Quantumveilige Cryptografie

Luuk Danes & Sander Dorigo

Platform voor InformatieBeveiliging

18 september 2025

CRYPTOGRAPHY IN CONTEXT

Overwin crypto-uitstelgedrag, zet vandaag je eerste (kleine) stap naar quantumveiligheid!

Luuk Danes

Platform voor InformatieBeveiliging, 18 september 2025

Crypto-uitstelgedrag

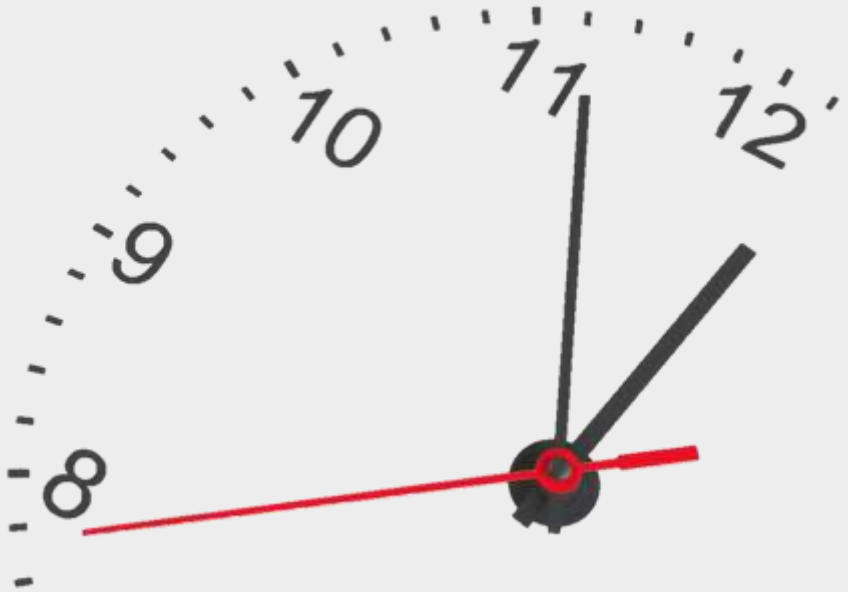
Het gevaar van crypto-uitstelgedrag

Q-day komt dichterbij.

Sommige toepassingen zijn al eerder kwetsbaar.

Tijdslijnen, adviezen en regels verschijnen.

De vraag naar expertise neemt toe.



Luuk Danes

CRYPTOGRAPHY
INCONTEXT

SECURITY
ACADEMY

We gaan kijken naar...

Waarom wij crypto-uitstelgedrag vertonen.

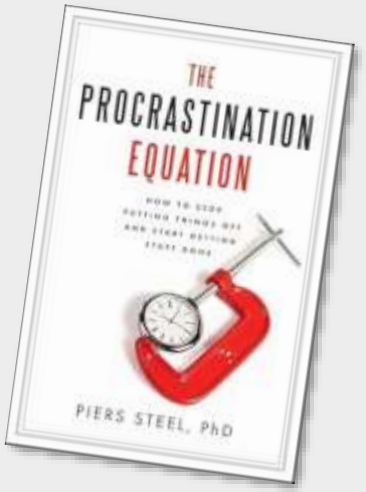
Hoe te beginnen? Vergroot de motivatie!

3 mogelijke stappen.

De Uitstelvergelijking

$$\text{Motivatie} = \frac{\text{Verwachting} \times \text{Waarde}}{\text{Impulsiviteit} \times \text{Vertraging}}$$

Bron: Piers Steel, The Procrastination Equation
Gebaseerd op de temporal motivation theory (TMT):
Steel, P.; Konig, C. J. (2006). "Integrating Theories of Motivation“



De Uitstelvergelijking

Motivatie

neemt toe

als je verwacht dat je kan slagen

en

als je gelooft dat de taak waardevol is.

De Uitstelvergelijking

Motivatie

neemt af

als je gemakkelijk afgeleid wordt

of

als de beloning nog ver weg is.

Jouw doel

Maak je organisatie ‘quantumveilig’!

Jouw doel

Maak je  mveilig’!

Jouw kleinere doel

Begin met een crypto-inventarisatie.

Maak een roadmap.

Voer quantumrisico-analyses uit.

Breng al je stakeholders in kaart
en ga met hen in gesprek.

Jouw kleinere doel

Begin met entarisatie.

Voer q ses uit.

Breng a in kaart
en g brek.

