
FIPS 140-2 Certificate Statistics for Q1 2018



April 2, 2018

This report may be freely shared

Prepared by *KeyPair Consulting Inc.*

Introduction

In this report, we take a look at the FIPS 140-2 certificates issued by the CMVP in the first quarter of 2018. For historical information, summary graphs for the years 2013-2017 are included.

About KeyPair Consulting Inc

Mark Minnoch and Steve Weymann are Co-Founders of KeyPair Consulting Inc. and creators of this report.

With over two decades of combined experience and hundreds of successful FIPS validations, KeyPair Consulting Inc. expertly guides technology companies in achieving their FIPS goals.



Mark Minnoch



Steve Weymann

Get In Touch

Please contact KeyPair Consulting Inc. at +1 (805) 316-5024 or mark@KeyPair.us

Our dramatically superior service will squash your FIPS pains.

FIPS Certificates for Q1 2018

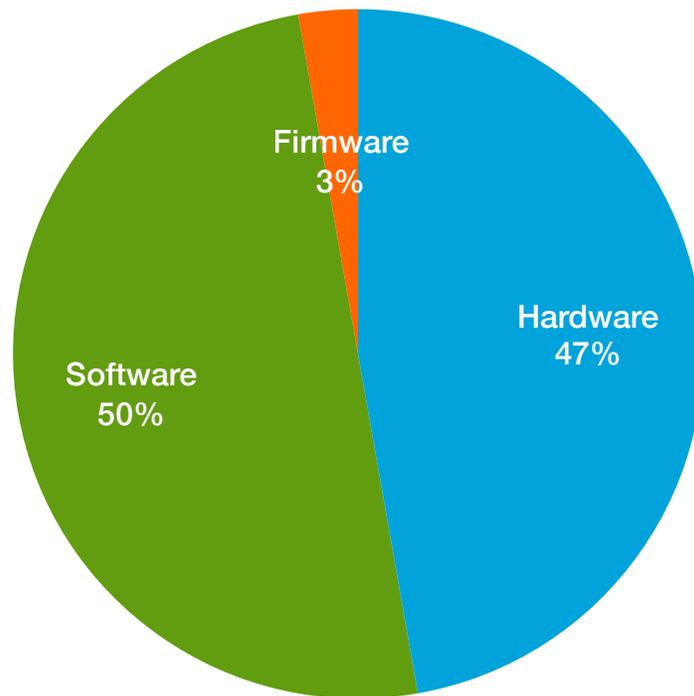
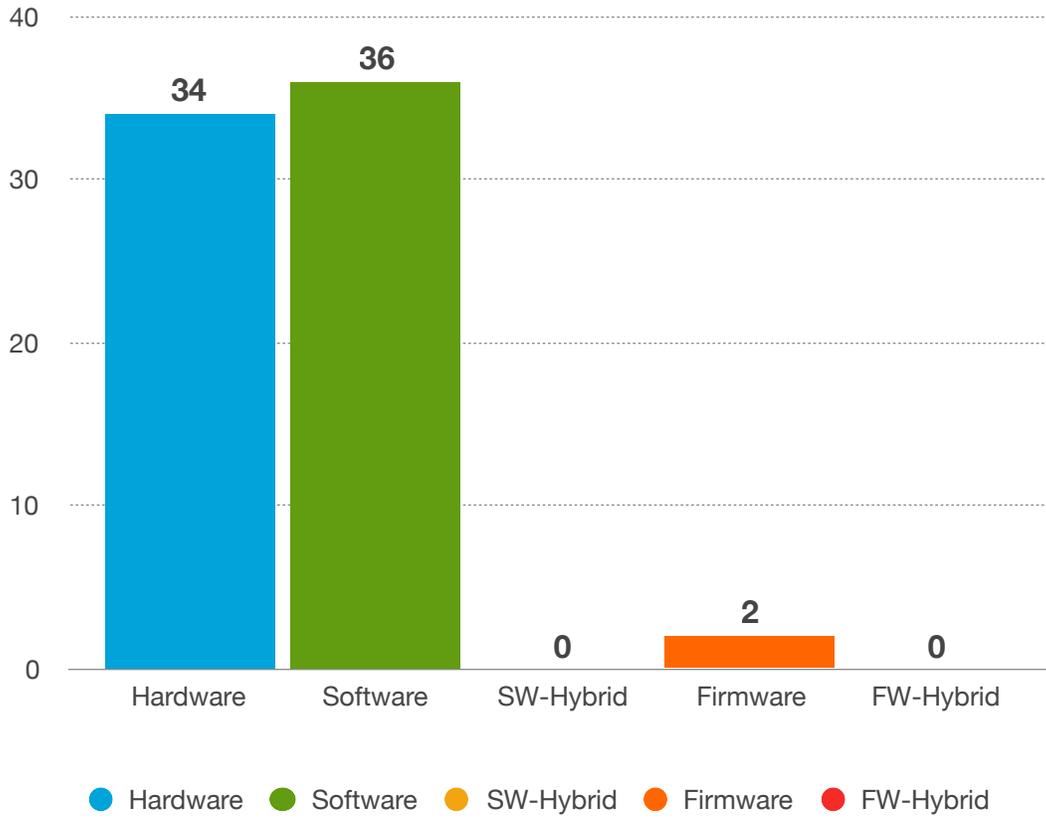
For Q1 2018, the following trends are interesting:

- **Software-only Modules.** The percentage of **software modules receiving FIPS 140-2 certificates is 50%**, significantly higher than the 5 year average of 33% (in 2017, software modules made up 39% of the total).
- **Level 1 Modules.** The percentage of **Level 1 modules receiving FIPS 140-2 certificates is 68%**, significantly higher than the 5 year average of 48% (in 2017, Level 1 modules made up 53% of the total).
- **Total number of FIPS Certificates issued in Q1 2018 is 72.** This is the ahead of the Q1 2017 total of 62.
- **Historical Validation Status.** Of the 21 modules from 2017 that were moved to the “Historical” list in 2018, 11 have returned to the “Active” list.

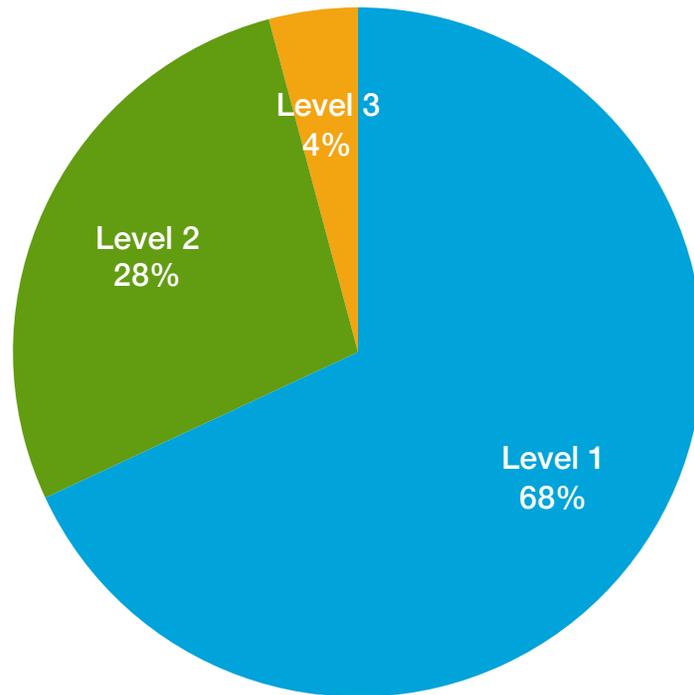
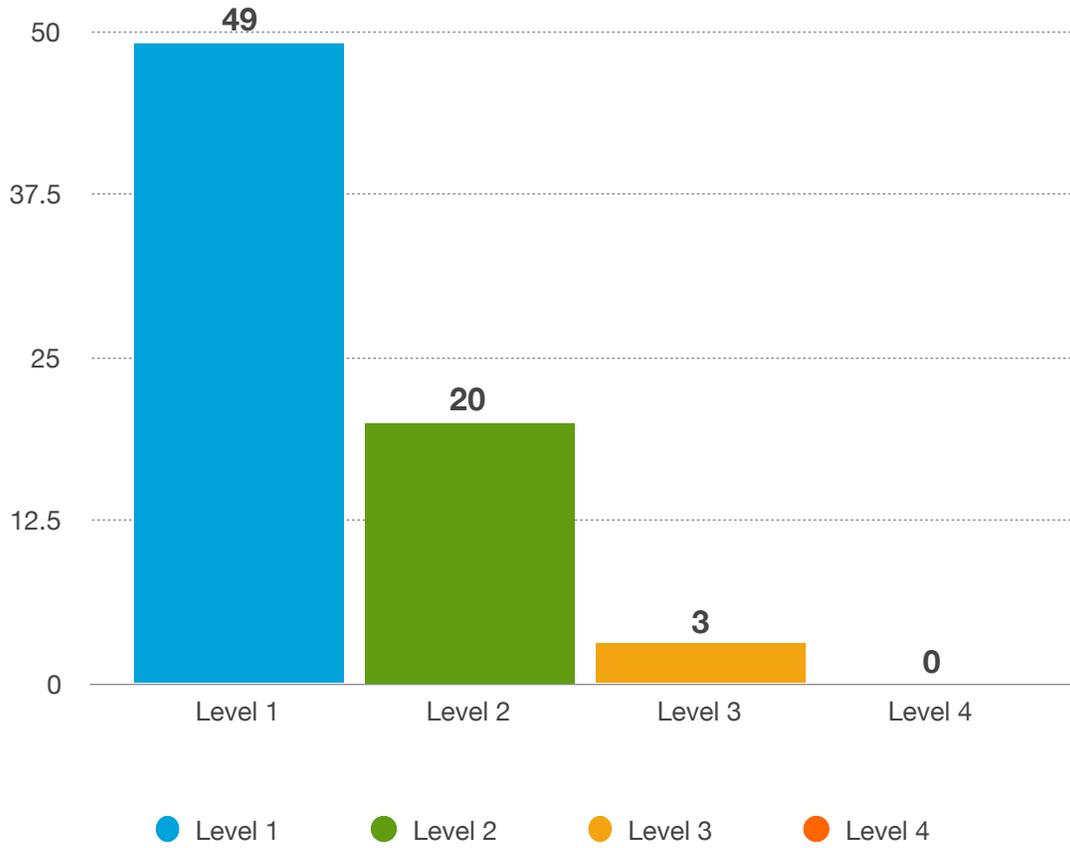
Creating this report is time intensive and requires some manual effort. Much care and love went into ensuring the accuracy of the information. KeyPair Consulting will correct any errors you find. The compensation for any reported errors shall not exceed the price of an adult beverage at the ICMC 18 conference.

