Implementing a Crypto Services Strategy at ABN AMRO Bank

Christiane Peters, IBM
Tiago Teles, ABN AMRO Bank

with inputs from Barbara Vieira, Jeroen van der Harst, and the ABN AMRO Crypto Services team

RWC 2020

Studies on encryption trends have shown that 45% of large organizations have implemented an enterprise-wide **“encryption and key management strategy”** in 2018 [1].

45%

ABN·AMRO IBM

[1] Ponemon Institute. “2019 Global Encryption Trends Study”. https://www.ncipher.com/2019/global-encryption-trends-study. 2019.

Let’s see how ABN AMRO started this journey in

2016

- Smart card CA for user authentication ☺
- TLS certificate management is a mailbox ☹
- Key management is a 3FA safe with good procedures 😐
- HSMs are kept up and running for payment systems (regulated) 😐
- Google and Microsoft announced SHA-1 Deprecation ☹

First Step: Definition Strategy in 2016

WHAT: Crypto Services Portfolio 2019

CS 2019 >>

1
Cryptographic Services Application

- Key and Certificate Management
- Data in Transit and Data at Rest
- Application of Crypto Solutions

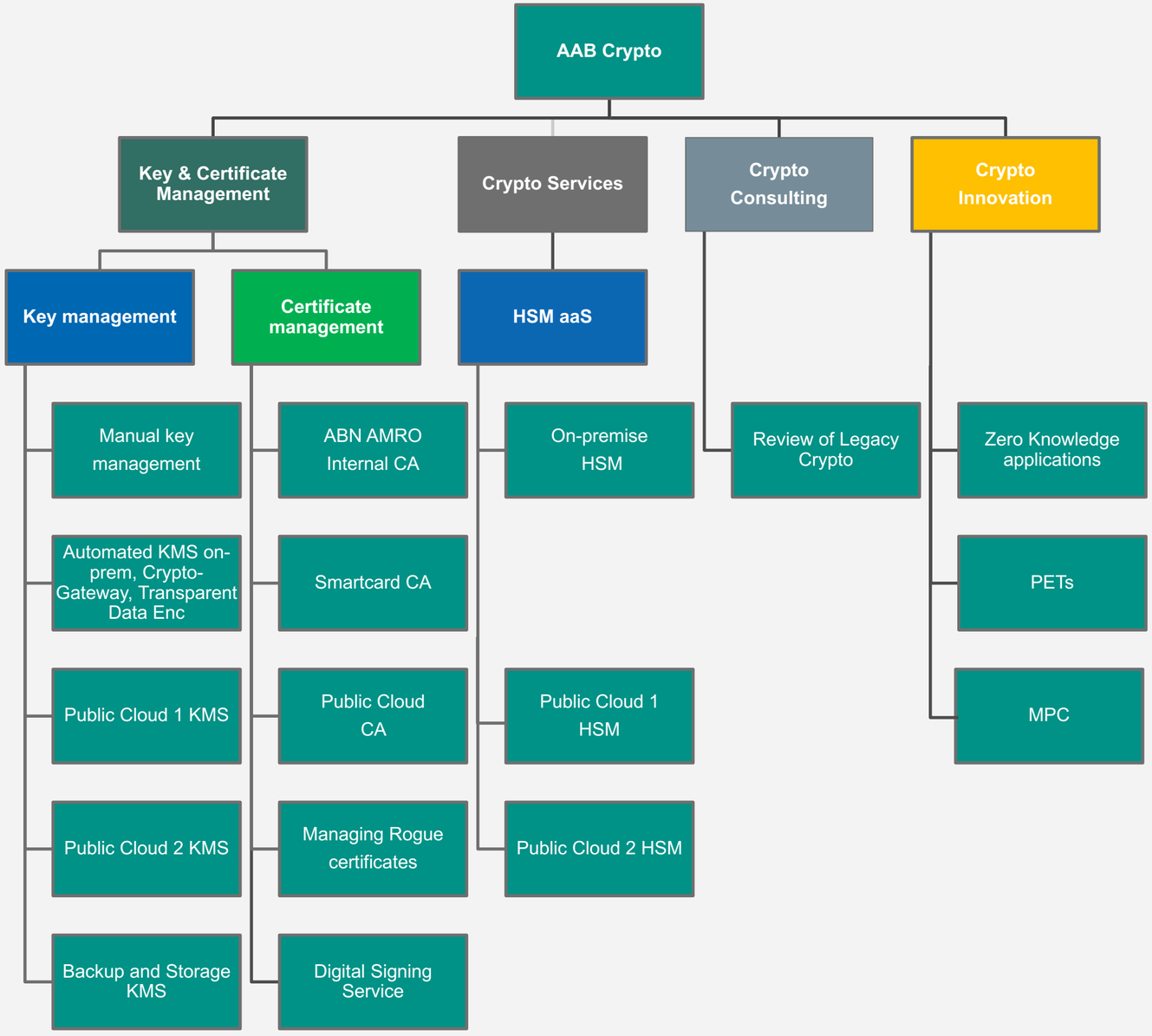
2
