h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

ATHENE
National Research Center
for Applied Cybersecurity

UCS
USER-CENTERED SECURITY

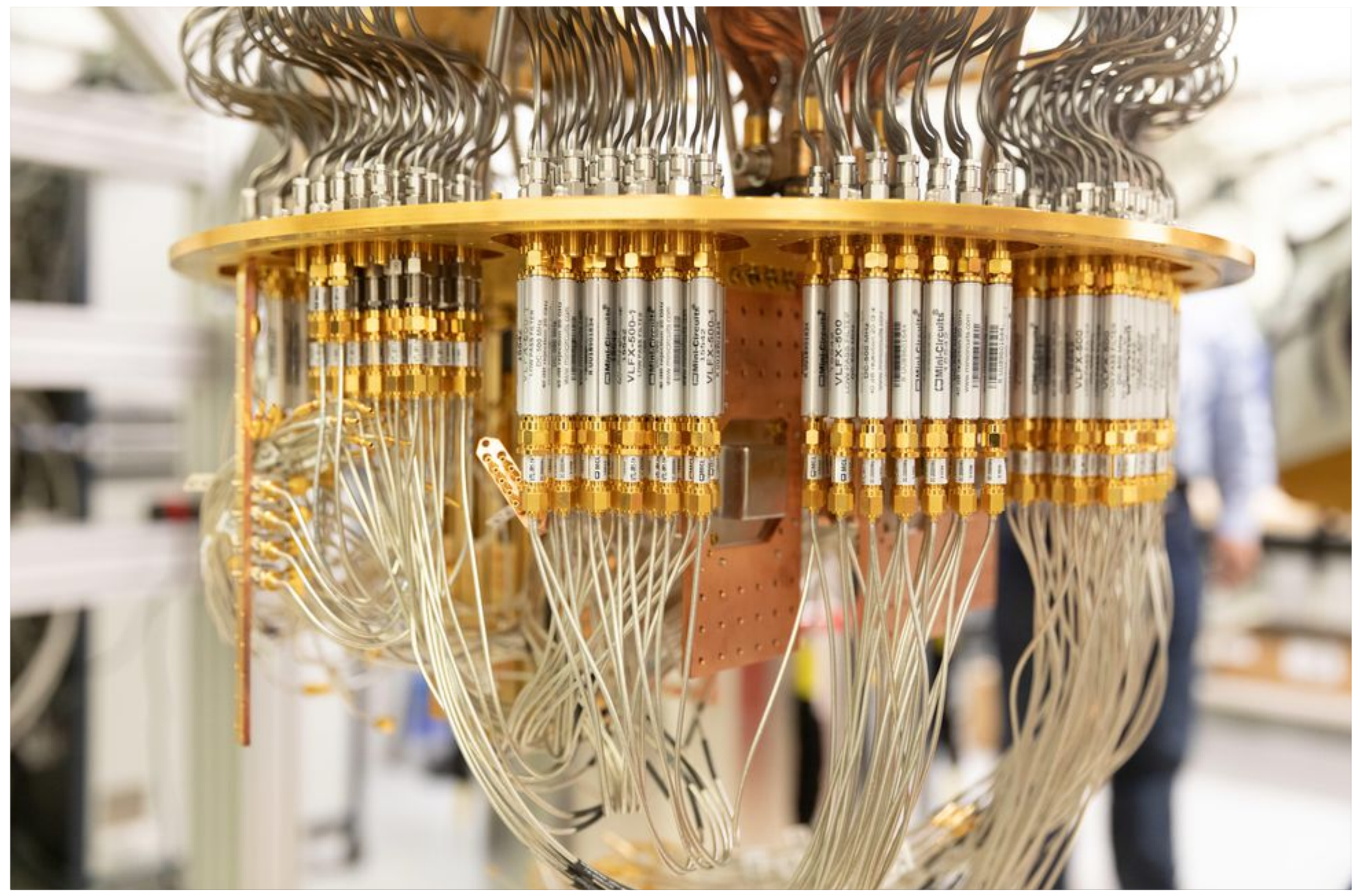
Towards a maturity model for crypto-agility assessment

Andreas Heinemann

Hochschule Darmstadt

it-sa 365, 15.03.2022, 13.45h – 14.00h

Motivation



© Shankland/CNET (2019)