You may share this report freely.

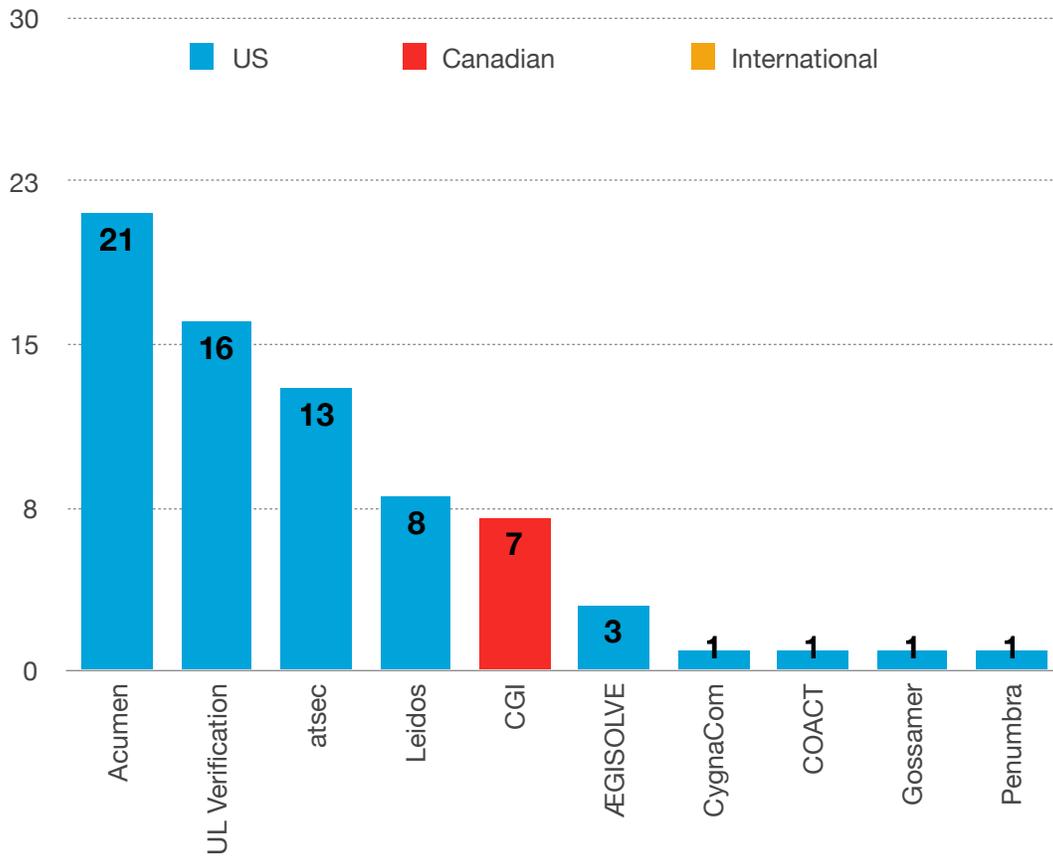
Certificates by Module Type Q1 2018



