EBICS-Forum Schweiz 2025

SIX ConventionPoint, Zürich

19. Mai 2025

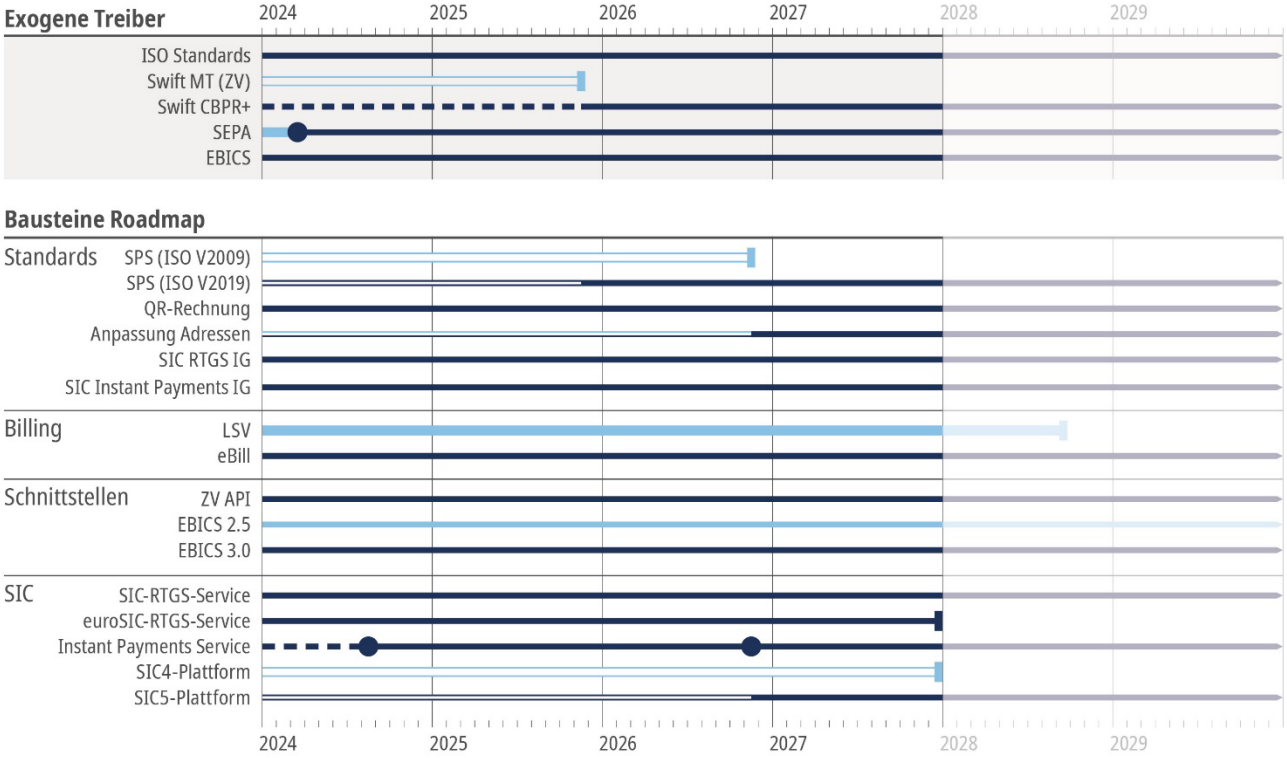
Agenda

ZEIT	THEMA	REFERIERENDE
10.00 Uhr	**Begrüssung**	Martin Walder
10.05 Uhr	**Eröffnung des Forums**	Boris Brunner
10.10 Uhr	**Swiss Market Practice Updates**	Corinne Bellwald
10.25 Uhr	**Die Migration vom MBS zu EBICS 3.x in Österreich – ein Update**	Werner Guttmann
10.45 Uhr	PAUSE	
11.10 Uhr	**Quantencomputer: Revolution und Risiko**	Christian Bühler
11.30 Uhr	**Sicherheit in EBICS: Ein langer Weg von EBICS 3.0 zu 4.0**	Werner Guttmann
11.50 Uhr	**Abschluss und Fragen**	Corinne Bellwald
12.00 Uhr	Stehlunch	
13.30 Uhr	**Deep-Dive-Session: Sicherheit in EBICS 4.0 – Technische Vertiefung in Szenarios**	Werner Guttmann Dr. Alain Hiltgen

