Post-Quantum Cryptography in Identity Management–the time to act is now

Why the longevity of today's ID credentials and systems is becoming a risk

IDENTITY

POSTED ON 10.08.24

Most people have heard about quantum computers, one way or another. Most people also understand there is a high risk involved in the security of our data. According to McKinsey[1], insurance, banking, and the public sector are at risk of being the first ones targeted due to the long shelf life of the handled data, and the long lifecycle of the systems involved. However, without a clear understanding of what future attacks will look like, many security professionals are unclear as to how to prepare.

Let us take a deeper look at the situation we are in.

Quantum computers will not be widely available tomorrow. In reality, the earliest we should expect the threat to become tangible is in about ten years. Several challenges remain:

- **Size:** Most existing quantum computers are currently huge, occupying several square meters, making them accessible only to large-scale organizations.
- **Operating conditions:** They often require extremely low temperatures to function, close to absolute zero (-273°C).
- **Error correction:** For every effective qubit, multiple additional qubits are needed to correct calculation errors, leading to the need for very large quantum computers. Reducing these calculation errors is a key priority.

Modern physical identity credentials issued these days have an average lifetime of ten years after issuance. The durability of polycarbonate and today's impressive security features add to the fact that there is really no pressure on citizens to voluntarily renew their ID cards or passports earlier than the expiration date. The status of identity management systems across the globe is very varied. Security incidents and attacks are rapidly growing and are becoming more and more sophisticated. This requires constant adaptation to develop patches and update systems while ensuring overall consistency. Unfortunately, this approach is not always followed. Combining this with the sensitivity of the citizens' data stored—even if biometric data would be ignored—it is clear why preparing for the post-quantum era cannot wait until the first breach happens or the regulations and standards are all in place.

> *The key is to be on the journey today and not wait until the last minute.*
>
> Rob Joyce, Director of NSA Cybersecurity

However, how can you prepare now for a threat that is so theoretical? The answer lies in crypto-agility and adopting a hybrid approach.

Cryptographic agility

Cryptographic agility is defined as the ability to smoothly transition from one cryptographic system to another. Currently, we clearly lack a long-term perspective on post-quantum cryptography (PQC) algorithms, especially when it comes to security. Even if the selected algorithms have been studied, new improvements may lead to reconsideration of usage or configuration and even lead to new change to different one.

Therefore, there is a clear need to be able to easily replace one post-quantum algorithm with another, or at least be able to increase the size of the keys used. Identity management systems need to be modular and adaptable, so we can update them after their deployment. Only then will they be future-proof.

Interoperability and Hybrid Cryptography for gradual transition

Today, most systems rely on pre-quantum cryptography and could remain in operation for decades. There is a need for a seamless transition to post-quantum cryptography while ensuring current systems stay compatible with the newly deployed PQC systems. Integrating both pre-quantum and post-quantum algorithms simultaneously on a system will allow pre-quantum systems to function alongside post-quantum ones and maintain interoperability during the transition to PQC. For example, a citizen with a quantum-safe electronic passport should be able to cross the borders of countries that have not yet implemented quantum-safe border systems, and vice versa.

Moreover, since we lack sufficient confidence in PQC algorithms, designing systems with hybrid cryptography is essential. Hybrid cryptography involves two layers of protection, one with a pre-quantum algorithm and one with a post-quantum algorithm, hence offering security in the two worlds. If a classical attack against the post-quantum algorithm is discovered, the pre-quantum algorithm within the hybrid solution will still provide protection.

Furthermore, all experts are very clear that this journey of preparation for the post-quantum era is a long and complex one. Therefore, creating a detailed risk mitigation plan that prioritizes the most critical assets first is key to ensuring scarce resources are used where needed.

Identifying the most critical assets in identity management

As in any risk mitigation plan, the critical first step is the analysis of the most vulnerable assets. In identity management, we need to first protect what is exposed to third parties (network entry points): tokens such as corporate badges or eID cards for digital use (e.g., signatures, government portal access) that allow users to connect to systems and make the system vulnerable to attacks.

Equally important is ensuring that data remains authentic and confidential. Taking the case of enrollment where biometric data is captured, the data transfer to a central database could be vulnerable to interception. Hence, it is important to prioritize the protection of the data first and address the channel's security later.

Conclusion: Be prepared, be agile, be resilient

With all the stated uncertainties around quantum computers, most importantly when they will be available, it is understandable that we currently observe a certain ostrich mentality. Preparing for something so uncertain seems difficult and a potential waste of time and money. However, as explained, if we follow a few key principles, we will already have reached an important first milestone in our post-quantum preparedness:

1. Ensure your identity management systems are cryptographically agile.

2 – Start updating your identity management system with post-quantum cryptography, while remaining compliant with pre-quantum systems at the same time.

3 – Update the most vulnerable assets first.

About the author:

Jerôme Boudineau, Product Manager and PQC Expert at IDEMIA Smart Identity. IDEMIA Smart Identity is at the forefront of advising governments and organizations in transitioning their identity management systems to the post-quantum era.

How prepared are you for PQC ?

We invite you to take this short survey to help us understand your organization's preparedness, as well as the current perceptions and status of PQC in the field of identity management.

Your insights are highly valuable to us!

Take the survey

---

[1] How to prepare for post quantum cryptography | McKinsey