Certificates by Security Level Q1 2018



Certificates by Lab Q1 2018

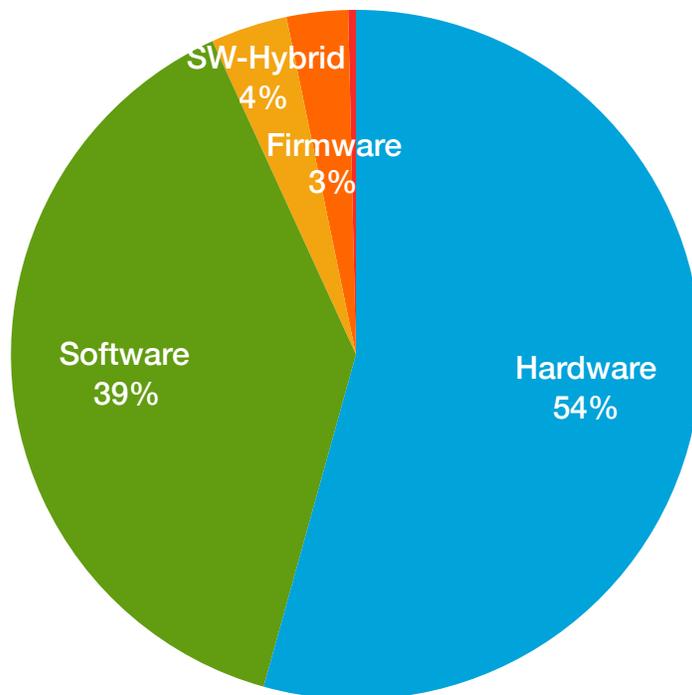
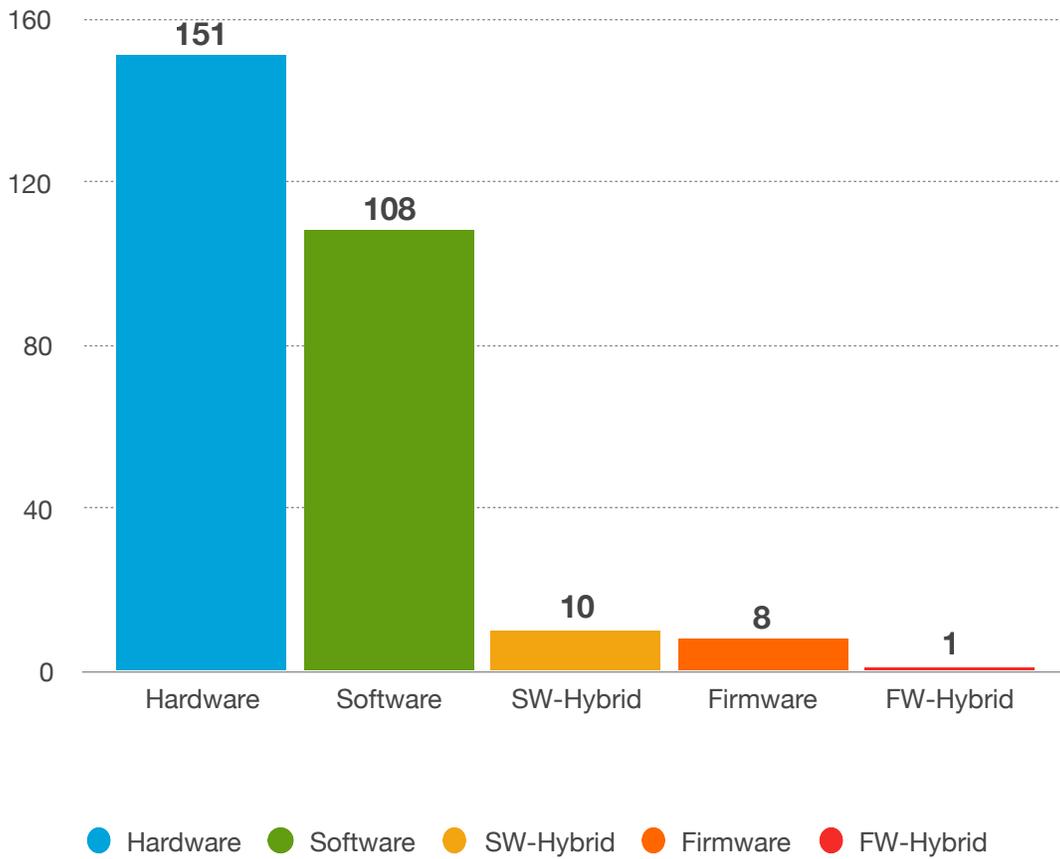