Optimaliseer je motivatie

Begin met een eerste stap
naar een quantumveilige toekomst...

...met:

Grote kans op **succes**

Waarde die verder gaat dan alleen quantumveiligheid

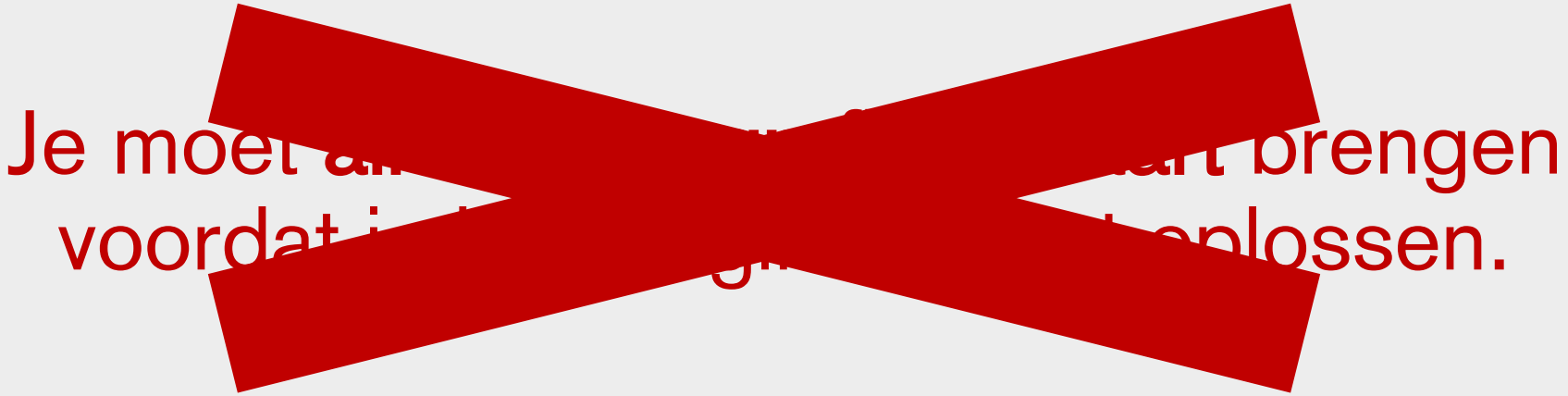
Concrete, planbare acties

Resultaat op **korte termijn**

Motivatiebarrières

Je moet **alle cryptografie in kaart** brengen
voordat je kan beginnen met oplossen.

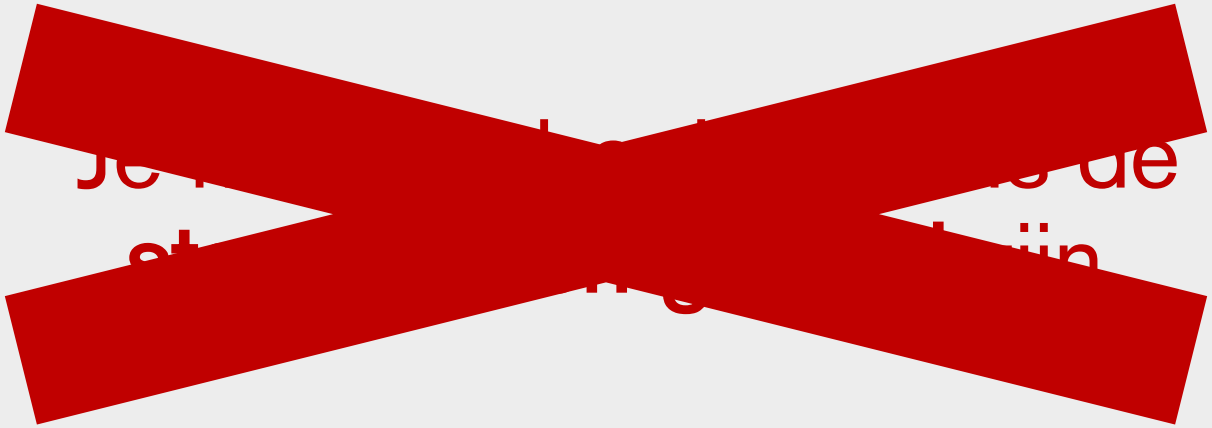
Motivatiebarrières



Motivatiebarrières

Je kan pas beginnen als de
standaarden gereed zijn.

