

PSA Certified Spotlight

Veridify



psacertified™
level one

PSA Certified Level 1

DOME Client Library

Certified Security for a Security Solution

Low-resource processors powering the internet of things (IoT) require highly efficient authentication and data protection solutions that use public key (asymmetric) methods. Veridify Security addresses this need with quantum-resistant security solutions suitable for the smallest Arm Cortex-M0 processors and has achieved PSA Certified Level 1 for its DOME Client Software Library, part of the company's DOME (Device Ownership Management and Enrollment) solution.

The certified configuration includes the DOME Client running on the STMicroelectronics STM32L5 hardware (which is also PSA Certified Level 1 and PSA Certified Level 2) built on the Arm Mbed OS to create a safe and secure IoT platform.

"When it comes to security, the challenge has always been how to deploy effective lightweight crypto on small devices like wearables, actuators, or smart appliances," explains Louis Parks, chairman and CEO of Veridify. "And as wireless protocols and connected platforms demand even more security, there are many real-world examples of where even well-recognized crypto will not fit to prevent hacking. Growing connectivity makes how you implement security even more important and trusted implementations is the value of being PSA Certified. The PSA Certified approach to security is critical to building a trusted environment."

"Our PSA Certified product is a security offering, so by its nature, it must already meet a high security standard. But without question, PSA Certified delivers a better product by giving developers using PSA Certified Level 1 or higher solutions a road map to a more trusted deployment."

Louis M. Parks
CEO and Chairman, Veridify

Holistic View of Security

When Veridify looked at PSA Certified, the program's main security principles and goals reflected the company's similar holistic view on security so it was already well aligned with the PSA Certified approach. The key security considerations for the DOME Client are that a DOME-enabled product shall never communicate with any other device without first authenticating that device is authentic using a cryptographic method that provides at least 128-bit security and that a DOME product shall never communicate with any other device without encrypting the data exchanged between the devices. PSA Certified specifies the same security goal and served as a model for the DOME Client to follow.

"PSA Certified is important because of the architectural component and layered approach to implementation," Parks says. "We chose to certify DOME on an STMicroelectronics certified processor running the Arm Mbed OS which is already accredited using the PSA Functional APIs and API extensions. PSA Certified is a very strict review process that very succinctly describes what is certified and on what platform and that lets us market our solution as a trusted environment."



Powerful Third-Party Endorsement

The Veridify team worked on PSA Certified with the Brightsight test lab over a three-month period, an investment that Parks believes is a powerful endorsement of the DOME solution's value.

"We talk to a lot of entities who know they need security and want to do it, but don't have the knowledge base to implement trusted tools," Parks explains. "Security tends to be a bit of the Wild West with companies producing numerous white papers to prove they can be trusted. Not only does PSA Certified offer third-party validation, but it provides a growing platform within the PSA Certified program with opportunities for strategic alignment."

Parks is confident that PSA Certified will help speed adoption of its DOME solution and plans to certify other solutions, as well as pursue additional PSA Certified collaborations.

"Our PSA Certified product is itself a security offering, so by its nature, it must already meet a high security standard," he adds. "But without question, PSA Certified delivers a better product by giving developers using PSA Certified Level 1 or higher solutions a road map to a more trusted deployment."