Highlights for 2017

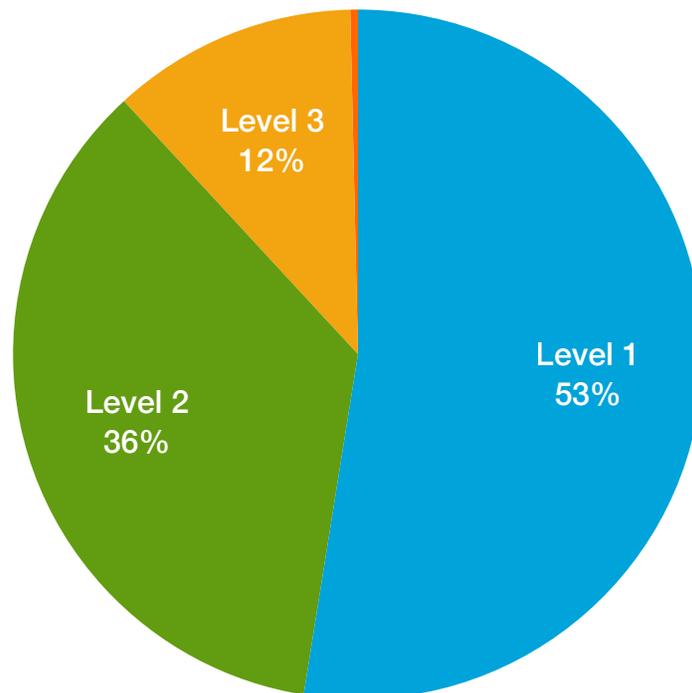
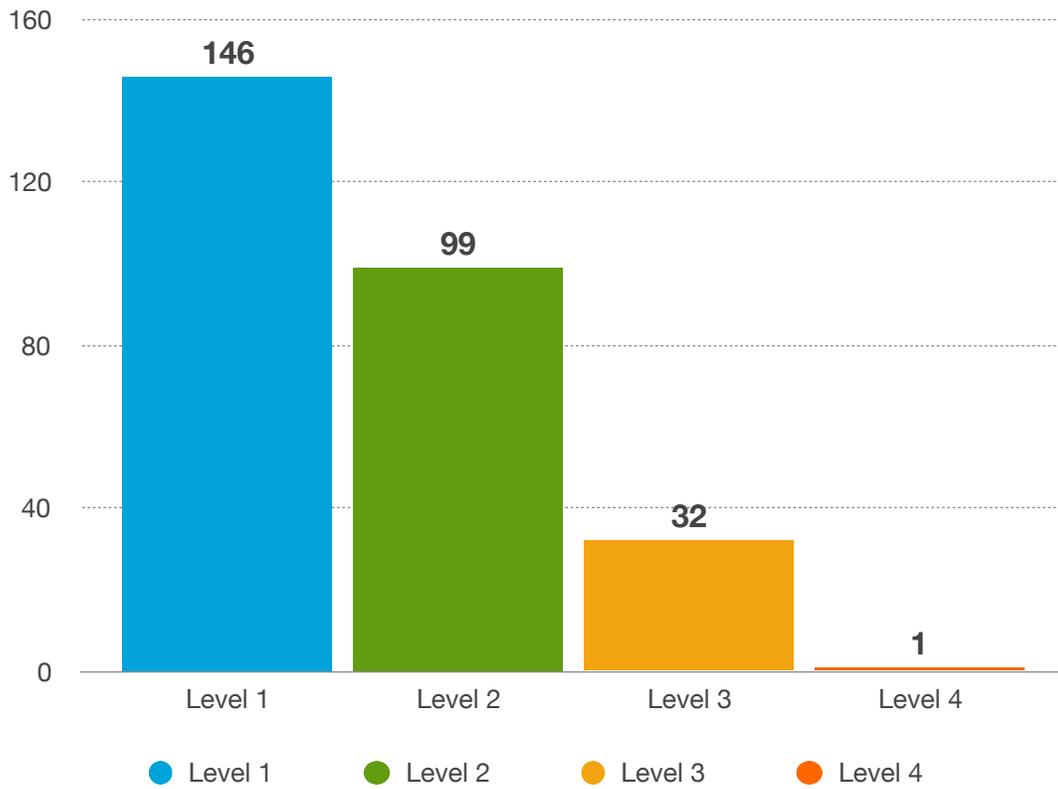
For 2017, the following trends are note worthy:

- **Software-only Modules.** The percentage of software modules receiving FIPS 140-2 certificates is increasing. **In 2017, software modules accounted for 39% of the total.** The five year running average is 33% .
- **Level 1 Modules.** As we would expect, the increase in software modules is also driving up the percentage of Level 1 modules receiving FIPS 140-2 certificates. **In 2017, Level 1 modules made up 53% of the total.** The five year running average is 48%.
- **Total number of FIPS Certificates.** The number of **FIPS 140-2 certificates for 2017 was 278.** This is the second most number of certificates posted in a year (the record year in 2016 was 294 FIPS certificates posted).

