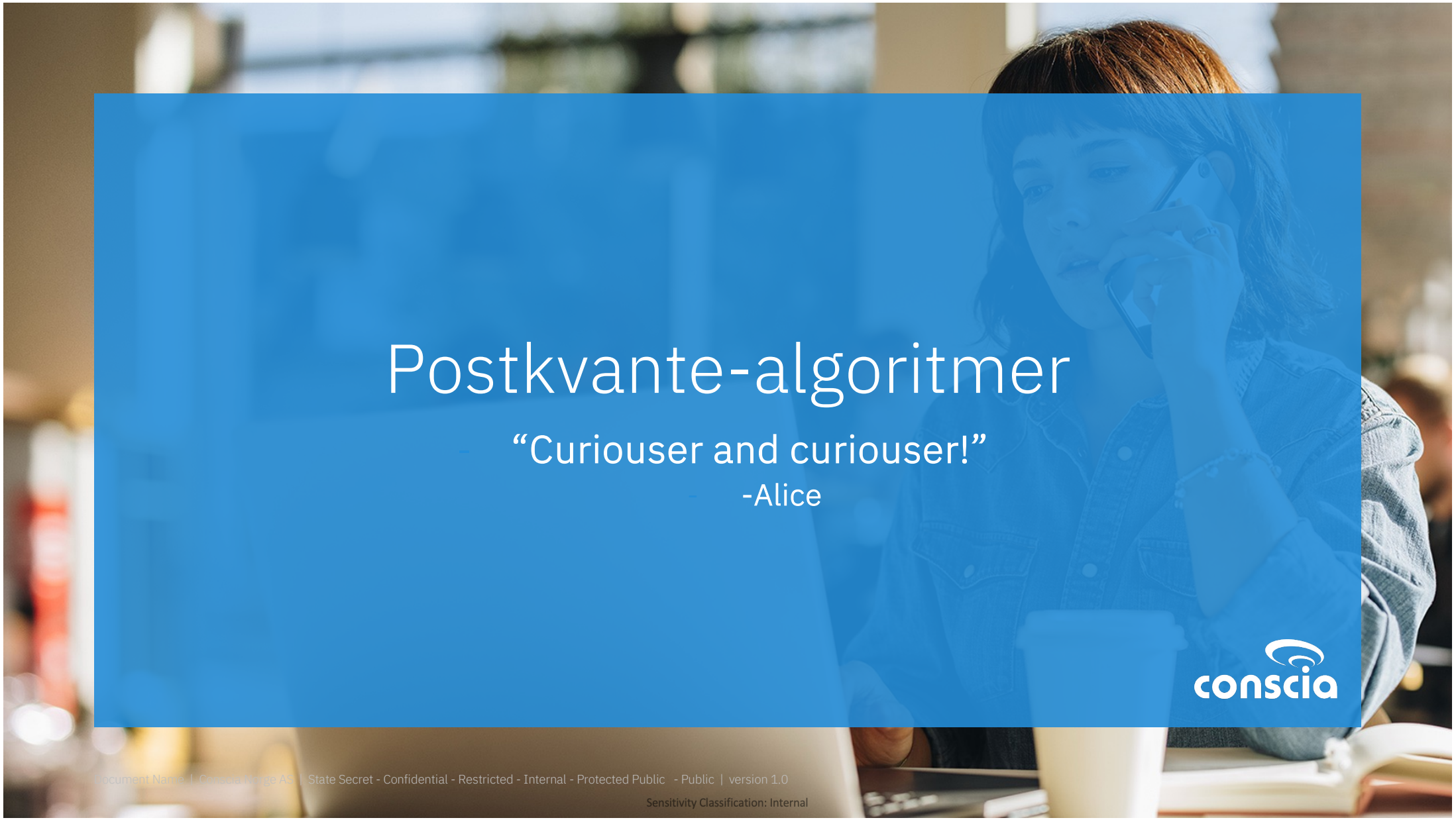


Postkvante-algoritmer

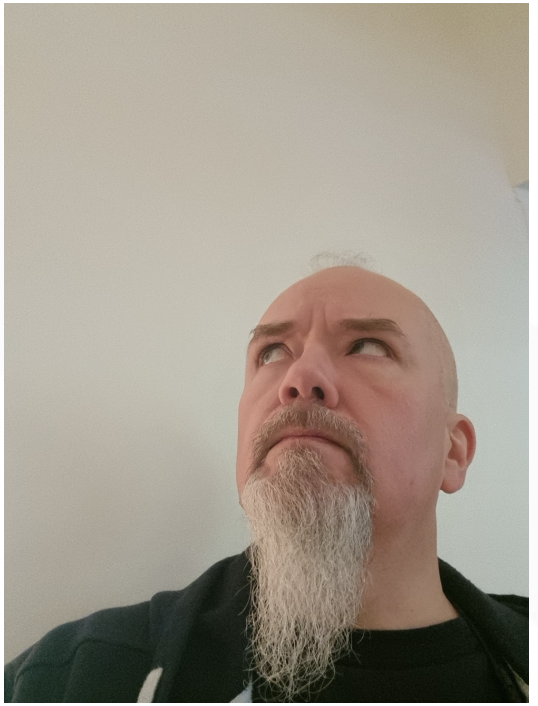
"Curiouser and curiouser!"

