

PKI vs. QC – Halbzeitstand 1:0

Spiel läuft noch

15. Security Forum der TH Brandenburg

Holger von Rhein

Asymmetrische Kryptographische Verfahren

Öffentlicher Schlüssel

Privater Schlüssel

Verschlüsseln

Entschlüsseln

Signatur überprüfen

Signieren

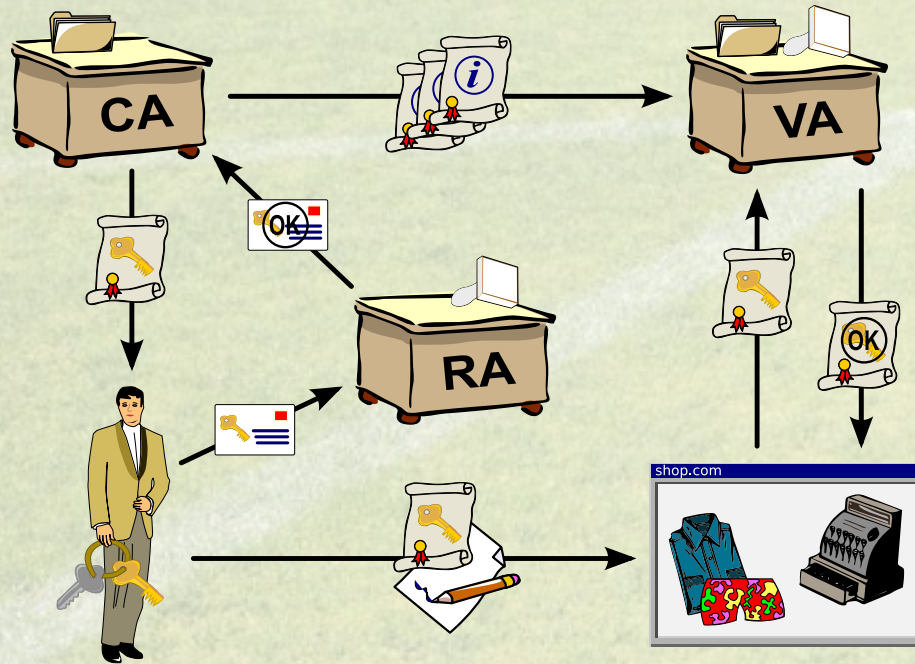


Digitales Zertifikat

- Krypto-Material
 - öffentlicher Schlüssel
 - Signatur
- Infrastruktur Informationen
 - OCSP/CRL-URL
 - Policy-URL
- Metadaten
 - Inhaber Bezeichner (Subject)
 - Aussteller Bezeichner (Issuer)
 - Verwendungszweck: KeyUsage, Extended KeyUsage

Zertifikate-Aussage:
„Ich (Aussteller) bestätige die Korrektheit
der hier enthaltenen Informationen.“

Public-Key-Infrastructure (PKI)



„System“, zum ...