Swiss Market Practice Updates

Corinne Bellwald
Senior Standards Manager

Roadmap Zahlungsverkehr Schweiz

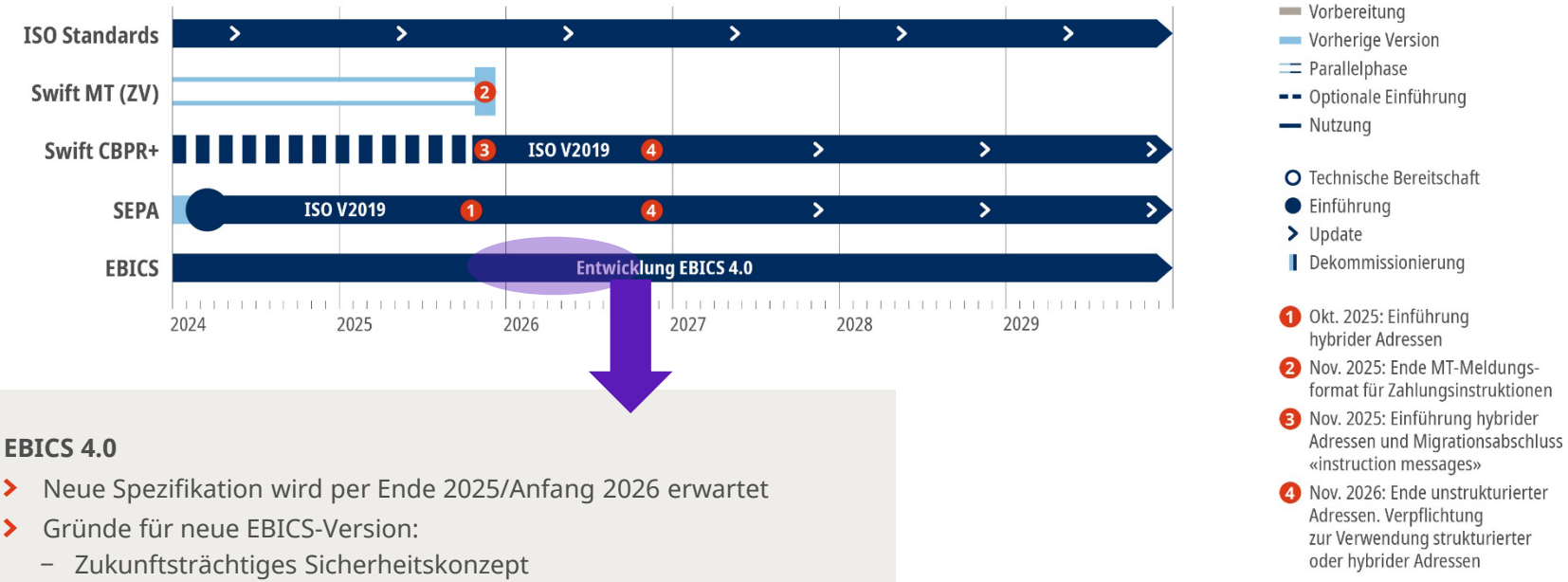


- Vorbereitung
- Vorherige Version
- Parallelphase
- Optionale Einführung
- Nutzung

- Technische Bereitschaft
- Einführung
- Update
- Dekommissionierung

Planung 2028/2029 noch offen

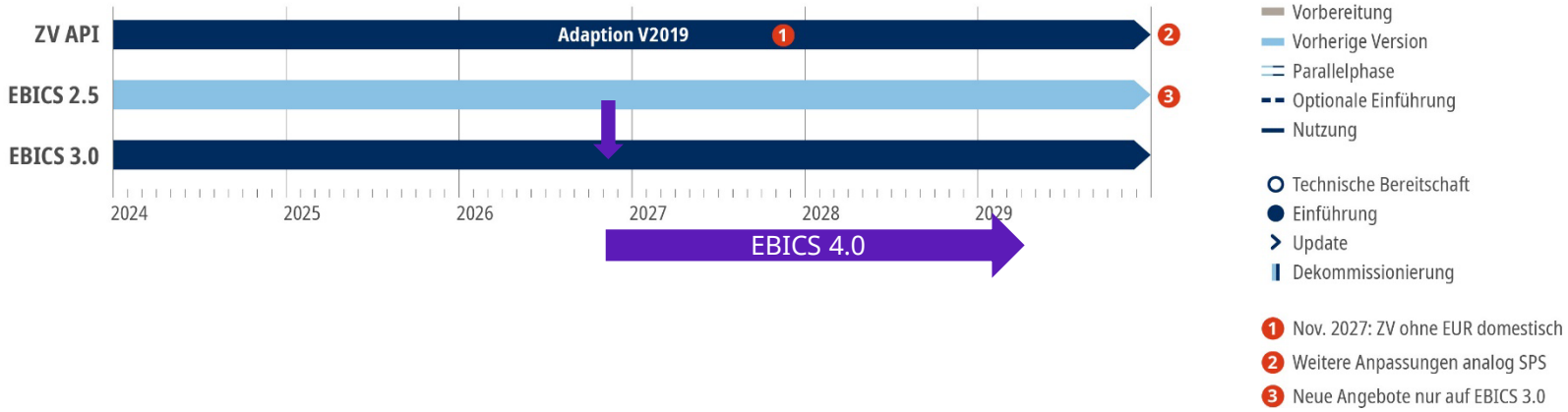
Exogene Treiber



EBICS 4.0

- Neue Spezifikation wird per Ende 2025/Anfang 2026 erwartet
- Gründe für neue EBICS-Version:
  - Zukunftsträchtiges Sicherheitskonzept
  - Überarbeitung veralteter Aspekte
  - Neue Funktionen

