Key obstacles to Post-Quantum Cryptography (PQC) Adoption

Lack of Clear Regulations, Education, and Expertise Hindering the Implementation of PQC.

# IDENTITY

POSTED ON 02.26.25

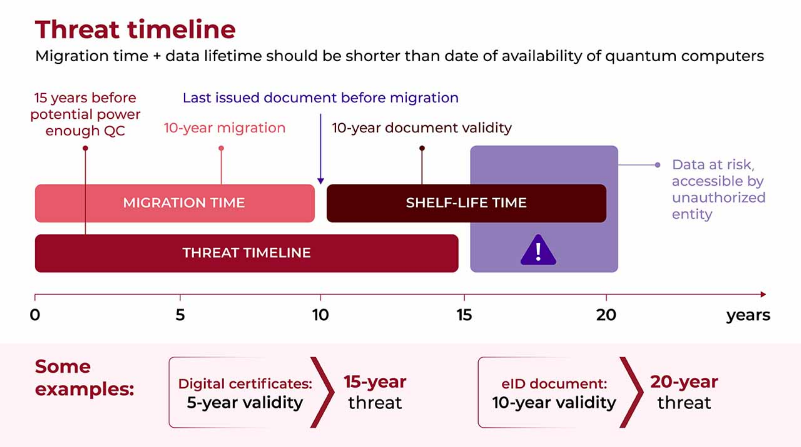
With the announcement this month from Microsoft* that it has successfully fabricated its first quantum processor based on a novel material known as a 'topological conductor', the ID and secure document market faces a critical challenge: ensuring the security of cryptographic systems against potential quantum threats. A recent survey on Post-Quantum Cryptography (PQC) reveals insightful perspectives from industry professionals, highlighting both the readiness and the hurdles in adopting PQC solutions.

The survey, organized by Reconnaissance in cooperation with IDEMIA Smart Identity, was conducted between September and November 2024. A small number of selected PQC and Cyber Security professionals have shared their view on the status of preparedness for the era of quantum computers in both private and public organizations.

The survey results indicate a strong awareness among respondents regarding the potential impact of quantum computing (QC) on current cryptographic systems. Out of 35 respondents, 29 rated their understanding as 'Good', 'Very Good', or 'Excellent', while only 6 rated it as 'Fair' or 'Poor'. This high level of awareness is crucial as it underscores the industry's recognition of the impending quantum threat.

The belief in the emergence of QC is nearly unanimous among participants in the survey. Only four respondents expressed scepticism, stating that QC is 'Not very likely' or 'I don't think it will happen'. The majority view underscores the urgency in preparing for a quantum-secure future, as most professionals anticipate QC becoming a reality within the next decade.

The survey highlights a strong consensus on the importance of implementing PQC within organizations.
15 respondents rated it as 'Very Important', 9 as 'Moderately' or 'Slightly' Important' and only 1 as 'Not at all important'. This recognition is a positive indicator that the industry is aware of the need to transition to quantum-resistant cryptographic solutions to safeguard sensitive personally identifiable information. The 'Threat timeline' chart illustrates the urgency of transitioning to quantum-resistant cryptographic systems before quantum computers break current encryption, as 'store now, decrypt later' threats put sensitive eID documents at risk due to their 10-year 'shelf-life' time.


Threat timeline
Migration time + data lifetime should be shorter than date of availability of quantum computers
15 years before potential power enough QC
Last issued document before migration
10-year migration
10-year document validity
Data at risk, accessible by unauthorized entity
MIGRATION TIME
SHELF-LIFE TIME
THREAT TIMELINE
0
5
10
15
20
years
Some examples:
Digital certificates: 5-year validity
15-year threat
eID document: 10-year validity
20-year threat

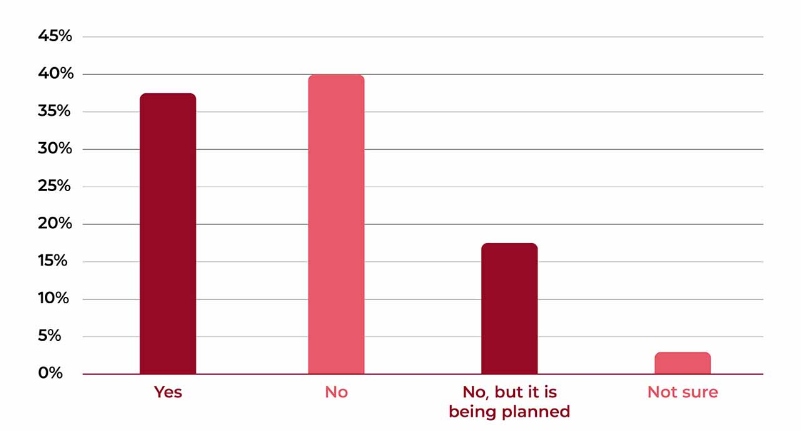
Key Obstacles: Lack of Know-how, Education, and Regulations & Standards

Despite the awareness and recognition, significant barriers to PQC adoption remain. The primary challenges identified in the survey are the lack of knowledge and expertise, and the technical complexity of PQC technologies. Many organizations lack the necessary know-how to implement PQC solutions effectively. Cybersecurity professionals, who are typically tasked with this responsibility, often do not have a background in quantum cryptography. The complexity of PQC technologies poses a significant hurdle, as organizations need to navigate the intricate technical landscape to develop and deploy quantum-resistant solutions.

The ID and secure document industry is not alone in facing these challenges. According to an article in Forbes**, hundreds of companies are actively seeking skilled quantum workers. This demand highlights the broader industry trend and the need for specialized talent to drive PQC adoption.

Encouragingly, as shown in the chart below, just over 50% of the respondents have either started implementing PQC solutions or are planning to do so. This proactive approach demonstrates a commitment to securing cryptographic systems against future quantum threats. However, these organizations are also seeking support and guidance to navigate the complexities of PQC adoption.

Question: Has your organization started researching or implementing PQC solutions?



The survey respondents identified three key initiatives to facilitate PQC adoption: increased awareness, better education, and clarification on regulations and standards. There is a clear need for educational initiatives to enhance understanding of PQC technologies and their implementation. Clear and consistent regulations and standards are essential to guide organizations in developing their PQC strategies. Within each organization it will fall to the Information Security Office to become the key point of contact for support, providing the necessary expertise and resources to assist in the transition to PQC.

> *When we discuss PQC-readiness with our clients, it becomes obvious that, although the topic is high up on the list of priorities, the professionals tasked simply don't know where to start. We see a respect towards the topic's complexity that we can only solve by joining forces as an industry. We won't double the number of PQC-experts over night, but there are enough of us, to give the relevant advice at this point in time.*
>
> Jerome Boudineau – PQC Expert at IDEMIA Smart Identity

The road towards post-quantum cryptography is complex and challenging, but the survey showed that the ID and secure document market is making significant strides. With a strong understanding of the potential impact of QC, a conviction in its emergence, and a recognition of the importance of PQC, the industry is well-positioned to tackle the challenges ahead. By addressing the barriers of knowledge and technical complexity, and seeking support from key stakeholders, organizations can successfully navigate this transition.

*https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/
**https://www.forbes.com/councils/forbestechcouncil/2024/12/12/beyond-quantum-where-to-look-for-quantum-ready-talent/