



Teknisk Dybdeanalyse av Kvantebestandighet i Open Source Prosjekter: En Studie av Post- Kvante Kryptografi

Fredrik, Simen og Sander

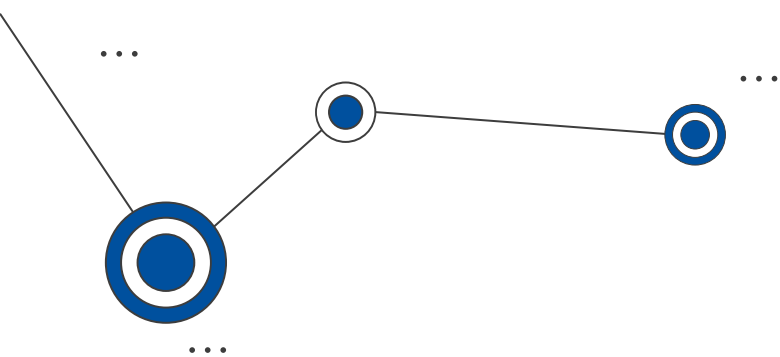
Oppgaven

- Hva er utfordringen DigDir ønsker å få belyst?

Mål

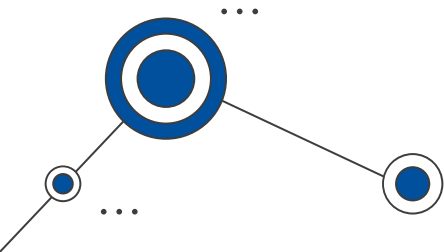
- Hvilke algoritmer og hvor?
- Hvordan kan de erstattes?
- Hvilke verktøy og metoder for analyse?
- utfordringer ved å erstatte algoritmene?





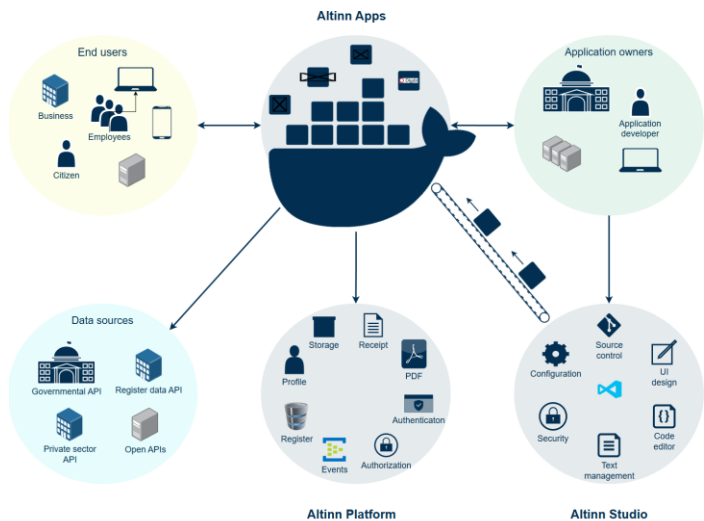
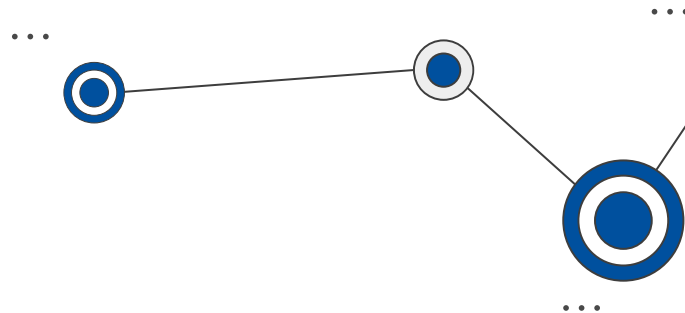
- Ett repository
- Kun kodeanalyse
- Enkel prosess
- Mindre omfattende