Kunde-Bank-Schnittstellen

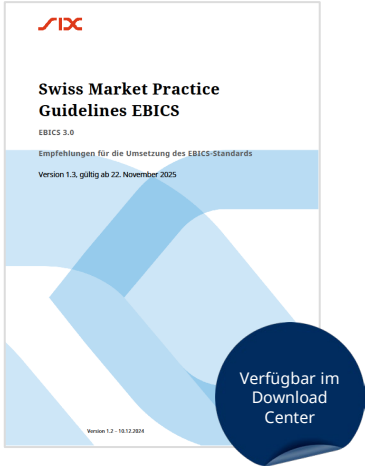


Von EBICS 2.5 auf EBICS 3.0

- Vorantreiben der Migration auf EBICS 3.0 bis November 2026 (Ende der Grace Period)
- EBICS 3.0 als Zielversion für alle neuen Angebote

Swiss Market Practice Guidelines EBICS 3.0

Version 1.3



- Inkraftsetzung: 22. November 2025
- Überarbeitete Kapitel:
  - 2.2.1 EBICS Timeline
  - 5.4.1 Attribut «Version»

Ausgangslage heute (Version 1.2)

- Obligatorische Verwendung des Attributes «Version» für die ISO-20022-Meldungen der Swiss Payment Standards

Ausgangslage ab November 2025 (Version 1.3)

- Serverseitig unterstützten alle Finanzinstitute, die im Schweizer Markt tätig sind, bei der Ein- und Auslieferung von ISO-20022-Meldungen sowohl die Variante mit Attribut «Version» als auch ohne Attribut «Version».

Entscheidungsgrundlagen

- Vereinfachung der Zusammenarbeit mit anderen Finanzmärkten
- Fortlaufende Unterstützung von Self-Service-Lösungen
- Kein Parsing/Pre-Processing notwendig
- Zukunftsorientierte Lösung für parallel betriebene Meldungsversionen

Weitere Unterlagen zu EBICS in unserem Download Center

Swiss Market Practice Guidelines EBICS 2.5

- Status: in Revision
- Publikation der Version 1.4 geplant für Q3/Q4 2025
- Überarbeitete Themen
  - Errata bezüglich institutsspezifischen Auftragsarten
  - Anpassung der Zahlungsarten

EBICS 3.0 BTF – AA List CH

- Status: Aktualisierung bei Bedarf

EBICS offering Matrix of Swiss financial institutions

- Status: Aktualisierung bei Bedarf

EBICS FAQ

- Status: in Erarbeitung

Q&A

Corinne Bellwald

Senior Standards Manager, SIX

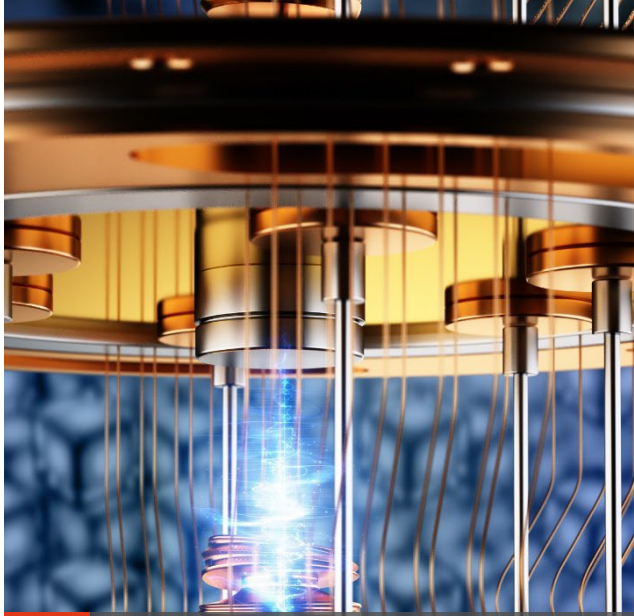
corinne.bellwald@six-group.com

Quantencomputer: Revolution und Risiko

Christian Bühler
Senior IT Security & Compliance Officer

Die Wichtigkeit von Kryptografie

- **Kryptografie** ist **zentral** in vielen Bereichen unseres Alltags
- **Quantencomputer als Herausforderung**
  - Nutzen die Quantenmechanik, um Aufgaben **exponentiell schneller** zu lösen als herkömmliche Computer
  - **Asymmetrische**[1] Algorithmen können **gebrochen** werden
  - **Symmetrische**[2] Algorithmen und Hash-Funktionen sind **nicht nennenswert betroffen**
- **Auswirkungen und Folgen**
  - Quantencomputer werden die **Sicherheit** sensibler Daten und kritischer Anwendungen (Blockchains, Onlinebanking, Messaging-Dienste, Finanztransaktionen) **stark gefährden**



Wie kann man **Kryptosysteme entwickeln**, die **resistent gegenüber Quantencomputern** sind?

