved lekket database.
Alle passord er direkte tilgjengelig.

Database med hashede passord: Moderat sikkerhet

- Database med hashede passord betyr at passord mottatt fra bruker må hashes før det sammenlignes med det lagrede hashede passordet.
- I tilfelle stjålet/lekket database er ikke passord direkte tilgjengelig i klartekst.
- Dette gir moderat sikkerhet, men kraftige cracke-verktøy kan brukes for å gjenfinne relativt svake passord i databasen.







Moderat sikkerhet ved lekket database.
Cracking krever en viss regnekraft.

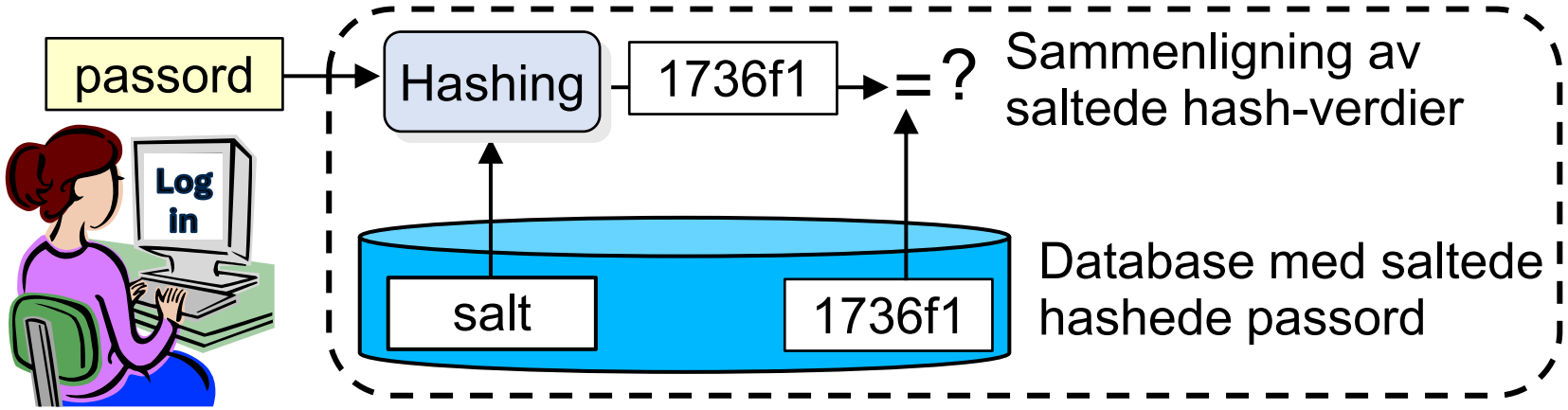
Passord-cracking av stjålede passord-databaser

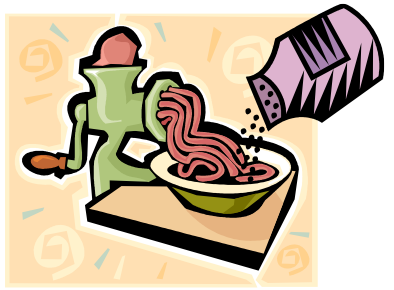


- Brute Force
  - Prøv alle mulige tegnkombinasjoner for å finne riktig hash
- Intelligent søk for å finne riktig hash
  - Brukernavn
  - Navn på venner / slektninger
  - Telefonnummer
  - Fødselsdatoer
  - Ordbokangrep
    - Prøv alle ord fra en ordliste
  - Forhåndsberegnede hash-tabeller og rainbow-tabeller

Database med saltede hashede passord: God sikkerhet

- Database med saltede hashede passord betyr at passord kombineres med et tilfeldig tall (salt) før det hashes og lagres i databasen. Saltet lagres også.
- Passord mottatt fra bruker må hashes sammen med saltet før det sammenlignes med det lagrede saltede hashede passordet.
- I tilfelle stjålet/lekket database kreves stor regnekraft for å cracke passord.
- Dette gir god sikkerhet, og regnes som standard praksis for passorddatabaser.

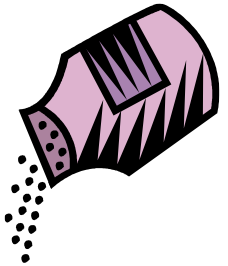






God sikkerhet ved lekket database.
Cracking krever stor regnekraft.

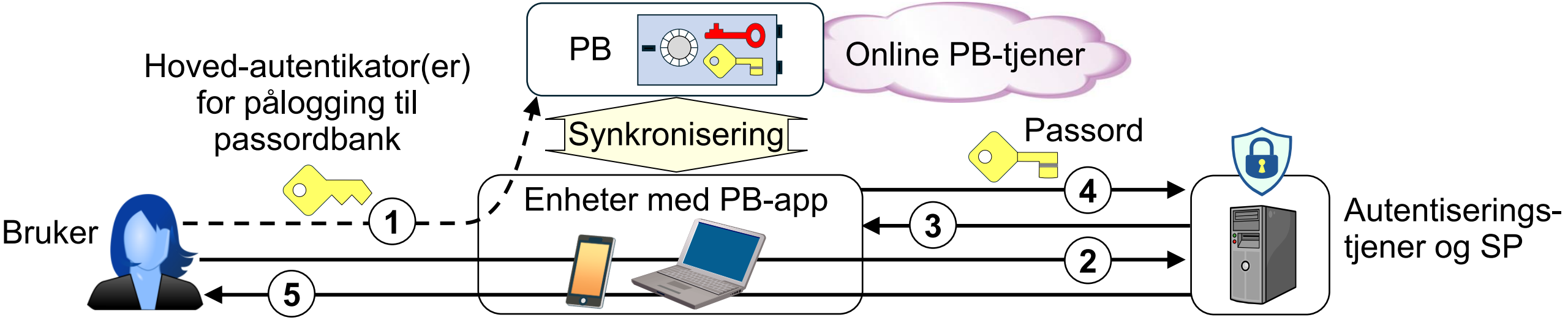
Passord-salting:
Forsvar mot passord-cracking



- Tilføy tilfeldige data (salt) til brukerens passord før det hashes
  - I Linux: et tilfeldig valgt heltall fra 0 til 4095.
  - Ulike salt for hver bruker
  - Forskjellig salt gir forskjellige hash for like passord
- Forhindrer at brukere med identiske passord har samme passord-hash-verdi lagret i databasen
- Gjør det praktisk umulig for angripere å bruke hash-tabeller og rainbow-tabeller
  - De måtte generere en hash-tabell for hver mulig saltverdi
  - Passord over 8 tegn gir tabellstørrelse over Petabyte

Passordbanker (Password Managers)

- **Innebygd i OS.** For eksempel, på Apple-enheter, er Keychain en innebygd, slik at brukere ikke trenger å laste ned eller installere noen separat app.
- **Innebygd i nettleser.** Firefox og Chrome har innebygde passordbanker som lar brukere lagre passord for ulike nettsteder, og generere sterke passord.
- **Tredjeparts passordbanker.** Dedikert programvare kombinert med online lagring, som krever at brukere installerer en app eller en nettleserutvidelse.