Forventninger



 Altinn Studio

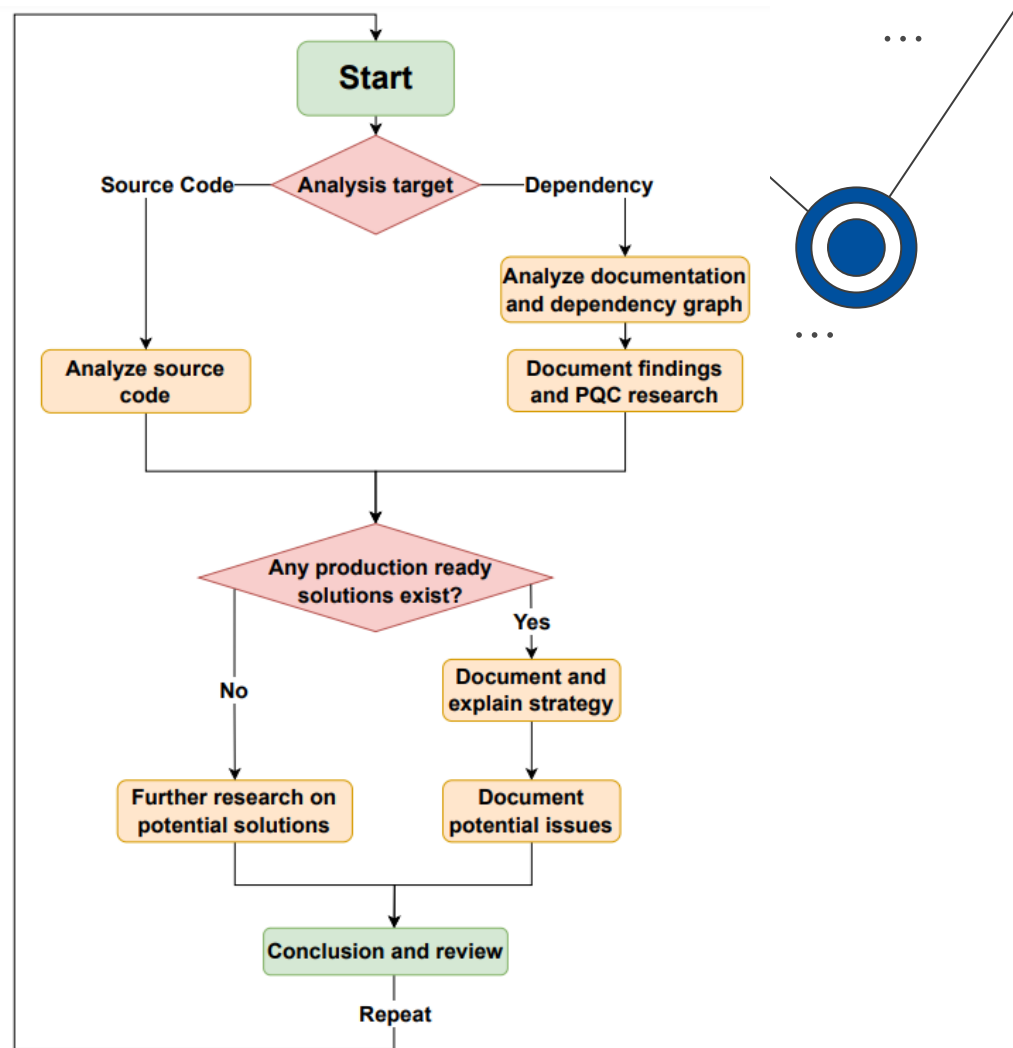
- 121 repositories
- Rundt 4 600 unike avhengigheter (git dependency graph)
- Lite kryptografi i kode



Virkeligheten

Metode

- Kildekode og avhengigheter
- Statisk analyse
- Avhengigheter = dokumentasjon + grafer
- PQC-alternativer
- Fordeler og ulemper

