Which IoT board?

To show off our IoT potential we need to pick on a suitable board. We are currently using an Arduino 33 IoT board which has an ARM M0+ processor clocked at 48MHz, and 256K of flash and just 32K of SRAM. A demo of our TLS1.3 client just about fits and successfully executes.

But there is no point in shoe-horning our TLS1.3 capability into the tiniest possible space, leaving no room for an application to use it. That kind of show-boating is quite common in the crypto world, but pointless in the real world. And there is no point either in using something which is too big, like a Raspberry Pi which runs full Linux and has gigabytes of memory and major CPU fire-power – but cannot reasonably be powered by a battery.

So what else is out there?

What do we need.

I would suggest that we need a micro-controller board with a minimum of 4M of flash memory, and 256K of SRAM. At the moment we are a comfortable fit inside of that, and I think we should aim for TLS1.3 to occupy no more than about 15% of a boards capacity. A lot of our client size is down to our store of CA root certificates, but in a real deployment we can cut that right back. From recent researches I conclude that lattice-based PQ crypto is not very CPU intensive but does require more SRAM. We would also like the board to be cheap and well-known. It would be nice if it had some hardware crypto/hashing support.

And the winner is...

The Raspberry Pi Pico https://www.raspberrypi.com/products/raspberry-pi-pico/. No I hadn't heard of it either. It has a dual core ARM M0+ clocked at 133MHz and 264K of SRAM, and it costs $4.

It is also available in a nice Arduino form factor, the Arduino Nano RP2040 - https://store-usa.arduino.cc/products/arduino-nano-rp2040-connect-with-headers which adds 16M of flash, WiFi and a crypto co-processor. The relative weakness of the processor is offset by the impressive clock speed. And being dual core – well that is interesting.

And being a Raspberry Pi device it also comes with an awesome software ecosystem. Based on the fact that the RP2040 is currently out of stock from most suppliers, it seems to be quite popular.

I want one!