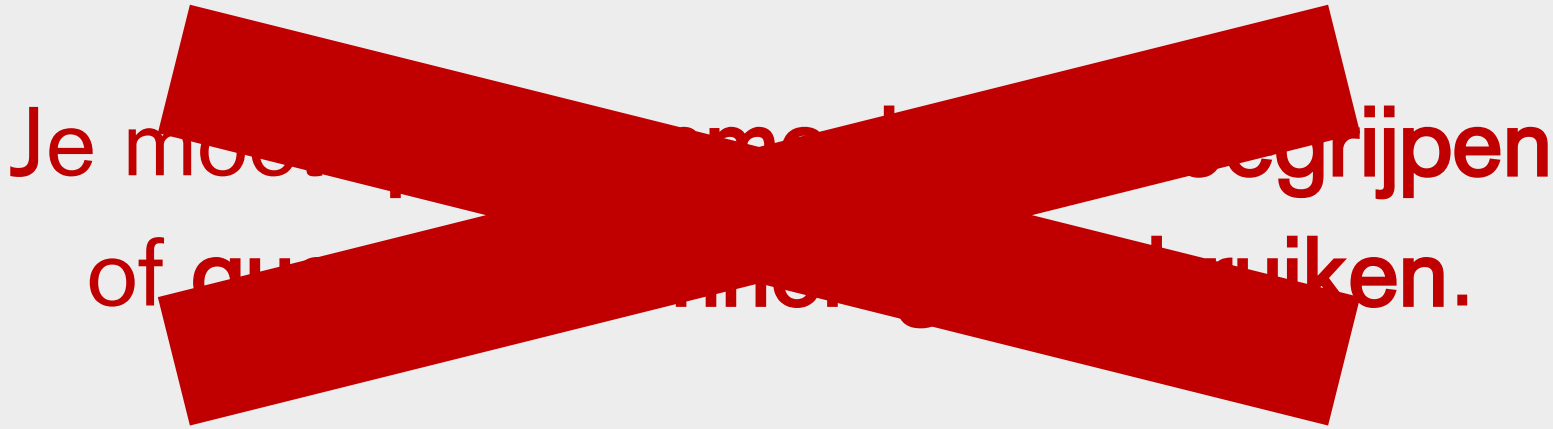
Motivatiebarrières



Motivatiebarrières

Je moet **quantummechanica begrijpen**
of **quantumtechnologie gebruiken**.

Motivatiebarrières



Motivatiebarrières

Je moet weten waar en hoe je
(quantumveilige) cryptografie toepast.

Motivatiebarrières

JA

Je moet weten waar en hoe je
(quantumveilige) cryptografie toepast.

Suggestie 1

Kennis opdoen en delen

Plan een activiteit om kennis over quantumveilige cryptografie op te doen en te delen.

☐ Succes | ☐ Waarde | ☐ Concreet | ☐ Korte termijn

Suggestie 2

Praatplaat Business Impact

Maak een praatplaat over de business impact van de quantumcomputer op cryptografie in jouw organisatie.

☐ Succes | ☐ Waarde | ☐ Concreet | ☐ Korte termijn

Suggestie 2

Praatplaat Business Impact

Het PQC-migratiehandboek

AIVD, CWI & TNO / 2e editie

Suggestie 3

TLS-beleid of -implementatie up-to-date

Maak je TLS-beleid of een TLS-implementatie gereed voor quantumveilige cryptografie door TLS 1.3 en Forward Secrecy te ondersteunen.

☐ Succes | ☐ Waarde | ☐ Concreet | ☐ Korte termijn

Suggestie 3

TLS-beleid of -implementatie up-to-date

Transport Layer Security (TLS)
Beveiligingsrichtlijnen

NCSC / versie 2025-05

Overwin crypto-uitstelgedrag,
zet vandaag je eerste (kleine) stap naar
quantumveiligheid!

En zorg voor:

Grote kans op **succes**

Waarde die verder gaat dan alleen quantumveiligheid

Concrete, planbare acties

Resultaat op **korte termijn**

Sentyron

Quantumveilige certificaten

Sander Dorigo

18 september 2025

PUBLIC

Van Fox Crypto naar Sentyron

1948	1957	1990	2003	2025
Nederlandse Seintoestellen Fabriek	Philips USFA (**U**ltra**s**one **fa**briek)	Philips Crypto	Fox Crypto	Sentyron

Vanavond

- OK algoritmes, en nu?
- OK protocollen, en nu?
- Quantumveilige certificaten en PKI infrastructuur

OK algoritmes, en nu?