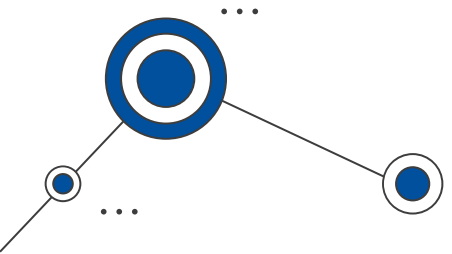
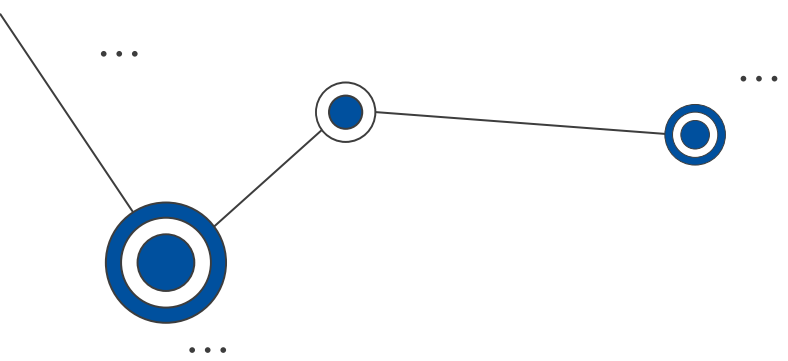


- Testet: Aikido, Semgrep, SonarQube
- Vanskelig å utføre
- CodeQL = fleksible søk

 Semgrep  aikido

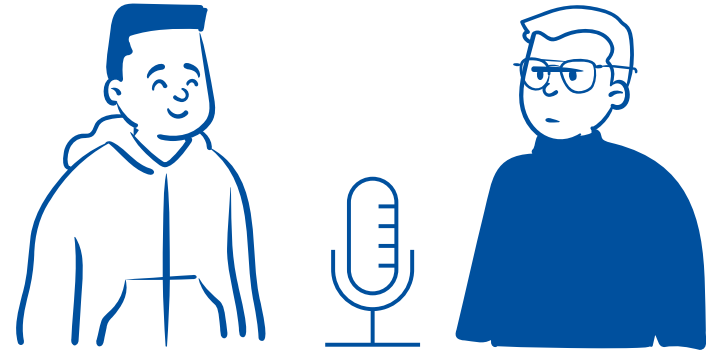
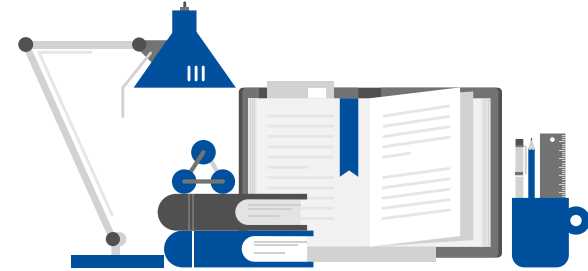
 sonarqube

Valg av verktøy



Intervju og litteraturstudie

- Strukturert litteraturgjennomgang
- Fokus på PQC
- Vurdering av relevans
- Eirik Mikkelsen og Arne Tobias Ødegaard



- Ikke bare kode
- Migrasjonsveiledning
- Altinn 3-spesifikt?
- Relevans for andre?

Oppgavens retning



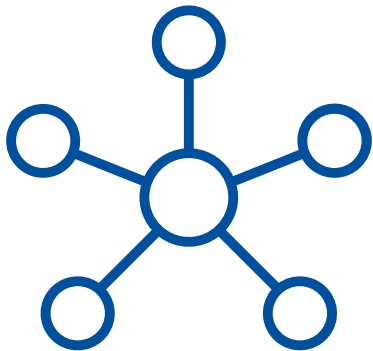
NSM

NIST

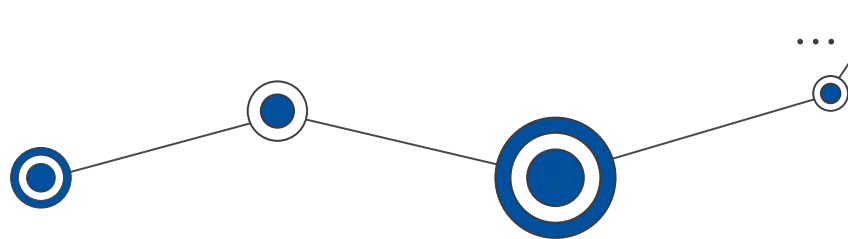


Bundesamt
für Sicherheit in der
Informationstechnik

Hvor fant vi kryptografi?