Cryptographic Services Innovation

- Crypto Intelligence
- Consulting, Information and Knowledge Sharing
- Development of Crypto Solutions

ABN·AMRO IBM

6

Crypto Services Overview 2020



SHA-1 Deprecation

WHAT: Crypto Services Portfolio 2019

CS 2019 >>

1
Cryptographic Services Application

- Key and Certificate Management
- Data in Transit and Data at Rest
- Application of Crypto Solutions

2
Cryptographic Services Innovation

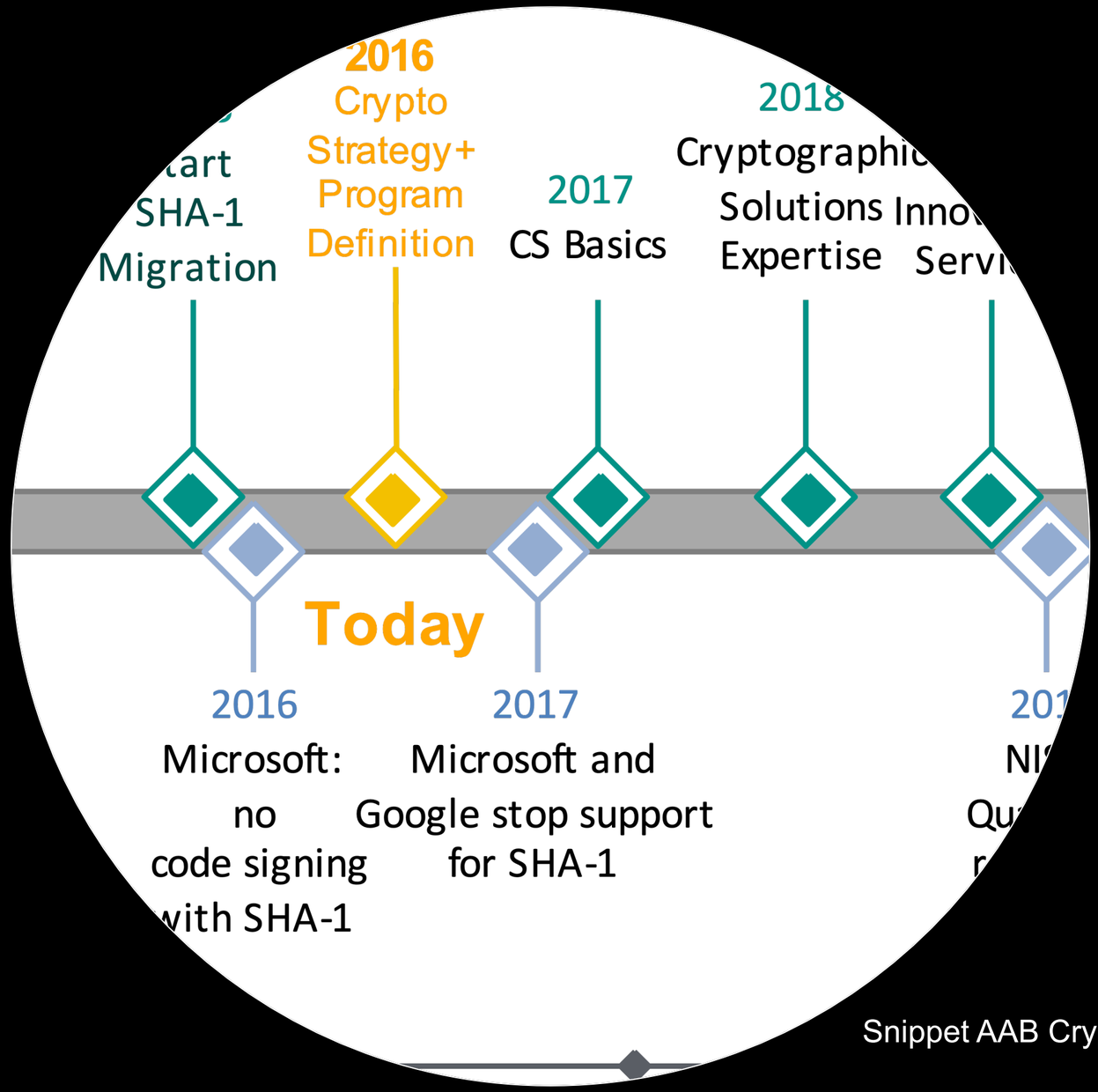
- Crypto Intelligence
- Consulting, Information and Knowledge Sharing
- Development of Crypto Solutions

