Exploring Crypto-Agile Solutions for Modern Financial Institutions



KBC is one of Belgium's leading financial institutions, combining banking, insurance, and advanced technology to serve millions of customers. With a strong focus on digital transformation and security, KBC relies heavily on modern cryptography to protect data and deliver trusted digital services. As emerging technologies such as quantum computing threaten current cryptographic schemes, algorithms may become obsolete more rapidly. To address this, KBC requires crypto-agile systems capable of switching cryptographic algorithms and protocols efficiently across a heterogeneous IT landscape, ranging from legacy systems to modern cloud platforms.

The goal of this thesis is to research, identify, and evaluate crypto-agile design approaches that can be integrated into KBC's existing infrastructure. The outcome may include an overview of crypto-agility approaches, an assessment of their feasibility within KBC's infrastructure, and a proposed high-level architecture or roadmap for achieving crypto agility. The focus is primarily on research, with optional conceptual prototyping and evaluation of vendor solutions where relevant.

The work will begin with a study of crypto-agility concepts, current cryptographic standards, and emerging post-quantum requirements. This is followed by an analysis of how cryptography is deployed in large financial institutions, identifying relevant constraints and integration challenges. Subsequently, different architectural approaches enabling crypto agility, such as modular cryptographic services, pluggable libraries, or algorithm-switching mechanisms, will be explored and evaluated based on feasibility, security impact, and alignment with system requirements. Finally, one suitable design will be proposed, for example a high-level architecture or conceptual prototype, accompanied by practical recommendations including next steps, potential risks, and long-term considerations.

This thesis is well suited for students interested in cybersecurity, cryptography, and IT architecture. A strong interest in the topic and willingness to learn are more important than prior in-depth expertise, as guidance will be provided throughout the project.

Practicalities

Promotor:	Prof. dr. ir. Bart Preneel
	Dr. Aysajan Abidin
Daily supervisor:	Marija Dražić-Balov marija.drazic-balov@kbc.be office KBC
Nature of the work:	40% literature, 40% analysis and design, 20% optional prototyping
Number of students:	1

 © 2026 – 2027 COSIC