Dieses Teilgebiet der Kryptografie wird als **Post-Quanten-Kryptographie (PQC)** bezeichnet.

Source: GettyImages.advanth

1) z.B. RSA für Signaturen oder Diffie-Hellman für den Schlüsselaustausch
2) z.B. AES-256 Verschlüsselung oder SHA-256

Quantencomputer – wo stehen wir?

Angreiferperspektive

- **Qubits** (Quantenbits) bestimmen die Leistungsfähigkeit von Quantencomputern
- **Atom Computing**[1)] kündigt **2023** den ersten industriellen Quantencomputer mit **+1000** Qubits an
- **IBM** prognostiziert:
  - Bis **Ende 2025** Quantencomputer mit **4.000 Qubits** herzustellen[2)]
  - Bis **2033** einen Computer mit **100.000 Qubits** zu entwickeln[3)]
- Schätzungen zufolge sind etwa **20.000.000 Qubits** erforderlich, um den asymmetrischen kryptografischen Algorithmus RSA 2048 innerhalb von 8 Stunden zu brechen.[4)]

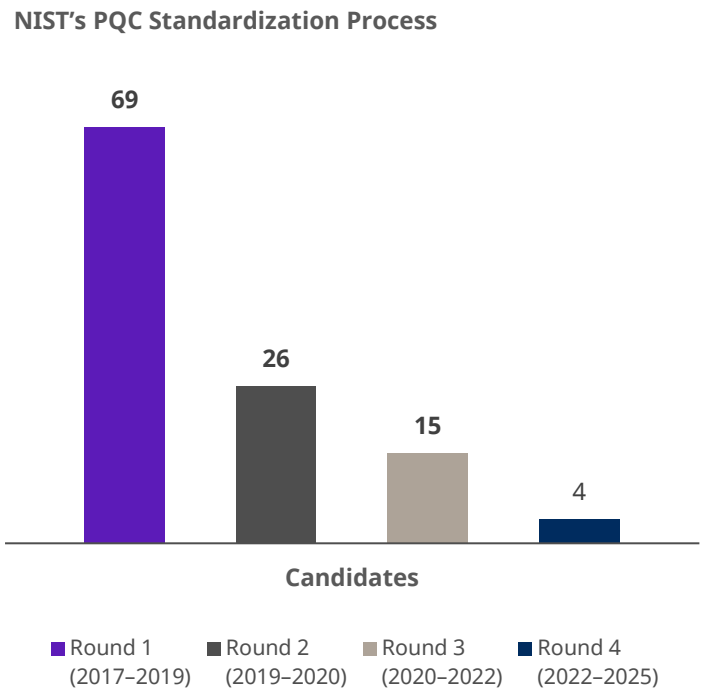
[1)] Atom Computing Quantum startup Atom Computing
[2)] IBM: IBMs Pläne für das Quanten-Supercomputing
[3)] IBM: Charting the course to 100,000 qubits
[4)] Federal Office for Information Security (BSI) (August, 2023): The status of quantum computer development

Quantensichere Kryptografie – Status Quo

Verteidigungsperspektive

- National Institute of Standards and Technology (NIST) führt seit 2017 einen Auswahlprozess durch, um die besten quantensicheren PQC-Verfahren zu evaluieren, die als neue kryptografische Standards gelten sollen
- Drei Algorithmen wurden im **August 2024** standardisiert: FIPS-203, FIPS-204 und FIPS-205
- Zwei weitere Kandidaten wurden zur Standardisierung ausgewählt: FALCON und HQC

Der **Forschungsbereich** der **Post-Quanten-Kryptographie** ist relativ **jung** und anfällig für **Schwachstellen**.[1)]

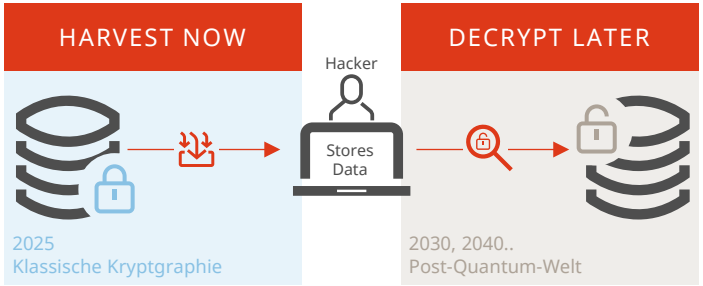


[1)] Post-quantum encryption contender is taken out by single-core PC and 1 hour | Ars Technica

Heutige Bedrohungen durch Quantencomputer

«Harvest Now, Decrypt Later»

Angreifer sammelt bereits heute grosse Datenmenge, indem verschlüsselter Netzwerkverkehr mitgelesen und abgelegt wird.



Angreifer speichert Daten, in der Hoffnung, dass diese in Zukunft mithilfe Quanten-computer entschlüsselt werden können.