ABN·AMRO IBM

6

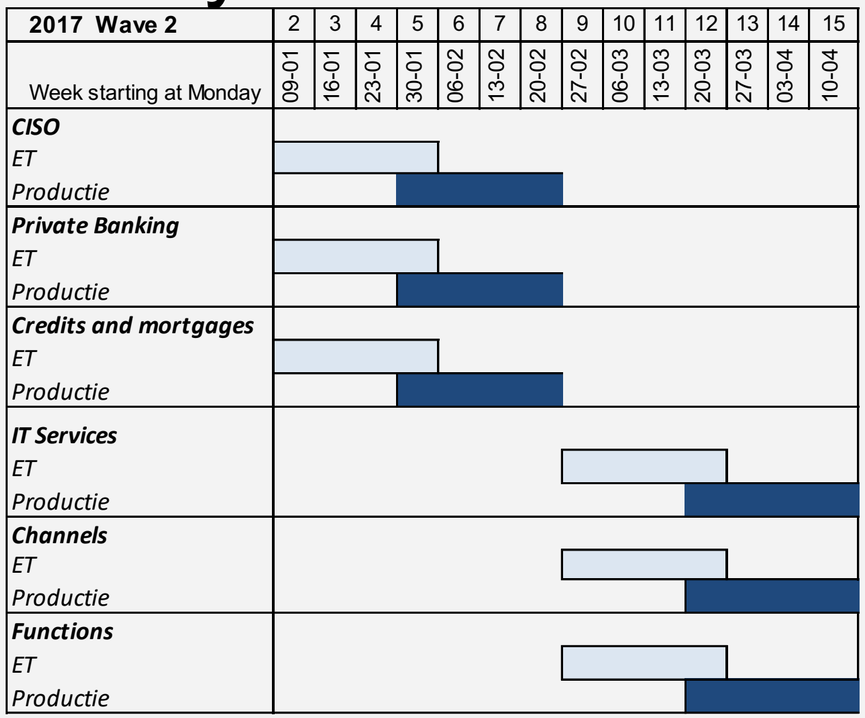
SHA-1 deprecation

- Taskforce 1 to migrate external (client facing) certificates to secure certificates.
  - ➢ TF1 ended in the first week of January 2016.
- Taskforce 2 to migrate internal certificates to secure certificates, or to propose other solutions to mitigate this risk.
  - ➢ TF2 ran from 2016 to 2017.