Eierskapsbasert autentisering

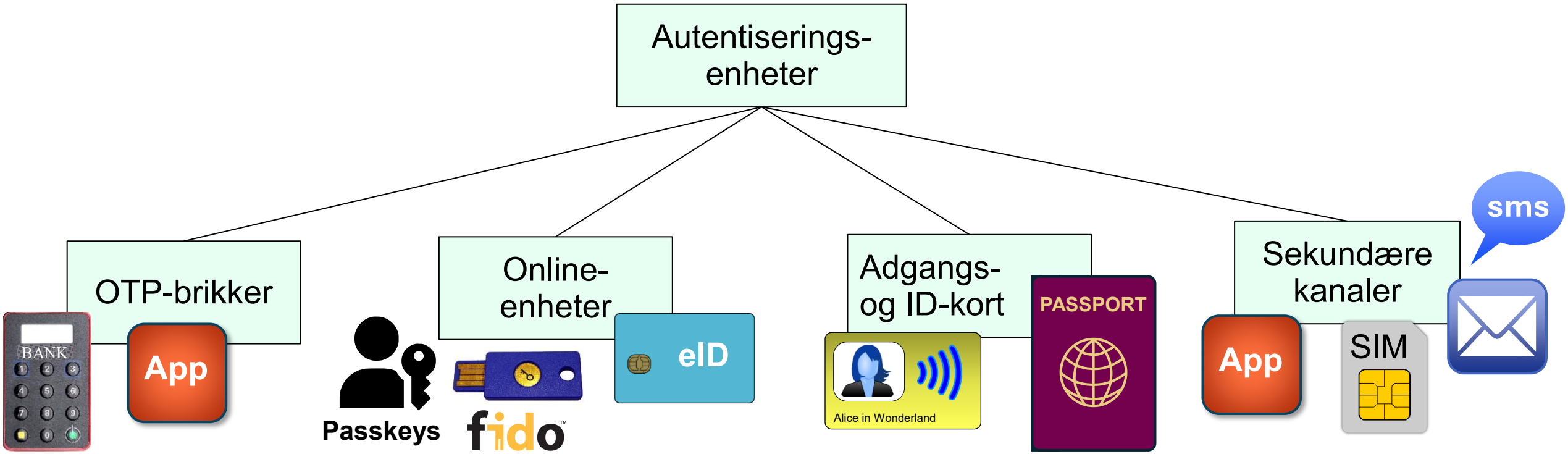
Noe du har: Enheter







Typer av autentiseringsenheter



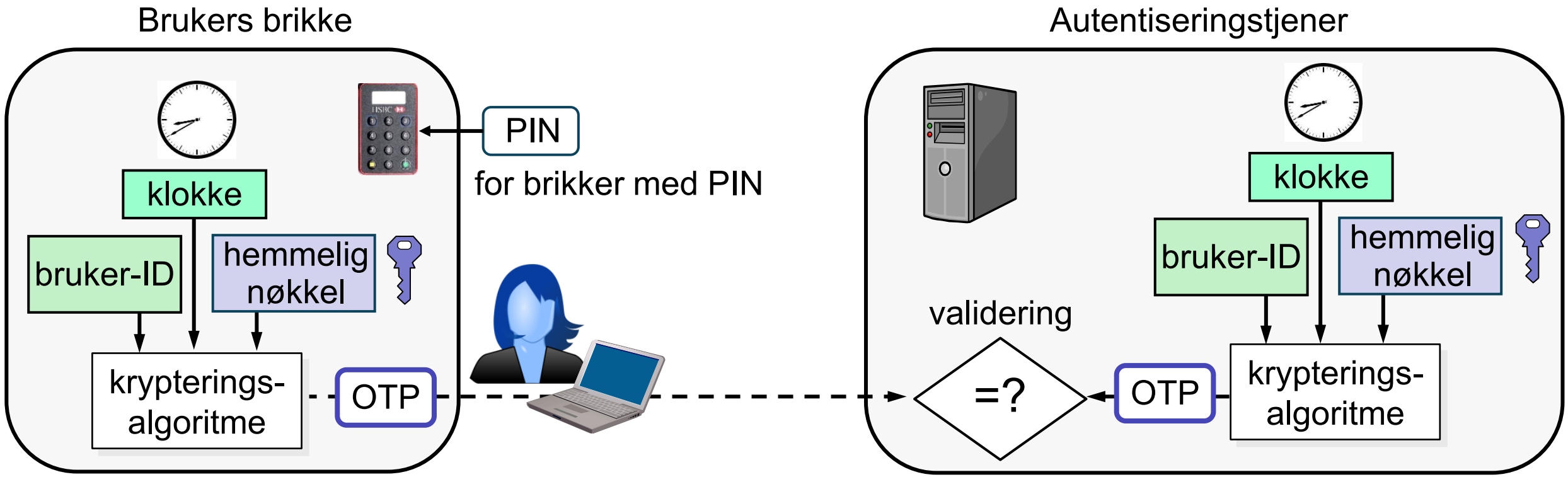
OTP-brikker (One-Time-Password):



- Brikken inneholder en klokke
- Viser tidsavhengig kode (engangskode) på skjermen
  - Bruker kopierer kode til terminal for å logge på
- Hver kode er gyldig for et bestemt tidsvindu
- Koder fra nære nabo-tidsvinduer aksepteres
- Klokkene må alltid være synkrone
  - Trenger strøm på batteri
- Eksempel: BankID og SecurID

Diagram

Synkron OTP-brikke, med klokke (og PIN) f.eks. Bank-ID



Tidsbaserte OTP-kodebrikker:



SafeID OTP-brikke med PIN



ActiveID OTP-brikke med PIN



BankID OTP-brikke med PIN



Feitan OTP-brikke uten PIN



RSA SecurID uten PIN



BankID OTP brikke uten PIN

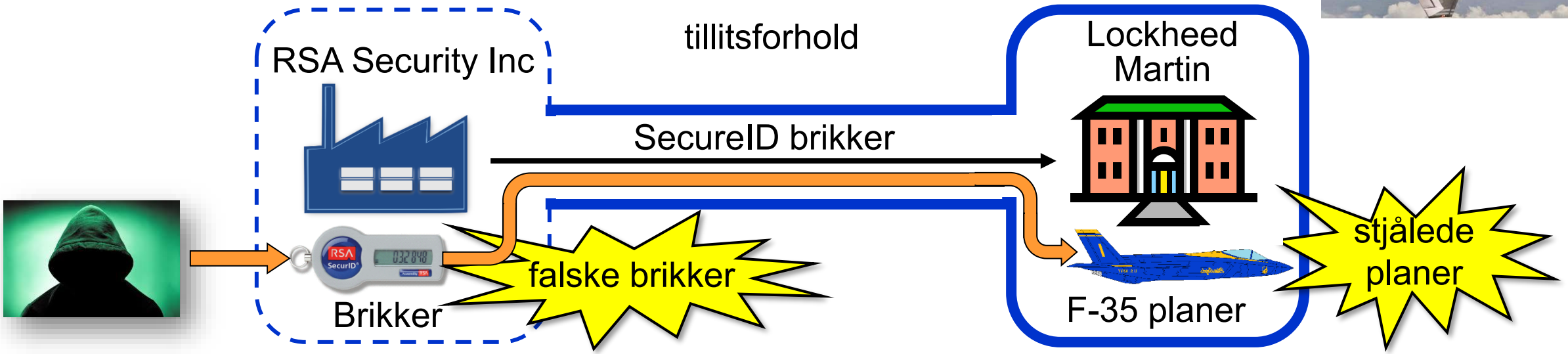
Leveransekjedeangrep: Hacking av kodebrikke



- RSA Security Inc. ble hacket i 2007, hackerne stjal hemmelig info for å designe SecureID-brikker
- Hackerne laget falske SecureID-brikker for ID-tyveri
- Virksomheter som brukte RSA SecureID var sårbare
- Lockheed Martin brukte RSA SecureID
- Kinesiske angripere begikk ID-tyveri mot Lockheed Martin -ansatte
  - Stjal planer for F-35 jagerfly