- Avhengighetsanalyse
- GitHub dependency graphs
- Dokumentasjon
- SSLlabs og TLS-inspeksjon



Kodeanalyse

Kodenavn	Algoritme(r)	Komponent	Erstatnings Algoritme
MP.RSA.SHA-SIG	RSA og SHA-256 via X.509	.NET client for Maskinporten	ML-DSA
ALTINN-ORG-TOKEN-GEN	RSA og SHA-256	Altinn-Authentication	ML-DSA
AUTH-NONCE-HASHER	SHA-256 og base64	Altinn-Authentication	Ikke nødvendig
AUTH-RSA-JWKS-SIG	RSA	Altinn-Authentication	ML-DSA
AUTH-JWT-PROVIDER	RSA og SHA-256 via X.509	Altinn-Authentication	ML-DSA
CERT-CA-509	RSA og SHA-256 via X.509	Cert-Generator	ML-DSA
CERT-ROOT-CA-509	RSA og SHA-256 via X.509	Cert-Generator	ML-DSA
CERT-RSA-KEY	RSA og SHA-256	Cert-Generator	ML-DSA
CERT-PEM-CONVERTER	RSA	Cert-Generator	ML-DSA
CORR-RSA-SHA-VALIDATOR	RSA og SHA-256	Altinn-Correspondence	ML-DSA
CORR-MD5-VALIDATOR	MD5	Altinn-Correspondence	SHA-256
AS-MD5-CHECKSUM	MD5	Altinn-Storage	SHA-256
ASPNET-CONFIG-EDDSA	ED25519	Dialogporten	ML-DSA
DP-DSIGN-GETJWS-EDDSA	ED25519 og Base64 koding	Dialogporten	ML-DSA for ED25519
DP-JWSGEN-VERIFY-JWS-EDDSA	ED25519 og Base64 koding	Dialogporten	ML-DSA for ED25519
DP-EDMASK-SHA-HASH	SHA-256	Dialogporten	Ikke nødvendig
DP-JWS-DTO-EDDSA	ED25519	Dialogporten	ML-DSA
DP-JOKUL-INIT-EDDSA	ED25519	Dialogporten	ML-DSA
DP-SIG-VALIDATOR-EDDSA	ED25519	Dialogporten	ML-DSA
DP-TOKEN-BENCHMARK-GEN-VALIDATOR	Flere for benchmark	Dialogporten	Legg til ML-DSA og ML-KEM som minimum
Program.cs	ED25519	Dialogporten	ML-DSA

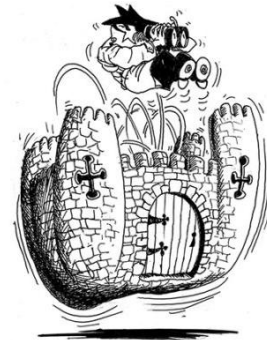
- Digitale signaturer
- SHA-256
- MD5 fra Altinn 1
- Andre positive konsekvenser
- ML-DSA



