Crypto agility spider chart

CrossFyre22

Leonie Wolf
Fraunhofer SIT, October 6, 2022

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

Existing definitions

NIST

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.

Existing definitions

BSI

6.2 Kryptoagilität

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografischen Mechanismen möglichst flexibel zu gestalten, um auf Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, 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?

Existing scales

CAMM

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

Towards a maturity model for crypto-agility assessment

Julian Steffen Hohm
Hochschule Darmstadt
Germany

Andreas Heinemann
Hochschule Darmstadt
Germany

Alexander Wiesmaier
Hochschule Darmstadt
Germany

arXiv:2202.07645v2 [cs.CR] 17 Feb 2022

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 cryptographic agility of an IT landscape can be systematically measured and improved step by step. We expect that this will enable companies and to respond better and faster to threats resulting from broken cryptographic schemes. This work serves to promote CAMM and encourage others 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 current 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 [38] against RSA, the more fundamental concept of *cryptographic agility* (*crypto-agility* 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 common understanding of crypto-agility in general, it is often associated with the ability to replace a cryptographic scheme in an agile manner with very little efforts.

Following the view of Ott et. al [9], in our opinion, crypto-agility needs to be discussed and addressed in a broader sense. Ott et. al propose the concept of *modalities* for an expanded notion of crypto-agility. For example, context agility refers to a crypto-agile solution,

IT System. CAMM is composed of 5 maturity levels. For a system to reach a certain level, a number of given requirements must be met. 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 assess their IT infrastructure 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 used 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 brief preliminary evaluation of CAMM is provided in Section 5, followed by a short discussion and outlook in Section 6. There we point out issues we would like to address in the future.

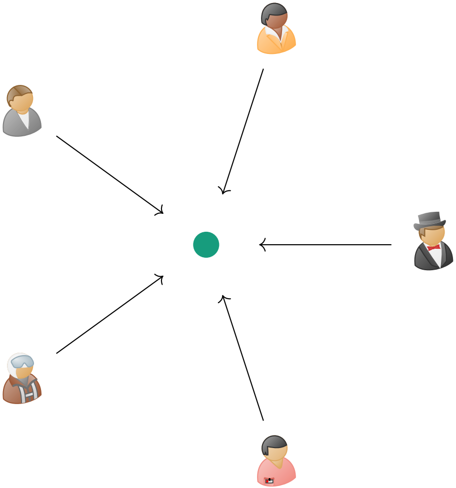
2 CRYPTOGRAPHIC AGILITY: DEFINITIONS, REQUIREMENTS AND ASPECTS

To the best of our knowledge, the notion of cryptographic agility was first mentioned around 2009/2010 by Bryan Sullivan [42, 43] as a programming style for abstracting .NET code from hard-coded use of a concrete hash algorithm, in his case MD5. 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 different manners. Without claiming completeness, the following understandings can be found in literature. According to McKay at NIST [20] crypto-agility includes (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*

Motivation again

Different perspectives

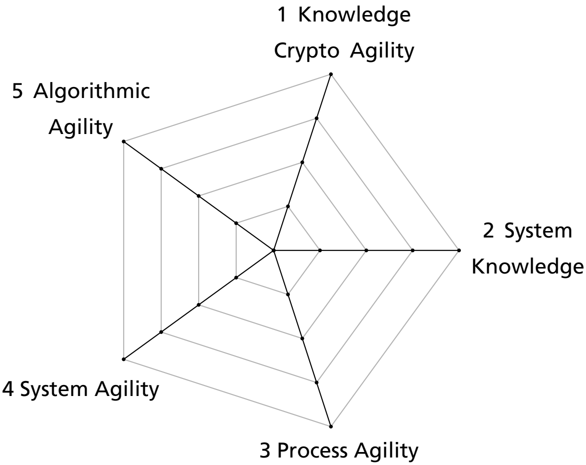
- Hardware: computational resources and memory
- Software: interfaces
- Management: responsibility
- ...



Crypto Agility Spider Chart

Different perspectives
→ dimensions

- 5 dimensions
- 5 levels each



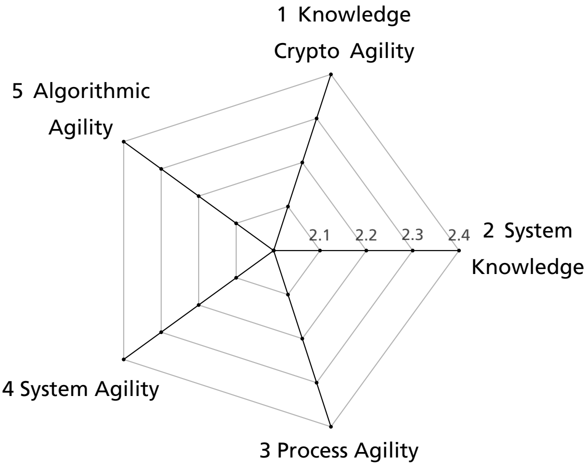
ATHENE National Research Center for Applied Cybersecurity

Fraunhofer SIT

Crypto Agility Spider Chart

Different perspectives
→ dimensions

- 5 dimensions
- 5 levels each



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

Crypto Agility Spider Chart

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
- Why? Concepts? Best practice?

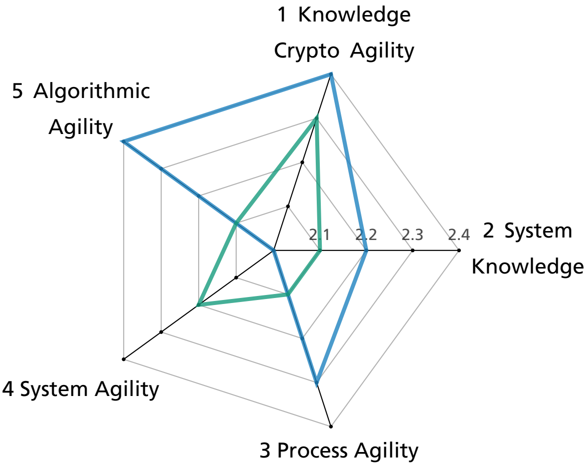
1.2 Practical knowledge crypto agility
- How effect the system? Exceptions?

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?