Typische Ziele solcher Attacken:

- Regierungsgeheimnisse
- Medizinische Daten
- Personenbezogene Daten und Finanz-informationen (z. B. SIC-Transaktionen)

Typische Angreifer:

- Staatliche Akteure
- Cyberkriminelle Gruppen
- Insider

Aufgrund der potenziell sehr langlebigen Sensibilität von Finanztransaktion und der breiten Anwendbarkeit, stellt diese Attacke eine ernstzunehmende Bedrohung dar, die eine rasche Mitigation verlangt.

Swiss Interbank Clearing (SIC)

Das zentrale Schweizer Zahlungssystem

>1

Milliarde

verarbeitete Transaktionen

57

Billionen

CHF Umsatz

99,97%

Systemverfügbarkeit

KPIs 2024

- Seit 1987 verarbeitet SIX im Auftrag der Schweizerischen Nationalbank bargeldlose **Interbank-Zahlungen** über das SIC-System höchst effizient, in Echtzeit und rund um die Uhr.
- Als Systemmanagerin überwacht und steuert die **Schweizerische Nationalbank (SNB)** das wichtigste Schweizer Zahlungssystem.
- Das SIC-System verarbeitet sowohl **Hochbetragszahlungen** (High Value Payments) als auch **Kundenzahlungen** (Retail Payments) auf der gleichen technischen Plattform und bietet so eine effiziente Basis für den Schweizer Zahlungsverkehr.

PQC – Erwartungshaltung der SNB und des Finanzplatzes

- Speziell für das SIC-System entwickelte Lösung: **Sicherheitssoftware SASS** (SIX Advanced Security Server) in Kombination mit **Schweizer HSM** (Hardware-Sicherheitsmodul) zur Authentisierung und Chiffrierung von Meldungen
- SNB und Finanzplatz erwarten von der SIC AG, sich auf die **Post-Quanten-Ära vorzubereiten**, getrieben durch:
  - *«Harvest Now, Decrypt Later»* – eine Form von Attacke, auf die es *asap* zu reagieren gilt
  - Beobachtung von ähnlichen Anstrengungen bei Finanzmarktinfrastrukturen international

Grundsatz:

Schutz der Vertraulichkeit & Integrität der im SIC-System ein- und ausgehenden Zahlungsmeldungen

SIC AG analysierte 2024 folgende **Fragestellungen:**

- Erstellung eines **Kryptoinventars** für das SIC-System. Wo kommen im SIC welche Verfahren für welche Daten zum Einsatz und wie sind diese hinsichtlich PQC-Sicherheit zu bewerten?
- Was sind die **Risiken** für das SIC-System und was die kurz-, mittel- und langfristig empfohlenen Massnahmen?
- Wie wird die **Kryptoagilität** des SIC-Systems bewertet?

Erste Erfolge und nächste Schritte (SIC-System)

2023	2024	2025	2026…
Umstellung auf symmetrische Verschlüsselungs-mechanismen	Start Einführung neue HSM-Generation (unterstützt Post-Quanten-Algorithmen) Durchführung PQC-Analyse im SIC-System	Einführung Post-Quanten-Schlüsselaustausch im SIC-System und Start Pilotbetrieb	Post-Quanten-Schlüsselaustausch produktiv Einführung HSM-Generation abgeschlossen Einführung hybrider Signaturen Erhöhung Agilität im Sicherheits-Setup

Zusammenfassung

Quantencomputer stellen ein hohes Risiko für die IT-Sicherheit dar

- Wirken sich direkt auf die Menschen, Technologien und Prozesse aus
- Regulierungsbehörden erkundigen sich und fordern bereits heute PQC-Strategien

Die Umstellung der Kryptografie-Implementierungen auf PQC wird äusserst komplex sein

Unterscheidung zwischen asymmetrischen und symmetrischen Algorithmen

Q&A

Christian Bühler

Senior IT Security & Compliance Officer, SIX

christian.buehler1@six-group.com

PSA

1

EBICS FORUM

Sicherheit in EBICS – ein langer Weg von EBICS 3.0 zu 4.0

TLP:AMBER

PSA

ME, MYSELF AND I

- Senior Business-Analayst bei der Payment Services Austria (PSA)
- Moderiere/leite die Österreichische EBICS AT Gruppe (alle österreichischen Banken vertreten)
- Vertrete Österreich in der EBICS SC *working group*
- Lead der EBICS 4.0 ***security rework*** Sub-Gruppe
- Tätig seit 01.01.2023

EBICS 4.0 - SUBGRUPPEN

- Security rework
- Performance and technical aspects
- Improvements for communication
- Digitalization and automation
- Compliance
- XML-Schema

PSA

2

EBICS FORUM

PROBLEME

TLP:AMBER

SECURITY REWORK - PROBLEME

- Bestimmte sicherheitsrelevante Details sind ausschließlich in der Spezifikation verschriftlicht (und nur dort)

```
<BankPubKeyDigests>
   <Authentication Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" Version="X002">
      P6GIOJBug/49yZEW/KwC8zW+3UrqUHmrHAaOpd8hfsk=
   </Authentication>
   <Encryption Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" Version="E002">
      13vXTEVcq9xOdfT0KLUkQvBpD2r8CcULgQPdo6/pyqQ=
   </Encryption>
</BankPubKeyDigests>
```

- **X002** = ?, **E002** = ?, **A005/A006** = ?