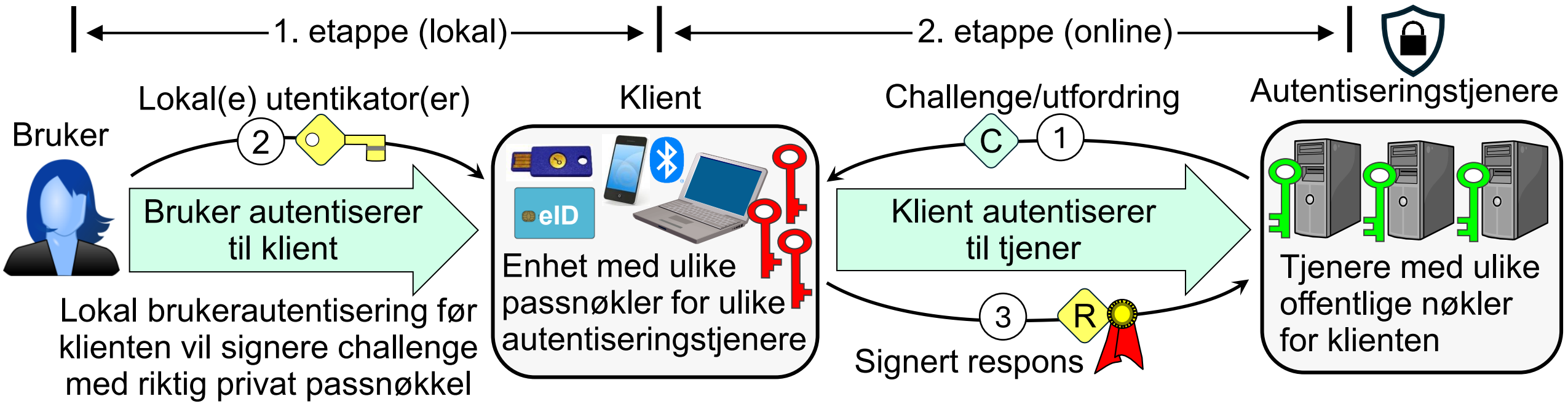
Phishing-resistent autentisering



- Phishingangrep utnytter at brukeren ikke forstår falske nettsteder.
  - ID-spoofing skjer hvis falske nettsteder får tak i autentikatorer
- Autentiseringsordningen som ikke er phishing-resistente avhenger av at **brukeren** forstår domenenavn, kjenner og sjekker domenenavn til nettsteder
  - Mange brukere forstår ikke domenenavn, og/eller kjenner ikke domenenavn til ekte nettsted
  - Domenenavn kan være villedende, slik at selv eksperter blir forvirret
- Vanlige autentiseringsbrikker og -apper (f.eks. BankID) er ikke phishing-resistente.
  - Fordi mange brukere ikke forstår domenenavn, og dermed blir lurt av falske nettsteder.
- Allmenopplæring forteller ikke folk hvor ekstremt viktig det er å forstå domenenavn.
- Phishing-resistens forhindrer at autentikator(er) kan bli utnyttet av falske nettsteder.
- Phishingsresistent autentisering krever at **klient** sjekker domenenavn til nettsted
  - Domenenavn er integrert som del av private passnøkler (autentikatorer) lagret på klienten
  - Klienten blokkerer autentisering til falsk nettsted, fordi domenenavnet ikke fins i lagrede nøkler
  - Passnøkler skaper kompleksitet for gjenoppretting av konto og synkronisering mellom enheter

Autentisering med Passnøkler, FIDO og WebAuthn

- Klient/brikke autentiserer seg på brukerens vegne til en autentiseringstjener.
- Passnøkler kan være lagret:
  - innebygd i klient (smarttelefon eller en laptopp), i nettleser, OS eller maskinvare
  - i en brikke (USB-brikke eller smartkort) koblet til klientplattform fysisk, eller via NFC eller blåtann
  - online i en passordbank (eng. password manager/wallet)
- Klienten krever å autentisere brukeren lokalt før den foretar online-autentisering.
- Phishing-resistent, fordi passnøkler inneholder autentiseringstjeners domenenavn.



Autentisering med passnøkler (Passkeys)

- En passnøkkel (eng. passkey) er en kryptografisk privat nøkkel.
- En passnøkkel er på mange måter som et passord.
- Passordbanker støtter passnøkler.
- Brukerklienten/brikken lagrer separate passnøkler for ulike autentiseringstjenere.
- Passnøkler vil antagelig oftest lagres innebygd i klienten, i stedet for i separat brikke.
- Hver passnøkkel inneholder domenenavn for en spesifikk autentiseringstjener.
- Klienten krever at autentiseringstjenerens domenenavn stemmer med passnøkkelen.
- Brukeren kan ikke overstyre klienten til å signere challenge fra falske nettsider.
- Mobil plattform kan støtte passnøkkel-autentisering via laptop med blåtann-tilkobling.

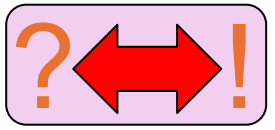


Fordeler og utfordringer med passnøkler/FIDO/WebAuthn

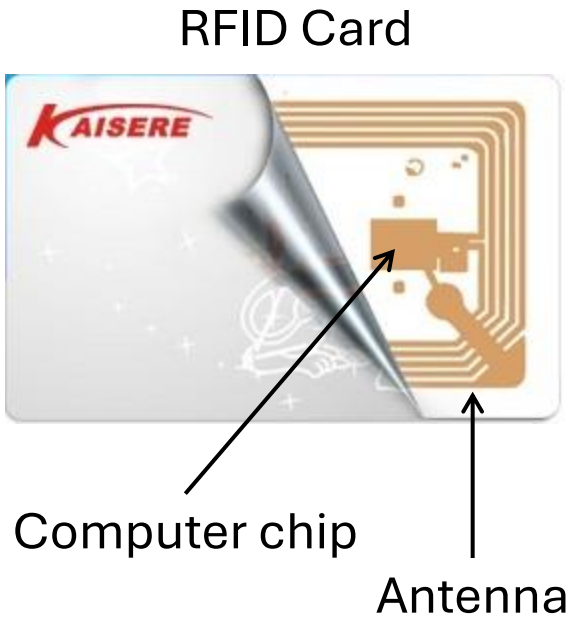


- Fordeler
  - Passnøkler/FIDO/WebAuthn gir phishingresistent autentisering
  - Private nøkler lagret i plattform/enhet er spesifikke for IdP-ens domenenavn, som betyr at plattformen/enheten ikke finner passnøkkel for falsk nettsider.
  - Brukeren slipper å håndtere passord
- Utfordringer
  - Det kan være teknisk komplisert å synkronisere (overføre) passnøkler til ny plattform/enhet ved utskifting eller tap av plattform/enhet.
  - Synkroniseringsløsninger for passnøkler er basert på lagring av i skyen, f.eks:
    - egen passordbank
    - passnøkkelbank kontrollert av produsenten for platform/enhet
  - Tilgang til passnøkler i skyen krever til syvende og sist tradisjonell autentisering med passord eller andre autentikatorer, som ikke er phishing-resistent.
  - Ordninger med passnøkler er vanskelig å forstå for vanlige brukere.