-Alice

conscia

Introduksjon

- **Navn:** Thomas Kjensmo
- **Tittel:** Senior Networking and Security Consultant
- **Gift med:** Camilla ❤️
- **Bor:** Oslo
- **Dyr/Barn:** 2 katter
- **God på:** Sarkasme og PKI



Vi må forberede oss på fremtiden

Bytt fra dagens sikre algoritmer til postkvante-algoritmer!

conscia

Kryptografi

The art of turning information into nonsense and, hopefully, back again

Matematikk

Numbers and stuff

Kvantefysikk

Black magic

Hvordan beskytter vi data i dag ?

- Symmetrisk kryptografi : AES (kryptering med delt nøkkel)
- Asymmetrisk kryptografi: RSA, ECC (kryptering med offentlig og privat nøkkel)
- Vi stoler på at vanskelige matematiske problemer ikke kan reverseres

Hva er en kvantedatamaskin ?

- Flere forskjellige teknologier som brukes i dag
  - Trapped-ION
  - Silicon based
  - Photonic
  - Carbon-based
  - Superconducting
  - Neutral atom
- Felles er at det er skjør teknologi, som trenger strengt kontrollerte miljøer

- Qubits – Minste informasjonenhet - tilsvarer klassisk bit
- Quantum Gates – operatører som påvirker qubits
- Quantum Circuits – kommunikasjon på quantum nivå

- Kan løse problemer parallelt som klassiske maskiner bruker evigheter på

Shors Algoritme(r) – Kryptografens mareritt

“The world of quantum mechanics is not the world of your intuition”
- Peter Shor

- Faktorisering av store primtall – RSA brytes
- Diskrete logaritmeproblemer – ECC brytes
- Matematiske periodiske funksjoner - Diffie-Hellman nøkkelutveksling svekkes

Hva med symmetrisk kryptografi?

- Her er det heldigvis færre problemer.
- Grovers algoritme legger press på AES
- Vi kan omgå problemene her med å øke nøkkelstørrelse

Hvordan kom vi frem til nye algoritmer?

- NIST utlyste en åpen konkurrnse i 2016
- 3 runder med testing av kandidater - > valg av Kyber, Dilithium, Falcon, SPHINCS+
- Standardisert i august 2024

Den nye vinen – Postkvante-algoritmer på godt og vondt

- NIST Standarder
  - FIPS 203 ML-KEM - Public Key Encryption, Lattice based, strong encryption
  - FIPS 204 ML-DSA – Digital Signatures, Lattice based
  - FIPS 205 SLH-DSA - Digital Signatures – Hash based, well understood, minimal assumptions
  - Draft FIPS 206 FN-DSA Falcon – Digital Signatures – Lattice based, short signatures, fast

- Valg for standardisering 2025
  - HQC - KEM

Men skjer det da? - Dagens trusselbilde

- Så vidt vi vet er det ingen kvantedatamaskiner i dag som kan bryte RSA, ECC eller DH med normale nøkkelstørrelser
- Google, IBM og andre aktører har maskiner med over ~~1100~~ ustabile **6100** fysiske qubits, et stykke fra de 20 000 000 som er estimert for å knekke RSA-2048
- Ingen akutt trussel i dag, men latente og fremtidige trusler er nesten garanterte
- Feilrettingsmetoder og -algoritmer blir stadig bedre
- Kvantekappløp mellom de store aktørene – Estimert 45 milliarder dollar i utvikling i 2025
- Store now, decrypt later
  - Store aktører (f.eks USA, Kina, Russland) samler inn store mengder data i dag som kan knekkes i fremtiden.