... ausstellen von digitalen Zertifikaten

... verteilen von digitalen Zertifikaten

... prüfen von digitalen Zertifikaten

Zertifikats-Hierarchien

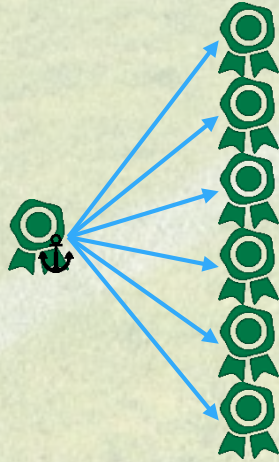
No-Hierarchy

Self-Signed



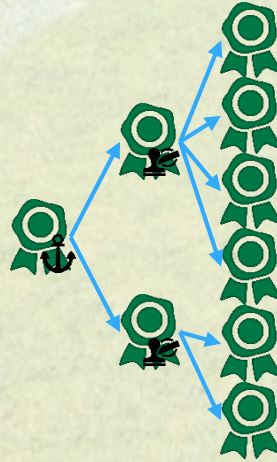
1-Layer-Hierarchy

Root-CA



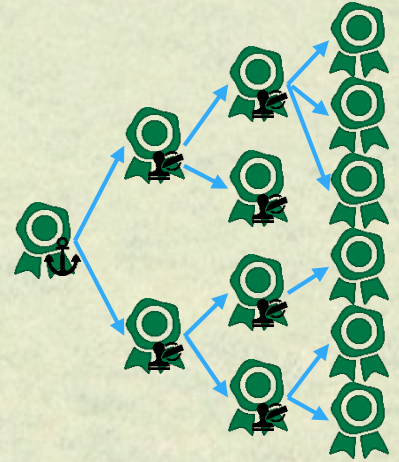
2-Layer-Hierarchy

Root-CA, Issuing-CA



3-Layer-Hierarchy

Root-CA, Intermediate-CA,
Issuing-CA



Artikel Diskussion

Zertifikat-Viewer: *.wikipedia.org

Allgemein Details

Ausgestellt für

Allgemeiner Name (CN)	*.wikipedia.org
Organisation (O)	Wikimedia Foundation, Inc.
Organisationseinheit	<Not Part Of Certificate>

Ausgestellt von

Allgemeiner Name (CN)	DigiCert TLS Hybrid ECC SHA384 2020 CA1
Organisation (O)	DigiCert Inc
Organisationseinheit	<Not Part Of Certificate>

Gültigkeitsdauer

Ausgestellt am	Dienstag, 27. Oktober 2022 um 02:00:00
Lauf ab am	Samstag, 18. November 2023 um 00:59:59

Fingerabdrücke

DNA-256-Fingerabdruck	95 AB 25 3C F5 8A 9E 3C 79 C9 E1 66 74 AE 48 DA 28 96 75 A3 93 FF 3F A4 5C 48 05 10 83 8D 95 A7
DNA-1-Fingerabdruck	91 04 00 00 2F F9 18 8D 18 07 D8 48 C7 54 54 F1 14 BF 2C DC

- 4.2 BEAST
- 4.3 Kompressionsangriffe
- 4.4 Downgrade auf Exportverschlüsselung
- 4.5 Implementierungsfehler
- 4.6 Öffentlicher und vorsätzlicher Bruch der Verschlüsselung
- 5 Vor- und Nachteile
- 6 Implementierungen
- 7 Siehe auch
- 8 Literatur
- 9 Weblinks
- 10 Einzelnachweise

Sichere Kommunikation

Zweck Zertifikat:
Identitätsnachweis Server



Vermieters an den Mieter.

Die Durchsetzung der Gemeinschaftsordnung gegenüber dem Mieter obliegt der jeweils eingesetzten Hausverwaltung.

Salvatorische Klausel

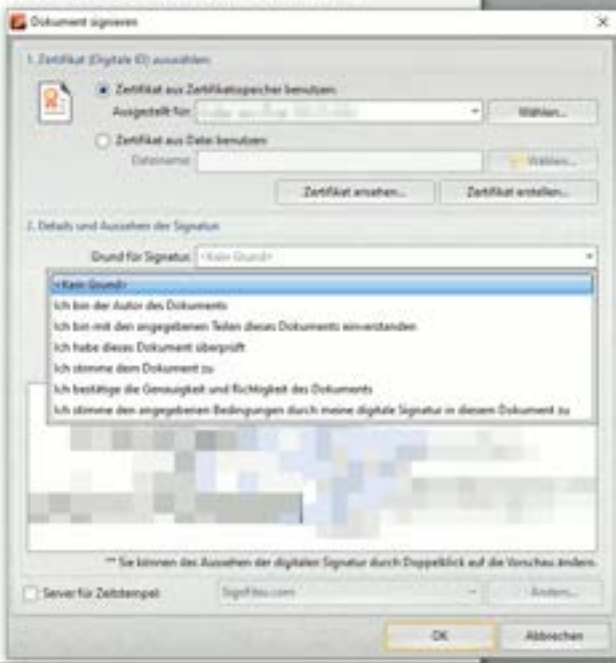
Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder sollte dieser Vertrag Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Anfüllung der Lücke ist diejenige wirksame Bestimmung zu vereinbaren, welche dem Sinn und Zweck der unwirksamen Bestimmung entspricht oder am nächsten kommt.