CRYSTALS-KYBER

FIPS-203, ML-KEM (512, 768, 1024)

Module-Lattice Key Encapsulation Mechanism

CRYSTALS-DILITHIUM

FIPS-204, ML-DSA

Module-Lattice-Based Digital Signature Algorithm

SPHINCS+

FIPS-205, SLH-DSA

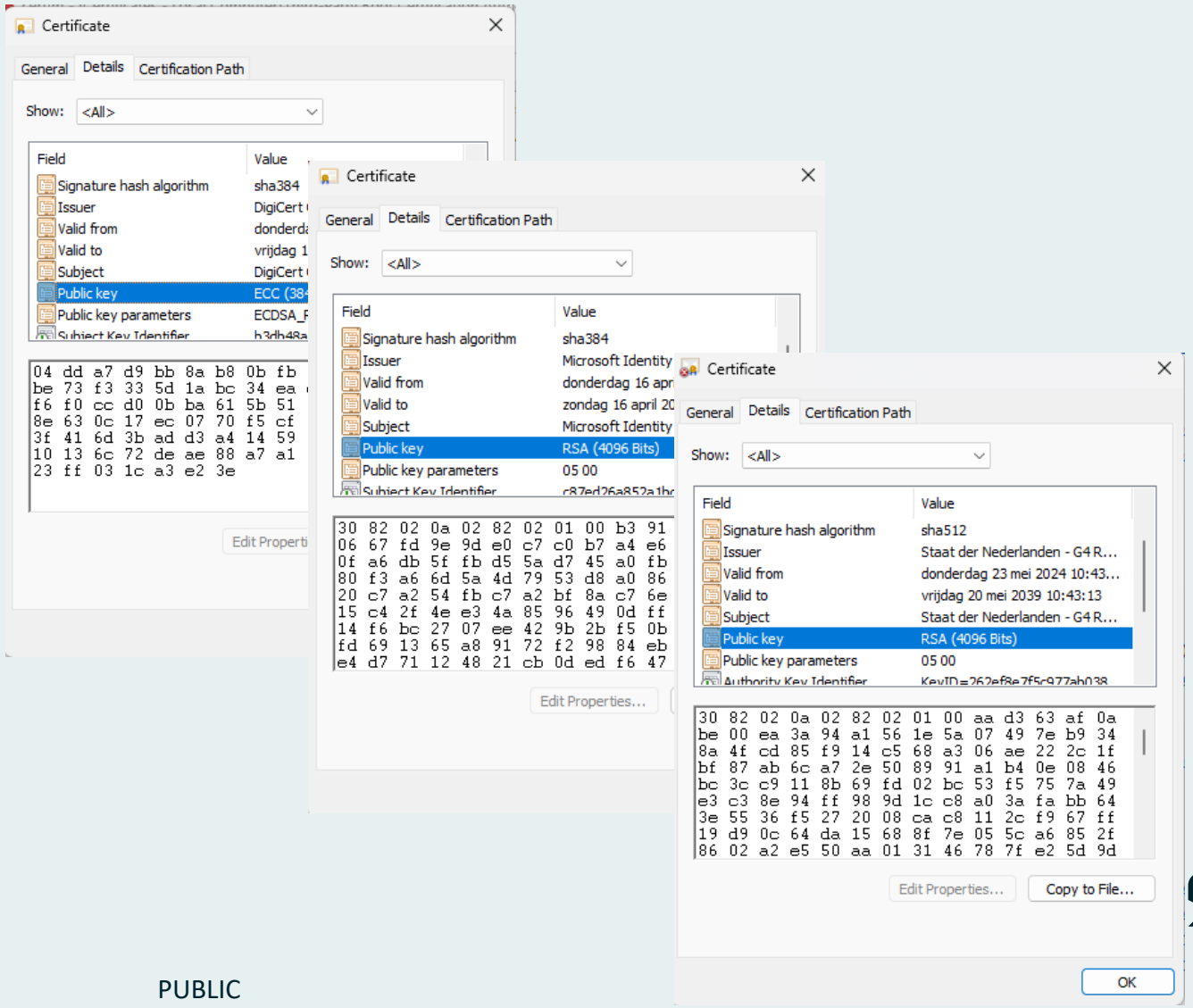
Stateless Hash-Based Digital Signature Algorithm

OK protocollen, en nu?