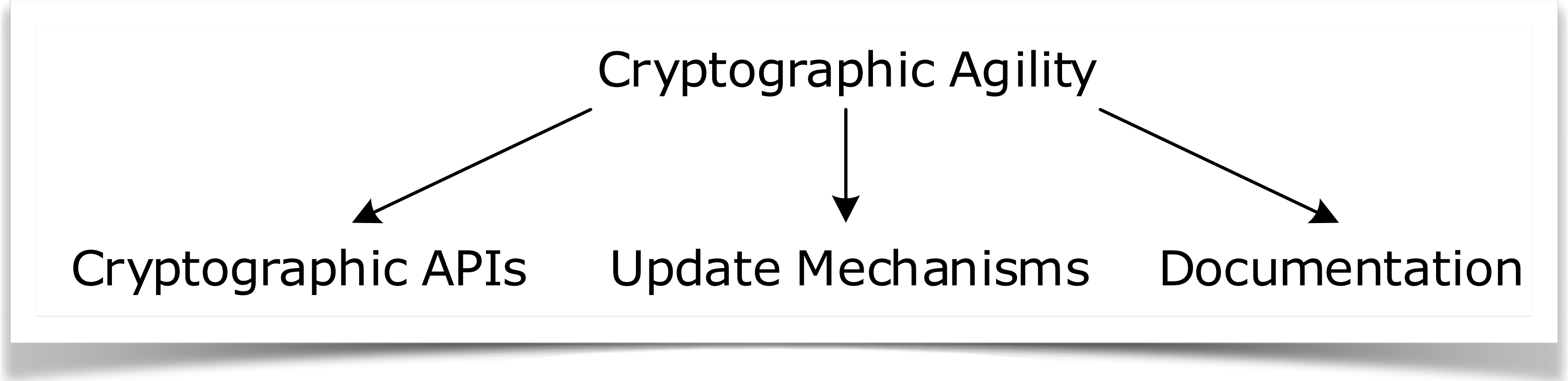
- Shor's algorithm (Shor 1997) combined with a powerful quantum computer (QC) would break currently widely used asymmetric cryptographic techniques, e.g., RSA, DSA, ECDSA, ECDH (Chen et al. 2016).

  → **many security mechanisms found, e.g., in commonly used Internet protocols are threatened**

- Different estimates of when a powerful QC will be available
- Goal: Replace classic asymmetric crypto schemes with quantum-resistant public-key crypto schemes (PQC schemes, cf. NIST Post-Quantum Cryptography Standardization)
- As of today: IT infrastructures must be able to respond timely and agile as soon as a cryptographic scheme is broken, e.g., by a QC
- In other words: **IT architectures need to evolve towards crypto-agile IT architectures**

Cryptographic Agility (CA): Intro

- *Cryptographic agility refers to **how easy** it is to **evolve** or **replace** the hardware, software, or entire information technology (IT) systems being used to implement cryptographic algorithms or protocols (and, in particular, whether the resulting systems remain "interoperable")* Schneider noted in opening remarks by Johnson, Millett (2017).
- Another view: Building blocks



Paul, Niethammer (2019)

- Problem: There is no common understanding on the term cryptographic agility
- Our approach: Map definitions, requirements and aspects onto a maturity model (CAMM)
- Goal: Apply CAMM in order to determine the CA level of a given software or IT System and improve it step by step

Crypto-Agility: More Definitions

- CA is
  1. the ability for machines to select their security algorithms in real time and based on their combined security functions;
  2. the ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features; and
  3. the ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete

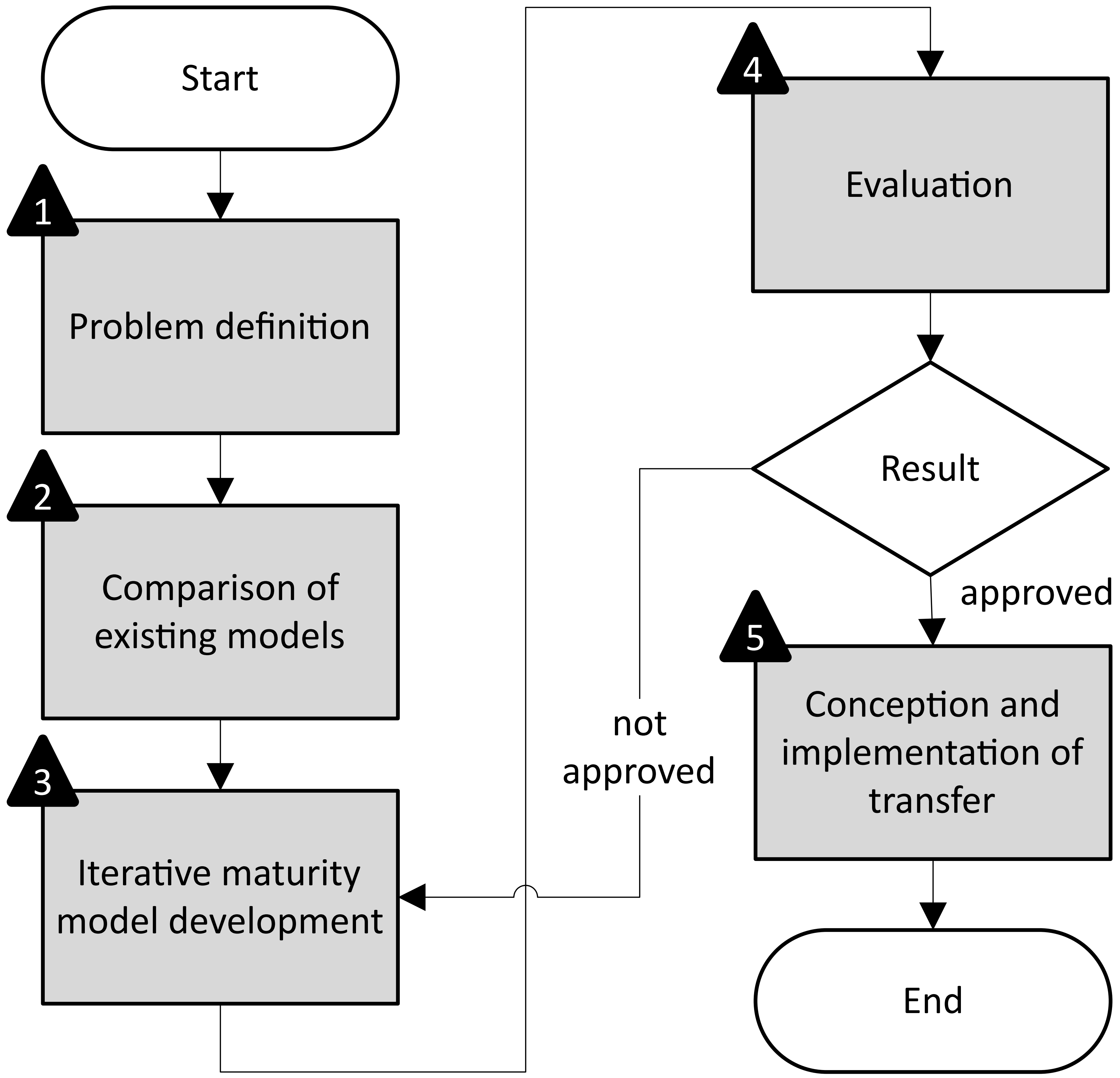
     K. McKay in Johnson and Millett (2017)
- CA denotes
  - an easy migration from one crypto scheme to another

    Mehrez and El Omri (2018)

Crypto-Agility: Requirements and Aspects

- IDs (for algorithms or sets of algorithms), transitioning, key management, interoperability (mandatory algorithms), balancing security strengths, opportunistic security, (effective) migration mechanism
  Russ Housley (2015)
- Measurability, interpretability, enforceability, security, performance
  Computing Community Consortium (CCC) (2019)
- Switch between crypto schemes in realtime, support for heterogenous environments, policy-aware access to crypto primitives, automatability (centralized), scalability
  T. Macaulay, R. Henderson (2019)
- Extensibility, removeability, interoperability, flexibility, fungibility, reversability, updateability, transition mechanism, backwards compatibility
  Mehrez and El Omri (2018)
- Testable Steel (2019), usage of SDKs, crypto APIs Niederhagen (2017) Utimaco (2018), preparing for failure Johnson, Millett (2017)