Unterschriften der Parteien:

[Datum, Ort] _____

[Datum, Ort] _____

[Datum, Ort] _____



Dokumentensignatur

Zweck Zertifikat:
Identitätsnachweis Unterzeichner

An aerial photograph of a green soccer field with white boundary lines. A central circle is drawn on the field. Several players in various colored jerseys are scattered across the field. Two goalposts are visible at the ends of the field. The field is surrounded by a concrete or asphalt border.

Begegnung

Ressourcen vs. Schlüssellänge

Zu erwartende Aufwände für Primfaktorzerlegung einer RSA-Zahl

n: Bit-Größe der RSA-Zahl

MD: Rechen-Tiefe

T: Fehlerkorrektur

	Abstract Qubits	Measurement Depth	Toffoli+T/2 Count
Factoring RSA integers	Asymptotic		
Vedral et al. 1996 [87]	$7n + 1$	$80n^3 + O(n^2)$	$80n^3 + O(n^2)$
Zalka 1998 (basic) [90]	$3n + O(1)$	$12n^3 + O(n)$	$12n^3 + O(n^2)$
Zalka 1998 (log add) [90]	$5n + O(1)$	$600n^2 + O(n)$	$52n^3 + O(n^2)$
Zalka 1998 (fft mult) [90]	$\approx 96n$	$\approx 2^{17}n^{1.2}$	$\approx 2^{17}n^2$
Beauregard 2002 [6]	$2n + 3$	$144n^3 \lg n + O(n^2 \lg n)$	$576n^3 \lg^2 n + O(n^3 \lg n)$
Fowler et al. 2012 [28]	$3n + O(1)$	$40n^3 + O(n^2)$	$40n^3 + O(n^2)$
Häner et al. 2016 [42]	$2n + 2$	$52n^3 + O(n^2)$	$64n^3 \lg n + O(n^3)$
(ours) 2019	$3n + 0.002n \lg n$	$500n^2 + n^2 \lg n$	$0.3n^3 + 0.0005n^3 \lg n$
Solving elliptic curve DLPs	Asymptotic		
Roetteler et al. 2017 [74]	$9n + O(\lg n)$	$448n^3 \lg n + 4090n^3$	$448n^3 \lg n + 4090n^3$



2001 – 7 Qubits – IBM

2005 – 8 Qubits – Uni Innsbruck

2011 – 16 Qubits – Uni Innsbruck

2017 – 20 Qubits – IBM

2018 – 72 Qubits – Google

2020 – 127 Qubits – IBM

2023 – 433 Qubits – IBM

2048 Bits RSA Schlüssel – Issuing CA

4096 Bits RSA Schlüssel – Root CA



When we set the upper limit of PC-DOS at 640K,

we thought nobody would ever need that much memory

1985 – Bill Gates

Working Group

Quantum-safe Security

The goal of this working group is to support the quantum-safe cryptography community in development and deployment of a framework to protect data whether in movement or at rest.

[View Current Projects](#)

Practical
Preparations
for the Post-
Quantum World

Download

[RESEARCH TOPICS](#)[ABOUT TOPIC](#)[WORKING GROUP](#)[DISCUSSION COMMUNITY](#)[PUBLICATIONS](#)

