Motivation

Why do we need crypto agility?
→ no 100 % security
→ Cryptographic schemes need to be replaced continuously.
→ Crypto(graphic) agility

Why do we need metrics?
→ to be more accurate
→ make crypto agility part of specifications
Impact of Quantum Computing Technology on Classical Cryptography

From time to time, the discovery of a cryptographic weakness, constraints imposed by dependent technologies, or advances in the technologies that support cryptanalysis make it necessary to replace a legacy cryptographic algorithm. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Many information systems lack *crypto agility*—that is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure. As a result, an organization may not possess complete control over its cryptographic mechanisms and processes so that it can make accurate alterations to them without involving intense manual effort.
6.2 Kryptoagilität

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografi-
schen Mechanismen möglichst flexibel zu gestalten, um auf
Entwicklungen reagieren, kommende Empfehlungen und
Standards umsetzen und möglicherweise in Zukunft Algo-
rimthen, die nicht mehr das gewünschte Sicherheitsniveau
garantieren, austauschen zu können („Kryptoagilität“). Dies
gilt insbesondere aufgrund der Bedrohung durch Quanten-
Existing Definitions

Crypto Agility

- adapt to new cryptographic algorithms
- fast
- without a lot of effort
- minimal impact on the rest of the system
Existing Definitions

Crypto Agility

- adapt to new cryptographic algorithms
- fast
- without a lot of effort
- minimal impact on the rest of the system
  → Agreement on outcome of crypto agility.
  → But how to achieve it?
Towards a maturity model for crypto-agility assessment

Julian Steffen Hohm
Hochschule Darmstadt
Germany
Andreas Heinemann
Hochschule Darmstadt
Germany
Alexander Wiesmaier
Hochschule Darmstadt
Germany

ABSTRACT
This work proposes the Crypto-Agility Maturity Model (CAMM for short), a maturity model for determining the state of crypto-agility of a given software or IT landscape. CAMM consists of five levels, for each level a set of requirements have been formulated based on literature review. Initial feedback from field experts confirms that CAMM has a well-designed structure and is easy to comprehend. Based on our model, the crypto-agility of an IT landscape can be systematically measured and improved step by step. We expect that this work will complement and be superior to existing standards and frameworks. The model itself is open-source and can be used to apply it in practice and develop it jointly.

KEYWORDS
cryptographic agility, Crypto-Agility Maturity Model, CAMM, IT security management

1 INTRODUCTION
In the light of NIST’s recent initiative to standardize post-quantum cryptographic (PQC) algorithms [8], in order to withstand potential attacks by powerful quantum computers, for example by running Shor’s algorithm [8] against RSA, the more fundamental concept of cryptographic agility (CryptoAgility for short) has received an increasing focus recently, at least as a desirable property in the context of PQC issues [9, 13, 20, 23, 28, 32]. Although there is no commonly accepted definition of crypto-agility as of now, it often refers to the ability to replace a cryptographic scheme in an agile manner with very little effort. Following the view of Otte et al. [27], in our opinion, crypto-agility needs to be discussed and addressed at a broader sense. Otte et al. point out the need to address cryptographic limitations in crypto-agility. For example, current agility refers to a crypto-agile solution, which stems from the ability to replace a cryptographic scheme by a stronger scheme [27], if the latter is considered more secure. This is in contrast to cryptographic agility, which was coined in 2011 in RFC 6421 [31] as a communication protocol property. According to McKay at al. [27], crypto-agility includes (1) the ability for machines to select cryptographic algorithms based on their characteristics; (2) the ability to use various cryptographic algorithms to encrypt data; (3) the ability to gracefully retire cryptographic schemes; and (4) the ability to switch between crypto schemes in real-time. In her case, MD5. The term was also coined in 2011 in RFC 6421 [31] as a communication protocol property. According to McKay at al. [27], crypto-agility includes (1) the ability for machines to select cryptographic algorithms based on their characteristics; (2) the ability to use various cryptographic algorithms to encrypt data; (3) the ability to gracefully retire cryptographic schemes; and (4) the ability to switch between crypto schemes in real-time. In her case, MD5.

2 CRYPTOGRAPHIC AGILITY: DEFINITIONS, REQUIREMENTS, AND ASPECTS
To the best of our knowledge, the notion of cryptographic agility was first mentioned around 2005/06 by Neys and Volckaert [26, 45] as a programming style for abstracting NIST seed-based hard-coded use of a concrete hash algorithm. At the time, the term was also coined in 2011 in RFC 6421 [31] as a communication protocol property. Since then, several authors have used the term in an informal manner. However, a comprehensive understanding can be found in literature. According to Hojat at al. [27], crypto-agility includes (1) the ability for machines to select cryptographic algorithms based on their characteristics; (2) the ability to use various cryptographic algorithms to encrypt data; (3) the ability to gracefully retire cryptographic schemes; and (4) the ability to switch between crypto schemes in real-time.