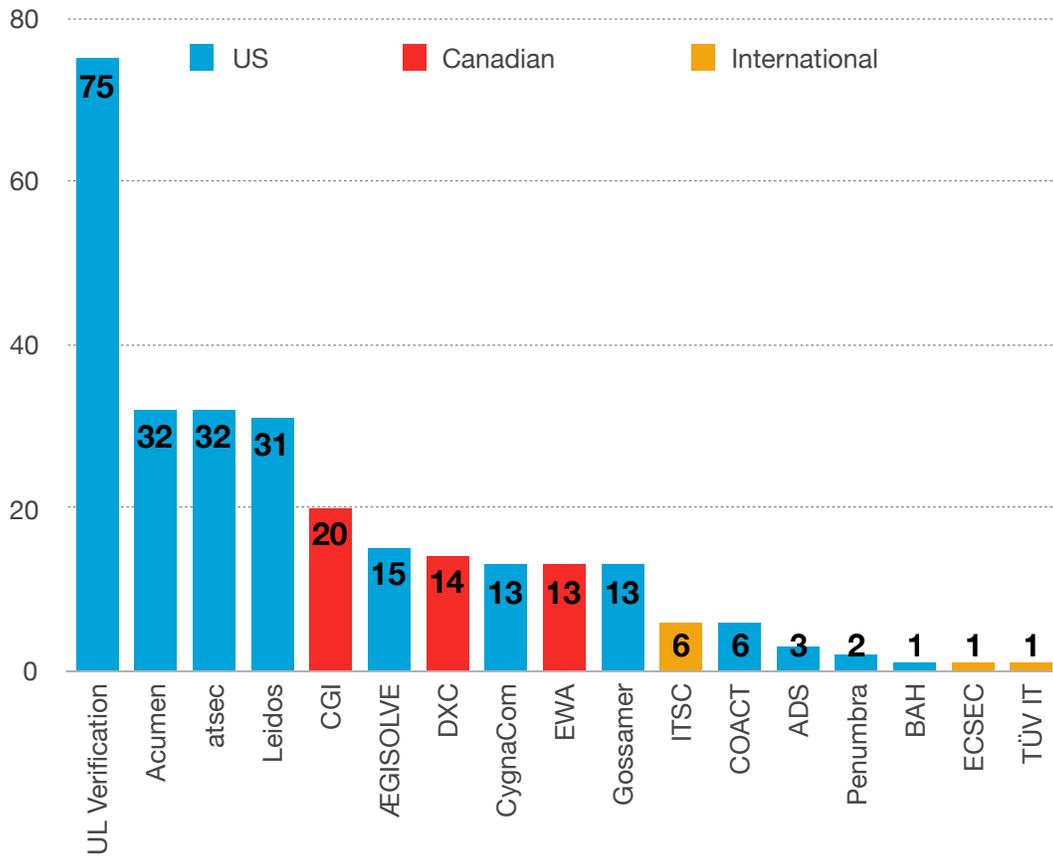
Certificates by Module Type 2017



Certificates by Security Level
2017

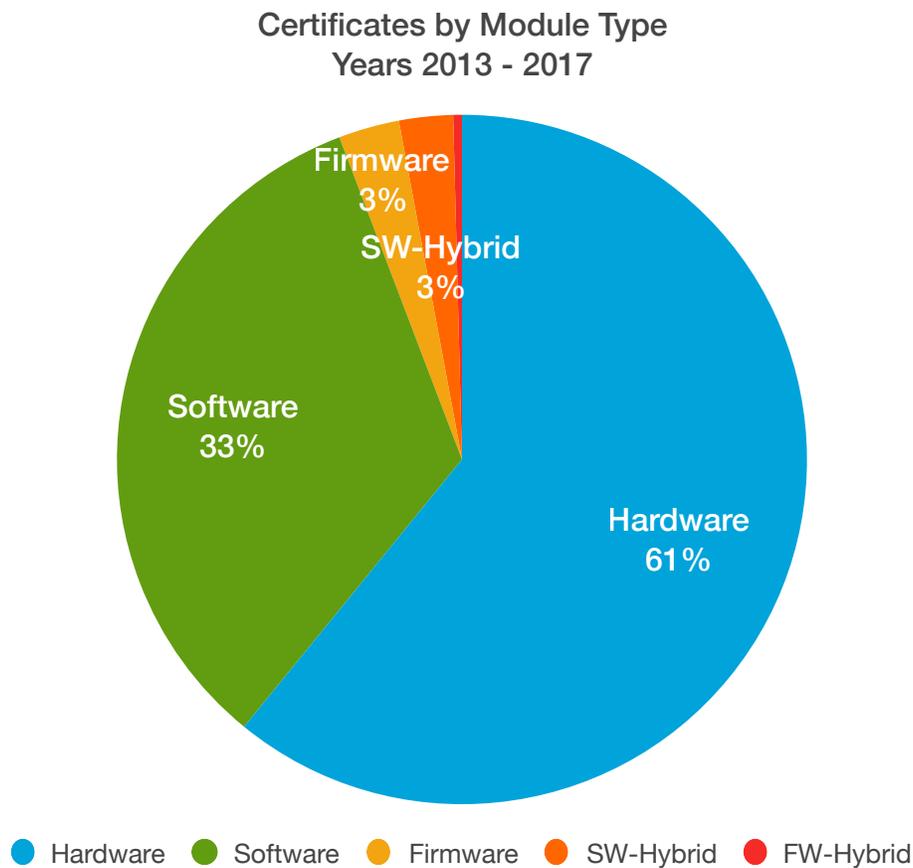


Certificates by Lab 2017



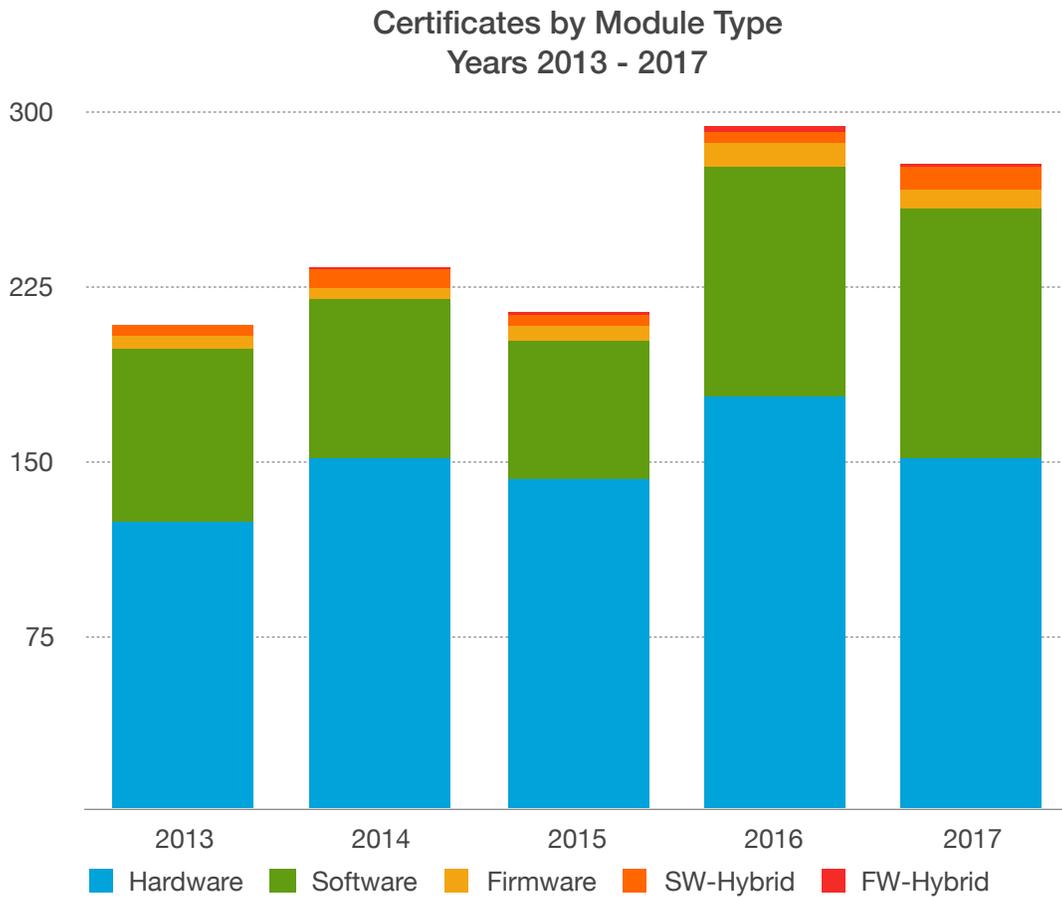
Statistics for 2013-2017

This section contains FIPS 140-2 Program trending information for the five years between 2013 and 2017.



For the five year period including 2013 and 2017, **61%** of all FIPS 140-2 validated cryptographic modules were **hardware**. Software modules accounted for 33% of the cryptographic modules validated.