Biblioteker som brukes

Bibliotek	Språk	Nøkkelalgoritmer	Beskrivelse
crypto-browserify	JavaScript	AES, DES, SHA (1, 256, 512), HMAC, RSA	Node.js krypto modul implementering for nettlesere, muliggjør kryssplattform kryptografi i JavaScript
crypto-random-string	JavaScript	Platform CSPRNG	Lettvekts bibliotek spesifikt for å generere kryptografisk sterke tilfeldige strenger
x/crypto	Go	Argon2, Blake2, ChaCha20, Ed25519, scrypt, NaCl	Offisiell Go tilleggskryptografisk pakke med avanserte algoritmer utover standardbiblioteket
Microsoft.Bcl.Cryptography	C#	AES, RSA, ECDSA, SHA	Base Class Library kryptografiske komponenter for .NET applikasjoner, del av Microsofts økosystem
minimalistic-crypto-utils	JavaScript	HMAC, hash operasjoner	Minimale verktøy for grunnleggende kryptografiske operasjoner i JavaScript
NSec.Cryptography	C#	ChaCha20-Poly1305, AES-GCM, Ed25519, X25519, BLAKE2b	Moderne kryptografisk bibliotek bygget på libsodium, med vekt på sikkerhet og brukervennlighet
System.Security.Cryptography	C#	Innebygd kryptografibibliotek i .NET	Spesialisert kryptografibibliotek spesifikt for .NET applikasjoner
tweetnacl	JavaScript	Curve25519, XSalsa20, Poly1305	Høysikkerhet, moderne kryptografi
node-forge	JavaScript	RSA, AES, SHA, HMAC, PBKDF2, TLS/SSL	Implementerer mange protokoller, inkludert X.509 sertifikater
jsonwebtoken	JavaScript	HMAC, RSA, ECDSA	Mye brukt for autentisering

- SSC
- NSec
- Bouncy Castle





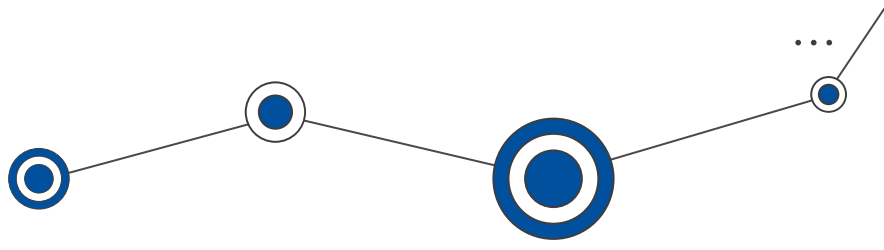
Sertifikater



COMMFIDES

 buypass™

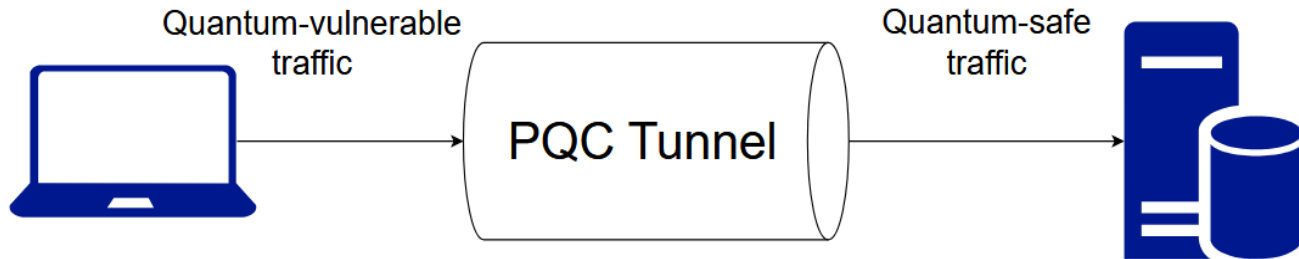
digicert®

- Commfides og Buypass i dag
 - Hverken composite eller pqc
 - Digicert
- 

Verktøy til Migrasjon



- IBM Quantum Safe
- Cloudflare Zero Trust

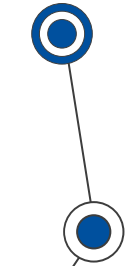
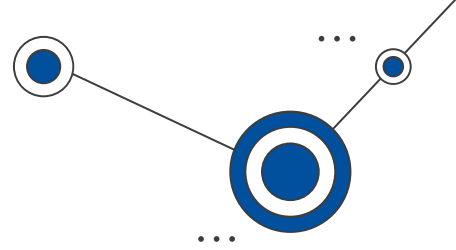