Countdown to Y2Q

07 91 14 06 26

Years

Days

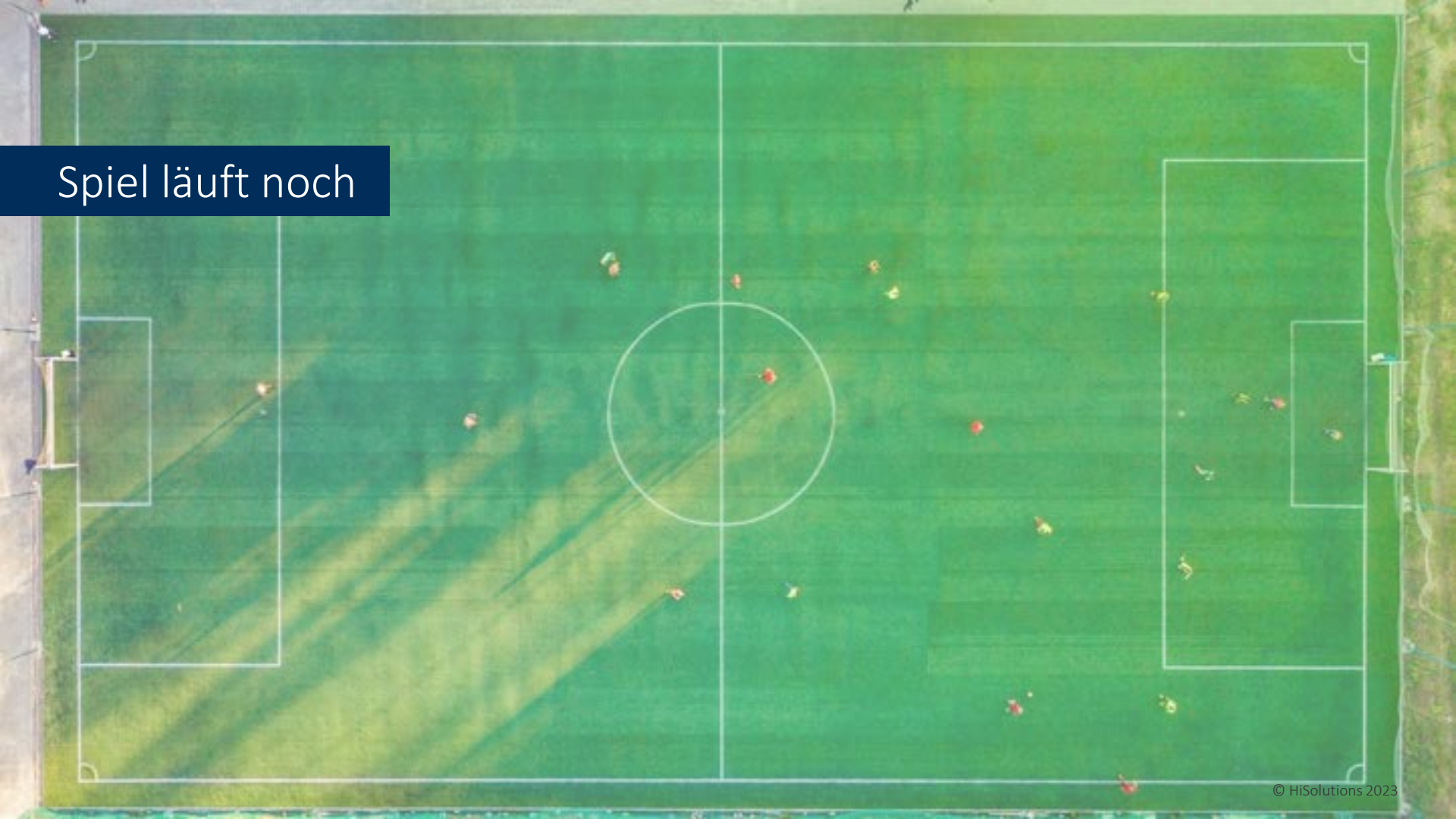
Hours

Minutes

Seconds

<https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/>

Spiel läuft noch



RFC5280 – X.509 Zertifikate

RFC3279 – Algorithmen und Identifier

Kein PQC-Algorithmen



IACR - Cryptology ePrint Archive
“The Viability of Post-Quantum X.509 Certificates”

A group of children in colorful winter jackets are playing soccer on a green artificial turf field. A soccer goal is visible in the background. The scene is outdoors with trees and a fence in the distance.

meisten PQ-Schemas: Public Key und Signaturen sind um Faktoren größer

Aktuelle Verfahren: kleiner 520 Bytes

Bei Dokumenten/Code-Signaturen vermutlich kein Problem

Bei Kommunikationsverbindungen ein nicht zu verachtender Mehraufwand

Größe in Bytes (von NIST Submissions)

Algorithmus	Öffentlicher Schlüssel	Chiffretext / Signatur
RSA	256 bis 512	256 bis 512
Kyber	800 bis 1.568	786 bis 1.568
CRYSTALS-Dilithium	1.312 bis 2.592	2.420 bis 4.595
Falcon	897 bis 1.793	666 bis 1.280
Sphincs	32 bis 64	7.856 bis 49.856
Classic-McEliece	262.144 bis 1.048.576	128 bis 240



Krypto-Agilität

X.509 für anerkannte PQ-Schemas erweitern

Protokolle identifizieren für die große X509-Zertifikate ein Problem darstellen

Alternativen Zertifikatsaustausch spezifizieren

Parallele / Hybrid Komposition PKI



Fragen ?