Snippet AAB Crypto strategy 2016

Weekly Stats on Task Force 2 SHA1 Migration



Wave	WAS	MQ	NETWORK	Wintel W1	Wintel W2
Systems in scope	182	1573	497	57	189
Systems to be changed, in scope Match	64	n.a.	n.a.	0	0
Verified migration Match	18	n.a.	n.a.	0	0
Systems in research (SHA 1)	0	0	n.a.	0	0
Systems change started (project)	0	322	27	0	64
Systems remaining for change (project)	0	0	429	0	42
Systems finished (SHA 2)	112	1107	32	57	11
Systems in Backlog SHA 2 incompatible	6	144	9	0	11

Number of systems migrated

Status 2017

ABN·AMRO IBM

Key Management – HSM as a Service

WHAT: Crypto Services Portfolio 2019

CS 2019 >>

1 Cryptographic Services Application

- Key and Certificate Management
- Data in Transit and Data at Rest
- Application of Crypto Solutions

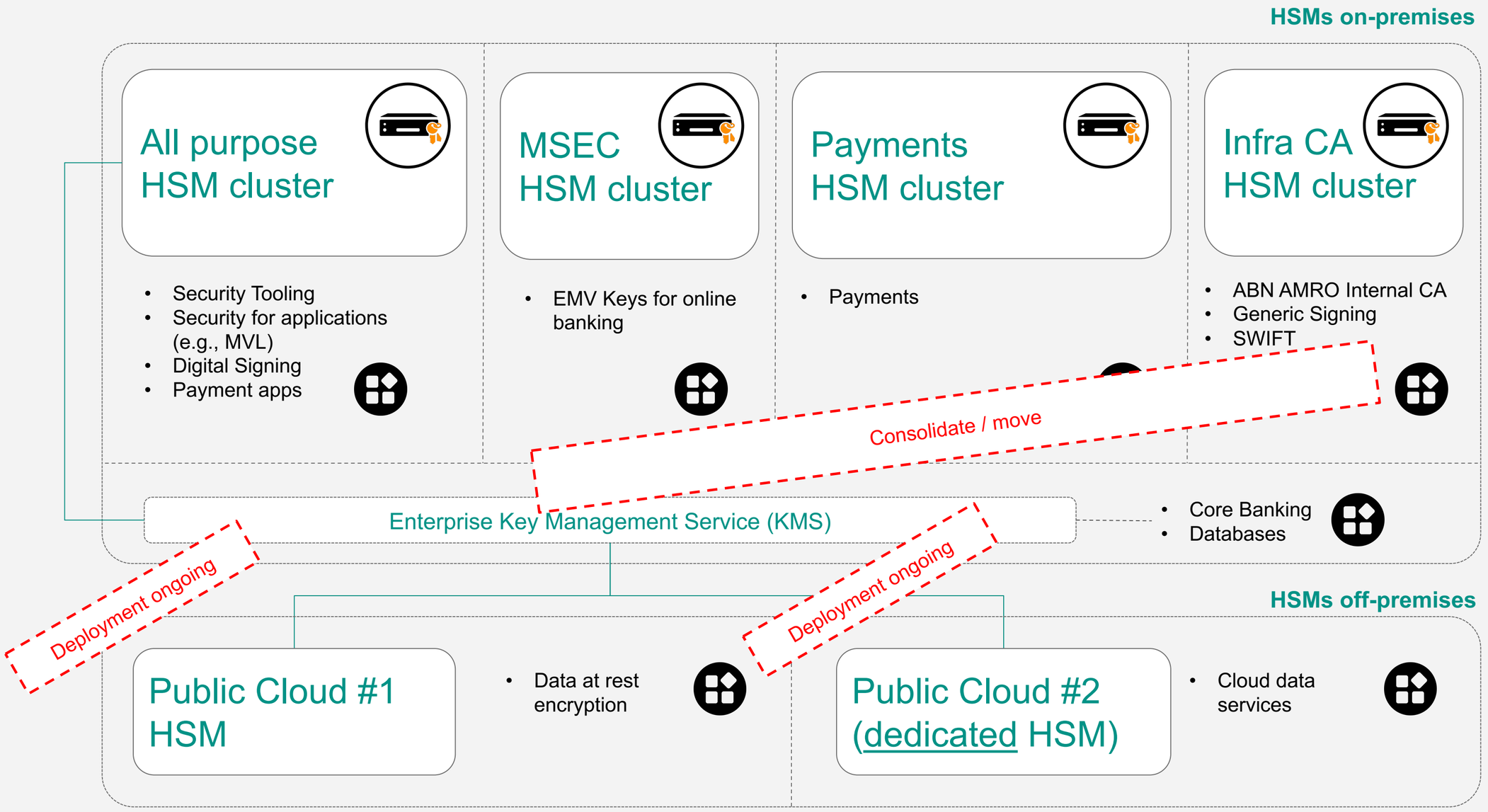
2 Cryptographic Services Innovation

- Crypto Intelligence
- Consulting, Information and Knowledge Sharing
- Development of Crypto Solutions

ABN·AMRO IBM

6

HSM as a Service landscape



ABN·AMRO IBM

Crypto Consulting

WHAT: Crypto Services Portfolio 2019

CS 2019 >>

1
Cryptographic Services Application

- Key and Certificate Management
- Data in Transit and Data at Rest
- Application of Crypto Solutions

2
Cryptographic Services Innovation

- Crypto Intelligence
- Consulting, Information and Knowledge Sharing
- Development of Crypto Solutions