SECURITY REWORK – PROBLEME (2)

- X002 = ???

11.1.1 Verfahren

Authentifikationssignaturen basieren auf dem RSA-Signaturverfahren. Die folgenden Parameter bestimmen das Verfahren zur Authentifikationssignatur: Länge des (geheimen) RSA-Schlüssels, Hashalgorithmus, Paddingverfahren, Kanonisierungsverfahren.

Für die Authentifikationssignatur definiert EBICS das **Verfahren „X002“** mit den folgenden Parametern:

Parameter	**Wert**
Schlüssellänge in KBit	>=2KBit (2048 Bit) und <=16KBit
Hashalgorithmus	SHA-256
Paddingverfahren	PKCS #1
Kanonisierungsverfahren	http://www.w3.org/TR/2001/REC-xml-c14n-20010315

SECURITY REWORK – PROBLEME (2)

- Ändern sich die Voraussetzungen, kann es zu einer (major) Änderung in der Spezifikation und damit zu einem Versionssprung kommen
- Dies führt zu unnötigem **version creep**

SECURITY REWORK – PROBLEME (3)

- Diverse administrative order types für das key magagement (HCS, HPB, …)
  - HPB … Bezug der „öffentlichen Bankenschlüssel“
  - HCS … Upload der Teilnehmerschlüssel
- minimal key size = 2K, max key size = 16K
- Signal für „Bankenschlüssel haben sich geändert“
- RSA als corner stone der EBICS Spezifikation
- Beginnende Diskussion zu nationalen (Export-) Beschränkungen ab einer bestimmten key size
  - *Ausgelöst durch: Anfrage* einer französischen CA an die EBICS SC zur verpflichtenden Einführung von 16K keys

SECURITY REWORK – PROBLEME (4)

- Aktuelle mögliche Entwicklungen
  - z.B. RSA (in einer bestimmten key size) nicht mehr als ausreichend sicher eingestuft
  - *elliptic curve cryptography* Algorithmen als (ausreichend) sicher eingestuft
  - *hybrid cryptography* Algorithmen als wünschenswert eingestuft
- Jede dieser möglichen/notwendigen Änderungen kann zu einer (major) Änderung in der Spezifikation und damit zu einem Versionssprung führen
- Dies führt zu unnötigem **version creep**
- Außerdem erhöht sich die Komplexität der Spezifikation per se, und die notwendige Pflege (weiterer minor version creep)

PSA

3

EBICS FORUM

ANSATZ

TLP:AMBER

SECURITY REWORK – ANSATZ

- Alle relevanten Sicherheitsinformationen müssen **explizit** in jedem XML *request/response payload* ausgedrückt sein (bzw. dürfen nicht mehr in Form von Text-Blöcken in der Spezifikation stehen)

```
<BankCertificates>
   <Authentication Algorithm="http://www.w3.org/2001/04/xmlenc#sha256">
      P6GIOJBug/49yZEW/KwC8zW+3UrqUHmrHAaOpd8hfsk=
   </Authentication>
</BankCertificates>
```

SECURITY REWORK – ANSATZ

- Aus den vorher genannten Gründen (Verfügbarkeit, Einstufung als sicher, …) bedarf es weiters einer **Security Negotiation**, welche …
  - **sicher (**per se**)**
  - **ausreichend flexibel** (neue Algorithmen, die sich am Markt durchsetzen, können in Zukunft herangezogen werden)
  - **ausreichend reduzierbar** (ehemals als sicher geltende Algorithmen dürfen ab einem Stichtag nicht mehr herangezogen werden)
- Und welche einen *agreed-upon, shared* **security context** zwischen den beiden Parteien etabliert

PSA

4

EBICS FORUM

SECURITY NEGOTIATION

TLP:AMBER

SECURITY REWORK – ECKPUNKTE

- Neue administrative **order types** zur dynamischen Herstellung eines sicheren **security contexts** zwischen dem EBICS Client und Server
  - SCN … security context **negotiate**
  - Key management requests/responses
  - SCV … security context **verify**

SECURITY REWORK – SCN

- SCN … security context **negotiate**
  - Wird immer durch den Client angestoßen
  - Der Client übermittelt eine Liste an Algorithmen, die er unterstützen könnte (und für welche er eventuell selbst valide Zertifikate besitzt) und zwar für beide Richtungen (up-/downstream)
  - Der Server vergleicht diese Liste an möglichen Algorithmen mit seiner eigenen Konfiguration (Liste an Algorithmen, Zertifikats-Speicher) und **bestimmt** die zu verwendende Technologien (up-/down-stream) und schickt diese in der SCN response zurück; weiters schickt er in dieser Antwort alle relevanten Server-Zertifikate mit (eventuell redundant)