Extending the view of Ott et al. [27], in our opinion, crypto-agility needs to be discussed and addressed at a broader sense. Ott et al. point out the need to address cryptographic limitations in crypto-agility. For example, current agility refers to a crypto-agile solution, which stems from the ability to replace a cryptographic scheme by a stronger scheme [27], if the latter is considered more secure. This is in contrast to cryptographic agility, which was coined in 2011 in RFC 6421 [31] as a communication protocol property.

3 MATUREITY MODEL
Since the notion of cryptographic agility is not well defined, we propose the concept of modalities for an expanded notion of crypto-agility (PQC). Following the view of Ott et al. [9], in our opinion, crypto-agility needs to be discussed and addressed at a broader sense. Ott et al. point out the need to address cryptographic limitations in crypto-agility. For example, current agility refers to a crypto-agile solution, which stems from the ability to replace a cryptographic scheme by a stronger scheme if the latter is considered more secure. This is in contrast to cryptographic agility, which was coined in 2011 in RFC 6421 as a communication protocol property.

4 EVALUATION
As a first step, we applied CAMM to an existing website at https://camm.h-da.io in order to disseminate the model more widely. A first preliminary evaluation of CAMM is provided in Section 5, followed by a short discussion and outlook in Section 6. There we point out areas we would like to address in the future.

5 CONCLUSIONS
We have formulated these requirements based on an intensive literature review on identified crypto-agility publications and assigned them to the appropriate levels. With CAMM at hand, IT managers can systematically measure IT landscapes and derive concrete measures to further develop their IT landscape in the direction of crypto-agility.

The further text is structured as follows. Section 2 identifies important requirements, aspects and properties of crypto-agility derived from literature, which we will later integrate into our maturity model. This is followed by the methodology and in order to develop our maturity model for crypto-agility (Section 3). The model itself is described in Section 4. We have set up an accompanying website at https://camm.h-da.io in order to disseminate the model more widely. A first preliminary evaluation of CAMM is provided in Section 5, followed by a short discussion and outlook in Section 6. There we point out areas we would like to address in the future.

Existing scales
CAMM

- Julian Hohm, Andreas Heinemann, Alexander Wiesmaier (Hochschule Darmstadt)
- 24 Requirements
  - one dimensional scale
  - some perspectives missing
Motivation again

Different perspectives
- Hardware: computational resources and memory
- Software: interfaces
- Management: responsibility
- ...

Leonie Wolf, CrossFyre2022
Different perspectives → dimensions
- 5 dimensions
- 5 levels each
Crypto Agility Spider Chart

Different perspectives → dimensions
- 5 dimensions
- 5 levels each

Cripto Agility Spider Chart

Leonie Wolf, CrossFyre2022
Crypto Agility Spider Chart

5 Algorithmic Agility

5.1 Exchange of algorithms
- Alg. A → alg. B

5.2 Modularity and interfaces
- Alg. A and B have same interfaces

5.3 Adding and deletion of algorithms
- Alg. A and B can both be used (e.g. TLS Handshake)

5.4 Unification/Harmonization
- Every cryptographic function has the same interface
4 System Agility

4.1 Capacities for currently established schemes
   ■ E.g. enough computational power to double key size

4.2 Backwards compatibility
   ■ Mechanisms for transition phase

4.3 Hard-/Software independence
   ■ Can be exchanged independently

4.4 Capacities for PQC
   ■ Schemes in general need more resources
Crypto Agility Spider Chart

3 Process Agility

3.1 Updateability
- Includes testing. Exceptions for devices with short life cycle.

3.2 Guidelines
- Specifies what (not) to use + who decides

3.3 Effectiveness
- Might depend on protection goals

3.4 (a) Migration to PQC
- Existing process

3.4 (b) Automatization
- After decision and testing
Crypto Agility Spider Chart

2 System Knowledge

2.1 Basic system knowledge
   ■ Access? Support? Responsibility?

2.2 Cryptography
   ■ Where and what crypto is used?
Crypto Agility Spider Chart

1 Knowledge crypto agility

1.1 Theoretical knowledge crypto agility

1.2 Practical knowledge crypto agility
   ■ How effect the system? Exceptions?

1.3 Concept for realization of crypto agility
   ■ Step-by-step plan

1.4 Post quantum cryptography
   ■ New requirements. Difficulties?
Summary

- Spider Chart
- includes different perspectives
- like knowledge
- Validation?
Thank you!
Questions?
New perspectives?