ABN·AMRO IBM

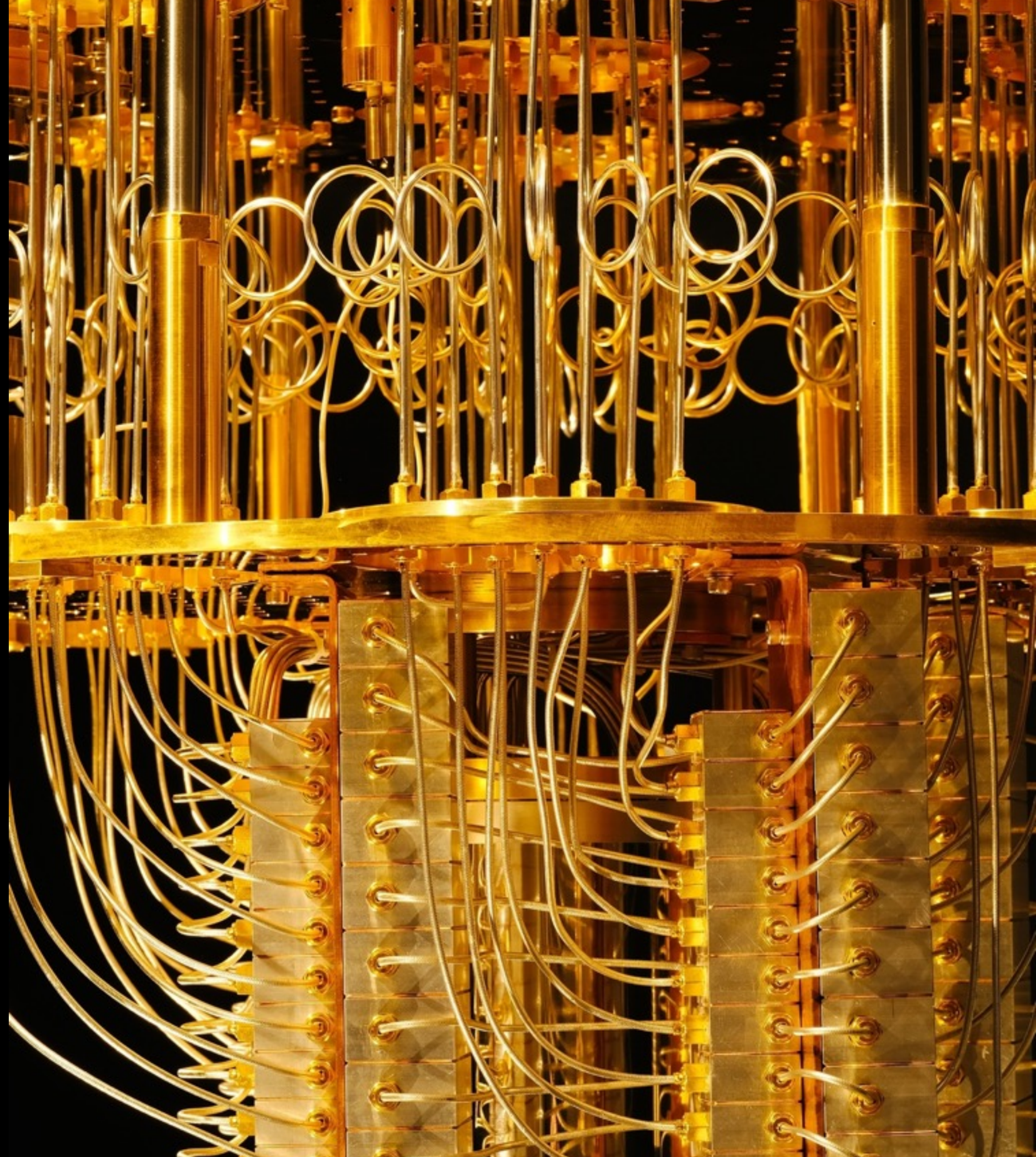
6

Quantum computing puts data at risk

Lessons learned from SHA-1 deprecation:

do nothing will keep bank unprepared

Crypto migrations take time and are very costly.