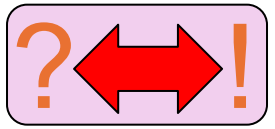
Adgangskort, ID-kort og pass



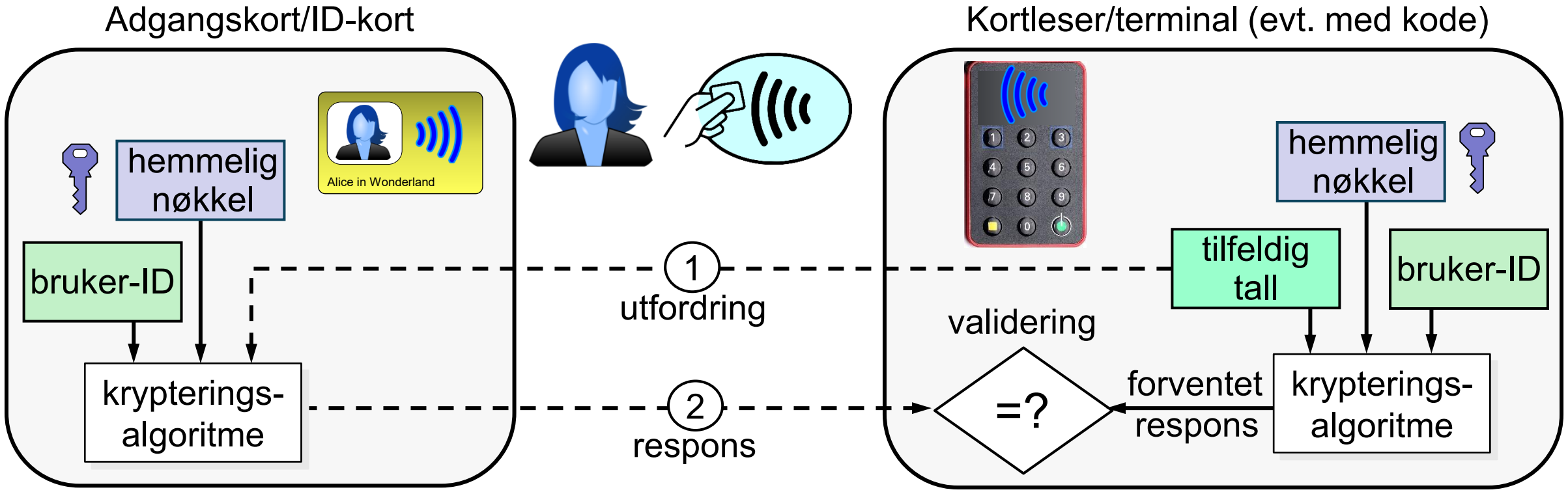
- Kontaktløse kort, også kalt RFID (Radio Frequency Id), består av en computer-chip og en antenne.
  - trenger ikke fysisk kontakt med leser
  - kommuniserer via radiosignaler
  - strøm generert av magnetfelt fra leser
  - utenfor leserens rekkevidde får kortet ingen strøm og forblir inaktivt
  - batteridrevne RFID-brikker finnes også
- Egnet for bruk i varme, kalde, skitne og fuktige omgivelser



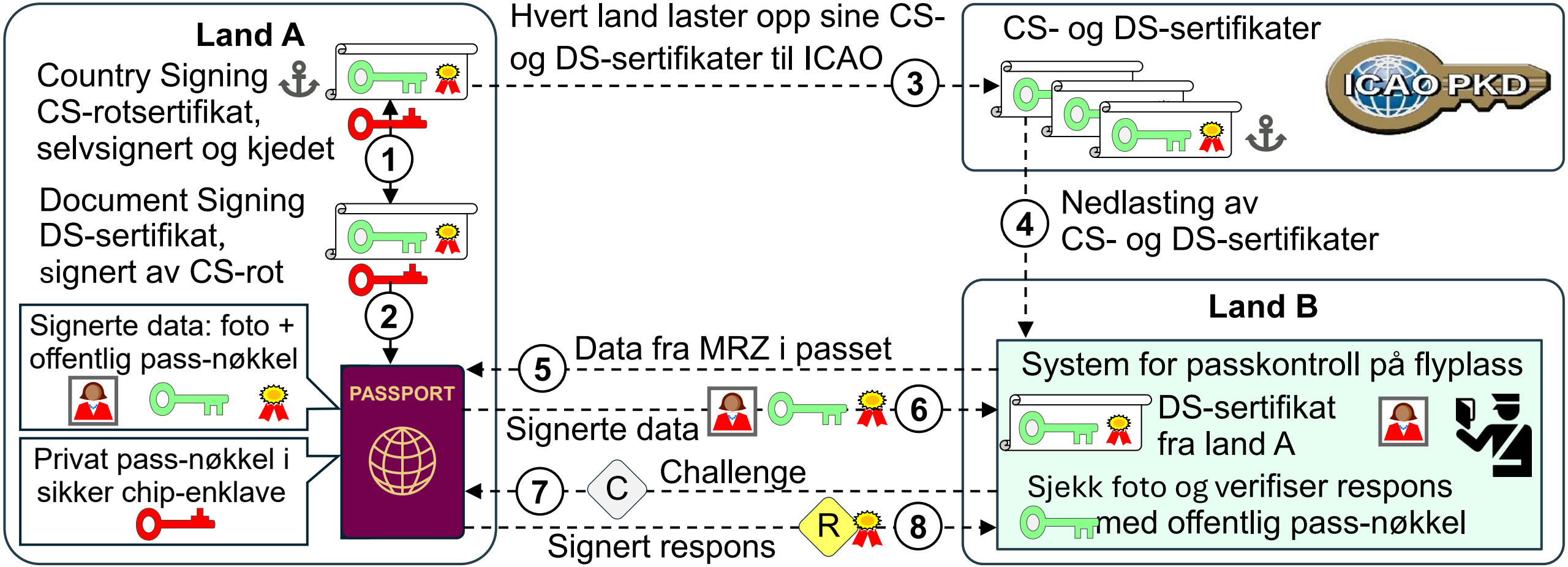
Adgangskort, ID-kort



- Eksempel adgangskort med symmetrisk nøkkel
- Nasjonalt ID-kort og pass bruker asymmetrisk nøkkel