Tredjepartsutbyttinger

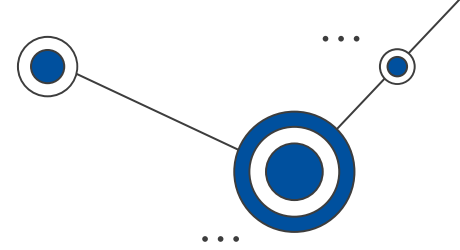




linkerd



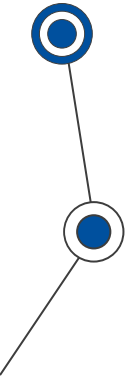
Hastighet



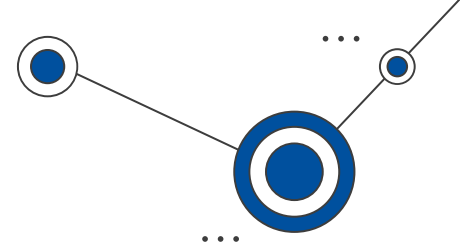
- ML-KEM
- ML-DSA
- Størrelse på nøkler
- Dilemma

Algoritme	Klient (bytes)	Server (bytes)
ML-KEM-512	800	768
X25519	32	32

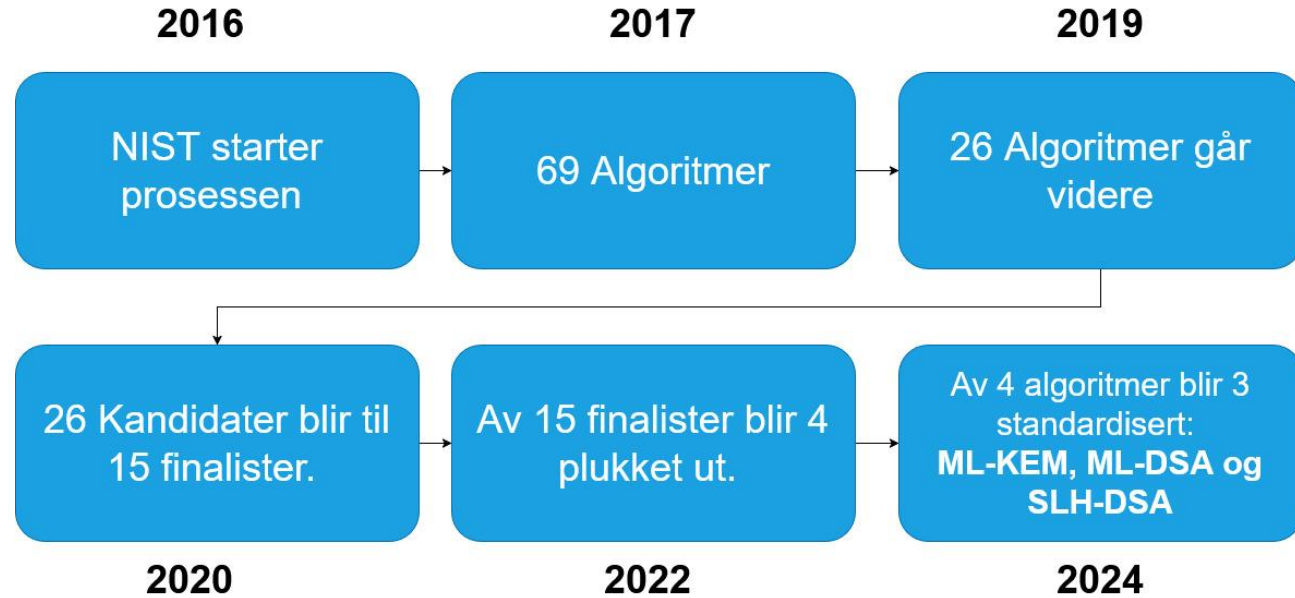
Algoritme	Offentlig Nøkkel (bytes)	Signatur (bytes)
ML-DSA-44	1312	2420
Ed25519	32	64