Developing CAMM – Approach



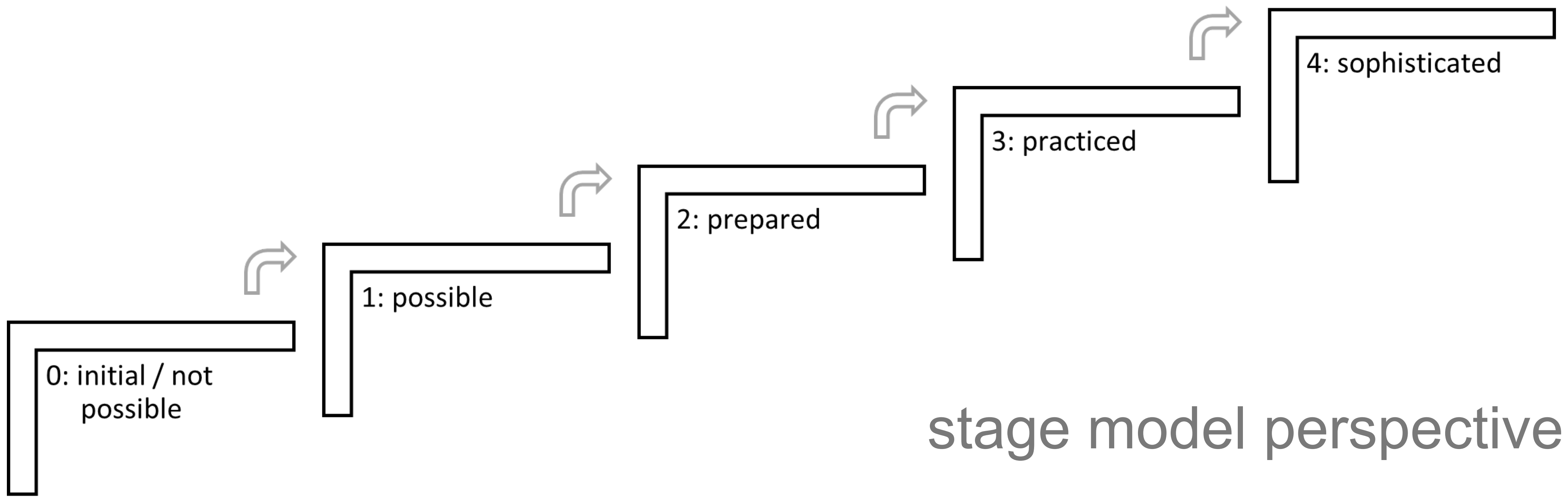
- Details / further info:
  Hohm, J., Heinemann, A., Wiesmaier, A., (2022)

adapted from

Becker, Knackstedt, Pöppelbuß (2009)

CAMM – Overview

Level	Name
0	Initial / Not possible
1	Possible
2	Prepared
3	Practiced
4	Sophisticated



stage model perspective

Five maturity levels

- Each level contains a certain number of requirements, all of which must be met in order to reach that level

Meaning

- L. 0 Initial: Reached by default
- L. 1 Possible: Necessary conditions are met, no activities
- L. 2 Prepared: CA is an implementable goal, sufficient conditions are met
- L. 3 Practiced: Migration is securely feasible and verifiable
- L. 4 Sophisticated: Fast migration, automation

Example
CAMM – Level 1 (Possible) Requirements: No 10 and No 11

Knowledge, Process, System property

No 10

ID	10
Name	Systemknowledge
Description	For crypto-agility requirements to be effectively evaluated, detailed knowledge of the affected system and its environment is required.
Category	Knowledge
Problem	Without knowledge about the systems and understanding about their domain, no assertions can be made about them and crypto-agility cannot be measured.
Acceptance	An in-depth understanding of the structure and operation of the systems being evaluated is available.
Dependency	none
Source	Ott et al. 2019
Example	Access to source code and/or hardware specification. Black boxes cannot be evaluated.

No 11

ID	11
Name	Updateability
Description	Maintainers can modify the system and provide updates to new software versions.
Category	Process
Problem	If vulnerabilities are identified in the system and its cryptography, it should be possible to fix them.
Acceptance	Performing updates with modifications is possible.
Dependency	10
Source	Kempka 2020 Mehrez and El Omri 2018
Example	Mobile apps are often modified by updates. Updateability is not possible for legacy devices without support.