In the *Certificates by Module Type (2017)* chart (earlier in this report), the percentage of **software modules shows an increasing trend to 39%**.

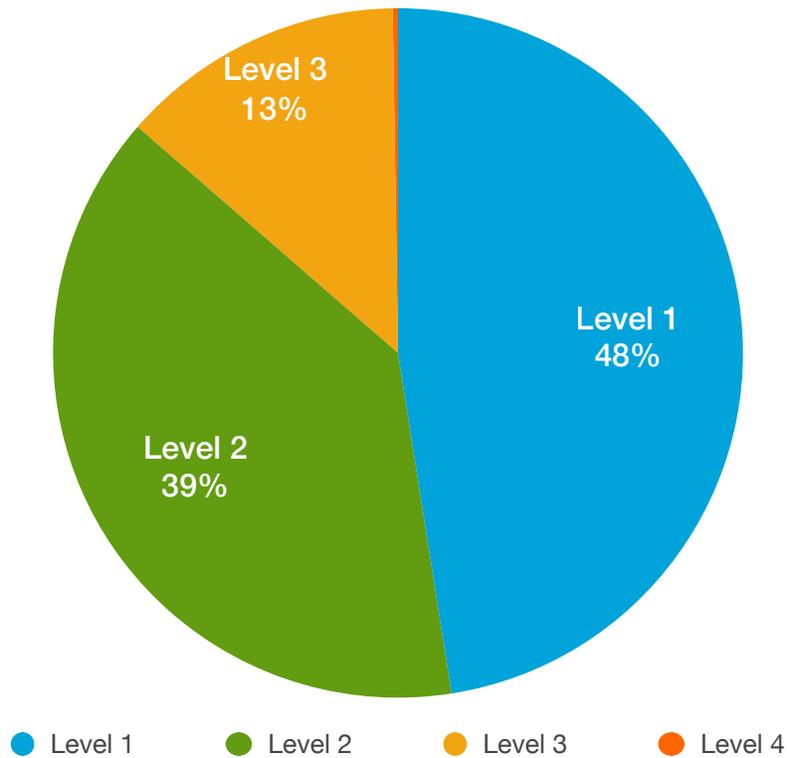


For the five year period including 2013 and 2017, an **average of 245** cryptographic modules were validated by the CMVP **each year**.

The CMVP issued 278 FIPS 140-2 certificates in 2017 – the second most of any year in the program history.

