# How will POST-QUANTUM *CRYPTOGRAPHY* Affect *Contactless Travel* in ENTRY-EXIT SOLUTIONS?

By Lutz Richter – Mühlbauer

*This article will look at the impact post quantum cryptography has on entry/exit systems, on the topic of seamless travel.*

*It was transcribed and edited for readability from an original presentation given by Lutz Richter during the Silicon Trust webinar:* ***Post-Quantum Cryptography and its Impact upon Identity.*** (April 10th 2024)

## The travel process today

Everyone is familiar with the way we travel today. We start with the registration of the traveler at a self-service kiosk. This is normally a passport, or in terms of ICAO, the eMRTD – where the document is read and, ensuring everything is correct according to the specification, the verification of the individual against this travel document takes place. Next, more or less seamlessly, you go to a gate that uses face recognition. The traveler is verified and can cross the border or go to the aircraft and make the boarding process (Figure 1). This is currently state-of-the-art, is established in different setups, and the trust element here is the travel document with the electronic chip and the digital information from a government authority. This is what we call the Trust Anchor.

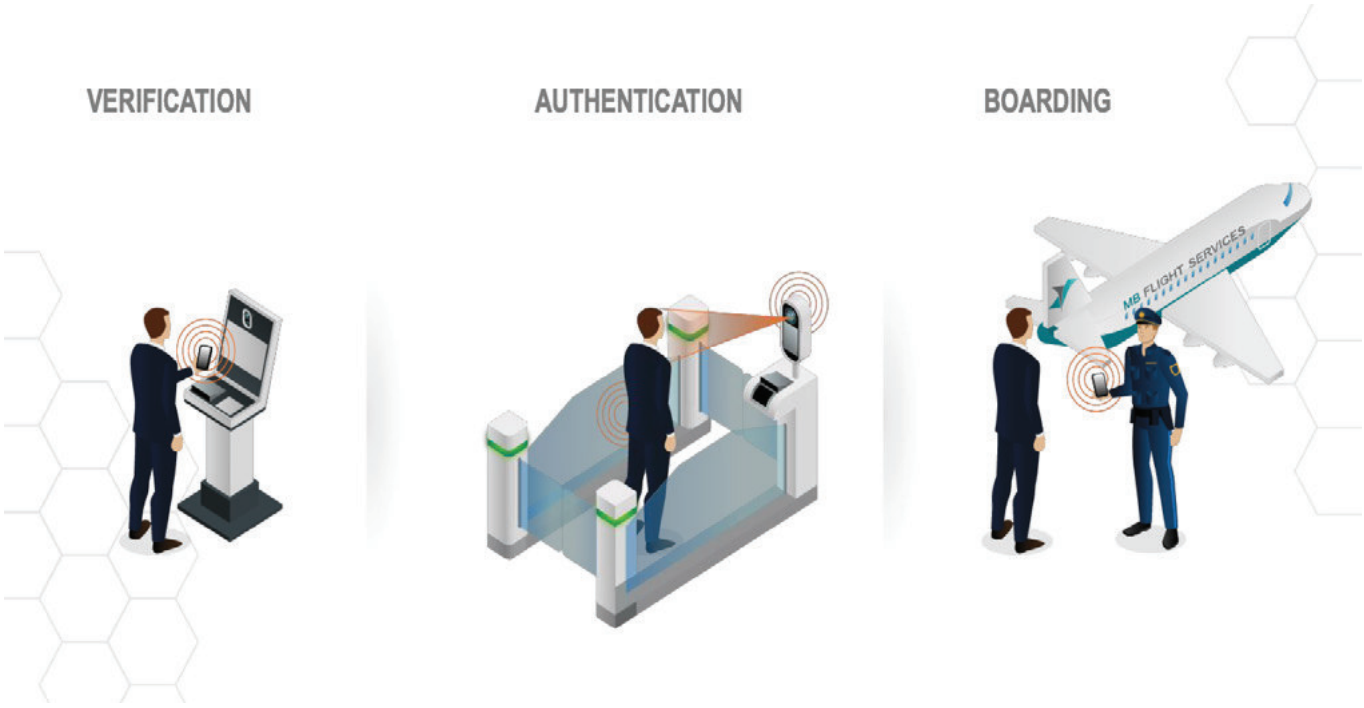


*Figure 1 Verification, Authentication & Boarding*

But what is behind the establishment of such a system and what do we have to consider as a solution consultant or as a technology partner in this market segment? The basis of this entire system are international standards.