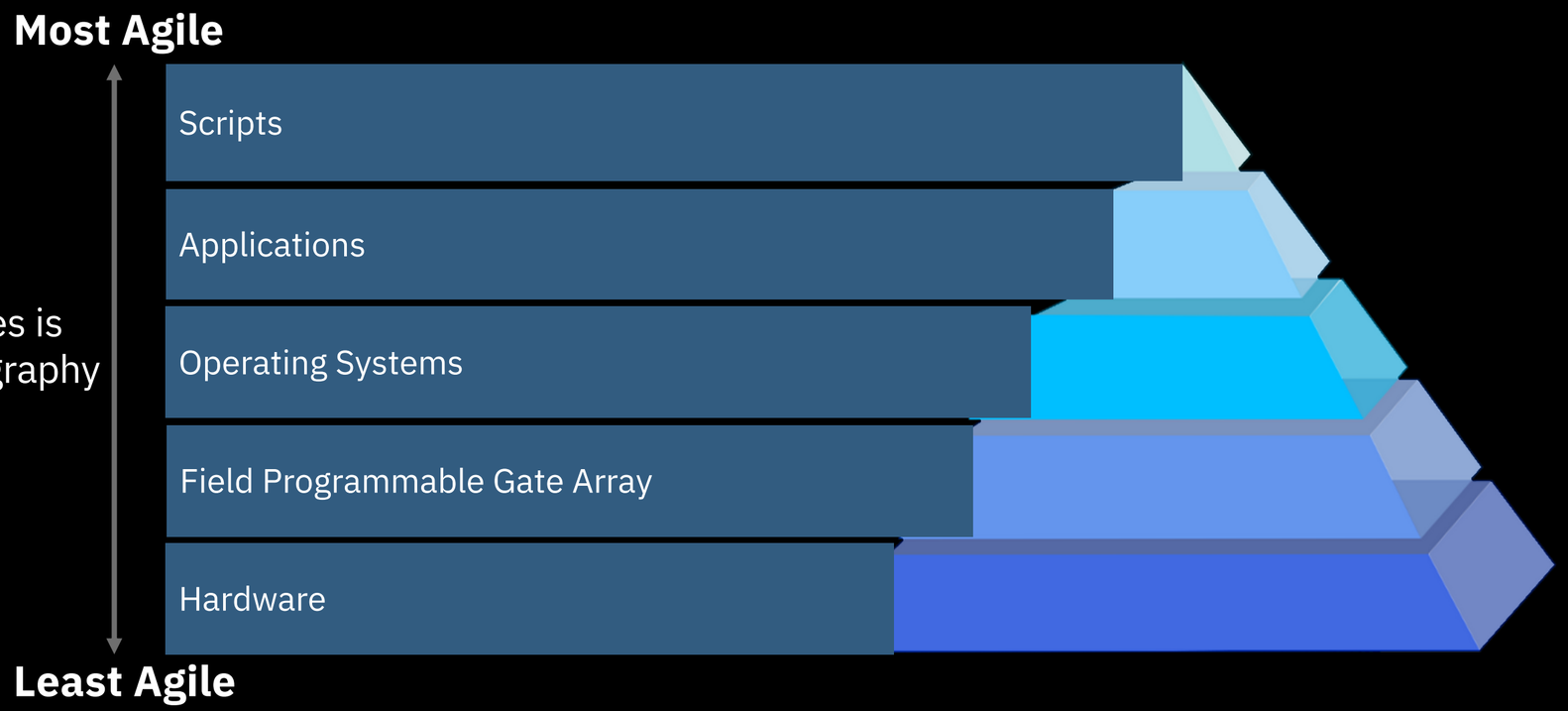


ABN·AMRO IBM

Crypto Agility: end-to-end view needed

The ease of crypto migrations can be viewed as follows:

The ability to migrate crypto implementations to new schemes is dependent on how today's cryptography is deployed.



Crypto Innovation

WHAT: Crypto Services Portfolio 2019

CS 2019 >>

1
Cryptographic Services Application

- Key and Certificate Management
- Data in Transit and Data at Rest
- Application of Crypto Solutions

