Post-Quantum

Cryptography Conference

Is your HSM quantum-ready? Here's what you need to know!

Every currently deployed HSM must be replaced with a quantum-safe HSM. But what is a quantum-safe HSM. First, it must itself utilize quantum-safe root keys and algorithms for its processing. Second, it must support quantum-safe firmware updates to remain agile and current as algorithms and protocols evolve. Third, it must provide access to PQC algorithms for application integration. These capabilities must be bult-in not bolted-on to an existing HSM. An HSM that exposes PQC algorithms but itself uses classic algorithms is NOT quantum-safe. This talk will explore these issues in detail.

Bruno Couillard
Co-Founder & CEO at Crypto4A

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

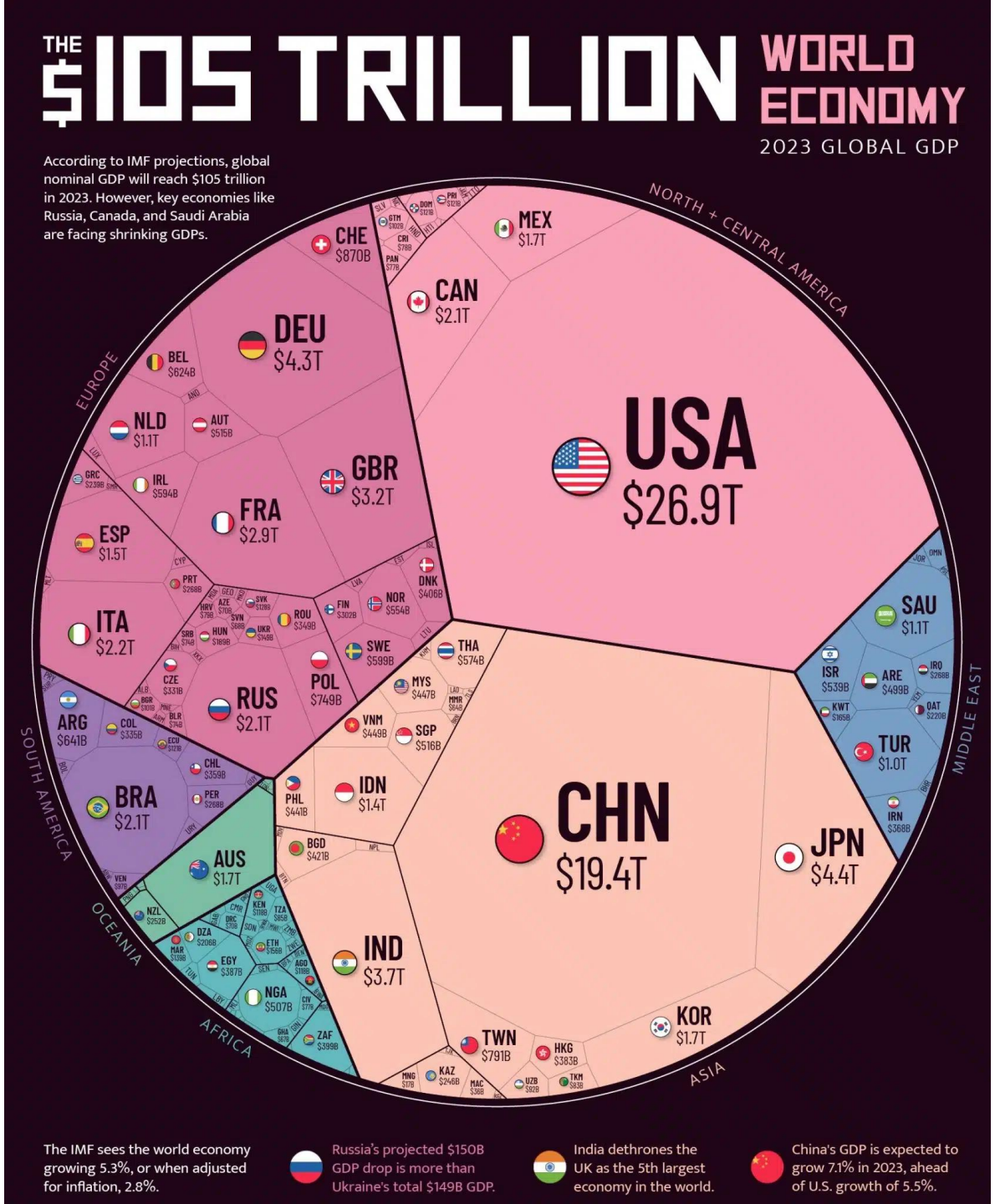
PKI Consortium

CRYPTO4A

Is your HSM quantum-ready? Here's what you need to know!

