



**Francisco José Vial-Prado**  
**Staff Cryptography Engineer - Fortanix**  
*Fortanix*  
*High Tech Campus 5*  
*5656 AE Eindhoven, The Netherlands*  
*+31850608282*

**Recommendation for Mr. Étienne Richard**

August 26, 2024

To whom it may concern,

It is my pleasure to recommend Mr. Étienne Richard **in the strongest terms**. Without any reservation, he was an exceptional addition to our cryptography team.

My name is Francisco José Vial-Prado. I have 7 years of experience working in applied cryptography. I currently work as Senior Cryptography Engineer for Fortanix, where we have the mission of securing data with state-of-the-art algorithms, using cryptographic modules we implement and maintain.

Mr. Richard was hired in June 2024 for a three-month internship within our cryptography team. In this internship, Mr. Richard was tasked with the implementation of ML-DSA, one of the first digital signature standards for post-quantum cryptography. During this mission, he displayed remarkable talent and discipline.

ML-DSA is a complex algorithm that requires deep understanding of lattices, polynomial rings, and delicate implementation details outlined in FIPS 204. Apart from designing the cryptographic module itself, the mission also included integration with our products – this implies documentation, incorporation to existing codebases, API reviews, and end-to-end testing.

During his internship, Mr. Richard produced a solid ML-DSA implementation in Rust which I reviewed myself. His implementation is secure against known side-channel attacks, avoids common pitfalls, and has comparable performances to the reference implementations by the CRYSTALS suite authors. Additionally, he fully integrated his implementation with our existing codebase and APIs, providing thorough documentation and answering engineering questions from the team. It is also noteworthy that, while testing interoperability, Mr. Richard reported errors in third-party ML-DSA implementations.

Through and through, it was a pleasure working with Mr. Richard. I am confident he will be a great fit to your project.

Please do not hesitate to contact me at [francisco.vialprado@fortanix.com](mailto:francisco.vialprado@fortanix.com), I will happily elaborate further on my time working with Mr. Richard.

Sincerely,

**Francisco José Vial-Prado**  
**Staff Cryptography Engineer - Fortanix**