2
Cryptographic Services Innovation

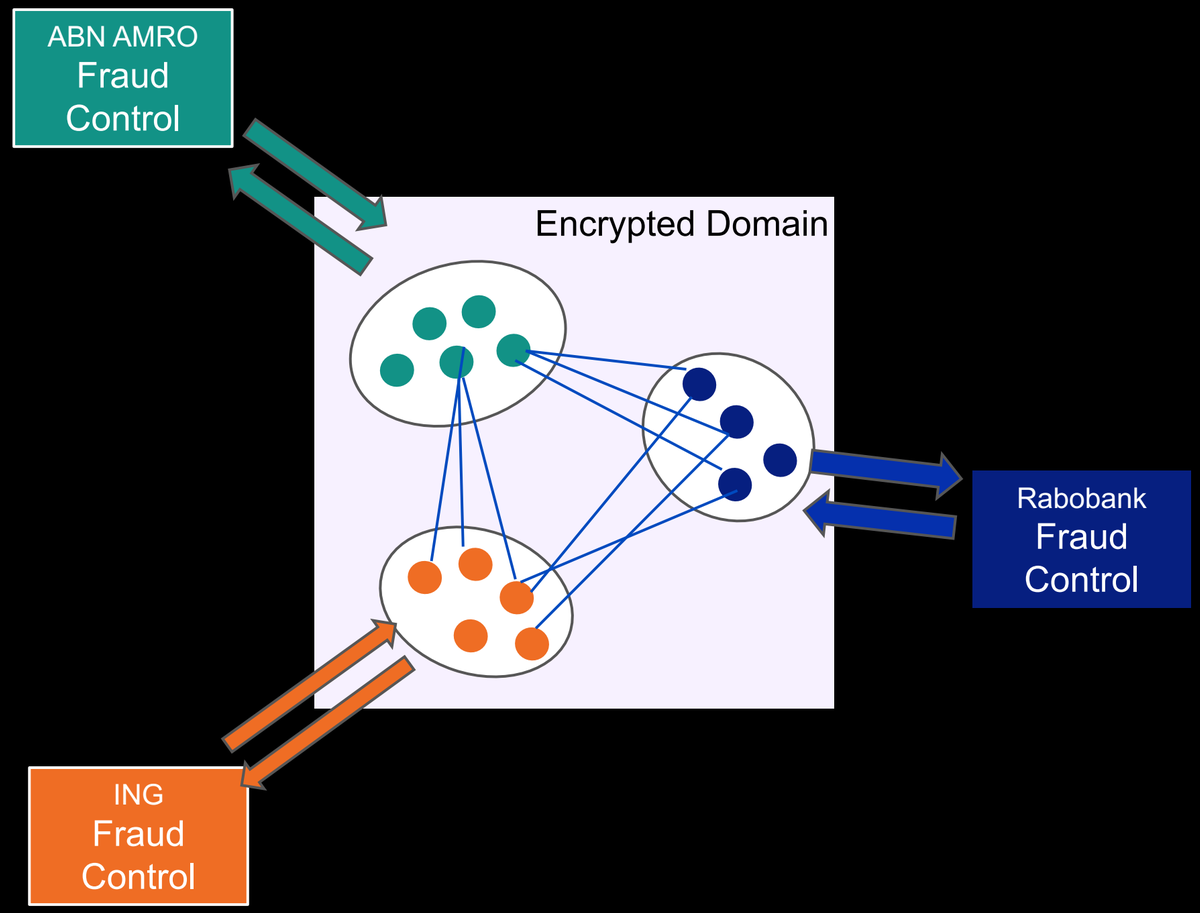
- Crypto Intelligence
- Consulting, Information and Knowledge Sharing
- Development of Crypto Solutions

ABN·AMRO IBM

6

Research Collaborations

- ABN AMRO Innovation Center works together with Crypto experts in CISO department.
- Collaborations with industrial and academic researchers
- Success Story: Fraud Detection
  - MPC to solve the problem to exchange insights with other banks
  - Implemented in practice



IBM Research & ABN AMRO :
I. Molloy, S. Chari, U. Finkler, M. Wiggerman, C. Jonker, T. Habeck, Y. Park, F. Jordens, R. van Schaik: **Graph Analytics for Real-Time Scoring of Cross-Channel Transactional Fraud.** Financial Cryptography 2016.

TNO, ABN AMRO, RABOBANK, ING, CWI:
A. Sangers, M. van Heesch, T. Attema, T. Veugen, M. Wiggerman, J. Veldsink, O. Bloemen, D. Worm: **Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection.** Financial Cryptography 2019.

ABN·AMRO IBM

What’s next?

WHAT: Crypto Services Portfolio 2023

CS 2023 >>

Challenges

- Crypto and Quantum Challenges
- Crypto Agility
- Crypto in DevSecOps
- Crypto in / for Public Cloud
- Secure Crypto Keys in times of Big Data

ABN·AMRO IBM

Thank you

Christiane Peters
Global Lead Crypto Services – IBM Security Services
cpeters@be.ibm.com
@cbcrypto (twitter)

Tiago Teles
InfoSec Evangelist – ABN AMRO Bank
tiago.teles@nl.abnamro.com
@tiagomteles (twitter)