SECURITY REWORK – KEY EXCHANGE

- Upload von notwendigen Client-Zertifikaten (HCS)
  - optionaler Schritt, da sich eventuell für up-stream Nachrichten eventuell nichts ändert (da Client und Server auf bereits etablierten Algorithmen und Zertifikaten verharren)

SECURITY REWORK – SCV

- SCN … security context **verify**
  - Wird immer durch den Client angestoßen
  - Der Client übermittelt einen Hash-Wert über alle im Rahmen der security negotiation ausgetauschten Nachrichten
    - SCN request/response (inkl. Zertifikate)
    - optional: HCS request/response
- Der Server verifiziert den übermittelten Hash-Wert gegen einen lokal errechneten Hash-Wert (auf Basis der 2/4-Nachrichten) und aktiviert bei erfolgreichem Check einen neuen Security Context

PSA

5

EBICS FORUM

SECURITY CONTEXT

TLP:AMBER

SECURITY REWORK – SECURITY CONTEXT

- Dualität Client/Server (immer in sync)
- Eindeutige Identifikation über eine UUID
- Unterscheidung zwischen **aktivem** und **pending** Security-Kontext (temporäres Konstrukt während der security negotiation); hinterlegt mit
- Weist die notwendigen security algorithms (up-/downstream; encryption/authentication/signature) aus
- Enlists die jeweiligen Zertifikate (Client-Zertifikate, Server-Zertifikate, …)
- Diese kommen aber in einem separaten **certificate store** zu liegen

PSA

6

EBICS FORUM

SAMPLE FLOW
(EC as new server technology)

TLP:AMBER

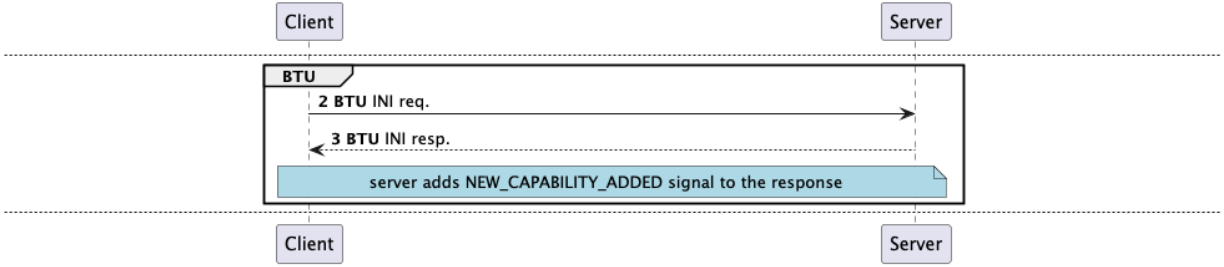
SECURITY REWORK – SAMPLE FLOW

- **Preconditions**
  - Client/Server unterstützen RSA als Technologie, Client unterstützen EC als Technology
  - Client/Server haben gültige RSA Certs (per se), Client hat gültiges EC Cert
  - Client/Server haben zu einem früheren Zeitpunkt bereits eine *security negotiation* abgewickelt und sich auf RSA up, RSA down als Technologie verständigt und auch RSA-up/RSA-down Certs ausgetauscht
- **Auslöser**
  - Server Admin fügt EC als Technologie hinzu

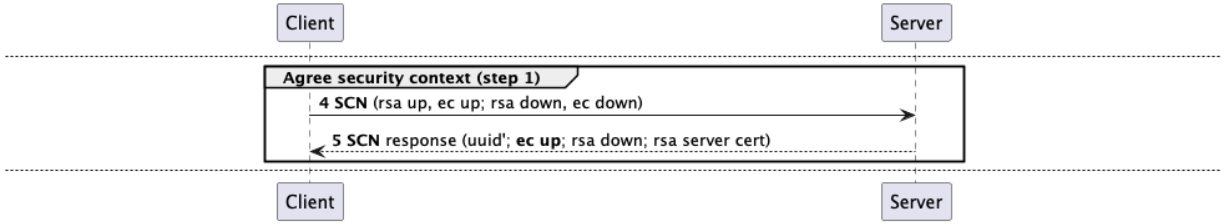
SECURITY REWORK – SAMPLE FLOW

SECURITY REWORK – SAMPLE FLOW

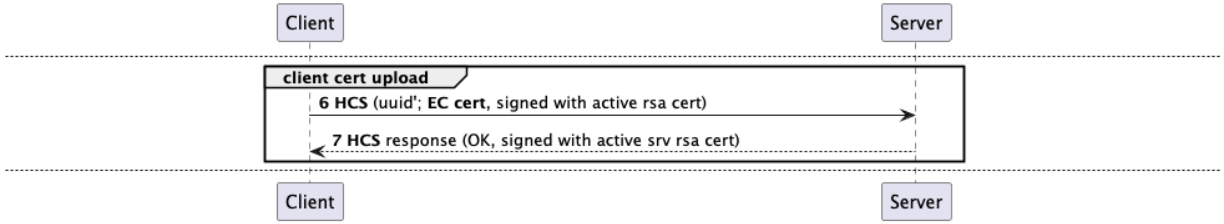
SECURITY REWORK – SAMPLE FLOW (2)



