

**CONTACT:** Anne Price, PR Works, Inc.  
+1-602-330-6495  
[anne@prworksonline.com](mailto:anne@prworksonline.com)  
Twitter: @TrustedComputin

## **Trusted Computing Group Announces New Work Group To Address Security In Persistent Memory**

**SANTA CLARA, Calif., August 8, 2016** – Trusted Computing Group has announced here at the Flash Memory Summit a new work group to develop industry standards and specifications for persistent memory to prevent data theft and attacks, especially in data centers.

TCG previously has developed widely adopted standards for self-encrypting drives, or [SEDs](#), that are used in almost all new solid state drives and enterprise storage devices, as well as in most hard disk drives and many USB drives.

Persistent memory, storage class memory, and NVDIMMs are emerging technologies that create new concerns about the security of data at rest. Without security protections, data stored in these devices can be vulnerable to various attacks and require support for instant erase, for example. As it has with its SED standards for storage, TCG will work closely with related memory technology groups to ensure integration of the TCG specifications with other standardization activities related to persistent memory, storage class memory and NVDIMMs.

“We are excited to announce the TCG Persistent Memory Work Group to bring greater security to these new memory architectures and designs. Familiar security risks are faced by the non-volatile elements, and we plan to address those issues through a standards-based approach, which will benefit developers, users and customers of the technology”, TCG Executive Director Mark Schiller.

TCG welcomes industry participation and support for the persistent memory standards work. More info on membership can be seen at <http://www.trustedcomputinggroup.org/membership/>.

During this week’s Flash Memory Summit, TCG members Drive Trust Alliance, Micron and ULink will demonstrate self-encrypting storage in enterprise, client and Internet of Things applications. Member experts also will participate in sessions addressing encryption and related applications, including Session 103-A: Security in a Flash! (Security Track) and Session 104-A: Privacy Versus (In)security: Who Should Win and Why Between Apple and the FBI?. Members also can discuss TCG membership

benefits. More information on TCG at the summit can be found at <http://www.trustedcomputinggroup.org/event/flash-memory-summit/>.

### **About TCG**

More information and TCG's specifications and work groups are available at the Trusted Computing Group's website, [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org). Follow TCG on [Twitter](#) and on [LinkedIn](#).

-- 30 --

Brands and trademarks are the property of their respective owners.

**Tweet this:** Persistent memory=security concerns. @TrustedComputin forms new WG to secure data at rest for emerging technologies  
<http://ow.ly/o2LU3032vR7>