Here, the three main player for international travelling documents is ICAO, which is obliged to standardize all data which is going to a machine-readable travel document such as a passport or ID card, including the chip. And ISO, in turn, concerns themselves with the detailed technical specification for the chip and the data processing. Now for Post Quantum Cryptography, the National Institute for Standardization and Technology in the US is engaged in qualifying the algorithm, with which Post Quantum Cryptography-proven solutions, and solution supplier, have to consider when building up a system or transferring this system to the next level.

## What are the challenges?

The hot topic today is Post-Quantum Cryptography. But equally important is cybersecurity, because communication in today's digital world is also the science of secure digital encryption.

This is not only dependent upon architectural guidelines, but also an element of sustainability. When we travel in this digital world, we consume energy. And this energy element should be considered when upgrading such a system; how much energy must we consume while making this area secure? In short, it is a lot, and it's thanks to the Quantum Computer. This type of computer can be unbelievable fast in its' calculations. The Quantum Computer may

All this is in line with activities from the IATA, the International Air Transport Association, which has, of course, a requirement to further digitalize the passenger facilitation. They are working currently on a contactless travelling system, which makes the whole journey for a traveler digitalized from the check-in at home (there is no airport check-in counter), to a kiosk, luggage drop-off, and security check. Next step is the entry/exit section, which is government controlled, and then on to boarding. There is a need for digitalization to encourage and facilitate such self-service within the process.

As a solution supplier, Mühlbauer gets asked from governments and clients for Requests for Information (RFI) and Request for Proposals (RFP) that pertain to new systems and the upgrading of current systems. It is currently very hard to incorporate design sections that pertain to PQC when we have so little idea of the time frame involved in the wide-scale introduction and adoption of quantum computers. These RFI's and RFP's are not only focused upon travel documents and their future digitalization. Here at Mühlbauer, we see a continuous trend for mobile driving licenses based on the ISO 1813-5. There's another ISO in development – DTC and LDS, and in the European Union, an initiative for Trusted E-Services, eIDAS, and finally the e-Wallet. Everything together in one hand.

We can, and will, interact more and more with digital services, but will it remain safe under the shadow of quantum computers? When we come to an architecture, PKI is really the trust anchor (the private key). The private key is always stored in the so-called HSM, (High Secure Module). We have different components in the PKI such as the CSCA, the country signer, country authority, and the document signer, which is very important for the issuance of the electronic documents. It doesn't matter if it's digital or mobile.

These very specific components are needed. When the current algorithms are, let's say, violated and cannot be used any longer, then we have to consider the replace of these components because the HSMs, as long as we know, may not be easily upgraded somehow. They would have to be replaced. Both for the master list and the variation list signer that is also within the HSM.

## What does this mean in terms of timelines?

When a government entity is working on a tender, we usually see that two or three years is not too long to issue this tender and Request for Proposal. Looking at a fictitious timeline we could say that a tender is published in 2025. Tender processes can take somewhere between six months to one year. So now arrive in 2026. And then the implementation timeline could be between 6 months to 12 months – brining us to 2027, and with a 5 to 10 years' timeline. And then we are easily in the middle of 2030 and the customer will ask, what is your strategy, your architecture, to be PQC protected? Are you able to upgrade the system? Are you able to update the system? These are difficult questions to answer at this point in time.

However, the fundamental starting point for these questions lies with the architecture. It means working with other technology providers from the chip supplier, the HSM supplier manufacturer, all the way to the security infrastructure, because all the components which handle the digital signature and encryptions, get affected by design. We believe that this will not stop because the industry and the market is calling for more and more digitalization – or more self-services.

## But what does that really mean?

It means having discussions with the relevant parties now, on upgrading digital mobile documents with PQC-proven chips and secure elements. It means working with partners in the near future on upgrading personalization systems from machine to the issuing system, to support PQC and then upgrading the inspection system in total. This will require a new generation of high secure modules, upgraded algorithms for secure communication between the involved system components, and planning for new projects now which will have to run over the next 10 years to be ready for PQC.

As a solutions provider, our clients expect us to be informed about these upcoming changes. It is vital that there is co-operation between interested parties in this field to develop proof of concept papers, field trials and use every platform available to convince audiences those solutions based on Quantum Computers, Quantum Cryptography and Post-Quantum Cryptography are not a fad but an oncoming reality.

Because each of our human identities in any government system is the biggest asset that we, as individuals have. We have to do everything we can to protect it. ☒