Example
CAMM – Level 1 (Possible) Requirements: No 13 and No 14

No 13

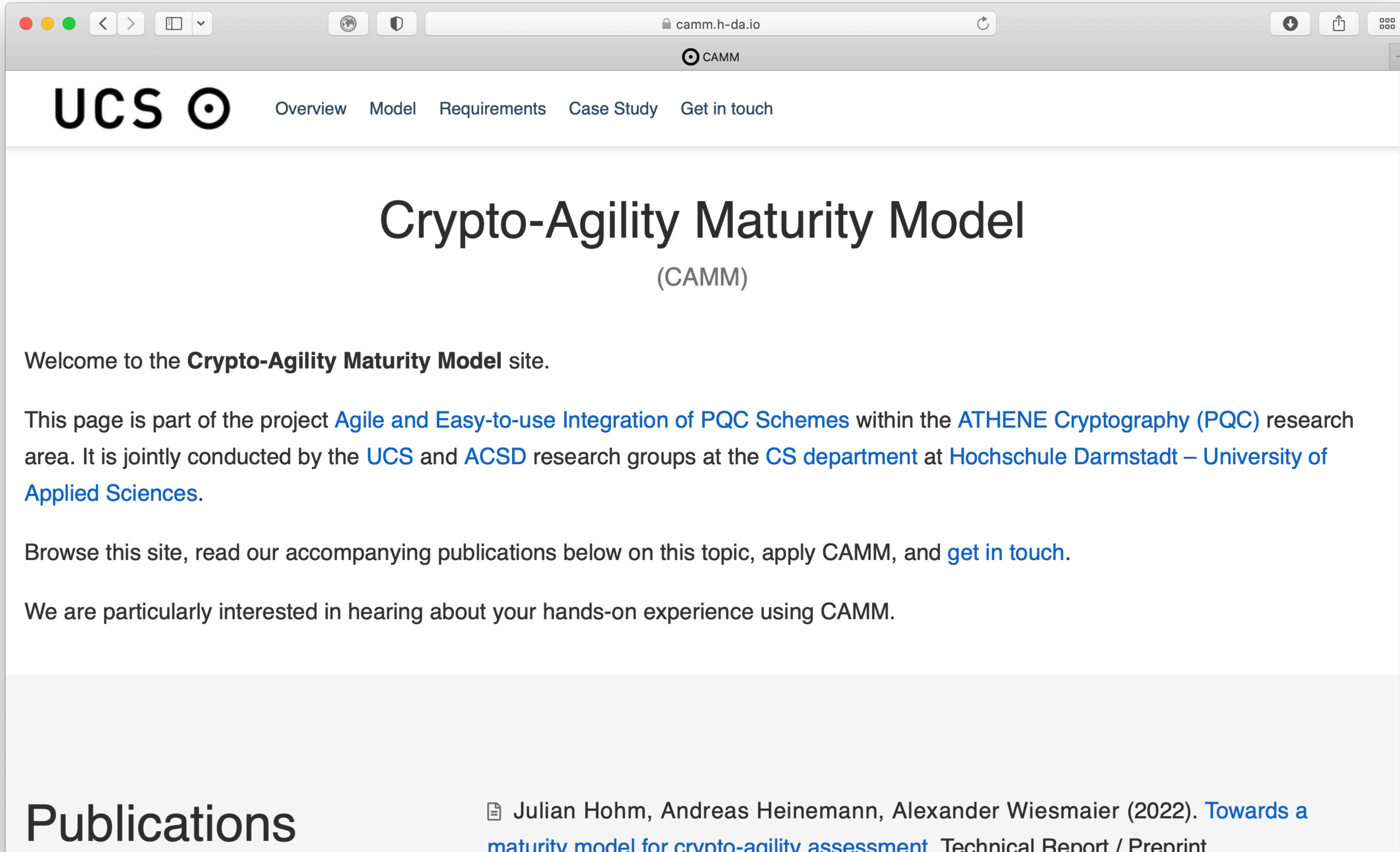
ID	13
Name	Reversibility
Description	The system can be rolled back to a previous state.
Category	Process
Problem	If an update results in problems, the system can be can be rolled back to a previous, functional state.
Acceptance	Rollbacks to previous versions are possible.
Dependency	10
Source	Mehrez and El Omri 2018
Example	Due to a bug in a system update the system does not behave as expected and is rolled back to a previous state.