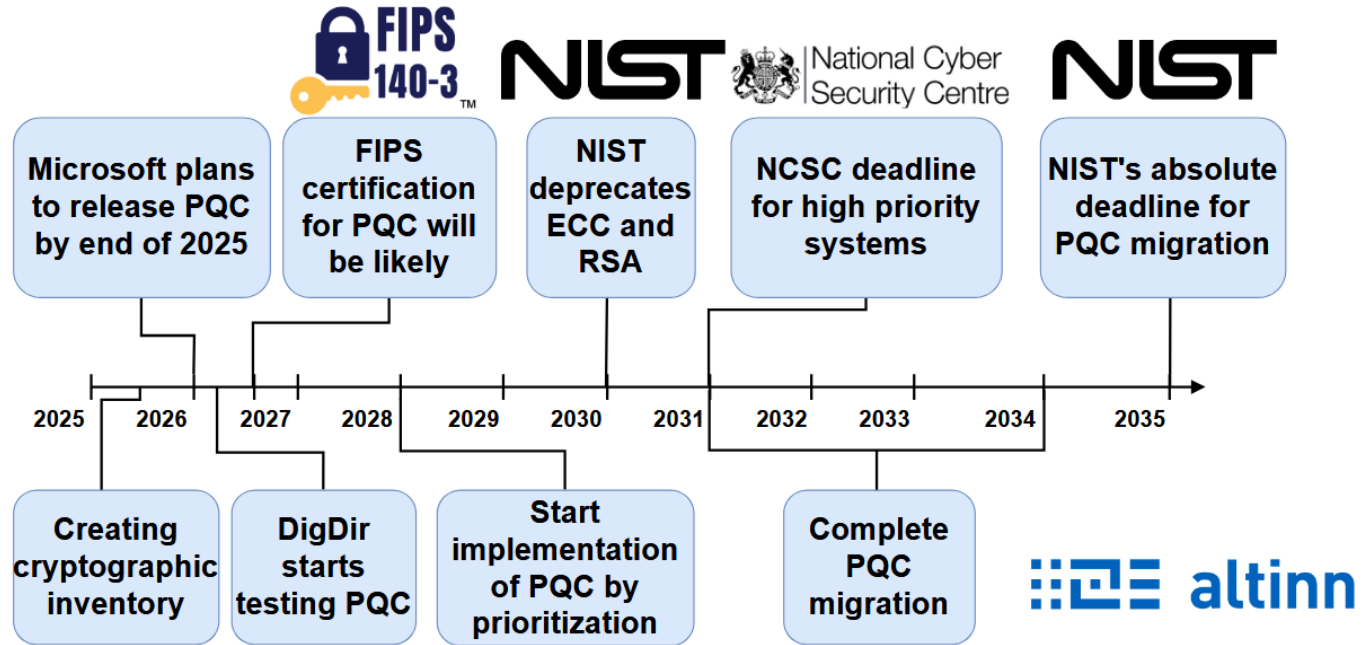
Sikkerhet



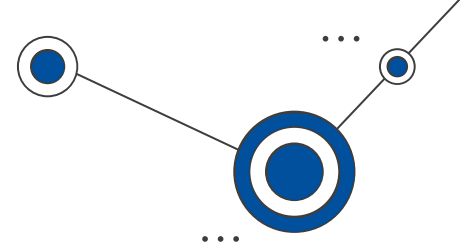
- NIST sin prosess
- Rainbow og Sike
- Gradvis testing
- Hybride løsninger



Tidslinje



Konklusjon



- Reel trussel
- Lite forberedt
- Begynne i dag
- 2035
- Fleksibilitet