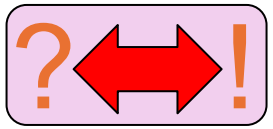


Autentisering med pass



- ICAO: International Civil Aviation Authority

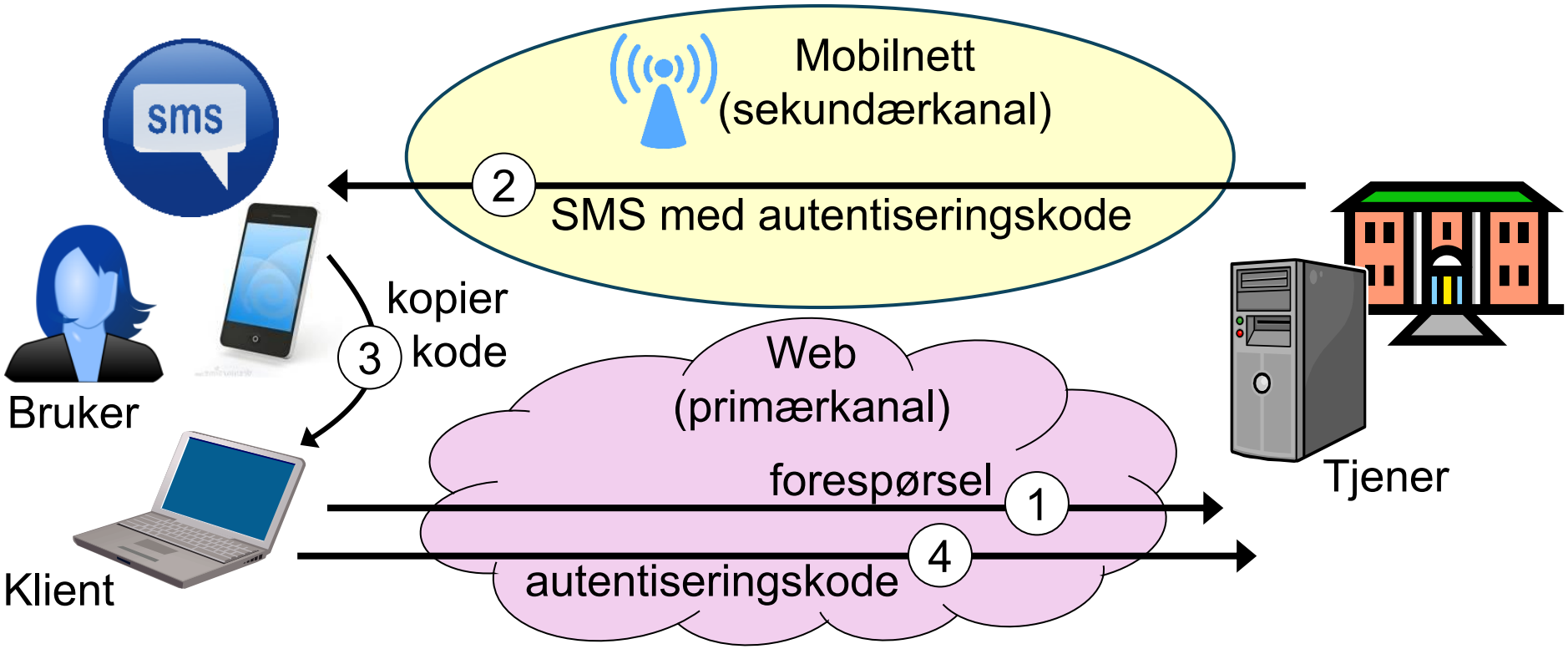
Autentisering med sekundære kanaler



- Hvis web-kommunikasjon betraktes som en primærkanal, kan autentisering skje via andre sekundære kanaler:
- Eksempel sekundære er f.eks.:
  - SMS
  - App
  - e-post
  - SIM (tidligere bruk for Bank-ID på mobil)

- Noen sekundære kanaler er sikrere enn andre.
  - SMS regnes som relativt svak, fordi SMS relativt lett kan stjeles
  - Bank-ID app benytter en app på mobiltelefon som sekundærkanal

Autentisering med sekundære kanaler



Egenskap-basert autentisering

Biometri







Noe du er





Noe du gjør

Biometri intro



- Hva er det?
  - Automatiserte metoder for å verifisere eller gjenkjenne en person basert på fysiologiske egenskaper.
- Biometriske modaliteter, eksempler:
  - fingeravtrykk
  - ansiktsgjenkjenning
  - øye retina / iris skanning
  - håndgeometri
  - håndsignatur
  - stemme/tale-karakteristikk
  - tastetrykk dynamikk

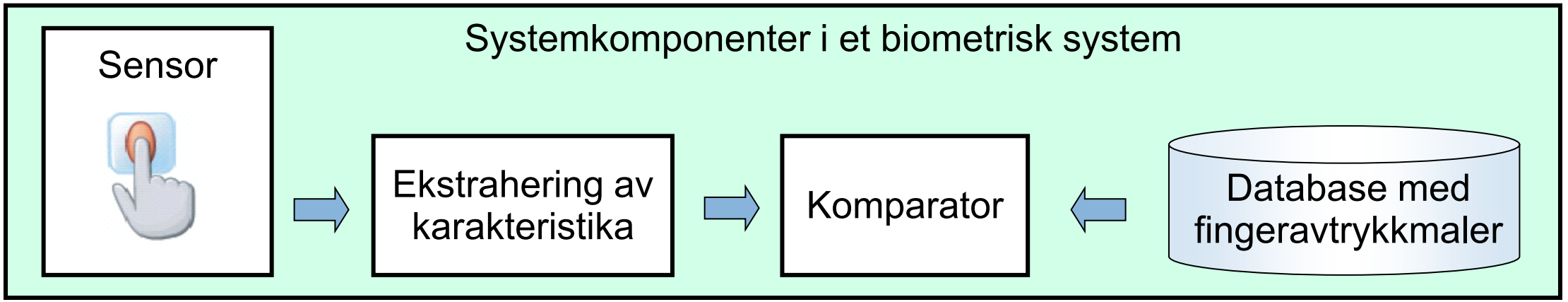
Krav til biometriske modaliteter



- Universalitet:
  - Hver person skal ha modaliteten
- Særpreg:
  - Ulike personer skal være tilstrekkelig forskjellige med hensyn til karakteristikker ved modaliteten;
- Permanens:
  - Karakteristikken skal holde seg uendret (med hensyn til kriterier for sammenligning) over tid;
- Målbarhet:
  - Karakteristikken skal være lett å innhente og måle på en kvantitativt måte.
- Nøyaktighet:
  - Nøyaktighet til et biometrisk system, uttrykt som EER (Equal Error Rate).
- Ytelse:
  - hastigheten på analysen, ressursene som kreves for å oppnå ønsket hastighet,
- Aksept:
  - i hvilken grad folk er villige til å akseptere bruken av en bestemt biometrisk modalitet
- Beskyttelse mot forfalskning:
  - Vanskelighetsgrad av å lure det biometriske systemet

Biometri: Systemkomponenter

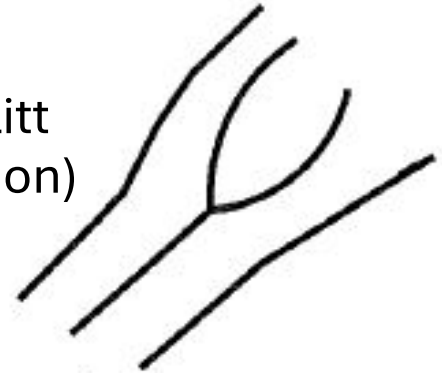




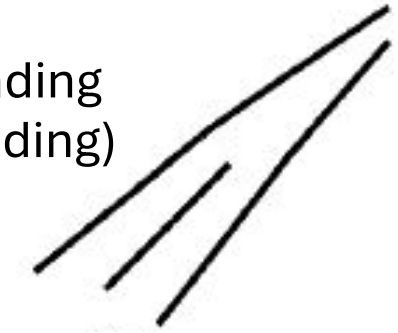
Ekstrahering av karakteristikker (features)