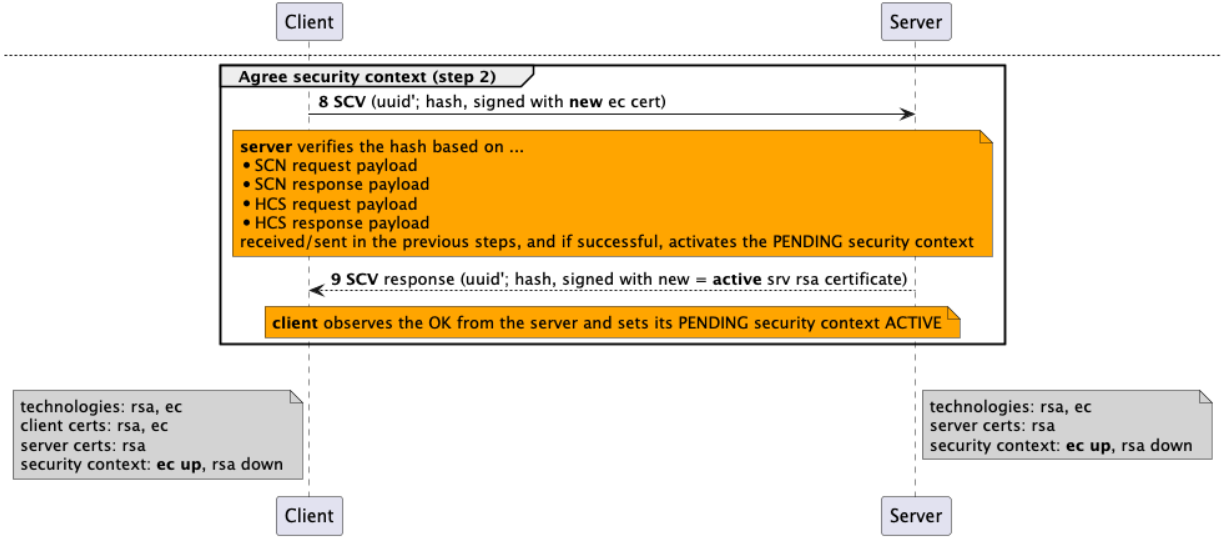
SECURITY REWORK – SAMPLE FLOW (3)



SECURITY REWORK – SAMPLE FLOW (3)



SECURITY REWORK – SAMPLE FLOW



PSA

7

EBICS FORUM

NOCH OFFEN

TLP:AMBER

SECURITY REWORK – OFFENE PUNKTE

- *Period of validity of the security contexts*
- *Frequency of establishing* (je TLS Session; alle 24h; …)
- Veröffentlichung und Pflege eines **minimalen Sets** an Algorithmen (Stichwort: garantierte Interoperabilität)
  - Zumindest in Form eines versionierten *implementation guides*
  - *Governance dessen*
  - Eventuell als elektronische abrufbare Resource
  - Definition von *phase-out periods* (Stichtage, …)

SECURITY REWORK – AUSWIRKUNGEN

- Aushandlung eines aktiven *security context* bewirkt die Einführung von **state**
- Wechsel von einem *stateless protocol* zu einem **stateful protocol**
- **State** gehört immer **managed** (mit all den damit verbundenen Nachteilen)
- → Sorgfältige Abwägung der Vor- und Nachteile dieser Vorgangsweise

SECURITY REWORK – STATE

- Relevante Ereignisse im Kontext von **state**
  - Upload neuer Schlüssel
  - Ablauf der *grace period* bei der Verwerfung eines Algorithmus
    - Wie viele *security contexts* habe ich aktuell am Server, welche zu invalidieren sind
  - Etc.

KONTAKT

IHRE FRAGEN?

PSA Payment Services Austria GmbH (PSA) ist ein Transaktionsdienstleister und das österreichische Kompetenzzentrum für den bargeldlosen Zahlungsverkehr. Als verlässlicher Partner bieten wir unseren Kunden Produkte in den Bereichen Karte, Konto und Identität und sorgen für sichere, schnelle und bequeme Transaktionen im In- und Ausland. Mit diesen Geschäftsfeldern wickelt PSA rund 3 Milliarden Transaktionen jährlich ab.

Für weitere Fragen stehen wir gerne zur Verfügung

PSA Payment Services Austria GmbH

Handelskai 92, Gate 2, 6.0G
1200 Wien
office@psa.at
www.psa.at

TLP:AMBER

All content, in this presentation © 2024 by PSA Payment Services Austria GmbH. All rights reserved.
Duplication or redistribution of the contents of this presentation are prohibited without prior written authorization.

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, “SIX”) for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.

© 2025 SIX Group Ltd. All rights reserved.