PKI Consortium Post-Quantum Cryptography Conference

January 15th to 16th 2025


THE $105 TRILLION WORLD ECONOMY
2023 GLOBAL GDP
According to IMF projections, global nominal GDP will reach $105 trillion in 2023. However, key economies like Russia, Canada, and Saudi Arabia are facing shrinking GDPs.
NORTH + CENTRAL AMERICA
EUROPE
MIDDLE EAST
SOUTH AMERICA
OCEANIA
AFRICA
ASIA
USA $26.9T
CHN $19.4T
DEU $4.3T
GBR $3.2T
FRA $2.9T
ITA $2.2T
ESP $1.5T
NLD $1.1T
BEL $624B
CHE $870B
AUT $515B
IRL $594B
DNK $406B
FIN $302B
NOR $554B
SWE $599B
POL $749B
ROU $349B
HUN $169B
UKR $149B
CZE $331B
RUS $2.1T
CAN $2.1T
MEX $1.7T
JPN $4.4T
KOR $1.7T
TWN $791B
HKG $383B
IND $3.7T
IDN $1.4T
THA $574B
MYS $447B
VNM $449B
SGP $516B
PHL $441B
BGD $421B
AUS $1.7T
NZL $252B
BRA $2.1T
ARG $641B
COL $335B
CHL $359B
PER $268B
SAU $1.1T
ARE $499B
ISR $539B
TUR $1.0T
IRN $368B
IRQ $268B
KWT $165B
QAT $220B
NGA $507B
EGY $387B
DZA $206B
ZAF $399B
KAZ $246B
The IMF sees the world economy growing 5.3%, or when adjusted for inflation, 2.8%.
Russia's projected $150B GDP drop is more than Ukraine's total $149B GDP.
India dethrones the UK as the 5th largest economy in the world.
China's GDP is expected to grow 7.1% in 2023, ahead of U.S. growth of 5.5%.

$35 Trillion

CRYPTO4A

What is an HSM?

- An HSM is Black-Box that provides:
  - Strong anti-tamper techniques to maintain the integrity of its functions
  - Mitigation services around side-channel attacks
  - Strong sources of entropy
  - Cryptographic services to external applications
  - Other ancillary services
- Used to guard private keys used to impart trusted digital identities

What does an HSM do?

- Key Generation, Key Storage & Key Usage
  - Crypto-Agility
- Ancillary Functions:
  - F/W Updates
  - External Key Storage (extended storage, backup, archival, etc…)
  - HSM to HSM communications
    - High-availability
    - Load-balancing
    - Geo-diversity
    - Auto-scaling/Auto-healing/Auto-rebalancing
- Attestation

HSM is both a Crypto Supplier & Consumer

- Supplier of cryptographic services:
  - Provides key generation, management and operational usage of cryptographic services via cryptographic APIs to external applications

- Consumer of cryptographic services:
  - F/W Updates
  - External key storage (extended storage, backup, archival, etc…)
  - HSM-to-HSM communications
  - Attestation
  - Anti-tamper
  - Secure-boot

Design Assurance/Compliance

- FIPS 140 / CAVP / NIAP / CSfC / …
  - Cryptographic algorithm compliance
  - Entropy design
  - Physical security

- Mainly concerned about the “Supply side” of things

What is a Quantum-Safe HSM?

- Supplier of post-quantum cryptographic services:
  - Provides key generation, management and operational usage of both classic and post-quantum cryptographic services via cryptographic APIs to external applications

- Consumer of cryptographic services:
  - F/W Updates
  - External key storage (extended storage, backup, archival, etc…)
  - HSM-to-HSM communications
  - Attestation
  - Anti-tamper
  - Secure-boot

What is not a Quantum-Safe HSM

- FIPS 140-3 validation of a classic HSM ≠ Quantum-Safe HSM
- Adding a QRNG to a classic HSM ≠ Quantum-Safe HSM
- A F/W update to a classic HSM ≠ Quantum-Safe HSM
- Adding quantum-algorithm support to a classic HSM ≠ Quantum-Safe HSM
- Shinny marketing material claiming “quantum-safe” ≠ Quantum-Safe HSM

Consider:

- FS-ISAC paper[1] – “Building **Cryptographic Agility** in the Financial Sector”
  - Second vendor

- HSM Refresh – Why not go with quantum-safe and crypto-agility?

1: https://www.fsisac.com/hubfs/Knowledge/PQC/BuildingCryptographicAgilityInTheFinancialSector.pdf

Thank you
bruno@crypto4a.com

You can’t achieve quantum readiness without
Quantum-safe Crypto-agile foundations - QxHSM™

CRYPTO4A