No 14

ID	14
Name	Cryptography inventory
Description	The cryptographic functions used are documented and their current security level is known.
Category	Knowledge
Problem	In order to assess whether the system is affected by known vulnerabilities in certain cryptography variants, there must be an overview of the cryptography implementations used.
Acceptance	A listing of the cryptographic methods used, their parameters and intended use is available, and current developments and recommendations for action on cyber security are observed.
Dependency	10
Source	Kreutzer et al. 2018 Horvath and Mahdi 2017
Example	Inventory as a table with table with the following information: cryptography methods, primitives used, key length, purpose of use, security level, date of deployment, date of deactivation. Trends and developments in cryptographic security are tracked at conferences and in related publications.

CAMM – Further Information

- https://camm.h-da.io
  - Model
  - All requirements
  - Publications
    (cf. slide 6)
  - Contact info



Summary and next steps

- CAMM aims to help IT officers to asses their state/maturity concerning crypto agility.
- With the aid of the CAMM requirements, concrete activities can be initiated to implement the respective requirement.
- The ultimate goal of any IT should be CAMM level 4 to be able to meet the QC threat

- Provide tools to support requirement assessment whenever possible
- Promote CAMM so that it is applied in practice and we gain more experiences
- Jointly develop CAMM further, adapt and evolve requirements if necessary

Literature

- Shankland/CNET, Stephen (2019). Take a look at Google's quantum computing technology. https://www.cnet.com/pictures/take-a-look-at-googles-quantum-computing-technology/ (visited 13.03.2022).
- Shor, Peter W. (Okt. 1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In:SIAM J. Comput.26.5, S. 1484–1509
- Chen, Lily et al. (2016). Report on Post-Quantum Cryptography. US Department of Commerce, National Institute of Standards und Technology
- Johnson, A.F., Millett, L.I.(eds.): Cryptographic Agility and Interoperability: Proceedings of a Workshop. The National Academies Press, Washington, DC (2017).
- Paul, S., & Niethammer, M. (2019). On the importance of cryptographic agility for industrial automation, at - Automatisierungstechnik, 67(5), 402-416.
- Hohm, J., Heinemann, A., Wiesmaier, A., (2022). Towards a maturity model for crypto-agility assessment. Technical Report / Preprint.
- Julian Hohm (2021). Reifegradmodell für die Krypto-Agilität. Master thesis, Hochschule Darmstadt, Germany
- Hassane Aissaoui Mehrez and Othmane El Omri (2018). The Crypto-Agility Properties. In The 12th International Multi-Conference on Society, Cybernetics and Informatics, Nagib C. Callaos (Ed.). IIIS, Winter Garden, Florida, U.S.A., 99–103.
- Russ Housley (2015). Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms. RFC 7696.
- Computing Community Consortium (CCC) (2019). Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. Computing Community Consortium (CCC).
- Tyson Macaulay and Richard Henderson (2019). Cryptographic Agility in practice: emerging use-cases. Infosec Global.
- Graham Steel. 2019. Achieving 'Crypto Agility'. Cryptosense. https://cryptosense.com/blog/achieving-crypto-agility
- Ruben Niederhagen and Michael Waidner. 2017. Practical post-quantum cryptography. White Paper. Technical Report. Fraunhofer SIT, Darmstadt.
- Utimaco. 2018. Post-quantum cryptography: Secure encryption for the quantum age
- Jörg Becker, Ralf Knackstedt, and Jens Pöppelbuß. 2009. Developing Maturity Models for IT Management. 1, 3 (06 2009), 213–222.

Contact

Prof. Dr. Andreas Heinemann
Fachbereich Informatik
Hochschule Darmstadt - University of Applied Sciences
Haardtring 100
D-64295 Darmstadt

Tel: 06151-16-3 8482
Fax: 06151-16-3 8935
E-Mail: andreas.heinemann@h-da.de
Web: https://www.fbi.h-da.de