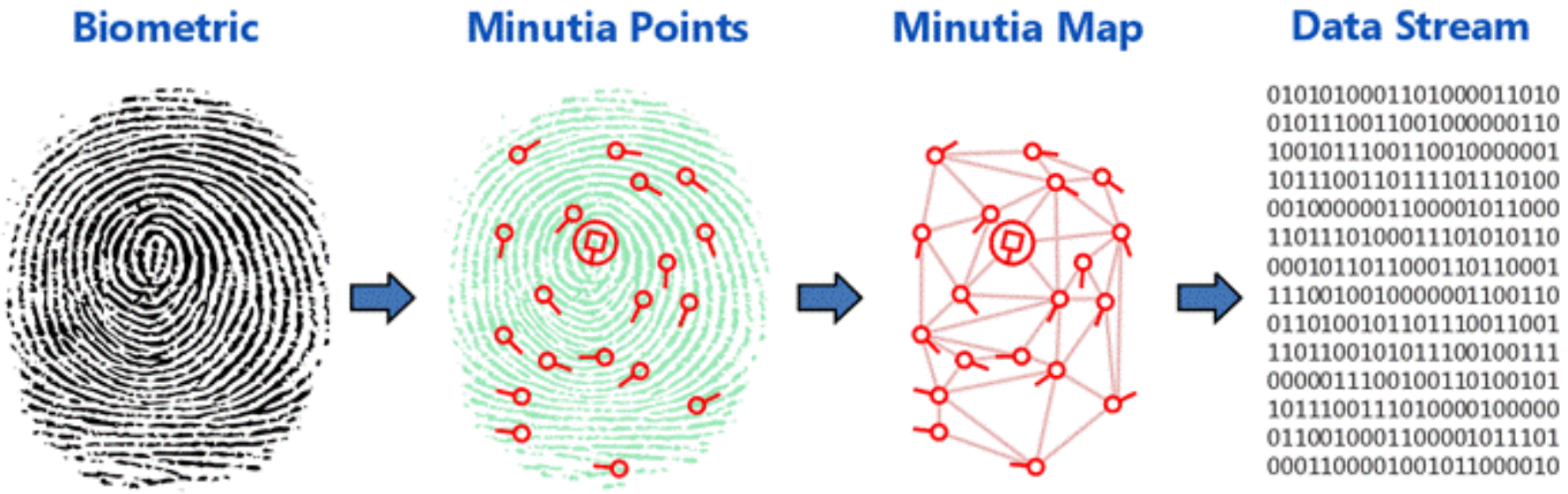
Eksempel: Ekstrahere minutia fra fingeravtrykk

Linjesplitt
(bifurcation)



Linje-ending
(ridge ending)



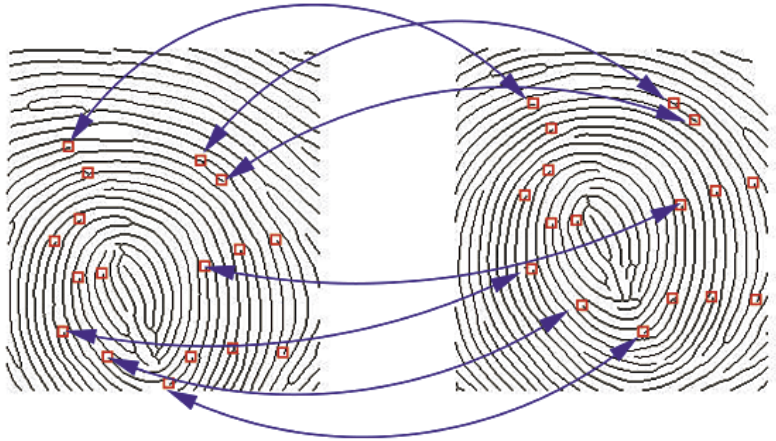


Biometri: Operasjonsmoduser



- Registrering:
  - analog innhenting av brukeres biometriske karakteristika.
  - behandling av innhentede prøve for å generere en mal for brukeres karakteristika som lagres for senere bruk.
  - database med biometriske maler
- Identifikasjon (1:N, en-til-mange)
  - innhenting av ny biometrisk prøve fra kandidat-person(er)
  - søk i databasen med lagrede maler for et treff basert utelukkende på innsamlede prøve(r).
- Autentisering (1:1, en-til-en):
  - Innhenting av ny biometrisk prøve fra bruker for autentiseing
  - sammenligning av ny prøve med brukerens lagrede mal

Sammenligning av prøver:



- Karakteristika fra innhentede prøver sammenlignes med karakteristikker fra lagret mal
- Ofte basert på klassifisering med maskinlæring
- Sammenligningen gir skåring *S*
  - Jo større likhet, desto høyere skåring *S*
- Terskelverdi *T* avgjør om prøven gir *match (treff)*
  - *match* (antatt riktig person) er når $S \geq T$
  - *non-match* (antatt feil person) er når $S < T$

Sammenligning av prøver

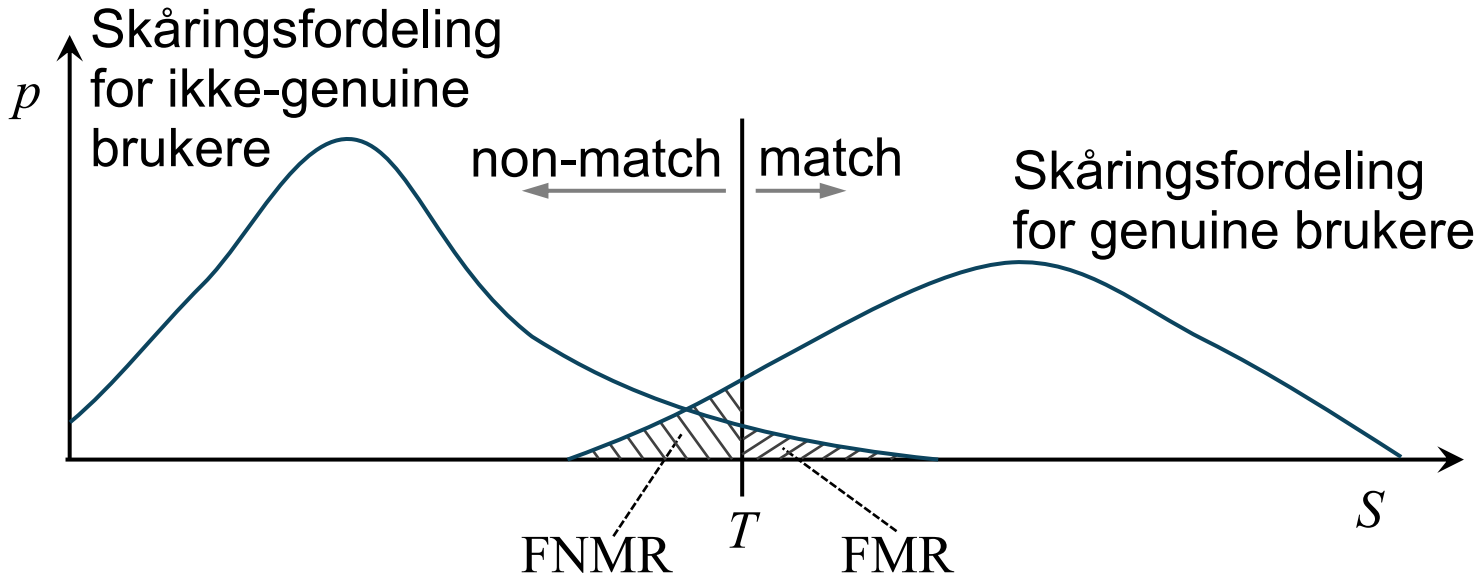


- Sann positivt
  - *match av genuin prøve* → genuin bruker godtas
- Sann negativt
  - *non-match av ikke-genuin prøve* → ikke-genuin bruker avvises
- Falske positive
  - *match av ikke-genuin prøve* → ikke-genuin bruker godtas
- Falske negativer
  - *non-match av genuin prøve* → genuin bruker avvises
- Falsk-match-rate og Falsk-Non-match-rate
  - FMR = (*# match av ikke-genuine prøver*) / (*totalt # ikke-genuine prøver*)
  - FNMR = (*# non-match genuine prøver*) / (*totalt # genuine prøver*)
- Terskel *T* bestemmer balanse mellom FMR og FNMR