Ihr Ansprechpartner

Barbara Drotzig

info@hisolutions.com
Fon: +49 30 333 289-0

Algorithmen extrem schnell und der Cipher-Text ist der bisher kleinste aller NIST-Post-Quanten-Kryptografie-Kandidaten.

VERFAHREN DER ZUKUNFT

Auch das BSI hat bereits erste Empfehlungen ausgesprochen. Dazu zählen z. B. die Entwicklung von kryptoagilen Lösungen und die Verwendung von Post-Quanten-Kryptographie-Algorithmen in hybrider Form. Hybrid bedeutet die Kombination mit klassischen kryptografischen Algorithmen, da viele Verfahren noch sehr jung und wenig erprobt sind. Dies führt zu den nächsten Herausforderungen. Kryptografische Protokolle müssen weiterentwickelt werden und die Public-Key-Infrastruktur muss in der Lage sein, Zertifikate zu verarbeiten, die sowohl die längeren klassischen Schlüsseln als auch die quantensicheren Schlüsseln enthalten.

Auch wenn es bisher nur sehr wenige offizielle Lösungen gibt, die die asymmetrischen kryptografischen Verfahren ersetzen, kann man heute schon einiges tun.

- Sensibilisierung für das Thema
 - Vorbereitung auf die Migration
 - Verantwortlichkeiten finden
 - Identifizierung der Bausteine wo werden in der Organisation kryptografische Produkte eingesetzt und welche IT
 - Migrationskonzept erstellen
- Umsetzung der Maßnahmen, die bereits zertifiziert sind
 - Migration auf größere Schlüsselängen (mind. 256 Bit bei symmetrischen Verfahren)
 - Flexible Gestaltung der kryptografischen Mechanismen um kommende Standards einfacher/schneller umsetzen zu können (Kryptoagilität)

IHR QUANTENSPRUNG MIT HISOLUTIONS

Unsere Experten von HiSolutions analysieren für Sie Ihre spezifischen Systeme, die kryptografische Verfahren verwenden. Danach werden die notwendigen Änderungen für die Migration zu Post-Quanten-Kryptografie-Lösungen unter Berücksichtigung spezifischer Anforderungen identifiziert. Dabei entwickeln wir für Sie geeignete Migrations- und Übergangslösungen. Ebenfalls möchten wir das Bewusstsein für die Problematik schärfen, die sich aus der Entwicklung der Quantenformatik für Unternehmen ergibt.

Mehr Informationen zum Quantencomputer und den Gefahren durch wie Lösungsmöglichkeiten finden Sie in einem [Dokument des BSI](#) oder in unserem Beitrag im [HiSolutions Research Blog](#).

VORGEHENSWEISE: MIGRATION ZUR POST-QUANTEN-KRYPTOGRAFIE

1. Entscheidung zur Migration
 - a. Sensibilisierung
 - b. Entscheidung zur Migration
2. Vorbereitung auf die Migration
 - a. Festlegung der Verantwortlichkeit
 - b. Identifizierung der Ressourcen
 - c. Festlegung der Post-Quanten-Kryptografie-Verfahren
 - d. Analyse der vorhandenen Public-Key-Infrastruktur
3. Planung der Migration
 - a. Erstellung eines Umsetzungsplans
 - b. Risikomanagement
 - c. Planung von Auslastzeiten
4. Durchführung der Krypto-Strukturanalyse
 - a. Klassifizierung von Informationen
 - b. Durchführung der Krypto-Strukturanalyse
 - c. Outsourcing Identifizierung der relevanten Dienstleister
 - d. Identifizierung der eingesetzten kryptografischen Verfahren
5. Durchführung der Migration
 - a. Migration der Verfahren
 - b. Reporting
6. Überprüfung der Migration
 - a. Durchführung eines technischen Audits



Wir sind auch immer auf der Suche nach Werkstudenten

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com