Brave new world – Veien videre

- NSM, NIST og EU(ETSI) har migreringsanbefalinger
- NSA krever PQC algoritmer for nye klassifiserte systemer, det gjør også andre lands etterretningsorganisasjoner

- Kartlegge organisasjonens bruk av kryptografiske algoritmer
- Risikovurdere bruksområdene og dataene som beskyttes
- Bli kjent med nye standarder
- Planlegge migrering (helst før 2030)
- Implementere migrering

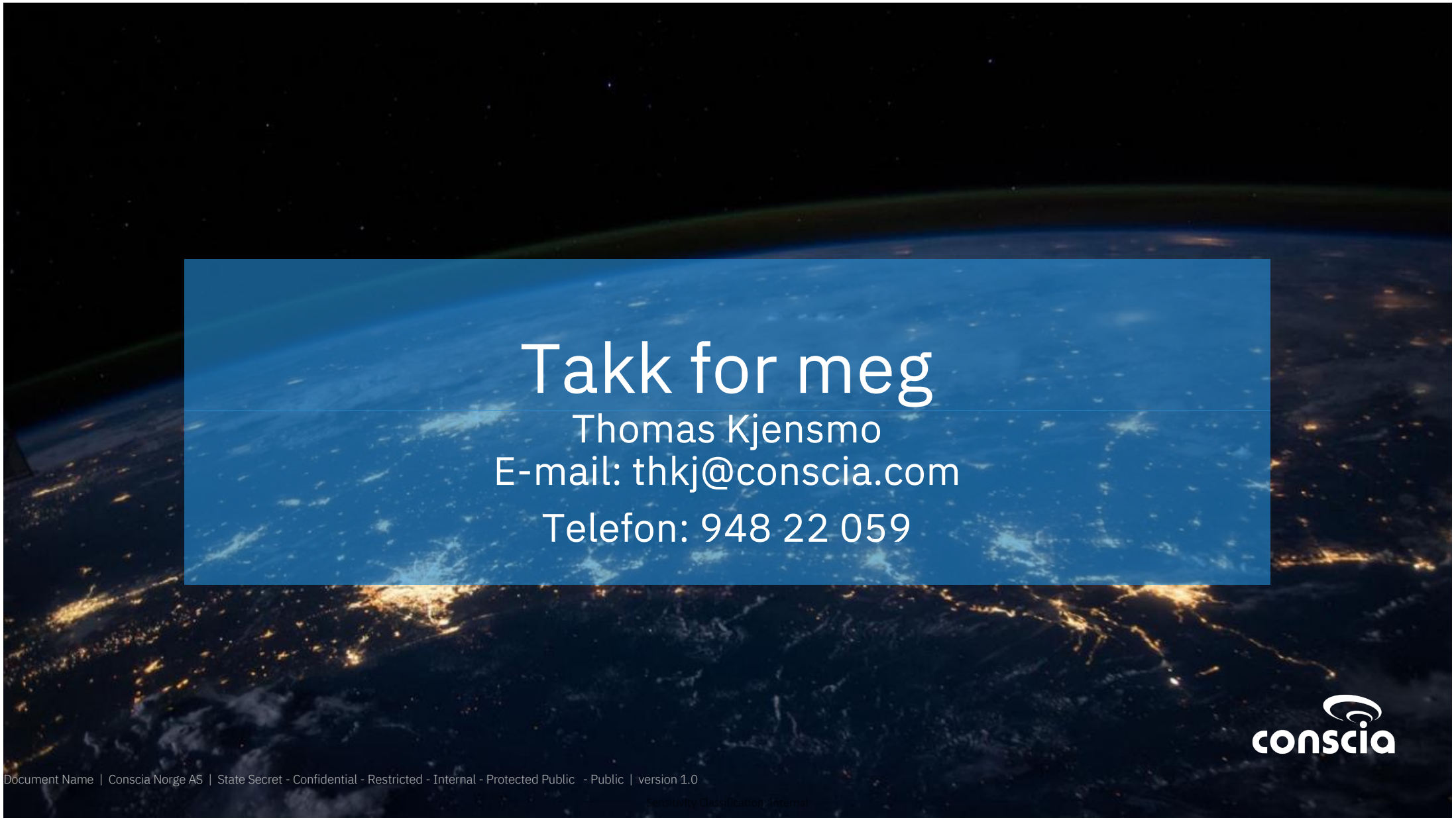
- Conscia kan hjelpe til i denne prossessen

Oppsummering!

- Vi må forbereder oss på kvanteangrep, ikke fordi de skjer i dag – men fordi dataene vi beskytter i dag fortsatt skal være hemmelige om 30 år

Veiledere og standarder

- NSM Kvantemigrasjons veileder
  - https://nsm.no/fagomrader/digital-sikkerhet/kryptosikkerhet/kvantemigrasjon/kvantemigrasjon-veileder/kvantemigrasjon/
- EU kommisjonens roadmap
  - https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- NIST standarder
  - https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- ETSI standarder
  - https://www.etsi.org/technologies/quantum-safe-cryptography


Takk for meg
Thomas Kjensmo
E-mail: thkj@conscia.com
Telefon: 948 22 059
conscia