Nøyaktighet: Skille mellom genuine og ikke-genuine brukere

- Plot fordelingene av skåringer *S* fra et utvalg av genuine og ikke-genuine brukere
- Terskelen *T* bestemmer relativ størrelse på FMR og FNMR
  - Lav *T* gir stor FMR, dermed lav sikkerhet, men liten FNMR og dermed god brukervennlighet
  - Høy *T* gir liten FMR, dermed høy sikkerhet, men stor FNMR og dermed dårlig brukervennlighet
- «Rate» (ekvivalent med prosentandel) er relativ størrelse på de skraverte arealene
- Når terskel *T* er justert slik at FMR = FNMR kalles raten for EER (Equal Error Rate)
- Liten EER gir høy nøyaktighet

- Lite overlapp mellom kurvene gir liten EER
- Alle biometrisystemer har mer eller mindre overlappende kurver



Forfalskning av biometri: Presentasjonsangrep

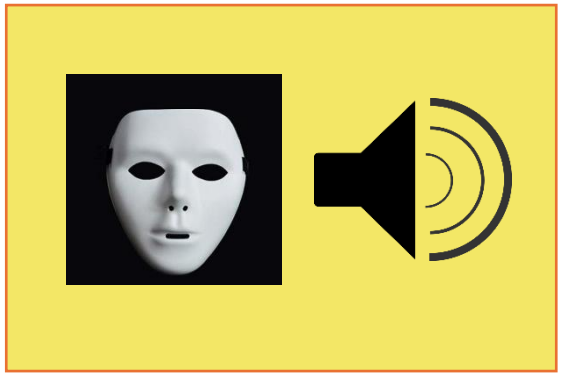
- Relativt enkelt å lure et biometrisk system
  - Terminologi: Presentasjonsangrep



Falsk finger



Falsk ansikt



Deepfake lyd/bilde/video

- Biometrisk autentisering på smarttelefoner er usikker
- Det forskes mye på PAD (Presentation Attack Detection) for å gjøre biometri mer sikker
- Et alternativ er å kontrollere omgivelsen for innhenting av biometriprøver

Trygghet ved bruk av biometri



- Det kan være aktuelt å sette krav til personsikkerhet ved bruk av biometriske systemer, ettersom brukeren involveres fysisk.
- I USA i 2023 er det rapportert at ofre har blitt dopet ned for å låse opp deres smarttelefoner med ansiktsgjenkjenning for å få tilgang til deres bankkontoer.
- I alle tilfellene dreier det seg om *kroppsbaserte biometriske modaliteter*, der en kroppsdel, som for eksempel ansikt eller finger, benyttes for autentisering.
- *Atferdsbaserte biometriske modaliteter*, som stemmegjenkjenning og tastaturdynamikk, krever at brukeren er bevisst, slik at det ikke er like lett for en angriper å tvinge frem en biometrisk prøve.



Car thieves chopped off part of the driver's left index finger to start S-Class Mercedes Benz equipped with fingerprint key.
Malaysia, March 2005
(NST picture by Mohd Said Samad)

Flerfaktor-autentisering



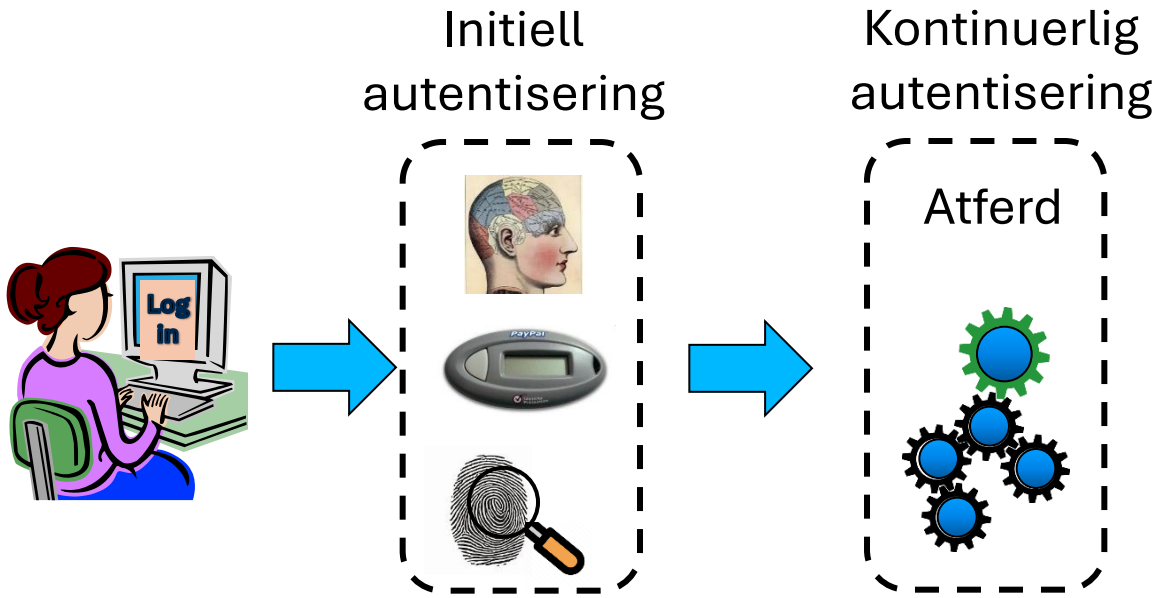




- Flerfaktorautentisering kombinerer to eller flere teknikker for å gi sterkere autentisering.
- Tofaktorautentisering er ofte basert på noe brukeren vet (1.faktor) pluss noe brukeren har (2.faktor).
- Eksempler
  - passord og brikke (f.eks. BankID)
  - passord og sekundærkanal (f.eks. SMS)

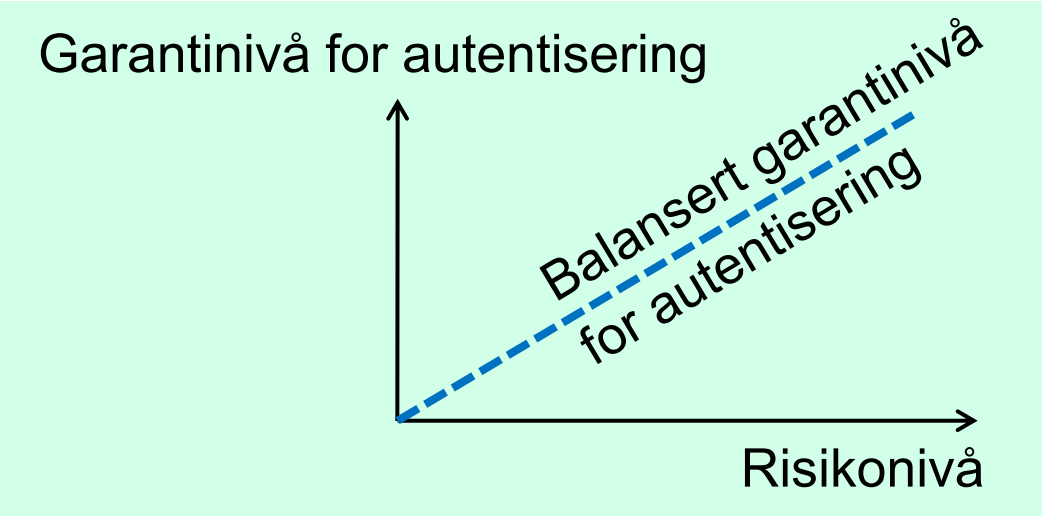
Kontinuerlig autentisering

- Kontinuerlig autentisering er å sammenligne faktiske atferd med forventet atferd under interaksjon med systemet.
- Hvis likheten faller under en gitt terskelverdi vil brukeren bli logget ut, eller kan alternativt få redusert autorisering.
- Vanlig autentisering først, deretter kontinuerlig autentisering