- TLS1.3 met PQC support
- Signal protocol
- iMessage (Apple)
- FIDO2 security keys

PKI-infrastructuur leunt op “gewone” certificaten

En ze zijn nog heel lang geldig



Hoe moeilijk kan het zijn?

- RFC X.509 updaten zodat we correct naar de nieuwe algoritmes kunnen verwijzen
- Clients moeten deze certificaten begrijpen en aan kunnen vragen
- Servers moeten deze certificaten hebben (en begrijpen)
- Het Certificate Authority/Browser (CA/B) forum moet dit ook goed vinden allemaal
- CA’s moeten deze certificaten kunnen uitgeven
- HSM’s moeten deze algoritmes implementeren (PKCS #11, FIPS-140)

Nieuwe certificaten

Hybride
Ruimte in een klassiek certificaat voor een alternatieve PQC sleutel en handtekening.

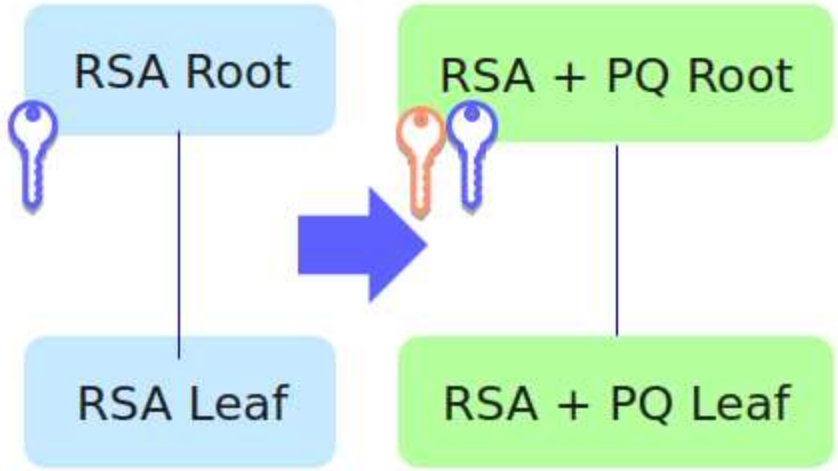
Chameleon
Een klassiek certificaat bevat genoeg gegevens om een PQC-certificaat te extraheren.

Composite
Een certificaat met een uit meerdere algoritmes samengestelde sleutel en handtekening.

Merkle-Tree
De handtekening en publieke sleutels worden opgeslagen in een (losstaande) server. Daar moet je mee verbinden en de data ophalen.

Nieuwe certificaten

- Old to new, backwards compatible, PKI
- Old clients and new clients mixed



Signing Algorithm	SHA256WithRSA Signing Algorithms supported by the keys present in the selected crypto token
Alternative Signing Algorithm	DILITHIUM2 Alternative signing algorithm if a hybrid certificate is desired.
defaultKey	defaultKey
certSignKey	signKey
alternativeCertSignKey	signKeyAlternative
crlSignKey	Use same as Certificate Signing Key (certSignKey).
keyEncryptKey	- Default key Note: Only RSA or ECDH compatible ECC key algorithms (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) may be used. Also, the encryption key must be of the same curve as the signing key.
testKey	testKey

Nadenken over PKI-migraties

Strategie	Voordelen	Nadelen
De harde knip	Nieuwe omgeving is sowieso quantumveilig	Boze ~~studenten~~ medewerkers Harde deadline voor upgrades
Dubbele PKI	Altijd backwards compatible	Twee PKI's onderhouden
Backwards-compatible PKI	Slechts één PKI-infra	Veel certificaatprofielen
Composite-PKI	Composite certificaten zijn ook beveiligd met klassieke cryptografie	Géén backwards compatibility

Conclusie

Er bestaan diverse (al dan niet) backwards compatible standaarden voor digitale (root)certificaten. Kortom: het kan.

Experimenteren is belangrijk: TLS1.3 was ook “100% backwards compatible”

Experimenteren

- ejbca.org
- pkic.org/pqccm
- github.com/open-quantum-safe/oqs-provider
- github.com/globalsign/example-pq-safe-x509

Vragen

En antwoorden :-)

sander.dorigo@sentyron.com

luuk.danes@cryptoincontext.nl

info@sentyron.com
www.sentyron.com

www.linkedin.com/in/luukdanes
qvc.securityacademy.nl