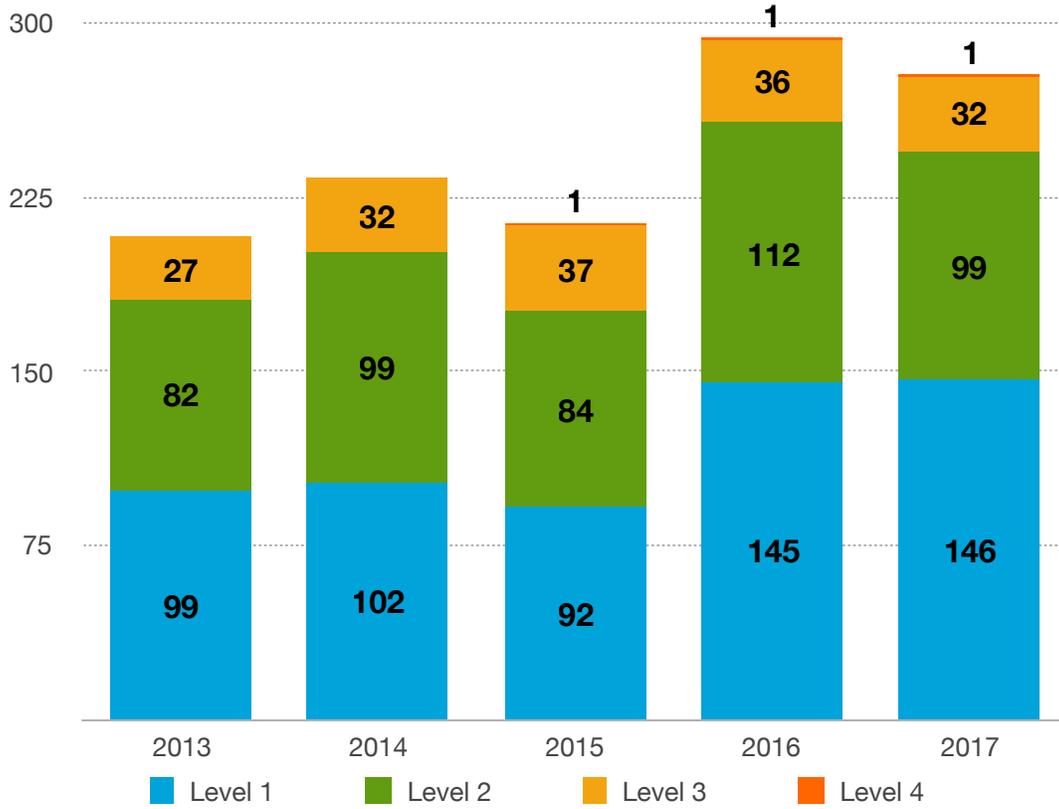
In 2016, the CMVP set the record number of certificates issued with 294.

Certificates by Security Level Years 2013 - 2017

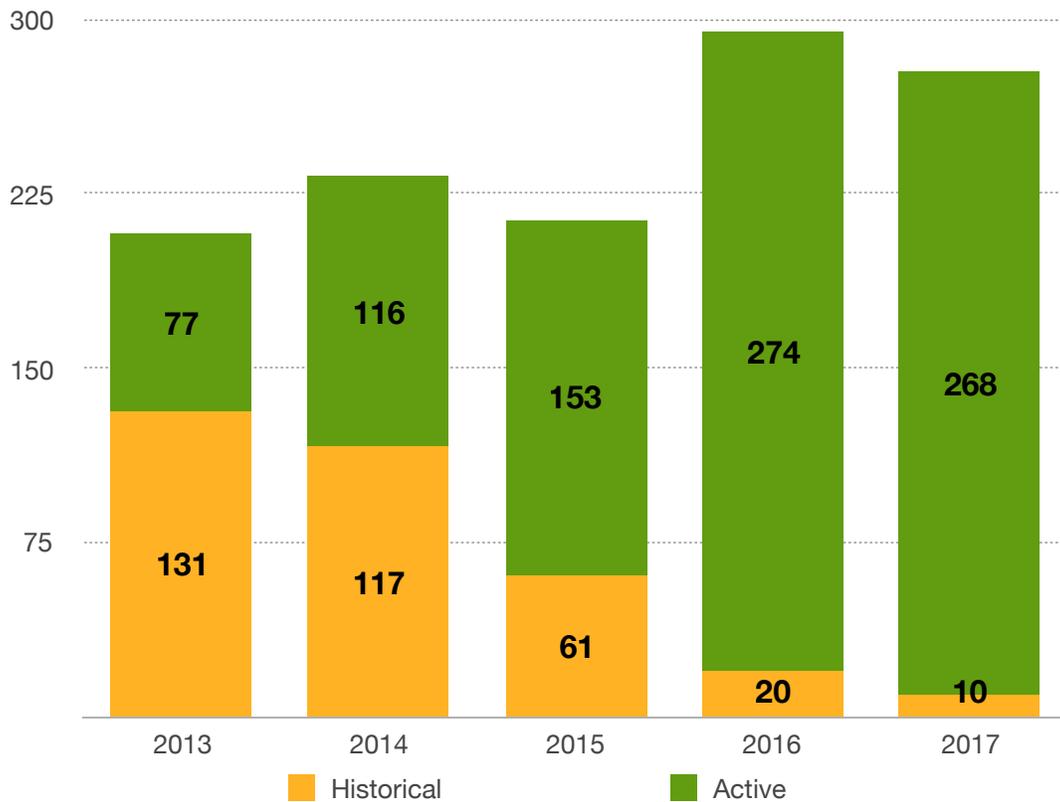


For the five year period including 2013 and 2017, **48%** of all FIPS 140-2 validated cryptographic modules were **Security Level 1**.

Certificates by Security Level Years 2013 - 2017



Certificates by Validation Status Years 2013 - 2017



The *Certificates by Validation Status* chart above shows the break down of modules that are currently “Active” and those that have been moved to the Historical list. No modules have been revoked during the years 2013 to 2017.

As a reminder, the CMVP makes the following statement about modules with a Historical Validation Status:

Historical - The referenced cryptographic module should not be included by Federal Agencies in new procurements. Agencies may make a risk determination on whether to continue using this module based on their own assessment of where and how it is used.

Thank you for reading our report. Our contact information is on page 2.