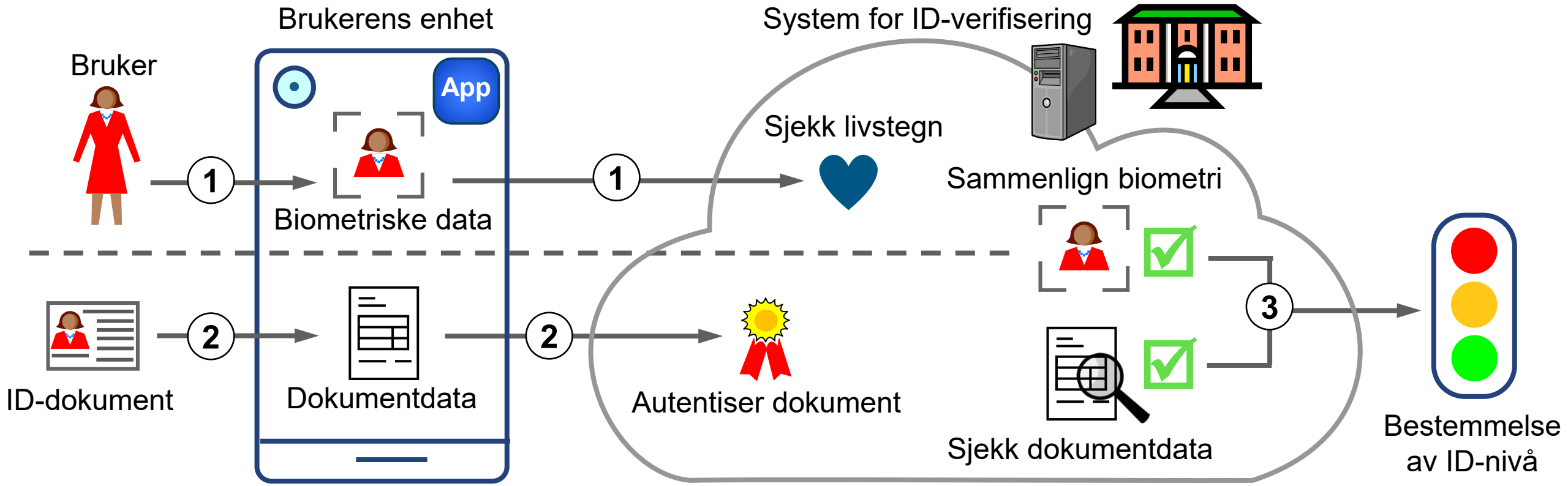


Garantinivå for autentisering

- Garantinivå for autentisering = robusthet av autentiseringen
- Tjenester med ulike sensitivitets- og risikonivåer setter ulike krav til autentisering
  - Alvorlig konsekvens og risiko i tilfelle autentiseringsfeil gir krav om sterk autentisering med høyt garantinivå
- Sterk autentisering koster mer enn svak autentisering
  - Unødvendig sterk autentisering er sløsing med penger
- Garantinivå for autentisering bør derfor være balansert



Fjernverifisering av identitet



- Mange eID-tilbydere bruker ICAOs PKD for å verifisere autentisitet av pass
- Eksempel: https://youtu.be/fx47qzAKlvs
- For kommersiell bruk av PKD kreves skriftlig tillatelse fra ICAO

Rammeverk for e-autentisering

- Tillit til identitet er et krav for sikker e-forvaltning
- Sterk autentisering gir tillit til identitet.
- Autentisering avhenger av teknologi, regulering, policy, standarder, praksis og, bevissthet.
- Konsistente rammeverk for autentisering gir grunnlag for effektivitet av e-forvaltning.



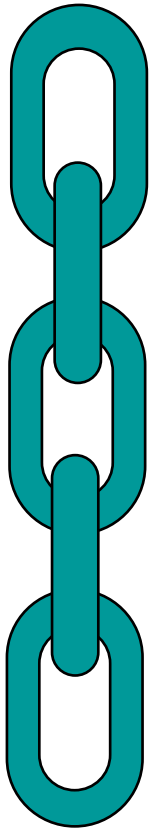
Rammeverk for e-autentisering, med ulike garantinivåer

Veileder/standard for autentisering	***Garantinivå for autentisering***			
SP 800-63-4 Digital Identity Guidelines NIST, USA 2025 		Assurance Level 1	Assurance Level 2	Assurance Level 3
Assurance levels for electronic identification means eIDAS 2.0, EU 2024 		Low	Substantial	High
Veileder for identifikasjon og sporbarhet DigDir 2022 (basert på eIDAS 1.0, 2018) 		LAVT	BETYDELIG	HØYT
IS 29115 Entity authentication assurance framework ISO/IEC 2013 	Low (1)	Medium (2)	High (3)	Very High (4)

- Garantinivå for autentisering kalles også “autentiseringsnivå” eller “sikkerhetsnivå”. På engelsk: “Level of Assurance” (LoA), eller “Authentication Assurance Level (AAL).

Kategorier av krav til autentisering

Garantinivå for autentisering er hovedsakelig en funksjon av 3 kategorier av krav



a) ID-registrering og autentikatorhåndtering

Metoder for sjekk av identitet og klargjøring av autentikatorer

Krav til identitetsbevis og korrekt registrering:
- fødselsattest, pass, biometri

Krav til klargjøring og håndtering av autentikator:
- overlevering og gjenoppretting, fysisk, post eller online

b) Autentiseringsmetode

Teknologi og kombinasjon av metoder for brukerautentisering.

Krav til autentiseringsmetoder:
- passordlengde og kvalitet
- kryptografisk styrke og PKI
- flere autentiseringsfaktorer (2FA, MFA)
- phishingresistens (kun nevnt i USA NIST SP 800-63-4)

c) Fødereringssikkerhet

Tillitsnivåer og sikkerhet i samhandling mellom IdP og SP.

Krav til sertifisering av IdP (autentiseringstjener) og ID-portaler, og juridiske avtaler mellom interessenter.

eIDAS

electronic IDentification, Authentication and trust Services

- eIDAS er EUs forskrift om e-autentisering og tillitstjenester for e-forvaltning.
- "Trust service" er EU-sjargong for PKI-sertifiseringstjenester.
- eIDAS spesifiserer tre garantinivåer for autentisering: Level of Assurance (LoA).

Low Assurance eDAS LoA-1	Substantial Assurance eIDAS LoA-2	High Assurance eIDAS LoA-3
Limited degree of confidence in the claimed or asserted identity of a person	Substantial degree of confidence in the claimed or asserted identity of a person	High degree of confidence in the claimed or asserted identity of a person



EU sitt symbol for kvalifiserte tillitstjenester

Adekvat autentiseringsnivå utifra risiko

Tabell for å bestemme adekvat garantinivå for autentisering for en tjeneste innen e-forvaltning (eIDAS)

medfører	Konsekvens av e-autentiseringsfeil		
	Liten	**Betydelig**	**Alvorlig**
Krav til LoA →	Low eIDAS LoA-1	Substantial eIDAS LoA-2	High eIDAS LoA-3

Eksempel risikomatrise for eIDAS

e-autentiseringsfeil betyr at en angriper er i stand til å forfalske og stjele andres identiteter

Slutt på presentasjon